FORTINET INC
Form 10-K
February 26, 2018
Table of Contents

UNITED STATES
SECURITIES AND EXCHANGE COMMISSION
Washington, D.C. 20549

FORM 10-K
(Mark One)
x ANNUAL REPORT PURSUANT TO SECTION 13 OR 15(d) OF THE SECURITIES EXCHANGE ACT OF 1934
For the fiscal year ended December 31, 2017
or
o 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: 001-34511

FORTINET, INC.
(Exact name of registrant as specified in its charter)

Delaware	77-0560389
(State or other jurisdiction of incorporation or organization)	(I.R.S. Employer Identification No.)
899 Kifer Road Sunnyvale, California	94086
(Address of principal executive offices)	(Zip Code)

(408) 235-7700
(Registrant's telephone number, including area code)

Securities registered pursuant to Section 12(b) of the Act:

Common Stock, $0.001 Par Value	The Nasdaq Stock Market LLC
(Title of each class)	(Name of exchange on which registered)

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 x No o
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 o No x

Table of Contents

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 ("Exchange Act") 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 x No o

Indicate by check mark whether the registrant has submitted electronically and posted on its corporate Website, if any, every Interactive Data File required to be submitted and posted pursuant to Rule 405 of Regulation S-T (§232.405 of this chapter) during the preceding 12 months (or for such shorter period that the registrant was required to submit and post such files). Yes x No o

Indicate by check mark if disclosure of delinquent filers pursuant to Item 405 of Regulation S-K (§229.405 of this chapter) is not contained herein, and will not be contained, to the best of the registrant's knowledge, in definitive proxy or information statements incorporated by reference in Part III of this Form 10-K or any amendment to this Form 10-K. x

Indicate by check mark whether the registrant is a large accelerated filer, an accelerated filer, a non-accelerated filer, a 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	x	Accelerated filer	o
Non-accelerated filer	o (Do not check if smaller reporting company)	Smaller reporting company	o
		Emerging growth company	o

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. o

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

The aggregate market value of voting stock held by non-affiliates of the registrant, as of June 30, 2017, the last business day of the registrant's most recently completed second quarter, was $4,597,906,585 (based on the closing price for shares of the registrant's common stock as reported by The Nasdaq Global Select Market on that date). Shares of common stock held by each executive officer, director, and holder of 5% or more of the registrant's outstanding common stock have been excluded in that such persons may be deemed to be affiliates. This determination of affiliate status is not necessarily a conclusive determination for other purposes.

As of February 16, 2018, there were 168,024,163 shares of the registrant's common stock outstanding.

DOCUMENTS INCORPORATED BY REFERENCE

Portions of the registrant's definitive Proxy Statement relating to its 2018 Annual Meeting of Stockholders are incorporated by reference into Part III of this Annual Report on Form 10-K where indicated. Such Proxy Statement will be filed with the United States Securities and Exchange Commission within 120 days after the end of the fiscal year to which this report relates.

FORTINET, INC.
ANNUAL REPORT ON FORM 10-K
For the Year Ended December 31, 2017
Table of Contents

Table of Contents

Part I

ITEM 1. Business

Overview

Fortinet is a global leader in broad, automated and integrated cybersecurity solutions. We provide high performance cybersecurity solutions to a wide variety of businesses, such as carriers, data centers, enterprises and distributed offices, including a majority of the Fortune 100 companies. Our cybersecurity solutions are designed to provide broad, automated and integrated protection against dynamic and sophisticated security threats, while simplifying the information technology ("IT") and security infrastructure of our end-customers.

We have four current focus areas for our business.

- Core Business (FortiGate)—We derive a majority of product sales from our FortiGate appliances. Our FortiGate appliances include the FortiGate-20 to -100 series, designed for small businesses and enterprises with distributed offices ("low-end products"), the FortiGate-200 to -900 series for medium-sized businesses ("mid-range products") and the FortiGate-1000 to -7000 series for large businesses and service providers ("high-end products"). In February 2018, we launched the new FortiGate 6000 series, which is built upon a new hardware process and architecture that delivers over 100 gigabytes of advanced threat protection and secure sockets layer ("SSL") inspection to handle the volume of traffic driven by increased adoption of the cloud.

Our FortiOS operating system provides the foundation for all FortiGate security functions and offers end-customers the ability to manage security capabilities across their cloud assets and software-defined wireless area networks. Our network security platform also includes our FortiGuard security subscription services, which end-customers can subscribe to in order to obtain access to updates to application control, anti-virus, intrusion prevention, web filtering and anti-spam functionality. End-customers may also purchase FortiCare technical support services for our products and FortiCare professional services to assist in the design, implementation and maintenance of their networks. We complement our core FortiGate product line with other products and software that offer additional protection from security threats to other critical areas of the business.

- Fortinet Security Fabric—We developed the Fortinet Security Fabric to provide unified security across the entire digital attack surface, including network core, endpoints, applications, data centers, access and private and public cloud. The Fortinet Security Fabric is designed to enable traditionally disparate security devices to work together as an integrated and collaborative whole. It delivers integrated scalability, access control, awareness, security, traffic segmentation, centralized management, visibility and orchestration. The breadth of the Fortinet Security Fabric helps businesses and government agencies defend the expanding attack surface.

At the core of the Fortinet Security Fabric are our FortiGate hardware products and software, which include a broad set of security services, including firewall, virtual private network, anti-malware, anti-spam, application control, intrusion prevention, access control, web filtering, traffic and device segmentation and advanced threat protection ("ATP"). Through these security services, our FortiGuard Labs team provides updates using threat research and a global cloud network of data collection and intelligence resources to deliver subscription-based security services to FortiGate appliances and software products.

We continue to expand the adoption of the Fortinet Security Fabric to third-party solution providers. In 2017, we welcomed 18 new partners to our Fabric-Ready partner program, including Intel, Amazon Web Services and Microsoft. Our Fabric-ready program consisted of 37 ecosystem partners as of February 3, 2018. Billings for non-FortiGate products and services increased in 2017.

- Fortinet Cloud Security—Our technology positions us to deliver security to the cloud and for the cloud. We help our customers secure their cloud implementations by offering integration, visibility and automation across multi-cloud and hybrid deployments. We have a variety of software products designed to extend traditional network security protection into the cloud as standalone solutions, or as part of our distributed Security Fabric architecture. Our FortiCASB extends the core capabilities of our security fabric architecture to provide businesses the same level of cybersecurity and threat intelligence in cloud environments as they do on their physical networks. The Fortinet cloud security is available across all major cloud providers, including Microsoft Azure, Amazon Web Services, Google Cloud, IBM Cloud and Oracle Cloud.

Table of Contents

- Internet of Things ("IoT") and Operational Technology Security ("OT")—The emergence of the IoT has created an environment where data moves freely between devices across locations, network environments, remote offices, mobile workers and public cloud environments, making it difficult to consistently track and secure. We are continuing to extend broad security to these IoT and OT environments. Our products enable critical infrastructure and industrial organizations to deliver advanced segmentation, access control and malware protection needed to unify their security architecture and defend their OT networks regardless of the operating environment.

During our year ended December 31, 2017, we generated total revenue of $1.49 billion and net income of $31.4 million. See Part II, Item 8 of this Annual Report on Form 10-K for more information on our consolidated balance sheets as of December 31, 2017 and 2016 and our consolidated statements of operations, comprehensive income, stockholders' equity and cash flows for each of the three years ended December 31, 2017, 2016 and 2015.

We were incorporated in Delaware in November 2000. Our principal executive office is located at 899 Kifer Road, Sunnyvale, California 94086 and our telephone number at that location is (408) 235-7700.

Technology and Architecture

Our proprietary SPU hardware architecture, FortiOS operating system and associated security and networking functions combine to form the Fortinet Security Fabric. This approach to security ties together discrete security solutions into an integrated whole, which enables our products to perform security processing for networks with high throughput requirements across a broad threat landscape.

SPU

Our proprietary SPU consists of Application-Specific Integrated Circuits ("ASICs") consisting of three main lines of processors: (i) the Content Processor ("SPU CP"), (ii) the Network Processor ("SPU NP") and (iii) the System-on-a-Chip ("SPU SOC"). Our proprietary ASICs are designed to enhance the security processing capabilities implemented in software by accelerating computationally intensive tasks such as firewall policy enforcement, network address translation, IPS threat detection and encryption. This architecture provides the flexibility of implementing accelerated processing of new threat detection without requiring a new ASIC. The SPU CP is currently included in most of our entry-level and all of our mid-range and high-end FortiGate appliances. The SPU NP is currently included in some of our mid-range and high-end FortiGate appliances, delivering additional accelerated firewall and VPN performance. Entry-level FortiGate products often use the SPU SOC2 or SPU SOC3 to provide the necessary acceleration at this level. Mid-range FortiGate products use a central processing unit ("CPU") and include the SPU NP and SPU CP hardware acceleration. The high-end FortiGate products use multiple CPUs, SPU CPs and SPU NPs.

FortiOS

Our proprietary FortiOS operating system provides the foundation for the operation of all FortiGate appliances, whether physical, virtual, private or public cloud or on-demand based, and is at the heart of our Security Fabric implementation. The core kernel functions to the security processing feature sets work together to provide a highly integrated solution. FortiOS provides (i) multiple layers of security, including a hardened kernel layer providing protection for the FortiGate system, (ii) a network security layer providing security for end-customers' network infrastructures and (iii) application content protection providing security for end-customers' workstations and applications. FortiOS directs the operations of processors and SPUs and provides system management functions such as command-line, graphical user interfaces, multiple network and security topology views.

Key high-level functions and capabilities of FortiOS include:

- key enablement for the Fortinet Security Fabric architecture;
- allowing for FortiGate appliances to be configured into different security environments such as our Internal Network Firewall, NGFW and DCFW;
- configuration of the physical aspects of the appliance such as ports, onboard Wi-Fi and switching;
- extending the Fortinet Security Fabric by directly managing FortiSwitch and FortiAP devices;
- key network functions such as routing and deployment modes (network routing, transparent, sniffer, etc.);
- implementation of security updates from our FortiGuard distribution network, delivering ATP, such as IPS, antivirus and application control;
- access to cloud-based web and email filtering databases;
- direct integration with both cloud and on premises FortiSandbox technology;
- security policy objects and enforcement;

Table of Contents

- data leak prevention and document finger printing; and
- real-time reporting and logging.

FortiOS also enables advanced, integrated routing and switching, allowing end-customers to deploy FortiGate devices within a wide variety of networks, as well as providing a direct replacement solution option for legacy switching and routing equipment. FortiOS implements a suite of commonly used standards-based routing protocols as well as network address translation technologies, allowing the FortiGate appliance to integrate and operate in a wide variety of network environments. Additional features include virtual domain capabilities, which can provide support for multiple customers on a single device or FortiOS instance. FortiOS also provides capabilities for logging of traffic for forensic analysis purposes that are particularly important for regulatory compliance initiatives like payment card industry data security standard. FortiOS is designed to help control network traffic in order to optimize performance by including functionality such as packet classification, queue disciplines, policy enforcement, congestion management, WAN optimization and caching. These features enable administrators to set the appropriate configurations and policies that meet their infrastructure needs. We make updates to FortiOS available through our FortiCare technical support services.

Products

Our core product offerings consist of our FortiGate product family, along with our non-FortiGate products, all of which may be purchased to complement commercial and enterprise deployments. Our FortiGate hardware and software licenses are sold with a set of broad security services. These security services are enabled by FortiGuard which provides extensive threat research and artificial intelligence capabilities from a global cloud network to deliver protection services to each FortiGate appliance. Our non-FortiGate products include the Fortinet Security Fabric (such as FortiSandbox, FortiSIEM and FortiManager), cloud security products (such as Fabric virtual machines and cloud services) and other products.

FortiGate

Our flagship FortiGate hardware appliances and software offer a broad set of security and networking functions, including firewall, intrusion prevention, anti-malware, VPN, application control, web filtering, anti-spam and WAN acceleration. All FortiGate models run on our FortiOS operating system. FortiGate platforms can be centrally managed through both embedded web-based and command line interfaces, as well as through FortiManager, which provides central management architecture for thousands of FortiGate hardware appliance and software licenses across a range of hypervisor platforms.

By combining multiple network security functions in our purpose-built security platform, the FortiGate appliances provide broad, high-quality protection capabilities and deployment flexibility while reducing the operational burden and costs associated with managing multiple point products. With over 30 models in the FortiGate product line, FortiGate is designed to address security requirements for small- to medium-sized businesses, large enterprises and government organizations worldwide.

Typically, all FortiGate hardware appliances include our SPUs to accelerate content and network security features implemented within FortiOS. The significant differences between each model are the performance and scalability targets each model is designed to meet, while the security features and associated services offered are common throughout all models. The FortiGate-20 through -100 series models are designed for perimeter protection for small- to medium-sized businesses and enterprises with distributed offices. The FortiGate-200 through -900 series models are designed for perimeter deployment in medium-sized to large enterprise networks. The FortiGate-1000 through -7000 series models deliver high performance and scalable network security functionality for perimeter, data center and core deployment in large enterprises.

We also incorporate additional technologies within FortiGate appliances that differentiate our solutions, including data leakage protection, traffic optimization, secure socket layer inspection, threat vulnerability management and wireless controller technology. In addition to these in-built features, we offer a full range of wireless access points and controllers, complementing FortiGate with the flexibility of wireless local area network access.

Table of Contents

FortiSandbox

The FortiSandbox technology delivers proactive detection and mitigation with the capability to generate a directly actionable protection capability. Available in both hardware and cloud-based form, the FortiSandbox technology has a dual-layer sandbox complemented by FortiGuard's anti-malware intelligence. FortiSandbox allows suspicious code to be subject to a set of multi-layer protection techniques culminating in execution within an operating system to allow detailed real-time behavioral analysis to be performed. When malicious code is identified in this way, a signature can be generated locally for distribution across the Fortinet Security Fabric. Additional insight on the nature of the threat is provided through an intuitive dashboard showing threat information, including system activity, exploit efforts, web traffic and any related subsequent downloads. In addition to integrating within FortiOS, the FortiSandbox can also deliver its detection and local threat intelligence to registered FortiMail, FortiWeb appliances and FortiClient enabled end points.

FortiSIEM

Our FortiSIEM family of products provides a cloud-ready security information and event management ("SIEM") solution for enterprises and service providers. FortiSIEM unifies analytics that are traditionally monitored discretely, parses the information and then processes it in an event-based analytics engine for handling real-time searches, rules, dashboards and ad-hoc queries. This unification of diverse sources of data enables organizations to create comprehensive dashboards and reports to identify root causes of threats, and take the steps necessary to remediate and prevent them in the future. Our FortiSIEM products are available either through subscription or perpetual licenses.

FortiSwitch

Our FortiSwitch product family provides secure switching solutions. It can be deployed in traditional network switching designs with layer 2 and layer 3 access control features. FortiSwitch is part of Fortinet's Security Fabric solution. FortiSwitch within Fortinet Security Fabric creates a scalable and secure access layer on which customers depend for connecting their end devices, such as computers and laptops, as well as an expanding field of IoT devices.

Fortinet Management and Analysis Products

Our FortiManager and FortiAnalyzer hardware and software products are typically sold in conjunction with most commercial and enterprise deployments.

FortiManager. Our FortiManager family of products provides a central and scalable management solution for our FortiGate products, including software updates, configuration, policy settings and security updates. One FortiManager product is capable of managing thousands of FortiGate units. FortiManager facilitates the coordination of policy-based provisioning, device configuration and operating system revision management, as well as network security monitoring and device control.

FortiAnalyzer. Our FortiAnalyzer family of products provides centralized network logging, analyzing and reporting solutions that securely aggregate content and log data from our FortiGate devices and other Fortinet products as well as third-party devices to enable network logging, analysis and reporting.

Services

FortiGuard Security Subscription Services

Security requirements are dynamic due to the constantly changing nature of threats. Our FortiGuard security subscription services are designed to allow us to quickly deliver new threat detection and prevention capabilities to end-customers worldwide as new threats evolve. Our FortiGuard Labs global threat research team identifies emerging threats, collects threat samples, and replicates, reviews, characterizes and collates attack data. Based on this research, we develop updates for virus signatures, attack definitions, scanning engines and other security solution components to distribute to end-customers. End-customers purchase FortiGuard security subscription services in advance, typically with terms of one or more years, to obtain access to regular updates for application control, antivirus, intrusion prevention, web filtering and anti-spam functions for our FortiGate products; antivirus, web filtering and VPN functions for our FortiClient software; antivirus and anti-spam functions for our FortiMail products; vulnerability management for our FortiGate, FortiAnalyzer and FortiMonitor products; database functions for our FortiDB appliance; web functions for our FortiWeb appliances; and ATP for our FortiSandbox on premise and cloud products. We provide FortiGuard security subscription services 24 hours a day, seven days a week.

Table of Contents

FortiCare Technical Support Services

Our FortiCare services portfolio includes technical support and extended product warranty. For our standard technical support, our channel partners may provide first-level support to the end-customer. We also provide first-level support to our end-customers, as well as second- and third-level support as appropriate. We also provide knowledge management tools and customer self-help portals to help augment our support capabilities in an efficient and scalable manner. We deliver technical support to partners and end-customers 24 hours a day, seven days a week through regional technical support centers located worldwide. In addition to our appliance technical support services, we offer a range of advanced services, including premium support and professional services.

Professional Services

We offer professional services to end-customers including Technical Account Managers ("TAMs"), Resident Engineers ("REs") and professional service consultants for implementations.

Dedicated support engineers are available to help identify and eliminate issues before problems arise. These TAMs and REs are seasoned professionals with broad and deep experience in the security and networking field. Each TAM and RE acts as a single point of contact and customer advocate within Fortinet, and is focused on building and maintaining a deep understanding of our customers' businesses and security requirements.

Our professional services consultants help in the design of deployments of our products and work closely with end-customer engineers, managers and other project team members to implement our products according to design, utilizing network analysis tools, traffic simulation software and scripts.

Training Services

We offer training services to our end-customers and channel partners through our training department and authorized training partners. We have also implemented a training certification program, Network Security Expert, to help ensure an understanding of our products and services.

Customers

We typically sell our security solutions to channel partners, who in turn sell to end-customers of various sizes and, at times, we also sell directly to end-customers. Our end-customers include small and medium-sized businesses, large enterprises and government organizations across a wide range of industries, including telecommunications, technology, government, financial services, education, retail, manufacturing and healthcare. An end-customer deployment may involve one of our appliances or thousands, depending on our end-customer's size and security requirements. We also offer access to our products via the cloud through certain cloud providers such as Amazon Web Services and Microsoft Azure. Many of our customers also purchase our FortiGuard security subscription services and FortiCare technical support services. For information regarding our geographic revenue based on billing address, see Note 14 to our consolidated financial statements in Part II, Item 8 of this Annual Report on Form 10-K.

One distributor, Exclusive Networks Group ("Exclusive"), which distributed our solutions to a large group of resellers and end-customers, accounted for 18%, 20% and 25% of total revenue during 2015, 2016 and 2017, respectively. In July 2017, Exclusive acquired the U.S. division of Fine Tec Computers ("Fine Tec U.S."). Fine Tec U.S.'s revenue has been combined with Exclusive's from the date of acquisition. Since the acquisition of Fine Tec U.S., Exclusive's business with us has increased and may continue to increase in the future.

Sales and Marketing

We primarily sell our products and services through a distribution model. We sell to distributors that sell to networking security and enterprise-focused resellers and service providers, who, in turn, sell to our end-customers. In certain cases, we sell directly to government-focused resellers, as well as to large service providers and financial institutions who have large purchasing power and unique customer deployment demands. We work with many technology distributors, including Exclusive, Ingram Micro Inc., Westcon and Tech Data.

Table of Contents

We support our channel partners with a dedicated team of experienced channel account managers, sales professionals and sales engineers who provide business planning, joint marketing strategy, and pre-sales and operational sales support. Additionally, our sales teams help drive and support large enterprise and service provider sales through a direct touch model. Our sales professionals and engineers typically work closely with our channel partners and directly engage with large end-customers to address their unique security and deployment requirements. To support our broadly dispersed global channel and end-customer base, we have sales professionals in over 80 countries around the world.

Our marketing strategy is focused on building our brand and driving end-customer demand for our security solutions. We use a combination of internal marketing professionals and a network of regional and global channel partners. Our internal marketing organization is responsible for messaging, branding, demand generation, product marketing, channel marketing, event marketing, digital marketing, communications, analyst relations, public relations and sales enablement. We focus our resources on campaigns, programs and activities that can be leveraged by partners worldwide to extend our marketing reach, such as sales tools and collateral, product awards and technical certifications, media engagement, training, regional seminars and conferences, webinars and various other demand-generation activities.

In 2017, we continued to invest in sales and marketing, particularly in the enterprise market where enterprise customers tend to have a higher lifetime value. We intend to continue to make investments in our sales resources and infrastructure and marketing strategy, which are critical to support our growth.

Manufacturing and Suppliers

We outsource the manufacturing of our security appliance products to a variety of contract manufacturers and original design manufacturers. Our current manufacturing partners include Micro-Star International Co., Wistron Corporation, Flextronics International Ltd, Senao Networks, Inc., Adlink Technology, Inc. and a number of manufacturers located in Taiwan and other countries outside the United States. We submit purchase orders to our contract manufacturers that describe the type and quantities of our products to be manufactured, the delivery date and other delivery terms. Once our products are manufactured, they are sent to either our warehouse in California, or to our logistics partner in Taoyuan City, Taiwan, where accessory packaging and quality-control testing are performed. We believe that outsourcing our manufacturing and a substantial portion of our logistics enables us to focus resources on our core competencies. Our proprietary SPUs, which are the key to the performance of our appliances, are built by contract manufacturers including Faraday Technology Corporation (“Faraday”), Kawasaki Microelectronics America, Inc. and Renesas Electronics Corporation (“Renesas”). These contract manufacturers use foundries operated by either United Microelectronics Corporation (“UMC”) or Taiwan Semiconductor Manufacturing Company Limited (“TSMC”), or their own foundry, such as Renesas’ fab.

The components included in our products are sourced from various suppliers by us or more frequently by our contract manufacturers. Some of the components important to our business, including specific types of CPUs from Intel Corporation (“Intel”), network chips from Broadcom Corporation (“Broadcom”), Marvell Technology Group Ltd. (“Marvell”) and Intel, and solid-state drives (silicon-based storage devices) from Intel, ADATA Technology Co., Ltd. (“ADATA”), OCZ Technology Group, Inc. (“OCZ”), Samsung Electronics Co., Ltd. (“Samsung”), and Western Digital Technologies, Inc. (“Western Digital”), are available from a limited or sole source of supply.

We have no long-term contracts related to the manufacturing of our ASICs or other components that guarantee any capacity or pricing terms.

Research and Development

We focus our research and development efforts on developing new products and services, and adding new features to existing products and services. Our development strategy is to identify features, products and systems for both software and hardware that are, or are expected to be, important to our end-customers. Our success in designing, developing, manufacturing and selling new or enhanced products will depend on a variety of factors, including the identification of market demand for new products, product selection, timely implementation of product design and development, product performance, effective manufacturing and assembly processes and sales and marketing. Our research and development expense was $210.6 million, $183.1 million and $158.1 million in 2017, 2016 and 2015, respectively.

Table of Contents

Intellectual Property

We rely primarily on patent, trademark, copyright and trade secrets laws, confidentiality procedures and contractual provisions to protect our technology. As of December 31, 2017, we had 467 issued U.S.- and foreign-issued patents and 291 pending U.S. and foreign patent applications. We also license software from third parties for inclusion in our products, including open source software and other software available on commercially reasonable terms.

Despite our efforts to protect our rights in our technology, unauthorized parties may attempt to copy aspects of our products or obtain and use information that we regard as proprietary. We generally enter into confidentiality agreements with our employees, consultants, vendors and customers, and generally limit access to and distribution of our proprietary information. However, we cannot provide assurance that the steps we take will prevent misappropriation of our technology. In addition, the laws of some foreign countries do not protect our proprietary rights to as great an extent as the laws of the United States, and many foreign countries do not enforce these laws as diligently as government agencies and private parties in the United States.

Our industry is characterized by the existence of a large number of patents and frequent claims and related litigation regarding patent and other intellectual property rights. Third parties have asserted, are currently asserting and may in the future assert patent, copyright, trademark or other intellectual property rights against us, our channel partners or our end-customers. Successful claims of infringement by a third party could prevent us from distributing certain products or performing certain services or require us to pay substantial damages (including treble damages if we are found to have willfully infringed patents or copyrights), royalties or other fees. Even if third parties may offer a license to their technology, the terms of any offered license may not be acceptable and the failure to obtain a license or the costs associated with any license could cause our business, operating results or financial condition to be materially and adversely affected. We typically indemnify our end-customers, distributors and certain resellers against claims that our products infringe the intellectual property of third parties.

Seasonality

For information regarding seasonality in our sales, see the section entitled “Management’s Discussion and Analysis of Financial Condition and Results of Operations—Quarterly Results of Operations—Seasonality, Cyclicality and Quarterly Revenue Trends” in Part II, Item 7 of this Annual Report on Form 10-K.

Competition

The markets for our products are extremely competitive and are characterized by rapid technological change. The principal competitive factors in our markets include the following:

•product performance, features, effectiveness, interoperability and reliability;
•our ability to add and integrate new networking and security features and technological expertise;
•compliance with industry standards and certifications;
•price of products and services and total cost of ownership;
•brand recognition;
•customer service and support;
•sales and distribution capabilities;
•size and financial stability of operations; and
•breadth of product line.

Among others, our competitors include Check Point Software Technologies Ltd. (“Check Point”), Cisco Systems, Inc. (“Cisco”), F5 Networks, Inc. (“F5 Networks”), FireEye, Inc. (“FireEye”), Forcepoint LLC (“Forcepoint”), Imperva, Inc.

(“Imperva”), Juniper Networks, Inc. (“Juniper”), McAfee, LLC. (“McAfee”), Palo Alto Networks, Inc. (“Palo Alto Networks”), Proofpoint, Inc. (“Proofpoint”), SonicWALL, Inc. (“SonicWALL”), Sophos Group Plc (“Sophos”), Symantec Corporation (“Symantec”) and Trend Micro Incorporated (“Trend Micro”).

We believe we compete favorably based on our products’ performance, reliability and breadth, our ability to add and integrate new networking and security features and our technological expertise. Several competitors are significantly larger, have greater financial, technical, marketing, distribution, customer support and other resources, are more established than we are and have significantly better brand recognition. Some of these larger competitors have substantially broader product offerings and leverage their relationships based on other products or incorporate functionality into existing products in a manner that discourages users from purchasing our products. Based in part on these competitive pressures, we may lower prices or attempt to add incremental features and functionality.

Table of Contents

Conditions in our markets could change rapidly and significantly as a result of technological advancements or continuing market consolidation. The development and market acceptance of alternative technologies could decrease the demand for our products or render them obsolete. Our competitors may introduce products that are less costly, provide superior performance, market their products better, or achieve greater market acceptance than us. In addition, our larger competitors often have broader product lines and are in a better position to withstand any significant reduction in capital spending by end-customers in these markets, and will therefore not be as susceptible to downturns in a particular market. The above competitive pressures are likely to continue to impact our business. We may not be able to compete successfully in the future, and competition may harm our business.

Employees

As of December 31, 2017, our total headcount was 5,066 employees and contractors. None of our U.S. employees are represented by a labor union; however, our employees in certain European countries have the right to be represented by external labor organizations if they maintain up-to-date union membership. We have not experienced any work stoppages, and we consider our relations with our employees to be good.

Available Information

Our web site is located at www.fortinet.com, and our investor relations web site is located at http://investor.fortinet.com. The information posted on our website is not incorporated by reference into this Annual Report on Form 10-K. Our Annual Report on Form 10-K, Quarterly Reports on Form 10-Q, Current Reports on Form 8-K and amendments to reports filed or furnished pursuant to Sections 13(a) and 15(d) of the Securities Act, are available free of charge on our investor relations web site as soon as reasonably practicable after we electronically file such material with, or furnish it to, the SEC. You may also access all of our public filings through the SEC's website at www.sec.gov. Further, a copy of this Annual Report on Form 10-K is located at the SEC's Public Reference Room at 100 F Street, NE, Washington, D.C. 20549. Information on the operation of the Public Reference Room can be obtained by calling the SEC at 1-800-SEC-0330.

We webcast our earnings calls and certain events we participate in or host with members of the investment community on our investor relations web site. Additionally, we provide notifications of news or announcements regarding our financial performance, including SEC filings, investor events, press and earnings releases, as part of our investor relations web site. The contents of these web sites are not intended to be incorporated by reference into this report or in any other report or document we file.

Table of Contents

ITEM 1A. Risk Factors

Investing in our common stock involves a high degree of risk. Investors should carefully consider the following risks and all other information contained in this Annual Report on Form 10-K, including our consolidated financial statements and the related notes, before investing in our common stock. The risks and uncertainties described below are not the only ones we face. Additional risks and uncertainties that we are unaware of, or that we currently believe are not material, also may become important factors that affect us. If any of the following risks materialize, our business, financial condition and results of operations could be materially harmed. In that case, the trading price of our common stock could decline substantially, and investors may lose some or all of their investment.

Risks Related to Our Business

Our operating results are likely to vary significantly and be unpredictable.

Our operating results have historically varied from period to period, and we expect that they will continue to do so as a result of a number of factors, many of which are outside of our control or may be difficult to predict, including:

- our ability to attract and retain new end-customers or sell additional products and subscriptions to our existing end-customers;
- the level of demand for our products and services, which may render forecasts inaccurate;
- the timing of channel partner and end-customer orders, and our reliance on a concentration of shipments at the end of each quarter;
- the timing of shipments, which may depend on factors such as inventory levels, logistics, manufacturing or shipping delays, our ability to ship new products on schedule and our ability to accurately forecast inventory requirements;
- inventory management;
- the mix of products sold and the mix of revenue between products and services, as well as the degree to which products and services are bundled and sold together for a package price;
- the purchasing practices and budgeting cycles of our channel partners and end-customers;
- the effectiveness of our sales organization, generally or in a particular geographic region, the time it takes to hire sales personnel and the timing of hiring, and our ability to retain, sales personnel;
- the seasonal buying patterns of our end-customers;
- the timing and level of our investments in sales and marketing, and the impact of such investments on our operating expenses, operating margin and the productivity and effectiveness of execution of our sales and marketing teams;
- the timing of revenue recognition for our sales;
- the level of perceived threats to network security, which may fluctuate from period to period;
- changes in the requirements, market needs or buying practices and patterns of our distributors, resellers or end-customers;

- changes in the growth rate of the network security market;

- the timing and success of new product and service introductions or enhancements by us or our competitors, or any other change in the competitive landscape of our industry, including consolidation among our competitors, partners or end-customers;

Table of Contents

- the deferral of orders from distributors, resellers or end-customers in anticipation of new products or product enhancements announced by us or our competitors;

- increases or decreases in our billings, revenue and expenses caused by fluctuations in foreign currency exchange rates or a strengthening of the U.S. dollar, as a significant portion of our expenses is incurred and paid in currencies other than the U.S. dollar, and the impact such fluctuations may have on the actual prices that our partners and customers are willing to pay for our products and services;

- compliance with existing laws and regulations that are applicable to our ability to conduct business with the public sector;

- the impact of cloud-based platforms on the timing of our revenue recognition, billings and free cash flow;

- decisions by potential end-customers to purchase network security solutions from newer technology providers, from larger, more established security vendors or from their primary network equipment vendors;

- price competition and increased competitiveness in our market;

- our ability to both increase revenues and manage and control operating expenses in order to improve our operating margins;

- changes in customer renewal rates for our services;

- changes in the payment terms of services contracts or the length of services contracts sold;

- changes in our estimated annual effective tax rates;

- changes in circumstances and challenges in business conditions, including decreased demand, which may negatively impact our channel partners' ability to sell the current inventory they hold and negatively impact their future purchases of products from us;

- increased demand for cloud-based services and the uncertainty associated with transitioning to providing such services;

- increased expenses, unforeseen liabilities or write-downs and any impact on results of operations from any acquisition consummated;

- our channel partners having insufficient financial resources to withstand changes and challenges in business conditions;

- disruptions in our channel or termination of our relationship with important channel partners, including as a result of consolidation among distributors and resellers of security solutions;

- insolvency, credit or other difficulties confronting our key suppliers and channel partners, which could affect their ability to purchase or pay for products and services and which could disrupt our supply or distribution chain;

- policy changes and uncertainty with respect to immigration laws, trade policy, foreign imports and tax laws related to international commerce;

- political, economic and social instability;

- general economic conditions, both in domestic and foreign markets;

- future accounting pronouncements or changes in our accounting policies, such as changes in the revenue recognition standards or accounting for leases, as well as the significant costs that may be incurred to adopt and comply with these new pronouncements;

Table of Contents

- possible impairments or acceleration of depreciation of our existing real estate due to our current real estate holdings and future development plans; and

- legislative or regulatory changes, such as with respect to privacy, information and cybersecurity, exports, the environment and applicable accounting standards.

Any one of the factors above or the cumulative effect of some of the factors referred to above may result in significant fluctuations in our quarterly financial and other operating results. This variability and unpredictability could result in our failing to meet our internal operating plan or the expectations of securities analysts or investors for any period. If we fail to meet or exceed such expectations for these or any other reasons, the market price of our shares could fall substantially and we could face costly lawsuits, including securities class action suits. In addition, a significant percentage of our operating expenses are fixed in nature over the near term. Accordingly, in the event of revenue shortfalls, we are generally unable to mitigate the negative impact on margins in the short term.

Adverse economic conditions or reduced information technology spending may adversely impact our business.

Our business depends on the overall demand for information technology and on the economic health of our current and prospective customers. In addition, the purchase of our products is often discretionary and may involve a significant commitment of capital and other resources. Weak global economic conditions and spending environments, weak economic conditions in certain regions or a reduction in information technology spending regardless of macro-economic conditions could have adverse impacts on our business, financial condition and results of operations, including longer sales cycles, lower prices for our products and services, higher default rates among our channel partners, reduced unit sales and slower or declining growth.

Our billings, revenue, operating margin and free cash flow growth may slow or may not continue.

We may experience slowing growth, or a decrease, in billings, revenue, operating margin and free cash flow for a number of reasons, including a slowdown in demand for our products or services, a shift in demand from products to services, increased competition, a decrease in the growth of our overall market or softness in demand in certain geographies or industry verticals, such as the service provider industry, changes in our strategic opportunities and our failure for any reason to continue to capitalize on growth opportunities and due to other risks identified in the risk factors described in this periodic report. Our expenses as a percentage of total revenue may be higher than expected if our revenue is lower than expected and, if our investments in sales and marketing and other functional areas do not result in expected billings and revenue growth, we may experience margin declines and may not be able to sustain profitability in future periods if we fail to increase billings, revenue or deferred revenue, do not appropriately manage our cost structure and free cash flow or encounter unanticipated liabilities. Any failure by us to maintain profitability, maintain our margins and continue our billings, revenue and free cash flow growth could cause the price of our common stock to materially decline.

Table of Contents

We rely significantly on revenue from FortiGuard security subscription and FortiCare technical support services, and revenue from these services may decline or fluctuate. Because we recognize revenue from these services over the term of the relevant service period, downturns or upturns in sales of FortiGuard security subscription and FortiCare technical support services are not immediately reflected in full in our operating results.

Our FortiGuard security subscription and FortiCare technical support services revenue has historically accounted for a significant percentage of our total revenue. Revenue from the sale of new, or from the renewal of existing, FortiGuard security subscription and FortiCare technical support service contracts may decline and fluctuate as a result of a number of factors, including fluctuations in purchases of FortiGate appliances, changes in the sales mix between products and services, end-customers' level of satisfaction with our products and services, the prices of our products and services, the prices of products and services offered by our competitors, reductions in our customers' spending levels and the timing of revenue recognition with respect to these arrangements. If our sales of new, or renewals of existing, FortiGuard security subscription and FortiCare technical support service contracts decline, our revenue and revenue growth may decline and our business could suffer. In addition, in the event significant customers require payment terms for FortiGuard security subscription and FortiCare technical support services in arrears or for shorter periods of time than annually, such as monthly or quarterly, this may negatively impact our billings and revenue. Furthermore, we recognize FortiGuard security subscription and FortiCare technical support services revenue monthly over the term of the relevant service period, which is typically from one to three years, to a lesser extent, five years. As a result, much of the FortiGuard security subscription and FortiCare technical support services revenue we report each quarter is the recognition of deferred revenue from FortiGuard security subscription and FortiCare technical support services contracts entered into during previous quarters or years. Consequently, a decline in new or renewed FortiGuard security subscription and FortiCare technical support services contracts in any one quarter will not be fully reflected in revenue in that quarter but will negatively affect our revenue in future quarters. Accordingly, the effect of significant downturns in sales of new, or renewals of existing, FortiGuard security subscription and FortiCare technical support services is not reflected in full in our statements of operations until future periods. Our FortiGuard security subscription and FortiCare technical support services revenue also makes it difficult for us to rapidly increase our revenue through additional service sales in any period, as revenue from new and renewal support services contracts must be recognized over the applicable service period.

We generate a majority of revenue from sales to distributors, resellers and end-customers outside of the United States, and we are therefore subject to a number of risks associated with international sales and operations.

We market and sell our products throughout the world and have established sales offices in many parts of the world. Our international sales have represented a majority of our total revenue in recent periods. Therefore, we are subject to risks associated with having worldwide operations. We are also subject to a number of risks typically associated with international sales and operations, including:

- economic or political instability in foreign markets;
- greater difficulty in enforcing contracts and accounts receivable collection, including longer collection periods;
- longer sales processes for larger deals, particularly during the summer months;
- changes in regulatory requirements;
- difficulties and costs of staffing and managing foreign operations;
- the uncertainty of protection for intellectual property rights in some countries;

- costs of compliance with foreign policies, laws and regulations and the risks and costs of non-compliance with such policies, laws and regulations;

- protectionist policies and penalties, and local laws, requirements, policies and perceptions that may adversely impact a U.S.-headquartered business's sales in certain countries outside of the United States;

- costs of complying with, and the risks and costs of non-compliance with, U.S. or other foreign laws and regulations for foreign operations, including the U.S. Foreign Corrupt Practices Act, the United Kingdom Bribery Act 2010, the General Data Protection Regulation (which will be implemented by the European Union in May 2018), import and export control laws, tariffs, trade barriers and economic sanctions;

Table of Contents

- other regulatory or contractual limitations on our ability to sell our products in certain foreign markets, and the risks and costs of non-compliance;

- heightened risks of unfair or corrupt business practices in certain geographies and of improper or fraudulent sales or sales-related arrangements that could disrupt the sales team through terminations of employment or otherwise, and may adversely impact financial results as compared to those already reported or forecasted and result in restatements of financial statements and irregularities in financial statements;

- our ability to effectively implement and maintain adequate internal controls to properly manage our international sales and operations;

- the potential for political unrest, changes and uncertainty, and for terrorism, hostilities, war or natural disasters;

- changes in foreign currency exchange rates;

- management communication and integration problems resulting from cultural differences and geographic dispersion; and

- changes in tax, employment and other laws.

Product and service sales and employee and contractor matters may be subject to foreign governmental regulations, which vary substantially from country to country. Further, we may be unable to keep up-to-date with changes in government requirements as they change over time. Failure to comply with these regulations could result in adverse effects to our business. In many foreign countries, it is common for others to engage in business practices that are prohibited by our internal policies and procedures or U.S. regulations applicable to us. Although we implemented policies and procedures designed to ensure compliance with these laws and policies, there can be no assurance that all of our employees, contractors, channel partners and agents will comply with these laws and policies. Violations of laws or key control policies by our employees, contractors, channel partners or agents could result in litigation, regulatory action, costs of investigation, delays in revenue recognition, delays in financial reporting, financial reporting misstatements, fines, penalties or the prohibition of the importation or exportation of our products and services, any of which could have a material adverse effect on our business and results of operations.

If we are not successful in continuing to execute our strategy to increase our sales to large and medium-sized end-customers, our results of operations may suffer.

An important part of our growth strategy is to increase sales of our products to large and medium-sized businesses, service providers and government organizations. While we have increased sales in recent periods to large and medium-sized businesses, our sales volume varies by quarter. Such sales are often for a longer contract term and may be at higher discount levels. We also have experienced uneven traction selling to certain government organizations and service providers, and there can be no assurance that we will be successful selling to these customers. Sales to these organizations involve risks that may not be present, or that are present to a lesser extent, with sales to smaller entities. These risks include:

- increased competition from competitors that traditionally target large and medium-sized businesses, service providers and government organizations and that may already have purchase commitments from those end-customers;

- increased purchasing power and leverage held by large end-customers in negotiating contractual arrangements;

-

unanticipated changes in the capital resources or purchasing behavior of large end-customers, including changes in the volume and frequency of their purchases and changes in the mix of products and services and related payment terms;

- more stringent support requirements in our support service contracts, including stricter support response times, more complex requirements and increased penalties for any failure to meet support requirements;

- longer sales cycles and the associated risk that substantial time and resources may be spent on a potential end-customer that elects not to purchase our products and services; and

Table of Contents

• longer ramp-up periods for enterprise sales personnel as compared to other sales personnel.

Large and medium-sized businesses, service providers and government organizations often undertake a significant evaluation process that results in a lengthy sales cycle, in some cases longer than 12 months. Although we have a channel sales model, our sales representatives typically engage in direct interaction with end-customers, along with our distributors and resellers, in connection with sales to large and medium-sized end-customers. We may spend substantial time, effort and money in our sales efforts without being successful in producing any sales. In addition, product purchases by large and medium-sized businesses, service providers and government organizations are frequently subject to budget constraints, multiple approvals and unplanned administrative, processing and other delays. Furthermore, service providers represent our largest industry vertical and consolidation or continued changes in buying behavior by larger customers within this industry could negatively impact our business. Large and medium-sized businesses, service providers and government organizations typically have longer implementation cycles, require greater product functionality and scalability, expect a broader range of services, including design services, demand that vendors take on a larger share of risks, require acceptance provisions that can lead to a delay in revenue recognition and expect greater payment flexibility from vendors. In addition, large and medium-sized businesses, service providers and government organizations may require that our products and services be sold differently from how we offer our products and services, which could negatively impact our operating results. Our large business and service provider customers may also become more deliberate in their purchases as they plan their next-generation network security architecture, leading them to take more time in making purchasing decisions or to purchase based only on their immediate needs. All these factors can add further risk to business conducted with these customers. In addition, if sales expected from a large and medium-sized end-customer for a particular quarter are not realized in that quarter or at all, our business, operating results and financial condition could be materially and adversely affected.

Managing inventory of our products and product components is complex. Insufficient inventory may result in lost sales opportunities or delayed revenue, while excess inventory may harm our gross margins.

Managing our inventory is complex. Our channel partners may increase orders during periods of product shortages, cancel orders or not place orders commensurate with our expectations if their inventory is too high, return products or take advantage of price protection (if any is available to the particular partner) or delay orders in anticipation of new products, and accurately forecasting inventory requirements and demand can be challenging. Our channel partners also may adjust their orders in response to the supply of our products and the products of our competitors that are available to them and in response to seasonal fluctuations in end-customer demand. Furthermore, if the time required to manufacture or ship certain products increases for any reason, inventory shortfalls could result. Management of our inventory is further complicated by the significant number of different products and models that we sell which may impact our billings, revenue and free cash flow. Mismanagement of our inventory, whether due to imprecise forecasting, employee errors or malfeasance, inaccurate information or otherwise, may adversely affect our results of operations.

Inventory management remains an area of focus as we balance the need to maintain inventory levels that are sufficient to ensure competitive lead times against the risk of inventory obsolescence because of rapidly changing technology and customer requirements, or excess inventory levels. If we ultimately determine that we have excess inventory, we may have to reduce our prices and write-down inventory, which in turn could result in lower gross margins. Alternatively, insufficient inventory levels may lead to shortages that result in delayed revenue or loss of sales opportunities altogether as potential end-customers turn to competitors' products that are readily available. For example, we have in the past experienced inventory shortages and excesses due to the variance in demand for certain products from forecasted amounts. In addition, for those channel partners that have rights of return, inventory held by such channel partners affects our results of operations. Our inventory management systems and related supply chain

visibility tools may be inadequate to enable us to effectively manage inventory. If we are unable to effectively manage our inventory and that of our channel partners, our results of operations could be adversely affected.

Table of Contents

We are dependent on the continued services and performance of our senior management, the loss of any of whom could adversely affect our business, operating results and financial condition.

Our future performance depends on the continued services and continuing contributions of our senior management to execute on our business plan and to identify and pursue new opportunities and product innovations. The loss of services of members of senior management, particularly Ken Xie, our Co-Founder, Chief Executive Officer and Chairman or Michael Xie, our Co-Founder, President and Chief Technology Officer, or of any of our senior sales leaders or functional area leaders, could significantly delay or prevent the achievement of our development and strategic objectives. In February 2018, we underwent a transition in senior management as Drew Del Matto resigned as our Chief Financial Officer and Keith Jensen was appointed as our Interim Chief Financial Officer. The loss of the services or the distraction of our senior management for any reason could adversely affect our business, financial condition and results of operations.

If we are unable to hire, retain and motivate qualified personnel, our business will suffer.

Our future success depends, in part, on our ability to continue to attract and retain highly skilled personnel. The loss of the services of any of our key personnel, the inability to attract or retain qualified personnel, or delays in hiring required personnel, particularly in engineering, sales and marketing, may seriously harm our business, financial condition and results of operations. From time to time, we experience turnover in our management-level personnel. None of our key employees has an employment agreement for a specific term, and any of our employees may terminate their employment at any time. Our ability to continue to attract and retain highly skilled personnel will be critical to our future success. Competition for highly skilled personnel is frequently intense, especially for qualified employees in network security and especially in the locations where we have a substantial presence and need for highly skilled personnel, such as the San Francisco Bay Area and Vancouver, Canada. We may not be successful in attracting, assimilating or retaining qualified personnel to fulfill our current or future needs. Also, to the extent we hire personnel from competitors, we may be subject to allegations that they have been improperly solicited or divulged proprietary or other confidential information. Changes in immigration laws, including changes to the rules regarding H1-B visas, may also harm our ability to attract personnel from other countries.

If we do not increase the effectiveness of our sales organization, we may have difficulty adding new end-customers or increasing sales to our existing end-customers and our business may be adversely affected.

Although we have a channel sales model, members of our sales organization often engage in direct interaction with our prospective end-customers. Therefore, we continue to be substantially dependent on our sales organization to obtain new end-customers and sell additional products and services to our existing end-customers. There is significant competition for sales personnel with the skills and technical knowledge that we require. Our ability to grow our revenue depends, in large part, on our success in recruiting, training and retaining sufficient numbers of sales personnel to support our growth and on the effectiveness of those personnel. New hires require substantial training and may take significant time before they achieve full productivity. Our recent hires and planned hires may not become productive as quickly as we expect, and we may be unable to hire or retain sufficient numbers of qualified individuals in the markets where we do business or plan to do business. For example, we realigned our sales organization in early 2016 and it has taken more time than we expected to ramp up the productivity of our realigned sales organization. Furthermore, hiring sales personnel in new countries requires additional setup and upfront costs that we may not recover if the sales personnel fail to achieve full productivity. If our sales employees do not become fully productive on the timelines that we have projected, our revenue will not increase at anticipated levels and our ability to achieve long-term projections may be negatively impacted. If we are unable to hire and train sufficient numbers of effective sales personnel, or the sales personnel are not successful in obtaining new end-customers or increasing sales to our existing customer base, our business, operating results and prospects will be adversely affected.

15

Table of Contents

The sales prices of our products and services may decrease, which may reduce our gross profits and operating margin, and which may adversely impact our financial results and the trading price of our common stock.

The sales prices for our products and services may decline for a variety of reasons, including competitive pricing pressures, discounts or promotional programs we offer, a change in our mix of products and services and anticipation of the introduction of new products and services. Competition continues to increase in the market segments in which we participate, and we expect competition to further increase in the future, thereby leading to increased pricing pressures. Larger competitors with more diverse product offerings may reduce the price of products and services that compete with ours in order to promote the sale of other products or services or may bundle them with other products or services. Additionally, although we price our products and services worldwide in U.S. dollars, currency fluctuations in certain countries and regions have in the past, and may in the future, negatively impact actual prices that partners and customers are willing to pay in those countries and regions. Furthermore, we anticipate that the sales prices and gross profits for our products or services will decrease over product life cycles. We cannot ensure that we will be successful in developing and introducing new offerings with enhanced functionality on a timely basis, or that our product and service offerings, if introduced, will enable us to maintain our prices, gross profits and operating margin at levels that will allow us to maintain profitability.

Reliance on a concentration of shipments at the end of the quarter could cause our billings and revenue to fall below expected levels.

As a result of customer-buying patterns and the efforts of our sales force and channel partners to meet or exceed quarterly quotas, we have historically received a substantial portion of each quarter's sales orders and generated a substantial portion of each quarter's billings and revenue during the last two weeks of the quarter. If expected orders at the end of any quarter are delayed for any reason, including the failure of anticipated purchase orders to materialize, our logistics partners' inability to ship products prior to quarter-end to fulfill purchase orders received near the end of the quarter, our failure to accurately forecast our inventory requirements and to appropriately manage inventory to meet demand, our inability to release new products on schedule, any failure of our systems related to order review and processing, any delays in shipments due to trade compliance requirements, labor disputes or logistics changes at shipping ports or otherwise, our billings and revenue for that quarter could fall below our expectations or those of securities analysts and investors, resulting in a decline in our stock price.

Unless we continue to develop better market awareness of our company and our products, and to improve lead generation and sales enablement, our revenue may not continue to grow.

Increased market awareness of our capabilities and products and increased lead generation are essential to our continued growth and our success in all of our markets, particularly for the large businesses, service provider and government organization market. We have historically had relatively low spending on marketing activities. While we have increased our investments in sales and marketing, it is not clear that these investments will continue to result in increased revenue. If our investments in additional sales personnel or if our marketing programs are not successful in continuing to create market awareness of our company and products or increasing lead generation, or if we experience turnover and disruption in our sales and marketing teams, we will not be able to achieve sustained growth, and our business, financial condition and results of operations will be adversely affected.

We rely on third-party channel partners to generate substantially all of our revenue. If our partners fail to perform, our ability to sell our products and services will be limited, and if we fail to optimize our channel partner model going forward, our operating results will be harmed.

A significant portion of our sales is generated through a limited number of distributors, and substantially all of our revenue is generated through sales by our channel partners, including distributors and resellers. We depend on our

channel partners to generate a significant portion of our sales opportunities and to manage our sales process. To the extent our channel partners are unsuccessful in selling our products, or we are unable to enter into arrangements with and retain a sufficient number of high-quality channel partners in each of the regions in which we sell products, or if we are unable to keep them motivated to sell our products, our ability to sell our products and operating results will be harmed. The termination of our relationship with any significant channel partner may adversely impact our sales and operating results.

Table of Contents

We provide sales channel partners with specific programs to assist them in selling our products and incentivize them to sell our products, but there can be no assurance that these programs will be effective. In addition, our channel partners may be unsuccessful in marketing, selling and supporting our products and services and may purchase more inventory than they can sell. Our channel partners generally do not have minimum purchase requirements. Some of our channel partners may have insufficient financial resources to withstand changes and challenges in business conditions. In addition, if our channel partners' financial condition or operations weaken it could negatively impact their ability to sell our product and services. Our channel partners may also market, sell and support products and services that are competitive with ours, and may devote more resources to the marketing, sales and support of such products. They may also have incentives to promote our competitors' products to the detriment of our own, or they may cease selling our products altogether. We cannot ensure that we will retain these channel partners or that we will be able to secure additional or replacement partners or that existing channel partners will continue to perform. The loss of one or more of our significant channel partners or the failure to obtain and ship a number of large orders each quarter through them could harm our operating results.

In addition, we may be impacted by consolidation of our existing channel partners. In such instances, we may experience changes to our overall business and operational relationships due to dealing with a larger combined entity, and our ability to maintain such relationships on favorable contractual terms may be more limited. We may also become increasingly dependent on a more limited number of channel partners, as consolidation increases the relative proportion of our business for which each channel partner is responsible, which may magnify the risks described in the preceding paragraphs. In July 2017, Exclusive, which distributes our solutions to a large group of resellers and end-customers, acquired Fine Tec U.S. Since the acquisition of Fine Tec U.S., Exclusive's business with us has increased and may continue to increase in the future. The two channel partners together accounted for 35% of our total net accounts receivable as of December 31, 2017 and 25% of our total revenue during 2017. In the fourth quarter of 2017, the combined Exclusive/Fine Tec U.S. entity accounted for 30% of our total revenue. During 2015 and 2016, Exclusive accounted for 18% and 20% of our total revenue, respectively.

In addition, any new sales channel partner will require extensive training and may take several months or more to achieve productivity. Our channel partner sales structure could subject us to lawsuits, potential liability and reputational harm if, for example, any of our channel partners misrepresent the functionality of our products or services to end-customers or our channel partners violate laws or our corporate policies. We depend on our global channel partners to comply with applicable legal and regulatory requirements. To the extent that they fail to do so, that could have a material adverse effect on our business, operating results and financial condition. If we fail to optimize our channel partner model or fail to manage existing sales channels, our business will be seriously harmed.

Actual, possible or perceived defects or vulnerabilities in our products or services, the failure of our products or services to prevent a virus or security breach or the misuse of our products could harm our reputation and divert resources.

Because our products and services are complex, they have contained and may contain defects or errors that are not detected until after their commercial release and deployment by our customers. Defects or vulnerabilities may impede or block network traffic, cause our products or services to be vulnerable to electronic break-ins or cause them to fail to help secure networks. Different customers deploy and use our products in different ways, and certain deployments and usages may subject our products to adverse conditions that may negatively impact the effectiveness and useful lifetime of our products. Our networks and products, including cloud-based technology and subscriptions, could be targeted by attacks specifically designed to disrupt our business and harm our reputation. We cannot ensure that our products will prevent all security threats. Because the techniques used by computer hackers to access or sabotage networks change frequently and generally are not recognized until launched against a target, we may be unable to anticipate these techniques. In addition, defects or errors in our FortiGuard security subscription updates or our FortiGate appliances could result in a failure of our FortiGuard security subscription services to effectively update

end-customers' FortiGate appliances and cloud-based products and thereby leave customers vulnerable to attacks. Furthermore, our solutions may also fail to detect or prevent viruses, worms or similar threats due to a number of reasons such as the evolving nature of such threats and the continual emergence of new threats that we may fail to add to our FortiGuard databases in time to protect our end-customers' networks. Our FortiGuard or FortiCare data centers and networks may also experience technical failures and downtime, and may fail to distribute appropriate updates, or fail to meet the increased requirements of our customer base. Any such technical failure, downtime or failures in general may temporarily or permanently expose our end-customers' networks, leaving their networks unprotected against the latest security threats.

An actual, possible or perceived security breach or infection of the network of one of our end-customers, regardless of whether the breach is attributable to the failure of our products or services to prevent the security breach, could adversely affect the market's perception of our security products and services and, in some instances, subject us to potential liability that is not contractually limited. We may not be able to correct any security flaws or vulnerabilities promptly, or at all. Our products may also be misused by end-customers or third parties who obtain access to our products. For example, our products could be used to censor private access to certain information on the internet. Such use of our products for censorship could result in negative

Table of Contents

press coverage and negatively affect our reputation, even if we take reasonable measures to prevent any improper shipment of our products or if our products are provided by an unauthorized third party. Any actual, possible or perceived defects, errors or vulnerabilities in our products, or misuse of our products, could result in:

- the expenditure of significant financial and product development resources in efforts to analyze, correct, eliminate or work around errors or defects or to address and eliminate vulnerabilities;
- the loss of existing or potential end-customers or channel partners;
- delayed or lost revenue;
- delay or failure to attain market acceptance;
- negative publicity and harm to our reputation; and
- litigation, regulatory inquiries or investigations that may be costly and harm our reputation and, in some instances, subject us to potential liability that is not contractually limited.

Our business and operations have experienced growth, and if we do not appropriately manage any future growth, including through the expansion of our real estate holdings, or are unable to improve our systems and processes, our operating results will be negatively affected.

Our business has grown over the last several years. We rely heavily on information technology and accounting systems to help manage critical functions such as order processing, revenue recognition, financial forecasts, inventory and supply chain management and trade compliance reviews. Certain of these systems were developed by us for our internal use and, as such, may have a higher risk of failure or not receive the same level of support as systems purchased from and supported by external technology companies. In addition, we have been slow to adopt and implement certain automated functions, which could have a negative impact on our business. For example, a large part of our order processing relies on manual data entry of customer purchase orders received through email and, to a lesser extent, through electronic data interchange from our customers. Combined with the fact that we may receive a large amount of our orders in the last few weeks of any given quarter, an interruption in our email service or other systems could result in delayed order fulfillment and decreased billings and revenue for that quarter.

To manage any future growth effectively, we must continue to improve and expand our information technology and financial, operating and administrative systems and controls, and continue to manage headcount, capital and processes in an efficient manner. We may not be able to successfully implement requisite improvements to these systems, controls and processes, such as system capacity, access and change management controls, in a timely or efficient manner. Our failure to improve our systems and processes, or their failure to operate in the intended manner, whether as a result of the significant growth of our business or otherwise, may result in our inability to manage the growth of our business and to accurately forecast our revenue, expenses and earnings, or to prevent certain losses. Moreover, the failure of our systems and processes could undermine our ability to provide accurate, timely and reliable reports on our financial and operating results and could impact the effectiveness of our internal control over financial reporting. In addition, our systems and processes may not prevent or detect all errors, omissions or fraud. Our productivity and the quality of our products and services may also be adversely affected if we do not integrate and train our new employees quickly and effectively. Any future growth would add complexity to our organization and require effective coordination throughout our organization. Failure to manage any future growth effectively could result in increased costs and harm our results of operations.

We have expanded our office real estate holdings to meet our projected growing need for office space. We purchased office buildings in Ottawa and Burnaby, Canada in 2017, and we have purchased various small buildings adjacent to our Sunnyvale headquarters as we expand our headquarters in Sunnyvale, California. These plans will require significant capital expenditure over the next several years and involve certain risks, including impairment charges and acceleration of depreciation, changes in future business strategy that may decrease the need for expansion (such as a decrease in headcount) and, risks related to construction. Future changes in growth or fluctuations in cash flow may also negatively impact our ability to pay for these projects or free cash flow. Additionally, inaccuracies in our projected capital expenditures could negatively impact our business, operating results and financial condition.

Table of Contents

We may experience difficulties maintaining and expanding our ERP and CRM systems.

The maintenance of our ERP and CRM systems has required, and will continue to require, the investment of significant financial and human resources. In addition, we may choose to upgrade or expand the functionality of our ERP and CRM systems, leading to additional costs. We may also discover deficiencies in our design or maintenance of the ERP or CRM systems that could adversely affect our ability to process orders, ship products, provide services and customer support, send invoices and track payments, fulfill contractual obligations, accurately maintain books and records, provide accurate, timely and reliable reports on our financial and operating results, or otherwise operate our business. Additionally, if the system does not operate as intended, the effectiveness of our internal control over financial reporting could be adversely affected or our ability to assess it adequately could be delayed. Further, we recently implemented new systems to comply with the new revenue recognition standard and may further expand the scope of our ERP and CRM systems. Our operating results may be adversely affected if these upgrades or expansions are delayed or if the systems do not function as intended or are not sufficient to meet our revenue recognition accounting requirements.

If our estimates or judgments relating to our critical accounting policies are based on assumptions that change or prove to be incorrect, our operating results could fall below expectations of securities analysts and investors, resulting in a decline in our stock price.

The preparation of financial statements in conformity with generally accepted accounting principles requires management to make estimates and assumptions that affect the amounts reported in the consolidated 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, as provided in “Management’s Discussion and Analysis of Financial Condition and Results of Operations” in this Annual Report on Form 10-K, the results of which form the basis for making judgments about the carrying values of assets and liabilities that are not readily apparent from other sources. Additionally, in connection with adopting and implementing the new revenue accounting standard, management will make judgments and assumptions based on our interpretation of the new standard. The new revenue standard is principles based and interpretation of those principles may vary from company to company based on their unique circumstances. It is possible that interpretation, industry practice and guidance may evolve as we work toward implementing the new standard. Our operating results may be adversely affected if our assumptions change or if actual circumstances differ from those in our assumptions, which could cause our operating results to fall below the expectations of securities analysts and investors, resulting in a decline in our stock price. Significant assumptions and estimates used in preparing our consolidated financial statements include those related to revenue recognition and sales return reserves, stock-based compensation expense, valuation of inventory, investments, accounting for business combination, goodwill and other long-lived assets, restructuring, accounting for income taxes, and litigation and settlement costs.

We offer retroactive price protection to certain of our major distributors, and if we fail to balance their inventory with end-customer demand for our products, our allowance for price protection may be inadequate, which could adversely affect our results of operations.

We provide certain of our major distributors with price protection rights for inventories of our products held by them. If we reduce the list price of our products, certain distributors receive refunds or credits from us that reduce the price of such products held in their inventory based upon the new list price. Future credits for price protection will depend on the percentage of our price reductions for the products in inventory and our ability to manage the levels of our major distributors’ inventories. If future price protection adjustments are higher than expected, our future results of operations could be materially and adversely affected.

19

Table of Contents

Because we depend on several third-party manufacturers to build our products, we are susceptible to manufacturing delays that could prevent us from shipping customer orders on time, if at all, and may result in the loss of sales and customers, and third-party manufacturing cost increases could result in lower gross margins and free cash flow.

We outsource the manufacturing of our security appliance products to contract manufacturing partners and original design manufacturing partners including Micro-Star International Co., Ltd., Wistron Corporation, Flex Ltd., Senao Networks, Inc., ADLINK Technology, Inc. and a number of manufacturers located in Taiwan and other countries outside the United States. Our reliance on our third-party manufacturers in Asia and elsewhere reduces our control over the manufacturing process, exposing us to risks, including reduced control over quality assurance and product costs, supply and timing. Any manufacturing disruption by our third-party manufacturers could impair our ability to fulfill orders. If we are unable to manage our relationships with these third-party manufacturers effectively, or if these third-party manufacturers experience delays, increased manufacturing lead-times, disruptions, capacity constraints or quality control problems in their manufacturing operations, or fail to meet our future requirements for timely delivery, our ability to ship products to our customers could be impaired and our business would be seriously harmed.

These manufacturers fulfill our supply requirements on the basis of individual purchase orders. We have no long-term contracts or arrangements with our third-party manufacturers that guarantee capacity, the continuation of particular payment terms or the extension of credit limits. Accordingly, they are not obligated to continue to fulfill our supply requirements, and the prices we are charged for manufacturing services could be increased on short notice. If we are required to change third-party manufacturers, our ability to meet our scheduled product deliveries to our customers would be adversely affected, which could cause the loss of sales and existing or potential customers, delayed revenue or an increase in our costs, which could adversely affect our gross margins. Our individual product lines are generally manufactured by only one manufacturing partner. Any production or shipping interruptions for any reason, such as a natural disaster, epidemic, capacity shortages, quality problems or strike or other labor disruption at one of our manufacturing partners or locations or at shipping ports or locations, would severely affect sales of our product lines manufactured by that manufacturing partner. Furthermore, manufacturing cost increases for any reason could result in lower gross margins.

Our proprietary SPU, which is the key to the performance of our appliances, is built by contract manufacturers including Faraday, MegaChips Corporation and Renesas. These contract manufacturers use foundries operated by UMC, TSMC or Renesas on a purchase-order basis, and these foundries do not guarantee their capacity and could reject orders or increase their pricing. Accordingly, the foundries are not obligated to continue to fulfill our supply requirements, and due to the long lead time that a new foundry would require, we could suffer temporary or long-term inventory shortages of our SPU as well as increased costs. In addition to our proprietary SPU, we also purchase off-the-shelf ASICs from vendors for which we have experienced, and may continue to experience, long lead times. Our suppliers may also prioritize orders by other companies that order higher volumes or more profitable products. If any of these manufacturers materially delays its supply of ASICs or specific product models to us, or requires us to find an alternate supplier and we are not able to do so on a timely and reasonable basis, or if these foundries materially increase their prices for fabrication of our ASICs, our business would be harmed.

In addition, our reliance on third-party manufacturers and foundries limits our control over environmental regulatory requirements such as the hazardous substance content of our products and therefore our ability to ensure compliance with the Restriction of Hazardous Substances Directive (the “EU RoHS”) adopted in the European Union (the “EU”) and other similar laws. It also exposes us to the risk that certain minerals and metals, known as “conflict minerals,” that are contained in our products have originated in the Democratic Republic of the Congo or an adjoining country. As a result of the passage of the Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010 (“Dodd-Frank”), the SEC adopted disclosure requirements for public companies whose products contain conflict minerals that are necessary to the functionality or production of such products. Under these rules, we are required to obtain sourcing data from suppliers, perform supply chain due diligence, and file annually with the SEC a specialized disclosure report

on Form SD covering the prior calendar year. Although the SEC has provided guidance with respect to a portion of the conflict minerals filing requirements that somewhat reduced the reporting required, we have incurred and expect to incur additional costs to comply with the rules, including costs related to efforts to determine the origin, source and chain of custody of the conflict minerals used in our products and the adoption of conflict minerals-related governance policies, processes and controls. Moreover, the implementation of these compliance measures could adversely affect the sourcing, availability and pricing of materials used in the manufacture of our products to the extent that there may be only a limited number of suppliers that are able to meet our sourcing requirements. There can be no assurance that we will be able to obtain such materials in sufficient quantities or at competitive prices. We may also encounter customers who require that all of the components of our products be certified as conflict-free. If we are not able to meet customer requirements, such customers may choose to not purchase our products, which could impact our sales and the value of portions of our inventory.

Table of Contents

Because some of the key components in our products come from limited sources of supply, we are susceptible to supply shortages, long lead times for components, and supply changes, each of which could disrupt or delay our scheduled product deliveries to our customers, result in inventory shortage, cause loss of sales and customers or increase component costs resulting in lower gross margins and free cash flow.

We and our contract manufacturers currently purchase several key parts and components used in the manufacture of our products from limited sources of supply. We are therefore subject to the risk of shortages and long lead times in the supply of these components and the risk that component suppliers discontinue or modify components used in our products. We have in the past experienced, and are currently experiencing, shortages and long lead times for certain components. Certain of our limited source components for particular appliances and suppliers of those components include: specific types of CPUs from Intel, network chips from Broadcom, Marvell and Intel, and memory devices from Intel, ADATA, OCZ, Samsung and Western Digital. We also may face shortages in the supply of the capacitors and resistors that are used in the manufacturing of our products. The introduction by component suppliers of new versions of their products, particularly if not anticipated by us or our contract manufacturers, could require us to expend significant resources to incorporate these new components into our products. In addition, if these suppliers were to discontinue production of a necessary part or component, we would be required to expend significant resources and time in locating and integrating replacement parts or components from another vendor. Qualifying additional suppliers for limited source parts or components can be time-consuming and expensive.

Our manufacturing partners have experienced long lead times for the purchase of components incorporated into our products. Lead times for components may be adversely impacted by factors outside of our control, such as natural disasters and other factors. Our reliance on a limited number of suppliers involves several additional risks, including: