FORTINET INC
Form 10-K
March 02, 2015
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, 2014
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, or a smaller reporting company. See the definitions of "large accelerated filer," "accelerated filer" and "smaller reporting 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

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, 2014, the last business day of the registrant's most recently completed second quarter, was $3,163,303,736 (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 20, 2015, there were 168,865,460 shares of the registrant's common stock outstanding.

DOCUMENTS INCORPORATED BY REFERENCE

Portions of the registrant's definitive Proxy Statement relating to its 2015 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 ("SEC") 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 Fiscal Year Ended December 31, 2014
Table of Contents

Table of Contents

Part I

ITEM 1. Business

Overview

We provide high performance cyber security solutions to some of the largest enterprise, service providers and government organizations across the globe, including a majority of the 2014 Fortune 100. Our cyber security solutions are fast and secure and designed to provide broad, high-performance protection against dynamic security threats while simplifying the information technology ("IT") infrastructure of our end-customers worldwide.

Our flagship integrated network security solution consists of our FortiGate physical and virtual appliance products that provide a broad array of integrated security and networking functions to protect data, applications, and users from network- and content-level security threats. These functions, which can be integrated in a variety of ways, include firewall, intrusion prevention ("IPS") anti-malware, application control, virtual private network ("VPN"), web-filtering, vulnerability management, anti-spam, wireless controller, and wide area network ("WAN") acceleration. Our FortiGate appliances may be deployed as Next Generation Firewalls ("NGFW"), Data Center Firewalls ("DCFW"), Unified Threat Management ("UTM") systems, Internal Network Firewall ("INFW"), Virtual Machine Firewalls or Cloud Firewalls. Our FortiGate appliances range from the FortiGate-20 series for small businesses and branch offices to the FortiGate-5000 series for large enterprises and service providers, and are based on our proprietary technology platform. This platform includes our FortiASICs, which are specifically designed for accelerated processing of security and networking functions, and our FortiOS operating system, which provides the foundation for all FortiGate security functions. Our FortiGuard security subscription services provide end-customers with access to dynamic updates to our application control, anti-malware, intrusion prevention, web filtering, and anti-spam functionality. Our security services are based on intelligence gathered by our FortiGuard Labs team, which is comprised of a large team of threat researchers who detect threats and help protect our customers. By combining multiple proprietary security and networking functions with our purpose-built FortiASIC and FortiOS, our FortiGate solution delivers broad protection against dynamic security threats while reducing the operational burden and costs associated with managing multiple point products.

We complement our FortiGate product line with the FortiManager product family, which enables end-customers to manage the system configuration and security functions of multiple FortiGate devices from a centralized console, as well as the FortiAnalyzer product family, which enables collection, analysis and archiving of content and log data generated by our products. We also offer other product lines that provide additional protection, such as:

- FortiAP, secure wireless access points;
- FortiWeb, security for web-based applications;
- FortiMail, multi-feature, high performance messaging security;
- FortiDB, centrally managed database-specific security;
- FortiClient, endpoint security for desktops, laptops and mobile devices which is primarily used in conjunction with our FortiGate appliances;
- FortiScan, endpoint vulnerability assessment and remediation;
- FortiSwitch, Ethernet switches;
- FortiBridge, bypass appliances to help ensure network availability;
- FortiAuthenticator, scalable secure authentication for enterprise networks;
- FortiADC, Application Delivery Controller ("ADC") optimizing the availability and performance of mobile, cloud, and enterprise applications;
- FortiSandbox, detecting and mitigating Advanced Persistent Threats ("APTs");
- FortiCache, reducing the cost of and impact of cached internet content;
- FortiDNS, providing secure Domain Name System ("DNS") caching;

- FortiDDoS, protection against Distributed Denial of Service ("DDOS") attacks; and
- FortiVoice, business telephone communication.

We offer virtual appliances for the FortiGate, FortiManager, FortiAnalyzer, FortiWeb, FortiMail, FortiCache, and FortiADC product lines that can be used in conjunction with traditional Fortinet physical appliances, such as FortiGate, FortiManager, and FortiAnalyzer, to help ensure the visibility, management, and protection of physical and virtual environments. We also offer on-demand cloud-based versions of FortiGate and FortiWeb.

During our fiscal year ended December 31, 2014, we generated total revenue of $770.4 million and net income of $25.3 million. See Part II, Item 8 of this Annual Report on Form 10-K for more information on our consolidated balance sheets as of

Table of Contents

December 31, 2014 and 2013 and our consolidated statements of operations, comprehensive income, stockholders' equity, and cash flows for each of the three years ended December 31, 2014, 2013, and 2012.

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 FortiASIC hardware architecture, FortiOS operating system and associated security and networking functions combine to form a platform that integrates security features and enables our products to perform sophisticated security processing for networks with high throughput requirements.

FortiASIC

Our proprietary FortiASIC family of Application-Specific Integrated Circuits ("ASICs") is comprised of three lines of processors: the FortiASIC content processor ("CP"), the FortiASIC network processor ("NP"), and the FortiASIC system-on-a-chip ("SOC"). Our custom ASICs are designed to enhance the sophisticated security processing capabilities implemented in software by accelerating computation-intensive tasks such as firewall policy enforcement or IPS anomaly detection. This architecture provides the flexibility of implementing accelerated processing of new threat detection without requiring a new ASIC. The FortiASIC CP is currently included in most of our entry-level and all of our mid-range and high-end FortiGate appliances. The FortiASIC 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 (FortiGate 20 to 100 series) often use the SOC2. Mid-range FortiGate products (FortiGate 200 to 800 series) use a central processing unit ("CPU") and include the NP and CP. The high-end FortiGate products (FortiGate 1000 to 5000 series) use multiple CPUs, CPs and NPs.

FortiOS

Our proprietary FortiOS operating system provides the foundation for the operation of all FortiGate appliances, from the core kernel functions to the security processing feature sets. 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 ASICs and provides system management functions such as command-line and graphical user interfaces.

Key high-level functions and capabilities of FortiOS include:

- helping enable FortiGate appliances to be configured into different security environments such as our Internal Network Firewall, Next Generation Firewall, and the Data Center Firewall;
- configuration of the physical aspects of the appliance such as ports, Wi-Fi and switching;
- key network functions such as routing and deployment modes (network routing, transparent, sniffer, etc.);
- implementation of security updates delivering advanced threat protection, such as IPS, antivirus, and application control;
- access to cloud-based web and email filtering databases;
- security policy objects and enforcement;
- data leak prevention and document finger printing; and
- real-time reporting and logging.

We make updates to FortiOS available through our FortiCare technical support services. 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 address translation technologies, allowing the FortiGate appliance to integrate and operate in a wide variety of network environments. Additional features include Virtual Domain ("VDOM"), capabilities and traffic queuing and shaping. These features enable administrators to set the appropriate configurations and policies that meet their infrastructure needs. FortiOS also provides capabilities for logging of traffic for forensic analysis purposes which are particularly important for regulatory compliance initiatives like payment card industry data security standard ("PCI DSS"). 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.

Table of Contents

Products

Our core product offerings consist of our FortiGate product family, along with our FortiManager central management and FortiAnalyzer central logging and reporting product families, both of which are typically purchased to complement a large FortiGate deployment.

FortiGate

Our flagship FortiGate physical and virtual appliances 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. Substantially all of the FortiGate physical appliances include our FortiASICs to accelerate content and network security features implemented within FortiOS. 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 up to thousands of FortiGate physical and virtual appliances.

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 mid-sized businesses, large enterprises, service providers and government organizations worldwide.

Each FortiGate model runs on our FortiOS operating system, and substantially all FortiGate physical appliances include our FortiASICs. 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 mid-sized businesses. The FortiGate-200 through -800 series models are designed for perimeter deployment in mid-sized to large enterprise networks. And, the FortiGate-1000 through -5000 series models deliver high performance and scalable network security functionality for perimeter, data center and core deployment in large enterprise and service provider networks.

We also incorporate additional technologies within FortiGate appliances that differentiate our solutions, including data leakage protection (“DLP”), traffic optimization, SSL inspection, threat vulnerability management, and wireless controller technology.

Fortinet Management and Analysis Products

Our FortiManager and FortiAnalyzer physical and virtual products are typically sold in conjunction with a large FortiGate deployment.

FortiManager. Our FortiManager family of products provides a central management solution for our FortiGate products, including the wide variety of network and security features offered within FortiOS. One FortiManager product is capable of managing thousands of FortiGate units, and also provides central management for FortiClient software. 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 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.

We also offer other physical and virtual appliances and software that protect our end-customers from security threats to other critical areas in the enterprise, such as messaging, web-based applications and databases, and employees' computers or mobile devices.

Services

FortiGuard Security Subscription Services

Security requirements are dynamic due to the constantly changing nature of threats. Our FortiGuard Labs global threat research team uses automated and manual processes to identify emerging threats, collects threat samples, and FortiGuard Labs replicates, reviews and characterizes attacks. Based on this research, we develop updates for virus signatures, attack definitions,

Table of Contents

scanning engines, and other security solution components to distribute to end-customers. Our FortiGuard security subscription services are designed to allow us to quickly deliver new threat detection capabilities to end-customers worldwide as new threats evolve. End-customers purchase FortiGuard security subscription services in advance, typically with terms of one to three 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 anti-spam functions for our FortiClient software; antivirus and anti-spam functions for our FortiMail products; vulnerability management for our FortiGate, FortiAnalyzer and FortiScan products, database functions for our FortiDB appliance, web functions for our FortiWeb appliances, and advanced threat protection for our FortiSandbox products. We provide FortiGuard services 24 hours a day, seven days a week.

FortiCare Technical Support Services

Our FortiCare services are our technical support services for the software, firmware and hardware in our products, as well as our extended product warranty service. In addition to our standard support service offering, we offer a premium service that offers faster response times and dedicated support oriented towards mission-critical applications.

For our standard technical support offering for our products, channel partners often provide first level support to the end-customer, especially for small and mid-sized end-customers, and we typically provide second and third level support to our end-customers. 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.

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 to help ensure an understanding of our products and services.

Professional Services

We offer professional services to end-customers primarily for large implementations where expert technical resources are required. 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, attack simulation software and scripts.

Customers

We sell our security solutions through channel partners to end-customers of various sizes—from small businesses to large enterprises, government organizations, and service providers—and across a variety of industries including telecommunications, technology, government, financial services, education, retail, manufacturing, and healthcare for a variety of security functions across a variety of deployment scenarios. An end-customer deployment may involve one of our appliances or thousands, depending on our end-customers' size and security requirements. Many of our customers also purchase our FortiGuard security subscription services and FortiCare technical support services. For information regarding our sales by customer location, see Note 14 to our consolidated financial statements in Part II, Item 8 of this Annual Report on Form 10-K.

During fiscal 2014, fiscal 2013, and fiscal 2012, one distributor, Exclusive Networks Group, which distributed our solutions to a large group of resellers and end-customers, accounted for 15%, 12%, and 11% of total revenue, respectively.

Sales and Marketing

We primarily sell our products and services directly 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, very large service providers and major systems integrator partners who have large purchasing power and unique customer deployment demands. We work with many of the world's leading technology distributors, including Exclusive Networks Group, Ingram Micro Inc., Fine Tec Computer, and Arrow Electronics, Inc and enterprise security-focused resellers including Accuvant and Fishnet Security.

We support our channel partners with a 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 team often helps drive and support large enterprise and service provider sales through a direct touch model. Our sales

Table of Contents

professionals and engineers typically work closely with our channel partners and directly engage with large end-customers to help address their unique security and deployment requirements. Our sales cycle for an initial end-customer purchase typically ranges from three to six months but can be longer especially for large enterprises, service providers and government organizations. To support our broadly dispersed global channel and end-customer base, we have sales offices in over 30 countries around the world.

Our marketing strategy is focused on building our brand and driving end-customer demand for our security solutions. We execute this strategy by leveraging a combination of internal marketing professionals and a network of regional and global channel partners. Our internal marketing organization is responsible for messaging, branding, product marketing, channel marketing, event marketing, communications and sales support programs. We focus our resources on programs, tools 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 fiscal 2014, we invested in sales and marketing to capture market share, particularly in the enterprise market where enterprise customers tend to have a higher lifetime value, and to accelerate our growth. We intend to continue investing in sales and marketing in order to capture additional market share in the high-return enterprise market, which we believe also offers higher lifetime value.

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 Flextronics International Ltd., Micro-Star International Co., Ltd., Adlink Technology, Inc., Senao Networks, Inc., and a number of Taiwan-based manufacturers. 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 headquarters in Sunnyvale, 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 FortiASICs, which are the key to the performance of our appliances, are fabricated by contract manufacturers in foundries operated by United Microelectronics Corporation (“UMC”) and Taiwan Semiconductor Manufacturing Company Limited (“TSMC”). Faraday Technology Corporation (using UMC’s foundry), Kawasaki Microelectronics America, Inc. (“K-Micro”) (using TSMC’s foundry) and Renesas Electronics Corporation (“Renesas”) (using UMC’s foundry) manufacture our ASICs on a purchase order basis. Accordingly, they are not obligated to continue to fulfill our supply requirements, and the prices we are charged for the fabrication of our ASICs could be increased on short notice.

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 central processing units from Intel Corporation (“Intel”), network chips from Broadcom Corporation (“Broadcom”), Marvell Technology Group Ltd. (“Marvell”) and Intel, and solid-state drives (silicon-based storage device) from OCZ Technology Group, Inc. and Samsung Electronics Co., Ltd., 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 systems, and adding new features to existing products and systems. 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 $122.9 million in fiscal 2014, $102.7 million in fiscal 2013 and $81.1 million in fiscal 2012.

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, 2014, we had 191 issued U.S. and foreign patents and 156 pending U.S.

Table of Contents

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 “—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.

Our competitors include Cisco Systems, Inc. (“Cisco”), Juniper Networks, Inc. (“Juniper”), Check Point Software Technologies Ltd. (“Check Point”), Intel (through its acquisition of McAfee, Inc. (“McAfee”)), F5 Networks, Inc. (“F5 Networks”), Dell Inc. (through its acquisition of SonicWALL, Inc. (“SonicWALL”) , BlueCoat Systems, Inc. (“BlueCoat”), FireEye, Inc. (“FireEye”) and Palo Alto Networks, Inc. (“Palo Alto Networks”), amongst others.

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.

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, are in a better position to withstand any significant reduction in capital spending by end-customers in these markets,

Table of Contents

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, 2014, our total headcount was 2,854 full-time equivalent employees. None of our U.S. employees are represented by a labor union; however, our employees in Belgium, Finland, France, Italy, and Spain are represented by collective bargaining agreements. 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, and investors may lose some or all of their investment.

Risks Related to Our Business

Our quarterly 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 and may be difficult to predict, including:

- 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 many factors such as inventory levels, logistics, shipping delays at ports or otherwise, our ability to ship new products on schedule and to accurately forecast inventory requirements, and potential delays in the manufacturing process;
- inventory imbalances, such as those related to new products and the end of life of existing products;