UNITED STATES
SECURITIES AND EXCHANGE COMMISSION
Washington, D.C. 20549
FORM 10-K

(Mark One)

☑ **ANNUAL REPORT PURSUANT TO SECTION 13 OR 15(d) OF THE SECURITIES EXCHANGE ACT OF 1934**

For the fiscal year ended January 31, 2020

or

☐ **TRANSITION REPORT PURSUANT TO SECTION 13 OR 15(d) OF THE SECURITIES EXCHANGE ACT OF 1934**

For the transition period from_____ to_____

Commission file number: 001-37748

SecureWorks Corp.

(Exact name of registrant as specified in its charter)

Delaware	**27-0463349**
(State or other jurisdiction of incorporation or organization)	(I.R.S. Employer Identification No.)

One Concourse Parkway NE Suite 500, Atlanta, Georgia 30328
(Address of principal executive offices) (Zip Code)

Registrant's telephone number, including area code: **(404)327-6339**
Securities registered pursuant to Section 12(b) of the Act:

Title of each class	Trading Symbol(s)	Name of each exchange on which registered
Class A Common Stock, par value $0.01 per share	**SCWX**	**The Nasdaq Stock Market LLC (Nasdaq Global Select Market)**

Securities registered pursuant to Section 12(g) of the Act: **None**

Indicate by check mark if the registrant is a well-known seasoned issuer, as defined in Rule 405 of the Securities Act. Yes ☐ No ☑

Indicate by check mark if the registrant is not required to file reports pursuant to Section 13 or Section 15(d) of the Act. Yes ☐ No ☑

Indicate by check mark whether the registrant (1) has filed all reports required to be filed by Section 13 or 15(d) of the Securities Exchange Act of 1934 during the preceding 12 months (or for such shorter period that the registrant was required to file such reports), and (2) has been subject to such filing requirements for the past 90 days. Yes ☑ No ☐

Indicate by check mark whether the registrant has submitted electronically every Interactive Data File required to be submitted pursuant to Rule 405 of Regulation S-T during the preceding 12 months (or for such shorter period that the registrant was required to submit such files). Yes ☑ No ☐

Indicate by check mark whether the registrant is a large accelerated filer, an accelerated filer, a non-accelerated filer, smaller reporting company, or an emerging growth company. See the definitions of "large accelerated filer," "accelerated filer," "smaller reporting company," and "emerging growth company" in Rule 12b-2 of the Exchange Act.

Large accelerated filer	☐	Accelerated filer	☑
Non-accelerated filer	☐	Smaller reporting company	☐
		Emerging growth company	☑

If an emerging growth company, indicate by check mark if the registrant has elected not to use the extended transition period for complying with any new or revised financial accounting standards provided pursuant to Section 13(a) of the Exchange Act. ☑

Indicate by check mark whether the registrant is a shell company (as defined in Rule 12b-2 of the Exchange Act). Yes ☐ No ☑

As of August 2, 2019, the last business day of the registrant's most recently completed second fiscal quarter, the aggregate market value of the registrant's common stock held by non-affiliates was approximately $128.9 million (based on the closing price of $11.51 per share of Class A common stock reported on the Nasdaq Global Select Market on that date).

As of March 26, 2020, there were 81,523,081 shares of the registrant's common stock outstanding, consisting of 11,523,081 outstanding shares of Class A common stock and 70,000,000 outstanding shares of Class B common stock.

DOCUMENTS INCORPORATED BY REFERENCE

The information required by Part III of this report, to the extent not set forth herein, is incorporated by reference from the registrant's proxy statement relating to the annual meeting of stockholders in 2019. Such proxy statement will be filed with the Securities and Exchange Commission within 120 days after the end of the fiscal year to which this report relates.

TABLE OF CONTENTS

CAUTIONARY NOTE REGARDING FORWARD-LOOKING STATEMENTS

This report contains "forward-looking statements" within the meaning of Section 27A of the Securities Act of 1933 and Section 21E of the Securities Exchange Act of 1934. The words "may," "will," "anticipate," "estimate," "expect," "intend," "plan," "aim," "seek" and similar expressions as they relate to us or our management are intended to identify these forward-looking statements. All statements by us regarding our expected financial position, revenues, cash flows and other operating results, business strategy, legal proceedings, and similar matters are forward-looking statements. Our expectations expressed or implied in these forward-looking statements may not turn out to be correct. Our results could be materially different from our expectations because of various risks, including the risks discussed in this report under "Part I – Item 1A – Risk Factors" and in our other periodic and current reports filed with the Securities and Exchange Commission. Any forward-looking statement speaks only as of the date as of which such statement is made, and, except as required by law, we undertake no obligation to update any forward-looking statement after the date as of which such statement was made, whether to reflect changes in circumstances or our expectations, the occurrence of unanticipated events, or otherwise.

Except where the context otherwise requires or where otherwise indicated, all references in this report to "Secureworks," "we." "us," "our" and "our company" refer to SecureWorks Corp. and our subsidiaries on a consolidated basis, and all references to "Dell" refer to Dell Inc. and its subsidiaries on a consolidated basis.

Our fiscal year is the 52- or 53-week period ending on the Friday nearest January 31. Our 2020 fiscal year ended on January 31, 2020, our 2019 fiscal year ended on February 1, 2019, and our 2018 fiscal year ended on February 2, 2018.

Part I

Item 1. Business

Overview

We are a leading global provider of technology-driven information security solutions singularly focused on protecting our customers from cyber attacks. We combine deep experience from service to thousands of customers, machine learning and automation from our proprietary technology, and actionable insights from our team of elite researchers, analysts, and consultants to create a powerful network effect that provides increasingly strong protection for our customers. By aggregating and analyzing data from various sources around the world, we prevent security breaches, detect malicious activity in real time, respond rapidly and predict emerging threats.

Our vision is to be the essential cybersecurity company for a digitally connected world. Through our vendor-neutral approach, we create integrated and comprehensive solutions by proactively managing the collection of "point" products deployed by our customers to address specific security issues and provide supplemental solutions where gaps exist in our customers' defenses. We seek to provide the right level of security for each customer's unique situation, which evolves as the customer's organization grows and changes.

We have pioneered an integrated approach that delivers a broad portfolio of information security solutions to organizations of varying size and complexity. Our flexible and scalable solutions support the evolving needs of the largest, most sophisticated enterprises staffed with in-house security experts, as well as small and medium-sized businesses and government agencies with limited in-house capabilities and resources.

Our solutions enable organizations to:

- prevent security breaches by fortifying their cyber defenses,
- detect malicious activity,
- respond rapidly to security breaches, and
- predict emerging threats.

Our solutions leverage the proprietary technologies, processes and extensive expertise and knowledge of the tactics, techniques and procedures of the adversary that we have developed over more than 21 years. Key elements of our strategy include:

- maintain and extend our technology leadership,
- expand and diversify our customer base,
- deepen our existing customer relationships, and
- attract and retain top talent.

Our technology-driven information security solutions offer an innovative approach to prevent, detect, respond to and predict cybersecurity breaches. Through our managed security solutions, which are largely sold on a subscription basis, we provide global visibility and insight into malicious activity, enabling our customers to detect and effectively remediate threats quickly.

In fiscal 2020, we launched our first software-as-a-service application, Red Cloak Threat Detection and Response (TDR) and related Managed Detection and Response (MDR) powered by Red Cloak. This application gives customers visibility across their entire environment, applies advanced analytics developed using machine and deep learning on diverse data from a wide range of sources, and leverages workflows designed using our 21 years of security operations expertise and integrated

orchestration and automation capabilities that increase the speed of response actions. Threat intelligence, which is typically deployed as part of our managed security solutions, delivers early warnings of vulnerabilities and threats along with actionable information to help prevent any adverse impact.

In addition to these solutions, we also offer a variety of services, which includes security and risk consulting and incident response to accelerate adoption of our capabilities. Through security and risk consulting, we advise customers on a broad range of security and risk-related matters. Incident response minimizes the impact and duration of security breaches through proactive customer preparation, rapid containment and thorough event analysis followed by effective remediation. We have a single organization responsible for the delivery of our security solutions, which enables us to respond quickly to our customers' evolving needs and help them secure themselves against cyber attacks.

As of January 31, 2020, we served a customer base of approximately 5,200 customers, including 4,100 subscription customers, across 52 countries. Our success in serving our customers has resulted in consistent recognition of our company as a market leader in managed security solutions by leading industry research firms.

The fees we charge for our solutions vary based on a number of factors, including the solutions selected, the number of customer devices covered by the selected solutions, and the level of management we provide for the solutions. Approximately 76% of our revenue is derived from subscription-based arrangements, attributable to managed security solutions, while approximately 24% is derived from professional services engagements. As we respond to the evolving needs of our customers, the relative mix of subscription-based solutions and professional services we provide our customers may fluctuate.

Corporate Information

We are a holding company that conducts operations through our wholly-owned subsidiaries. The mailing address of our principal executive offices is One Concourse Parkway NE, Suite 500, Atlanta, Georgia 30328. Our telephone number at that address is (404) 327-6339.

The predecessor company of SecureWorks Corp. was originally formed as a limited liability company in Georgia in March 1999, and Secureworks was incorporated in Georgia in May 2009. In February 2011, Secureworks was acquired by Dell Inc. In November 2015, our company reincorporated from Georgia to Delaware and, in connection with the reincorporation, changed its name from SecureWorks Holding Corporation to SecureWorks Corp. On April 27, 2016, Secureworks completed its initial public offering, or IPO. Upon the closing of the IPO, Dell Technologies Inc., the ultimate parent company of Dell, Inc., owned indirectly through Dell Inc. and Dell Inc.'s subsidiaries no shares of our outstanding Class A common stock and all shares of our outstanding Class B common stock, which as of January 31, 2020 represented approximately 86.2% of our total outstanding shares of common stock and approximately 98.4% of the combined voting power of both classes of our outstanding common stock.

We maintain a corporate Internet website at www.secureworks.com. We make available free of charge through our website our annual reports on Form 10-K, quarterly reports on Form 10-Q, current reports on Form 8-K, and amendments to those reports, as soon as reasonably practicable after we electronically file the reports with, or furnish the reports to, the Securities and Exchange Commission. Information appearing on, or that can be accessed through, our website is not a part of this report.

Industry Background

Increasing cybersecurity challenges have created a large and fragmented market for IT security products and services.

We believe that many organizations that use the information technology, or IT, security products and services available in the market remain vulnerable to cyber attacks because they rely on a collection of uncoordinated "point" products that address specific security issues but fall short in identifying and defending against next-generation cyber threats.

Organizations of all sizes are using new information technologies to make their businesses more productive and effective.

Modern IT infrastructures are growing in complexity and often include a combination of on-premises, cloud and hybrid environments. In addition, the adoption of mobile computing allows access to critical business information from various devices and locations. The widespread adoption of these advanced IT architectures, along with the rapid growth of connected devices and new ways of delivering IT services, enables organizations to benefit from business applications that are more powerful and easier to deploy, use and maintain.

This rapidly evolving IT environment is increasingly vulnerable to frequent and sophisticated cyber attacks.

The evolving landscape of applications, modes of communication and IT architectures makes it increasingly challenging for businesses to protect their critical business assets from cyber threats. New technologies heighten security risks by increasing the number of ways a threat actor can attack a target by giving users greater access to important business networks and information and by facilitating the transfer of control of underlying applications and infrastructure to third-party vendors.

Cyber attacks have evolved from computer viruses written by amateur hackers into highly complex and targeted attacks led by highly-skilled adversaries intent on stealing information or causing financial and reputational damage.

The economic and reputational impact of attacks, coupled with growing regulatory requirements, makes cybersecurity defense increasingly a priority for senior management and boards of directors.

In the wake of numerous high-profile data breaches, organizations are increasingly aware of the financial and reputational risks associated with IT security vulnerabilities. We believe that the cybersecurity programs of most organizations do not rival the persistence, tactical skill and technological prowess of today's cyber adversaries. As a result, cyber attacks are successfully breaching organizations' networks. Security breaches can be highly public and result in reputational damage and legal liability as well as large losses in productivity and revenue. Many organizations are particularly concerned about attacks that attempt to misappropriate sensitive and valuable business information. Adding to the urgency of the IT security challenge, new regulations and industry-specific compliance requirements direct organizations to design, implement, document and demonstrate controls and processes to maintain the integrity and confidentiality of information received and stored on their systems.

The traditional cybersecurity approach of using numerous point products often fails to detect threats and block attacks.

Information systems at many organizations are vulnerable to breach because they rely on a collection of uncoordinated point security products that address security risks in a piecemeal fashion rather than in a proactive and coordinated manner. An effective cyber defense strategy requires the coordinated deployment of multiple products and solutions tailored to an organization's specific security needs. Point products, however, primarily address security issues in a reactive manner by employing passive auditing or basic blocking techniques, and often lack the integration and intelligent monitoring capabilities and management within a common framework necessary to provide effective information security throughout an organization.

Identifying and hiring qualified security professionals are significant challenges for many organizations.

The difficulty in providing effective information security is exacerbated by the highly competitive environment for identifying, hiring and retaining qualified information security professionals.

As a result, organizations engage information security solutions vendors to integrate, monitor and manage their point products to enhance their defenses against cyber threats.

Because many organizations cannot adequately protect their networks from cyber threats, they are augmenting their IT security strategies to include information security solutions. By using these solutions, organizations seek to decrease their vulnerability to security breaches, increase the effectiveness of their existing investments in security products and free their own IT staff to focus on other responsibilities.

Traditional information security solutions vendors, however, often fail to satisfy the IT security needs of organizations, causing many of them to seek the advantages of our solutions.

Many organizations lack sufficient internal cybersecurity expertise to keep pace with the rapidly evolving threat landscape. As a result, these organizations engage the support of information security solutions providers as part of their IT security strategy. However, traditional information security solutions offered by telecommunications providers, security product vendors, large IT outsourcing firms and small regional providers often lack a broad perspective on the threat landscape, are unable to scale their solutions to match organizations' data processing requirements, fail to provide actionable security information, focus only on a subset of organizations' security needs or have limited deployment options.

Our technology-driven information security solutions, as described below, offer an innovative approach to prevent, detect, respond to and predict emerging threats. We believe that our singular focus on providing a comprehensive portfolio of information security solutions focused on protecting our customers from cyber attacks makes us a trusted advisor and an attractive partner for our customers. Our vendor-neutral approach enables our customers to enhance their evolving IT security infrastructure, appliances and best of breed technologies with our solutions and capabilities, which together provide our

customers with the right level of security for their unique situation. This focus enables us to pursue a go-to-market strategy that addresses the diverse needs of our customers around the world.

Our Solutions

Our Counter Threat Platform™ constitutes the core of our technology-driven information security solutions and provides our customers with a powerful integrated perspective regarding their network environments and security threats. Our integrated suite of solutions includes:

- *Managed security*, through which we provide our customers global visibility and insight into malicious activity enabling them to detect and effectively remediate threats quickly
- *Threat intelligence*, through which we deliver early warnings of vulnerabilities and threats, along with actionable information to help prevent any adverse impact
- *Security and risk consulting*, through which we advise our customers on a variety of security and risk-related matters, such as how to design and build strategic security programs, assess and test security capabilities and meet regulatory requirements
- *Incident response*, through which we help our customers minimize the impact and duration of security breaches through proactive customer preparation, rapid containment and thorough event analysis followed by effective remediation

As part of our security and risk consulting solutions, we emphasize cloud security, through which we help customers deliver cloud-based services securely.

Our customers may subscribe to our full suite of solutions or elect to subscribe to various combinations of our individual solutions. All of our solutions are enabled by our Counter Threat Platform and our team of highly-skilled security experts.

Global Visibility. We have global visibility into the cyber threat landscape through our approximately 4,100 subscription-based customers across 52 countries. We are able to gain near real time insights that enable us to predict, detect and respond to threats quickly and effectively. We also are able to identify threats originating within a particular geographic area or relating to a particular industry and proactively leverage this threat intelligence to protect other customers against these threats.

Scalable Platform with Powerful Network Effects. Our proprietary Counter Threat Platform features a multi-tenant, distributed architecture that enables our software to scale and to provide faster performance while efficiently utilizing its underlying infrastructure. The platform collects, aggregates, correlates and analyzes as many as 320 billion events daily from our extensive customer base to provide near real time risk assessment and rapid response. As our customer base increases, our platform is able to analyze more events, and the intelligence derived from these additional events makes the platform more effective. This in turn drives broader customer adoption and enhances the value of the solutions to both new and existing customers.

Contextual and Predictive Threat Intelligence. Our proprietary and purpose-built technology analyzes and correlates billions of events using advanced analytical tools and sophisticated algorithms to generate threat intelligence. This intelligence is augmented by our Counter Threat Unit™ research team, which conducts research into threat actors, uncovers new attack techniques, analyzes emerging threats and evaluates the risks posed to our customers. Applying this intelligence across our solutions portfolio provides customers with deeper insights and enriched context regarding tactics, techniques and procedures employed by those threat actors.

Integrated, Vendor-Neutral Approach. Our solutions are designed to monitor alerts, logs and other messages across multiple stages of the threat lifecycle by integrating a wide array of proprietary and third-party security products. This vendor-neutral approach allows us to aggregate events from a wide range of security and network devices, applications and endpoints to enhance our understanding of customers' networks and increase the effectiveness of our monitoring solutions.

Flexible Solution and Delivery Options. Our technology-driven information security solutions are purpose-built to serve a broad array of evolving customer needs, regardless of a customer's size or the complexity of its security infrastructure. Our customers may subscribe to any combination of our solutions and also choose how much control they will maintain over their IT security infrastructure by selecting among our fully managed, co-managed or monitored delivery options. Our flexible approach enables customers to tailor our solutions to reduce large and risky investments and costly implementations and to ensure quick and easy deployment.

Our Competitive Strengths

We believe that the following key competitive advantages will allow us to maintain and extend our leadership position in providing technology-driven information security solutions:

A Leader in Technology-Driven Information Security Solutions. We are a global leader in providing technology-driven information security solutions and believe we have become a mission-critical vendor to many of the large enterprises, small and medium-sized businesses and U.S. state and local government agencies we serve. We believe our position as a technology and market leader enhances our brand and positions us as a comprehensive solution.

Purpose-Built, Proprietary Technology. At the core of our solutions is a proprietary technology platform that collects, correlates and analyzes billions of daily events and data points, and generates enriched security intelligence on threat actor groups and global threat indicators.

Specialist Focus and Expertise. We have built our company, technology and culture with a singular focus on protecting our customers by delivering technology-driven information security solutions. We believe this continued focus reinforces our differentiation from other information security services vendors, including telecommunications and network providers, IT security product companies, and local and regional information security solutions providers.

Strong Team Culture. At our company, the fight against sophisticated and malicious cybersecurity threats is a personal one, and we take great pride in helping our customers protect their critical business data and processes. We dedicate significant resources to ensure that our culture and brand reflect our focus on protecting our customers.

Seasoned Management Team and Extensive IT Security Expertise. We have a highly experienced and tenured management team with extensive IT and cybersecurity expertise, and a record of developing successful new technologies and solutions to help protect our customers.

Our Growth Vision

Our vision is to be the essential cybersecurity company for a digitally connected world. To pursue our strategy, we seek to:

Maintain and extend our technology leadership: We intend to enhance our leading technology-driven integrated suite of solutions by adding complementary solutions that strengthen the security posture of our customers, such as security solutions for cloud-based environments. We intend to meet this goal by continuing to invest in research and development, increasing our global threat research capabilities and hiring personnel with extensive IT security expertise.

Expand and diversify our customer base: We intend to continue to expand and diversify our customer base, both domestically and internationally, by investing in our demand generation and marketing capabilities, investing in direct sales force, further developing our strategic and distribution relationships, expanding our alliance partnerships with key technology providers, pursuing opportunities across a broad range of industries, and creating new cloud-based solutions. We also intend to continue increasing our geographic footprint to further enhance our deep insight into the global threat landscape and our ability to deliver comprehensive threat intelligence to our customers.

Broaden portfolio to include software-as-a-service solutions: We intend to continue to expand our portfolio to include software-as-a-service solutions that our customers' in-house cybersecurity operations can use as an alternative to or in parallel with our existing solutions. In fiscal 2020, we launched our first software-as-a-service application, Red Cloak Threat Detection and Response (TDR) and related Managed Detection and Response (MDR).

Deepen our existing customer relationships: We intend to continue leveraging the strong customer relationships and high customer satisfaction from across our customer base to sell additional solutions to existing customers. We will continue to invest in our account management, marketing initiatives and customer support programs in seeking to achieve high customer renewal rates, help customers realize greater value from their existing solutions and encourage them to expand their use of our solutions over time.

Attract and retain top talent: Our technology leadership, brand, exclusive focus on information security, customer-first culture and robust training and development program have enabled us to attract and retain highly skilled professionals with a passion for building a career in the information security industry. We will continue to invest in attracting and retaining top talent to support and enhance our information security offerings.

Our Customers

As of January 31, 2020, our customer base was approximately 5,200 customers, including 4,100 subscription customers, across 52 countries. Our customers included approximately 23% of the companies in the Fortune 500 in fiscal 2020. We had no customer that represented 10% or more of our annual revenue in any of our last three fiscal years.

We serve customers in a broad range of industries, including the financial services, manufacturing, technology, retail, insurance, utility and healthcare sectors. In fiscal 2020, financial services and manufacturing customers accounted for 24.5% and 23.9%, respectively, of our revenue. No other industries accounted for 10% or more of our fiscal 2020 revenue.

International revenue, which we define as revenue contracted through non-U.S. entities, represented approximately 25%, 22% and 16% of our total net revenue in fiscal 2020, fiscal 2019 and fiscal 2018, respectively. For additional information about our non-U.S. revenues and assets, see "Notes to Consolidated Financial Statements—Note 12—Selected Financial Information" in our consolidated financial statements included in this report.

Our Technology Offerings

We utilize the key components of our infrastructure described below to deliver our technology-driven information security solutions to our customers.

Counter Threat Platform

Our proprietary Counter Threat Platform was purpose-built to be the foundation of our information security solutions. It has a multi-tenant, distributed architecture that enables our software to run on a single platform while providing simultaneous access to multiple users. The platform collects, aggregates, correlates and analyzes billions of daily events (currently as many as 320 billion per day) from our extensive customer base, and uses sophisticated algorithms to detect malicious activity and deliver security countermeasures, dynamic intelligence and valuable context regarding the intentions and actions of cyber adversaries. The timely analysis and routing of this security information enables our solutions to assess risk in near real time and allows us to report rapidly to our customers worldwide. The platform is highly flexible, permitting us to tailor our solutions to a customer's unique environment, and can be configured to identify specific security events of interest to a particular customer. Our platform was designed to be vendor-neutral. As a result, it can aggregate events from a wide range of security and network devices, applications and endpoints.

The platform leverages our intelligence, gained over 21 years of processing and handling events, to provide insight into how attacks are initiated and spread across our customers' networks. The platform also applies security intelligence based on threat indicators continuously gathered by our Counter Threat Unit research team through in-depth analysis of the cyber threat environment. This team conducts research into emerging threat actors and new attack tactics, and develops countermeasures that we apply to the platform to enable our customers proactively to prevent and detect compromises of their security. Our ability to see more security incidents along with the applied intelligence acts as an early warning system that enables our security analysts proactively to alert customers, apply protections and respond quickly with appropriate context. The more security events we see, the more accurate our protections are and the more accurately we can respond.

The Counter Threat Platform is supported by the following proprietary technologies:

- *Counter Threat Appliance.* Our Counter Threat Appliance performs several of the important functions of the Counter Threat Platform. The Counter Threat Appliance is a server that facilitates secure non-intrusive communications of security information used to provide managed security solutions, while our platform enriches data with our intimate knowledge of threats and customer specific intelligence to detect security incidents. A Counter Threat Appliance may be physical or virtual, which refers to the manner by which our technology is deployed to transmit information: "physical" being through the provisioning of a physical Company-owned server to a customer's site, and "virtual" being through the use of the existing customer infrastructure and residing and operating in a customer's virtual environment or platform. This technology supports a wide range of security and network devices, applications and endpoints to collect information on the customer environment, perform analytics and report to our counter threat operations centers.

- *Foresee.* Foresee, our behavioral and self-learning technology, identifies malicious events through the use of machine learning algorithms to determine the probability and confidence that a particular event or a collection of events is malicious. Foresee learns which events are malicious or non-malicious based on ongoing feedback from our certified security analysts and applies machine-learning analysis techniques for the discovery of previously unknown threats.
- *Multi-Purpose Logic Engine.* Our Multi-Purpose Logic Engine is an analytics engine that leverages our broad visibility into the global threat environment and applied intelligence from the Counter Threat Unit to identify security incidents of interest. The engine intelligently analyzes billions of events into actionable information, providing

valuable context to our security analysts to help inform their analysis of the security incidents and shorten the customer's response time.

- *Very Large Database.* Our Very Large Database efficiently and cost-effectively collects, correlates, analyzes and stores billions of structured and unstructured data elements, which help us to identify new security threats, provide valuable context to our security analysts and customers and enable Counter Threat Unit researchers to perform historical threat analysis.
- *Threat Intelligence Management System, or TIMS.* We manage structured and unstructured data in TIMS. TIMS collects, correlates and analyzes billions of data points to catalogue threat actors and generate threat indicators applied to the Counter Threat Platform and across our solutions. The data points are sourced from our managed security solutions, malware, social media, honeypots (or traps set to detect or counteract attempts at unauthorized use of information systems), open source intelligence, hunting and incident response engagements, strategic relationships and priority research.
- *Catalog for Artifact and Signal Extraction, or CASE.* CASE is a repository and a set of tools for the dynamic analysis of malware to catalogue its behaviors and generate threat indicators. CASE feeds into TIMS threat indicators identified from the analysis of malware.
- *Attacker Database.* Our Counter Threat Unit research team maintains a patented process for generating a proprietary Attacker Database that contains machine readable threat intelligence we apply to the Counter Threat Platform, iSensor™, Red Cloak™ Advanced Endpoint Threat Detection and third-party security controls.
- *Portal.* Powered by integrated intelligence and analytics tools, the portal delivers near real time information to customer executives, managers and security professionals and provides insights that help customers make better security decisions. It also facilitates near real time communication between customers and our security analysts, measures the effectiveness of a customer's security profile using asset-based and risk-weighted analyses, supports regulatory compliance requirements, links threat intelligence from our Counter Threat Unit and enables a visualization of point-in-time, comparative and historical security trends across multiple security metrics. Our portal is accessible via web and mobile applications as well as via customer applications that leverage our application programming interfaces.

Security Operations Center Automation

We have developed several technologies to automate operations within our counter threat operations centers, where our security professionals identify, diagnose and respond to security information.

- *Threat Analysis Platform*. We present threat information to our certified security analysts in a graphical user interface. This interface supports the delivery of high-quality security analysis of threats targeting or occurring within a customer's environment. Visualization enables our security analysts to detect patterns and to determine in near real time relationships of security incidents within a customer environment and across our entire customer base. Our security analysts have access to all data collected from customer environments and human readable threat intelligence from our Counter Threat Unit to provide them with the context necessary to inform their analysis and to help them determine whether they should communicate information about a security incident to a customer.
- *Ticket Management.* Our ticket management system is based on Information Technology Infrastructure Library principles and delivers security monitoring and device management solutions to customers. A sophisticated and configurable workflow provides incident, change and problem management in a leveraged-service delivery model to enable our counter threat operations centers to handle a higher volume of work with consistent quality.
- *Management and Monitoring Tools.* To effectively manage and monitor our infrastructure at customer sites and our data centers, we rely on a suite of purpose-built software applications to facilitate the full lifecycle management of all software and configuration deployments and updates, efficient management and troubleshooting, and monitoring of the health and availability of devices.

Other Enabling Technologies

- *iSensor*. Many of our customers use our proprietary network intrusion detection and prevention appliance, the iSensor. The iSensor eliminates malicious inbound and outbound traffic in near real time by performing in-line deep packet inspection (which is an examination of packet data as the data passes through the device for signs of malware, intrusions or other threats) and by applying countermeasures from the Counter Threat Unit.
- *Red Cloak*. Advanced Endpoint Threat Detection software, allows us to apply our threat intelligence and advanced analytics to the endpoint to reduce the amount of time required to detect a compromise of security and reduce the

effort required to respond. Red Cloak also allows us to develop strategic countermeasures that interdict tactics used by threat actors.

- *Third-Party Technologies*. Our technology-driven information security solutions are designed to monitor alerts, logs and other messages across multiple stages of the threat lifecycle. In addition to security monitoring, we offer device management for many leading security platforms. In deploying these solutions, we integrate a wide array of proprietary and third-party security products. Our technology supports firewalls from market-leading vendors, including, but not limited to, Cisco Systems, Inc., Palo Alto Networks, Inc., Check Point Software Technologies Ltd., Juniper Networks, Inc., Fortinet, Inc. and SonicWall, Inc. In addition, we also support intrusion prevention systems from vendors such as Intel Corporation (McAfee), and web application firewalls from vendors such as Imperva, Inc., F5 Networks, Inc. and Citrix Systems, Inc.

Software as a Service

In fiscal 2020, the Company launched its first software-as-a-service application, Red Cloak Threat Detection and Response (TDR). This gives customers visibility across their entire environment, applies advanced analytics developed using machine and deep learning on diverse data from a wide range of sources, and leverages workflows designed using the Company's 21 years of security operations expertise and integrated orchestration and automation capabilities that increase the speed of response actions. Threat intelligence, which is typically deployed as part of our managed security solutions, delivers early warnings of vulnerabilities and threats along with actionable information to help prevent any adverse impact.

Red Cloak TDR integrates Secureworks' threat intelligence which is compiled from billions of events across thousands of security environments and continuously updated to include new and emerging threats. Additionally, Red Cloak TDR integrates data from a variety of third-party sources to give organizations the best possible understanding of their threat landscape.

- Red Cloak TDR analyzes activity from endpoint, network and cloud while reducing the number of false positives security professionals face. It detects advanced threats by correlating information from a variety of sources and threat intelligence feeds, integrating Secureworks' knowledge of threat actor behaviors, and applying machine learning to provide much-needed context about the threat. Red Cloak TDR builds trust in security alerts and frees security teams to focus on threats that matter.
- Designed around Secureworks' defense in concert methodology, Red Cloak TDR unifies security environments and analyzes all relevant signals in one place. Users gain additional context so they can quickly and accurately judge the implications of each event.
- By seamlessly working on investigations together, teams can quickly reach conclusions with confidence. The built-in chat feature can be used right from the user interface during an investigation to get expert help based upon years of experience hunting, analyzing and defending against threats.
- The application allows for a quick, accurate, software-driven response that gives users the ability to automate the right action.
- Because Red Cloak TDR is a cloud-based SaaS application, companies would not have the burden of installing on-premises hardware or maintaining software version upgrades. Updates, backups and tuning are provided through the broader solution.
- Red Cloak TDR does not charge by data consumption, so subscribers are free to process the security-relevant data they need to keep their organization safe.
- Onboarding is quick and easy because the application is designed to easily integrate into an organization's current control framework.

Red Cloak Threat Detection and Response is the first in a suite of software-driven products and services that Secureworks plans to release.

Our Alliance Partnerships

Further, we maintain alliance partnerships with key technology providers who deliver capabilities we see as valuable in keeping our customers secure. These partnerships involve technology licensing, joint technology development, integration, research cooperation, co-marketing and sell-through arrangements. The principal technologies we license or resell from some of these key technology partners provide our customers with the following capabilities that in many instances we integrate into our solutions:

- Cisco (Sourcefire) – network security
- CrowdStrike – endpoint security

- Lastline – malware detection and protection
- Microsoft Defender – spyware and malware protection
- Qualys – vulnerability management
- TIBCO (LogLogic) – log management
- VMware Carbon Black – endpoint security

For information regarding transactions between us and Carbon Black, see "Notes to Consolidated Financial Statements —Note 13 — Related Party Transactions" in our consolidated financial statements included in this report.

We license the technologies under agreements that generally have terms ranging from one to five years, subject to renewal in most cases, either upon notice of renewal or upon failure by us or the provider to give notice of termination to the other party. The provider generally may terminate any license upon advance notice to us of between 90 and 270 days. The technology partner license agreements generally provide for post-termination support, transition and wind-down periods that are intended to limit any disruption to our business that could result from a license termination. We generally are required under the agreements to make licensing payments in the form of fees or royalties at a discount off the list price, although some agreements also include volume or tiered pricing.

Our Service Offerings

We offer an integrated suite of technology-driven information security solutions. Our customers may subscribe to our full suite of solutions or elect to subscribe to various combinations of our individual solutions. All of our solutions are enabled by our Counter Threat Platform and our team of highly-skilled security experts.

Managed Security and Managed Detection and Response

We offer a broad range of managed security solutions, including those highlighted below.

Managed Detection and Response. Secureworks' Managed Detection and Response (MDR) service leverages the detectors, analytics and correlation capabilities of Red Cloak TDR to find advanced threats that aren't typically found with normal detection, and to expand the context around each alert. Knowledge gained from more than 1,000 incident response engagements per year informs the continuously updated threat intelligence and analytics used to recognize malicious activity. With more accurate detections and better context, false alerts are reduced, and customers can focus on the events that matter. When an event requires action, customers have the option to check analyst recommendations via an intuitive interface or collaborate directly with Secureworks analysts using a built-in chat box. The Secureworks MDR service includes threat hunting to proactively isolate and contain threats that evade existing controls, and it comes with IR support for peace of mind during critical investigations.

Security Monitoring. Security appliances, systems and servers generate extensive logs, alerts and other messages every day. This raw information must be continuously monitored, correlated and analyzed in order to identify security events of actual concern while generating a minimal number of falsely-positive results. Our security monitoring solution collects, correlates and analyzes logs, alerts and other messages generated by most leading security technologies and critical information assets, on a 24/7 basis, to identify anomalies and respond to threats in near real time. This solution functions either on a stand-alone basis or in concert with customer-owned security information and event management platforms.

Advanced Malware Protection and Detection. Our advanced malware protection and detection solution, or AMPD, provides a layer of defense against emerging zero-day threats for enterprise and medium-sized organizations, which are threats whose existence is unknown to the targeted organization or those responsible for its security before the first exploitation occurs. AMPD uses next-generation sandboxing technology with full-system emulation to execute and analyze malware within a controlled environment, and draws on our threat intelligence data pool and our expert threat analysis teams. AMPD’s combination of deep intelligence capabilities developed by the Counter Threat Unit and advanced technology permits our customers to see, rapidly analyze and accurately diagnose previously unknown malware, and to obtain focused guidance that expedites threat remediation.

Advanced Endpoint Threat Detection. Advanced endpoint threat detection, or AETD, improves situational awareness and visibility through proprietary endpoint intelligence developed by the Counter Threat Unit. AETD is a fully managed security solution that monitors the state of endpoints, which include Windows servers, laptops and desktops, for threat indicators, investigates events to determine their severity, accuracy and context, and quickly escalates critical events to the customer’s attention indicating that an endpoint may be compromised.

Firewall and Next-Generation Firewall Solutions. Firewalls provide critical information necessary to identify and evaluate security events. We provide an array of firewall solutions ranging from the collection, organization and reporting of firewall information to the full management of a customer's firewall by our security analysts, including rule-set changes and overall configuration of the device for optimal performance. Our experts hold certifications from leading vendors and have significant experience with the relevant technologies, enabling us to provide solutions to support market-leading vendors in various types of environments. Our firewall management solutions ease the adoption of next-generation firewall technology through policy-based control over applications, users and content, device provisioning and deployment and enable customers to respond immediately to security events.

Managed Web Application Firewall Solutions. Web application firewalls are designed specifically to protect applications that deliver critical services via Internet web protocols. These firewalls block certain connections while permitting others based on the configuration of the firewall in order to ensure that only legitimate traffic reaches protected applications. Web application firewalls are increasingly utilized to address various compliance mandates, including the Payment Card Industry Data Security Standard, or PCI DSS. Our managed web application firewall solution assists customers with the end-to-end management of these complex devices, from initial configuration and periodic policy changes to patching, updating and full-time monitoring of system health and performance.

Managed Network Intrusion Detection System, or IDS, and Intrusion Prevention System, or IPS, Solutions. IDS and IPS technologies can provide a highly effective layer of security. We provide a wide range of solutions to enable our customers to realize the benefits from these technologies, and effectively identify threats faster. Our solutions include security monitoring, performance and availability management, device upgrades and patch management, policy and signature management, integration of Counter Threat Unit intelligence and use of our proprietary iSensor device. We manage leading vendors' IDS and IPS products as well as our iSensor.

Vulnerability Management. Our Vulnerability Management solution, which is fully managed and maintained by a dedicated vulnerability management team, encompasses the two solutions described below.

- *Managed Vulnerability Scanning*. A vulnerability scan is designed to alert an organization to potential exposures and vulnerabilities in its network. As part of our solution, we perform internal and external scan audits across network devices, servers, databases and other assets in on-premises and cloud environments.

- *Managed Web Application Scanning.* Applications that deliver services via the web are the lifeblood of business-to-business and business-to-consumer e-commerce. A vulnerability scan can alert an organization to potential exposures and weaknesses in these web-based applications before a threat actor exploits those weaknesses. Our managed web application scanning solution performs deep and accurate scans of web applications that are hosted on customer premises or in cloud environments. These scans search for vulnerabilities specific to the web protocols that are foundational to web applications. Our solution also supports the ability to log into web applications and discover vulnerabilities that may lie behind the login page.

Log Retention Solutions. We offer comprehensive log aggregation, retention, searching and reporting solutions. Log retention enables our customers to satisfy various compliance obligations, which require full log retention from critical IT systems to ensure the integrity of confidential data, and to conduct forensic investigations. Our log retention solutions provide support for a wide range of sources, allowing the capture and aggregation of millions of logs generated every day by critical information assets such as servers, routers, firewalls, databases, applications and other systems of the log retention appliance.

Managed Policy Compliance. To assist customers in improving their security and compliance with regulatory mandates, our managed policy compliance solution ensures that the configurations of customers' critical systems are known and tracked and comply with pre-established security guidelines. Our solution consists of two key components, software that automatically retrieves the configurations of critical systems and compares them to pre-established configuration targets, and a library of security and compliance-driven configuration checks across three systems. Our solution helps customers establish configuration targets, set up the scans, monitor the output and report on the results.

Delivery Options for Managed Security. Our managed security customers can choose how much control they maintain over their IT security infrastructure by selecting among our fully managed, co-managed or monitored solution delivery options. Our solutions are designed to be flexible and scalable to complement the evolving security needs of our customers. Our customers often migrate between the different delivery options in response to their changing needs as well as to the changing threat landscape.

Fully Managed. With our fully managed delivery options, we assume control of a customer's security technology so the customer can focus on running its business rather than becoming a security administrator. Customers selecting fully managed delivery obtain all of the benefits of our monitored delivery option, including access to our on-demand Counter Threat Platform. In addition, our team of security analysts will monitor and manage a customer's security technology or selected devices, proactively update that security infrastructure to protect against emerging threats, identify vulnerabilities, ensure that the devices are properly configured with our latest countermeasures, and block or respond to immediate threats in accordance with the customer's escalation policies. We believe that our fully managed solutions provide customers with increased security protection based on our best practices and security expertise applied across our customer base, as well as improved operational efficiency by removing the overhead costs associated with managing security technology.

Co-Managed. Customers often deploy our managed solutions on a co-managed basis as an extension of their security personnel. The co-managed delivery option enables the customer to retain control over its security infrastructure to the extent that it prefers to do so, and enables its security staff to work with our experts as a team while maintaining full access and visibility into the management process. This option is particularly suitable for organizations that already possess in-house security expertise, but that seek to remove the burden of managing devices from their staff so they can focus on more strategic security initiatives.

Monitored. Customers selecting our monitored solutions obtain access to our on-demand Counter Threat Platform through our web-based portal, plus near real time monitoring and analysis by our security analysts of events collected from security and network devices and applications. Our monitored solutions enhance our customers' security position by providing them with valuable context from our team of security analysts and comprehensive reporting to demonstrate regulatory compliance. Our ability to see more security incidents across our entire customer base along with our threat intelligence acts as an early warning system, which benefits customers by proactively alerting them to potential threats, applying protections and helping them respond quickly. We believe that the more we see, the more accurate our protections are, and the more accurately we can respond. Through our monitored solutions, we leverage our on-demand Counter Threat Platform to correlate information from many devices and applications, providing security analysts with the context they need to significantly reduce falsely-positive results and alert customers to actual threats against their organizations.

In general, our managed delivery options require our security professionals to be directly involved with our customer's security technology, and as a result, the cost to service these delivery options is generally higher than the cost to service monitored delivery options. Over the last three fiscal years, we have generated the majority of our managed security solutions revenue from either fully managed or co-managed delivery options. Our future success depends on our ability to manage efficiently the costs of our security offerings and to price our security solutions in an effective manner.

Threat Intelligence

Powered by our Counter Threat Unit research team, threat intelligence provides early warnings and actionable intelligence that enables rapid protection against threats and vulnerabilities before they affect an organization. Threat intelligence is applied as part of our managed security offerings, but also may be offered separately.

Global Threat Intelligence. Our global threat intelligence solutions provide proactive, actionable intelligence tailored to an organization's environment. This intelligence includes clear, concise threat and vulnerability analysis, detailed remediation information and recommendations, consultation with our threat experts, on-demand access to extensive threat and vulnerability databases, malware analysis upon request, intelligence feeds and integration with our other solutions for correlation and unified reporting.

Borderless Threat Monitoring. Our borderless threat monitoring solution delivers organizations with timely and actionable security intelligence that provides them with insight into threat activities that may exist beyond the edge of their network. This solution proactively informs organizations of network threat indicators that apply to their particular network environment and allows them to manage the threat in accordance with their escalation policies.

Malware Code Analysis. Our malware code analysis solution focuses on reverse engineering malicious or unknown code identified in security events in order to provide an organization with a better understanding of the code's behavior and its impact on the organization's systems and information. Using advanced computer forensic tools and techniques, our security experts dissect the code to determine its functionality, purpose, composition and source.

Enterprise Brand Surveillance. Our enterprise brand surveillance solution offers near real time monitoring of a range of intelligence outlets to identify developing threats from exposure of sensitive data, targeting by threat actors and risks to perception of the customer's brand. This solution provides our customers with live notifications delivered upon discovery of

actionable intelligence. It also provides customers with context regarding potential threats and helps them to develop informed risk mitigation strategies.

Security and Risk Consulting

Our consulting organization provides expertise and analysis to help customers improve their security posture by comprehensively assessing security capabilities, designing and building robust security programs, preparing employees against cyber attacks, facilitating regulatory compliance and helping customers identify, prioritize and resolve the vulnerabilities that pose the greatest threat. We offer both project-based and long-term contracts, including retainer contracts sold together with our managed security solutions. For example, we may enter into a managed security contract bundled together with an incident response retainer.

Our team has extensive experience conducting security, compliance and risk engagements across many industries and geographic areas, and under recent regulations and industry standards that impose security mandates. Professional services offered by the team include the following:

Technical Testing and Assessments. Our testing and assessment solutions provide customers with the knowledge, expertise and efficiency needed to conduct thorough security and risk evaluations of their environments. We offer testing and assessments that address logical, physical, technical and non-technical threats in order to identify gaps that create risk, construct a stronger security posture and meet compliance mandates. Our testing and assessments solutions include application security, network security and Red Team testing, which simulates cyber attacks using real-world tactics, techniques and procedures.

Security and Governance Program Development. Our security and governance program development solutions provide our customers with security, risk and compliance expertise to help them develop strategic security and governance programs based on industry and observed best practices. These solutions include internal audit support and the development of corporate information security and computer security incident response security awareness programs.

Targeted Threat Hunting. The Targeted Threat Hunting solution uses proprietary technology to search customer networks to identify the presence of security compromises and entrenched threat actors operating in a customer's environment. The solution draws on our threat intelligence and extensive experience countering cyber adversaries.

Cloud Security. We help customers to deliver cloud-based services securely and to satisfy their compliance requirements. Our cloud security solutions include cloud security strategic consulting, cloud risk assessment, assurance testing of cloud deployments, incident response in cloud environments and cloud security architecture and design.

Security Design and Architecture Solutions. Our security design and architecture solutions help customers to clarify their information security priorities and identify their most vulnerable assets that require security monitoring, as well as to obtain a prioritized roadmap of upgrades to help with budgeting and determining resource requirements. Our solutions include security health check solutions, security architecture assessment solutions and security architecture and design consulting.

Security Residency Solutions. Our security residency solutions provide customers with security consultants who serve as extended members of their staff either on-site or remotely to extend and heighten an organization's security expertise and capabilities. We offer several levels of resident security consultants, including executive, expert and technical consultants tailored to the security expertise and leadership our customers need. Residency solutions often are combined with managed security solutions in complex enterprise environments to enhance the value customers obtain from our solutions. Consulting residents align our solutions with the customers' internal processes, integrate our data feeds into customer applications and dashboards, and produce customized analytics and reporting. In addition, residents can assist customers with handling the security events identified by our managed security solutions.

Incident Response

Incident response typically is deployed along with security and risk consulting. The professionals who deliver incident response engagements help customers rapidly analyze, contain and remediate security breaches to minimize their duration and impact.

Incident Management Proactive Solutions. Through our incident management proactive solutions, our security consultants work with customers to prepare them to respond quickly and effectively to a security incident. In providing these solutions, we feature both incident management risk assessment and response plan review and development solutions. Our incident management risk assessment solution evaluates a customer's ability to detect, resist and respond to a targeted or advanced threat and is designed to help our customers understand their exposure to these threats, including advanced persistent threats, or

APTs, in order to reduce their risk of compromise. Our response plan review and development solution supports our customers in developing an effective computer security incident response plan, or CSIRP, based on IT security best practices, incorporating the latest threat intelligence tailored to the customer's specific needs.

Incident Response Testing and Capability Analysis. Through real-world simulations, incident response testing and capability analysis tests and evaluates the effectiveness of an organization's CSIRP and attack response procedures. We employ tabletop exercises to subject IT teams to simulated threats, such as cyber-crime and APTs. The exercises demonstrate the ways a customer's systems and network can be breached and the critical actions required during a breach to contain a threat.

Emergency Incident Response Solutions. Through our comprehensive range of incident response and management solutions, we seek to ensure that organizations experience minimal economic loss and operational disruption when a security incident occurs. We offer an incident response retainer, through which our security experts can provide emergency incident response solutions within minutes of a reported breach. Our security consultants work to minimize the duration and impact of any breach through incident management, surveillance, digital forensic analysis, malware analysis and reverse engineering.

Backlog

We define backlog as the non-cancellable value of subscription-based solutions to be provided under managed security solutions contracted with a customer that have not yet been installed. Backlog is not recorded in revenue, deferred revenue or elsewhere in the consolidated financial statements until we establish a contractual right to invoice, at which point it is recorded as revenue or deferred revenue, as appropriate. All contractual amounts included in backlog are available to be installed and revenue recognition commenced within the coming fiscal year. As of January 31, 2020 and February 1, 2019, backlog of subscription-based solutions was approximately $12.9 million and $29.1 million, respectively. Backlog is influenced by several factors, including seasonality, the compounding effects of renewals and the mix of solutions under contract with customers. Accordingly, we believe that fluctuations in backlog are not always a reliable indicator of future revenues and we do not utilize these measurements as key management metrics.

Sales and Marketing

Our sales and marketing organizations work together closely to drive revenue growth by enhancing market awareness of our solutions, building a strong sales pipeline and cultivating customer relationships. We offer managed security and threat intelligence on a subscription basis. We sell these solutions under contracts with initial terms that typically range from one to three years and, as of January 31, 2020, averaged two years in duration. We provide security and risk consulting primarily under fixed-price contracts, although we perform some engagements under variable-priced contracts on a time-and-materials basis.

Sales

We sell primarily through our direct sales organization, supplemented by sales through our channel partners, including referral agents, regional value-added resellers and trade associations. Approximately 91% of our revenue in fiscal 2020 was generated through our direct sales force, in some cases in collaboration with members of Dell's sales force, with the remaining portion generated through our channel partners.

Our direct sales organization consists of inside sales and field sales personnel and solutions architects organized by core customer segments and geography. Our sales strategy varies based on the size of the company and the target point-of-entry into an organization, which is primarily through chief information security officers or other IT and business leaders. Within North America, our direct sales organization has separate teams focused on the large enterprises, small and medium-sized businesses, and U.S. state and local government agencies. We believe that continued additional investment in our direct and channel sales staff will contribute to our long-term growth.

We believe that our sales process differentiates us in the marketplace for information security solutions. The process typically begins by emphasizing the importance of educating key decision makers within a customer organization with respect to the organization's information security needs. We deliver a technical evaluation performed by a team that includes both highly trained sales personnel and security experts. This allows us to tailor the solution design, including the level of service and deployment options, to the organization's specific security needs and to become its long-term advisor and partner. A typical large enterprise sales team includes an inside sales team that is responsible for developing sales leads, a direct sales team that is responsible for obtaining new customers and some cross-sales, an enterprise account management team that is responsible for renewals and some cross-sales, and security engineers who provide technical support to our sales personnel.

Since our acquisition by Dell in February 2011, we have marketed our solutions through Dell's channel partners as well as through our own and have entered into agreements with Dell to preserve, and potentially expand, our existing commercial arrangements with Dell.

Marketing

Our marketing strategy is to drive customer insights, generate demand, enable sales, build customer loyalty and increase the strength of the Secureworks brand. Our marketing team consists primarily of customer experience, solutions marketing, field marketing, demand generation and corporate communications functions.

Our primary marketing activities include:

- Press and industry analyst relations to build third-party validation and generate positive coverage for our company and our solutions;
- Events, trade shows and industry events, to create customer and prospect awareness;
- Leveraging our proprietary research through content marketing and engagement on social channels like Twitter, LinkedIn and Facebook and on our own blogs;
- Search engine marketing and advertising to drive traffic to our website;
- Website development to engage and educate prospects and generate interest through product information and demonstrations, case studies, white papers, blog posts and marketing collateral;
- Multi-channel marketing campaigns;
- Customer testimonials and references; and
- Sales tools and field marketing events to enable our sales organization to more effectively convert leads into customers.

Customer Service, Training and Support

Customer service, training and support are key elements of our commitment to provide superior customer service. We have a comprehensive customer service training and support program to communicate our commitment to customer service and to enhance the value that our customers derive from our solutions. We provide extensive education, training and support on the functionality of our solutions, so that our customers are able to fully utilize their benefits. Our customer service training and support team provides dependable and timely resolution of customer security concerns and technical inquiries, and our certified security analysts are continuously available to customers for consultation by telephone or e-mail and over the Internet through our portal. We regularly conduct customer surveys to help us evaluate and develop our existing solutions and other solutions that we believe could enhance our customer relationships.

Competition

The market for information security services is very competitive, and we expect competition to continue to increase in the future. Changes in the threat landscape and the broader IT infrastructure have led to quickly evolving customer requirements for protection from security threats and adversaries.

We compete primarily against the following four types of security services and product providers, some of which operate principally in the large enterprise market and others in the market for small and medium-sized businesses:

- global telecommunications and network services providers such as AT&T Inc., BT Group plc, Verizon Communications Inc. and NTT Communications Corp.;
- providers of specialized or niche IT security products and services such as FireEye, Inc., and Palo Alto Networks, Inc.;
- diversified technology companies such as Cisco Systems, Inc., Hewlett Packard Enterprise Company, International Business Machines Corporation and Intel Corporation; and
- regional information security services providers that compete in the small and medium-sized businesses market with some of the features present in our information security solutions.

We believe that the principal competitive factors in our market include:

- global visibility into the threat landscape;
- ability to generate actionable intelligence based on historical data and emerging threats;
- scalability and overall performance of platform technologies;
- ability to integrate with, monitor and manage a variety of third-party products;
- ability to provide a flexible deployment option to cater to specific customer needs;
- ability to attract and retain high-quality professional staff with information security expertise;
- brand awareness and reputation;
- strength of sales and marketing efforts;
- cost effectiveness;
- customer service and support; and
- breadth and richness of threat intelligence, including history of data collection and diversity and geographic scope of customers.

We believe that we generally compete favorably with our competitors on the basis of these factors as a result of the architecture, features and performance of our Software-as-a-Service offerings, Counter Threat Platform, the quality of our threat intelligence, the security expertise within our organization and the ease of integration of our solutions and platform with other technology infrastructures. However, many of our existing and potential competitors, particularly in the large enterprise market, have advantages over us because of their longer operating histories, greater brand name recognition, larger customer bases, more extensive relationships within large commercial enterprises, more mature intellectual property portfolios and greater financial and technical resources.

Research and Development

We invest significant time and resources to maintain, enhance and add new functionality to our Counter Threat Platform and purpose-built technologies that are critical enablers of our solutions. Our research and development organization is responsible for the design, development and testing of all aspects of our suite of information security solutions. The members of the organization have deep security and software expertise and work closely with our product management and customer service training and support teams to gain insights into customers' environments for use in threat research, product development and innovations. The organization focuses its research on identifying next-generation threats and adversaries and developing countermeasures, which are continuously applied to our platform and used to respond to the rapidly evolving security threat landscape. The majority of our research and development team is based in Atlanta, Georgia, Providence, Rhode Island, Pittsburgh, Pennsylvania, Edinburgh, Scotland, and Hyderabad, India.

We believe that innovation and the timely development of new solutions are essential to meeting the needs of our customers and improving our competitive position. Several of the solutions we have released in the past year are the result of our internal processes within our company to identify and solve difficult security issues and use the best ideas to develop new solutions. As our customers move their applications and data into third-party cloud environments, we will extend and integrate our solutions into these environments globally. In addition, point solutions we develop for customers during security and risk consulting engagements often are integrated into our portfolio of solutions and made available to our broader customer base.

Intellectual Property

Our intellectual property is an essential element of our business. To protect our intellectual property rights, we rely on a combination of patent, trademark, copyright, trade secret and other intellectual property laws as well as confidentiality, employee non-disclosure and invention assignment agreements.

Our employees and contractors involved in technology development are required to sign agreements acknowledging that all inventions, trade secrets, works of authorship, developments, processes and other intellectual property rights conceived or reduced to practice by them on our behalf are our property, and assigning to us any ownership that they may claim in those

intellectual property rights. We maintain internal policies regarding confidentiality and disclosure. Our customer and resale contracts prohibit reverse engineering, decompiling and other similar uses of our technologies and require that our technologies be returned to us upon termination of the contract. We also require our vendors and other third parties who have access to our confidential information or proprietary technology to enter into confidentiality agreements with us.

Despite our precautions, it may be possible for third parties to obtain and use without our consent intellectual property that we own or otherwise have the right to use. Unauthorized use of our intellectual property by third parties, and the expenses we incur in protecting our intellectual property rights, may adversely affect our business.

Our industry is characterized by the existence of a large number of patents, which leads to frequent claims and related litigation regarding patent and other intellectual property rights. In particular, large and established companies in the IT security industry have extensive patent portfolios and are regularly involved in both offensive and defensive litigation. From time to time, third parties, including some of these large companies as well as non-practicing entities, may assert patent, copyright, trademark and other intellectual property rights against us, our channel partners or our end-customers, which we are obligated to indemnify against such claims under our standard license and other agreements. Successful claims of infringement by a third party, if any, could prevent us from performing certain solutions, require us to expend time and money to develop non-infringing solutions, or force us to pay substantial damages (including, in the United States, treble damages if we are found to have willfully infringed patents), royalties or other fees.

Patents and Patent Applications

As of January 31, 2020, we owned 32 issued patents and 24 pending patent applications in the United States and four issued patents and three pending patent applications outside the United States. The issued patents are currently expected to expire between 2020 and 2037. Although we believe that our patents as a whole are important to our business, we are not substantially dependent on any single patent.

We do not know whether any of our patent applications will result in the issuance of a patent or whether the examination process will require us to modify or narrow our claims, as has happened in the past with respect to certain claims. Any patents that may be issued to us may not provide us with any meaningful protection or competitive advantages, or may be contested, circumvented, found unenforceable or invalid, and we may not be able to prevent third parties from infringing them.

Trademarks and Copyrights

The U.S. Patent and Trademark Office has granted us federal registrations for some of our trademarks. Federal registration of trademarks is effective for as long as we continue to use the trademarks and maintain our registrations as permitted under federal law. We also have obtained protection for some of our trademarks, and have pending applications for trademark protection, in the European Community and various countries. We may, however, be unable to obtain trademark protection for our technologies and names that we use, and names, slogans or logos that we use or may use may be deemed non-distinctive, and therefore unable to distinguish our solutions from those of our competitors in one or more countries.

We do not generally register any of our works of authorship, including software and source code, with the U.S. Copyright Office, but instead rely on the protection afforded to such works by U.S. copyright laws, which provide protection to authors of original works whether published or unpublished and whether registered or unregistered.

We have entered into a trademark license agreement with Dell Inc. under which Dell Inc. has granted us a non-exclusive, royalty-free worldwide license to use the trademark “DELL,” solely in the form of “SECUREWORKS-A DELL COMPANY,” in connection with our business and products, services and advertising and marketing materials related to our business.

Employees

As of January 31, 2020, we employed 2,663 full-time employees in the United States and 22 other countries. None of our employees in the United States are represented by a labor organization or the subject of a collective-bargaining agreement. Employees of some of our foreign subsidiaries are represented on workers’ councils.

Information about our Executive Officers

The following table sets forth information as of March 27, 2020 concerning our executive officers.

Name	Age	Position
Michael R. Cote	59	President and Chief Executive Officer
Paul M. Parrish	58	Senior Vice President, Chief Financial Officer and Principal Accounting Officer

Each executive officer is appointed by, and serves at the discretion of, our board of directors.

Michael R. Cote has served as our President and Chief Executive Officer since May 2015. He served as our General Manager and as Vice President of Dell from our acquisition by Dell in February 2011 through the closing of our initial public offering in April 2016. Before our acquisition by Dell, Mr. Cote had served as our Chairman, President and Chief Executive Officer since February 2002. Prior to joining Secureworks, Mr. Cote held executive positions with Talus Solutions Inc., a pricing and revenue management software firm acquired by Manugistics Group, Inc. in 2000. Mr. Cote joined Talus from MSI Solutions Inc., a web application development and systems integration company. In addition to his service in other technology executive roles, Mr. Cote's early career included international assignments with KPMG LLP, an accounting and consulting firm. Mr. Cote serves on the board of Children's Healthcare of Atlanta, the board of regents at Boston College, the board of trustees at Marist School, and in February 2019, he joined the board of directors at Extrahop Networks, Inc. Mr. Cote also served as a director of FSLogix, Inc. until the company was acquired by Microsoft Corporation in November 2018. Mr. Cote is a Certified Public Accountant and a member of Business Executives for National Security.

Paul M. Parrish has served as our Senior Vice President and Chief Financial Officer since December 2019, and as our principal accounting officer since January 2020. Before joining us, Mr. Parrish most recently served as Chief Financial Officer of CIOX Health, LLC, a healthcare data management solutions company, from August 2016 to December 2019. Before joining Ciox, Mr. Parrish served as Chief Financial Officer of Brightree, LLC, a company providing a cloud-based software and services platform for the post-acute medical care market, from June 2014 to July 2016. Mr. Parrish's previous experience includes multiple senior financial and accounting roles, including service as Chief Financial Officer of US Security Associates, Inc., a security services company, from September 2012 to January 2014, and Chief Financial Officer of S1 Corporation, a payments and financial services software company, from January 2009 to February 2012. Earlier in his career, Mr. Parrish was a Senior Manager with the global accounting firm Deloitte. Mr. Parrish is a Certified Public Accountant.

Item 1A. Risk Factors

Our business, operating results, financial condition and prospects are subject to a variety of significant risks, many of which are beyond our control. The following is a description of some of the important risk factors that may cause our actual results in future periods to differ substantially from those we currently expect or seek. The risks described below are not the only risks we face. There are additional risks and uncertainties not currently known to us or that we currently deem to be immaterial that also may materially adversely affect our business, operating results, financial condition or prospects.

Risks Related to Our Business and Our Industry

We have a history of losses and may not achieve or maintain profitability.

We incurred net losses of $31.7 million in fiscal 2020, $39.1 million in fiscal 2019 and $10.4 million in fiscal 2018. Any failure to increase our revenue as we grow our business could prevent us from achieving or maintaining profitability on a consistent basis or at all. We expect our operating expenses to continue to increase as we implement our growth strategy to maintain and extend our technology leadership, expand and diversify our customer base and attract and retain top talent. Our strategic initiatives may be costlier than we expect, and we may not be able to increase our revenue to offset these increased operating expenses. Our revenue growth may slow or revenue may decline for a number of reasons, including increased competition, reduced demand for our solutions, a decrease in the growth or size of the information security market or any failure by us to capitalize on growth opportunities. If we are unable to meet these risks and challenges as we encounter them, our business, financial condition and results of operations may suffer.

We must continue to enhance our existing solutions and technologies and develop or acquire new solutions and technologies, or we will lose customers and our competitive position will suffer.

Many of our customers operate in markets characterized by rapidly changing technologies, which require them to support a variety of hardware, software applications, operating systems and networks. As their technologies grow more complex, we expect these customers to face new and increasingly sophisticated methods of cyber attack. To maintain or increase our market share, we must continue to adapt and improve our solutions in response to these changes without compromising the high service levels demanded by our customers. If we fail to predict accurately or react in a timely manner to the changing needs of our customers and emerging technological trends, we will lose customers, which will negatively affect our revenue, financial condition and results of operations.

The forces behind changes in technology, which we do not control, include:

- the establishment by organizations of increasingly complex IT networks that often include a combination of on-premise, cloud and hybrid environments;
- the rapid growth of smart phones, tablets and other mobile devices and the “bring your own device” trend in enterprises;
- action by hackers and other threat actors seeking to compromise secure systems;
- evolving computer hardware and software standards and capabilities;
- changing customer requirements for information technology; and
- introductions of new products and services or enhancements to existing products and services by our competitors.

Our future growth also depends on our ability to scale our Counter Threat Platform to analyze an ever increasing number of events. As of January 31, 2020, our platform analyzed as many as 320 billion events each day. If the number of events grows to a level that our platform is unable to process effectively, or if our platform fails to handle automatically an increasing percentage of events or is unable to process a sudden, sharp increase in the number of events, we might fail to identify network, application and/or endpoint events as significant threat events, which could harm our customers and negatively affect our business and reputation.

We operate in a rapidly evolving market, and if the new solutions and technologies we develop or acquire do not achieve sufficient market acceptance, our growth rates will decline and our business, results of operations and competitive position will suffer.

We spend substantial time and money researching and developing new information security solutions and technologies and enhancing the functionality of our current solutions and technologies to meet the rapidly evolving demands of our customers for information security in our highly competitive industry. For us to realize the benefits from our significant investments in developing and bringing our solutions to market, our new or enhanced solutions must achieve high levels of market acceptance, which may not occur for many reasons, including as a result of:

- delays in our introduction of new, enhanced or modified solutions that address and respond to innovations in computer technology and customer requirements;
- defects, errors or failures in any of our solutions or delivery of our solutions;
- any inability by us to integrate our solutions with the security and network technologies used by our current and prospective customers;
- any failure by us to anticipate, address and respond to new and increasingly sophisticated security threats or techniques used by hackers and other threat actors;
- negative publicity about the performance or effectiveness of our solutions; and
- disruptions or delays in the availability and delivery of our solutions.

Even if the initial development and commercial introduction of any new solutions or enhancements to our existing solutions are successful, the new or enhanced solutions may not achieve widespread or sustained market acceptance. In such an event, our competitive position may be impaired, and our revenue and profitability may be diminished. The negative effect of inadequate market acceptance on our results of operations may be particularly acute because of the significant research, development, marketing, sales and other expenses we will have incurred in connection with the new or enhanced solutions.

We rely on personnel with extensive information security expertise, and the loss of, or our inability to attract and retain, qualified personnel in the highly competitive labor market for such expertise could harm our business.

Our future success depends on our ability to identify, attract, retain and motivate qualified personnel. We depend on the continued contributions of Michael R. Cote, our President and Chief Executive Officer, and our other senior executives, who have extensive information security expertise. The loss of any of these executives could harm our business and distract from the operating responsibilities of other executives engaged to search for their replacements.

Our Counter Threat Unit and security analyst teams are staffed with experts in information security, software coding, data science and advanced mathematics. Because there are a limited number of individuals with the education and training necessary to fill these roles, such individuals are in high demand. We face intense competition in hiring individuals with the requisite expertise, including from companies with greater resources than ours. As a result, we may be unable to attract and retain suitably qualified individuals who are capable of meeting our growing technical, operational and managerial requirements, or may be required to pay increased compensation to satisfy our staffing needs. Further, if we hire personnel from competitors, we may be subject to allegations that the new employees were improperly solicited or have divulged proprietary or other confidential information in breach of agreements with their former employers. Any inability by us to attract and retain the qualified personnel we need to succeed could adversely affect our competitive market position, revenue, financial condition and results of operations.

Our quarterly results of operations or other operating measures may fluctuate significantly based on a number of factors that could make our future results difficult to predict.

Our results of operations or other operating measures have fluctuated in the past from quarter to quarter. We expect that quarterly fluctuations will continue as a result of a number of factors, many of which are outside of our control and may be difficult to predict, including:

- our ability to increase sales to existing customers and to renew contracts with our customers;
- delays in deployment of solutions under our customer contracts;
- our ability to attract new customers;
- interruptions or service outages in our data centers, cloud providers and other technical infrastructure, other technical difficulties or security breaches;

- customer budgeting cycles, seasonal buying patterns and purchasing practices;
- changes in our pricing policies or those of our competitors;
- fluctuations in the demand for our information security solutions and in the growth rate of the information security market generally;
- the level of awareness of IT security threats and the market adoption of information security solutions;
- the timing of the recognition of revenue and related expenses;
- our ability to expand our direct sales force and our strategic and distribution relationships;
- our ability to develop in a timely manner new and enhanced information security solutions and technologies that meet customer needs;
- our ability to retain, hire and train key personnel, including sales personnel, security analysts, security consultants and members of our security research team;
- fluctuations in available cash flow from prepayments for our solutions;
- changes in the competitive dynamics of our market, including the launch of new products and services by our competitors;
- the effectiveness and efficiency of in-house information security solutions;
- our ability to control costs, including our operating and capital expenses;
- our ability to keep our proprietary technologies current;
- any failure of or technical issues affecting a significant number of our appliances or software;
- adverse litigation judgments, settlements or other litigation-related costs;
- costs related to the acquisition of businesses, talent, technologies or intellectual property, including potentially significant amortization costs and possible write-downs;
- stock-based compensation expense associated with attracting and retaining personnel; and
- general economic conditions, geopolitical events and natural catastrophes and public health issues, including the novel strain of coronavirus, COVID-19, which began spreading globally in early 2020.

The factors above, individually or in combination, may result in significant fluctuations in our financial and other results of operations from quarter to quarter. As a result of this variability and unpredictability, investors should not unduly rely on our historical results of operations as an indication of future performance.

We face intense competition, including from larger companies, and may lack sufficient financial or other resources to maintain or improve our competitive position.

The market for managed security and other information security services is highly competitive, and we expect competition to intensify in the future. Increased competition in our market could result in intensified pricing pressure, reduced profit margins, increased sales and marketing expenses and a failure to increase, or a loss of, market share. Our competitors vary in size and in the scope and breadth of the products and services they offer.

Many of our existing and potential competitors, particularly in the large enterprise market, enjoy substantial competitive advantages because of their longer operating histories, greater brand name recognition, larger customer bases, more extensive customer relationships within large commercial enterprises, more mature intellectual property portfolios and greater financial and technical resources. As a result, they may be able to adapt more quickly than we can to new or emerging technologies and changing opportunities, standards or customer requirements. In addition, several of our competitors have made acquisitions or entered into partnerships or other strategic relationships with one another to offer more comprehensive cybersecurity solutions than each could offer individually. Mergers, consolidations or alliances among competitors, or acquisitions of our competitors by large companies, may result in more formidable competition for us if their security products and services are bundled into sales packages with their widely utilized non-security-related products and services. For example, large telecommunications companies have chosen to integrate managed security solutions as a complement to their existing communications offerings, a trend which may accelerate in the future. In addition, we expect pricing pressures within the information security market to intensify as a result of action by our larger competitors to reduce the prices of their security monitoring, detection and prevention products and managed security solutions. If we are unable to maintain or improve our competitive position with respect to our current or future competitors, our failure to do so could adversely affect our revenue growth and financial condition. Further, if our competitors are able to successfully use artificial intelligence to enhance the ability of their solutions

to prevent, detect, respond to or predict cybersecurity breaches and we do not successfully implement any comparable technologies, our solutions could be viewed less favorably by potential customers and our revenues and competitive position could be negatively affected.

If we are unable to attract new customers, retain existing customers or increase our annual contract values, our revenue growth will be adversely affected.

To achieve revenue growth, we must expand our customer base, retain existing customers, and increase our annual contract values. In addition to attracting additional large enterprise and small and medium-sized business customers, our strategy is to continue to pursue non-U.S. customers, government entity customers and customers in other industry sectors in which our competitors may have a stronger position. The renewal rates of our existing customers may decline or fluctuate as a result of a number of factors, including their satisfaction or dissatisfaction with our solutions, the price of our solutions, the prices or availability of competing solutions and technologies or consolidation within our customer base. If we fail to attract new customers, or our customers do not renew their contracts for our solutions or renew them on less favorable terms, our revenue may cease to grow or may decline and our business may suffer.

Some customers elect not to renew their contracts with us or renew them on less favorable terms, and we may not be able, on a consistent basis, to increase our annual contract values by obtaining advantageous contract renewals. We offer managed security and threat intelligence on a subscription basis under contracts with initial terms that typically range from one to three years and, as of January 31, 2020, averaged two years in duration. Our customers have no obligation to renew their contracts after the expiration of their terms, and we cannot be sure that customer contracts will be renewed on terms favorable to us or at all. The fees we charge for our solutions vary based on a number of factors, including the solutions selected, the number of customer devices covered by the selected solutions and the level of management we provide for the solutions. Our initial contracts with customers may include amounts for hardware, installation and professional services that may not recur. Further, if a customer renews a contract for a term longer than the preceding term, it may pay us greater total fees than it paid under the preceding contract, but still pay lower average annual fees, because we generally offer discounted rates in connection with longer contract terms. In any of these situations, we would need to sell additional solutions to maintain the same level of annual fees from the customer, but may be unable to do so.

We generate a significant portion of our revenue from customers in the financial services industry, and changes within that industry or an unfavorable review by the federal banking regulatory agencies could reduce demand for our solutions.

We derived approximately 25% of our revenue in fiscal 2020 from financial services institutions and expect to continue to derive a substantial portion of our revenue from customers in the financial services industry. Any of a variety of changes in that industry could adversely affect our revenue, profitability and financial condition. Spending by financial services customers on technology generally has fluctuated, and may continue to fluctuate, based on changes in economic conditions and on other factors, such as decisions by customers to reduce or restructure their technology spending in an attempt to improve profitability. Further, mergers or consolidations of financial institutions could reduce our current and potential customer base, resulting in a smaller market for our solutions.

Some of our solutions have been deemed to be mission-critical functions of our financial institution customers that are regulated by one or more member agencies of the Federal Financial Institutions Examination Council, or the FFIEC. We therefore are subject to examination by the member agencies of the FFIEC. The agencies conduct periodic reviews of our operations to identify existing or potential risks associated with our operations that could adversely affect our financial institution customers, evaluate our risk management systems and controls, and determine our compliance with applicable laws that affect the solutions we provide to financial institutions. Areas of examination include our management of technology, data integrity, information confidentiality, service availability and financial stability. A sufficiently unfavorable review could result in our financial institution customers not being allowed, or not choosing, to continue using our solutions, which could adversely affect our revenue, financial condition and results of operations

If we fail to manage our growth effectively, we may be unable to execute our business plan and maintain high levels of customer service, and our operations may be disrupted.

As our customer base and solutions offerings continue to grow, we will be required to further expand our operations, which could place a strain on our resources and infrastructure and affect our ability to maintain the quality of our solutions, deploy our solutions, support our customers after deployment and foster our customer-focused culture. If we are unable to manage our growth, expenses or business effectively, our financial condition, results of operations and profitability could be adversely affected.

As we grow, we must continue to manage efficiently our employees, operations, finances, research and development and capital investments. Our productivity, customer-focused culture and the quality of our solutions may be negatively affected if we do not integrate and train our new employees, particularly our sales and account management personnel, quickly and effectively. In addition, we may need to make substantial investments in additional IT infrastructure to support our growth and will need to maintain or improve our operational, financial and management controls and our reporting procedures, which will require substantial management effort and additional investments in our operations. Further, if we expand our offerings, we may compete more directly with security software and service providers that may be better established or have greater resources than we do, our relationships with our channel and strategic partners may be impaired, and we may be required to comply with additional industry regulations.

Failure to maintain high-quality customer service and support functions could adversely affect our reputation and growth prospects.

Once our solutions are deployed within our customers' networks, our customers depend on our technical and other support services to ensure the security of their IT systems. If we fail to hire, train and retain qualified technical support and professional services employees, our ability to satisfy our customers' requirements could be adversely affected, particularly if the demand for our solutions expands more rapidly than our ability to implement our solutions and provide customer support. The potential for human error in connection with our customer service and support functions or the internal systems and networks that underpin our ability to provide solutions to our customers, even if promptly discovered and remediated, could disrupt customer operations, cause losses for customers or harm our internal operations, lead to regulatory fines or damage our reputation. In addition, if we do not effectively assist our customers to deploy our solutions, resolve post-deployment issues or provide effective ongoing support, our ability to sell additional solutions or subscriptions to existing customers could suffer and our reputation with potential customers could be damaged. If we fail to meet the requirements of our existing customers, particularly larger enterprises that may require higher levels of support, it may be more difficult to realize our strategy of selling higher-margin or different types of solutions to those customers.

Our results of operations may be adversely affected by service level agreements with some of our customers that require us to provide them with credits for service failures or inadequacies.

We have agreements with some of our customers in which we have committed to provide them our solutions at specified levels. If we are unable to meet the commitments, we may be obligated to extend service credits to those customers, or could face terminations of the service agreements. Damages for failure to meet the service levels specified in our service level agreements generally are limited to the fees charged over the previous 12 months, but, if challenged, such limits on damages payable by us may not be upheld, and we may be required to pay damages greater than such fees. Repeated or significant service failures or inadequacies could adversely affect our reputation and results of operations.

If we are unable to continue the expansion of our sales force, the growth of our business could be harmed.

We are substantially dependent on our direct sales force to obtain new customers and increase sales to existing customers, and we believe that our growth will be constrained if we are not successful in recruiting, training and retaining a sufficient number of qualified sales personnel. There is significant competition for sales personnel with the deep skills and technical knowledge required to sell our information security solutions. We may be unable to hire or retain sufficient numbers of qualified individuals in the domestic and international markets in which we do business or plan to do business. Because we seek to grow rapidly, many members of our sales force may be new to our company at any time. Newly hired sales personnel require extensive training and experience in selling activity before they achieve full productivity. Sales force members we have hired recently or plan to hire may not become productive as quickly as we expect. If we are unable to hire and train a sufficient number of effective sales personnel, or the sales personnel we hire are not successful in obtaining new customers or increasing sales to our existing customer base, our business, results of operations and growth prospects will be adversely affected.

Our sales cycles are long and unpredictable, and our sales efforts require considerable time and expense, which could adversely affect our results of operations.

Sales of our information security solutions usually require lengthy sales cycles, which are typically three to nine months, but can exceed 12 months for larger customers. Sales to our customers can be complex and require us to educate our customers about our technical capabilities and the use and benefits of our solutions. Customers typically pursue a significant evaluation and acceptance process, and their subscription decisions frequently are influenced by budgetary constraints, technology evaluations, multiple approvals and unplanned administrative, processing and other delays. We spend substantial time, effort

and money in our sales efforts without any assurance that our efforts will generate long-term contracts. If we do not realize the sales we expect from potential customers, our revenue and results of operations could be adversely affected.

As we continue to expand sales of our information security solutions to customers located outside the United States, our business increasingly will be susceptible to risks associated with international sales and operations.

We have limited experience operating in international jurisdictions compared to our experience operating in the United States. We expect to increase our presence internationally through additional relationships with local and regional strategic and distribution partners and potentially through acquisitions of other companies. International revenue, which we define as revenue contracted through non-U.S. entities, contributed approximately 25% of our total revenue in fiscal 2020. Our lack of experience in operating our business outside the United States increases the risk that any international expansion efforts will not be successful. In addition, operating in international markets requires significant management attention and financial resources. The investment and additional resources required to establish operations and manage growth in other countries may not produce the expected levels of revenue or earnings.

Conducting international operations subjects us to risks that include:

- the time, resources and expense required for localization of our solutions, including translation of our Internet-based portal interface into other languages, provision of customer support in other languages and creation of localized agreements;
- the burdens of complying with a wide variety of international laws, regulations and legal standards, including local data privacy laws, local consumer protection laws that could regulate permitted pricing and promotion practices, and restrictions on the use, import or export of encryption technologies;
- longer accounts receivable payment cycles and difficulties in collecting accounts receivable;
- fluctuations in currency exchange rates;
- tariffs and trade barriers and other regulatory or contractual limitations on our ability to sell or develop our solutions in some international markets;
- difficulties in managing and staffing international operations;
- compliance with U.S. laws that apply to operations outside of the United States, including the Foreign Corrupt Practices Act, or FCPA, the Trading with the Enemy Act and regulations of the Office of Foreign Assets Control;
- potentially adverse tax consequences and compliance costs resulting from the complexities of international tax systems and overlap of different tax regimes;
- reduced or varied protection of intellectual property rights in some countries that could expose us to increased risk of infringement of our patents and other intellectual property;
- global disruptions in custom spending patterns or our ability to provide service to our customers as a result of any widespread public health issues, including a pandemic such as COVID-19; and
- political, social and economic instability, terrorist attacks and security concerns in general.

The occurrence of any of these risks could negatively affect our international business and, consequently, our overall business, results of operations and financial condition.

The United Kingdom's withdrawal from the European Union may adversely impact our operations in the United Kingdom and elsewhere.

Effective on January 31, 2020, the United Kingdom, or U.K., withdrew from the European Union, or EU, commonly referred to as "Brexit," in accordance with the Treaty on European Union. The unsettled terms of the withdrawal, which are subject to negotiation during an 11-month transition period, have created significant uncertainty in areas currently regulated by EU law, such as cross border data transfers. Currently, the most immediate impact on our company may be on certain data transfers from the EU to the U.K., which could impose compliance burdens and cause disruptions to our business. Further, trade, immigration and commercial regulation may be modified during the transition period or permanently, and some of our customers may relocate some or all of their operations to jurisdictions outside of the U.K. in anticipation or as a result of Brexit. Any of these effects of Brexit, and others we cannot anticipate, could adversely affect our business, business opportunities and solutions.

An inability to expand our key distribution relationships would constrain the growth of our business.

We intend to expand our distribution relationships to increase domestic and international sales. Approximately 9% of our revenue in fiscal 2020 was generated through our channel partners, which include referral agents, regional value-added resellers and trade associations. Our strategy is to increase the percentage of our revenue that we derive from sales through our channel partners. Our inability to maintain or further develop relationships with our current and prospective distribution partners could reduce sales of our information security solutions and adversely affect our revenue growth and financial condition.

Our agreements with our partners generally are non-exclusive, and our partners may have more established relationships with one or more of our competitors. If our partners do not effectively market and sell our solutions, if they choose to place greater emphasis on their own products or services or those offered by our competitors or if they fail to meet our customers' needs, our ability to expand our business and sell our solutions may be adversely affected. Our business also may suffer from the loss of a substantial number of our partners, the failure to recruit additional partners, any reduction or delay in the sales of our solutions by our partners, or conflicts between sales by our partners and our direct sales and marketing activities. The gross margins to us from sales by our partners generally are lower than gross margins to us from direct sales. In addition, sales by our partners are more likely than direct sales to involve collectability concerns and may contribute to periodic fluctuations in our results of operations.

Our technology alliance partnerships expose us to a range of business risks and uncertainties that could prevent us from realizing the benefits we seek from these partnerships.

We have entered, and intend to continue to enter, into technology alliance partnerships with third parties to support our future growth plans. Such relationships include technology licensing, joint technology development and integration, research cooperation, co-marketing and sell-through arrangements. We face a number of risks relating to our technology alliance partnerships that could prevent us from realizing the benefits we seek from these partnerships on a timely basis or at all. Technology alliance partnerships can require significant coordination between the partners and a significant commitment of time and resources by their technical staffs. In cases where we wish to integrate a partner's products or services into our solutions, the integration process may be more difficult than we anticipate, and the risk of integration difficulties, incompatibility and undetected programming errors or defects may be higher than the risks normally associated with the introduction of new products or services. In addition, we have no assurance that any particular relationship will continue for any specific period of time. If we lose a significant technology alliance partner, we could lose the benefit of our investment of time, money and resources in the relationship. Moreover, we could be required to incur significant expenses to develop a new strategic alliance or to formulate and implement an alternative plan to pursue the opportunity that we targeted with the former partner.

Real or perceived defects, errors or vulnerabilities in our solutions or the failure or perceived failure of our solutions to prevent or detect a security breach could harm our reputation, cause us to lose customers and expose us to costly litigation.

Our solutions are complex and may contain defects or errors that are not detected until after their adoption by our customers. As a result of such defects, our customers may be vulnerable to cyber attacks, and hackers or other threat actors may misappropriate our customers' data or other assets or otherwise compromise their IT systems. In addition, because the techniques used to access or sabotage IT systems and networks change frequently and generally are not recognized until launched against a target, an advanced attack could emerge that our solutions are unable to detect or prevent. A security breach of proprietary information could result in significant legal and financial exposure, damage to our reputation and a loss of confidence in the security of our solutions that could have an adverse effect on our business.

If any of our customers experiences an IT security breach after adopting our solutions, even if our solutions have blocked the theft of any data or provided some form of remediation, the customer could be disappointed with our solutions and could look to our competitors for alternatives to our solutions. In addition, if any enterprise or government entity publicly known to use our solutions is the subject of a publicized cyber attack, some of our other current customers could seek to replace our solutions with those provided by our competitors. Further, our reputation could be damaged if a cyber attack were to occur through a customer's security or network devices, applications or endpoints that we are not contractually obligated to monitor, if there is a perception that Secureworks monitors all the affected customer's devices, applications and endpoints. Any real or perceived defects, errors or vulnerabilities in our solutions, or any other failure of our solutions to detect an advanced threat, could result in:

- expenditure of significant financial and development resources in efforts to analyze, correct, eliminate or work around the cause of any related vulnerabilities;
- loss of existing or potential customers or channel partners;
- delayed or lost revenue;
- extension of service credits to affected customers, which would reduce our revenue;
- failure to attain or retain market acceptance of our solutions; and
- litigation, regulatory inquiries or investigations that may be costly and harm our reputation.

Any person that circumvents our security measures could misappropriate the confidential information or other valuable property of our customers or disrupt their operations. If such an event occurs, affected customers or others may sue us. Defending a lawsuit, regardless of its merit, could be time-consuming and costly. Because our solutions provide and monitor information security and may protect valuable information, we could face liability claims or claims for breach of service level agreements. Provisions in our service agreements that limit our exposure to liability claims may not be enforceable in some circumstances or may not protect us fully against such claims and related costs. Alleviating any of these problems could require significant expenditures by us and result in interruptions to and delays in the delivery of our solutions, which could cause us to lose existing or potential customers and damage our business and prospects.

Cyber attacks or other data security incidents that disrupt our operations or result in the breach or other compromise of proprietary or confidential information about us or our workforce, customers or other third parties could harm our business and expose us to costly regulatory enforcement and other liability.

As a well-known information security solutions provider, we are a high-profile target and our websites, networks, information systems, solutions and technologies may be selected for sabotage, disruption or misappropriation by cyber attacks specifically designed to interrupt our business and harm our reputation. Our solutions frequently involve the collection, filtering and logging of our customers' information and our enterprise operations involve the collection, processing, storage and disposition of our own human resources, intellectual property and other information. Criminal or other threat actors may seek to penetrate our network security and misappropriate or compromise our confidential information or that of our customers or other third parties, create system disruptions or cause shutdowns. We may experience breaches or other compromises of our information technology systems. Further, hardware and operating system software and applications that we produce or procure from third parties may contain defects in design or manufacture, including "bugs" and other problems that could unexpectedly interfere with the operation of such systems.

The costs to address the foregoing security problems and security vulnerabilities before or after a cyber incident could be significant. Remediation efforts may not be successful and could result in interruptions, delays or cessation of service and loss of existing or potential customers that may impede our sales or other critical functions. Breaches of our security measures and the unapproved dissemination of proprietary information or sensitive or confidential data about us or our customers or other third parties could expose us, our customers or other affected third parties to a risk of loss or misuse of this information, result in regulatory enforcement, litigation and potential liability for us, damage our brand and reputation or otherwise harm our business. We rely in certain limited capacities on third-party data management providers and other vendors whose possible security problems and security vulnerabilities may have similar effects on us.

Adverse legislative or regulatory tax changes or unfavorable outcomes in tax audits and other tax compliance matters could result in an increase in our tax expense or effective income tax rate.

Changes in tax laws (including any future Treasury notices or regulations related to the Tax Cuts and Jobs Act that was signed into law on December 22, 2017) could adversely affect our operations and profitability. In recent years, numerous legislative, judicial, and administrative changes have been made to tax laws applicable to us and similar companies. The Organization for Economic Co-operation and Development (the "OECD"), an international association of 36 countries, including the United States, has issued guidelines that change long-standing tax principles. This may introduce tax uncertainty as countries amend their tax laws to adopt certain parts of the OECD guidelines.

Additional changes to tax laws are likely to occur, and such changes may adversely affect our tax liability. The effective tax rate also could be impacted if our geographic sales mix changes. In addition, any actions by the Company to repatriate non-U.S. earnings for which it has not previously provided for U.S. taxes may affect the effective tax rate.

We are continually under audit in various tax jurisdictions. We may not be successful in resolving potential tax claims that arise from these audits. An unfavorable outcome in certain of these matters could result in an increase in our tax expense. In addition, our provision for income taxes could be adversely affected by changes in the valuation of deferred tax assets.

If our solutions do not interoperate with our customers' IT infrastructure, our solutions may become less competitive and our results of operations may be harmed.

Our solutions must effectively interoperate with each customer's existing or future IT infrastructure, which often has different specifications, utilizes multiple protocol standards, deploys products and services from multiple vendors and contains multiple generations of products and services that have been added over time. As a result, when problems occur in a network, it may be difficult to identify the sources of these problems and avoid disruptions when we provide software updates or patches to defend against particular vulnerabilities. Ineffective interoperation could increase the risk of a successful cyber attack and violations of our service level agreements, which would require us to provide service credits that would reduce our revenue.

In addition, government entities and other customers may require our solutions to comply with security or other certifications and standards. If our solutions are late in achieving or fail to achieve compliance with these certifications and standards, or our competitors achieve compliance with these certifications and standards before we do, we may be disqualified from selling our solutions to such customers or otherwise may be placed at a competitive disadvantage.

Loss of our right or ability to use various third-party technologies could result in short-term disruptions to our business.

We incorporate some third-party technologies into our solutions and may seek to incorporate additional third-party technologies in the future. Any loss of our right to use third-party or other technologies could result in delays in producing or delivering our solutions until we identify and integrate equivalent technologies. If any of the technologies we license or purchase from others, or functional equivalents of these technologies, are no longer available to us or are no longer offered to us on commercially reasonable terms, we would be required either to redesign our solutions and devices to function with technologies available from other parties or to develop these components ourselves, which could result in increased costs or delays in the delivery of our solutions and in the release of new offerings. We also might have to limit the features available in our current or future solutions. If we fail to maintain or renegotiate some of our technology agreements with third parties, we could face significant delays and diversion of resources in attempting to license and integrate other technologies with equivalent functions. Any errors or defects in third-party technologies, any inability to utilize third-party technologies as contemplated, or any inability to procure and implement suitable replacement technologies could adversely affect our business and results of operations by impeding delivery of our solutions.

New and evolving information security, cybersecurity, and data privacy laws and regulations may result in increased compliance costs, impediments to the development or performance of our offerings, and monetary or other penalties.

We are currently subject, and may become further subject, to federal, state and foreign laws and regulations regarding the privacy and protection of personal data or other potentially sensitive information. These laws and regulations address a range of issues, including data privacy, cybersecurity and restrictions or technological requirements regarding the collection, use, storage, protection, retention or transfer of data. The regulatory framework for data privacy and cybersecurity issues worldwide can vary substantially from jurisdiction to jurisdiction, is rapidly evolving and is likely to remain uncertain for the foreseeable future. In the United States, these include laws and regulations promulgated under the authority of state attorneys general. For example, the California Consumer Privacy Act, or CCPA, became effective January 1, 2020, and, among other things, requires covered entities to provide new disclosures to California consumers, affords such consumers new abilities to opt-out of certain sales of personal information, and gives such consumers a private right of action with the possibility of statutory damages between $100 and $750 per California resident per incident for data breaches resulting from the covered entity's violation of its duty to implement and maintain reasonable security measures. We cannot yet predict the full impact of the CCPA on our business or operations, or predict any future changes to the language of the CCPA, but it may require us to modify our data processing practices and policies and to incur substantial costs and expenses in an effort to comply with any such changes. In the United States, state laws also provide for disparate data breach notification regimes that may trigger consumer, customer or regulator notifications, all of which could apply to us in a situation where consumer or employee information is accessed or acquired by unauthorized persons (a "data breach") depending on the information affected. There also have been a number of recent legislative proposals in the United States, at both the federal and state level, that would impose new obligations in the areas of privacy, information security and cybersecurity.

Internationally, most of the jurisdictions in which we operate have established their own data security and privacy legal frameworks with which we or our customers must comply. For example, in the European Economic Area, the General Data Protection Regulation, or GDPR, imposes stringent operational and governance requirements for companies that collect or process personal data of residents of the European Union and Iceland, Norway and Lichtenstein. The GDPR also provides for significant penalties for non-compliance, which can be up to four percent of annual worldwide "turnover" (a measure similar to revenues in the United States). Some countries are considering or have enacted legislation requiring local storage and processing of data that could increase the cost and complexity of delivering our services. In addition, under the GDPR and a

growing number of other legislative and regulatory requirements globally, jurisdictions are adopting consumer, regulator and customer notification and other requirements in the event of a data breach, with the potential for fines and the possibility of such notifications resulting in penalties for late notice or investigations or litigation relating to the reasonableness of security measures.

The costs of compliance with, and other burdens imposed by, these laws and regulations may become substantial and may limit the use and adoption of our offerings, require us to change our business practices, impede the performance and development of our solutions, lead to significant fines, penalties or liabilities for noncompliance with such laws or regulations, including through individual or class action litigation, or result in reputational harm.

If we are not able to maintain and enhance our brand, our revenue and profitability could be adversely affected.

We believe that maintaining and enhancing the Secureworks brand is critical to our relationships with our existing and potential customers, channel partners and employees and to our revenue growth and profitability. Our brand promotion activities, however, may not be successful. Any successful promotion of our brand will depend on our marketing and public relations efforts, our ability to continue to offer high-quality information security solutions and our ability to differentiate successfully our solutions from the services offered by our competitors.

We believe our association with Dell has helped us to build relationships with many of our customers because of Dell's globally recognized brand and the favorable market perception of the quality of its products. We have entered into a trademark license agreement with Dell Inc. under which Dell Inc. has granted us a non-exclusive, royalty-free worldwide license to use the trademark "DELL," solely in the form of "SECUREWORKS-A DELL COMPANY," in connection with our business and products, services and advertising and marketing materials related to our business. Under the agreement, our use of the Dell trademark in connection with any product, service or otherwise is subject to Dell Inc.'s prior review and written approval, which may be revoked at any time. We must immediately cease use of the licensed trademark generally or in connection with any product, services or materials upon Dell Inc.'s written request. The agreement is terminable at will by either party, and we must cease all use of the Dell trademark upon any such termination. If we discontinue our association with Dell in the future, our ability to attract new customers may suffer.

Extending our brand to new solutions that differ from our current offerings may dilute our brand, particularly if we fail to maintain our quality standards in providing the new solutions. Moreover, it may be difficult to maintain and enhance our brand in connection with sales through channel partners. The promotion of our brand will require us to make substantial expenditures, and we anticipate that the expenditures will increase as the information security market becomes more competitive and as we continue to increase our geographic footprint. Even if our promotional activities yield increased revenue, the increased revenue may not offset the additional expenses we incur.

We may expand through acquisitions of other companies, which could divert our management's attention from our current business and could result in unforeseen operating difficulties, increased costs and dilution to our stockholders.

We may make strategic acquisitions of other companies to supplement our internal growth. We could experience unforeseen operating difficulties in assimilating or integrating the businesses, technologies, services, products, personnel or operations of acquired companies, especially if the key personnel of any acquired company choose not to work for us. Further, future acquisitions may:

- involve our entry into geographic or business markets in which we have little or no experience;
- create difficulties in retaining the customers of any acquired business;
- result in a delay or reduction of customer sales for both us and the company we acquire because of customer uncertainty about the continuity and effectiveness of solutions offered by either company; and
- disrupt our existing business by diverting resources and significant management attention that otherwise would be focused on developing our existing business.

To complete an acquisition, we may be required to use a substantial amount of our cash, sell or use equity securities or incur debt to secure additional funds. If we raise additional funds through issuances of equity or convertible debt securities, our existing stockholders could suffer significant dilution, and any new equity securities we issue could have rights, preferences and privileges senior to those of our Class A common stock. Any debt financing obtained by us in the future could involve restrictive covenants that will limit our capital-raising activities and operating flexibility. In addition, we may not be able to obtain additional financing on terms favorable to us or at all, which could limit our ability to engage in acquisitions. We may not realize the anticipated benefits of any acquisition we are able to complete. An acquisition also may negatively affect our results of operations because it may:

- expose us to unexpected liabilities;
- require us to incur charges and substantial indebtedness or liabilities;
- have adverse tax consequences;
- result in acquired in-process research and development expenses, or in the future require the amortization, write-down or impairment of amounts related to deferred compensation, goodwill and other intangible assets; or
- fail to generate a financial return sufficient to offset acquisition costs.

Because we recognize revenue ratably over the terms of our managed security and threat intelligence contracts, decreases in sales of these solutions may not immediately be reflected in our results of operations.

In fiscal 2020, approximately 76% of our revenue was derived from subscription-based solutions, attributable to managed security contracts, while approximately 24% was derived from professional services engagements. Our subscription contracts typically range from one to three years in duration and, as of January 31, 2020, averaged two years in duration. Revenue related to these contracts generally is recognized ratably over the contract term. As a result, we derive most of our quarterly revenue from contracts we entered into during previous fiscal quarters. A decline in new or renewed contracts and any renewals at reduced annual dollar amounts in a particular quarter may not be reflected in any significant manner in our revenue for that quarter, but would negatively affect revenue in future quarters. Accordingly, the effect of significant downturns in contracts may not be fully reflected in our results of operations until future periods. As of January 31, 2020, we billed approximately 58% of our recurring revenue in advance. We may not be able to adjust our outflows of cash to match any decreases in cash received from prepayments if sales decline. In addition, we may be unable to adjust our cost structure to reflect reduced revenue, which would have a negative effect on our earnings in future periods. Our subscription model also makes it difficult for us to increase our revenue rapidly through additional sales in any period, as revenue from new customers must be recognized over the applicable contract term. Accordingly, the effect of significant downturns in sales and market acceptance of our solutions may not be fully reflected in our results of operations in the current period, making it more difficult for investors to evaluate our financial performance.

If the estimates or judgments relating to our critical accounting policies prove to be incorrect, our reported results of operations may be adversely affected.

The preparation of financial statements in conformity with generally accepted accounting principles in the United States of America, or GAAP, requires our management to make estimates and assumptions that affect the amounts reported in our financial statements and accompanying notes. We base our estimates on historical experience and on various other assumptions that we believe to be reasonable under the circumstances. Our reported results of operations may be adversely affected if our assumptions change or if actual circumstances differ from those in our assumptions. Significant assumptions and estimates used in preparing our financial statements include those related to revenue recognition, stock-based compensation and estimates of the amount of loss contingencies. In addition, GAAP is subject to interpretation by the Securities and Exchange Commission, or the SEC, and various other bodies. A change in GAAP or interpretations of GAAP could have a significant effect on our reported results and may affect our reporting of transactions completed before a change is announced. Changes to those rules or the interpretation of our current practices may adversely affect our reported financial results or the way in which we conduct our business.

We are exposed to fluctuations in currency exchange rates, which could negatively affect our financial condition and results of operations.

Our revenue and expenses denominated in foreign currencies are subject to fluctuations due to changes in foreign currency exchange rates. As we expand internationally in accordance with our growth strategy, we will enter into more sales contracts denominated in foreign currencies and incur incremental operating expenses outside the United States. Further, a strengthening of the U.S. dollar could increase the real cost of our solutions and subscriptions to our customers outside the United States, which could adversely affect our non-U.S. sales and results of operations. We do not currently hedge against the risks associated with currency fluctuations, but, as our international operations grow, we may begin to use foreign exchange forward contracts to partially mitigate the impact of fluctuations in net monetary assets denominated in foreign currencies. Any such hedges may be ineffective to protect us fully against foreign currency risk.

Governmental export or import controls could subject us to liability or limit our ability to compete in foreign markets.

Our information security solutions and technologies incorporate encryption technology and may be exported outside the United States only if we obtain an export license or qualify for an export license exception. Compliance with applicable regulatory requirements regarding the export of our solutions and technologies may create delays in the introduction of our solutions and technologies in international markets, prevent our customers with international operations from utilizing our solutions and technologies throughout their global systems or prevent the export of our solutions and technologies to some countries altogether. In addition, various countries regulate the import of our appliance-based technologies and have enacted laws that could limit our ability to distribute, and our customers' ability to implement, our technologies in those countries. Any new export or import restrictions, new legislation or shifting approaches in the enforcement or scope of existing regulations, or in the countries, persons or technologies targeted by such regulations, could result in decreased use of our solutions and technologies by existing customers with international operations, loss of sales to potential customers with international operations and decreased revenue. If we fail to comply with export and import regulations, we may be denied export privileges, be subjected to fines or other penalties or fail to obtain entry for our technologies into other countries.

Failure to comply with the Foreign Corrupt Practices Act, and similar laws associated with our current and future international activities, could subject us to penalties and other adverse consequences.

In some countries where we currently operate or expect to conduct business in the future, it is common to engage in business practices that are prohibited by U.S. laws and regulations, including the FCPA, regardless of where such behavior occurs. Such laws prohibit improper payments or offers of payments to foreign governments and their officials and political parties by U.S. and other business entities for the purpose of obtaining or retaining business. Although we have implemented policies and procedures intended to preclude such practices, some of our employees, consultants, sales agents or channel partners, including those that may be based in or from countries where practices that violate U.S. laws may be customary, may take actions in violation of our procedures and for which we ultimately may be responsible. Violations of the FCPA may result in severe criminal or civil sanctions, including suspension or debarment from contracting with government entities in the United States, and could subject us to other liabilities, which could negatively affect our business and financial condition.

Our disclosure controls and procedures may not prevent or detect all errors or acts of fraud.

We are subject to the periodic reporting requirements of the Securities Exchange Act of 1934, or Exchange Act, and are required to maintain effective disclosure controls and procedures. Our disclosure controls and procedures are designed to provide reasonable assurance that information required to be disclosed by us in reports we file with or furnish to the SEC under the Exchange Act is accumulated and communicated to management and is recorded, processed, summarized and reported within the periods specified in SEC rules and forms. Because of the inherent limitations in our control system, however, misstatements due to error or fraud may occur and not be detected. These inherent limitations include the realities that judgments in decision-making can be faulty and that breakdowns can occur because of simple error. In addition, controls can be circumvented by the individual acts of some persons, by collusion of two or more people or by an unauthorized override of the controls.

Earthquakes, fires, power outages, floods, terrorist attacks, public health issues and other catastrophic events could disrupt our business and ability to serve our customers and could have a material adverse effect on our business, results of operations or financial condition.

A significant natural disaster, such as an earthquake, a fire, a flood or a significant power outage, or a widespread public health issue, such as the COVID-19 pandemic, which began spreading globally in early 2020, could have a material adverse effect on our business, results of operations or financial condition. Although our five counter threat operations centers are designed to be redundant and to offer seamless backup support in an emergency, we rely on two primary data centers and public cloud providers to sustain our operations. While each of these data centers and public cloud providers are capable of sustaining our operations individually, a simultaneous failure of the centers or public cloud providers could disrupt our ability to serve our customers. In addition, our ability to deliver our solutions as agreed with our customers depends on the ability of our supply chain, manufacturing vendors or logistics providers to deliver products or perform services we have procured from them. If any natural disaster, including a pandemic such as COVID-19, impairs the ability of our vendors or service providers to support us on a timely basis, our ability to perform our customer engagements may suffer. Disruptions from COVID-19 or a similar pandemic or public health issue could include, and have included, restrictions on the ability of our employees or the employees of our customers, vendors or suppliers to travel, or closures of our facilities or the facilities of these third parties. Such restrictions or closures could affect our ability to sell our solutions, develop and maintain customer relationships or render services, such as our consulting services, could adversely affect our ability to generate revenues or could lead to inadvertent

breaches of contract by us or by our customers, vendors or suppliers. The COVID-19 pandemic has led to significant disruption of normal business operations globally, as businesses, including Secureworks, have needed to implement modifications to employee travel, employee work locations and employee productivity, in some instances as required by federal, state and local authorities, and has given rise to significant volatility in the global capital markets and financial system. The extent of the impact of COVID-19 on our future operational and financial performance will depend on various future developments, including the duration and spread of the outbreak, impact on our employees, impact on our customers, effect on our sales cycles or costs and effect on our vendors, all of which are uncertain and cannot be predicted, but which could have a material adverse effect on our business, results of operations or financial condition. Acts of terrorism or other geopolitical unrest also could cause disruptions in our business or the business of our supply chain, manufacturing vendors or logistics providers. The adverse impacts of these risks may increase if the disaster recovery plans for us and our suppliers prove to be inadequate.

Risks Related to Intellectual Property

We rely in part on patents to protect our intellectual property rights, and if our patents are ineffective in doing so, third parties may be able to use aspects of our proprietary technology without compensating us.

As of January 31, 2020, we owned 32 issued patents and 24 pending patent applications in the United States and four issued patents and three pending patent applications outside the United States. Obtaining, maintaining and enforcing our patent rights is costly and time-consuming. Moreover, any failure of our patents and patent strategy to protect our intellectual property rights adequately could harm our competitive position. We do not know whether any of our pending patent applications will result in the issuance of patents or whether the examination process will require us to modify or narrow our claims, and even if any of our pending patent applications issues, such patents may not provide us with meaningful protection or competitive advantages, and may be circumvented by third parties. Changes in patent laws, implementing regulations or the interpretation of patent laws may diminish the value of our rights. Our competitors may design around technologies we have patented, licensed or developed. In addition, the issuance of a patent does not give us the right to practice the patented invention. Third parties may have blocking patents that could prevent us from marketing our solutions or practicing our own patented technology.

Third parties may challenge any patent that we own or license, through adversarial proceedings in the issuing offices or in court proceedings, including as a response to any assertion of our patents against them. In any of these proceedings, a court or agency with jurisdiction may find our patents invalid or unenforceable or, even if valid and enforceable, insufficient to provide adequate protection against competing solutions. The standards by which the United States Patent and Trademark Office and its foreign counterparts grant technology-related patents are not always applied predictably or uniformly. The legal systems of some countries do not favor the aggressive enforcement of patents, and the laws of other countries may not allow us to protect our inventions with patents to the same extent as U.S. laws. If any of our patents is challenged, invalidated or circumvented by third parties, and if we do not own or have exclusive rights to other enforceable patents protecting our solutions or other technologies, competitors and other third parties could market products or services and use processes that incorporate aspects of our proprietary technology without compensating us, which may have an adverse effect on our business.

If we are unable to protect, maintain or enforce our non-patented intellectual property rights and proprietary information, our competitive position could be harmed and we could be required to incur significant expenses to enforce our rights.

Our business relies in part on non-patented intellectual property rights and proprietary information, such as trade secrets, confidential information and know-how, all of which offer only limited protection to our technology. The legal standards relating to the validity, enforceability and scope of protection of intellectual property rights in the information technology industry are highly uncertain and evolving. Although we regularly enter into non-disclosure and confidentiality agreements with employees, vendors, customers and other third parties, these agreements may be breached or otherwise fail to prevent disclosure of proprietary or confidential information effectively or to provide an adequate remedy in the event of such unauthorized disclosure. In addition, the existence of our own trade secrets, confidential information and know-how affords no protection against independent discovery or development of such intellectual property by other persons. If our employees, consultants or contractors use technology or know-how owned by third parties in their work for us, disputes may arise between us and those third parties as to the rights in related inventions. Our ability to police that misappropriation or infringement is uncertain, particularly in other countries. Costly and time-consuming litigation could be necessary to enforce and determine the scope of our proprietary rights, and failure to maintain trade secret protection could adversely affect our competitive business position.

Claims by others that we infringe their proprietary technology could harm our business and financial condition.

Third parties could claim that our technologies and the processes underlying our solutions infringe or otherwise violate their proprietary rights. The software and technology industries are characterized by the existence of a large number of patents, copyrights, trademarks and trade secrets and by frequent litigation, including by non-practicing entities, based on allegations of infringement or other violations of intellectual property rights, and we expect that such claims may increase as competition in the information security market continues to intensify, as we introduce new solutions (including in geographic areas where we currently do not operate) and as business-model or product or service overlaps between our competitors and us continue to occur. For example, in fiscal 2016, we settled litigation in which a third party alleged that aspects of our business and solutions infringed and induced the infringement of two of its U.S. patents relating to network intrusion and event monitoring technology.

To the extent that we achieve greater prominence and market exposure as a public company, we may face a higher risk of being the target of intellectual property infringement claims. From time to time, we may receive notices alleging that we have infringed, misappropriated or misused other parties' intellectual property rights. There may be third-party intellectual property rights, including patents and pending patent applications, that cover significant aspects of our technologies, processes or business methods. Any claims of infringement by a third party, even claims without merit, could cause us to incur substantial defense costs and could distract our management and technical personnel from our business, and there can be no assurance that our technologies and processes will be able to withstand such claims. Competitors may have the capability to dedicate substantially greater resources to enforce their intellectual property rights and to defend claims that may be brought against them than we do. Further, a party making such a claim, if successful, could secure a judgment that requires us to pay substantial damages, which potentially could include treble damages if we are found to have willfully infringed patents. A judgment also could include an injunction or other court order that could prevent us from offering our solutions. In addition, we might be required to seek a license or enter into royalty arrangements for the use of the infringed intellectual property, which may not be available on commercially reasonable terms or at all. The failure to obtain a license or the costs associated with any license could materially and adversely affect our business, financial condition and results of operations. If a third party does not offer us a license to its technology or other intellectual property on reasonable terms, we could be precluded from continuing to use such intellectual property. Parties with which we currently have license agreements, or with which we may enter into license agreements in the future, including Dell, may have the right to terminate such agreements for our material breach or for convenience at any time, which could affect our ability to make use of material intellectual property rights. Alternatively, we might be required to develop non-infringing technology, which could require significant effort and expense and ultimately might not be successful.

Third parties also may assert infringement claims against our customers relating to our devices or technology. Any of these claims might require us to initiate or defend potentially protracted and costly litigation on their behalf, regardless of the merits of these claims, because under specified conditions we agree to indemnify our customers from claims of infringement of proprietary rights of third parties. If any of these claims were to succeed, we might be forced to pay damages on behalf of our customers, which could adversely affect our profitability and harm our reputation in the industry.

Our use of open source technology could require us in some circumstances to make available source code of our modifications to that technology, which could include source code of our proprietary technologies, and also may restrict our ability to commercialize our solutions.

Some of our solutions and technologies incorporate software licensed by its authors or other third parties under open source licenses. To the extent that we use open source software, we face risks arising from the scope and requirements of common open source software licenses. Some of these licenses contain requirements that we make available source code for modifications or derivative works we create based on the open source software, and that we license such modifications or derivative works under the terms of a particular open source license or other license granting third parties certain rights of further use. If we combine our proprietary technology with open source software in a certain manner, we may face claims from time to time from third parties claiming ownership of, or demanding release of, the open source software or derivative works that we developed using such software, which could include our proprietary source code, or otherwise seeking to enforce the terms of the applicable open source license. For example, the GNU General Public License could subject certain portions of our proprietary technologies to the requirements of that license, and these, or similar requirements, may have adverse effects on our sale of solutions incorporating such open source software.

Our ability to commercialize solutions or technologies incorporating open source software may be restricted because, among other reasons, open source license terms may be ambiguous and may result in unanticipated or uncertain obligations regarding our solutions, litigation or loss of the right to use this software. The terms of many open source licenses to which we are subject have not been interpreted by courts in the United States or other countries. Therefore, there is a risk that the terms of these

licenses will be construed in a manner that imposes unanticipated conditions or restrictions on our ability to commercialize our solutions, and we could be required to seek licenses from third parties to continue offering our solutions, to re-engineer our technology or to discontinue offering our solutions if re-engineering cannot be accomplished in a commercially reasonable manner. In addition, use of open source software can lead to greater risks than use of third-party commercial software, as open source licensors generally do not provide warranties or controls on the origin of the software, and it may be difficult for us to identify accurately the developers of the open source code and determine whether the open source software infringes third-party intellectual property rights. We would be subject to similar risks with respect to software or technologies we acquire that include open source components. Our need to comply with unanticipated license conditions and restrictions, the need to seek licenses from third parties or any judgments requiring us to provide remedies typically covered by third-party product warranties – each as a result of our use of open source software – could adversely affect our business, results of operations and financial condition.

Risks Related to Our Relationship with Dell and Dell Technologies

As long as Dell Technologies Inc. controls us, the ability of our other stockholders to influence matters requiring stockholder approval will be limited.

We became an indirect wholly-owned subsidiary of Dell Inc. and Dell Inc.'s subsidiaries when we were acquired by Dell on February 8, 2011. On October 29, 2013, Dell Inc. was acquired in a going-private transaction by Denali Holding Inc., a holding company that changed its name to Dell Technologies Inc., or Dell Technologies, in August 2016. Upon the completion of the going-private transaction, we became an indirect wholly-owned subsidiary of Dell Technologies. As of February 1, 2019, the principal beneficial owners of Dell Technologies' outstanding voting securities were Michael S. Dell, the Chairman, Chief Executive Officer and founder of Dell, and investment funds affiliated with Silver Lake Partners, a global private equity firm.

As of January 31, 2020, Dell Technologies owned, indirectly through Dell Inc. and Dell Inc.'s subsidiaries, no shares of our outstanding Class A common stock and all 70,000,000 outstanding shares of our Class B common stock, which represented approximately 86.2% of our total outstanding shares of common stock and approximately 98.4% of the combined voting power of both classes of our outstanding common stock.

So long as Dell Technologies controls the majority of the voting power of our outstanding common stock, our other stockholders will not be able to affect the outcome of any stockholder vote in which holders of the Class B common stock are entitled to vote. Dell Technologies is able to control, directly or indirectly and subject to applicable law, significant matters affecting us, including:

- the election and removal of our directors;
- amendments to our certificate of incorporation;
- determinations with respect to mergers, business combinations, dispositions of assets or other extraordinary corporate transactions; and
- agreements that may adversely affect us.

If Dell Technologies does not provide any requisite affirmative vote on matters requiring stockholder approval allowing us to take particular corporate actions when requested, we will not be able to take such actions, and, as a result, our business and our results of operations may be adversely affected.

Dell Technologies could have interests that differ from, or conflict with, the interests of our other stockholders, and could cause us to take corporate actions even if the actions are not in the interest of our company or our other stockholders, or are opposed by our other stockholders. For example, Dell Technologies' voting control could discourage or prevent a change in control of our company even if some of our other stockholders might favor such a transaction. Even if Dell Technologies were to control less than a majority of the voting power of our outstanding common stock, it may be able to influence the outcome of significant corporate actions by us for as long as it owns a significant portion of the voting power. If Dell Technologies is acquired or otherwise experiences a change in control, any acquiror or successor will be entitled to exercise Dell Technologies' voting control with respect to us, and might do so in a manner that could vary significantly from the manner in which Dell Technologies would have exercised such rights.

Our inability to resolve in a manner favorable to us any potential conflicts or disputes that arise between us and Dell or Dell Technologies with respect to our past and ongoing relationships may adversely affect our business and prospects.

Potential conflicts or disputes may arise between Dell or Dell Technologies and us in a number of areas relating to our past or ongoing relationships, including:

- actual or anticipated variations in our quarterly or annual results of operations;
- tax, employee benefit, indemnification and other matters arising from our relationship with Dell;
- employee retention and recruiting;
- business combinations involving us;
- our ability to engage in activities with certain channel, technology or other marketing partners;
- sales or dispositions by Dell Technologies of all or any portion of its beneficial ownership interest in us;
- the nature, quality and pricing of services Dell has agreed to provide us;
- business opportunities that may be attractive to both Dell and us;
- Dell's ability to use and sublicense patents that we have licensed to Dell under a patent license agreement; and
- product or technology development or marketing activities that may require consent of Dell or Dell Technologies.

The resolution of any potential conflicts or disputes between us and Dell or Dell Technologies over these or other matters may be less favorable to us than the resolution we might achieve if we were dealing with an unaffiliated party.

In April 2016, in connection with our IPO, we entered into a shared services agreement, an employee matters agreement, a tax matters agreement, intellectual property agreements, real estate-related agreements and commercial agreements with Dell or Dell Technologies, which are of varying durations and may be amended upon agreement of the parties. The terms of these agreements were primarily determined by Dell and Dell Technologies, and therefore may not be representative of the terms we could obtain on a stand-alone basis or in negotiations with an unaffiliated third party. For so long as we are controlled by Dell Technologies, we may not be able to negotiate renewals or amendments to these agreements, if required, on terms as favorable to us as those we would be able to negotiate with an unaffiliated third party.

If Dell Technologies, Dell or Dell Technologies' other affiliates or Silver Lake Partners or its affiliates engage in the same type of business we conduct or take advantage of business opportunities that might be attractive to us, our ability to operate successfully and expand our business may be hampered.

Our certificate of incorporation, or charter, provides that, except as otherwise agreed in writing between us and Dell Technologies, Dell or Dell Technologies' other affiliates (other than us or our controlled affiliates), referred to as the Dell Technologies Entities, have no duty to refrain from:

- engaging in the same or similar activities or lines of business as those in which we are engaged;
- doing business with any of our customers, customers or vendors; or
- employing, or otherwise engaging or soliciting for such purpose, any of our officers, directors or employees.

In addition, under our charter, Silver Lake Partners and its affiliates, referred to as the Silver Lake Entities, have no duty to refrain from any of the foregoing activities except as otherwise agreed in writing between us and a Silver Lake Entity.

Provisions of our charter could result in the Dell Technologies Entities and the Silver Lake Entities having rights to corporate opportunities in which both we and the Dell Technologies Entities or the Silver Lake Entities have an interest. Our charter addresses potential conflicts of interest between our company, on the one hand, and the Dell Technologies Entities or the Silver Lake Entities and their respective officers and directors who are officers or directors of our company, on the other hand. If any Dell Technologies Entity or Silver Lake Entity is offered, or acquires knowledge of, a potential corporate opportunity suitable for both it and us, we will have no interest in that opportunity. Our charter also provides that if any of our directors or officers who is also a director or officer of any Dell Technologies Entity or Silver Lake Entity is offered, or acquires knowledge of, a potential corporate opportunity suitable for both the Dell Technologies Entity or the Silver Lake Entity and us, we will have no interest in that opportunity unless the opportunity is expressly offered to that person in writing solely in such person's capacity as our director or officer.

Our historical financial information as a subsidiary of Dell before our initial public offering may not be representative of our results as an independent public company.

The historical financial statements and the related financial information presented in this annual report on Form 10-K for periods before our initial public offering do not purport to reflect what our results of operations, financial position, equity or cash flows would have been if we had operated as a stand-alone public company during those periods. Such financial statements include allocations for various corporate services Dell has provided to us in the ordinary course of our business, including finance, tax, human resources, legal, insurance, IT, procurement and facilities-related services. As a result, those historical financial statements may not be comparable to our financial statements as a stand-alone public company.

To preserve Dell Technologies' ability to conduct a tax-free distribution of the shares of our Class B common stock that it beneficially owns and its ability to consolidate with us for tax purposes, we may be prevented from pursuing opportunities to raise capital, acquire other companies or undertake other transactions, which could hurt our ability to grow.

To preserve its ability to effect a future tax-free spin-off of our company, or certain other tax-free transactions involving us, Dell Technologies is required to maintain "control" of us within the meaning of Section 368(c) of the Internal Revenue Code, which is defined as 80% of the total voting power and 80% of each class of nonvoting stock. In addition, to preserve its ability to consolidate with us for tax purposes, Dell Technologies generally is required to maintain 80% of the voting power and 80% of the value of our outstanding stock. We have entered into a tax matters agreement with Dell Technologies, that restricts our ability to issue any stock, issue any instrument that is convertible, exercisable or exchangeable into any of our stock or which may be deemed to be equity for tax purposes, or take any other action that would be reasonably expected to cause Dell Technologies to beneficially own stock in us that, on a fully diluted basis, does not constitute "control" within the meaning of Section 368(c) of the Internal Revenue Code or to cause a deconsolidation of us for tax purposes with respect to the Dell Technologies consolidated group. We also have agreed to indemnify Dell Technologies for any breach by us of the tax matters agreement. As a result, we may be prevented from raising equity capital or pursuing acquisitions or other growth initiatives that involve issuing equity securities as consideration.

Our ability to operate our business effectively may suffer if we are unable to establish in a cost-effective manner our own administrative and other support functions in order to operate as a stand-alone company after the expiration of our shared services and other agreements with Dell.

As a subsidiary of Dell, we have relied on administrative and other resources of Dell to operate our business. In connection with our IPO, we entered into various agreements to retain the ability for varying periods to use these Dell resources. These services may not be sufficient to meet our needs, and if our agreements with Dell are not renewed by the parties after their initial terms, we may not be able to replace the services at all or obtain them at prices and on terms as favorable as those under our current arrangements with Dell. In such a case, we may need to create our own administrative and other support systems or contract with third parties to replace Dell's systems. In addition, we also license certain software from third parties used in support of our operations that utilize agreements to which Dell is a party and, as a result, enjoy favorable pricing relative to pricing we may otherwise have received had we negotiated pricing terms separately from Dell. If we no longer are able to utilize the pricing in such agreements, our costs to license such software may increase. Further, we have received informal support from Dell that may not be available under our new agreements, and the level of this informal support may diminish as we become a more independent company. Any significant performance failures affecting our own administrative systems or Dell's administrative systems on which we rely could result in unexpected costs, adversely affect our results and prevent us from paying our suppliers or employees and performing other administrative services on a timely basis.

In connection with our IPO, we entered into agreements with Dell that formalize the process and terms pursuant to which Dell purchases information security solutions from us, together with related hardware, and pursuant to which we procure hardware and software from Dell from time to time. These agreements may not be renewed after their expiration or, if they are renewed, Dell may not agree to renew them on the existing terms. The expiration or termination of these agreements, or their renewal on less favorable terms to us, could result in a loss of business or require us to procure comparable hardware and software from alternative sources, which could have a material adverse effect on our business, results of operations and financial condition.

Risks Related to Ownership of Our Class A Common Stock

The price of our Class A common stock may be volatile.

The trading prices of the securities of technology companies historically have experienced high levels of volatility, and the trading price of our Class A common stock has fluctuated since our IPO and may fluctuate substantially in future periods. The trading price of our Class A common stock could fluctuate as a result of the following factors, among others:

- announcements of new products, services or technologies, commercial relationships, acquisitions or other events by us or our competitors;
- changes in how customers perceive the effectiveness of our solutions in protecting against advanced cyber attacks;
- actual or anticipated variations in our quarterly or annual results of operations;
- changes in our financial guidance or estimates by securities analysts;
- price and volume fluctuations in the overall stock market from time to time;
- significant volatility in the market price and trading volume of technology companies in general and of companies in the information security industry in particular;
- actual or anticipated changes in the expectations of investors or securities analysts;
- fluctuations in the trading volume of our shares or the size of the trading market for our shares held by non-affiliates;
- litigation involving us, our industry, or both, including disputes or other developments relating to our ability to patent our processes and technologies and protect our other proprietary rights;
- regulatory developments in the United States and other jurisdictions in which we operate;
- general economic and political factors, including market conditions in our industry or the industries of our customers;
- major catastrophic events;
- sales of large blocks of our Class A common stock; and
- additions or departures of key employees.

If the market for technology stocks or the stock market in general experiences a loss of investor confidence, the trading price of our Class A common stock could decline for reasons unrelated to our business, results of operations or financial condition. The market price of our Class A common stock also might decline in reaction to events that affect other companies in our industry, even if these events do not directly affect us.

In the past, following periods of volatility in the market price of a company's securities, securities class action litigation has often been brought against that company. If our stock price is volatile, we may become the target of securities litigation, which could cause us to incur substantial costs and divert our management's attention and resources from our business.

If securities or industry analysts do not publish research or reports about our business, or publish inaccurate or unfavorable research reports about our business or prospects, the market price of our Class A common stock and trading volume could decline.

The trading market for our Class A common stock depends in part on the research and reports that securities or industry analysts publish about us, our business or our prospects. We do not have any control over these analysts. If one or more of the analysts covering us should downgrade our shares or express a change of opinion regarding our shares, the market price of our Class A common stock could decline. If one or more of these analysts should cease coverage of our company or fail to publish reports on us on a regular basis, we could lose following in the financial markets, which could cause the market price or trading volume of our Class A common stock to decline.

The dual-class structure of our common stock may adversely affect the trading price of our Class A common stock.

Our Class B common stock has ten votes per share and our Class A common stock has one vote per share. The limited ability of holders of our Class A common stock to influence matters requiring stockholder approval may adversely affect the market price of our Class A common stock.

In addition, in 2017, FTSE Russell and S&P Dow Jones changed their eligibility criteria to exclude new companies with multiple classes of shares of common stock from being added to certain stock indices. FTSE Russell instituted a requirement

that new and, beginning in September 2022, existing constituents of its indices have greater than 5% of their voting rights in the hands of public stockholders, as calculated by FTSE Russell, whereas S&P Dow Jones announced that companies with multiple share classes, such as ours, will not be eligible for inclusion in the S&P 500, S&P MidCap 400 and S&P SmallCap 600, which together make up the S&P Composite 1500. Other major stock indices might adopt similar requirements in the future. FTSE Russell has published an indicative list of companies affected by its policy, including its analysis of the percentage of each company's voting rights in the hands of public stockholders. FTSE Russell's calculation, in accordance with its analysis, of Secureworks' voting rights in the hands of public stockholders, was approximately 1.17%, as disclosed in this indicative list. FTSE Russell's determination may change at any time. Under the current criteria, our dual-class capital structure makes our Class A common stock ineligible for inclusion in any of these indices and, as a result, mutual funds, exchange-traded funds and other investment vehicles that track these indices will not invest in our stock. It is unclear what effect, if any, exclusion from any indices will have on the valuations of the affected publicly-traded companies. It is possible that such policies could depress the valuations of public companies excluded from such indices compared to those of other companies that are included.

As a "controlled company" under the marketplace rules of the Nasdaq Stock Market, we may rely on exemptions from certain corporate governance requirements that provide protection to stockholders of companies that are subject to such requirements.

As of January 31, 2020, Dell Technologies beneficially owns more than 50% of the combined voting power of both classes of our outstanding shares of common stock. As a result, we are a "controlled company" under the marketplace rules of the Nasdaq Stock Market, or Nasdaq, and eligible to rely on exemptions from Nasdaq corporate governance requirements generally obligating listed companies to maintain:

- a board of directors having a majority of independent directors;
- a compensation committee composed entirely of independent directors that approves the compensation payable to the company's chief executive officer and other executive officers; and
- a nominating committee composed entirely of independent directors that nominates candidates for election to the board of directors, or that recommends such candidates for nomination by the board of directors (or obligating the listed company to cause a majority of the board's independent directors to exercise this oversight of director nominations).

We currently rely on the exemption from the requirement to maintain a board of directors having a majority of independent directors. Although we do not currently rely on the other exemptions from Nasdaq's corporate governance requirements, we may decide to avail ourselves of one or more of these exemptions in the future. During any period in which we do so, investors may not have the same protections afforded to stockholders of companies that must comply with all of Nasdaq's corporate governance requirements. Our status as a controlled company could make our Class A common stock less attractive to some investors or otherwise adversely affect its trading price.

Future sales, or the perception of future sales, of a substantial amount of shares of our Class A common stock could depress the trading price of our Class A common stock.

Sales of a substantial number of shares of our Class A common stock in the public market, or the perception that these sales may occur, could adversely affect the market price of the Class A common stock at such time, which could make it more difficult for investors to sell their shares of our Class A common stock at a time and price that they consider appropriate, and could impair our ability to raise equity capital or use our Class A common stock as consideration for acquisitions of other businesses, investments or other corporate purposes.

As of January 31, 2020, we have outstanding 11,206,287 shares of our Class A common stock and 70,000,000 shares of our Class B common stock. Of these shares, the 8,000,000 shares of Class A common stock that were sold in our IPO are freely tradeable without restriction or further registration under the Securities Act of 1933, or Securities Act, unless these shares are held by our "affiliates," as that term is defined in Rule 144 under the Securities Act, or Rule 144. As of January 31, 2020, Dell Technologies owned, indirectly through its subsidiary Dell Inc. and through Dell Inc.'s subsidiaries, no shares of our Class A common stock and all 70,000,000 outstanding shares of our Class B common stock. The shares of our Class A common stock eligible for resale by our affiliates under Rule 144, subject to the volume limitations and other requirements of Rule 144, include the 70,000,000 shares of Class A common stock issuable upon conversion of the same number of shares of our Class B common stock that are outstanding.

We have entered into a registration rights agreement with Dell Marketing L.P. (the record holder of our Class B common stock), Michael S. Dell, the Susan Lieberman Dell Separate Property Trust, MSDC Denali Investors, L.P., MSDC Denali EIV, LLC and the Silver Lake Partners investment funds that own Dell Technologies common stock in which we have granted them and their respective permitted transferees demand and piggyback registration rights with respect to the shares of our Class A

common stock and Class B common stock held by them from time to time. In addition, we have entered into a registration rights agreement with the holders of shares of Class A common stock issued upon conversion of our convertible notes at the closing of our IPO in which we have granted such holders and their permitted transferees shelf and piggyback registration rights with respect to such shares. Registration of those shares under the Securities Act would permit the stockholders under each registration rights agreement to sell their shares into the public market.

Our issuance of additional capital stock in connection with financings, acquisitions, investments, our stock incentive plans or otherwise will dilute all other stockholders.

Our charter authorizes us to issue up to 2,500,000,000 shares of Class A common stock, up to 500,000,000 shares of Class B common stock and up to 200,000,000 shares of preferred stock with such rights and preferences as may be determined by our board of directors. Subject to compliance with applicable law, we may issue our shares of Class A common stock or securities convertible into our Class A common stock from time to time in connection with a financing, acquisition, investment, our stock incentive plans or otherwise. We may issue additional shares of Class A common stock from time to time at a discount to the market price of our Class A common stock at the time of issuance. Any issuance of Class A common stock could result in substantial dilution to our existing stockholders and cause the market price of our Class A common stock to decline.

Provisions in our charter and bylaws and in Delaware law could discourage takeover attempts even if our stockholders might benefit from a change in control of our company.

Provisions in our charter and bylaws and in Delaware law may discourage, delay or prevent a merger, acquisition or other change in control of our company that stockholders may favor, including transactions in which stockholders might receive a premium for their shares of Class A common stock. These provisions also could make it more difficult for investors in our Class A common stock to elect directors of their choosing and to cause us to take other corporate actions they support, including removing or replacing our current management. The charter and bylaw provisions:

- provide that our Class B common stock is entitled to ten votes per share, while our Class A common stock is entitled to one vote per share, enabling Dell Technologies, as the beneficial owner of all outstanding shares of our Class B common stock, to control the outcome of all matters submitted to a vote of our stockholders, including the election of directors, in which holders of the Class B common stock are entitled to vote;
- provide for the classification of the board of directors into three classes, with approximately one-third of the directors to be elected each year;
- limit the number of directors constituting the entire board of directors to a maximum of 15 directors, subject to the rights of the holders of any outstanding series of preferred stock, and provide that the authorized number of directors at any time will be fixed exclusively by a resolution adopted by the affirmative vote of the authorized number of directors (without regard to vacancies);
- provide that, at such time (if any) as the Dell Technologies Entities beneficially own capital stock representing less than 40% in voting power of the capital stock entitled to vote generally on the election of directors, any newly-created directorship and any vacancy on the board of directors may be filled only by the affirmative vote of a majority of the remaining directors then in office;
- provide that, at such time (if any) as the Dell Technologies Entities beneficially own capital stock representing less than 50% in voting power of the capital stock entitled to vote generally on the election of directors, directors may be removed only for cause and only by the affirmative vote of the holders of at least a majority in voting power of all outstanding shares of capital stock, voting together as a single class;
- provide that a special meeting of stockholders may be called only by our chairman of the board, a majority of the directors then in office or, so long as Dell Technologies Entities beneficially own capital stock representing at least 40% in voting power of the capital stock entitled to vote generally on the election of directors, Dell Technologies;
- provide that, at such time (if any) as the Dell Technologies Entities beneficially own capital stock representing less than 50% in voting power of the capital stock entitled to vote generally on the election of directors, any action required or permitted to be taken by our stockholders at any annual or special meeting may not be effected by a written consent in lieu of a meeting unless such action and the taking of such action by written consent have been approved in advance by our board of directors;
- establish advance notice procedures for stockholders to make nominations of candidates for election as directors or to present any other business for consideration at any annual or special stockholder meeting; and

- provide authority for the board of directors without stockholder approval to authorize the issuance of up to 200,000,000 shares of preferred stock, in one or more series, with terms and conditions, and having rights, privileges and preferences, to be determined by the board of directors.

In addition, we will become subject to Section 203 of the Delaware General Corporation Law at such time (if any) as the Dell Technologies Entities cease to own beneficially capital stock representing at least 10% in voting power of the capital stock entitled to vote generally on the election of directors. With specified exceptions, this statute prohibits a Delaware corporation listed on a national securities exchange from engaging in a business combination (as defined in Section 203) with an interested stockholder (generally a person who, together with its affiliates and associates, owns 15% or more of the corporation's voting stock) for a period of three years after the date of the transaction in which the person became an interested stockholder (unless the corporation's board of directors approved in advance the transaction in which such person became an interested stockholder).

Our charter designates the Court of Chancery of the State of Delaware as the sole and exclusive forum for certain types of actions and proceedings that may be initiated by our stockholders, which could limit our stockholders' ability to obtain a favorable judicial forum for disputes with us or with our directors, our officers or other employees, or our majority stockholder.

Our charter provides that, unless we consent in writing to the selection of an alternative forum, the Court of Chancery of the State of Delaware will, to the fullest extent permitted by law, be the exclusive forum for:

- any derivative action or proceeding brought on our behalf;
- any action asserting a claim of breach of a fiduciary duty owed by, or other wrongdoing by, any of our directors, officers or other employees, or stockholders to us or our stockholders;
- any action asserting a claim arising pursuant to any provision of the Delaware General Corporation Law or as to which the Delaware General Corporation Law confers jurisdiction on the Court of Chancery of the State of Delaware; and
- any action asserting a claim governed by the internal affairs doctrine.

Any person purchasing or otherwise acquiring any interest in shares of our capital stock is deemed to have received notice of and consented to the foregoing provisions. This choice of forum provision may limit a stockholder's ability to bring a claim in a judicial forum that it finds more favorable for disputes with us or with our directors, our officers or other employees, or our other stockholders, including our majority stockholder, which may discourage such lawsuits against us and such other persons. Alternatively, if a court were to find this choice of forum provision inapplicable to, or unenforceable in respect of, one or more of the specified types of actions or proceedings, we may incur additional costs associated with resolving such matters in other jurisdictions, which could adversely affect our business, results of operations and financial condition.

Our choice of forum provision is intended to apply to the fullest extent permitted by law to the above-specified types of actions and proceedings, including, to the extent permitted by the federal securities laws, to lawsuits asserting both the above-specified claims and claims under the federal securities laws. Application of the choice of forum provision may be limited in some instances by applicable law. Section 27 of the Exchange Act creates exclusive federal jurisdiction over all suits brought to enforce any duty or liability created by the Exchange Act or the rules and regulations thereunder. As a result, the choice of forum provision will not apply to actions arising under the Exchange Act or the rules and regulations thereunder. Section 22 of the Securities Act creates concurrent jurisdiction for federal and state courts over suits brought to enforce any duty or liability created by the Securities Act or the rules and regulations thereunder, subject to a limited exception for certain "covered class actions." There is uncertainty, particularly in light of current litigation, as to whether a court would enforce the choice of forum provision with respect to claims under the Securities Act. Our stockholders will not be deemed, by operation of our choice of forum provision, to have waived claims arising under the federal securities laws and the rules and regulations thereunder.

We do not expect to pay any dividends on our Class A common stock for the foreseeable future.

We intend to retain any earnings to finance the operation and expansion of our business, and do not expect to pay any cash dividends on our Class A common stock for the foreseeable future. Accordingly, investors must rely on sales of our Class A common stock after price appreciation, which may never occur, as the only way to realize any future gains on their investment.

We are an "emerging growth company," and our election to comply with the reduced disclosure requirements as a public company may make our Class A common stock less attractive to investors.

We have qualified as an "emerging growth company" as defined in the Jumpstart Our Business Startups Act of 2012, or JOBS Act, since we completed our initial public offering in April 2016. For so long as we remain an emerging growth company, we are permitted and currently intend to rely on the following provisions of the JOBS Act that contain exceptions from disclosure and other requirements that otherwise are applicable to companies that file periodic reports with the SEC. The JOBS Act provisions:

- provide an exemption from the auditor attestation requirement in the assessment of our internal control over financial reporting under the Sarbanes-Oxley Act of 2002, or the Sarbanes-Oxley Act;
- permit us to include reduced disclosure regarding executive compensation in our SEC filings; and
- provide an exemption from the requirement to hold a non-binding advisory vote on executive compensation and stockholder approval of any golden parachute arrangements not previously approved.

We will remain an emerging growth company until: (a) the first to occur of the last day of the fiscal year (1) which follows the fifth anniversary of the completion of our IPO, (2) in which we have total annual gross revenue of at least $1 billion or (3) in which the market value of our capital stock held by non-affiliates was $700 million or more as of the last business day of the preceding second fiscal quarter; or (b) if it occurs before any of the foregoing dates, the date on which we have issued more than $1 billion in non-convertible debt over a three-year period.

Some investors may find our Class A common stock less attractive if we rely on these exemptions, which could result in a less active trading market for our Class A common stock and higher volatility in our stock price.

We are obligated to develop and maintain proper and effective internal control over financial reporting and any failure to maintain the adequacy of our internal controls may adversely affect investor confidence in our company and, as a result, the value of our Class A common stock.

We are required, pursuant to Section 404 of the Sarbanes-Oxley Act, or Section 404, to furnish a report by our management on, among other matters, the effectiveness of our internal control over financial reporting. Our independent registered public accounting firm will not be required to attest to the effectiveness of our internal control over financial reporting until our first annual report required to be filed with the SEC following the date we are no longer an emerging growth company. We are required to disclose significant changes made in our internal control procedures on a quarterly basis.

During the evaluation and testing process of our internal controls, if we identify one or more material weaknesses in our internal control over financial reporting, we will be unable to assert that our internal control over financial reporting is effective. We may experience material weaknesses or significant deficiencies in our internal control over financial reporting. Any failure to maintain internal control over financial reporting could severely inhibit our ability to report accurately our financial condition or results of operations. If we are unable to conclude that our internal control over financial reporting is effective, or if our independent registered public accounting firm determines we have a material weakness in our internal control over financial reporting, we could lose investor confidence in the accuracy and completeness of our financial reports, the market price of our Class A common stock could decline, and we could be subject to sanctions or investigations by the SEC or other regulatory authorities. Failure to remedy any material weakness in our internal control over financial reporting, or to implement or maintain other effective control systems required of public companies, also could restrict our future access to the capital markets.

Item 1B. Unresolved Staff Comments

None.

Item 2. Properties

As of January 31, 2020, our facilities consisted of our corporate headquarters, five counter threat operations centers, two primary data centers, and various other Dell facilities housing our research and development, marketing and sales functions, and administrative and IT operations support. We either lease these facilities or have the right to use them pursuant to service agreements, either with Dell or with other third parties. As of January 31, 2020, we did not own any facilities.

Our corporate headquarters, as well as one of our counter threat operations centers and one of our data centers, is located in Atlanta, Georgia, where we lease facilities of approximately 141,229 square feet. As of January 31, 2020, we leased or licensed facilities for our other counter threat operations centers in the following locations: Chicago, Illinois; Providence, Rhode Island; Edinburgh, Scotland; and Bucharest, Romania. Our employees also operate out of a number of Dell facilities around the globe pursuant to arrangements with Dell. For information about our facility leases, see "Notes to Consolidated Financial Statements —Note 8—Leases" in our consolidated financial statements included in this report.

As we expand, we intend to lease or license additional sites, either from Dell or other third parties, for counter threat operations centers, sales offices and other functions. We believe that suitable additional facilities will be available on commercially reasonable terms to accommodate the foreseeable expansion of our operations.

Item 3. Legal Proceedings

From time to time, we are a party to or otherwise subject to legal proceedings that arise in the ordinary course of our business. As of January 31, 2020, we were not subject to any material pending legal proceedings.

Item 4. Mine Safety Disclosures

Not applicable.

Part II

Item 5. Market for Registrant's Common Equity, Related Stockholder Matters and Issuer Purchases of Equity Securities

Market for Class A Common Stock

Our Class A common stock is listed and traded on the Nasdaq Global Select Market under the symbol “SCWX.” There is no public market for our Class B common stock.

Holders

As of March 26, 2020, there were ten holders of record of our Class A common stock and one holder of record of our Class B common stock. The number of record holders does not include individuals or entities that beneficially own shares of Class A common stock, but whose shares are held of record by a broker, bank or other nominee.

Dividends

Subsequent to the listing of our Class A common stock on the Nasdaq Global Select Market, we have not declared or paid cash dividends on our common stock. We do not anticipate declaring or paying any cash dividends on our common stock in the foreseeable future. We currently intend to retain all available funds and any future earnings to support our operations and finance the growth and development of our business. Any future determination related to our dividend policy will be made at the discretion of our board of directors and will depend upon, among other factors, our results of operations, financial condition, capital requirements, contractual restrictions, business prospects and other factors our board of directors may deem relevant.

Purchases of Equity Securities

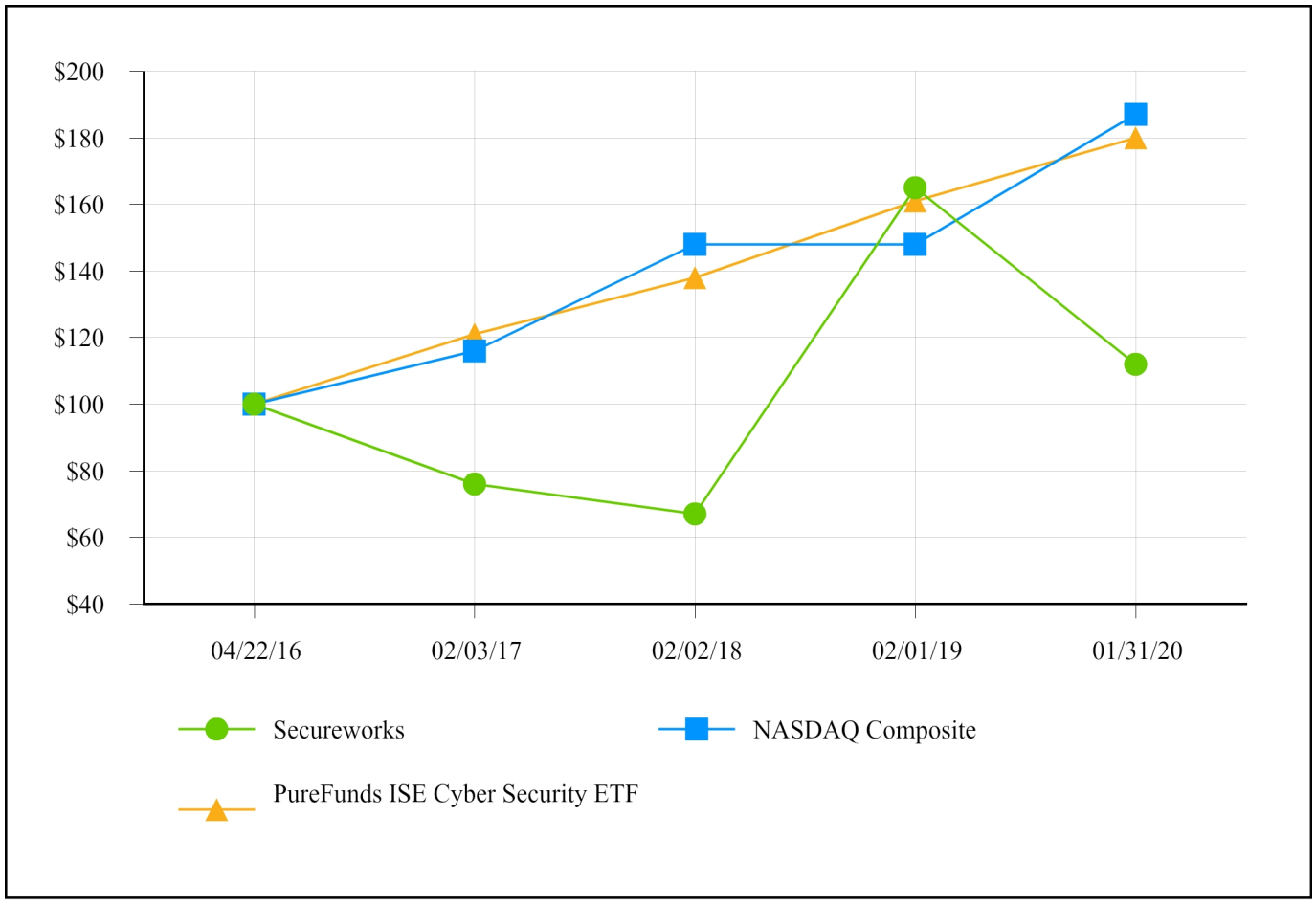
The following table presents information with respect to purchases of Class A common stock by the Company during the three months ended January 31, 2020.

Period	Total Number of Shares Purchased	Average Price Paid per Share	Total Number of Shares Purchased as Part of Publicly Announced Programs	Dollar Value of Shares that May Yet Be Purchased Under Publicly Announced Programs
November 2, 2019 through November 29, 2019	—	$ —	—	10,090,036
November 30, 2019 through December 27, 2019	—	—	—	10,090,036
December 28, 2019 through January 31, 2020	—	—	—	10,090,036
Total	—	$ —	—	$ 10,090,036

On September 27, 2018, the Company announced a stock repurchase program under which the Company is authorized to repurchase up to $15 million of its Class A common stock through September 30, 2019. On March 26, 2019, our board of directors expanded our stock repurchase program to authorize the repurchase of up to an additional $15 million of Class A common stock from time to time through May 1, 2020.

Stock Performance Graph

The following graph compares the cumulative total return on the Class A common stock for the period from April 22, 2016, the date on which the Class A common stock began trading on the Nasdaq Global Select Market, through January 31, 2020 with the total return over the same period on the Nasdaq Composite Index and the PureFunds ISE Cyber Security ETF Index. The graph assumes that $100 was invested on April 22, 2016 in the Class A common stock and in each of the foregoing indices and assumes reinvestment of dividends, if any. The comparisons in the graph are based on historical data and are not necessarily indicative of the future price performance of the Class A common stock.



	April 22, 2016	February 3, 2017	February 2, 2018	February 1, 2019	January 31, 2020
Secureworks	$ 100.00	$ 75.64	$ 67.43	$ 165.07	$ 112.36
NASDAQ Composite	100.00	115.50	147.59	148.05	186.52
PureFunds ISE Cyber Security ETF	100.00	121.21	137.94	161.01	179.55

This performance graph shall not be deemed to be incorporated by reference by means of any general statement incorporating by reference this annual report on Form 10-K into any filing under the Securities Act of 1933 or the Securities Exchange Act of 1934, except to the extent that Secureworks specifically incorporates such information by reference, and shall not otherwise be deemed filed under such Acts.

Item 6. Selected Financial Data

The following selected financial data presented below should be read in conjunction with Part II, Item 7, "Management's Discussion and Analysis of Financial Condition and Results of Operations," and with our audited financial statements and accompanying notes appearing in Part II, Item 8, "Financial Statements and Supplementary Data," of this Annual Report on Form 10-K to fully understand the factors that affect the comparability of the information presented below. The results of operations for the fiscal years ended January 31, 2020, February 1, 2019 and February 2, 2018 and the balance sheet data as of January 31, 2020 and February 1, 2019 are derived from our audited financial statements appearing in Part II, Item 8, "Financial Statements and Supplementary Data," of this Annual Report on Form 10-K. The results of operations for the fiscal years ended February 3, 2017 and January 29, 2016, and the balance sheet data as of February 2, 2018 and January 29, 2016 are derived from audited financial statements, while the balance sheet data for the fiscal year ended February 3, 2017 are derived from our financial statements not included in this Annual Report on Form 10-K. Our historical results are not necessarily indicative of the results to be expected in the future.

The selected balance sheet data as of January 31, 2020 reflects the prospective adoption of Accounting Standards Update No. 2016-02, "Leases (Topic 842)" ("ASU No. 2016-02"), also referred to as Topic 842. The selected results of operations and balance sheet data for fiscal 2018 and 2017 reflect the retrospective adoption of Accounting Standards Update ("ASU") No. 2014-09, "Revenue from Contracts with Customers, also referred to as Topic 606.

	Fiscal Year Ended				
	January 31, 2020	February 1, 2019	February 2, 2018	February 3, 2017	January 29, 2016
	(in thousands, except per share data)				
Results of Operations:					
Net revenue	$ 552,765	$ 518,709	$ 467,930	$ 432,751	$ 339,522
Gross margin	$ 299,969	$ 272,592	$ 242,846	$ 220,262	$ 155,713
Operating expenses	$ 352,143	$ 321,324	$ 312,827	$ 276,141	$ 261,721
Operating loss	$ (52,174)	$ (48,732)	$ (69,981)	$ (55,879)	$ (106,008)
Net loss	$ (31,666)	$ (39,101)	$ (10,417)	$ (31,641)	$ (72,381)
Share and Per Share Data					
Net loss per share - basic and diluted	$ (0.39)	$ (0.48)	$ (0.13)	$ (0.41)	$ (1.03)
Weighted average shares outstanding - basic and diluted	80,563	80,710	80,280	77,635	70,000

	January 31, 2020	February 1, 2019	February 2, 2018	February 3, 2017	January 29, 2016
			(in thousands)		
Balance Sheet:					
Cash and cash equivalents	$ 181,838	$ 129,592	$ 101,539	$ 116,595	$ 33,422
Accounts receivable	$ 111,798	$ 141,344	$ 157,764	$ 113,546	$ 116,357
Total assets[(1)]	$ 1,048,031	$ 1,036,159	$ 1,057,081	$ 1,047,544	$ 917,785
Short-term deferred revenue	$ 175,847	$ 157,865	$ 137,697	$ 117,999	$ 109,467
Short-term convertible notes	$ —	$ —	$ —	$ —	$ 27,993
Long-term deferred revenue	$ 12,690	$ 16,064	$ 14,948	$ 14,752	$ 18,352
Total stockholder's equity	$ 666,880	$ 692,707	$ 731,090	$ 725,455	$ 588,456

[(1)] Reflects the impact of the adoption of the new lease accounting standard in fiscal 2020 which was adopted prospectively.

Item 7. Management's Discussion and Analysis of Financial Condition and Results of Operations

This management's discussion and analysis is based upon the financial statements of Secureworks which have been prepared in accordance with accounting principles generally accepted in the United States, or GAAP, and should be read in conjunction with our consolidated financial statements and related notes included in this report. In addition to historical financial information, the following discussion contains forward-looking statements that reflect our plans, estimates and beliefs. Our actual results could differ materially from those discussed or implied in our forward-looking statements. Factors that could cause or contribute to these differences include those discussed in "Risk Factors."

Our fiscal year is the 52- or 53-week period ending on the Friday nearest January 31. We refer to our fiscal years ended January 31, 2020, February 1, 2019 and February 2, 2018, as fiscal 2020, fiscal 2019 and fiscal 2018, respectively. Fiscal 2020, fiscal 2019 and fiscal 2018 each included 52 weeks. All percentage amounts and ratios presented in this management's discussion and analysis were calculated using the underlying data in thousands. The following discussion focuses on our fiscal 2020 and fiscal 2019 financial condition and results of operations, including comparisons of the years ended January 31, 2020 and February 1, 2019. For discussion and analysis related to our financial condition and results of operations for fiscal 2018, including comparisons of the years ended February 1, 2019 and February 2, 2018, refer to Part II, Item 7. Management's Discussion and Analysis of Financial Condition and Results of Operations in our Annual Report on Form 10-K for fiscal 2019, which was filed with the Securities and Exchange Commission on March 28, 2019.

Except where the context otherwise requires or where otherwise indicated, all references to "Secureworks" "we," "us," "our" and "our company" in this management's discussion and analysis refer to SecureWorks Corp. and our subsidiaries on a consolidated basis, all references to "Dell" refer to Dell Inc. and its subsidiaries on a consolidated basis and all references to "Dell Technologies" refer to Dell Technologies Inc., the ultimate parent company of Dell Inc.

Overview

We are a leading global provider of technology-driven information security solutions singularly focused on protecting our customers from cyber attacks. We combine deep expertise from service to thousands of customers, machine learning and automation from our proprietary technology, and actionable insights from our team of elite researchers and analysts to create a powerful network effect that provides increasingly strong protection for our customers. By aggregating and analyzing data from various sources around the world, we prevent security breaches, detect malicious activity in real time, respond rapidly and predict emerging threats.

Our vision is to be the essential cybersecurity company for a digitally connected world. Through our vendor-neutral approach, we create integrated and comprehensive solutions by proactively managing the collection of "point" products deployed by our customers to address specific security issues and provide supplemental solutions where gaps exist in our customers' defenses. We seek to provide the right level of security for each customer's unique situation, which evolves as the customer's organization grows and changes.

We have pioneered an integrated approach that delivers a broad portfolio of information security solutions to organizations of varying size and complexity. Our flexible and scalable solutions support the evolving needs of the largest, most sophisticated enterprises staffed with in-house security experts, as well as small and medium-sized businesses and government agencies with limited in-house capabilities and resources.

Our solutions enable organizations to:

- prevent security breaches by fortifying their cyber defenses,
- detect malicious activity,
- respond rapidly to security breaches, and
- predict emerging threats.

Our solutions leverage the proprietary technologies, processes and extensive expertise and knowledge of the tactics, techniques and procedures of the adversary that we have developed over more than 21 years. Key elements of our strategy include:

- maintain and extend our technology leadership,
- expand and diversify our customer base,
- deepen our existing customer relationships, and
- attract and retain top talent.

Our technology-driven information security solutions offer an innovative approach to prevent, detect, respond to and predict cybersecurity breaches. Through our managed security solutions, which are largely sold on a subscription basis, we provide global visibility and insight into malicious activity, enabling our customers to detect and effectively remediate threats quickly.

In fiscal 2020, we launched our first software-as-a-service application, Red Cloak Threat Detection and Response (TDR) and related Managed Detection and Response (MDR) powered by Red Cloak. This application gives customers visibility across their entire environment, applies advanced analytics developed using machine and deep learning on diverse data from a wide range of sources, and leverages workflows designed using our 21 years of security operations expertise and integrated orchestration and automation capabilities that increase the speed of response actions. Threat intelligence, which is typically deployed as part of our managed security solutions, delivers early warnings of vulnerabilities and threats along with actionable information to help prevent any adverse impact.

In addition to these solutions, we also offer a variety of services, which includes security and risk consulting and incident response to accelerate adoption of our capabilities. Through security and risk consulting, we advise customers on a broad range of security and risk-related matters. Incident response minimizes the impact and duration of security breaches through proactive customer preparation, rapid containment and thorough event analysis followed by effective remediation. We have a single organization responsible for the delivery of our security solutions, which enables us to respond quickly to our customers' evolving needs and help them secure themselves against cyber attacks.

In December 2019, a novel strain of the coronavirus, COVID-19, was reported in mainland China. The World Health Organization declared the outbreak to constitute a "pandemic" on March 11, 2020. This has led to a significant disruption of normal business operations globally, as businesses, including Secureworks, have needed to implement modifications to employee travel, employee work locations and employee productivity, in some instances as required by federal, state and local authorities. The extent of the impact of COVID-19 on our future operational and financial performance will depend on various future developments, including the duration and spread of the outbreak, impact on our employees, impact on our customers, effect on our sales cycles or costs, and effect on our vendors, all of which are uncertain and cannot be predicted, but which could have a material adverse effect on our business, results of operations or financial condition. At this point, the extent to which COVID-19 may impact our financial condition or results of operations is uncertain. Due to our subscription-based business model, the effect of COVID-19 may not be fully reflected in our results of operations until future periods, if at all.

From April 2009 to January 31, 2020, the number of events processed by our technology platform increased from five billion to as many as 320 billion events per day. This significant growth has required continual investment in our business. We believe these investments are critical to our success, although they may continue to impact our near-term profitability.

Key Factors Affecting Our Performance

We believe that our future success will depend on many factors, including the adoption of our solutions by organizations, continued investment in our technology and threat intelligence research, our introduction of new solutions, our ability to increase sales of our solutions to new and existing customers and our ability to attract and retain top talent. Although these areas present significant opportunities, they also present risks that we must manage to ensure our future success. For additional information about these risks, refer to “Risk Factors” in this report. We operate in a highly competitive industry and face, among other competitive challenges, pricing pressures within the information security market as a result of action by our larger competitors to reduce the prices of their security monitoring, detection and prevention products, as well as their managed security solutions. We must continue to efficiently manage our investments and effectively execute our strategy to succeed. If we are unable to address these challenges, our business could be adversely affected.

Adoption of Technology-Driven Solution Strategy. The evolving landscape of applications, modes of communication and IT architectures makes it increasingly challenging for organizations of all sizes to protect their critical business assets, including proprietary information, from cyber threats. New technologies heighten security risks by increasing the number of ways a threat actor can attack a target, by giving users greater access to important business networks and information and by facilitating the transfer of control of underlying applications and infrastructure to third-party vendors. An effective cyber defense strategy requires the coordinated deployment of multiple products and solutions tailored to an organization’s specific security needs. Our integrated suite of solutions is designed to facilitate the successful implementation of such a strategy, but continuous investment in, and adaptation of, our technology will be required as the threat landscape continues to evolve rapidly. The degree to which prospective and current customers recognize the mission-critical nature of our technology-driven information security solutions, and subsequently allocate budget dollars to our solutions, will affect our future financial results.

Investment in Our Technology and Threat Intelligence Research. Our technology platform constitutes the core of our technology-driven information security solutions. It provides our customers with an integrated perspective and intelligence regarding their network environments and security threats. The platform is augmented by our Counter Threat Unit research team, which conducts exclusive research into threat actors, uncovers new attack techniques, analyzes emerging threats and evaluates the risks posed to our customers. Our performance is significantly dependent on the investments we make in our research and development efforts, and on our ability to be at the forefront of threat intelligence research, and to adapt our platform to new technologies as well as to changes in existing technologies. This is an area in which we will continue to invest, while leveraging a flexible staffing model to align with solutions development. We believe that investment in our platform will contribute to long-term revenue growth, but it may continue to adversely affect our near-term profitability.

Introduction of New Information Security Solutions. Our performance is significantly dependent on our ability to continue to innovate and introduce new information security solutions that protect our customers from an expanding array of cybersecurity threats. We continue to invest in solutions innovation and leadership, including hiring top technical talent and focusing on core technology innovation. In addition, we will continue to evaluate and utilize third-party proprietary technologies, where appropriate, for the continuous development of complementary offerings. We cannot be certain that we will realize increased revenue from our solutions development initiatives. We believe that our investment in solutions development will contribute to long-term revenue growth, but it may continue to adversely affect our near-term profitability.

Investments in Expanding Our Customer Base and Deepening Our Customer Relationships. To support future sales, we will need to continue to devote resources to the development of our global sales force. We have made and plan to continue to make significant investments in expanding our go-to-market efforts with direct sales, channel partners and marketing. Any investments we make in our sales and marketing operations will occur before we realize any benefits from such investments. The investments we have made, or intend to make, to strengthen our sales and marketing efforts may not result in an increase in revenue or an improvement in our results of operations. Although we believe our investment in sales and marketing will help us improve our results of operations in the long term, the resulting increase in operating expenses attributable to these sales and marketing functions may continue to adversely affect our profitability in the near term. The continued growth of our business also depends in part on our ability to sell additional solutions to our existing customers. As our customers realize the benefits of the solutions they previously purchased, our portfolio of solutions provides us with a significant opportunity to expand these relationships.

Investment in Our People. The difficulty in providing effective information security is exacerbated by the highly competitive environment for identifying, hiring and retaining qualified information security professionals. Our technology leadership, brand, exclusive focus on information security, customer-first culture, and robust training and development program have enabled us to attract and retain highly-talented professionals with a passion for building a career in the information security industry. These professionals are led by a highly experienced and tenured management team with extensive IT security expertise and a record of developing successful new technologies and solutions to help protect our customers. We will continue to invest in attracting and retaining top talent to support and enhance our information security offerings.

Key Operating Metrics

In recent years, we have experienced broad growth across our portfolio of technology-driven information security solutions being provided to all sizes of customers. We have achieved much of this growth by providing solutions to large enterprise customers, which generate substantially more average revenue than our small and medium-sized business, or SMB, customers, and by continually expanding the volume and breadth of the security solutions that we provide to all customers. Execution of this strategy has resulted in steady growth in our average revenue per customer. This growth has required continuous investment in our business, resulting in net losses. We believe these investments are critical to our success, although they may continue to impact our profitability.

We believe the operating metrics described below provide further insight into the long-term value of our subscription agreements and our ability to maintain and grow our customer relationships. Relevant key operating metrics are presented below as of the dates indicated and for the annual periods then ended:

	January 31, 2020	February 1, 2019	February 2, 2018
Subscription customer base	4,100	4,200	4,400
Total customer base	5,200	4,700	5,000
Monthly recurring revenue (in millions)	$ 36.5	$ 36.2	$ 35.3
Annual recurring revenue (in millions)	$ 437.5	$ 434.1	$ 423.0
Average subscription revenue per customer (in thousands)	$ 107.8	$ 103.3	$ 95.6
Revenue retention rate	95%	89%	96%

Subscription Customer Base. We define our subscription customer base as the number of customers who subscribe to our managed security solutions as of a particular date. We believe that growing our existing customer base and our ability to grow our average subscription revenue per customer represent significant future revenue opportunities for us.

Total Customer Base. We define our total customer base as the number of customers that subscribe to our managed security solutions as well as customers that buy professional and other services from us, as of a particular date.

Annual and Monthly Recurring Revenue. We define recurring revenue as the value of our subscription contracts as of a particular date. Because we use recurring revenue as a leading indicator of future annual revenue, we include operational backlog. We define operational backlog as the recurring revenue associated with pending contracts, which are contracts that have been sold but for which the service period has not yet commenced. Our increase in recurring revenue has been driven primarily by our continuing ability to expand our offerings and sell additional solutions to existing customers, as well as by larger subscription contracts to our enterprise customers.

Average Subscription Revenue Per Customer. Our average subscription revenue per customer is primarily related to the persistence of cyber threats and the results of our sales and marketing efforts to increase the awareness of our solutions. Additionally, our customer composition of both enterprise and SMB companies provides us with an opportunity to expand our professional services revenue. As of January 31, 2020, February 1, 2019, and February 2, 2018, approximately 60%, 50%, and 44%, respectively, of our professional services customers subscribed to our managed security solutions.

Revenue Retention Rate. Our revenue retention rate is an important measure of our success in retaining and growing revenue from our subscription-based customers. To calculate our revenue retention rate for any period, we compare the monthly recurring revenue excluding operational backlog of our subscription-based customer base at the beginning of the fiscal year, which we call our base recurring revenue, to the monthly recurring revenue excluding operational backlog from that same cohort of customers at the end of the period, which we call our retained recurring revenue. By dividing the retained recurring revenue by the base recurring revenue, we measure our success in retaining and growing installed revenue from the specific cohort of customers we served at the beginning of the period. Our calculation includes the positive revenue impacts of selling and installing additional solutions to this cohort of customers and the negative revenue impacts of customer or service attrition during the period. However, the calculation does not include the positive impact on revenue from sales of solutions to any customers acquired during the period. Our revenue retention rates may decline or increase from period to period as a result of several factors, including the timing of solutions installations and customer renewal rates.

Non-GAAP Financial Measures

We use supplemental measures of our performance, which are derived from our financial information, but which are not presented in our financial statements prepared in accordance with generally accepted accounting principles in the United States of America, referred to as GAAP. Non-GAAP financial measures presented in this management's discussion and analysis include non-GAAP revenue, non-GAAP gross margin, non-GAAP research and development expenses, non-GAAP sales and marketing expenses, non-GAAP general and administrative expenses, non-GAAP operating income (loss), non-GAAP net income (loss), non-GAAP earnings (loss) per share and adjusted EBITDA. We use non-GAAP financial measures to supplement financial information presented on a GAAP basis. We believe these non-GAAP financial measures provide useful information to help evaluate our operating results by facilitating an enhanced understanding of our operating performance and enabling more meaningful period-to-period comparisons.

In particular, we have excluded the impact of certain purchase accounting adjustments related to a change in the basis of deferred revenue for the acquisition of Dell by Dell Technologies in fiscal 2014. We believe it is useful to exclude such purchase accounting adjustments related to the foregoing transactions as this deferred revenue generally results from multi-year service contracts under which deferred revenue is established upon sale and revenue is recognized over the term of the contract. Pursuant to the fair value provisions applicable to the accounting for business combinations, GAAP requires this deferred revenue to be recorded at its fair value, which is typically less than the book value. In presenting non-GAAP earnings, we add back the reduction in revenue that results from this revaluation on the expectation that a significant majority of these service contracts will be renewed in the future and therefore the revaluation is not helpful in predicting our ongoing revenue trends. We believe that this non-GAAP financial adjustment is useful to investors because it allows investors to (1) evaluate the effectiveness of the methodology and information used by management in its financial and operational decision-making, and (2) compare past and future reports of financial results of our Company as the revenue reduction related to acquired deferred revenue will not recur when related service contracts are renewed in future periods.

There are limitations to the use of the non-GAAP financial measures presented in this management’s discussion and analysis. Our non-GAAP financial measures may not be comparable to similarly titled measures of other companies. Other companies, including companies in our industry, may calculate non-GAAP financial measures differently than we do, limiting the usefulness of those measures for comparative purposes.

Non-GAAP revenue, non-GAAP gross margin, non-GAAP research and development expenses, non-GAAP sales and marketing expenses, non-GAAP general and administrative expenses, non-GAAP operating income (loss), non-GAAP net income (loss), non-GAAP earnings (loss) per share and adjusted EBITDA, as defined by us, exclude the items described in the reconciliation below. As the excluded items can have a material impact on earnings, our management compensates for this limitation by relying primarily on GAAP results and using non-GAAP financial measures supplementally. The non-GAAP financial measures are not meant to be considered as indicators of performance in isolation from or as a substitute for revenue, gross margin, research and development expenses, sales and marketing expenses, general and administrative expenses, operating income (loss) or net income (loss) prepared in accordance with GAAP, and should be read only in conjunction with financial information presented on a GAAP basis.

Reconciliation of Non-GAAP Financial Measures

The table below presents a reconciliation of each non-GAAP financial measure to its most directly comparable GAAP financial measure. We encourage you to review the reconciliations in conjunction with the presentation of the non-GAAP financial measures for each of the periods presented. In future fiscal periods, we may exclude such items and may incur income and expenses similar to these excluded items. Accordingly, the exclusion of these items and other similar items in our non-GAAP presentation should not be interpreted as implying that these items are non-recurring, infrequent or unusual.

The following is a summary of the items excluded from the most comparable GAAP financial measures to calculate our non-GAAP financial measures:

- *Impact of Purchase Accounting.* The impact of purchase accounting consists primarily of purchase accounting adjustments related to a change in the basis of deferred revenue related to the acquisition of Dell by Dell Technologies in fiscal 2014.

- *Amortization of Intangible Assets.* Amortization of intangible assets consists of amortization of customer relationships and acquired technology. In connection with the acquisition of Dell by Dell Technologies in fiscal 2014, all of our tangible and intangible assets and liabilities were accounted for and recognized at fair value on the transaction date.

Accordingly, amortization of intangible assets consists of amortization associated with intangible assets recognized in connection with this transaction.

- *Stock-based Compensation Expense.* Non-cash stock-based compensation expense relates to both the Dell Technologies and Secureworks equity plans. We exclude such expense when assessing the effectiveness of our operating performance since stock-based compensation does not necessarily correlate with the underlying operating performance of the business.

- *Impact of Tax Cuts and Jobs Act*. The impact of the Tax Cuts and Jobs Act relates to final tax provision impacts of complying with the U.S. tax reform that was enacted in December 2017, as recorded in fiscal 2020 and fiscal 2019, as well as the provisional tax benefit of $27.0 million that was recorded in the fourth quarter of fiscal 2018. For additional information, see "Notes to Consolidated Financial Statements—Note 11—Income and Other Taxes" in our consolidated financial statements included in this report.

- *Aggregate Adjustment for Income Taxes.* The aggregate adjustment for income taxes is the estimated combined income tax effect for the adjustments mentioned above. The tax effects are determined based on the tax jurisdictions where the above items were incurred.

	Fiscal Year Ended		
	January 31, 2020	February 1, 2019	February 2, 2018
GAAP revenue	$ 552,765	$ 518,709	$ 467,930
Impact of purchase accounting	—	—	584
Non-GAAP revenue	$ 552,765	$ 518,709	$ 468,514
GAAP gross margin	$ 299,969	$ 272,592	$ 242,846
Amortization of intangibles	14,089	13,642	13,642
Impact of purchase accounting	—	—	624
Stock-based compensation expense	1,206	780	891
Non-GAAP gross margin	$ 315,264	$ 287,014	$ 258,003
GAAP research and development expenses	$ 94,964	$ 87,608	$ 80,164
Stock-based compensation expense	(4,280)	(4,133)	(3,261)
Non-GAAP research and development expenses	$ 90,684	$ 83,475	$ 76,903
GAAP sales and marketing expenses	$ 157,674	$ 141,818	$ 139,937
Stock-based compensation expense	(1,694)	(2,652)	(735)
Non-GAAP sales and marketing expenses	$ 155,980	$ 139,166	$ 139,202
GAAP general and administrative expenses	$ 99,505	$ 91,898	$ 92,726
Amortization of intangibles	(14,094)	(14,094)	(14,095)
Impact of purchase accounting	—	—	(1,025)
Stock-based compensation expense	(12,368)	(11,805)	(8,903)
Non-GAAP general and administrative expenses	$ 73,043	$ 65,999	$ 68,703
GAAP operating income (loss)	$ (52,174)	$ (48,732)	$ (69,981)
Amortization of intangibles	28,183	27,736	27,737
Impact of purchase accounting	—	—	1,649
Stock-based compensation expense	19,548	19,370	13,790
Non-GAAP operating income (loss)	$ (4,443)	$ (1,626)	$ (26,805)

GAAP net income (loss)	$ (31,666)	$ (39,101)	$ (10,417)
Amortization of intangibles	28,183	27,736	27,737
Impact of purchase accounting	—	—	1,649
Stock-based compensation expense	19,548	19,370	13,790
Impact of Tax Cuts and Jobs Act	(1,191)	4,325	(34,993)
Aggregate adjustment for income taxes	(14,688)	(10,978)	(15,129)
Non-GAAP net income (loss)	$ 186	$ 1,352	$ (17,363)
GAAP earnings (loss) per share	$ (0.39)	$ (0.48)	$ (0.13)
Amortization of intangibles	0.35	0.34	0.35
Impact of purchase accounting	—	—	0.02
Stock-based compensation expense	0.24	0.24	0.17
Impact of Tax Cuts and Jobs Act	(0.01)	0.05	(0.44)
Aggregate adjustment for income taxes	(0.18)	(0.13)	(0.19)
Non-GAAP earnings (loss) per share *	$ —	$ 0.02	$ (0.22)
** Sum of reconciling items may differ from total due to rounding of individual components*			
GAAP net income (loss)	$ (31,666)	$ (39,101)	$ (10,417)
Interest and other, net	(850)	(2,778)	2,735
Income tax benefit	(19,658)	(6,853)	(62,299)
Depreciation and amortization	42,932	41,207	42,171
Stock-based compensation expense	19,548	19,370	13,790
Impact of purchase accounting	—	—	584
Adjusted EBITDA	$ 10,306	$ 11,845	$ (13,436)

Our Relationship with Dell and Dell Technologies

On April 27, 2016, we completed our IPO. Upon the closing of our IPO, Dell Technologies owned, indirectly through Dell Inc. and Dell Inc.'s subsidiaries, no shares of our outstanding Class A common stock and all shares of our outstanding Class B common stock, which as of January 31, 2020 represented approximately 86.2% of our total outstanding shares of common stock and approximately 98.4% of the combined voting power of both classes of our outstanding common stock.

As a majority-owned subsidiary of Dell, we receive from Dell various corporate services in the ordinary course of business, including finance, tax, human resources, legal, insurance, IT, procurement and facilities related services. The costs of these services have been charged in accordance with a shared services agreement that went into effect on August 1, 2015, the effective date of our carve-out from Dell. For more information regarding the allocated costs and related party transactions, see "Notes to Consolidated Financial Statements—Note 13—Related Party Transactions" in our consolidated financial statements included in this report.

During the periods presented in the consolidated financial statements included in this report, Secureworks did not file separate federal tax returns, as Secureworks was generally included in the tax grouping of other Dell entities within the respective entity's tax jurisdiction. The income tax benefit has been calculated using the separate return method, modified to apply the benefits for loss approach. Under the benefits for loss approach, net operating losses or other tax attributes are characterized as realized or as realizable by Secureworks when those attributes are utilized or expected to be utilized by other members of the Dell consolidated group. For more information, see "Notes to Consolidated Financial Statements—Note 11—Income and Other Taxes" in our consolidated financial statements included in this report.

Additionally, we participate in various commercial arrangements with Dell, under which, for example, we provide information security solutions to third-party customers with which Dell has contracted to provide our solutions, procure hardware, software and services from Dell, and sell our solutions through Dell in the United States and some international jurisdictions. In connection with our IPO, effective August 1, 2015, we entered into agreements with Dell that govern these commercial arrangements. These agreements generally were initially effective for up to one to three years and include extension and cancellation options. To the extent that we choose to, or are required to, transition away from the corporate services currently

provided by Dell, we may incur additional non-recurring transition costs to establish our own stand-alone corporate functions. For more information regarding the allocated costs and related party transactions, see "Notes to Consolidated Financial Statements—Note 13—Related Party Transactions" in our consolidated financial statements included in this report.

Components of Results of Operations

Revenue

We sell managed security and threat intelligence solutions on a subscription basis and various professional services, including security and risk consulting and incident response solutions. Our managed security contracts typically range from one to three years and, as of January 31, 2020, averaged approximately two years in duration. The revenue and any related costs for these deliverables are recognized ratably over the contract term, beginning on the date on which service is made available to customers. Professional services customers typically purchase solutions pursuant to customized contracts that are shorter in duration. In general, these contracts have terms of less than one year. Professional services consist primarily of fixed-fee and retainer-based contracts. Revenue from these engagements is recognized under the proportional performance method of accounting. Revenue from time and materials-based contracts is recognized as costs are incurred at amounts represented by the agreed-upon billing rates.

The fees we charge for our solutions vary based on a number of factors, including the solutions selected, the number of customer devices covered by the selected solutions, and the level of management we provide for the solutions. In fiscal 2020, approximately 76% of our revenue was derived from subscription-based arrangements, attributable to managed security solutions, while approximately 24% was derived from professional services engagements. As we respond to the evolving needs of our customers, the relative mix of subscription-based solutions and professional services we provide our customers may fluctuate. International revenue, which we define as revenue contracted through non-U.S. entities, represented approximately 25%, 22% and 16% of our total net revenue in fiscal 2020, fiscal 2019 and fiscal 2018, respectively. Although our international customers are located primarily in the United Kingdom, Japan and Canada, we provide managed security solutions to customers across 52 countries as of January 31, 2020.

Over all of the periods presented in this report, our pricing strategy for our various offerings was relatively consistent, and accordingly did not significantly affect our revenue growth. However, we may adjust our pricing to remain competitive and support our strategic initiatives.

During the second quarter of fiscal 2019, a significant portion of our contract with Bank of America, N.A., a large customer, was amended and extended for two more years. During the term of the extended contract, the mix of services is different from the mix in prior periods, with higher gross margin, although the total value of services is lower than in prior periods.

Gross Margin

We operate in a challenging business environment, where the complexity and number of cyber attacks are constantly increasing. Accordingly, initiatives to drive the efficiency of our Counter Threat Platform and the continued training and development of our employees are critical to our long-term success. Gross margin has been and will continue to be affected by these factors as well as others, including the mix of solutions sold, the mix between large and small customers, timing of revenue recognition and the extent to which we expand our counter threat operations centers.

Cost of revenue consists primarily of personnel expenses, including salaries, benefits and performance-based compensation for employees who maintain our Counter Threat Platform and provide solutions to our customers, as well as perform other critical functions. Also included in cost of revenue are amortization of equipment and costs associated with hardware utilized as part of providing subscription services, amortization of technology licensing fees, amortization of intangible assets, fees paid to contractors who supplement or support our solutions, maintenance fees and overhead allocations. As our business grows, the cost of revenue associated with our solutions may fluctuate.

We operate in a high-growth industry and have experienced significant revenue growth since our inception. We continue to invest in initiatives to drive the efficiency of our business to increase gross margin as a percentage of total revenue. However, as we balance revenue growth and efficiency initiatives, gross margin as a percentage of total revenue may fluctuate from period to period.

Operating Costs and Expenses

Our operating costs and expenses consist of research and development expenses, sales and marketing expenses and general and administrative expenses.

- *Research and Development, or R&D, Expenses.* Research and development expenses include compensation and related expenses for the continued development of our solutions offerings, including a portion of expenses related to our threat research team, which focuses on the identification of system vulnerabilities, data forensics and malware analysis. R&D expenses also encompass expenses related to the development of prototypes of new solutions offerings and allocated overhead. Our customer solutions have generally been developed internally. We operate in a competitive and highly technical industry. Therefore, to maintain and extend our technology leadership, we intend to continue to invest in our R&D efforts by hiring more personnel to enhance our existing security solutions and to add complementary solutions.

- *Sales and Marketing, or S&M, Expenses.* Sales and marketing expenses include salaries, sales commissions and performance-based compensation benefits and related expenses for our S&M personnel, travel and entertainment, marketing and advertising programs (including lead generation), customer advocacy events, and other brand-building expenses, as well as allocated overhead. As we continue to grow our business, both domestically and internationally, we will invest in our sales capability, which will increase our sales and marketing expenses in absolute dollars.

- *General and Administrative, or G&A, Expenses.* General and administrative expenses include primarily the costs of human resources and recruiting, finance and accounting, legal support, information management and information security systems, facilities management, corporate development and other administrative functions, and are partially offset by allocations of information technology and facilities costs to other functions.

Interest and Other, Net

Interest and other, net consists primarily of the effect of exchange rates on our foreign currency-denominated asset and liability balances and interest income earned on our cash and cash equivalents. All foreign currency transaction adjustments are recorded as foreign currency gains (losses) in the Consolidated Statements of Operations. To date, we have had minimal interest income.

Income Tax Expense (Benefit)

Our effective tax benefit rate was 38.3%, 14.9% and 85.7% for the fiscal years ended January 31, 2020, February 1, 2019 and February 2, 2018, respectively. The change in effective tax rate from fiscal 2019 to fiscal 2020 was primarily attributable to the impact of certain discrete adjustments related to the vesting of stock-based compensation units, certain provisions from the Tax Cuts and Jobs Act, and the recognition of additional benefits relating to research and development credits.

We calculate a provision for income taxes using the asset and liability method, under which deferred tax assets and liabilities are recognized by identifying the temporary differences arising from the different treatment of items for tax and accounting purposes. We provide valuation allowances for deferred tax assets, where appropriate. We file U.S. federal returns on a consolidated basis with Dell and we expect to continue doing so until such time (if any) as we are deconsolidated for tax purposes with respect to the Dell consolidated group. According to the terms of the tax matters agreement between Dell Technologies and us that went into effect on August 1, 2015, Dell Technologies will reimburse us for any amounts by which our tax assets reduce the amount of tax liability owed by the Dell group on an unconsolidated basis. For a further discussion of income tax matters, see “Notes to Consolidated Financial Statements—Note 11—Income and Other Taxes" in our consolidated financial statements included in this report.

Results of Operations

Fiscal 2020 Compared to Fiscal 2019

The following table summarizes our key performance indicators for the fiscal years ended January 31, 2020 and February 1, 2019.

	Fiscal Year Ended				
	January 31, 2020			February 1, 2019	
	$	% of Revenue	% Change	$	% of Revenue
	(in thousands, except percentages)				
Net revenue	$ 552,765	100.0 %	6.6 %	$ 518,709	100.0 %
Cost of revenue	$ 252,796	45.7 %	2.7 %	$ 246,117	47.4 %
Total gross margin	$ 299,969	54.3 %	10.0 %	$ 272,592	52.6 %
Operating expenses	$ 352,143	63.7 %	9.6 %	$ 321,324	61.9 %
Operating loss	$ (52,174)	(9.4)%	7.1 %	$ (48,732)	(9.4)%
Net loss	$ (31,666)	(5.7)%	(19.0)%	$ (39,101)	(7.5)%
Other Financial Information [(1)]					
Non-GAAP revenue	$ 552,765	100.0 %	6.6 %	$ 518,709	100.0 %
Non-GAAP gross margin	$ 315,264	57.0 %	9.8 %	$ 287,014	55.3 %
Non-GAAP operating expenses	$ 319,707	57.8 %	10.8 %	$ 288,640	55.6 %
Non-GAAP operating loss	$ (4,443)	(0.8)%	173.2 %	$ (1,626)	(0.3)%
Non-GAAP net income	$ 186	— %	(86.2)%	$ 1,352	0.3 %
Adjusted EBITDA	$ 10,306	1.9 %	(13.0)%	$ 11,845	2.3 %

(1) See "Non-GAAP Financial Measures" and "Reconciliation of Non-GAAP Financial Measures" for more information about these non-GAAP financial measures, including our reasons for including the measures, material limitations with respect to the usefulness of the measures, and a reconciliation of each non-GAAP financial measure to the most directly comparable GAAP financial measure. Non-GAAP financial measures as a percentage of revenue are calculated based on non-GAAP revenue.

Revenue

Net revenue, which we refer to as revenue, increased $34.1 million, or 6.6%, in fiscal 2020, compared with fiscal 2019. The revenue increase resulted primarily from revenue generated by subscription-based solutions. Revenue attributable to our subscription-based solutions represented approximately 76% of revenue in fiscal 2020 and fiscal 2019. Our existing customers continued to increase their contracted subscriptions for our solutions, with our retention rate increasing 6% in fiscal 2020.

Revenue for certain services provided to or on behalf of Dell under our commercial agreements with Dell totaled approximately $27.2 million and $16.6 million for fiscal 2020 and 2019, respectively. For more information regarding the commercial agreements, see "Notes to Consolidated Financial Statements—Note 13—Related Party Transactions" in our consolidated financial statements included in this report.

We primarily generate revenue from sales in the United States. However, for fiscal 2020, international revenue, which we define as revenue contracted through non-U.S. entities, increased to $140.3 million, or 21.9%. Currently, our international customers are primarily located in the United Kingdom, Japan, and Canada. We are focused on continuing to grow our international customer base in future periods.

Gross Margin

Our total gross margin increased $27.4 million, or 10.0%, in fiscal 2020, compared with fiscal 2019. As a percentage of revenue, our gross margin percentage increased 170 basis points to 54.3% in fiscal 2020. Gross margin on a GAAP basis includes amortization of intangible assets, purchase accounting adjustments and stock-based compensation expense. On a non-GAAP basis, excluding these adjustments, gross margin increased $28.3 million, or 9.8%, in fiscal 2020. As a percentage of revenue, our non-GAAP gross margin increased 170 basis points to 57.0% in fiscal 2020. The increase in gross margin as a percentage of revenue on a GAAP and non-GAAP basis during the fiscal year was mainly attributable to improvement in our subscription-based solutions margins as we continue to focus on delivering comprehensive higher-value security solutions and driving scale and operational efficiencies. Growth in revenue from Safeguard and Response solutions sold through Dell, which have higher margins, also contributed to the increase in gross margin.

Operating Expenses

The following table presents information regarding our operating expenses during the fiscal years ended January 31, 2020 and February 1, 2019.

	Fiscal Year Ended				
	January 31, 2020			February 1, 2019	
	Dollars	% of Revenue	% Change	Dollars	% of Revenue
	(in thousands, except percentages)				
Operating expenses:					
Research and development	$ 94,964	17.2%	8.4%	$ 87,608	16.9%
Sales and marketing	157,674	28.5%	11.2%	141,818	27.3%
General and administrative	99,505	18.0%	8.3%	91,898	17.7%
Total operating expenses	$352,143	63.7%	9.6%	$321,324	61.9%
Other Financial Information					
Non-GAAP research and development	$ 90,684	16.4%	8.6%	$ 83,475	16.1%
Non-GAAP sales and marketing	155,980	28.2%	12.1%	139,166	26.8%
Non-GAAP general and administrative	73,043	13.2%	10.7%	65,999	12.7%
Non-GAAP operating expenses [(1)]	$319,707	57.8%	10.8%	$288,640	55.6%

(1) See “Non-GAAP Financial Measures” and “Reconciliation of Non-GAAP Financial Measures” for a reconciliation of each non-GAAP financial measure to the most directly comparable GAAP financial measure.

Research and Development Expenses. R&D expenses increased $7.4 million, or 8.4%, in fiscal 2020. As a percentage of revenue, on a GAAP basis, R&D expenses increased 30 basis points to 17.2% in fiscal 2020. As a percentage of revenue, on a non-GAAP basis, R&D expenses increased 30 basis points to 16.4% in fiscal 2020. The increases were primarily attributable to increased compensation and benefits associated with additional development resources, and other technology related cost for the continued development of our solutions, including the development of a new security analytics platform and software application.

Sales and Marketing Expenses. S&M expenses increased $15.9 million, or 11.2%, in fiscal 2020. As a percentage of revenue, S&M expenses increased 120 basis points to 28.5% in fiscal 2020. On a non-GAAP basis, S&M expenses as a percentage of revenue increased 140 basis points to 28.2% for fiscal 2020. The increases in S&M expenses as a percentage of revenue were primarily attributable to sales costs associated with new offerings launched in the first quarter of fiscal 2020 in partnership with Dell. In addition, commission expense increased due to the reduction in the period over which deferred commission costs are recognized.

General and Administrative Expenses. G&A expenses increased $7.6 million, or 8.3%, in fiscal 2020. As a percentage of revenue, G&A expenses increased 30 basis points to 18.0% in fiscal 2020. On a non-GAAP basis, G&A expenses as a percentage of revenue increased 50 basis points to 13.2% in fiscal 2020. The increases in G&A expenses as a percentage of revenue were primarily attributable to compensation and benefits, sales tax expense, and higher facilities-related costs.

Operating Loss

Our operating loss was $52 million for fiscal 2020 compared to $49 million for fiscal 2019. As a percentage of revenue, our operating loss was 9.4% in both fiscal 2020 and fiscal 2019. The increase in our operating loss was primarily attributable to increased operating expenses as we continue to invest in the business to drive growth. Operating loss on a GAAP basis includes amortization of intangible assets, purchase accounting adjustments and stock-based compensation expense. The increases in our non-GAAP operating loss on a dollar basis and as a percentage of revenue were primarily attributable to the same drivers as above.

Interest and Other, Net

Interest and other income was $0.9 million in fiscal 2020 compared with an expense of $2.8 million in fiscal 2019. The change primarily reflected the effects of foreign currency transactions and related exchange rate fluctuations.

Income Tax Expense (Benefit)

Our income tax benefit was $19.7 million, or 38.3%, and $6.9 million, or 14.9%, of our pre-tax loss in fiscal 2020 and fiscal 2019, respectively. The changes in the effective tax benefit rate were primarily attributable to the impact of certain discrete adjustments related to the vesting of stock-based compensation units, certain provisions from the Tax Cuts and Jobs Act and the research and development tax credit.

Net Income (Loss)

Our net loss of $(31.7) million decreased $7.4 million, or 19.0%, in fiscal 2020. The decrease in our net loss was attributable to the increased tax benefit in fiscal 2020 compared with fiscal 2019 related to the Tax Cuts and Jobs Act, which more than offset lower operating results. Net income on a non-GAAP basis was $0.2 million, which represents a decrease of $1.2 million, or 86.2%, from fiscal 2019. Overall, the decrease in non-GAAP net income was primarily due to the impacts of the operating losses discussed above.

Liquidity, Capital Commitments and Contractual Cash Obligations

Overview

We believe that our cash and cash equivalents together with our accounts receivable will provide us with sufficient liquidity to fund our business and meet our obligations for at least 12 months. Our future capital requirements will depend on many factors, including our rate of revenue growth, the rate of expansion of our workforce, the timing and extent of our expansion into new markets, the timing of introductions of new functionality and enhancements to our solutions, potential acquisitions of complementary businesses and technologies, continuing market acceptance of our solutions, as well as general economic and market conditions. We may need to raise additional capital or incur indebtedness to continue to fund our operations in the future or to fund our needs for less predictable strategic initiatives, such as acquisitions. In addition to our $30 million revolving credit facility from Dell, described below, sources of financing may include arrangements with unaffiliated third parties, depending on the availability of capital, the cost of funds and lender collateral requirements.

Selected Measures of Liquidity and Capital Resources

As of January 31, 2020, our principal sources of liquidity consisted of cash and cash equivalents of $181.8 million and accounts receivable of $111.8 million. Our cash and cash equivalents balance as of January 31, 2020 included $100.5 million invested in money market funds pending their use in our business.

Selected measures of our liquidity and capital resources are as follows:

	January 31, 2020	February 1, 2019
	(in thousands)	
Cash and cash equivalents	$ 181,838	$ 129,592
Accounts receivable, net	$ 111,798	$ 141,344

We invoice our customers based on a variety of billing schedules. During fiscal 2020, on average, 58% of our recurring revenue was billed in advance and approximately 42% was billed on either a monthly or a quarterly basis. Invoiced accounts receivable are generally collected over a period of 30 to 120 days. The decrease in accounts receivable as of January 31, 2020 compared with February 1, 2019 reflected increased collection activity, partially offset by an increase in revenue. We regularly monitor our accounts receivable for collectability, particularly in markets where economic conditions remain uncertain and continue to take actions to reduce our exposure to credit losses. As of January 31, 2020 and February 1, 2019, the allowance for doubtful accounts was $5.1 million and $6.2 million, respectively. The decrease in the allowance for doubtful accounts was due to overall improvement in our longer-aged receivables balances. Based on our assessment, we believe we are adequately reserved for credit risk.

Revolving Credit Facility

SecureWorks, Inc., our wholly-owned subsidiary, is party to a revolving credit agreement with a wholly-owned subsidiary of Dell Inc. under which we have obtained a $30 million senior unsecured revolving credit facility. Under the facility, up to $30 million principal amount of borrowings may be outstanding at any time. The maximum amount of borrowings may be increased by up to an additional $30 million by mutual agreement of the lender and borrower. The proceeds from loans made under the facility may be used for general corporate purposes. The facility is not guaranteed by us or our subsidiaries. There was no outstanding balance under the facility as of January 31, 2020. Effective as of March 26, 2020, the facility agreement was amended and restated to extend the maturity date to March 26, 2021 and to modify the annual rate at which interest accrues.

Each loan made under the amended and restated credit facility will accrue interest at an annual rate equal to the applicable London interbank offered rate plus 1.30%. Amounts under the facility may be borrowed, repaid and reborrowed from time to time during the term of the facility. The borrower will be required to repay in full all of the loans outstanding, including all accrued interest, and the facility will terminate upon a change of control of us or following a transaction in which SecureWorks, Inc. ceases to be a direct or indirect wholly-owned subsidiary of our company. The credit agreement contains customary representations, warranties, covenants and events of default. The unused portion of the facility is subject to a commitment fee of 0.35%, which is due upon expiration of the facility.

Cash Flows

	Fiscal Year Ended	
	January 31, 2020	February 1, 2019
	(in thousands)	
Net change in cash from:		
Operating activities	$ 78,839	$ 57,199
Investing activities	(12,590)	(10,200)
Financing activities	(14,003)	(18,946)
Change in cash and cash equivalents	$ 52,246	$ 28,053

- *Operating Activities* — Cash provided by operating activities was $78.8 million and $57.2 million in fiscal 2020 and fiscal 2019, respectively. The improvement in our operating cash flows was primarily driven by the decrease in our net accounts receivable due to improved collection rates, partially offset by our net transactions with Dell. We expect that our future transactions with Dell will be a source of cash over time as we anticipate that our charges to Dell will continue to exceed Dell's charges to us, although the timing of charges and settlements may vary period to period.
- *Investing Activities* — Cash used in investing activities totaled $12.6 million and $10.2 million in fiscal 2020 and fiscal 2019, respectively. For the periods presented, investing activities consisted primarily of capital expenditures for property and equipment to support our data center and facility infrastructure, as well as certain capitalized costs related to the development of our new security software application.
- *Financing Activities* — Cash used in financing activities was $14.0 million and $18.9 million in fiscal 2020 and fiscal 2019, respectively. The usage in fiscal 2020 reflected employee tax withholding payments of $8.5 million associated with the vesting of stock compensation grants and our repurchase of $6.4 million of our Class A common stock pursuant to our stock repurchase program re-authorized during fiscal 2020 and payment of a long-term financing arrangement of $0.5 million, which was partially offset by proceeds of $1.3 million from stock options exercised during fiscal 2020. The usage in fiscal 2019 reflected our repurchase of $13.5 million of our Class A common stock pursuant to our stock repurchase program authorized during fiscal 2019, payments of long-term financing arrangements of $3.2 million, including related

party obligations with a Dell subsidiary of $2.2 million, and employee tax withholding payments of $2.2 million associated with the vesting of stock compensation grants. For information about our stock repurchase program, see "Notes to Consolidated Financial Statements—Note 9—Stockholders' Equity" in our consolidated financial statements included in this report.

Contractual Cash Obligations

Contractual cash obligations are summarized in the following table:

	Payments Due by Fiscal Year				
(in thousands)	Less than 1 year	1-3 years	3-5 years	Thereafter	Total
Operating leases	$ 5,017	$ 12,285	$ 9,918	$ 7,648	$ 34,868
Purchase obligations	3,645	2,048	—	—	5,693
Credit facilities and other[(1)]	—	500	—	—	500
Total	$ 8,662	$ 14,833	$ 9,918	$ 7,648	$ 41,061

(1) Other reflects purchase obligations of annual maintenance services for hardware systems for internal use financed from a related party. See also "Notes to Consolidated Financial Statements—Note 13—Related Party Transactions" in our consolidated financial statements included in this report.

For information about leases and purchase obligations, see "Notes to Consolidated Financial Statements—Note 8—Leases" and "Notes to Consolidated Financial Statements—Note 7—Commitments and Contingencies" in our consolidated financial statements included in this report.

Off-Balance Sheet Arrangements

As of January 31, 2020, we were not subject to any obligations pursuant to any off-balance sheet arrangements that have or are reasonably likely to have a material effect on our financial condition, results of operations or liquidity.

Critical Accounting Policies and Estimates

We prepare our financial statements in conformity with GAAP, which requires certain estimates, assumptions and judgments to be made that may affect our consolidated financial statements. Accounting policies that have a significant impact on our results are described in "Notes to Consolidated Financial Statements—Note 2—Significant Accounting Policies" in our consolidated financial statements included in this report. The accounting policies discussed in this section are those that we consider to be the most critical. We consider an accounting policy to be critical if the policy is subject to a material level of judgment and if changes in those judgments are reasonably likely to materially impact our results.

Revenue Recognition. Secureworks derives revenue primarily from two sources: (1) subscription revenue related to managed security and threat intelligence solutions; and (2) professional services, including security and risk consulting and incident response solutions.

Subscription-based arrangements typically include security solutions, up-front installation fees and maintenance, and also may include the provision of an associated hardware appliance. The Company uses its hardware appliances in providing security solutions required to access the Company's technology platform. The arrangements that require hardware do not typically convey ownership of the appliance to the customer. Moreover, any related installation fees are non-refundable and are also incapable of being distinct within the context of the arrangement. Therefore, the Company has determined that these arrangements constitute a single performance obligation for which the revenue and any related costs are recognized over the term of the arrangement ratably, which reflects the Company's performance in transferring control of the services to the customer. Amounts that have been invoiced, but for which the above revenue recognition criteria have not been met, are included in deferred revenue.

Professional services consist primarily of fixed-fee and retainer-based contracts. Revenue from these engagements is recognized using an input method over the contract term.

Secureworks reports revenue net of any revenue-based taxes assessed by governmental authorities that are imposed on, and concurrently with, specific revenue-producing transactions.

We recognize revenue when all of the following criteria are met:

- ***Identification of the contract, or contracts, with a customer*—**A contract with a customer exists when (i) we enter into an enforceable contract with a customer, (ii) the contract has commercial substance and the parties are committed to perform, and (iii) payment terms can be identified and collection of substantially all consideration to which we will be entitled in exchange for goods or services that will be transferred is deemed probable based on the customer's intent and ability to pay. Contracts entered into for professional services and subscription-based solutions near or at the same time are generally not combined as a single contract for accounting purposes, since neither the pricing nor the services are interrelated.
- ***Identification of the performance obligations in the contract*—**Performance obligations promised in a contract are identified based on the goods or services that will be transferred to the customer that are both (i) capable of being distinct, whereby the customer can benefit from the goods or service either on its own or together with other resources that are readily available from third parties or from us, and (ii) distinct in the context of the contract, whereby the transfer of the goods or services is separately identifiable from other promises in the contract. When promised goods or services are incapable of being distinct, we account for them as a combined performance obligation. With regard to a typical contract for subscription-based solutions, the performance obligation represents a series of distinct services that will be accounted for as a single performance obligation. In a typical professional services contract, Secureworks has a separate performance obligation associated with each service. We are generally acting as a principal in each subscription-based and professional services arrangement and, thus, recognize revenue on a gross basis.
- ***Determination of the transaction price*—**The total transaction price is primarily fixed in nature as the consideration is tied to the specific services purchased by the customer, which constitutes a series for delivery of the solutions over the duration of the contract. For professional services contracts, variable consideration exists in the form of rescheduling penalties and expense reimbursements; no estimation is required at contract inception, since variable consideration is allocated to the applicable period.
- ***Allocation of the transaction price to the performance obligations in the contract*—**We allocate the transaction price to each performance obligation based on the performance obligation's standalone selling price. Standalone selling price is determined by considering all information available to us, such as historical selling prices of the performance obligation, geographic location, overall strategic pricing objective, market conditions and internally approved pricing guidelines related to the performance obligations.
- ***Recognition of revenue when, or as, the Company satisfies performance obligation*—**We recognize revenue over time using a time-elapsed output method to measure progress (i.e., ratable recognition) for the subscription-based performance obligation over the contract term. For any upgraded installation services, which we have determined represent a performance obligation separate from its subscription-based arrangements, revenue is recognized over time using hours elapsed over the service term as an appropriate method to measure progress. For the performance obligation pertaining to professional services arrangements, we recognize revenue over time using an input method based on time (hours or days) incurred to measure progress over the contract term.

Intangible Assets Including Goodwill. Identifiable intangible assets with finite lives are amortized on a straight-line basis over their estimated useful lives. Finite-lived intangible assets are reviewed for impairment on a quarterly basis, or as potential triggering events are identified. Goodwill and indefinite-lived intangible assets are tested for impairment on an annual basis in the third fiscal quarter, or sooner if an indicator of impairment occurs. To determine whether goodwill and indefinite-lived intangible assets are impaired, we first assess certain qualitative factors. Based on this assessment, if it is determined that the fair value of the goodwill or indefinite-lived intangible asset is less than its carrying amount, we perform the quantitative analysis of the impairment test.

The goodwill impairment test consists of a two-step process, if necessary. The first step is to compare the fair value of the reporting unit to its carrying value, including goodwill. We typically use a discounted cash flow model to determine the fair value of the reporting unit. The assumptions used in the model are consistent with those which we believe hypothetical marketplace participants would use. If the fair value of the reporting unit is less than its carrying value, the second step of the impairment test must be performed in order to determine the amount of the impairment loss, if any. The second step compares the implied fair value of the reporting unit’s goodwill with the carrying amount of that goodwill. If the carrying amount of the reporting unit’s goodwill exceeds its implied fair value, an impairment charge is recognized in an amount equal to that excess. The loss recognized cannot exceed the carrying amount of goodwill. We have determined that we have a single goodwill reporting unit, and, accordingly, for the quantitative analysis, we compare the fair value of this goodwill reporting unit to its carrying value. For indefinite-lived assets, other than goodwill, if the carrying amount determined through the quantitative analysis exceeds the fair value, an impairment charge is recognized in an amount equal to that excess.

Based on the qualitative assessment performed during fiscal 2020, we determined that it was not more likely than not that the fair value of the Secureworks reporting unit was less than its carrying amount and therefore, no impairment of goodwill or indefinite-lived intangible asset existed at our test date of November 1, 2019. Subsequently, no events occurred through our January 31, 2020 year end that would indicate an impairment exists.

Stock-Based Compensation. Our compensation programs include grants under the SecureWorks Corp. 2016 Long-Term Incentive Plan and, prior to the IPO date, grants under share-based payment plans of Dell Technologies Inc., or Dell Technologies. Under the plans, we and, prior to the IPO date, Dell Technologies have granted stock options, restricted stock awards and restricted stock units. Compensation expense related to stock-based transactions is measured and recognized in the financial statements based on fair value. Fair value for restricted stock awards and restricted stock units under our plan is based on the closing price of our Class A common stock as reported on the Nasdaq Global Select Market on the day of the grant. The fair value of each option award is estimated on the grant date using the Black-Scholes option-pricing model and a single option award approach. This model requires that at the date of grant we determine the fair value of the underlying common stock, the expected term of the award, the expected volatility, risk-free interest rates and expected dividend yield. The annual grant of restricted stock and restricted stock units issued during the fiscal year ended January 31, 2020 vest over an average service period of three years and approximately 50% of such awards are subject to performance conditions. Stock-based compensation expense, regarding service-based awards, is adjusted for forfeitures, and recognized using a straight-line basis over the requisite service periods of the awards, which is generally three to four years. Stock-based compensation expense, regarding performance awards, is adjusted for forfeitures and performance criteria, and recognized on a graded vesting basis. We estimate a forfeiture rate, based on an analysis of actual historical forfeitures, to calculate stock-based compensation expense.

Loss Contingencies. We are subject to the possibility of various losses arising in the ordinary course of business. We consider the likelihood of loss or impairment of an asset or the incurrence of a liability, as well as our ability to reasonably estimate the amount of loss, in determining loss contingencies. An estimated loss contingency is accrued when it is probable that an asset has been impaired or a liability has been incurred and the amount of loss can reasonably be estimated. We regularly evaluate current information available to us to determine whether such accruals should be adjusted and whether new accruals are required.

Recently Issued Accounting Pronouncements

Information about recently issued accounting pronouncements is presented in “Notes to Consolidated Financial Statements—Note 2—Significant Accounting Policies” in our consolidated financial statements included in this report.

Item 7A. Quantitative and Qualitative Disclosures About Market Risk

Our results of operations and cash flows have been and will continue to be subject to fluctuations because of changes in foreign currency exchange rates, particularly changes in exchange rates between the U.S. dollar and the Euro, the British Pound, the Romanian Leu and the Canadian Dollar; the currencies of countries where we currently have our most significant international operations. Our expenses in international locations are generally denominated in the currencies of the countries in which our operations are located.

As our international operations grow, we may begin to use foreign exchange forward contracts to partially mitigate the impact of fluctuations in net monetary assets denominated in foreign currencies.

Item 8. Financial Statements and Supplementary Data

INDEX TO CONSOLIDATED FINANCIAL STATEMENTS

Report of Independent Registered Public Accounting Firm

To the Board of Directors and Stockholders of SecureWorks Corp.

Opinion on the Financial Statements

We have audited the accompanying consolidated statements of financial position of SecureWorks Corp. and its subsidiaries (the "Company") as of January 31, 2020 and February 1, 2019, and the related consolidated statements of operations, comprehensive loss, stockholders' equity and cash flows for each of the three years in the period ended January 31, 2020, including the related notes and financial statement schedule listed in the accompanying index (collectively referred to as the "consolidated financial statements"). In our opinion, the consolidated financial statements present fairly, in all material respects, the financial position of the Company as of January 31, 2020 and February 1, 2019, and the results of its operations and its cash flows for each of the three years in the period ended January 31, 2020 in conformity with accounting principles generally accepted in the United States of America.

Change in Accounting Principle

As discussed in Note 2 to the consolidated financial statements, the Company changed the manner in which it accounts for leases in the year ended January 31, 2020.

Basis for Opinion

These consolidated financial statements are the responsibility of the Company's management. Our responsibility is to express an opinion on the Company's consolidated financial statements based on our audits. We are a public accounting firm registered with the Public Company Accounting Oversight Board (United States) (PCAOB) and are required to be independent with respect to the Company in accordance with the U.S. federal securities laws and the applicable rules and regulations of the Securities and Exchange Commission and the PCAOB.

We conducted our audits of these consolidated financial statements in accordance with the standards of the PCAOB. Those standards require that we plan and perform the audit to obtain reasonable assurance about whether the consolidated financial statements are free of material misstatement, whether due to error or fraud. The Company is not required to have, nor were we engaged to perform, an audit of its internal control over financial reporting. As part of our audits we are required to obtain an understanding of internal control over financial reporting but not for the purpose of expressing an opinion on the effectiveness of the Company's internal control over financial reporting. Accordingly, we express no such opinion.

Our audits included performing procedures to assess the risks of material misstatement of the consolidated financial statements, whether due to error or fraud, and performing procedures that respond to those risks. Such procedures included examining, on a test basis, evidence regarding the amounts and disclosures in the consolidated financial statements. Our audits also included evaluating the accounting principles used and significant estimates made by management, as well as evaluating the overall presentation of the consolidated financial statements. We believe that our audits provide a reasonable basis for our opinion.

/s/ PricewaterhouseCoopers LLP

Atlanta, Georgia
March 27, 2020

We have served as the Company's auditor since 2014.

SECUREWORKS CORP.

CONSOLIDATED STATEMENTS OF FINANCIAL POSITION
(in thousands)

	January 31, 2020	February 1, 2019
ASSETS		
Current assets:		
Cash and cash equivalents	$ 181,838	$ 129,592
Accounts receivable, net	111,798	141,344
Inventories	746	468
Other current assets	27,449	27,604
Total current assets	321,831	299,008
Property and equipment, net	27,606	35,978
Goodwill	416,487	416,487
Operating lease right-of-use assets, net	23,463	—
Intangible assets, net	180,052	206,448
Other non-current assets	78,592	78,238
Total assets	$ 1,048,031	$ 1,036,159
LIABILITIES AND STOCKHOLDERS' EQUITY		
Current liabilities:		
Accounts payable	$ 18,690	$ 16,177
Accrued and other current liabilities	98,855	86,495
Deferred revenue	175,847	157,865
Total current liabilities	293,392	260,537
Long-term deferred revenue	12,690	16,064
Operating lease liabilities, non-current	24,669	—
Other non-current liabilities	50,400	66,851
Total liabilities	381,151	343,452
Commitments and contingencies (Note 7)		
Stockholders' equity:		
Preferred stock - $0.01 par value: 200,000 shares authorized; 0 shares issued	—	—
Common stock - Class A of $0.01 par value: 2,500,000 shares authorized; 11,206 and 11,016 issued and outstanding, respectively	112	110
Common stock - Class B of $0.01 par value: 500,000 shares authorized; 70,000 shares issued and outstanding	700	700
Additional paid in capital	896,983	884,567
Accumulated deficit	(207,929)	(176,263)
Accumulated other comprehensive income (loss)	(3,090)	(2,884)
Treasury stock, at cost - 1,257 and 819 shares, respectively	(19,896)	(13,523)
Total stockholders' equity	666,880	692,707
Total liabilities and stockholders' equity	$ 1,048,031	$ 1,036,159

The accompanying notes are an integral part of these consolidated financial statements.

SECUREWORKS CORP.

CONSOLIDATED STATEMENTS OF OPERATIONS
(in thousands, except per share data)

	Fiscal Year Ended		
	January 31, 2020	**February 1, 2019**	**February 2, 2018**
Net revenue	$ 552,765	$ 518,709	$ 467,930
Cost of revenue	252,796	246,117	225,084
Gross margin	299,969	272,592	242,846
Research and development	94,964	87,608	80,164
Sales and marketing	157,674	141,818	139,937
General and administrative	99,505	91,898	92,726
Total operating expenses	352,143	321,324	312,827
Operating loss	(52,174)	(48,732)	(69,981)
Interest and other, net	850	2,778	(2,735)
Loss before income taxes	(51,324)	(45,954)	(72,716)
Income tax benefit	(19,658)	(6,853)	(62,299)
Net loss	(31,666)	(39,101)	(10,417)
Loss per common share (basic and diluted)	$ (0.39)	$ (0.48)	$ (0.13)
Weighted-average common shares outstanding (basic and diluted)	80,563	80,710	80,280

The accompanying notes are an integral part of these consolidated financial statements.

SECUREWORKS CORP.

CONSOLIDATED STATEMENTS OF COMPREHENSIVE LOSS

(in thousands)

	Fiscal Year Ended		
	January 31, 2020	**February 1, 2019**	**February 2, 2018**
Net loss	$ (31,666)	$ (39,101)	$ (10,417)
Foreign currency translation adjustments, net of tax	(206)	(2,914)	3,544
Comprehensive loss	$ (31,872)	$ (42,015)	$ (6,873)

The accompanying notes are an integral part of these consolidated financial statements.

SECUREWORKS CORP.
CONSOLIDATED STATEMENTS OF CASH FLOWS
(in thousands)

	Fiscal Year Ended		
	January 31, 2020	February 1, 2019	February 2, 2018
Cash flows from operating activities:			
Net loss	$ (31,666)	$ (39,101)	(10,417)
Adjustments to reconcile net loss to net cash provided by operating activities:			
Depreciation and amortization	42,932	41,207	42,171
Stock-based compensation expense	19,548	19,370	13,790
Effects of exchange rate changes on monetary assets and liabilities denominated in foreign currencies	270	(1,818)	3,256
Income tax benefit	(19,658)	(6,853)	(62,299)
Other non cash impacts	1,830	—	—
Provision for doubtful accounts	3,099	2,356	3,947
Changes in assets and liabilities:			
Accounts receivable	26,789	13,750	(48,540)
Net transactions with parent	(12,483)	(1,797)	11,024
Inventories	(278)	562	917
Other assets	13,293	(7,277)	14,610
Accounts payable	7,008	(6,117)	3,302
Deferred revenue	14,463	20,942	19,560
Accrued and other current liabilities	13,692	21,975	9,466
Net cash provided by operating activities	78,839	57,199	787
Cash flows from investing activities:			
Capital expenditures	(12,590)	(10,200)	(13,819)
Net cash used in investing activities	(12,590)	(10,200)	(13,819)
Cash flows from financing activities:			
Proceeds from stock option exercises	1,327	—	—
Principal payments on financing arrangement with Dell Financial Services	—	(2,208)	(800)
Taxes paid on vested restricted shares	(8,453)	(2,207)	(1,224)
Purchases of stock for treasury	(6,377)	(13,531)	—
Payments on financed capital expenditures	(500)	(1,000)	—
Net cash used in financing activities	(14,003)	(18,946)	(2,024)
Net (decrease) increase in cash and cash equivalents	52,246	28,053	(15,056)
Cash and cash equivalents at beginning of the period	129,592	101,539	116,595
Cash and cash equivalents at end of the period	$ 181,838	$ 129,592	$ 101,539
Supplemental Disclosures of Non-Cash Investing and Financing Activities:			
Financed capital expenditures	$ 724	$ 373	$ 1,390
Income taxes paid	$ 1,746	$ 1,961	$ 1,152

The accompanying notes are an integral part of these consolidated financial statements.

SECUREWORKS CORP.

CONSOLIDATED STATEMENTS OF STOCKHOLDERS' EQUITY

(in thousands, except per share data)

	Common Stock - Class A		Common Stock - Class B						
	Outstanding Shares	Amount	Outstanding Shares	Amount	Additional Paid in Capital	Accumulated Deficit	Accumulated Other Comprehensive (Loss) Income	Treasury Stock	Total Stockholders' Equity
Balances, February 3, 2017	**10,566**	**$ 107**	**70,000**	**$ 700**	**$ 854,907**	**$ (126,745)**	**$ (3,514)**	**$ —**	**$ 725,455**
Net loss	—	—	—	—	—	(10,417)	—	—	(10,417)
Other comprehensive (loss) income	—	—	—	—	—	—	3,544	—	3,544
Vesting of restricted stock units	384	4	—	—	(4)	—	—	—	—
Grants of restricted stock awards, net	284	2	—	—	(2)	—	—	—	—
Common stock withheld as payment for withholding taxes upon the vesting of restricted shares	(149)	(2)	—	—	(1,280)	—	—	—	(1,282)
Stock-based compensation	—	—	—	—	13,790	—	—	—	13,790
Balances, February 2, 2018	**11,085**	**$ 111**	**70,000**	**$ 700**	**$ 867,411**	**$ (137,162)**	**$ 30**	**$ —**	**$ 731,090**
Net loss	—	—	—	—	—	(39,101)	—	—	(39,101)
Other comprehensive (loss) income	—	—	—	—	—	—	(2,914)	—	(2,914)
Vesting of restricted stock units	598	5	—	—	(5)	$ —	—	—	—
Grants of restricted stock awards, net	386	4	—	—	(4)	$ —	—	—	—
Common stock withheld as payment for withholding taxes upon the vesting of restricted shares	(234)	(2)	—	—	(2,205)	—	—	—	(2,207)
Stock-based compensation	—	—	—	—	19,370	—	—	—	19,370
Shares repurchased	(819)	(8)	—	—	—	—	—	(13,523)	(13,531)
Balances, February 1, 2019	**11,016**	**$ 110**	**70,000**	**$ 700**	**$ 884,567**	**$ (176,263)**	**$ (2,884)**	**$ (13,523)**	**$ 692,707**
Net loss	—	—	—	—	—	(31,666)	—	—	(31,666)
Other comprehensive (loss) income	—	—	—	—	—	—	(206)	—	(206)
Vesting of restricted stock units	957	9	—	—	(9)	—	—	—	—
Exercise of stock options	95	1	—	—	1,326	—	—	—	1,327
Grants of restricted stock awards, net	122	1	—	—	(1)	—	—	—	—
Cancellation of unvested restricted stock awards	(124)	(1)	—	—	1	—	—	—	—
Common stock withheld as payment for withholding taxes upon the vesting of restricted shares	(422)	(4)	—	—	(8,449)	—	—	—	(8,453)
Stock-based compensation	—	—	—	—	19,548	—	—	—	19,548
Shares repurchased	(438)	(4)	—	—	—	—	—	(6,373)	(6,377)
Balances, January 31, 2020	**11,206**	**$ 112**	**70,000**	**$ 700**	**$ 896,983**	**$ (207,929)**	**$ (3,090)**	**$ (19,896)**	**$ 666,880**

The accompanying notes are an integral part of these consolidated financial statements.

NOTE 1 - DESCRIPTION OF THE BUSINESS AND BASIS OF PRESENTATION

Description of the Business

SecureWorks Corp. (individually and collectively with its consolidated subsidiaries, “Secureworks” or the “Company”) is a leading global provider of technology-driven information security solutions singularly focused on protecting the Company's customers from cyber attacks.

On April 27, 2016, the Company completed its initial public offering (“IPO”), as further described below. Upon the closing of the IPO, Dell Technologies Inc. (“Dell Technologies”) owned, indirectly through Dell Inc. (“Dell”) and Dell’s subsidiaries, no shares of the Company's outstanding Class A common stock and all shares of the Company's outstanding Class B common stock, which as of January 31, 2020 represented approximately 86.2% of the Company's total outstanding shares of common stock and approximately 98.4% of the combined voting power of both classes of the Company's outstanding common stock.

The Company has one primary business activity, which is to provide customers with information security solutions. The Company’s chief operating decision-maker, who is the President and Chief Executive Officer, makes operating decisions, assesses performance and allocates resources on a consolidated basis. There are no segment managers who are held accountable for operations and operating results below the consolidated unit level. Accordingly, Secureworks operates its business as a single reportable segment.

Basis of Presentation and Consolidation

The Company’s consolidated financial statements have been prepared in accordance with accounting principles generally accepted in the United States of America (“GAAP”). The preparation of financial statements in accordance with GAAP requires management to make estimates and assumptions that affect the amounts reported in the Company’s financial statements. The consolidated financial statements include assets, liabilities, revenue and expenses of all majority-owned subsidiaries. Intercompany transactions and balances are eliminated in consolidation.

For the periods presented, Dell has provided various corporate services to the Company in the ordinary course of business, including finance, tax, human resources, legal, insurance, IT, procurement and facilities-related services. The cost of these services are charged in accordance with a shared services agreement that went into effect on August 1, 2015. For more information regarding the related party transactions, see “Note 13—Related Party Transactions.”

During the periods presented in the financial statements, Secureworks did not file separate federal tax returns, as the Company is generally included in the tax grouping of other Dell entities within the respective entity’s tax jurisdiction. The income tax benefit has been calculated using the separate return method, modified to apply the benefits for loss approach. Under the benefits for loss approach, net operating losses or other tax attributes are characterized as realized or as realizable by Secureworks when those attributes are utilized or expected to be utilized by other members of the Dell consolidated group. See “Note 11—Income and Other Taxes” for more information.

Fiscal Year

The Company’s fiscal year is the 52- or 53-week period ending on the Friday closest to January 31. The Company refers to the fiscal years ended January 31, 2020, February 1, 2019 and February 2, 2018, as fiscal 2020, fiscal 2019 and fiscal 2018, respectively. Fiscal 2020, fiscal 2019 and fiscal 2018 each consisted of 52 weeks.

Use of Estimates

The preparation of financial statements in conformity with GAAP requires management to make estimates and assumptions that affect the reported amounts of assets and liabilities, the disclosure of contingent assets and liabilities at the date of the financial statements and the reported amounts of revenue and expenses during the reporting periods. Estimates are revised as additional information becomes available. In the Consolidated Statements of Operations, estimates are used when accounting for revenue arrangements, determining the cost of revenue, allocating cost and estimating the impact of contingencies. In the Statements of Financial Position, estimates are used in determining the valuation and recoverability of assets, such as accounts receivables, inventories, fixed assets, goodwill and other identifiable intangible assets, and estimates are used in determining the reported amounts of liabilities, such as taxes payable and the impact of contingencies, all of which also impact the Consolidated Statements of Operations. Actual results could differ from these estimates.

NOTE 2 — SIGNIFICANT ACCOUNTING POLICIES

Cash and Cash Equivalents. As of January 31, 2020 and February 1, 2019, cash and cash equivalents are comprised of cash held in bank accounts and money market funds. The cash and cash equivalents are reported at their current carrying value, which approximates fair value due to the short-term nature of these instruments. The money market funds are valued using quoted market prices and are included as Level 1 inputs. As of January 31, 2020 and February 1, 2019, the Company had $100.5 million and $90.7 million, respectively, invested in money market funds.

Accounts Receivable. Trade accounts receivable are recorded at the invoiced amount, net of allowances for doubtful accounts. Accounts receivable are charged against the allowance for doubtful accounts when deemed uncollectible. Management regularly reviews the adequacy of the allowance for doubtful accounts by considering the age of each outstanding invoice, each customer's expected ability to pay, and the collection history with each customer, when applicable, to determine whether a specific allowance is appropriate. As of January 31, 2020 and February 1, 2019, the allowance for doubtful accounts was $5.1 million and $6.2 million, respectively.

Unbilled accounts receivable included in accounts receivable, totaling $11.2 million and $13.8 million as of January 31, 2020 and February 1, 2019, respectively, relate to work that has been performed, though invoicing has not yet occurred. All of the unbilled receivables are expected to be billed and collected within the upcoming fiscal year.

Allowance for Doubtful Accounts. The Company recognizes an allowance for losses on accounts receivable in an amount equal to the estimated probable losses, net of recoveries. The allowance is based on an analysis of historical bad debt experience, current receivables aging, and expected future write-offs, as well as an assessment of specific identifiable customer accounts considered at risk or uncollectible. The expense associated with the allowance for doubtful accounts is recognized in general and administrative expenses.

Fair Value Measurements. The Company measures fair value within the guidance of the three-level valuation hierarchy. This hierarchy is based upon the transparency of inputs to the valuation of an asset or liability as of the measurement date. The categorization of a measurement within the valuation hierarchy is based upon the lowest level of input that is significant to the fair value measurement. The carrying amounts of the Company's financial instruments, including cash equivalents, accounts receivable, accounts payable and accrued expenses, approximate their respective fair values due to their short-term nature.

Inventories. Inventories consist of finished goods, which include hardware devices such as servers, log retention devices and appliances that are sold in connection with the Company's solutions offerings. Inventories are stated at lower of cost or net realizable value, with cost being determined on a first-in, first-out (FIFO) basis.

Prepaid Maintenance and Support Agreements. Prepaid maintenance and support agreements represent amounts paid to third-party service providers for maintenance, support and software license agreements in connection with the Company's obligations to provide maintenance and support services. The prepaid maintenance and support agreement balance is amortized on a straight-line basis over the contract term and is primarily recognized as a component of cost of revenue. Amounts that are expected to be amortized within one year are recorded in other current assets and the remaining balance is recorded in other non-current assets.

Property and Equipment. Property and equipment are carried at depreciated cost. Depreciation is calculated using the straight-line method over the estimated economic lives of the assets, which range from two to five years. Leasehold improvements are amortized over the shorter of five years or the lease term. For the fiscal years ended January 31, 2020, February 1, 2019 and February 2, 2018, depreciation expense was $14.7 million, $13.5 million and $14.4 million, respectively. Gains or losses related to retirements or disposition of fixed assets are recognized in the period incurred.

Leases. The Company determines if any arrangement is, or contains, a lease at inception based on whether or not the Company has the right to control the asset during the contract period and other facts and circumstances. Secureworks is the lessee in a lease contract when the Company obtains the right to control the asset. Operating leases are included in the line items operating lease right-of-use assets, net; accrued and other current liabilities; and operating lease liabilities, non-current in the consolidated statements of financial position. Leases with a lease term of 12 months or less at inception are not recorded in the consolidated statements of financial position and are expensed on a straight-line basis over the lease term in the consolidated statements of operations. The Company determines the lease term by assuming the exercise of renewal options that are reasonably certain. As most of the Company's leases do not provide an implicit interest rate, Secureworks uses the Company's incremental borrowing rate based on the information available at commencement date in determining the present value of future payments. When the Company's contracts contain lease and nonlease components, the Company accounts for both components as a single lease component. Refer to "Note 8—Leases" for further discussion.

Intangible Assets Including Goodwill. Identifiable intangible assets with finite lives are amortized on a straight-line basis over their estimated useful lives. Finite-lived intangible assets are reviewed for impairment on a quarterly basis, or as potential triggering events are identified. Goodwill and indefinite-lived intangible assets are tested for impairment on an annual basis in the third fiscal quarter, or sooner if an indicator of impairment occurs. To determine whether goodwill and indefinite-lived intangible assets are impaired, the Company first assesses certain qualitative factors. Based on this assessment, if it is determined that the fair value of the goodwill or indefinite-lived intangible asset is less than its carrying amount, the Company performs the quantitative analysis of the impairment test.

The goodwill impairment test consists of a two-step process, if necessary. The first step is to compare the fair value of the reporting unit to its carrying value, including goodwill. The Company used a combination of income (discounted cash flow) and market approach model to determine the fair value of the reporting unit. The assumptions used in the model are consistent with those which the Company believes hypothetical marketplace participants would use. If the fair value of the reporting unit is less than its carrying value, the second step of the impairment test must be performed in order to determine the amount of the impairment loss, if any. The second step requires the Company to determine the implied fair value of goodwill by allocating the reporting unit's fair value to each of its assets and liabilities as if the reporting unit was acquired in a business acquisition. If the carrying amount of the reporting unit’s goodwill exceeds its implied fair value, an impairment charge is recognized in an amount equal to that excess. The loss recognized cannot exceed the carrying amount of goodwill. The Company has determined that it has a single goodwill reporting unit, and, accordingly, for the quantitative analysis, it compares the fair value of this goodwill reporting unit to its carrying value. For indefinite-lived assets, other than goodwill, if the carrying amount determined through the quantitative analysis exceeds the fair value, an impairment charge is recognized in an amount equal to that excess.

Deferred Commissions and Deferred Fulfillment Costs. The Company accounts for both costs to obtain a contract for a customer, which are defined as costs that the Company would not have incurred if the contract had not been obtained, and costs to fulfill a contract by capitalizing and systematically amortizing the assets on a basis that is consistent with the transfer to the customer of the goods or services to which the assets relate. These costs generate or enhance resources used in satisfying performance obligations that directly relate to contracts. Applying the practical expedient guidance, the Company recognizes the incremental costs of obtaining contracts as an expense when incurred if the amortization period of the incremental costs of obtaining contracts that the Company otherwise would have recognized is one year or less.

The Company’s customer acquisition costs are primarily attributable to sales commissions and related fringe benefits earned by the Company's sales force and such costs are considered incremental costs to obtain a contract. Sales commissions for initial contracts are deferred and amortized taking into consideration the pattern of transfer to which assets relate and may include expected renewal periods where renewal commissions are not commensurate with the initial commission period. The Company recognizes the deferred commissions on a straight-line basis over the life of the customer relationship (estimated to be six years) in sales and marketing expenses. These assets are classified as non-current, and included in other non-current assets in the Consolidated Statements of Financial Position. As of January 31, 2020 and February 1, 2019, the amount of deferred commissions included in other non-current assets was $62.8 million and $62.9 million, respectively.

Additionally, the Company incurs certain costs to install and activate hardware and software used in its managed security solutions, primarily related to a portion of the compensation for the personnel who perform the installation activities. The Company makes judgments regarding the fulfillment costs to be capitalized. Specifically, the Company capitalizes direct labor and associated fringe benefits using standards developed from actual costs and applicable operational data. The Company updates the information quarterly for items such as the estimated amount of time required to perform such activity. The Company capitalizes and amortizes these fulfillment costs on a straight-line basis over the economic life of the services, or approximately four years, in cost of revenue. As of January 31, 2020 and February 1, 2019, the amount of deferred fulfillment costs included in other non-current assets was $11.4 million and $11.0 million, respectively.

Foreign Currency Translation. During the periods presented, Secureworks primarily operated in the United States. For the majority of the Company’s international businesses, the Company has determined that the functional currency of those subsidiaries is the local currency. Accordingly, assets and liabilities for these entities are translated at current rates of exchange in effect at the balance sheet date. Revenue and expenses from these international subsidiaries are translated using the monthly average exchange rates in effect for the period in which the items occur. Foreign currency translation adjustments are included as a component of accumulated other comprehensive loss, while foreign currency transaction gains and losses are recognized in the Statements of Operations within interest and other, net. These transaction (losses) gains totaled $(0.3) million, $1.8 million and $(3.3) million in the fiscal years ended January 31, 2020, February 1, 2019 and February 2, 2018, respectively.

Revenue Recognition. Secureworks derives revenue primarily from two sources: (1) subscription revenue related to managed security and threat intelligence solutions; and (2) professional services, including security and risk consulting and incident response solutions.

Subscription-based arrangements typically include security solutions, up-front installation fees and maintenance, and also may include the provision of an associated hardware appliance. The Company uses its hardware appliances in providing security solutions required to access the Company's technology platform. The arrangements that require hardware do not typically convey ownership of the appliance to the customer. Moreover, any related installation fees are non-refundable and are also incapable of being distinct within the context of the arrangement. Therefore, the Company has determined that these arrangements constitute a single performance obligation for which the revenue and any related costs are recognized over the term of the arrangement ratably, which reflects the Company's performance in transferring control of the services to the customer. Amounts that have been invoiced, but for which the above revenue recognition criteria have not been met, are included in deferred revenue.

Professional services consist primarily of fixed-fee and retainer-based contracts. Revenue from these engagements is recognized using an input method over the contract term.

The Company reports revenue net of any revenue-based taxes assessed by governmental authorities that are imposed on, and concurrently with, specific revenue-producing transactions.

The Company recognizes revenue when all of the following criteria are met:

- ***Identification of the contract, or contracts, with a customer—***A contract with a customer exists when (i) the Company enters into an enforceable contract with a customer, (ii) the contract has commercial substance and the parties are committed to perform, and (iii) payment terms can be identified and collection of substantially all consideration to which the Company will be entitled in exchange for goods or services that will be transferred is deemed probable based on the customer's intent and ability to pay. Contracts entered into for professional services and subscription-based solutions near or at the same time are generally not combined as a single contract for accounting purposes, since neither the pricing nor the services are interrelated.
- ***Identification of the performance obligations in the contract—***Performance obligations promised in a contract are identified based on the goods or services that will be transferred to the customer that are both (i) capable of being distinct, whereby the customer can benefit from the goods or service either on its own or together with other resources that are readily available from third parties or from the Company, and (ii) distinct in the context of the contract, whereby the transfer of the goods or services is separately identifiable from other promises in the contract. When promised goods or services are incapable of being distinct, the Company accounts for them as a combined performance obligation. With regard to a typical contract for subscription-based solutions, the performance obligation represents a series of distinct services that will be accounted for as a single performance obligation. In a typical professional services contract, the Company has a separate performance obligation associated with each service. The Company is generally acting as a principal in each subscription-based and professional services arrangement and, thus, recognizes revenue on a gross basis.
- ***Determination of the transaction price—***The total transaction price is primarily fixed in nature as the consideration is tied to the specific services purchased by the customer, which constitutes a series for delivery of the solutions over the duration of the contract. For professional services contracts, variable consideration exists in the form of rescheduling penalties and expense reimbursements; no estimation is required at contract inception, since variable consideration is allocated to the applicable period.
- ***Allocation of the transaction price to the performance obligations in the contract—***The Company allocates the transaction price to each performance obligation based on the performance obligation's standalone selling price. Standalone selling price is determined by considering all information available to the Company, such as historical selling prices of the performance obligation, geographic location, overall strategic pricing objective, market conditions and internally approved pricing guidelines related to the performance obligations.
- ***Recognition of revenue when, or as, the Company satisfies performance obligation—***The Company recognizes revenue over time using a time-elapsed output method to measure progress (i.e., ratable recognition) for the subscription-based performance obligation over the contract term. For any upgraded installation services, which the Company has determined represent a performance obligation separate from its subscription-based arrangements, revenue is recognized over time using hours elapsed over the service term as an appropriate method to measure progress. For the performance obligation pertaining to professional services arrangements, the Company recognizes revenue over time using an input method based on time (hours or days) incurred to measure progress over the contract term.

As indicated above, the Company has one primary business activity, which is to provide customers with technology-driven information security solutions. The Company's chief operating decision maker, who is the President and Chief Executive

Officer, makes operating decisions, assesses performance, and allocates resources on a consolidated basis. There are no segment managers who are held accountable for operations and operating results below the consolidated unit level. Accordingly, the Company is considered to be in a single reportable segment and operating unit structure.

The following table presents revenue by service type (in thousands):

	January 31, 2020	February 1, 2019	February 2, 2018
Managed Security Solutions revenue	$ 419,489	$ 396,130	$ 365,768
Security and Risk Consulting revenue	133,276	122,579	102,162
Total revenue	$ 552,765	$ 518,709	$ 467,930

Deferred Revenue (Contract Liabilities). Deferred revenue represents amounts contractually billed to customers or payments received from customers for which revenue has not yet been recognized. Deferred revenue that is expected to be recognized as revenue within one year is recorded as short-term deferred revenue and the remaining portion is recorded as long-term deferred revenue.

The Company has determined that its contracts generally do not include a significant financing component. The primary purpose of the Company's invoicing terms is to provide customers with simplified and predictable ways of purchasing its solutions, not to receive financing from customers or to provide customers with financing. Examples of such terms include invoicing at the beginning of a subscription term with revenue recognized ratably over the contract period.

Cost of Revenue. Cost of revenue consists primarily of compensation and related expenses, including salaries, benefits and performance-based compensation for employees who maintain the Counter Threat Platform and provide support services to customers, as well as perform other critical functions. Other expenses include depreciation of equipment and costs associated with maintenance agreements for hardware provided to customers as part of their subscription-based solutions. In addition, cost of revenue includes amortization of technology licensing fees, fees paid to contractors who supplement or support solutions offerings, maintenance fees and overhead allocations.

Research and Development Costs. Research and development costs are expensed as incurred. Research and development expenses include compensation and related expenses for the continued development of solutions offerings, including a portion of expenses related to the threat research team, which focuses on the identification of system vulnerabilities, data forensics and malware analysis and product management. In addition, expenses related to the development and prototype of new solutions offerings also are included in research and development costs, as well as allocated overhead. The Company’s solutions offerings have generally been developed internally.

Sales and Marketing. Sales and marketing expense includes compensation and related expenses, including salaries, benefits, and performance-based compensation, including sales commissions and related expenses for sales and marketing personnel, marketing and advertising programs, including lead generation, customer advocacy events, other brand-building expenses and allocated overhead. Advertising costs are expensed as incurred and were $13.3 million, $12.6 million and $14.7 million for the fiscal years ended January 31, 2020, February 1, 2019 and February 2, 2018, respectively.

General, and Administrative. General and administrative expense primarily includes the costs of human resources and recruiting, finance and accounting, legal support, management information systems and information security systems, facilities management and other administrative functions, offset by allocations of information technology and facilities costs to other functions.

Software Development Costs. Qualifying software costs developed for internal use are capitalized when application development begins, it is probable that the project will be completed, and the software will be used as intended. In order to expedite delivery of the Company’s security solutions, the application stage typically commences before the preliminary development stage is completed. Accordingly, no significant software development costs have been capitalized during any period presented.

The Company capitalizes development costs incurred for software and applications to be sold, leased or otherwise marketed after technological feasibility of the software or application is established. Under the Company’s current practice of developing new software, the technological feasibility of the underlying software or application is not established until substantially all product development and testing is complete, which generally includes the development of a working model. Software development costs that have been capitalized to date have been insignificant.

Income Taxes. Current income tax expense is the amount of income taxes expected to be payable for the current year. Deferred tax assets and liabilities are recorded based on the difference between the financial statement and tax basis of assets and liabilities using enacted tax rates in effect for the year in which the differences are expected to reverse. The effect on deferred tax assets and liabilities of a change in tax rates is recognized in the Statement of Operations in the period that includes the enactment date. The Company calculates a provision for income taxes using the asset and liability method, under which deferred tax assets and liabilities are recognized by identifying the temporary differences arising from the different treatment of items for tax and accounting purposes. The Company accounts for the tax impact of including Global Intangible Low Tax Income ("GILTI") in U.S. taxable income as a period cost. The Company provides valuation allowances for deferred tax assets, where appropriate. In assessing the need for a valuation allowance, Secureworks considers all available evidence for each jurisdiction, including past operating results, estimates of future taxable income, and the feasibility of ongoing tax planning strategies. In the event Secureworks determines all or part of the net deferred tax assets are not realizable in the future, it will make an adjustment to the valuation allowance that would be charged to earnings in the period such determination is made.

The accounting guidance for uncertainties in income tax prescribes a comprehensive model for the financial statement recognition, measurement, presentation and disclosure of uncertain tax positions taken or expected to be taken in income tax returns. The Company recognizes a tax benefit from an uncertain tax position in the financial statements only when it is more likely than not that the position will be sustained upon examination, including resolution of any related appeals or litigation processes, based on the technical merits and a consideration of the relevant taxing authority's administrative practices and precedents.

During the periods presented in the financial statements, the Company did not file separate federal tax returns, as the Company was generally included in the tax grouping of other Dell entities within the respective entity's tax jurisdiction. The income tax benefit has been calculated using the separate return method, modified to apply the benefits for loss approach. Under the benefits for loss approach, net operating losses or other tax attributes are characterized as realized or as realizable by the Company when those attributes are utilized or expected to be utilized by other members of the Dell consolidated group.

Stock-Based Compensation. The Company's compensation programs include grants under the SecureWorks Corp. 2016 Long-Term Incentive Plan and, prior to the IPO date, grants under share-based payment plans of Dell Technologies. Under the plans, the Company, and prior to the IPO, Dell Technologies, have granted stock options, restricted stock awards and restricted stock units. Compensation expense related to stock-based transactions is measured and recognized in the financial statements based on fair value. Fair value for restricted stock awards and restricted stock units under the Company's plan is based on the closing price of the Company's Class A common stock as reported on the Nasdaq Global Select Market on the day of the grant. The fair value of each option award is estimated on the grant date using the Black-Scholes option-pricing model and a single option award approach. This model requires that at the date of grant the Company must determine the fair value of the underlying common stock, the expected term of the award, the expected volatility, risk-free interest rates and expected dividend yield. The Company's annual grant of restricted stock and restricted stock units issued during the fiscal year ended January 31, 2020 vest over an average service period of three years and approximately 50% of such awards are subject to performance conditions. Stock-based compensation expense, with respect to service-based awards is adjusted for forfeitures, and recognized using a straight-line basis over the requisite service periods of the awards, which is generally three to four years. Stock-based compensation expense, with respect to performance awards is adjusted for forfeitures and performance criteria, and recognized on a graded vesting basis. The Company estimates a forfeiture rate, based on an analysis of actual historical forfeitures, to calculate stock-based compensation expense.

Loss Contingencies. Secureworks is subject to the possibility of various losses arising in the ordinary course of business. An estimated loss contingency is accrued when it is probable that an asset has been impaired or a liability has been incurred and the amount of loss can be reasonably estimated. The Company regularly evaluates current information available to determine whether such accruals should be adjusted and whether new accruals are required. See "Note 7–Commitments and Contingencies" for more information about these loss contingencies.

Recently Adopted Accounting Pronouncements

Leases. The Company adopted Accounting Standards Update ("ASU") No. 2016-02, "Leases (Topic 842)," effective February 2, 2019. Accounting Standards Codification ("ASC") 842 "Leases" requires lessees to recognize operating lease right-of-use ("ROU") assets, representing their right to use the underlying asset for the lease term, and lease liabilities on the balance sheet for all leases with lease terms greater than 12 months. The guidance also requires qualitative and quantitative disclosures designed to assess the amount, timing and uncertainty of cash flows arising from leases. The Company adopted ASU No. 2016-02 using the modified retrospective method and utilized the optional transition method under which the Company will continue to apply the legacy guidance in ASC 840, including its disclosure requirements, in the comparative period presented. In addition, Secureworks elected the package of practical expedients permitted under the transition guidance which permits the Company to: (i) carry forward the historical lease classification; (ii) not separate lease components from non-lease components within the Company's facility lease contracts; (iii) not present comparative periods but rather record a cumulative catch-up during fiscal 2020; and (iv) elect, by asset class, not to record on the balance sheet a lease whose term is twelve months or less including reasonably certain renewal options. As a result of the adoption for the fiscal year beginning February 2, 2019, the Company recorded initial operating lease ROU assets and operating lease liabilities, all related to real estate, of $28.0 million and $31.8 million, respectively.

Recently Issued Accounting Pronouncements

Income Taxes. In December 2019, the Financial Accounting Standards Board (the "FASB") issued ASU No. 2019-12, “Income Taxes (Topic 740): Simplifying the Accounting for Income Taxes.” ASU No. 2019-12 simplifies the accounting for income taxes by eliminating certain exceptions to the guidance in Topic 740 related to the approach for intraperiod tax allocation, the methodology for calculating income taxes in an interim period and the recognition of deferred tax liabilities for outside basis differences. The new guidance also simplifies aspects of the accounting for franchise taxes and enacted changes in tax laws or rates and clarifies the accounting for transactions that result in a step-up in the tax basis of goodwill and allocating consolidated income taxes to separate financial statements of entities not subject to income tax. ASU No. 2019-12 is effective for fiscal years beginning after December 15, 2020, with early adoption permitted. Upon adoption, the Company must apply certain aspects of this standard retrospectively for all periods presented while other aspects are applied on a modified retrospective basis through a cumulative-effect adjustment to retained earnings as of the beginning of the fiscal year of adoption. The Company is currently evaluating the impact of this new standard on its consolidated financial statements.

Intangibles - Goodwill and Other - Internal-Use Software. In August 2018, the FASB issued ASU No. 2018-15, “Intangibles-Goodwill and Other-Internal-Use Software (Subtopic 350-40): Customer’s Accounting for Implementation Costs Incurred in a Cloud Computing Arrangement That Is a Service Contract.” ASU No. 2018-15 aligns the requirements for capitalizing implementation costs in such cloud computing arrangements with the requirements for capitalizing implementation costs incurred to develop or obtain internal-use software. The updated guidance is effective for the Company for annual and interim periods beginning in the Company's 2021 fiscal year, with early adoption permitted. Entities may choose to adopt the new guidance prospectively or retrospectively. The Company does not expect that the adoption of this standard will have a material impact on its consolidated financial statements.

Intangibles - Goodwill and Other. In January 2017, the FASB issued ASU No. 2017-04, “Intangibles-Goodwill and Other (Topic 350): Simplifying the Test for Goodwill Impairment.” ASU No. 2017-04 eliminates Step 2 of the goodwill impairment test, which required the Company to determine the implied fair value of goodwill by allocating the reporting unit's fair value to each of its assets and liabilities as if the reporting unit was acquired in a business acquisition. Instead, the updated guidance requires an entity to perform its annual or interim goodwill impairment test by comparing the fair value of the reporting unit to its carrying value, and recognizing a non-cash impairment charge for the amount by which the carrying value exceeds the reporting unit's fair value, with the loss not exceeding the total amount of goodwill allocated to that reporting unit. The updated guidance is effective for the Company for annual and interim periods beginning in the Company's 2021 fiscal year, with early adoption permitted, and will be applied on a prospective basis. The Company does not expect that the adoption of this standard will have a material impact on its consolidated financial statements.

Financial Instruments - Credit Losses. In June 2016, the FASB issued ASU No. 2016-13, “Financial Instruments - Credit Losses (Topic 326): Measurement of Credit Losses on Financial Instruments.” The amendments in this update replace the incurred loss impairment methodology in current GAAP with a methodology that reflects expected credit losses and requires consideration of a broader range of reasonable and supportable information to inform credit loss estimates. The update is effective for the Company for fiscal years beginning with the Company’s 2021 fiscal year, including interim periods within those fiscal years. The Company does not expect that the adoption of this standard will have a material impact on its consolidated financial statements.

NOTE 3 — LOSS PER SHARE

Loss per share is calculated by dividing net loss for the periods presented by the respective weighted-average number of common shares outstanding, and excludes any dilutive effects of share-based awards that may be anti-dilutive. Diluted net loss per common share is computed by giving effect to all potentially dilutive common shares, including common stock issuable upon the exercise of stock options and unvested restricted common stock and restricted stock units. The Company applies the two-class method to calculate earnings per share. Because the Class A common stock and the Class B common stock share the same rights in dividends and earnings, earnings per share (basic and diluted) are the same for both classes. Since losses were incurred in all periods presented, all potential common shares were determined to be anti-dilutive.

The following table sets forth the computation of loss per common share (in thousands, except per share amounts):

	Fiscal Year Ended		
	January 31, 2020	February 1, 2019	February 2, 2018
Numerator:			
Net loss	$ (31,666)	$ (39,101)	$ (10,417)
Denominator:			
Weighted-average number of shares outstanding:			
Basic and Diluted	80,563	80,710	80,280
Loss per common share:			
Basic and Diluted	$ (0.39)	$ (0.48)	$ (0.13)
Weighted-average anti-dilutive stock options, non-vested restricted stock and restricted stock units	5,826	5,966	5,096

NOTE 4 — CONTRACT BALANCES AND CONTRACT COSTS

Promises to provide services related to the Company's subscription-based solutions are accounted for as a single performance obligation over an average period of two years. Performance obligations related to the Company's security and risk consulting professional service contracts are separate obligations associated with each service. Although the Company has many multi-year customer relationships for its various professional service solutions, the arrangement is typically structured as a separate performance obligation over the contract period and recognized over a duration of less than one year.

Deferred revenue represents the aggregate amount of billing in advance of service delivery. The deferred revenue balance does not represent the total contract value of annual or multi-year, non-cancelable subscription agreements. Therefore, the Company invoices its customers based on a variety of billing schedules. During the fiscal year ended January 31, 2020, on average, approximately 58% of the Company's recurring revenue was billed in advance and approximately 42% was billed on either a monthly or quarterly basis. In addition, many of the Company's professional services engagements are billed in advance of service commencement. The deferred revenue balance is influenced by several factors, including seasonality, the compounding effects of renewals, invoice duration and invoice timing.

Changes to the Company's deferred revenue during the fiscal years ended January 31, 2020 and February 1, 2019 are as follows (in thousands):

	As of February 1, 2019	Upfront payments received and billings during the fiscal year ended January 31, 2020	Revenue recognized during the fiscal year ended January 31, 2020	As of January 31, 2020
Deferred revenue	$ 173,929	$ 249,215	$ (234,607)	$ 188,537

	As of February 2, 2018	Upfront payments received and billings during the fiscal year ended February 1, 2019	Revenue recognized during the fiscal year ended February 1, 2019	As of February 1, 2019
Deferred revenue	$ 152,645	$ 206,960	$ (185,676)	$ 173,929

Remaining Performance Obligation

The remaining performance obligation represents the transaction price allocated to contracted revenue that has not yet been recognized, which includes deferred revenue and non-cancellable contracts that will be invoiced and recognized as revenue in future periods. The remaining performance obligation consists of two elements: (i) the value of remaining services to be provided through the contract term for customers whose services have been activated ("active"); and (ii) the value of services contracted with customers that have not yet been installed ("backlog"). Backlog is not recorded in revenue, deferred revenue or elsewhere in the consolidated financial statements until the Company establishes a contractual right to invoice, at which point it is recorded as revenue or deferred revenue, as appropriate. The Company applies the practical expedient in ASC paragraph 606-10-50-14(a) and does not disclose information about remaining performance obligations that are part of a contract that has an original expected duration of one year or less.

The Company expects that the amount of backlog relative to the total value of its contracts will change from year to year due to several factors, including the amount invoiced at the beginning of the contract term, the timing and duration of the Company's customer agreements, varying invoicing cycles of agreements and changes in customer financial circumstances. Accordingly, fluctuations in backlog are not always a reliable indicator of future revenues.

As of January 31, 2020, the Company expects to recognize remaining performance obligations as follows (in thousands):

	Total	Expected to be recognized in the next 12 months	Expected to be recognized in 12-24 months	Expected to be recognized in 24-36 months	Expected to be recognized thereafter
Performance obligation - active	$ 285,833	$ 160,195	$ 85,660	$ 28,497	$ 11,481
Performance obligation - backlog	25,391	10,067	9,707	5,494	123
Total	$ 311,224	$ 170,262	$ 95,367	$ 33,991	$ 11,604

Deferred Commissions and Fulfillment Costs

The Company capitalizes a significant portion of its commission expense and related fringe benefits earned by its sales personnel. Additionally, the Company capitalizes certain costs to install and activate hardware and software used in its managed security solutions, primarily related to a portion of the compensation for the personnel who perform the installation activities. These deferred costs are amortized on a systematic basis that is consistent with the transfer to the customer of the goods or services to which the assets relate.

Changes in the balance of total deferred commission and total deferred fulfillment costs during the fiscal years ended January 31, 2020 and February 1, 2019 are as follows (in thousands):

	As of February 1, 2019	Amount capitalized	Amount expensed	As of January 31, 2020
Deferred commissions	$ 62,895	$ 19,053	$ (19,163)	$ 62,785
Deferred fulfillment costs	10,973	5,921	(5,528)	11,366

	As of February 2, 2018	Amount capitalized	Amount expensed	As of February 1, 2019
Deferred commissions	$ 57,229	$ 19,915	$ (14,249)	$ 62,895
Deferred fulfillment costs	10,163	5,920	(5,110)	10,973

As referenced in “Note 2 — Significant Accounting Policies,” deferred commissions are recognized on a straight-line basis over the life of the customer relationship, which historically had been estimated to be seven years. During the third quarter of fiscal 2020, the Company determined to change the estimated life of the customer relationship to be six years, The net impact of this change was an increase in operating loss for the fiscal year ended January 31, 2020 of $3.5 million on a pre-tax basis, or $0.03 on a per share basis. The Company did not record any impairment losses on the deferred commissions or deferred fulfillment costs during the fiscal year ended January 31, 2020.

NOTE 5 — GOODWILL AND INTANGIBLE ASSETS

Goodwill relates to the acquisition of Dell by Dell Technologies and represents the excess of the purchase price attributable to Secureworks over the fair value of the assets acquired and liabilities assumed. There were no additions, adjustments or impairments to goodwill during the periods presented. Accordingly, goodwill totaled $416.5 million as of January 31, 2020 and February 1, 2019.

Goodwill and indefinite-lived intangible assets are tested for impairment on an annual basis during the third fiscal quarter of each fiscal year, or earlier if an indicator of impairment occurs. The Company completed the most recent annual impairment test in the third quarter of fiscal 2020 by performing a qualitative assessment of goodwill at the reporting unit level, as well as the Company's indefinite-lived intangible asset. In performing this qualitative assessment, the Company evaluated events and circumstances since the date of the last quantitative impairment test, including the results of that test, macroeconomic conditions, industry and market conditions, key financial metrics and the overall financial performance of the Company. After assessing the totality of the events and circumstances, the Company determined that it was not more likely than not that the fair value of the Secureworks reporting unit was less than its carrying amount and, therefore, that the first step of the quantitative goodwill impairment test was unnecessary. Additionally, based on the qualitative assessment performed in the third quarter of fiscal 2020, the Company determined that it was not more likely than not that the fair value of the other indefinite-lived intangible asset was less than its carrying amount and, therefore, that the first step of the quantitative goodwill impairment test was unnecessary. Further, no triggering events have subsequently transpired that would indicate a potential impairment subsequent to the test date through January 31, 2020.

Intangible Assets

The Company's intangible assets at January 31, 2020 and February 1, 2019 were as follows:

	January 31, 2020			February 1, 2019		
	Gross	Accumulated Amortization	Net	Gross	Accumulated Amortization	Net
			(in thousands)			
Customer relationships	$ 189,518	$ (91,246)	$ 98,272	$ 189,518	$ (77,152)	$ 112,366
Technology	137,371	(85,709)	51,662	135,584	(71,620)	63,964
Finite-lived intangible assets	326,889	(176,955)	149,934	325,102	(148,772)	176,330
Trade name	30,118	—	30,118	30,118	—	30,118
Total intangible assets	$ 357,007	$ (176,955)	$ 180,052	$ 355,220	$ (148,772)	$ 206,448

Amortization expense related to finite-lived intangible assets was approximately $28.2 million for the fiscal year ended January 31, 2020 and approximately $27.7 million in each of the fiscal years ended February 1, 2019 and February 2, 2018, respectively. Amortization expense is included within cost of revenue and general and administrative expenses in the Consolidated Statement of Operations. There were no impairment charges related to intangible assets during the fiscal years ended January 31, 2020, February 1, 2019 and February 2, 2018.

Estimated future pre-tax amortization expense of finite-lived intangible assets as of January 31, 2020 over the next five years and thereafter is as follows:

Fiscal Years	(in thousands)
2021	$ 28,332
2022	28,332
2023	27,885
2024	23,491
2025	14,094
Thereafter	27,800
Total	$ 149,934

NOTE 6 — DEBT

Revolving Credit Facility

On November 2, 2015, SecureWorks, Inc., a wholly-owned subsidiary of SecureWorks Corp., entered into a revolving credit agreement with a wholly-owned subsidiary of Dell Inc. under which the Company obtained a $30 million senior, unsecured revolving credit facility. This facility was initially available for a one-year term beginning on April 21, 2016 and was extended on the same terms for an additional one-year term ending on March 26, 2020. During fiscal 2021, the facility was amended and restated to extend the maturity date to March 26, 2021 and to decrease the annual rate at which interest accrues to the applicable London Interbank Offered Rate plus 1.30%. All other terms remained substantially the same.

Under the facility, up to $30 million principal amount of borrowings may be outstanding at any time. Amounts under the facility may be borrowed, repaid, and reborrowed from time to time during the term of the facility. The proceeds from loans made under the facility may be used for general corporate purposes. The credit agreement contains customary representations, warranties, covenants and events of default. The unused portion of the facility is subject to a commitment fee of 0.35%, which is due upon expiration of the facility.

The maximum amount of borrowings may be increased by up to an additional $30 million by mutual agreement of the lender and borrower. The borrower will be required to repay, in full, all of the loans outstanding, including all accrued interest, and the facility will terminate upon a change of control of SecureWorks Corp. or following a transaction in which SecureWorks, Inc. ceases to be a direct or indirect wholly-owned subsidiary of SecureWorks Corp. The facility is not guaranteed by SecureWorks Corp. or its subsidiaries. There was no outstanding balance under the credit facility as of January 31, 2020 or February 1, 2019.

NOTE 7 — COMMITMENTS AND CONTINGENCIES

Purchase Obligations —The Company had various purchase obligations at January 31, 2020 over a period of approximately four years with vendors or contractors, subject to the Company's operational needs. As of January 31, 2020, the purchase obligations (in thousands) are as follows:

	Payments Due For		
Fiscal Years Ending	Purchase Obligations	Credit Facilities and Other [1]	Total
2021	$ 3,645	$ —	$ 3,645
2022	1,788	500	2,288
2023	260	—	260
2024	—	—	—
2025	—	—	—
2026 and beyond	—	—	—
Total	$ 5,693	$ 500	$ 6,193

[1] Reflects purchase obligations of annual maintenance services for hardware systems for internal use from a related party. See also "Note 13 —Related Party Transactions."

Legal Contingencies — From time to time, the Company is involved in claims and legal proceedings that arise in the ordinary course of business. The Company accrues a liability when it believes that it is both probable that a liability has been incurred and that it can reasonably estimate the amount of the loss. The Company reviews the status of such matters at least quarterly and adjusts its liabilities as necessary to reflect ongoing negotiations, settlements, rulings, advice of legal counsel and other relevant information. Whether the outcome of any claim, suit, assessment, investigation or legal proceeding, individually or collectively, could have a material adverse effect on the Company's business, financial condition, results of operations or cash flows will depend on a number of factors, including the nature, timing and amount of any associated expenses, amounts paid in settlement, damages or other remedies or consequences. To the extent new information is obtained and the Company's views on the probable outcomes of claims, suits, assessments, investigations or legal proceedings change, changes in accrued liabilities would be recorded in the period in which such a determination is made. As of January 31, 2020, the Company does not believe that there were any such matters that, individually or in the aggregate, would have a material adverse effect on its business, financial condition, results of operations or cash flows.

Customer-based Taxation Contingencies—Various government entities ("taxing authorities") require the Company to bill its customers for the taxes they owe based on the services they purchase from the Company. The application of the rules of each taxing authority concerning which services are subject to each tax and how those services should be taxed involves the application of judgment. Taxing authorities periodically perform audits to verify compliance and include all periods that remain open under applicable statutes, which generally range from three to four years. These audits could result in significant assessments of past taxes, fines and interest if the Company were found to be non-compliant. During the course of an audit, a taxing authority may question the Company's application of its rules in a manner that, if the Company were not successful in substantiating its position, could result in a significant financial impact to the Company. In the course of preparing its financial statements and disclosures, the Company considers whether information exists that would warrant disclosure or an accrual with respect to such a contingency.

Indemnifications — In the ordinary course of business, the Company enters into contractual arrangements under which it agrees to indemnify its customers from certain losses incurred by the customer as to third-party claims relating to the services performed on behalf of the Company or for certain losses incurred by the customer as to third-party claims arising from certain events as defined within the particular contract. Such indemnification obligations may not be subject to maximum loss clauses. Historically, payments related to these indemnifications have been immaterial.

Concentrations — The Company sells solutions to customers of all sizes primarily through its direct sales organization, supplemented by sales through channel partners. During the fiscal years ended January 31, 2020, February 1, 2019 and February 2, 2018, the Company had no customer that represented 10% or more of its net revenue during any fiscal period.

NOTE 8 — LEASES

The Company recorded operating lease cost for facilities of approximately $7.9 million for the year ended January 31, 2020, which included expenses of $1.2 million incurred in connection with the consolidation of certain facilities, and variable lease costs of $1.2 million for utilities and common area charges.

For the fiscal year ended January 31, 2020, the Company recorded operating lease costs of approximately $2.3 million for equipment leases which included short-term lease costs of $1.2 million. Lease expense for equipment was included in cost of revenues.

Cash paid for amounts included in the measurement of operating lease liabilities was $6.8 million during the fiscal year ended January 31, 2020.

Weighted-average information associated with the measurement of the Company's remaining operating lease obligations is as follows:

	January 31, 2020
Weighted-average remaining lease term	5.8 years
Weighted-average discount rate	5.33%

The following table summarizes the maturity of the Company's operating lease liabilities as of January 31, 2020 (in thousands):

Fiscal Years Ending	January 31, 2020
2021	$ 5,017
2022	6,498
2023	5,787
2024	5,346
2025	4,572
Thereafter	7,648
Total operating lease payments	$ 34,868
Less imputed interest	(5,314)
Total operating lease liabilities	$ 29,554

The Company's leases have remaining lease terms of 1 month to 7 years, inclusive of renewal or termination options that the Company is reasonably certain to exercise.

Disclosure related to periods prior to adoption of the new lease standard

The Company recorded operating cost for facilities and equipment of approximately $5.5 million and $4.7 million for the years ended February 1, 2019 and February 2, 2018, respectively. As of February 1, 2019, the Company had the following future minimum lease payments under non-cancelable leases prior to the adoption of the new lease standard (in thousands):

Fiscal Years Ending	February 1, 2019
2020	$ 5,237
2021	4,446
2022	6,190
2023	5,440
2024	4,936
Thereafter	11,825
Total operating lease payments	$ 38,074

NOTE 9 — STOCKHOLDERS' EQUITY

On September 26, 2018, the Company's board of directors authorized a stock repurchase program, under which the Company was authorized to repurchase up to $15 million of the Company's Class A common stock through September 30, 2019. On March 26, 2019, the board of directors expanded the repurchase program to authorize the repurchase up to an additional $15 million of the Company's Class A common stock through May 1, 2020. Repurchases may be made from time to time through open market purchases, in privately negotiated transactions, or in other types of transactions. The timing and amount of any repurchases under the program will be determined by management based upon market conditions and other factors. During the fiscal year ended January 31, 2020, the Company repurchased 438,380 shares of Class A common stock at an average price of $14.55, for an aggregate cost of $6.4 million. As of January 31, 2020, $10.1 million remained available for further purchases under the stock repurchase program.

NOTE 10 — STOCK-BASED COMPENSATION AND EMPLOYEE BENEFIT PLAN

In connection with the IPO, the Company's board of directors adopted the SecureWorks Corp. 2016 Long-Term Incentive Plan (the “2016 Plan”). The 2016 Plan became effective on April 18, 2016, and will expire on the tenth anniversary of the effective date unless the 2016 Plan is terminated earlier by the board of directors or in connection with a change in control of SecureWorks Corp. The Company has reserved 12,500,000 shares of Class A common stock for issuance pursuant to awards under the 2016 Plan. The 2016 Plan provides for the grant of options, stock appreciation rights, restricted stock, restricted stock units, deferred stock units, unrestricted stock, dividend equivalent rights, other equity-based awards and cash bonus awards. Awards may be granted under the 2016 Plan to individuals who are employees, officers or non-employee directors of the Company or any of its affiliates, consultants and advisors who perform services for the Company or any of its affiliates, and any other individual whose participation in the 2016 Plan is determined to be in the best interests of the Company by the compensation committee of the board of directors. The Company utilizes both authorized and unissued shares to satisfy all shares issued under the 2016 Plan. During fiscal 2019, the 2016 Plan was amended to increase the total shares of Class A common stock available for issuance by an additional 4,000,000 shares. As of January 31, 2020, there were approximately 4,500,000 shares of Class A common stock available for future grants under the 2016 Plan.

Stock Options

Under the 2016 Plan, the exercise price of each option will be determined by the compensation committee, except that the exercise price may not be less than 100% (or, for incentive stock options to any 10% stockholder, 110%) of the fair market value of a share of Class A common stock on the date on which the option is granted. The term of an option may not exceed ten years (or, for incentive stock options to any 10% stockholder, five years) from the date of grant. The compensation committee will determine the time or times at which each option may be exercised and the period of time, if any, after retirement, death, disability or termination of employment during which options may be exercised. Options may be made exercisable in installments, and the exercisability of options may be accelerated by the compensation committee.

During the fiscal years ended January 31, 2020, February 1, 2019 and February 2, 2018, no stock options were granted to employees or directors. However, the Company recognized $2.7 million, $3.7 million and $3.7 million in compensation expense for the fiscal years ended January 31, 2020, February 1, 2019 and February 2, 2018, respectively, for previously granted options.

The fair value of stock options are estimated as of the date of the grant using the Black-Scholes option pricing model. This model requires the input of subjective assumptions that will usually have a significant impact on the fair value estimate. The expected term was estimated using the SEC simplified method. The risk-free interest rate is the continuously compounded, term-matching, zero-coupon rate from the valuation date. The volatility is the leverage-adjusted, term-matching, historical volatility of peer firms. The dividend yield assumption is consistent with management expectations of dividend distributions based upon the Company's business plan at the date of grant.

The following table summarizes stock option activity and options outstanding and exercisable for the fiscal years ended, and as of, January 31, 2020, February 1, 2019 and February 2, 2018.

	Number of Options	Weighted-Average Exercise Price Per Share	Weighted-Average Contractual Life (years)	Weighted-Average Grant date Fair Value Per Share	Aggregate Intrinsic Value[1]
					(in thousands)
Balance, February 3, 2017	2,578,167	$ 14.00			
Granted	—	—			
Exercised	—	—			
Canceled, expired or forfeited	(53,065)	14.00			
Balance, February 2, 2018	2,525,102	$ 14.00			
Granted	—	—			
Exercised	(9,826)	14.00			
Canceled, expired or forfeited	(27,514)	14.00			
Balance, February 1, 2019	2,487,762	$ 14.00			
Granted	—	—			
Exercised	(94,826)	14.00			
Canceled, expired or forfeited	(144,939)	14.00			
Balance, January 31, 2020	2,247,997	$ 14.00	6.10	$ 6.08	$ 3,890
Options vested and expected to vest, January 31, 2020	2,244,835	$ 14.00	6.10	$ 6.08	$ 3,884
Options exercisable, January 31, 2020	1,646,650	$ 14.00	6.06	$ 6.11	$ 2,849

(1) The aggregate intrinsic values represent the total pre-tax intrinsic values based on the Company's closing share price of $15.73 as reported on the Nasdaq Global Select Market on January 31, 2020, that would have been received by the option holders had all in-the-money options been exercised as of that date.

The total fair value of options vested was $3.6 million, $3.7 million and $3.8 million for the fiscal years ended January 31, 2020, February 1, 2019, and February 2, 2018, respectively. At January 31, 2020, unrecognized stock-based compensation expense related to stock options was $1.6 million, net of estimated forfeitures, which is expected to be recognized over the weighted-average remaining requisite period of 1.02 years.

In connection with the acquisition of Dell by Dell Technologies in 2013, the Company's compensation programs included grants under the Dell Technologies Inc. 2013 Stock Incentive Plan (the "2013 Plan"). Under the 2013 Plan, time-based and performance-based options to purchase shares of the Series C common stock of Dell Technologies were awarded to two of the Company's executive officers. Upon the closing of the Company's IPO, all unvested time-based awards were forfeited and 32,000 vested time-based stock options remained outstanding and 400,001 performance-based options remained unvested and outstanding subject to award terms. During the fiscal year ended February 1, 2019, the 400,001 performance-based options vested with a total fair value of $2.4 million. During the fiscal year ended January 31, 2020, 90,000 options were exercised with a pre-tax intrinsic value of $3.8 million. Cash proceeds received by Dell Technologies from the exercise of these stock options were $1.3 million and the tax benefit realized was $0.9 million for the fiscal year ended January 31, 2020. As of January 31, 2020, 32,000 time-based and 310,001 performance-based stock options remained outstanding. Given that all outstanding options vested in fiscal 2019, the Company recognized no related compensation expense for the fiscal year ended January 31, 2020, while $0.5 million and $0.3 million was recognized for the fiscal years ended February 1, 2019 and February 2, 2018, respectively.

Restricted Stock and Restricted Stock Units

Under the 2016 Plan, a restricted stock award ("RSA") is an award of shares of Class A common stock that may be subject to restrictions on transferability and other restrictions as the compensation committee determines in its sole discretion on the date of grant. The restrictions, if any, may lapse over a specified period of time or through the satisfaction of conditions, in installments or otherwise as the Company's compensation committee may determine. Unless otherwise provided in an award agreement, a grantee who receives restricted stock will have all of the rights of a stockholder as to those shares, including, without limitation, the right to vote and the right to receive dividends or distributions on the shares of Class A common stock, except that the compensation committee may require any dividends to be withheld and accumulated contingent on vesting of the underlying shares or reinvested in shares of restricted stock.

Under the 2016 Plan, a restricted stock unit ("RSU") represents the grantee’s right to receive a compensation amount, based on the value of the shares of Class A common stock, if vesting criteria or other terms and conditions established by the compensation committee are met. If the vesting criteria or other terms and conditions are met, the Company may settle, subject to the terms and conditions of the applicable award agreement, restricted stock units in cash, shares of Class A common stock or a combination of the two. All award agreements currently outstanding require settlement in shares of Class A common stock.

In connection with the IPO, the Company granted RSAs and RSUs to employees and directors. The fair value of the RSAs and RSUs was $14.00 per share and all will vest over an average service period of four years. During the fiscal years ended January 31, 2020, February 1, 2019 and February 2, 2018 the Company issued additional restricted stock and restricted stock units to employees at weighted-average fair values per share of $16.93, $9.78 and $10.40, respectively. The Company's annual grant of RSAs and RSUs issued during the fiscal years ended January 31, 2020, February 1, 2019 and February 2, 2018 vests ratably over three years and approximately 50% of such awards are subject to performance conditions. Of the 3.1 million RSAs and RSUs outstanding on January 31, 2020, approximately 1.0 million were performance-based awards and 2.1 million were service-based awards. During the fiscal year ended January 31, 2020, the Company's compensation committee approved an accounting modification to allow 100% payout upon vesting of performance-based awards tied to fiscal year 2020 results. This modification resulted in total incremental expense to be recognized over the remaining service period of approximately $2.6 million, of which $0.4 million was recognized during the fiscal year ended January 31, 2020.

The Company recognized compensation expense related to RSAs and RSUs of $16.8 million, $15.2 million and $9.8 million for the fiscal years ended January 31, 2020, February 1, 2019 and February 2, 2018, respectively. At January 31, 2020, unrecognized stock-based compensation expense related to restricted stock awards and restricted stock units was $25.0 million, which is expected to be recognized over the weighted-average remaining requisite period of 2.22 years.

The following table summarizes activity for restricted stock and restricted stock units for the fiscal years ended, and as of, January 31, 2020, February 1, 2019 and February 2, 2018.

	Number of Shares	Weighted-Average Grant Date Fair Value Per Share	Weighted-Average Contractual Life (years)	Aggregate Intrinsic Value[1]
				(in thousands)
Balance, February 3, 2017	2,242,486	$ 13.21		
Granted	1,134,966	10.40		
Vested	(507,196)	13.62		
Forfeited	(550,697)	11.46		
Balance, February 2, 2018	2,319,559	$ 12.16		
Granted	2,274,508	9.78		
Vested	(793,723)	11.99		
Forfeited	(453,866)	10.69		
Balance, February 1, 2019	3,346,478	$ 10.84		
Granted	2,087,872	16.93		
Vested	(1,282,743)	11.10		
Forfeited	(1,088,990)	12.44		
Balance, January 31, 2020	3,062,617	$ 14.32	1.25	$ 48,175
Restricted stock and restricted stock units expected to vest, January 31, 2020	2,909,217	$ 14.27	1.31	$ 45,762

(1) The aggregate intrinsic values represent the total pre-tax intrinsic values based on the Company's closing share price of $15.73 as reported on the Nasdaq Global Select Market on January 31, 2020, that would have been received by the restricted stock and restricted stock unit holders had all restricted stock and restricted stock units been issued as of that date.

As of January 31, 2020, restricted stock and restricted stock units representing 3.1 million shares of Class A common stock were outstanding, with an aggregate intrinsic value of $48.2 million based on the Company's closing stock price as reported on the Nasdaq Global Select Market on January 31, 2020. The total fair value of Secureworks' restricted stock and restricted stock units that vested during the fiscal years ended January 31, 2020, February 1, 2019 and February 2, 2018 was $14.2 million, $9.4 million and $6.9 million, respectively, and the pre-tax intrinsic value was $25.3 million, $8.5 million and $4.6 million respectively.

Stock-based Compensation Expense

The following table summarizes the classification of stock-based compensation expense related to stock options, restricted stock and restricted stock units for the fiscal years ended January 31, 2020, February 1, 2019 and February 2, 2018.

	Fiscal Year Ended		
	January 31, 2020	February 1, 2019	February 2, 2018
		(in thousands)	
Cost of revenue	$ 1,206	$ 780	$ 891
Research and development	4,280	4,133	3,261
Sales and marketing	1,694	2,652	735
General and administrative	12,368	11,805	8,903
Total stock-based compensation expense	$ 19,548	$ 19,370	$ 13,790

The tax benefit related to stock-based compensation expense was $4.6 million, $4.7 million and $3.3 million for the fiscal years ended January 31, 2020, February 1, 2019 and February 2, 2018 respectively.

Long-term Performance Cash Awards

In March 2017, the Company began granting long-term performance cash awards to certain employees. The employees who receive the performance cash awards do not receive equity awards as part of the long-term incentive program. The long-term performance cash awards are subject to various performance conditions and vest in equal annual installments over a three-year period. For the fiscal years ended January 31, 2020 and February 1, 2019, the Company granted approximately $6.9 million and $15.7 million of these awards, respectively, and recognized $7.3 million and $6.6 million of related compensation expense, respectively.

Employee Benefit Plan

Substantially all employees are eligible to participate in a defined contribution plan that complies with Section 401(k) of the Internal Revenue Code ("401(k) Plan"). The Company matches 100% of each participant's voluntary contributions, subject to a maximum contribution of 6% of the participant's compensation, and participants vest immediately in all contributions to the 401(k) Plan. For the fiscal years ended January 31, 2020, February 1, 2019 and February 2, 2018, total expense under this plan was $10.8 million, $10.2 million and $10.7 million, respectively.

NOTE 11 — INCOME AND OTHER TAXES

The Company's effective income tax rate for the fiscal years ended January 31, 2020, February 1, 2019 and February 2, 2018 was as follows:

	Fiscal Year Ended		
	January 31, 2020	February 1, 2019	February 2, 2018
Loss before income taxes	$ (51,324)	$ (45,954)	$ (72,716)
Income tax benefit	$ (19,658)	$ (6,853)	$ (62,299)
Effective tax rate	38.3%	14.9%	85.7%

During the periods presented in the accompanying Consolidated Financial Statements, the Company did not file separate federal tax returns, as the Company generally was included in the tax grouping of other Dell entities within the respective entity's tax jurisdiction. The income tax benefit has been calculated using the separate return method modified to apply the benefits-for-loss approach. Under the benefits-for-loss approach, net operating losses or other tax attributes are characterized as realized by the Company when those attributes are utilized by other members of the Dell consolidated group.

The change in the Company's effective income tax rate for the fiscal years ended January 31, 2020 and February 1, 2019 was primarily attributable to the impact of certain discrete adjustments related to stock-based compensation expense and the recognition of additional benefits relating to the research and development credits. The change in the Company's effective income tax rate for the fiscal years ended February 1, 2019 and February 2, 2018 was primarily driven by the decrease in the U.S. corporate income tax rate from 35% to 21% and the impact of the minimum tax on foreign earnings from the enactment of the U.S. Tax Cuts and Jobs Act ("U.S. Tax Reform" or the "Act") that was enacted in December 2017.

Throughout the fiscal year ended January 31, 2020, the U.S. Department of the Treasury and Internal Revenue Service issued preliminary and final regulatory guidance clarifying certain provisions of U.S. Tax Reform, and the Company anticipates additional regulatory guidance and technical clarifications to be issued. When additional guidance and technical clarifications are issued, the Company will recognize the related tax impact in the quarter in which such guidance is issued. The GILTI provisions of the Act signed into law on December 22, 2017 require the Company to include in its U.S. income tax return foreign subsidiary earnings in excess of an allowable return on the foreign subsidiary's tangible assets. The Company has elected to account for GILTI as a current period cost included in the year incurred.

A reconciliation of the Company's benefit from income taxes to the statutory U.S. federal tax rate is as follows:

	Fiscal Year Ended		
	January 31, 2020	February 1, 2019	February 2, 2018
U.S. federal statutory rate	21.0%	21.0%	33.7%
Impact of foreign operations	0.5	0.2	0.5
State income taxes, net of federal tax benefit	3.2	3.2	2.6
Research and development credits	6.5	4.4	2.1
Nondeductible/nontaxable items	(0.6)	(4.0)	(2.1)
U.S. Tax Reform	2.3	(9.4)	49.5
Stock-based compensation	5.4	(0.5)	(0.6)
Total	38.3%	14.9%	85.7%

The benefit for income taxes consists of the following:

	Fiscal Year Ended		
	January 31, 2020	February 1, 2019	February 2, 2018
		(in thousands)	
Current:			
Federal	$ (8,135)	$ (527)	$ (20,288)
State/Local	(895)	(421)	(886)
Foreign	1,918	1,274	80
Current	(7,112)	326	(21,094)
Deferred:			
Federal	(10,367)	(5,930)	(41,825)
State/Local	(931)	(1,132)	(444)
Foreign	(1,248)	(117)	1,064
Deferred	(12,546)	(7,179)	(41,205)
Income tax benefit	$ (19,658)	$ (6,853)	$ (62,299)

Loss before provision for income taxes consists of the following:

	Fiscal Year Ended		
	January 31, 2020	February 1, 2019	February 2, 2018
		(in thousands)	
Domestic	$ (55,800)	$ (47,523)	$ (77,390)
Foreign	4,476	1,569	4,674
Loss before income taxes	$ (51,324)	$ (45,954)	$ (72,716)

The components of the Company's net deferred tax balances are as follows:

	January 31, 2020	February 1, 2019
	(in thousands)	
Deferred tax assets:		
Deferred revenue	$ 2,743	$ 2,163
Provision for doubtful accounts	1,056	1,245
Credit carryforwards	5,796	—
Loss carryforwards	6,673	7,531
Stock-based and deferred compensation	9,249	8,468
Lease right-of-use asset	5,829	—
Other	2,135	2,948
Deferred tax assets	33,481	22,355
Valuation allowance	(4,613)	(4,742)
Deferred tax assets, net of valuation allowance	28,868	17,613
Deferred tax liabilities:		
Property and equipment	(3,733)	(1,842)
Purchased intangible assets	(44,444)	(50,509)
Operating and compensation related accruals	(16,723)	(18,614)
Lease liability	(4,589)	—
Other	(1,067)	(347)
Deferred tax liabilities	(70,556)	(71,312)
Net deferred tax liabilities	$ (41,688)	$ (53,699)

Net deferred tax balances are included in other non-current assets and other non-current liabilities in the Consolidated Statements of Financial Position.

As of January 31, 2020 and February 1, 2019, the Company had $4.6 million and $4.7 million, respectively, of deferred tax assets related to net operating loss carryforwards for state tax returns that are not included with those of other Dell entities. These net operating loss carryforwards began expiring in the fiscal year ended January 31, 2020. Due to the uncertainty surrounding the realization of these net operating loss carryforwards, the Company has provided valuation allowances for the full amount as of January 31, 2020 and February 1, 2019. Because the Company is included in the tax filings of certain other Dell entities, management has determined that it will be able to realize the remainder of its deferred tax assets. If the Company’s tax provision had been prepared using the separate return method, the unaudited pro forma pre-tax loss, tax benefit and net loss for the fiscal year ended January 31, 2020 would have been $51.3 million, $6.0 million and $45.3 million, respectively, as a result of the recognition of a valuation allowance that would have been recorded on certain deferred tax assets, as well as certain attributes from the Tax Cuts and Jobs Act of 2017 that would be lost if not utilized by the Dell consolidated group.

As of January 31, 2020, the Company has cumulative undistributed foreign earnings that would incur some amount of local withholding and state taxes if the earnings are distributed to SecureWorks Corp., which is domiciled in the United States. U.S. Tax Reform fundamentally changes the U.S. approach to taxation of foreign earnings. The Company has analyzed its global working capital and cash requirements and the potential tax liabilities attributable to repatriation, and has determined that it may be repatriating certain unremitted foreign earnings that were previously deemed indefinitely reinvested. As of January 31, 2020 and February 1, 2019, the Company has recorded withholding taxes of $0.3 million and $0.3 million, respectively, related to certain unremitted foreign earnings that may be repatriated.

A reconciliation of the Company's beginning and ending amount of unrecognized tax benefits is as follows:

	Fiscal Year Ended		
	January 31, 2020	February 1, 2019	February 2, 2018
		(in thousands)	
Beginning unrecognized tax benefits	$ 7,285	$ 763	$ 579
Increases related to tax positions of the current year	27	1,204	285
Increases related to tax position of prior years	13	5,589	—
Reductions for tax positions of prior years	(1,191)	(271)	(101)
Ending unrecognized tax benefits	$ 6,134	$ 7,285	$ 763

The Company's net unrecognized tax benefits of $6.6 million, $7.5 million and $0.8 million include amounts reflected in the table above, plus accrued interest and penalties of $0.5 million, $0.3 million and $0.0 million as of January 31, 2020, February 1, 2019 and February 2, 2018, respectively, and are included in other non-current liabilities in the Consolidated Statements of Financial Position. The net unrecognized tax benefits, if recognized, would increase the Company's income tax benefit and effective income tax benefit rate. Interest and penalties related to income tax liabilities are included in income tax expense. The Company recorded interest and penalties of $0.2 million, $0.2 million and $0.0 million for the fiscal years ended January 31, 2020, February 1, 2019 and February 2, 2018, respectively.

Judgment is required in evaluating the Company's uncertain tax positions and determining the Company's provision for income taxes. The Company does not anticipate a significant change to the total amount of unrecognized tax benefits within the next twelve months.

The Company is also currently under income tax audit in foreign jurisdictions. The Company is undergoing negotiations, and in some cases contested proceedings, relating to tax matters with the taxing authorities in these jurisdictions. The Company believes that it has provided adequate reserves related to all matters contained in tax periods open to examination. Although the Company believes it has made adequate provisions for the uncertainties surrounding these audits, should the Company experience unfavorable outcomes, such outcomes could have a material impact on its results of operations, financial position and cash flows.

The Company takes certain non-income tax positions in the jurisdictions in which it operates and has received certain non-income tax assessments from various jurisdictions. The Company believes that a material loss in these matters is not probable and that it is not reasonably possible that a material loss exceeding amounts already accrued has been incurred. The Company believes its positions in these non-income tax litigation matters are supportable and that it ultimately will prevail. In the normal course of business, the Company's positions and conclusions related to its non-income taxes could be challenged and assessments may be made. To the extent new information is obtained and the Company's views on its positions, probable outcomes of assessments, or litigation change, changes in estimates to the Company's accrued liabilities would be recorded in the period in which such a determination is made. In the resolution process for income tax and non-income tax audits, the Company may be required to provide collateral guarantees or indemnification to regulators and tax authorities until the matter is resolved.

The Company is no longer subject to tax examinations for years prior to fiscal 2013.

NOTE 12 — SELECTED FINANCIAL INFORMATION

The following table provides information on amounts included in accounts receivable, net, other current assets, property and equipment, net, accrued and other current liabilities, and other non-current liabilities as of January 31, 2020 and February 1, 2019.

	Consolidated	
	January 31, 2020	February 1, 2019
	(in thousands)	
Accounts receivable, net:		
Gross accounts receivable	$ 116,919	$ 147,504
Allowance for doubtful accounts	(5,121)	(6,160)
Total	$ 111,798	$ 141,344
Other current assets:		
Income tax receivable	10,040	6,853
Prepaid maintenance and support agreements	8,425	10,602
Prepaid other	8,984	10,149
Total	$ 27,449	$ 27,604
Property and equipment, net		
Computer equipment	$ 53,012	$ 67,468
Leasehold improvements	25,087	26,151
Other equipment	2,956	2,978
Total property and equipment	81,055	96,597
Accumulated depreciation and amortization	$ (53,449)	$ (60,619)
Total	$ 27,606	$ 35,978
Other noncurrent assets		
Prepaid maintenance agreements	1,260	1,351
Deferred tax asset	1,633	648
Deferred commission and fulfillment costs	74,151	73,868
Other	1,548	2,371
Total	$ 78,592	$ 78,238
Accrued and other current liabilities		
Compensation	$ 52,450	$ 48,242
Related party payable, net	3,209	15,634
Other	43,196	22,619
Total	$ 98,855	$ 86,495
Other non-current liabilities		
Deferred tax liabilities	$ 43,321	$ 54,347
Other	7,079	12,504
Total	$ 50,400	$ 66,851

The allocation between domestic and foreign net revenue is based on the location of the Company's customers. Net revenue from any single foreign country did not constitute 10% or more of the Company's net revenue during any of the periods presented. As of January 31, 2020 and February 1, 2019, net property and equipment in Romania represented 14% and 13%, respectively, of the Company's consolidated net property and equipment.

The following tables present net revenue and property, plant and equipment allocated between the United States and international locations. The Company defines international revenue as revenue contracted through non-U.S. entities.

	Fiscal Year Ended		
	January 31, 2020	February 1, 2019	February 2, 2018
Net revenue			
United States	$ 412,511	$ 403,614	$ 391,159
International	140,254	115,095	76,771
Total	$ 552,765	$ 518,709	$ 467,930

	January 31, 2020	February 1, 2019
Property and equipment, net		
United States	$ 22,772	$ 29,684
International	4,834	6,294
Total	$ 27,606	$ 35,978

NOTE 13 — RELATED PARTY TRANSACTIONS

Allocated Expenses

For the periods presented, Dell has provided various corporate services to Secureworks in the ordinary course of business. The costs of services provided to Secureworks by Dell are governed by a shared services agreement between Secureworks and Dell Inc. The total amounts of the charges under the shared services agreement with Dell were $9.1 million, $3.7 million and $4.9 million for the fiscal years ended January 31, 2020, February 1, 2019 and February 2, 2018, respectively. Management believes that the basis on which the expenses have been allocated is a reasonable reflection of the utilization of services provided to or the benefit received by the Company during the periods presented.

Related Party Arrangements

For the periods presented, related party transactions and activities involving Dell Inc. and its wholly-owned subsidiaries were not always consummated on terms equivalent to those that would prevail in an arm’s-length transaction where conditions of competitive, free-market dealing may exist.

The Company purchases computer equipment for internal use from Dell and its subsidiaries that is capitalized within property and equipment in the Consolidated Statements of Financial Position. These purchases were made at pricing that is intended to approximate arm's-length pricing. Purchases of computer equipment from Dell and EMC Corporation, a wholly-owned subsidiary of Dell that provides enterprise software and storage ("EMC"), totaled $3.1 million, $2.7 million and $2.6 million for the fiscal years ended January 31, 2020, February 1, 2019 and February 2, 2018, respectively.

EMC maintains a majority ownership interest in a subsidiary, VMware, Inc. (“VMware”), that provides cloud and virtualization software and services. The Company's purchases of annual maintenance services, software licenses and hardware systems for internal use from Dell, EMC and VMware totaled $3.4 million, $1.2 million and $1.3 million for the fiscal years ended January 31, 2020, February 1, 2019 and February 2, 2018, respectively. Additionally, during the fiscal year ended January 31, 2020, VMware acquired Carbon Black Inc., a security business with which the Company had an existing commercial relationship. From the date of the acquisition through the end of fiscal 2020, purchases of solutions by the Company from Carbon Black totaled $2.2 million and, as of January 31, 2020, the Company had liabilities to Carbon Black totaling $0.3 million.

The Company recognized revenue related to security solutions provided to other subsidiaries of Dell Technologies, consisting of RSA Security LLC, Pivotal Software, Inc. and Boomi, Inc. The revenue recognized by the Company for security solutions provided to these entities totaled $0.1 million, $0.3 million and $0.2 million for the fiscal years ended January 31, 2020, February 1, 2019 and February 2, 2018, respectively. Purchases by the Company from these other subsidiaries totaled $0.1 million, $0.7 million and $0.1 million during the fiscal years ended January 31, 2020, February 1, 2019 and February 2, 2018, respectively.

The Company also recognized revenue related to solutions provided to significant beneficial owners of Secureworks common stock, which include Michael S. Dell, Chairman and Chief Executive Officer of Dell Technologies, and affiliates of Mr. Dell. The revenues recognized by the Company from solutions provided to Mr. Dell, MSD Capital, L.P. (a firm founded for the purposes of managing investments of Mr. Dell and his family), DFI Resources LLC, an entity affiliated with Mr. Dell, and the Michael and Susan Dell Foundation totaled $0.4 million, $0.5 million and $0.4 million for the fiscal years ended January 31, 2020, February 1, 2019 and February 2, 2018, respectively.

The Company provides solutions to certain customers whose legal contractual relationship has historically been with Dell rather than Secureworks, although the Company has the primary responsibility to provide the services. Effective on August 1, 2015, upon the creation of new subsidiaries to segregate some of the Company's operations from Dell's operations, as described in "Note 1—Description of the Business and Basis of Presentation," many of such customer contracts were transferred from Dell to the Company, forming a direct legal contractual relationship between the Company and the end customer. For customers whose contracts have not yet been transferred or whose contracts were subsequently originated through Dell under a reseller agreement, the Company recognized revenues of approximately $57.8 million, $59.0 million and $44.7 million for the fiscal years ended January 31, 2020, February 1, 2019 and February 2, 2018, respectively. In addition, as of January 31, 2020, the Company had approximately $1.8 million of contingent obligations to Dell related to outstanding performance bonds for certain customer contracts, which Dell issued on behalf of the Company.

As the Company's customer and on behalf of certain of its own customers, Dell also purchases solutions from the Company. Beginning in the third quarter of the fiscal year ended January 29, 2016, in connection with the effective date of the Company's commercial agreements with Dell, the Company began charging Dell for these services at pricing that is intended to approximate arm's-length pricing, in lieu of the prior cost recovery arrangement. Such revenues totaled approximately $27.2 million, $16.6 million, and $21.1 million for the fiscal years ended January 31, 2020, February 1, 2019, and February 2, 2018, respectively.

As a result of the foregoing related party arrangements beginning in the third quarter of the fiscal year ended January 29, 2016, the Company has recorded the following related party balances in the Consolidated Statement of Financial Position as of January 31, 2020 and February 1, 2019:

	January 31, 2020	February 1, 2019
	(in thousands)	
Related party payable (in accrued and other current liabilities)	$ 3,209	$ 15,634
Accounts receivable from customers under reseller agreements with Dell (in accounts receivable, net)	$ 13,674	$ 21,760
Net operating loss tax sharing receivable under agreement with Dell (in other current assets)	$ 10,040	$ 6,853

NOTE 14 — UNAUDITED QUARTERLY RESULTS OF OPERATIONS

The following table presents selected unaudited Statements of Operations for each quarter of fiscal 2020 and fiscal 2019. The statement have been prepared on a basis consistent with our audited annual financial statements included in this Annual Report on Form 10-K and include, in the Company's opinion, all normal recurring adjustments necessary for the fair presentation of the financial information contained in those statements. The following quarterly financial data should be read in conjunction with the audited financial statements and the related notes included in this Annual Report on Form 10-K.

	Fiscal Year 2020			
	First Quarter	Second Quarter	Third Quarter	Fourth Quarter
Net revenue	$ 132,842	$ 136,605	$ 141,332	$ 141,986
Gross margin	$ 70,001	$ 73,010	$ 79,764	$ 77,194
Net loss	$ (8,270)	$ (10,260)	$ (7,908)	$ (5,228)
Net loss per common share (basic and diluted) [1]	$ (0.10)	$ (0.13)	$ (0.10)	$ (0.06)
Weighted-average common shares outstanding (basic and diluted)	80,467	80,674	80,518	80,591

[1] Basic and diluted net loss per common share are computed independently for each of the quarters presented. Therefore, the sum of the quarterly basic and diluted net loss per common share amounts may not equal the annual basic and diluted net loss per common share amounts.

	Fiscal Year 2019			
	First Quarter	Second Quarter	Third Quarter	Fourth Quarter
Net revenue	$ 126,161	$ 128,778	$ 133,060	$ 130,710
Gross margin	$ 65,631	$ 66,230	$ 70,927	$ 69,804
Net (loss) income	$ (13,819)	$ (9,769)	$ (3,735)	$ (11,778)
Net (loss) income per common share (basic and diluted) [1]	$ (0.17)	$ (0.12)	$ (0.05)	$ (0.15)
Weighted-average common shares outstanding (basic and diluted)	80,522	80,839	80,892	80,587

[1] Basic and diluted net loss per common share are computed independently for each of the quarters presented. Therefore, the sum of the quarterly basic and diluted net loss per common share amounts may not equal the annual basic and diluted net loss per common share amounts.

NOTE 15 — SUBSEQUENT EVENTS

On March 11, 2020, the World Health Organization declared the novel strain of coronavirus (COVID-19) a global pandemic and recommended containment and mitigation measures worldwide. At this point, the Company cannot reasonably estimate the length or severity of this pandemic, or the extent to which the disruption may impact the Company’s consolidated financial position, consolidated results of operations, and consolidated cash flows in fiscal 2021. Due to the Company’s subscription-based business model, the effect of COVID-19 may not be fully reflected in the Company’s results of operations until future periods, if at all.

Effective as of March 26, 2019, SecureWorks, Inc., the Company's wholly-owned subsidiary, extended a revolving credit agreement with a wholly-owned subsidiary of Dell Inc. under which the Company has a $30 million senior unsecured revolving credit facility. This facility was scheduled to expire on March 26, 2020. Subsequent to the end of fiscal 2020, the revolving credit agreement was further amended and restated, effective as of March 26, 2020, to extend the maturity date to March 26, 2021 and to decrease the annual rate at which interest accrues from the applicable London interbank offered rate plus 1.50% to such rate plus 1.30%. The amended and restated revolving credit agreement otherwise has terms substantially similar to those of the facility before the amendment and restatement.

SCHEDULE II - VALUATION AND QUALIFYING ACCOUNTS

Valuation and Qualifying Accounts

Fiscal Year	Description	Balance at Beginning of Period	Charged to Income Statement	Charged to Allowance	Balance at End of Period
Trade Receivables:					
2020	Allowance for doubtful accounts	$ 6,160	$ 3,099	$ (4,138)	$ 5,121
2019	Allowance for doubtful accounts	$ 8,246	$ 2,356	$ (4,442)	$ 6,160
2018	Allowance for doubtful accounts	$ 6,132	$ 3,947	$ (1,833)	$ 8,246

Item 9. Changes in and Disagreements With Accountants on Accounting and Financial Disclosure

None

Item 9A. Controls and Procedures

Evaluation of Disclosure Controls and Procedures

Disclosure controls and procedures (as defined in Rules 13a-15(e) and 15d-15(e) under the Exchange Act) are designed to ensure that information required to be disclosed in reports filed or submitted under the Exchange Act is recorded, processed, summarized and reported within the time periods specified in SEC rules and forms and that such information is accumulated and communicated to management, including the chief executive officer and the chief financial officer, to allow timely decisions regarding required disclosures.

In connection with the preparation of this report, our management, under the supervision and with the participation of our Chief Executive Officer and Chief Financial Officer, conducted an evaluation of the effectiveness of the design and operation of our disclosure controls and procedures as of January 31, 2020. Based on that evaluation, our management has concluded that our disclosure controls and procedures were effective as of January 31, 2020.

Management's Report on Internal Control Over Financial Reporting

Management, under the supervision of the Chief Executive Officer and the Chief Financial Officer, is responsible for establishing and maintaining adequate internal control over financial reporting. Internal control over financial reporting (as defined in Rules 13a-15(f) and 15d(f) under the Exchange Act) is a process designed to provide reasonable assurance regarding the reliability of financial reporting and the preparation of financial statements for external purposes in accordance with generally accepted accounting principles. Internal control over financial reporting includes those policies and procedures which (a) pertain to the maintenance of records that, in reasonable detail, accurately and fairly reflect the transactions and dispositions of assets, (b) provide reasonable assurance that transactions are recorded as necessary to permit preparation of financial statements in accordance with generally accepted accounting principles, (c) provide reasonable assurance that receipts and expenditures are being made only in accordance with appropriate authorization of management and the board of directors, and (d) provide reasonable assurance regarding prevention or timely detection of unauthorized acquisition, use, or disposition of assets that could have a material effect on the financial statements.

In connection with the preparation of this report, our management, under the supervision and with the participation of our Chief Executive Officer and Chief Financial Officer, conducted an evaluation of the effectiveness of our internal control over financial reporting as of January 31, 2020, based on the criteria established in *Internal Control — Integrated Framework (2013)* issued by the Committee of Sponsoring Organizations of the Treadway Commission. As a result of that evaluation, management has concluded that our internal control over financial reporting was effective as of January 31, 2020.

Changes in Internal Control Over Financial Reporting

There were no changes in our internal control over financial reporting identified in connection with the evaluation required by Rules 13a 15(e) and 15d 15(e) under the Exchange Act that occurred during the quarter ended January 31, 2020 that have materially affected, or are reasonably likely to materially affect, our internal control over financial reporting.

Item 9B. Other Information

Effective as of March 26, 2019, SecureWorks, Inc., our wholly-owned subsidiary, extended a revolving credit agreement with a wholly-owned subsidiary of Dell Inc. under which we have a $30 million senior unsecured revolving credit facility. This facility was set to expire on March 26, 2020. Subsequent to the end of fiscal 2020, the revolving credit agreement was further amended and restated, effective as of March 26, 2020, to extend the maturity date to March 26, 2021 and to decrease the annual rate at which interest accrues from the applicable London interbank offered rate plus 1.50% to such rate plus 1.30%. The amended and restated revolving credit agreement otherwise has terms substantially similar to those of the facility before the amendment and restatement. The credit facility and the recent amendment and restatement to the credit facility to extend the term are described under “Notes to Consolidated Financial Statements—Note 6—Debt” and “—Note 15—Subsequent Events” in our consolidated financial statements included in this annual report on Form 10-K.

Part III

Item 10. Directors, Executive Officers and Corporate Governance

We have adopted a code of ethics applicable to our principal executive officer and other senior financial officers. The code of ethics, which we refer to as our Code of Ethics for Senior Financial Officers, is available on the Investors page of our website at www.secureworks.com. To the extent required by SEC rules, we intend to disclose any amendments to this code and any waiver of a provision of the code for the benefit of any senior financial officer on our website within any period that may be required under SEC rules from time to time.

See "Part I — Item 1 — Business — Information about our Executive Officers" for information about our executive officers, which is incorporated by reference in this Item 10. Other information required by this Item 10 is incorporated herein by reference to our definitive proxy statement for our 2020 annual meeting of stockholders, referred to as the "2020 proxy statement," which we will file with the SEC on or before 120 days after our 2020 fiscal year end, and which will appear in the 2020 proxy statement under the captions "Proposal 1 — Election of Directors" and "Additional Information — Delinquent Section 16(a) Reports."

The following lists the members of our board of directors and the principal occupation of each director as of the date of this report.

Michael R. Cote
President and Chief Executive Officer
SecureWorks Corp.

Michael S. Dell
Chairman and Chief Executive Officer
Dell Technologies Inc.

Egon Durban
Managing Partner
Silver Lake Partners
(private equity)

Pamela Daley
Retired Senior Vice President and
Senior Advisor to the Chairman
of General Electric Company

Mark J. Hawkins
President and Chief Financial Officer
Salesforce.com, Inc.
(software)

Yagyensh C. (Buno) Pati
Partner
Centerview Capital Technology
(investments)

Item 11. Executive Compensation

Information required by this Item 11 is incorporated herein by reference to the 2020 proxy statement, including the information in the 2020 proxy statement appearing under the captions "Proposal 1 — Election of Directors — Director Compensation" and "Compensation of Executive Officers."

Item 12. Security Ownership of Certain Beneficial Owners and Management and Related Stockholder Matters

Information required by this Item 12 is incorporated herein by reference to the 2020 proxy statement, including the information in the 2020 proxy statement appearing under the captions "Equity Compensation Plan Information" and "Security Ownership of Certain Beneficial Owners and Management."

Item 13. Certain Relationships and Related Transactions, and Director Independence

Information required by this Item 13 is incorporated herein by reference to the 2020 proxy statement, including the information in the 2020 proxy statement appearing under the captions "Proposal 1—Election of Directors" and "Additional Information—Certain Relationships and Related Transactions."

Item 14. Principal Accounting Fees and Services

Information required by this Item 14 is incorporated herein by reference to the 2020 proxy statement, including the information in the 2020 proxy statement appearing under the caption "Proposal 2 — Ratification of Appointment of Independent Registered Public Accounting Firm."

Part IV

Item 15. Exhibits, Financial Schedules

The following documents are filed as a part of this annual report on Form 10-K:

(1) *Financial Statements*: The following financial statements are filed as a part of this report under "Part II — Item 8 Financial Statements and Supplementary Data":

Report of Independent Registered Public Accounting Firm
Consolidated Statements of Financial Position as of January 31, 2020 and February 1, 2019
Consolidated Statements of Operations for the fiscal years ended January 31, 2020, February 1, 2019 and February 2, 2018
Consolidated Statements of Comprehensive Loss for the fiscal years ended January 31, 2020, February 1, 2019 and February 2, 2018
Consolidated Statements of Cash Flows for the fiscal years ended January 31, 2020, February 1, 2019 and February 2, 2018
Consolidated Statements of Stockholder's Equity for the fiscal years ended January 31, 2020, February 1, 2019 and February 2, 2018
Notes to Consolidated Financial Statements
Schedule II - Valuation and Qualifying Accounts

(2) *Financial Statement Schedules*: The following financial statement schedule is included following the Notes to the Consolidated Financial Statements under "Part II — Item 8 — Financial Statements and Supplementary Data":

Schedule II — Valuation and Qualifying Accounts

(3) *Exhibits*:

EXHIBIT INDEX

Exhibit No.	Description
3.1	Restated Certificate of Incorporation of SecureWorks Corp. (the "Company") (incorporated by reference to Exhibit 4.1 to the Company's Registration Statement on Form S-8 filed with the Securities and Exchange Commission (the "Commission") on April 22, 2016 (the "Form S-8")) (Registration No. 333-210866).
3.2	Amended and Restated Bylaws of SecureWorks Corp. (incorporated by reference to Exhibit 4.2 to the Form S-8) (Registration No. 333-210866).
4.1	Specimen Certificate of Class A Common Stock, $0.01 par value per share, of the Company (incorporated by reference to Exhibit 4.1 to the Company's Registration Statement on Form S-1 filed with the Commission on December 17, 2015 (the "Form S-1")) (Registration No. 333-208596).
4.2††	Description of the Company's Securities Registered Pursuant to Section 12 of the Securities Exchange Act of 1934.
10.1	Shared Services Agreement, effective as of August 1, 2015, between Dell Inc., for itself and its subsidiaries, and the Company (formerly known as SecureWorks Holding Corporation), for itself and its subsidiaries (incorporated by reference to Exhibit 10.1 to the Form S-1) (Registration No. 333-208596).
10.1.1	Amendment #1 to Shared Services Agreement, dated December 8, 2015, between Dell Inc., for itself and its subsidiaries, and the Company, for itself and its subsidiaries (incorporated by reference to Exhibit 10.1.1 to the Form S-1) (Registration No. 333-208596).
10.1.2	Amendment #2 to Shared Services Agreement, dated November 8, 2017, between Dell Inc., for itself and its subsidiaries, and the Company, for itself and its subsidiaries (incorporated by reference to Exhibit 10.1.2 to the Company's Annual Report on Form 10-K for the fiscal year ended February 2, 2018) (Commission File No. 001-37748).
10.1.3	Amendment #3 to Shared Services Agreement, dated as of July 11, 2018, between Dell Inc., for itself and its subsidiaries, and the Company, for itself and its subsidiaries (incorporated by reference to Exhibit 10.2 to the Company's Quarterly Report on Form 10-Q for the quarterly period ended August 3, 2018) (Commission File No. 001-37748).
10.1.4	Amendment #4 to Shared Services Agreement, dated as of May 29, 2019, between Dell Inc., for itself and its subsidiaries, and the Company, for itself and its subsidiaries (incorporated by reference to Exhibit 10.1 to the Company's Quarterly Report on Form 10-Q for the quarterly period ended May 3, 2019) (Commission File No. 001-37748).
10.2	Intellectual Property Contribution Agreement, effective as of August 1, 2015, among Dell Inc., the Company and other subsidiaries of Dell Inc. party thereto (incorporated by reference to Exhibit 10.2 to the Form S-1) (Registration No. 333-208596).
10.3	Patent License Agreement, effective as of August 1, 2015, between Dell Inc., for itself and its subsidiaries, and the Company, for itself and its subsidiaries (incorporated by reference to Exhibit 10.3 to the Form S-1) (Registration No. 333-208596).
10.4	License Agreement, dated as of September 9, 2015, between Dell Inc. and the Company (incorporated by reference to Exhibit 10.4 to the Form S-1) (Registration No. 333-208596).
10.5	Tax Matters Agreement, effective as of August 1, 2015, between the Company, for itself and its subsidiaries, and Dell Technologies Inc. (formerly known as Denali Holding Inc.), for itself and its subsidiaries other than the Company (incorporated by reference to Exhibit 10.5 to the Form S-1) (Registration No. 333-208596).
10.5.1	Amendment #1 to Tax Matters Agreement, dated December 8, 2015, between the Company, for itself and its subsidiaries, and Dell Technologies Inc., for itself and its subsidiaries other than the Company (incorporated by reference to Exhibit 10.5.1 to the Form S-1) (Registration No. 333-208596).
10.6	Amended and Restated Employee Matters Agreement, effective as of August 1, 2015, among Dell Technologies Inc., Dell Inc. and the Company (incorporated by reference to Exhibit 10.6 to the Form S-1) (Registration No. 333-208596).
10.7+	Security Services Customer Master Services Agreement, effective as of August 1, 2015, between SecureWorks, Inc. and Dell USA L.P., on behalf of itself, Dell Inc., and Dell Inc.'s subsidiaries (incorporated by reference to Exhibit 10.7 to the Form S-1) (Registration No. 333-208596).
10.8	Letter Agreement to Security Services Customer Master Services Agreement and Reseller Agreement, effective as of August 1, 2015, between Dell Inc. and SecureWorks, Inc. (incorporated by reference to Exhibit 10.8 to the Form S-1) (Registration No. 333-208596).
10.8.1+	First Amendment to Security Services Customer Master Services Agreement, effective as of November 3, 2017, between Dell USA L.P. and SecureWorks, Inc. (incorporated by reference to Exhibit 10.8.1 to the Company's Annual Report on Form 10-K for the fiscal year ended February 2, 2018) (Commission File No. 001-37748).

EXHIBIT INDEX - Continued

Exhibit No.	Description
10.9+	Amended and Restated Master Commercial Customer Agreement, effective as of August 1, 2015, between Dell Marketing L.P. and SecureWorks, Inc. (incorporated by reference to Exhibit 10.9 to the Form S-1) (Registration No. 333-208596).
10.9.1+	Amendment No. 1 to Amended and Restated Master Commercial Customer Agreement, effective as of August 4, 2018, between Dell Marketing L.P. and SecureWorks, Inc. (incorporated by reference to Exhibit10.9.1 to the Company's Quarterly Report on Form 10-Q for the quarterly period ended November 2, 2018) (Commission File No. 001-37748).
10.9.2	Joinder of EMC Corporation to the Amended and Restated Master Commercial Customer Agreement, dated as of March 8, 2019 (incorporated by reference to Exhibit 10.2 to the Company's Quarterly Report on Form 10-Q for the quarterly period ended May 3, 2019) (Commission File No. 001-37748).
10.10+	Amended and Restated Reseller Agreement, effective as of August 1, 2015, between SecureWorks, Inc., for itself and its subsidiaries, and Dell Inc., for itself and its subsidiaries other than the Company (incorporated by reference to Exhibit 10.10 to the Form S-1) (Registration No. 333-208596).
10.10.1+	Amendment No. 1 to Amended and Restated Reseller Agreement, dated as of January 23, 2019, between Dell, Inc., for itself and its subsidiaries other than SecureWorks, Inc. and SecureWorks, Inc., for itself and its subsidiaries (incorporated by reference to Exhibit 10.10.1 to the Company's Annual Report on Form 10-K for the fiscal year ended February 1, 2019) (Commission File No. 001-37748).
10.10.2+	Addendum No. 1 to Amendment No. 1 to Amended and Restated Reseller Agreement, dated as of May 8, 2019, between Dell, Inc., for itself and its subsidiaries other than SecureWorks, Inc., and SecureWorks, Inc., for itself and its subsidiaries (incorporated by reference to Exhibit 10.5 to the Company's Quarterly Report on Form 10-Q for the quarterly period ended May 3, 2019) (Commission File No. 001-37748).
10.10.3+	Amendment No. 2 to Amended and Restated Reseller Agreement, dated as of May 21, 2019, between Dell Inc., for itself and its subsidiaries other than SecureWorks, Inc., and SecureWorks, Inc., for itself and its subsidiaries (incorporated by reference to Exhibit 10.1 to the Company's Quarterly Report on Form 10-Q for the quarterly period ended August 2, 2019) (Commission File No. 001-37748).
10.10.4+	Amendment No. 3 to Amended and Restated Reseller Agreement, dated as of June 13, 2019, between Dell Inc., for itself and its subsidiaries other than SecureWorks, Inc., and SecureWorks, Inc., for itself and its subsidiaries (incorporated by reference to Exhibit 10.2 to the Company's Quarterly Report on Form 10-Q for the quarterly period ended August 2, 2019) (Commission File No. 001-37748).
10.10.5+	Amendment No. 4 to Amended and Restated Reseller Agreement, dated as of July 30, 2019, between Dell Inc., for itself and its subsidiaries other than SecureWorks, Inc., and SecureWorks, Inc., for itself and its subsidiaries (incorporated by reference to Exhibit 10.3 to the Company's Quarterly Report on Form 10-Q for the quarterly period ended August 2, 2019) (Commission File No. 001-37748).
10.10.6	Amendment No. 5 to Amended and Restated Reseller Agreement, dated as of October 1, 2019, between Dell Inc., for itself and its subsidiaries other than SecureWorks, Inc., and SecureWorks, Inc., for itself and its subsidiaries (incorporated by reference to Exhibit 10.1 to the Company's Quarterly Report on Form 10-Q for the quarterly period ended November 1, 2019) (Commission File No. 001-37748).
10.10.7+	Amendment No. 6 to Amended and Restated Reseller Agreement, dated as of October 23, 2019, between Dell Inc., for itself and its subsidiaries other than SecureWorks, Inc., and SecureWorks, Inc., for itself and its subsidiaries (incorporated by reference to Exhibit 10.2 to the Company's Quarterly Report on Form 10-Q for the quarterly period ended November 1, 2019) (Commission File No. 001-37748).
10.11	Registration Rights Agreement, dated as of August 3, 2015, among the Company and the Holders party thereto (incorporated by reference to Exhibit 10.22 to the Form S-1) (Registration No. 333-208596).
10.12	Registration Rights Agreement, dated as of April 27, 2016, among the Company, Dell Marketing L.P., Michael S. Dell, the Susan Lieberman Dell Separate Property Trust, MSDC Denali Investors, L.P., MSDC Denali EIV, LLC, Silver Lake Partners III, L.P., Silver Lake Technology Investors III, L.P., Silver Lake Partners IV, L.P., Silver Lake Technology Investors IV, L.P. and SLP Denali Co-Invest, L.P. (incorporated by reference to Exhibit 10.1 to the Company's Current Report on Form 8-K filed with the Commission on April 27, 2016) (Commission File No. 001-37748).
10.13	Second Amended and Restated Revolving Credit Agreement, dated as of March 26, 2019, between SecureWorks, Inc. and Dell USA L.P. (incorporated by reference to Exhibit 10.3 to the Company's Quarterly Report on Form 10-Q for the quarterly period ended May 3, 2019) (Commission File No. 001-37748).
10.14	Note Purchase Agreement, dated as of June 30, 2015 and amended on July 31, 2015, among the Company, Dell Technologies Inc. and the Investors party thereto (incorporated by reference to Exhibit 10.21 to the Form S-1) (Registration No. 333-208596).
10.15	Office Lease between Teachers Concourse, LLC and SecureWorks, Inc., dated as of April 20, 2012, as amended (incorporated by reference to Exhibit 10.23 to the Form S-1) (Registration No. 333-208596).

EXHIBIT INDEX - Continued

Exhibit No.	Description
10.16	Unconditional Guaranty of Payment and Performance, entered into on April 20, 2012, by Dell Inc. in favor of Teachers Concourse, LLC (incorporated by reference to Exhibit 10.24 to the Form S-1) (Registration No. 333-208596).
10.17	Sublease Agreement between Dell International Services SRL and SecureWorks Europe SRL, dated as of June 22, 2015, as amended (incorporated by reference to Exhibit 10.26 to the Form S-1) (Registration No. 333-208596).
10.18	Lease Deed between Dell International Services India Private Limited and SecureWorks India Private Limited, dated as of August 8, 2015 (incorporated by reference to Exhibit 10.27 to the Form S-1) (Registration No. 333-208596).
10.19*	Dell Technologies Inc. 2013 Stock Incentive Plan (as amended and restated) (incorporated by reference to Exhibit 10.8 to Dell Technologies Inc.'s Current Report on Form 8-K filed with the Commission on December 28, 2018) (Commission File No. 001-37867).
10.20*	Dell Technologies Inc. 2012 Long-Term Incentive Plan (formerly known as Dell Inc. 2012 Long-Term Incentive Plan) as amended and restated as of October 6, 2017 (incorporated by reference to Exhibit 10.4 to Dell Technologies Inc.'s Quarterly Report on Form 10-Q for the quarterly period ended November 3, 2017) (Commission File No. 001-37867).
10.21*	Form of Indemnification Agreement between the Company and each director and executive officer of the Company (incorporated by reference to Exhibit 10.20 to the Form S-1) (Registration No. 333-208596).
10.22*	SecureWorks Corp. 2016 Long-Term Incentive Plan, as amended and restated as of June 21, 2018 (incorporated by reference to Exhibit 10.1 to the Company's Current Report on Form 8-K filed with the Commission on June 27, 2018) (Commission File No. 001-37748).
10.23*	Form of Nonqualified Stock Option Agreement for Executives under SecureWorks Corp. 2016 Long-Term Incentive Plan (incorporated by reference to Exhibit 10.13 to the Form S-1) (Registration No. 333-208596).
10.24*	Form of Nonqualified Stock Option Agreement for Directors under SecureWorks Corp. 2016 Long-Term Incentive Plan (incorporated by reference to Exhibit 10.13.1 to Amendment No. 1 to the Form S-1 filed with the Commission on March 22, 2016) (Registration No. 333-208596).
10.25*	Form of Restricted Stock Unit Agreement for Executives under SecureWorks Corp. 2016 Long-Term Incentive Plan (incorporated by reference to Exhibit 10.14 to the Form S-1) (Registration No. 333-208596).
10.26*	Form of Restricted Stock Unit Agreement for Directors under SecureWorks Corp. 2016 Long-Term Incentive Plan (incorporated by reference to Exhibit 10.14.1 to Amendment No. 1 to the Form S-1 filed with the Commission on March 22, 2016) (Registration No. 333-208596).
10.27*	Form of Restricted Stock Agreement for Executives under SecureWorks Corp. 2016 Long-Term Incentive Plan (incorporated by reference to Exhibit 10.15 to the Form S-1) (Registration No. 333-208596).
10.28*	SecureWorks Corp. Amended and Restated Severance Pay Plan for Executive Employees (incorporated by reference to Exhibit 10.3 to the Company's Quarterly Report on Form 10-Q for the quarterly period ended November 1, 2019) (Commission File No. 001-37748).
10.29*	SecureWorks Corp. Non-Employee Director Compensation Policy, adopted March 2, 2018 and effective June 21, 2018 (incorporated by reference to Exhibit 10.2 to the Company's Quarterly Report on Form 10-Q for the quarterly period ended May 4, 2018) (Commission File No. 001-37748).
10.30*	SecureWorks Corp. Form of Protection of Sensitive Information, Noncompetition and Nonsolicitation Agreement (incorporated by reference to Exhibit 10.1 to the Company's Current Report on Form 8-K filed with the Commission on December 7, 2016) (Commission File No. 001-37748).
10.31*	Form of Performance-Based Restricted Stock Agreement for Executives under the SecureWorks Corp. 2016 Long-Term Incentive Plan (incorporated by reference to Exhibit 10.1 to the Company's Current Report on Form 8-K filed with the Commission on March 10, 2017) (Commission File No. 001-37748).
10.32*	Form of Performance Stock Unit Agreement for Executives under the SecureWorks Corp. 2016 Long-Term Incentive Plan (incorporated by reference to Exhibit 10.2 to the Company's Current Report on Form 8-K filed with the Commission on March 10, 2017) (Commission File No. 001-37748).
10.33*	Amended and Restated SecureWorks Corp. Incentive Bonus Plan (incorporated by reference to Exhibit 10.33 to the Company's Annual Report on Form 10-K for the fiscal year ended February 3, 2017) (Commission File No. 001-37748).
10.34*	Separation Agreement and Release, dated as of April 18, 2019, between SecureWorks, Inc., for itself, its subsidiaries, its parents and related entities, and Wayne Jackson (incorporated by reference to Exhibit 10.4 to the Company's Quarterly Report on Form 10-Q for the quarterly period ended May 3, 2019) (Commission File No. 001-37748).
21.1††	Subsidiaries of SecureWorks Corp.

EXHIBIT INDEX - Continued

Exhibit No.	Description
23.1††	Consent of PricewaterhouseCoopers LLP, independent registered public accounting firm of SecureWorks Corp.
31.1††	Certification of Chief Executive Officer of the Company pursuant to Rule 13a-14(a) or Rule 15d-14(a) under the Securities Exchange Act of 1934, as adopted pursuant to Section 302 of the Sarbanes-Oxley Act of 2002.
31.2††	Certification of Chief Financial Officer of the Company pursuant to Rule 13a-14(a) or Rule 15d-14(a) under the Securities Exchange Act of 1934, as adopted pursuant to Section 302 of the Sarbanes-Oxley Act of 2002.
32.1†††	Certifications of Chief Executive Officer and Chief Financial Officer of the Company pursuant to Rule 13a-14(b) or Rule 15d-14(b) under the Securities Exchange Act of 1934 and 18 U.S.C. Section 1350, as adopted pursuant to Section 906 of the Sarbanes-Oxley Act of 2002.
101 .INS††	XBRL Instance Document - the instance document does not appear in the Interactive Data File because its XBRL tags are embedded within the Inline XBRL document.
101 .SCH††	XBRL Taxonomy Extension Schema Document.
101 .CAL††	XBRL Taxonomy Extension Calculation Linkbase Document.
101 .DEF††	XBRL Taxonomy Extension Definition Linkbase Document.
101 .LAB††	XBRL Taxonomy Extension Label Linkbase Document.
101 .PRE††	XBRL Taxonomy Extension Presentation Linkbase Document.
104††	Cover Page Interactive Data File (the cover page XBRL tags are embedded within the Inline XBRL document, which is contained in Exhibit 101).

+	Certain portions of this exhibit have been omitted pursuant to a confidential treatment request. Omitted information has been filed separately with the SEC.
††	Filed with this report.
†††	Furnished with this report.
*	Management contracts or compensation plans or arrangements in which directors or executive officers participate.

Item 16. Form 10-K Summary

None.

SIGNATURES

Pursuant to the requirements of Section 13 or 15(d) of the Securities Exchange Act of 1934, the registrant has duly caused this report to be signed on its behalf by the undersigned, thereunto duly authorized.

SecureWorks Corp.

By: /s/ Michael R. Cote
Michael R. Cote
President and Chief Executive Officer
(Duly Authorized Officer)

Date: March 27, 2020

Pursuant to the requirements of the Securities Exchange Act of 1934, this report has been signed below by the following persons on behalf of the registrant and in the capacities and on the dates indicated.

SIGNATURE	TITLE	DATE
/s/ Michael R. Cote Michael R. Cote	President, Chief Executive Officer and Director (Principal Executive Officer)	March 27, 2020
/s/ Paul M. Parrish Paul M. Parrish	SVP, Chief Financial Officer (Principal Financial Officer and Principal Accounting Officer)	March 27, 2020
/s/ Michael S. Dell Michael S. Dell	Chairman of the Board of Directors	March 27, 2020
/s/ Egon Durban Egon Durban	Director	March 27, 2020
/s/ Pamela Daley Pamela Daley	Director	March 27, 2020
/s/ Yagyensh C. Pati Yagyensh C. Pati	Director	March 27, 2020
/s/ Mark J. Hawkins Mark J. Hawkins	Director	March 27, 2020