SOURCEFIRE INC
Form 10-K
February 28, 2013

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

FORM 10-K
(Mark One)

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

FOR THE FISCAL YEAR ENDED DECEMBER 31, 2012

.. 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 1-33350
SOURCEFIRE, INC.
(Exact name of Registrant as Specified in its Charter)

Delaware (State or Other Jurisdiction of Incorporation or Organization)	52-2289365 (I.R.S. Employer Identification No.)
9770 Patuxent Woods Drive Columbia, Maryland (Address of Principal Executive Offices)	21046 (Zip Code)

Registrant's telephone number, including area code: (410) 290-1616
Securities registered pursuant to Section 12(b) of the Act:

Title of Each Class	Name of Exchange on Which Registered
Common Stock, $0.001 par value, including associated Series A Junior Participating Preferred Stock Purchase Rights	NASDAQ Global Select Market

Securities registered pursuant to Section 12(g) of the Act:
none
Indicate by check mark if the registrant is a well-known seasoned issuer, as defined in Rule 405 of the Securities Act. Yes ¨ No ý
Indicate by check mark if the registrant is not required to file reports pursuant to Section 13 or Section 15(d) of the Act. Yes ¨ No ý
Indicate by check mark whether the registrant: (1) has filed all reports required to be filed by Section 13 or 15(d) of the Securities Exchange Act of 1934 during the preceding 12 months (or for such shorter period that the registrant was required to file such reports), and (2) has been subject to such filing requirements for the past 90 days. Yes ý No ¨
Indicate by check mark whether the registrant has submitted electronically and posted on its corporate Web site, 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 ý No ¨
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 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. ý

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 definitions of "large accelerated filer," "accelerated filer," and "smaller reporting company" in Rule 12b-2 of the Exchange Act.

Large Accelerated Filer	ý	Accelerated Filer	¨
Non-Accelerated Filer	(Do not check if smaller reporting company)	Smaller reporting company	¨

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

As of June 30, 2012, the aggregate market value of the registrant's Common Stock held by non-affiliates, based upon the closing sale price of the Common Stock on the NASDAQ Global Select Market on such date, was approximately $1.5 billion.

As of February 22, 2013, there were 30,670,141 outstanding shares of the registrant's Common Stock.

DOCUMENTS INCORPORATED BY REFERENCE

Certain portions of the definitive Proxy Statement to be used in connection with the registrant's 2013 Annual Meeting of Stockholders are incorporated by reference into Part III of this Form 10-K to the extent stated. That Proxy Statement will be filed within 120 days of registrant's fiscal year ended December 31, 2012.

SOURCEFIRE, INC.
Form 10-K
TABLE OF CONTENTS

References in this Annual Report on Form 10-K to “Sourcefire,” “we,” “us,” “our” or “the Company” refer to Sourcefire, Inc. and its subsidiaries, taken as a whole, unless a statement specifically refers to Sourcefire, Inc.

FORWARD-LOOKING STATEMENTS

This annual report contains both historical and forward-looking statements. All statements other than statements of historical fact are, or may be deemed to be, forward-looking statements. For example, statements concerning projections, predictions, expectations, estimates or forecasts and statements that describe our objectives, plans or goals are or may be forward-looking statements. These forward-looking statements reflect management's current expectations concerning future results and events and generally can be identified by use of expressions such as “may,” “will,” “should,” “could,” “would,” “predict,” “potential,” “continue,” “expect,” “anticipate,” “future,” “intend,” “plan,” “fores “estimate,” and similar expressions, as well as statements in future tense. These forward-looking statements include, but are not limited to, the following:

- expected growth in the markets for cybersecurity products and solutions;
- our plans to continue to invest in and develop innovative technology and products for our existing markets and other security markets;
- the timing of expected introductions of new or enhanced products and solutions;
- our expectation of growth in our customer base and increasing sales to existing customers;
- our plans to increase revenue through additional relationships with resellers, distributors, managed security service providers, government integrators and other partners;
- our plans to grow international sales;
- our plans to acquire and integrate new businesses and technologies;
- our plans to hire more security professionals and broaden our knowledge base; and
- our plans to hire additional sales personnel and the additional revenue we expect them to generate.

The forward-looking statements included in this annual report are made only as of the date of this annual report. We expressly disclaim any intent or obligation to update any forward-looking statements to reflect subsequent events or circumstances. Forward-looking statements involve known and unknown risks, uncertainties and other factors that may cause our actual results, performance or achievements to be different from any future results, performance and achievements expressed or implied by these statements. These risks and uncertainties include, but are not limited to, those discussed in Item 1A. Risk Factors of this annual report, as well as in Item 1. Business and Item 7. Management's Discussion and Analysis of Financial Condition and Results of Operations.

Sourcefire, the Sourcefire logo, Snort, the Snort and Pig logo, ClamAV, FireAMP, FirePOWER, FireSIGHT, Agile Security and certain other trademarks and logos are trademarks or registered trademarks of Sourcefire, Inc. in the United States and other countries. This annual report also refers to the products or services of other companies or persons by the trademarks and trade names used and owned by those companies or persons.

PART I

Item 1. BUSINESS

Overview

Sourcefire delivers intelligent cybersecurity technologies. Our comprehensive portfolio of solutions enables commercial enterprises and government agencies worldwide to manage and minimize cybersecurity risks. From our industry-leading next-generation network security platform to our advanced malware protection, Sourcefire provides customers with Agile Security® that addresses the need for more informed, adaptive, and automated security solutions to protect today's dynamic information technology environments from constantly changing threats.

We sell our solutions to a diverse customer base that includes Global 2000 companies, global enterprises, U.S. and international government agencies and small and mid-size businesses. For the years ended December 31, 2012, 2011 and 2010, we generated approximately 67%, 75%, and 75% of our revenue from customers in the United States and 33%, 25%, and 25% from customers outside of the United States, respectively. We increased our total revenue from $165.6 million in 2011 to $223.1 million in 2012, representing an annual growth rate of 35%. For the year ended December 31, 2012, product revenue and services revenue represented 61% and 39% of our total revenue, respectively. We manage our operations on a consolidated basis for purposes of assessing performance and making operating decisions. Accordingly, we do not have reportable segments of our business.

Business Developments

Product Enhancements and New Product Markets

During 2012, we enhanced our core next-generation intrusion prevention system, or NGIPS, products and our next-generation firewall, or NGFW, products. In addition, we entered the advanced malware protection market with the launch of a new set of solutions. This included the introduction of:

- Sourcefire 8290, 8270, & 7000 Series FirePOWER™ Appliances - the addition of these new models gives the FirePOWER Appliance family a performance range from 50 Mbps to 40+ Gbps of inspected throughput.

- Sourcefire Virtual Next-Generation IPS with Application Control - provides advanced threat protection for virtualized environments along with application control, URL filtering and a virtual management console.

- Sourcefire FireAMP® - an intelligent, enterprise-class malware discovery and analysis solution that analyzes and blocks malware through big data analytics.

- Sourcefire FireAMP Mobile - a mobile device security product that identifies and remediates advanced malware using big data analytics.

- Sourcefire FireAMP Virtual - protects VMware virtual instances from advanced malware and stops threats that bypass other security layers.

- Advanced Malware Protection for FirePOWER - a comprehensive malware protection solution for networks that enables detection and blocking, continuous analysis and retrospective alerting and leverages cloud security intelligence.

Sales Channel Expansion

In 2012, we expanded our indirect sales channel by:

- Increasing the number of partners in our indirect sales channel from 576 at December 31, 2011 to 738 at December 31, 2012.
- Increasing the number of partner employees certified on our products from 343 at December 31, 2011 to 648 at December 31, 2012.

2

Our Industry

We expect that demand for enterprise network security equipment will continue to rise as organizations seek to address various growing and evolving security challenges, including:

Increasing Change of IT environments. Consumerization (bring your own device to work, or BYOD), mobilization, and virtualization are driving changes in IT environments and the rate of change is increasing. These trends have extended the network to include endpoints, mobile and virtual and spawned new attack vectors including web-enabled and mobile applications, hypervisors, social media and browsers. Malware writers are leveraging these attack vectors to access identity data, trade and classified secrets, intellectual property, and critical infrastructure.

Greater Sophistication, Severity and Frequency of Attacks. In contrast to the hobbyist hackers of the past, the last five years have seen “Industrialization of Hacking” which has spurred more menacing attacks. Today’s attackers are motivated by financial gain, theft of intellectual property and malicious disruption. These motivated attackers are employing much more sophisticated tools and techniques to generate profits for themselves and their well-organized and well-financed sponsors, including organized crime and nation states. Their attacks are increasingly difficult to detect and their tools often establish command and control points on compromised network assets with little or no discernible effect, facilitating future access to the assets, the data, and the networks on which they reside.

Diverse Demands on Security Administrators. Targeted security solutions such as firewalls, intrusion prevention systems, URL filters, spam filters and advanced malware protection are critical layers to enhancing security. However, they can create significant administrative burdens on personnel who must manage numerous disparate technologies that are seldom integrated and often difficult to use. Most security products require manual, labor-intensive incident response and investigation by security administrators, especially when “false positive” results are generated. Compounding these resource constraint issues, many organizations are increasingly challenged by the loss of key personnel as the demand for security experts has risen dramatically in traditional corporate settings, government agencies and a growing number of start-up security companies.

Heightened Government and Industry Regulation. Rapidly increasing government regulation mandates compliance with increased security requirements, escalating demand for solutions that both meet compliance requirements and reduce the burden of compliance reporting and enforcement. These regulations include the Payment Card Industry Data Security Standard, or PCI DSS, the Health Insurance Portability and Accountability Act of 1996, or HIPAA, as well as the Sarbanes-Oxley Act of 2002 for risk management and the Federal Information Security Management Act, or FISMA, which is designed to protect national defense initiatives.

Our Vision

Due to the increasingly sophisticated and evolving nature of cybersecurity challenges, Sourcefire believes that the approach to cybersecurity must also evolve. The best solutions must be agile, based on a continuous process and supported by advanced technologies to better detect, analyze, prevent and remediate these attacks. Sourcefire calls this vision Agile Security.

Sourcefire’s Agile Security vision drives the innovation of our technology and solutions. This vision reflects the realities of today’s network and computer security disciplines and is grounded in four essential elements:

See .....Clarity and vision, reflecting the who, what, where reality of an environment, as it exists right now.

Learn ...Applying intelligence to raw data to improve understanding and decision-making.

Adapt ...Automatic evolution and modification of defenses in response to change.

Act .....Decisive, flexible, and automated responses to events.

Through a continuous process of See, Learn, Adapt and Act, solutions that enable Agile Security can deliver effective protection because they have the ability to respond to continuous change.

Our Approach

Given increasingly sophisticated, targeted and relentless attacks, Agile Security must span the full attack continuum - before, during and after an attack. Before an attack, defenders need comprehensive awareness and visibility of their extended network environment in order to implement appropriate policies and controls to defend it. During an attack, the ability to continuously detect the nature of the threat and block it is critical. After a successful attack, defenders need retrospective security to marginalize the impact of the attack by determining the scope of the attack, containing the threat, eliminating the risk of re-infection, and remediating the damage.

Sourcefire's portfolio of integrated solutions that span the network, endpoints, mobile and virtual as well as technologies that include big data analytics and cloud-based security intelligence, address the full attack continuum.

Our Products

Sourcefire’s portfolio of solutions and technologies designed to deliver Agile Security is comprised of hardware with embedded software, software and cloud-based solutions.

Network Security

The foundation for our network security solutions, our FirePOWER platform is a family of high-performance, energy-efficient, network security appliances with flexible deployment options that include NGIPS, NGFW and Advanced Malware Protection. Customers can enable the level of functionality required.

- Sourcefire NGIPS (Next Generation Intrusion Prevention System) – Sourcefire’s NGIPS uses a flexible rules-based language for advanced threat protection. Sourcefire appliances equipped with Sourcefire NGIPS software can be placed in passive intrusion detection, or IDS, mode to notify users of network traffic or in inline mode to block threats. Our FireSIGHT® awareness technology provides real-time contextual awareness and full stack visibility. Intelligent security automation reduces the total cost of ownership and enables continuous security.

- Sourcefire NGFW (Next Generation Firewall) – Sourcefire's NGFW offers application control integrated with Sourcefire’s industry-leading NGIPS and firewall capabilities in a universal, high-performance security appliance. The solution is designed to bring together control and effective prevention in a flexible, high-performance agile engine to satisfy the larger need for complete enterprise visibility, adaptive security, and advanced threat protection.

- Optional security licenses – includes Application Control for detailed control of client and web based applications; URL Filtering for filtering of URL's by site or reputation; and Advanced Malware Protection for FirePOWER to detect and block malware on the network.

- Sourcefire SSL Appliance – The Sourcefire SSL Appliance decrypts SSL traffic for inspection by network security appliances, allowing security teams to eliminate blind spots and monitor SSL traffic for embedded attacks and data leakage.

- Sourcefire Virtual Appliance – The Sourcefire Virtual Appliance extends our network security capabilities to environments where physical appliances are impractical. Sourcefire offers security solutions for VMware, Citrix (Xen) and Red Hat (KVM) virtual environments. These appliances inspect communications between different virtual machines residing on the same box, providing the same control and protection as their physical counterparts.

Advanced Malware Protection

Today's attackers are taking a comprehensive view of IT environments and using new attack vectors to accomplish their missions to gather data or simply to destroy. Sourcefire has entered the emerging advanced malware protection market with solutions to protect against malware targeting the network, endpoints, mobile and virtual. These solutions can be deployed separately or together for comprehensive coverage and they leverage big data analytics and

cloud-based security intelligence to quickly identify and defeat malware along the full attack continuum.

- FireAMP – FireAMP is an intelligent, enterprise-class advanced malware protection solution that uses big data analytics to discover, understand and block advanced malware outbreaks. FireAMP delivers the visibility and control needed to stop threats missed by other security layers, prevent reinfection and remediate retrospectively. FireAMP Mobile protects against mobile malware. FireAMP Virtual protects against malware targeting virtual machines.

- Advanced Malware Protection for FirePOWER – AMP for FirePOWER provides protection against sophisticated network malware, advanced persistent threats, or APTs, and targeted attacks by enabling continuous visibility, analysis and control before, during and after an attack. Available as standalone solution, or as an add-on subscription license for NGIPS or NGFW, eliminating the need for limited-purpose malware appliances.

Management

Sourcefire Defense Center® – The Defense Center unifies the critical security functions of the Sourcefire next-generation network security platform using FireSIGHT awareness technology to correlate and prioritize event data with network and user awareness. Through this powerful management tool, customers can conduct forensic analysis, trends analysis, reporting and alerting. Customers can control multiple Sourcefire appliances from a single management console while aggregating and analyzing security and compliance events from across the organization. The Defense Center is highly scalable and extensible, providing application programming interfaces, or APIs, to interoperate with a variety of third-party systems, such as firewalls, routers, log management, Security Information Event Management, or SIEMs, trouble ticketing, patch management systems and other technologies. The Sourcefire Virtual Defense Center™ provides the same monitoring and management controls as its physical counterpart. To centrally manage Sourcefire's advanced malware protection solutions, FireAMP Console provides management, deployment, policy configuration and reporting for desktop systems and mobile devices.

Our Open Source Projects

Sourcefire embraces open source technology as a means to fuel collaboration and innovation in the security industry. Marked by accelerated development and a community of experts that continually reviews, tests and proposes improvements, these technologies deliver high-quality, affordable solutions.

Sourcefire manages some of the world’s most respected open source security initiatives, including:

Snort® – The traffic inspection engine used in our intrusion prevention system is the open source technology called Snort. Snort uses a rule-driven language which combines the benefits of signature, protocol, and anomaly-based inspection methods. Snort has become the de facto industry standard for intrusion prevention. We believe that most Fortune 100 companies and 30 of the largest U.S. government agencies use Snort technology to monitor network traffic and that Snort is the most widely deployed intrusion prevention technology worldwide. Because of its wide availability, Snort is also the standard intrusion technology used in colleges and universities worldwide to teach network security.

ClamAV® – ClamAV is one of the most commonly used open source anti-malware products in the world. Renowned for its speed and accuracy, ClamAV has been integrated within leading enterprise solutions to identify deeply embedded threats such as viruses, trojans, spyware and other forms of malware.

Razorback™ Established in August 2010, Razorback is an innovative open-source project that addresses complex threat detection and protection, including deep file inspection and defense coordination. This project is intended to provide enterprise defense teams with an open source detection platform for developing the kinds of detection necessary to combat ‘advanced persistent threats’, or APTs, and client-side attacks in conjunction with their existing security technologies.

Our Services

In addition to our commercial product offerings and open source projects, we also offer the following services to aid our customers and partners with installing and supporting our solutions:

Sourcefire Customer Support – Sourcefire’s customer support is designed to ensure customer satisfaction with Sourcefire products. Sourcefire’s comprehensive support services include online technical support, over-the-phone support, hardware repair and advanced replacement, and ongoing software updates to Sourcefire products.

Sourcefire Professional Services – Sourcefire offers a variety of professional services solutions to provide customers and partners with best practices for planning, installing, configuring and managing all components of the Sourcefire product portfolio and applying the security intelligence gained from Sourcefire products for incident response. The Sourcefire Professional Services Team provides individualized, highly concentrated attention that gives organizations a “running start” and lasting knowledge transfer.

Sourcefire Education & Certification – Sourcefire offers a variety of training programs to use Sourcefire commercial or open source security solutions. Sourcefire training includes instructor-led and custom classes delivered at various locations around the world, onsite at customer premises, and online. Security professionals can achieve certifications for proprietary Sourcefire products as well as open source Snort.

Our Competitive Strengths

We are a leading provider of products and services that support Agile Security, enabling our customers to protect their IT environments in an intelligent, effective, and highly automated manner. Our competitive strengths include:

Advanced Protection. Sourcefire's innovative and industry-leading technologies have been demonstrated, through third party tests, to provide the best protection available against both client-side and server-side attacks. In a world with dynamically evolving threats, targeted attacks, and advanced persistent threats, the ability to customize protection is a requirement. Based on the flexibility of Snort, customers can create their own custom rules and signatures to protect their unique environments.

Comprehensive Network and User Intelligence. Sourcefire's FireSIGHT awareness technology provides real-time persistent visibility into the composition, behavior, topology (the relationship of network components), and risk profile of the network, as well as the correlation of security and network events with specific users. The ability to continuously and passively discover characteristics and vulnerabilities of practically any computing device communicating on a network enables Sourcefire NGIPS and NGFW to more precisely identify and block threatening traffic and to more efficiently classify threatening or suspicious behavior. Correlation and context provide automatic decision-making and automated policy enforcement and tuning to resolve security and compliance events more quickly and easily.

Intelligent Security Automation. Our solutions are designed to adapt to constant change with intelligent automation. Automated impact assessment and policy tuning enable customers to evolve and modify defenses for their unique environment based on intelligence gained before, during and after an attack, despite limited resources or lack of expertise.

Real-Time Approach to Security. Our approach to security enables our customers to secure their environments by providing real-time defense against both known and unknown threats. Our solutions are designed to support a continuum of security functions that span pre-attack hardening of assets, high fidelity attack identification and disruption and real-time compromise detection and incident response. This real-time approach is critical for protection across the full attack continuum.

Retrospective Security. We believe we offer the leading technology able to retrospectively understand the scope of a compromise and deliver actionable intelligence to manually or automatically clean up all affected devices based on customers' specific policies. Because today's advanced malware can disguise itself as safe, pass through defenses unnoticed and later exhibit malicious behavior, this is an important capability to minimize damage after an attack and remediate it.

Leading-Edge Performance. Our solutions are built to maintain high performance across the network while also providing high levels of network security. Specifically, our FirePOWER hardware acceleration technology delivers 10 Gbps of threat inspected throughput with latency in the microseconds, and up to 40 Gbps of threat inspected throughput and up to 80 Gbps throughput of packet filtering when stacked. Our NGIPS technology incorporates advanced traffic processing functionality, including packet acquisition, protocol normalization and target-based traffic inspection, which yields increased inspection precision and efficiency and enables more granular inspection of network traffic. Our next generation network security platform deploys a single-pass, hardware-accelerated design to afford maximum scalability, threat effectiveness, performance and security.

The Open Source Community. Since our founding in 2001, we have been a staunch advocate for open source security solutions. Over the years, this has developed into a key competitive distinction. We manage the security industry's leading open source initiative, Snort, which was first published in 1998 by Sourcefire founder, interim Chief Executive Officer and Chief Technology Officer, Martin Roesch, and has become the de facto standard for intrusion detection and prevention. We also manage the ClamAV and Razorback open source security initiatives. These solutions form the foundation of our commercial product offerings which we extend by including enterprise-class features, manageability, scalability, performance, and support. We believe that the combined open source user communities of Snort, ClamAV and Razorback, along with our collective security intelligence, provide us with significant benefits, including a broad threat intelligence network, significant research and development leverage, and a large pool of security experts that are skilled in the use of our technologies. These communities enable us to more

cost-effectively test new algorithms and concepts on a vast number of diverse networks and significantly expedite the process of product innovation. We believe that the broad acceptance of these products makes us one of the most trusted sources of security solutions.

Security Industry Intelligence. The Sourcefire VRT is a group of leading edge network security experts who proactively discover, assess and respond to the latest trends in hacking activities, intrusion attempts and vulnerabilities. Some of the most renowned security professionals in the industry, including the authors of several standard security reference books, are members of the Sourcefire VRT. This team is also supported by the vast resources of the open source Snort and ClamAV communities and our community of cloud-based users, making it the largest group dedicated to advances in the network security industry. The VRT's research and insights into network security are published on http://vrt-sourcefire.blogspot.com/. Information appearing on this website is not incorporated by reference in and is not a part of this annual report.

Our Growth Strategy

Our goal is to become the preeminent provider of commercial and open source cybersecurity solutions on a global basis by:

- Expanding the breadth of, and our leadership in, security solutions. Sourcefire is expanding its product and service portfolio by creating purpose-built solutions to address specific market and user problems. In 2011 and 2012 we launched two innovative solutions into two adjacent markets – next generation firewalls and advanced malware protection. Over time we expect to further penetrate these and additional markets with innovative products and technologies. By leveraging the intelligence from the open source community, we believe that we have more visibility into threats worldwide, and that we will be able to continue our leadership position in providing users access to the latest information on current threats and ways to protect their organizations against them.

- Growing our international presence. International expansion is a key initiative and we continue to increase our international head count to support our expansion into new territories, to manage our growing network of channel partners and to meet the growing demand for our solutions.

- Expanding relationships with partners, resellers, distributors, MSSPs and government integrators. We intend to expand our indirect sales channel, both internationally and domestically, to create a more leveraged sales model. We have established our Global Security Alliance Channel program to strengthen channel reseller relationships and support them through meaningful programs, including higher margin participation, training, and marketing activities. We are making investments in our partners and our objective is to continue to increase the percentage of channel-influenced revenue.

- Continuing to develop innovative security technology; evaluating selective adjacent market technologies for partnering or potential acquisition. We intend to maintain and enhance our technological leadership position in network, advanced malware, and cloud-based security. We will continue to invest significantly in internal development and product enhancements and to recruit, train, develop and retain experienced security professionals to broaden our proprietary knowledge base.

Awards and Certifications

We have received numerous industry awards and certifications since January 1, 2012, including:

- Leader in Security Effectiveness with 99% detection and protection and exceptional throughput; Sourcefire 8260, 8250 and 8120 appliances individual product test results, NSS Labs Inc., April 2012.

- ‘Five-Star Rating’ by Everything Channel Partner Program Guide, April 2012. For the third consecutive year, the Sourcefire Channel Program was recognized for its Global Security Alliance Program.

- 'Protector of the Year' by SC Magazine Australia, May 2012. Sourcefire was honored for doing the most to protect its users' online presences from attacks with the Sourcefire NGIPS.

- Leader in IPS Security Effectiveness and Total Cost of Ownership, Security Value Map for IPS, NSS Labs, July 2012.

- Named to the DoD Unified Capabilities Approved Products List, August, 2012. The Sourcefire NGIPS successfully completed Interoperability (IO) and Information Assurance (IA) certification.

- Named “One of 12 Hot Companies to Watch,” by Federal Computer Week, September 2012.

- Common Criteria Certification by the National Information Assurance Partnership, September 2012. Sourcefire’s FirePOWER Appliances, NGIPS, Virtual NGIPS and Defense Center were evaluated and certified using the Common Methodology for IT Security Evaluation for conformance to the Common Criteria.

- Leader in NGFW Security Effectiveness; FirePOWER 8250 NGFW achieved 99% protection, superior performance and total cost of ownership, Sourcefire Individual Product Test Results, NSS Labs Inc., October 2012.

Customers

We provide products and services to a broad spectrum of customers and organizations within diverse industry sectors,

including some of the world's largest financial institutions, health care providers, IT companies, telecommunication companies and retailers, as well as U.S. and other national, state and local government agencies.

For the year ended December 31, 2012, one customer, a distributor of our products to the U.S. government, EC America, a subsidiary of immixGroup, accounted for 19% of total revenue. For the year ended December 31, 2011, two customers, a distributor of our products to the U.S. government, EC America, a subsidiary of immixGroup, and a distributor of our products, Fishnet Security, accounted for 18% and 11%, respectively, of total revenue. For the year ended December 31, 2010, two customers, a distributor of our products to the U.S. government, immixTechnology, a subsidiary of immixGroup, and a distributor of our products, Fishnet Security, accounted for 16% and 11%, respectively, of total revenue.

Sales and Marketing

We market and sell our appliances, software and services to our customers primarily through our global network of resellers, distributors, MSSPs, government integrators and other partners.

Sales. Our sales organization is organized into two geographic regions: the U.S. and International. We maintain sales offices in North America, Europe, Latin America and Asia. Our sales personnel are responsible for market development, including managing our relationships with resellers and distributors, assisting them in winning and supporting key customer accounts and acting as liaisons between the end customers and our marketing and product development organizations. We employ dedicated, regional channel managers to support partner sales and activities. We are also investing in the capacity of our international sales and channel personnel to provide expanded levels of support throughout Europe, Latin America, and the Asia/Pacific region.

Each sales organization is supported by experienced security engineers who are responsible for providing pre-sales technical support and technical training for the sales team and for our resellers, distributors and other partners. All of our sales personnel are responsible for lead follow-up and account management. Our sales personnel have quota requirements and are compensated with a combination of base salary and earned commissions.

Our indirect sales channel, comprised primarily of resellers and distributors, is supported by our sales force, including dedicated channel managers, with substantial experience in selling cybersecurity products to, and through, resellers and distributors. We maintain a global network of value-added resellers and distributors. Our arrangements with our resellers and distributors are non-exclusive, generally cover all of our products and services, and provide for appropriate discounts based on a variety of factors, including their transaction volume. We also provide our resellers and distributors with marketing assistance, technical training and support.

Marketing. Our marketing activities consist primarily of product marketing, product management and sales support programs. Marketing also includes public relations, social media, advertising, our corporate website, trade shows, and direct marketing. Our marketing programs are designed to build the Sourcefire brand, increase customer awareness, generate leads and communicate our product advantages. We also use our marketing programs to support the sale of our products through new channels and to new markets.

Research and Development

Our research and development efforts are focused both on improving and enhancing our existing network security products and on developing new products, features and functionality. We communicate with our customers and the open source community when considering product improvements and enhancements, and we regularly release new versions of our products incorporating these improvements and enhancements.

Research & Development Team. Our Research and Development Team is comprised of highly skilled and experienced security and network experts. The team encompasses the full lifecycle of product concept, design, development, integration, quality assurance testing, deployment, maintenance and support. Our development experts focus on the FirePOWER platform, Sourcefire security products, as well as manage the administration and testing of the open source Snort, Clam AV and Razorback initiatives. The development is performed in the United States and, for our advanced malware protection solutions, in the United States and Canada.

Cloud Technology Group. The Cloud Technology Group focuses on the research and development of next generation cloud-based security technologies. This includes the development of advanced malware protection, cloud-delivered security intelligence, and a broader cloud-security platform.

Vulnerability Research Team. Our VRT is comprised of leading security experts working to proactively discover, assess and respond to the latest network threats and security vulnerabilities. By gathering and analyzing this information, our VRT

creates and updates Snort rules, ClamAV signatures, advanced malware file analysis and security tools that are designed to identify, characterize and defeat attacks. The VRT also supports FireAMP's file analysis that provides detailed information on malware behavior.

Our VRT participates in extensive collaboration with hundreds of network security professionals in the Snort, ClamAV, and Sourcefire user communities and other security authorities to learn of new vulnerabilities and exploits. Because of the knowledge and experience of our VRT personnel, as well as its extensive coordination with the open source community, we believe that we have access to one of the largest and most sophisticated groups of IT security experts researching vulnerabilities and threats on a real-time basis.

Our research and development expense was $41.6 million, $33.1 million, and $18.8 million for the years ended December 31, 2012, 2011 and 2010, respectively.

Backlog

While it is our practice to promptly ship our products upon receipt of properly finalized purchase orders, we generally have product license orders that have not shipped as of the end of a particular period. In the ordinary course of our business, such orders are generally shipped within 30 days. Although the amount of such product license orders varies, we do not believe the amount of such orders, as of any particular date, is a reliable indicator of our future performance.

Manufacturing and Suppliers

We typically hold limited inventory. We utilize two principal contract equipment manufacturers to source components, assemble, integrate and test our appliances and to ship those appliances to our customers. The two principle contract manufacturers give us manufacturing presence in North America, Latin America, Europe and Asia. In addition, we utilize a third contract manufacturer to design and integrate some of our software and hardware components for use in the high-performance models of our appliances. Our agreements with these contract manufacturers are non-exclusive and subject to expiration at the end of terms ranging from one to three years. We would be faced with the burden, cost and delay of having to qualify and contract with a new supplier if any of these agreements expire or terminate for any reason.

Intellectual Property

To protect our intellectual property, both domestically and abroad, we rely primarily on patent, trademark, copyright and trade secret laws. We hold 23 issued patents and have dozens of patent applications pending for examination in the U.S. and foreign jurisdictions. The claims for which we have sought patent protection relate to methods and systems we have developed for intrusion detection and prevention and anti-malware detection used in our solutions. In addition, we utilize contractual provisions, such as license agreements with our partners and customers, non-disclosure and non-compete agreements with our employees and consultants, and confidentiality procedures to strengthen our protection.

Despite our efforts to protect our intellectual property, unauthorized parties may attempt to copy aspects of our products or obtain and use information that we regard as proprietary. While we cannot determine the extent to which piracy of our software products occurs, we expect software piracy to be a persistent problem. In addition, the laws of some foreign countries do not protect our proprietary rights to as great an extent as do the laws of the United States, and many foreign countries do not enforce these laws as diligently as U.S. government agencies and private parties.

Seasonality

Our business is subject to seasonal fluctuations. For a discussion of seasonality affecting our business, see Item 7. Management's Discussion and Analysis of Financial Condition and Results of Operations — Results of Operations — Seasonality.

Competition

The market for cybersecurity solutions is intensely competitive and we expect strong competition to continue in the future. Many of our competitors have longer operating histories, greater brand recognition, stronger relationships with strategic channel partners, larger technical staffs, established relationships with hardware vendors and/or greater financial, technical and marketing resources and other market advantages. Increasingly, commoditized security protection is offered by third parties at significant discounts to our prices or, in some cases is bundled for free. Potential customers may perceive our products as less valuable or even unnecessary if similar functionality is

available at a significant discount or free.

Large companies may have advantages over us because of their longer operating histories, greater brand name recognition, larger customer bases or greater financial, technical and marketing resources. As a result, they may have greater

resources to devote to the promotion and sale of their products.

Our principal competitors are set forth below:

Network Security. In the market for network security, including intrusion prevention and next generation firewall, our chief competitors generally fall within the following categories:

- large companies, including Cisco Systems, Inc., IBM Corporation, HP Corporation, Check Point Software Technologies, Ltd. and Intel Corporation as a result of its acquisition of McAfee, Inc., that sell competitive products and offerings;
- software or hardware network infrastructure companies that could integrate features that are similar to our products into their own products;
- smaller software companies offering applications for network and Internet security monitoring, detection, prevention or response; and
- small and large companies offering point solutions that compete with components of our product offerings.

Advanced Malware Protection. Sourcefire has entered the emerging advanced malware protection market. Sourcefire's solutions complement existing endpoint and network security products to protect from threats that may bypass these existing defenses. In the advanced malware protection market, our chief competitors are large established endpoint protection market players and new entrants in an emerging network-based advanced malware protection market. New market entrants consist primarily of venture-backed point product companies with a singular focus and aggressive sales and marketing efforts.

Several companies currently sell security software products that our customers and potential customers have broadly adopted. Some of these companies sell products that perform the same functions as some of our products. In addition, the vendors of operating system software or networking hardware may enhance their products to include functions similar to those that our products currently provide.

We believe that the principal competitive factors affecting the market for information security solutions include security effectiveness, manageability, technical features, performance, ease of use, price, scope of product offerings, professional services capabilities, distribution relationships and customer service and support. We believe that our solutions generally compete favorably with respect to such factors.

Employees

As of December 31, 2012, we had 599 employees, of whom 182 were engaged in product research and development and 259 were engaged in sales and marketing. Our current employees are not represented by a labor union and are not the subject of a collective bargaining agreement. We believe that we have good relations with our employees.

Corporate Information

We were incorporated in Delaware in 2001. We completed our initial public offering in March 2007. Our executive offices are located at 9770 Patuxent Woods Drive, Columbia, Maryland 21046, and our main telephone number is (410) 290-1616.

Available Information

Our Internet address is www.sourcefire.com. We provide free of charge on the Investor Relations page of our corporate web site access to our Annual Report on Form 10-K, Quarterly Reports on Form 10-Q, Current Reports on Form 8-K and amendments to those reports filed or furnished pursuant to Section 13(a) or 15(d) of the Securities Exchange Act of 1934, as amended, as soon as reasonably practicable after they are electronically filed with or furnished to the Securities and Exchange Commission, or SEC. Information appearing on our website is not incorporated by reference in and is not a part of this annual report.

Item 1A. RISK FACTORS

Set forth below and elsewhere in this Annual Report on Form 10-K and in other documents we file with the SEC are risks and uncertainties that could cause actual results to differ materially from the results contemplated by the forward-looking statements contained in this Annual Report on Form 10-K. Because of the following factors, as well as other variables affecting our operating results, past financial performance should not be considered as a reliable indicator of future performance, and investors should not use historical trends to anticipate results or trends in future periods.

Risks Relating to Our Business, Operations and Industry

Adverse economic, market and political conditions may negatively affect our revenue and results of operations.

Our business depends significantly on a range of factors that are beyond our control. These include:

- general economic and business conditions;
- the overall demand for network security products and services and other security products and services; and
- constraints on budgets and changes in spending priorities of corporations and government agencies.

The U.S. and global economies have experienced a period of prolonged economic weakness, including a reduction in business confidence and activity, reduced capital spending, a lack of availability of credit, high unemployment and disruptions in financial markets. These and other factors have affected, and in the future may affect, one or more of the industries or geographies to which we sell our products and services. Our customers include, but are not limited to, financial institutions, defense contractors, health care providers, information technology companies, telecommunications companies and retailers. These customers may suffer from reduced operating budgets, which could cause them to defer or forego purchases of our products or services. In addition, negative effects on the financial condition of our resellers and distributors could affect their ability or willingness to market our product and service offerings; negative effects on the financial condition of our product manufacturers could affect their ability to manufacture our products; and declines in economic and market conditions could impair our short-term investment portfolio. Any of these developments could adversely affect our revenue and results of operations.

Federal and state governmental agencies have contributed to our revenue growth and have become important customers for us. If we cannot attract sufficient government agency customers, our revenue and competitive position will suffer. If U.S. Government Agencies reduce spending levels for network security programs, it could have a negative effect on our revenue and results of operations.

Federal and state governments have become important customers for us. There can be no assurance that we will maintain or grow our revenue from these customers. Contracts with the U.S. federal and state government agencies collectively accounted for 20%, 21% and 25% of our total revenue for the years ended December 31, 2012, 2011 and 2010, respectively.

Our reliance on government customers subjects us to a number of risks, including:

- Budgetary Constraints and Cycles. Demand and payment for our products and services are impacted by public sector budgetary cycles and funding availability. Reductions or delays in funding, including reductions or delays caused by the failure to pass a budget, automatic spending cuts, continuing resolutions or other temporary funding arrangements, could adversely impact public sector demand for our products. As of the date of this annual report, the U.S. federal government has not adopted a budget for its fiscal year ending September 30, 2013 and is operating under a continuing budget resolution. If U.S. Government Agencies reduce spending levels for network security programs, it may negatively affect our sales to the federal government for the year ended December 31, 2013, and negatively affect our results of operations;
- Procurement. Contracting with public sector customers is highly competitive and can be expensive and time-consuming, often requiring that we incur significant upfront time and expense without any assurance that we will win a contract;
- Modification or Cancellation of Contracts. Public sector customers often have contractual or other legal rights to terminate current contracts for convenience or due to a default. If a contract is canceled for convenience, which can occur if the customer’s product needs change, we may only be able to collect for products and services delivered prior to termination. If a contract is canceled because of our default, we may only be able to collect for products and

alternative products and services delivered to the customer;

- Governmental Audits. National governments and state and local agencies routinely investigate and audit government contractors' administrative processes. They may audit our performance and pricing and review our compliance with applicable rules and regulations. If they find that we improperly allocated costs, they may require us to refund those costs or may refuse to pay us for outstanding balances related to the improper allocation. An unfavorable audit could

result in a reduction of revenue, and may result in civil or criminal liability; and

- Replacing Existing Products. Many government agencies already have installed network security products of our competitors. It can be very difficult to convince government agencies or other prospective customers to replace their existing network security solutions with our products, even if we can demonstrate the superiority of our products.

We face intense competition in our markets, especially from larger, better-known companies, and we may lack sufficient financial or other resources to maintain or improve our competitive position.

The market for our products and services is intensely competitive and we expect competition to increase in the future. We may not compete successfully against our current or potential competitors, especially those with significantly greater financial resources or brand name recognition. Our chief competitors currently include: large software companies; software or hardware network infrastructure companies; smaller software companies offering applications for network and Internet security monitoring, detection, prevention or response; and small and large companies offering point solutions that compete with components of our product offerings.

For example, Cisco Systems, Inc., IBM Corporation, HP Corporation, Intel Corporation, as a result of its acquisition of McAfee, Inc., and Check Point Software Technologies, Ltd. have intrusion detection or prevention technologies that compete with our network security product offerings. Similarly, several large and small companies have anti-malware and endpoint protection products that compete with our FireAMP® product. In addition, our Next Generation Firewall product competes with both new and traditional firewall vendors.

Large companies may have advantages over us because of their longer operating histories, greater brand name recognition, larger customer bases, broader product portfolios, or greater financial, technical and marketing resources. They also have greater resources to devote to the promotion and sale of their products than we have. In addition, in some cases our competitors have aggressively reduced, and could continue to reduce, the price of their security monitoring, detection, prevention and response products, managed security services, maintenance and support services, and other security services and products which intensifies pricing pressures within our market. Moreover, in some cases, customers may make purchasing decisions based primarily on price rather than product functionality.

In addition, the vendors of operating system software or networking hardware may enhance their products to include functions similar to those that our products provide. The widespread inclusion of features comparable to our software in operating system software or networking hardware could render our products less competitive or obsolete, particularly if such features are of a high quality. Even if security functions integrated into operating system software or networking hardware are more limited than those of our products, a significant number of customers may accept more limited functionality to avoid purchasing additional products such as ours.

One of the characteristics of open source software is that anyone can offer new software products for free under an open source licensing model in order to gain rapid and widespread market acceptance. Such competition can develop without the degree of overhead and lead time required by traditional technology companies. It is possible for new competitors with greater resources than ours to develop their own open source security solutions, potentially reducing the demand for our solutions. We may not be able to compete successfully against current and future competitors. Competitive pressure and/or the availability of open source software may result in price reductions, reduced revenue, reduced operating margins and loss of market share, any one of which could seriously harm our business.

New competitors could emerge and could impair our sales.

New sources of competition for sales of our products could emerge. These include:

- emerging companies as well as larger companies who have not previously entered the market for network intrusion detection and prevention products, next generation firewall products or advanced malware protection products;
- established companies that develop their own network intrusion detection and prevention products, next generation firewall products or advanced malware protection products;
- established companies that acquire or establish product integration, distribution or other cooperative relationships with our current competitors; and
- new competitors or alliances among competitors that emerge and rapidly acquire significant market share due to factors such as greater brand name recognition, a larger installed customer base and significantly greater financial, technical, marketing and other resources and experience.

12

Our quarterly operating results are likely to vary significantly and be unpredictable, in part because of the purchasing and budget practices of our customers, which could cause the trading price of our stock to decline.

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

- the budgeting cycles, internal approval requirements and funding available to our existing and prospective customers for the purchase of network security products;
- reductions or delays in funding for projects by U.S. federal and state government agencies, for example the reductions and delays in spending that have resulted, and may continue to result, from the failure of the U.S. federal government to adopt a budget for its fiscal year ending September 30, 2013,
- the timing, size and contract terms of orders received, which have historically been highest in the third and fourth quarters, but may fluctuate seasonally in different ways;
- the effect of one or more large orders on our operating results for a particular quarter and the effect of such large order or orders on comparisons of operating results for subsequent quarters;
- the level of perceived threats to network security, which may fluctuate from period to period;
- the level of demand for products sold by resellers, distributors, MSSPs, government integrators and other partners;
- the market acceptance of open source software solutions;
- the announcement or introduction of new product offerings by us or our competitors, and the levels of anticipation and market acceptance of those products;
- price competition;
- general economic conditions, both domestically and in our foreign markets;
- the product mix of our sales; and
- the timing of revenue recognition for our sales.

In particular, the network security technology procurement practices of many of our customers have had a measurable influence on the historical variability of our operating performance. Our prospective customers usually exercise great care and invest substantial time in their network security technology purchasing decisions. As a result, our sales cycles are long, generally between six and twelve months or sometimes longer, which further impacts the variability of our results. Additionally, many of our customers have historically finalized purchase decisions in the last weeks or days of a quarter. A delay in even one large order beyond the end of a particular quarter can substantially diminish our anticipated revenue for that quarter. In addition, many of our expenses must be incurred before we generate revenue. As a result, the negative impact on our operating results would increase if our revenue fails to meet expectations in any period.

The cumulative effect of these factors may result in larger fluctuations and unpredictability in our quarterly operating results than in the operating results of many other software and technology companies. This variability and unpredictability could result in our failing to meet the revenue or operating results expectations of securities industry analysts or investors for a particular 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 securities class action suits as a result. Therefore, you should not rely on our operating results in any quarter as being indicative of our operating results for any future period, nor should you rely on other expectations, predictions or projections of our future revenue or other aspects of our results of operations.

We achieved profitability on an annual basis for the first time in 2009, which we may not be able to maintain.

We incurred operating losses each year from our inception in 2001 through 2008. We achieved profitability on an annual basis for the first time in 2009. Maintaining profitability will depend in large part on our ability to generate and sustain increased revenue levels in future periods. Although our revenue has generally been increasing, there can be no assurances that we will maintain or increase our level of profitability. Our operating expenses may continue to increase as we seek to expand our customer base, increase our sales and marketing efforts and continue to invest in research and development of our technologies and products. These efforts may be more costly than we expect and we may not be able to increase our revenue to offset our operating expenses. If we cannot increase our revenue at a

greater rate than our expenses, we will not remain profitable.

If we do not continue to establish and effectively manage our indirect distribution channels, or if our resellers, distributors and other partners fail to perform as expected, our revenue could suffer.

As part of our growth strategy, we have expanded, and intend to continue to expand, our indirect distribution channel. Our ability to sell our network security software and other products in new markets and to increase our share of existing

markets will be impaired if we fail to manage or expand our indirect distribution channels. Our sales strategy involves the establishment of multiple distribution channels domestically and internationally through strategic resellers, distributors, MSSPs, government integrators and other partners. We cannot predict the extent to which these companies will be successful in marketing or selling our products. In addition, our agreements with these companies could be terminated on short notice, and the agreements do not prevent these companies from selling the network security software of other companies, including our competitors. Any distributor of our products could give higher priority to other companies' products or to their own products than they give to ours, which could cause our revenue to decline. There is also a risk that some or all of our resellers, distributors and other partners may be acquired, change their business models or go out of business, any of which could adversely affect our business.

We are subject to risks of operating internationally that could impair our ability to grow our revenue abroad.

We market and sell our products in the United States and internationally, and we plan to increase our international sales presence. Therefore, we are subject to risks associated with having worldwide operations. Sales to customers located outside of the United States accounted for 33%, 25% and 25% of our total revenue for the years ended December 31, 2012, 2011 and 2010, respectively. The expansion of our existing operations and entry into additional worldwide markets will require significant management attention and financial resources. We are also subject to a number of risks customary for international operations, including:

- economic or political instability in foreign markets;
- greater difficulty in accounts receivable collection and longer collection periods;
- difficulties and costs of staffing and managing foreign operations;
- import and export controls;
- the uncertainty of protection for intellectual property rights in some countries;
- compliance with tax laws in multiple jurisdictions;
- the failure to realize expected tax benefits associated with our international operations;
- changes in regulatory or tax requirements;
- costs of compliance and penalties for noncompliance with foreign laws and laws applicable to companies doing business in foreign jurisdictions;
- costs of compliance and penalties for noncompliance with laws and regulations regarding consumer and data protection, privacy and encryption;
- management communication and integration problems resulting from cultural differences and geographic dispersion; and
- foreign currency exchange rate fluctuations.

To date, a substantial portion of our sales have been denominated in U.S. dollars, although the majority of our expenses that we incur in our international operations are denominated in local currencies. To date, we have not used risk management techniques or "hedged" the risks associated with fluctuations in foreign currency exchange rates. As a result, our results of operations are subject to losses from fluctuations in foreign currency exchange rates.

The market for network security products is rapidly evolving, and the complex technology incorporated in our products makes them difficult to develop. If we do not accurately predict, prepare for and respond promptly to technological and market developments and changing customer needs, our competitive position and prospects could be harmed.

The market for network security products is expected to continue to evolve rapidly. Moreover, many customers operate in markets characterized by rapidly changing technologies and business plans, which require them to add numerous network access points and adapt increasingly complex enterprise networks, incorporating a variety of hardware, software applications, operating systems and networking protocols. In addition, computer hackers and others who try to attack networks employ increasingly sophisticated techniques to gain access to and attack systems and networks. Customers look to our products to continue to protect their networks against these threats in this increasingly complex environment without sacrificing network efficiency or causing significant network downtime. The software in our products is especially complex because it needs to effectively identify and respond to new and increasingly sophisticated methods of attack, without impeding the high network performance demanded by our customers. Although the market expects speedy introduction of software to respond to new threats, the development

of these products is difficult and the timetable for commercial release of new products is uncertain. Therefore, in the future we may experience delays in the introduction of new products or new versions, modifications or enhancements of existing products. If we do not quickly respond to the rapidly changing and rigorous needs of our customers by developing and introducing on a timely basis new and effective products, upgrades and services that can respond adequately to new security threats, our competitive position and business prospects will be harmed.

If our new products and product enhancements do not achieve sufficient market acceptance, our results of operations and competitive position could suffer.

We spend substantial amounts of time and money to research and develop new products and enhance versions of our open source and proprietary commercial products. In 2012 and 2011, we developed and introduced new products in two adjacent markets, the next generation firewall market and the advanced malware protection market. In addition, we introduced new versions of our next generation intrusion prevention system products. We introduce new products and incorporate additional features, improve functionality or add other enhancements to our existing products in order to meet our customers' rapidly evolving demands for security in our highly competitive industry. When we develop a new product or an advanced version of an existing product, we typically expend significant money and effort upfront to develop, market, promote and sell the new offering. Therefore, when we develop and introduce new or enhanced products, they must achieve high levels of market acceptance in order to justify the amount of our investment in developing and bringing the products to market.

Our new products, including our next generation firewall products and advanced malware protection products, or enhancements could fail to attain sufficient market acceptance for many reasons, including:

- reluctance of customers to incur the costs of purchasing and implementing new products or product enhancements;
- delays in introducing new, enhanced or modified products;
- defects, errors or failures in any of our products;
- inability to operate effectively with the networks of our prospective customers;
- inability to protect against new types of attacks or techniques used by hackers;
- negative publicity about the performance or effectiveness of our network security products;
- reluctance of customers to purchase products based on open source software; and
- disruptions or delays in the availability and delivery of our products, including products from our contract manufacturers.

If our new products or enhancements do not achieve adequate acceptance in the market, our competitive position could be impaired, our revenue will be diminished and the effect on our operating results may be particularly acute because of the significant research, development, marketing, sales and other expenses we incurred in connection with the new product.

If existing customers do not make subsequent purchases from us or renew their support arrangements with us, or if our relationships with our largest customers are impaired, our revenue could decline.

For the years ended December 31, 2012, 2011 and 2010, existing customers that purchased additional products and services from us, whether for new locations or additional technology to protect existing networks and locations, generated a majority of our total revenue. Part of our growth strategy is to sell additional products to our existing customers. We may not be effective in executing this or any other aspect of our growth strategy. Our revenue could decline if our current customers do not continue to purchase additional products from us. In addition, as we deploy new versions of our existing products or introduce new products, our current customers may not require the functionality of these products and may not purchase them.

We also depend on our installed customer base for future service revenue from annual maintenance fees. Our maintenance and support agreements typically have durations of one year. If customers choose not to continue their maintenance service or seek to renegotiate the terms of maintenance and support agreements prior to renewing such agreements, our revenue may decline.

Defects, errors or vulnerabilities in our products could harm our reputation and business and divert our resources.

Because our products are complex, they may contain defects, errors or vulnerabilities that are not detected until after our commercial release and installation by our customers. We may not be able to correct any errors or defects or address vulnerabilities promptly, or at all. Any defects, errors or vulnerabilities in our products could result in:

- expenditure of significant financial and product development resources in efforts to analyze, correct and eliminate defects, to address and eliminate vulnerabilities or to create alternative solutions;
- loss of existing or potential customers;
- delayed or lost revenue;

- failure to timely attain or maintain market acceptance;
- increased service, warranty, product replacement and product liability insurance costs; and
- negative publicity, which could harm our reputation.

In addition, because our products and services provide and monitor network security and may protect valuable information, we could face claims for product liability, tort or breach of warranty. Anyone who circumvents our customers' security measures using our products could misappropriate the confidential information or other valuable property of, or interrupt the operations of, our customers. If that happens, affected customers or others could sue us. In addition, we may face liability for breaches of our product warranties or product failures. Provisions in our contracts relating to warranty disclaimers and liability limitations may be deemed by a court to be unenforceable. Some courts, for example, have found contractual limitations of liability in standard computer and software contracts to be unenforceable in some circumstances. Defending a lawsuit, regardless of its merit, could be costly and divert management attention from the operation of our business. Our business liability insurance coverage may be inadequate or future coverage may be unavailable on acceptable terms or at all.

Our networks, products and services may be subject to intentional disruption.

As a leading network security solutions company, we are a high profile target for cyberattacks. We expect our networks, products and services to be targeted by attacks specifically designed to disrupt our business and harm our reputation. Experienced computer programmers may attempt to penetrate our networks, information systems and websites and impede the performance of our products, cause interruptions of our services or misappropriate information. Although we believe we have sufficient controls in place to prevent disruption and misappropriation, and to respond to such situations, we expect efforts to intentionally disrupt our networks, products and services to continue. If these efforts are successful, our operations could be disrupted, our business could be significantly affected as a result of harm to our reputation, and we could suffer monetary and other losses.

We have acquired, and in the future may acquire, additional businesses, products or technologies as part of our long-term growth strategy, and such acquisitions may not ultimately be successful or may not result in expected strategic benefits.

In December 2010, we acquired Immunet Corporation. We may seek to buy or make investments in additional complementary or competitive businesses, products or technologies as part of our long-term growth strategy. We may not be successful in making these additional acquisitions. We may face competition for acquisition opportunities from other companies, including larger companies with greater financial resources. We may incur substantial expenses in identifying and negotiating acquisition opportunities, whether or not completed.

Acquisitions may not result in the expected strategic benefits, and completed acquisitions, including our acquisition of Immunet Corporation, could negatively affect our operating results and financial position because of the following and other factors:

- the Immunet acquisition was dilutive to our earnings per share for the years ended December 31, 2012 and 2011 and any acquisitions we complete in the future may also be dilutive to our earnings;
- in connection with our acquisition of Immunet Corporation, for the years ended December 31, 2012 and 2011 we recognized expenses for the amortization of intangible assets, employee retention payments and stock-based compensation expense and this and other acquisitions may result in substantial accounting charges for restructuring and other expenses, write-offs of in-process research and development, write-offs of goodwill, amortization of intangible assets and stock-based compensation expense;
- we may not effectively integrate an acquired business, product or technology into our existing business and operations;
- completing a potential acquisition and integrating an acquired business into our existing business could significantly divert management's time and resources from the operation of our business;
- acquired companies, particularly privately held and non-U.S. companies, may have internal controls, policies and procedures that do not meet the requirements of the Sarbanes-Oxley Act of 2002 and public company accounting standards;
- we may use a significant portion of our cash resources to fund acquisitions; and
- we may issue stock to fund acquisitions, which could dilute the interests of our existing stockholders.

In the future, we may not be able to secure financing necessary to make acquisitions or to operate and grow our business as planned.

In the future, we may need to raise additional funds to make acquisitions or to expand our sales and marketing and research and development efforts. Additional equity or debt financing may not be available on favorable terms, or at all. If adequate funds are not available on acceptable terms, we may be unable to take advantage of acquisition or other opportunities or to fund the expansion of our sales and marketing and research and development efforts, which could seriously harm our business and operating results. If we issue debt, the debt holders could have rights senior to common stockholders to make claims on our assets and the terms of any debt could restrict our operations, including our ability to pay dividends on our common stock. Furthermore, if we issue additional equity securities, stockholders would experience dilution, and the new

equity securities could have rights senior to those of our common stock.

If other parties claim commercial ownership rights to Snort®, Razorback™ or ClamAV®, our reputation, customer relations and results of operations could be harmed.

While we created a majority of the current Snort code base, Razorback code base and ClamAV code base, a portion of the current code for each of Snort, Razorback and ClamAV was created, or in the future may be created, by the combined efforts of Sourcefire and the open source software community, and a portion was created, or in the future may be created, solely by the open source community. We believe that the portions of the Snort code base, Razorback code base and ClamAV code base created by anyone other than us are required to be licensed by us pursuant to the GNU General Public License, or GPL, which is how we currently license Snort and ClamAV. There is a risk, however, that a third party could claim some ownership rights in Snort, Razorback or ClamAV, attempt to prevent us from commercially licensing Snort, Razorback or ClamAV in the future (rather than pursuant to the GPL as currently licensed) or claim a right to licensing royalties. Any such claim, regardless of its merit or outcome, could be costly to defend, harm our reputation and customer relations or result in our having to pay substantial compensation to the party claiming ownership.

We rely on software licensed from other parties, the loss of which could increase our costs and delay delivery of our products.

We utilize various types of software licensed from unaffiliated third parties. For example, we license MySQL database software that we use in our products. Our agreement with Oracle Corporation permits us to distribute MySQL software on our products to our customers worldwide until June 30, 2014. Our agreement with Oracle gives us the unlimited right to distribute MySQL software in exchange for a one-time lump-sum payment. We believe that the MySQL agreement is material to our business because we have spent a significant amount of development resources to allow the MySQL software to function in our products. If we were forced to find replacement database software or replacements for any of the other software we license from others for our products, our business would be disrupted and we could be required to expend significant resources, and there would be no guarantee that we would be able to procure the replacement on the same or similar commercial terms and conditions, or at all.

Additionally, we would be required to either redesign our products to function with software available from other parties or develop these components ourselves, which could result in increased costs and could result in delays in our product shipments and the release of new product offerings. Furthermore, we might be forced to limit the features available in our current or future products. If we fail to maintain or renegotiate any of these software licenses, we could face significant delays and diversion of resources in attempting to license and integrate a functional equivalent of the software.

Our inability to hire or retain key personnel, or to effectively manage headcount increases, could impair our intended growth.

Our business is dependent on our ability to hire, retain, motivate and manage highly qualified personnel, including senior management and sales and technical professionals. In particular, as part of our growth strategy, we have expanded, and intend to continue to expand the size of our sales force domestically and internationally and have hired, and expect to continue to hire, additional engineering, customer support and professional services personnel. However, competition for qualified engineering and services personnel is intense, and if we are unable to attract, train or retain the number of highly qualified sales, engineering and services personnel that our business needs, our reputation, customer satisfaction and potential revenue growth could be seriously harmed. To the extent that we hire personnel from competitors, we may also be subject to allegations that they have been improperly solicited or divulged proprietary or other confidential information. Our intended future growth may also place a significant strain on our management, financial, personnel and other resources.

In addition, our future success will depend to a significant extent on the continued services of our executive officers and senior personnel. Although we have adopted retention plans applicable to certain of these officers, there can be no assurance that we will be able to retain their services. The loss of the services of one or more of these individuals could adversely affect our business and could divert other senior management time in searching for their replacements.

The inability to effect a smooth transition to a new Chief Executive Officer could harm our business.

As previously disclosed, John C. Burris, our former Chief Executive Officer, retired on October 1, 2012 and passed away on October 19, 2012. Our efforts to identify and retain a permanent Chief Executive Officer are ongoing. A search for a permanent Chief Executive Officer may take longer than we expect, and there can be no assurance that we will be able to attract a permanent Chief Executive Officer on acceptable terms. Even if we are able to hire a qualified successor, the search process and transition period may be difficult to manage, may cause concerns from current and potential customers and other third parties with whom we do business, may result in operational disruptions during such time that could adversely affect our

business and may result in a drop in our stock price. In addition, we may incur substantial costs in connection with the transition, including the fees of the executive search firm we have retained to assist us in identifying Chief Executive Officer candidates and the cash and equity compensation for a new Chief Executive Officer.

Our business is subject to corporate governance, public disclosure, accounting and tax requirements that have increased both our costs and the risk of noncompliance.

Because our common stock is publicly traded, we are subject to the rules and regulations of federal, state and financial market exchange entities, such as the Public Company Accounting Oversight Board, the SEC, and the Nasdaq stock exchange, that are charged with the protection of investors and the oversight of companies whose securities are publicly traded. Our efforts to comply with these rules and regulations have resulted in, and are likely to continue resulting in, increased general and administrative expenses and diversion of management time and attention from revenue-generating activities to compliance activities.

We completed our evaluation of our internal controls over financial reporting for the fiscal year ended December 31, 2012 as required by the Sarbanes-Oxley Act of 2002. Although our assessment, testing and evaluation resulted in our conclusion that as of December 31, 2012, our internal controls over financial reporting were effective, we cannot predict the outcome of our testing in future periods. If our internal controls are ineffective in future periods, our business and reputation could be harmed. We may incur additional expenses and commitment of management's time in connection with further evaluations, either of which could materially increase our operating expenses.

Because new and modified laws, regulations and standards are subject to varying interpretations in many cases due to their lack of specificity, their application in practice may evolve over time as new guidance is provided by regulatory and governing bodies. This evolution may result in continuing uncertainty regarding compliance matters and additional costs necessitated by ongoing revisions to our disclosure and governance practices.

Any material disruption or problem with the operation of our information systems may adversely impact our business, operating processes and internal controls.

The efficient operation of our business is dependent on the successful operation of our information systems. In particular, we rely on our information systems to process financial information, manage inventory and administer our sales transactions. In recent years, we have experienced considerable growth in transaction volume and headcount, and we are increasingly relying upon international resources in our operations. Our information systems need to be sufficiently scalable to support the continued growth of our operations and the efficient management of our business. In an effort to improve the efficiency of our operations, achieve greater automation and support the growth of our business, we have implemented an enterprise resource planning, or ERP, system and a customer resource management, or CRM, system.

These information systems may not work as we currently intend. Any material disruption or similar problems with the operation of our information systems could have a material negative effect on our business and results of operations. In addition, if our information system resources are inadequate, we may be required to undertake costly modifications and the growth of our business could be harmed.

Potential uncertainty resulting from unsolicited acquisition proposals and related matters may adversely affect our business.

In the past we have received, and in the future we may receive, unsolicited proposals to acquire our company or our assets. The review and consideration of acquisition proposals and related matters could require the expenditure of significant management time and personnel resources. Such proposals may also create uncertainty for our employees, customers and business partners. Any such uncertainty could make it more difficult for us to retain key employees and hire new talent, and could cause our customers and business partners to not enter into new arrangements with us or to terminate existing arrangements. Additionally, we and members of our board of directors could be subject to future lawsuits related to unsolicited proposals to acquire us. Any such future lawsuits could become time consuming and expensive. These matters, alone or in combination, may harm our business.

Risks Relating to Our Intellectual Property and Litigation

Our products contain open source software, and failure to comply with the terms of the underlying open source software licenses could restrict our ability to sell our products.

Like many other technology companies, we use and distribute “open source” software in order to expedite development of new products and features. Open source software is generally licensed by its authors or other third parties under “open source” licenses, including, for example, the GNU General Public License, or GPL, the GNU Lesser Public License, or LGPL,

the BSD License and the Apache License. This open source software includes, without limitation, Snort, ClamAV, Linux Kernel, Apache HTTP Server, OpenSSL and Perl. These license terms may be ambiguous, in many instances have not been interpreted by the courts and could be interpreted in a manner that results in unanticipated obligations regarding our products. Depending upon how the open source software is deployed by our developers and the underlying licenses are interpreted by the courts, we could be required to offer our products that use the open source software for no cost, make available the source code for modifications or derivative works, or secure an additional license to the underlying patent rights. Any of these obligations could have an adverse impact on our intellectual property rights and revenue from products incorporating the open source software.

Our use of open source software could also result in us developing and selling products that infringe third-party intellectual property rights. It may be difficult for us to accurately determine the developers of the open source code and whether the code incorporates proprietary software or otherwise infringes another party's intellectual property rights (including patent rights). We have processes and controls in place that are designed to address these risks and concerns, including a review process for screening requests from our development organizations for the use of open source software. However, we cannot be sure that all open source software is submitted for approval prior to use in our products.

We also have processes and controls in place to review the use of open source software in the products developed by companies that we may acquire. Even if we conduct due diligence prior to completing an acquisition, the acquired products or technologies may nonetheless include open source software that was not identified during the initial due diligence. Our ability to commercialize products or technologies of any companies we may acquire that incorporate open source software or to otherwise fully realize the anticipated benefits of any such acquisition may be restricted in the same manner as if the open source software had been incorporated into our own products.

Our intellectual property rights may be difficult to enforce, which could enable others to compete with us or to copy or use aspects of our products without compensating us.

We rely primarily on a combination of copyright, trademark, patent and trade secret laws, confidentiality procedures and contractual provisions to establish and protect our proprietary rights in our technology. However, the steps we have taken to protect our proprietary rights and technology may not deter its misuse, theft or misappropriation. Competitors may independently develop technologies or products that are substantially equivalent or superior to our products or that inappropriately incorporate our proprietary technology into their products. Our products incorporate open source Snort software, which is readily available to the public. To the extent that our proprietary software is included by others in what are purported to be open source products, it may be difficult and expensive to enforce our intellectual property rights in such software. Competitors also may hire our former employees who may misappropriate our proprietary technology.

In addition, from time to time, we become aware that users of our security products may not have paid adequate license, technical support, or subscription fees to us. However, some jurisdictions may not provide an adequate legal infrastructure for effective protection or enforcement of our intellectual property rights. Furthermore, changing legal interpretations of liability for unauthorized use of our software or lessened sensitivity by corporate, government or institutional users to refraining from intellectual property piracy or other infringements of intellectual property could also harm our business.

In limited instances we have agreed to place, and in the future may agree to place, source code for our proprietary software in escrow. In most cases, the escrowed source code may be made available to certain of our customers and partners in the event that we were to file for bankruptcy or materially fail to support our products in the future. Release of our source code upon any such event would increase the likelihood of misappropriation or other misuse of our software. We have rarely agreed to source code escrow arrangements in the past and usually only in connection with prospective customers considering a significant purchase of our products and services.

If we are unable to protect our intellectual property rights in our technologies, we may find ourselves at a competitive disadvantage to others who need not incur the additional expense, time and effort required to create competitive technologies. As a result, litigation may be necessary to enforce and protect our intellectual property rights.

Efforts to assert intellectual property ownership rights in our products could impact our standing in the open source community, which could limit our product innovation capabilities.

If we were to undertake actions to protect and maintain ownership and control over our intellectual property rights, our standing in the open source community could be diminished. This could in turn limit our ability to rely on this community as a resource to identify and defend against new viruses, threats and techniques to attack secure networks, explore new ideas and concepts and further our research and development efforts.

Claims that our products infringe the proprietary rights of others could harm our business and cause us to incur significant costs.

The security technology industry has increasingly been subject to patent and other intellectual property rights litigation, particularly from special purpose entities that seek to monetize their intellectual property rights by asserting claims against others. We expect this trend to continue and accelerate and expect that we may from time to time be required to defend against this type of litigation. For example, as described under Item 3. Legal Proceedings below, we and nine other network security companies have been named as defendants in a patent infringement lawsuit. Third party asserted claims or initiated litigation can include claims against us or our customers, end-users, manufacturers, suppliers, partners or distributors, alleging infringement of intellectual property rights with respect to our existing or future products or components of those products. The litigation process can be costly and is subject to inherent uncertainties, so we may not prevail in litigation matters regardless of the merits of our position. In addition to the expense and distraction associated with litigation, adverse determinations could cause us to lose our proprietary rights, prevent us from manufacturing or selling our products, require us to obtain licenses to patents or other intellectual property rights that our products are alleged to infringe, which licenses may not be available on reasonable commercial terms or at all, and subject us to significant liabilities. Under the terms of our contracts, we may also be required to indemnify customers and others for losses or costs arising from such claims and such indemnification obligations may not be subject to maximum loss clauses.

If we acquire technology to include in our products from third parties, our exposure to infringement actions may increase because we must rely upon these third parties to verify the origin and ownership of such technology. Similarly, we face exposure to infringement actions if we hire software engineers who were previously employed by competitors and those employees inadvertently or deliberately incorporate proprietary technology of our competitors into our products despite efforts by our competitors and us to prevent such infringement.

Future litigation could have a material adverse impact on our results of operations, financial condition and liquidity.

From time to time we have been, and may be in the future, subject to litigation, including stockholder derivative actions. Risks associated with legal liability are difficult to assess and quantify, and their existence and magnitude can remain unknown for significant periods of time. While we maintain director and officer insurance, the amount of insurance coverage may not be sufficient to cover a claim, and there can be no assurance as to the continued availability of this insurance. We may in the future be the target of additional proceedings, with or without merit, and these proceedings may result in substantial costs and divert management’s attention and resources.

Risks Relating to Manufacturing

We depend on a limited number of manufacturers of our hardware products, which increases our vulnerability to supply disruption.

Our ability to meet our customers’ demand for our products depends upon obtaining adequate hardware platforms on a timely basis and integrating them with our software. We utilize two principal contract equipment manufacturers, Patriot Technologies, Inc. and Premio, Inc., to source components, assemble, integrate and test our appliances and to ship those appliances to our customers. In addition, we utilize a third contract manufacturer, Netronome Systems Inc., to design and integrate some of our software and hardware components for use in the high-performance models of our appliances. The unexpected termination of our relationship with any of these manufacturers would be disruptive to our business and our reputation, and could result in a material decline in our revenue as well as shipment delays and possible increased costs as we seek and implement production with an alternative manufacturer.

In addition, we rely on our contract manufacturers to source the majority of the components for our hardware platforms and they in turn obtain materials from a limited number of suppliers. These suppliers may extend lead times, limit the supply to our manufacturers or increase prices due to capacity constraints or other factors. Although we work closely with our manufacturers and suppliers to avoid shortages, we may encounter these problems in the future. Our results of operations would be adversely affected if we were unable to obtain adequate supplies of hardware platforms in a timely manner or if there were significant increases in the costs of hardware platforms or problems with the quality of those hardware platforms.

We commit in advance to purchase products from contract manufacturers based on our expectations of future demand and a portion of these commitments are non-cancelable. In addition, in some cases we purchase products from contract manufacturers and hold them in inventory based on our expectations of future demand. If demand for our products does not meet our expectations, or if products become obsolete as a result of our introduction of new products, we could be required to recognize an expense related to our purchase commitments or write down the value of our inventory, which could adversely affect our results of operations.

We commit in advance to purchase products from our contract manufacturers based on our expectations of future demand and a portion of these commitments are non-cancelable. In addition, in some cases we purchase products from contract manufacturers based on our expectations of future demand. Demand for our products may not meet our expectations as a result of a number of factors, including weakness in general economic conditions, reductions in our customers' purchasing budgets, discounting of prices on competitive products, defects or perceived defects in the products or the introduction by us or our competitors of new or enhanced products. In the past, we have recognized expenses related to purchase commitments and inventory write-offs and, in the future, if we reduce our estimate of future demand for products that we are committed to purchase or hold in inventory, or if such products become obsolete as a result of our introduction of new products, we may be required to recognize additional expenses for purchase commitments or inventory write-offs, which could negatively impact our gross margin and results of operations.

Risks Relating to Our Common Stock

The price of our common stock may be subject to wide fluctuations.

Since the time of our initial public offering in March 2007, the market price of our common stock has been subject to significant fluctuations, and we expect this volatility to continue for the foreseeable future. For example, during the year ended December 31, 2012, our stock traded between a high of $59.64 per share and a low of $29.25 per share. Among the factors that could affect our common stock price are the risks described in this "Risk Factors" section and other factors, including:

- quarterly variations in our operating results compared to market expectations;
- changes in expectations as to our future financial performance, including financial estimates or reports by securities analysts;
- changes in market valuations of similar companies or of our competitors;
- liquidity and activity in the market for our common stock;
- actual or expected sales of our common stock by our stockholders;
- strategic moves by us or our competitors, such as acquisitions or restructurings;
- general market conditions; and
- domestic and international economic, legal and regulatory factors unrelated to our performance.

Stock markets in general, and the stocks of technology companies in particular, have experienced extreme volatility that has often been unrelated to the operating performance of a particular company. These broad market fluctuations may adversely affect the trading price of our common stock, regardless of our operating performance.

Sales of substantial amounts of our common stock in the public markets, or the perception that they might occur, could reduce the price that our common stock might otherwise attain.

As of February 22, 2013, we had 30,670,141 outstanding shares of common stock. This number includes shares held by institutional investors who own a significant majority of our common stock. This number also includes shares held by directors and officers who may sell such shares at their discretion, subject to volume limitations contained in federal securities laws. Sales of substantial amounts of our common stock in the public market, or the perception that such sales could occur, could adversely affect the market price of our common stock and may make it more difficult for you to sell your common stock at a time and price that you deem appropriate.

Anti-takeover provisions in our charter documents and under Delaware law and our adoption of a stockholder rights plan could make an acquisition of our company, which may be beneficial to our stockholders, more difficult and may prevent attempts by our stockholders to replace or remove our current management.

Our certificate of incorporation and our bylaws contain provisions that may delay or prevent an acquisition of our company or a change in our management. These provisions include a classified board of directors, a prohibition on

actions by written consent of our stockholders and our ability to issue preferred stock without stockholder approval. In addition, we have adopted a stockholder rights plan under which we would issue preferred stock rights upon specified events, which could substantially dilute the stock ownership of a person or group attempting to take us over without the approval of our board of directors. Although we believe these provisions of our certificate of incorporation, bylaws, Delaware corporate law and our

stockholder rights plan collectively provide for an opportunity to receive higher bids by requiring potential acquirers to negotiate with us, they would apply even if stockholders consider the offer to be beneficial. In addition, these provisions may frustrate or prevent attempts by our stockholders to replace or remove our current management by making it more difficult for stockholders to replace members of our board of directors, which is responsible for appointing the members of our management.

Item 1B. UNRESOLVED STAFF COMMENTS
None.

Item 2. PROPERTIES
Our corporate headquarters and principal executive offices are located in Columbia, Maryland under a lease that expires in May 2015. Significant leased locations include offices in Vienna, Virginia; Livonia, Michigan; Calgary, Alberta; Bracknell, United Kingdom; Tokyo, Japan; and Singapore. We also lease other sales offices in multiple locations worldwide. We believe that our facilities are generally suitable to meet our needs for the foreseeable future; however, we will continue to seek additional space as needed in accordance with our growth.

Item 3. LEGAL PROCEEDINGS
On May 29, 2009 and August 3, 2009, Enhanced Security Research, LLC, or ESR, filed two nearly identical complaints in the United States District Court for the District of Delaware against 10 defendants, including Cisco Systems, Inc., International Business Machines Corporation, Check Point Software Technologies, Ltd., Check Point Software Technologies, Inc., SonicWALL, Inc., 3Com Corporation, Nokia Corporation, Nokia, Inc., Fortinet, Inc., and us. The only significant difference between the first and second complaints is the addition of Security Research Holdings LLC as a plaintiff. The complaints allege, among other things, that our network security appliances and software infringe two U.S. patents. Plaintiffs seek unspecified damages, enhancement of those damages, an attorney's fee award and an injunction against further infringement. We believe that the patents in this case are invalid and that the allegations of infringement are without merit, and we intend to defend this case vigorously on these bases. Both patents in this litigation have been subject to reexamination by the United States Patent and Trademark Office, or USPTO, and the USPTO has rejected all claims of both patents as not patentable. The patent owner has filed an appeal of the rejections of US Patent No 6,119,236 in the U.S. Court of Appeals for the Federal Circuit, or CAFC. The patent owner filed the opening brief on February 25, 2013 and briefing is not expected to be complete before April 29, 2013. The patent owner did not appeal the rejections of the other patent and, on January 9, 2013, the USPTO issued Reexamination Certificate US 6,304,975 C1 canceling all claims. On June 25, 2010, the District Court dismissed the action filed May 29, 2009, for lack of standing. The CAFC affirmed the dismissal following Plaintiff's appeal. Also on June 25, 2010, the District Court stayed the action filed August 3, 2009 pending conclusion of the reexaminations. Given the inherent unpredictability of litigation and jury trials, we cannot at this early stage of the matter estimate the possible outcome of this litigation. Because patent litigation is time consuming and costly to defend, we may incur significant costs related to this matter in future periods. In addition, an unfavorable outcome in this matter could have a material adverse effect on our future results of operations or cash flows.

Item 4. MINE SAFETY DISCLOSURES
Not Applicable.

PART II

Item 5. MARKET FOR REGISTRANT'S COMMON EQUITY, RELATED STOCKHOLDER MATTERS AND ISSUER PURCHASES OF EQUITY SECURITIES

Market Information

Our common stock is publicly traded on the NASDAQ Global Select Market under the symbol "FIRE." The following table sets forth, for the periods indicated, the high and low sales prices of our common stock as reported by the NASDAQ Global Select Market.

	High	Low
Year Ended December 31, 2011:		
First Quarter	$27.57	$22.61
Second Quarter	$30.23	$23.20
Third Quarter	$31.47	$23.26
Fourth Quarter	$35.90	$24.76
Year Ended December 31, 2012:		
First Quarter	$50.47	$29.25
Second Quarter	$59.64	$45.06
Third Quarter	$57.98	$41.34
Fourth Quarter	$50.85	$40.68

As of February 22, 2013, there were approximately 19 holders of record of our common stock. The number of holders of record of our common stock does not reflect the number of beneficial holders whose shares are held by depositories, brokers or other nominees.

Dividend Policy

We have never declared or paid any cash dividends on our common stock. We currently intend to retain all available funds and any future earnings for use in the operation and expansion of our business and do not anticipate paying any cash dividends in the foreseeable future.

Stock Performance Graph

The following graph illustrates a comparison of the total cumulative stockholder return on our common stock for the period beginning December 31, 2007 through December 31, 2012 to two indices: the Russell 2000 Index and the RDG Software Composite Index. The graph assumes an initial investment of $100 on December 31, 2007 in Sourcefire common stock in each of the two indices. The comparisons in the graph are required by the Securities and Exchange Commission and are not intended to forecast or be indicative of possible future performance of our common stock.

* $100 invested on 12/31/07 in stock or index, including reinvestment of dividends.

Use of Proceeds

In March 2007, we completed the initial public offering of shares of our common stock. Our portion of the net proceeds from the initial public offering was approximately $83.9 million after deducting underwriting discounts and commissions of $6.5 million and $2.4 million in offering expenses.

We intend to use the net proceeds from the offering for working capital and other general corporate purposes, including financing our growth, developing new products and funding capital expenditures. Pending such usage, we have invested the net proceeds primarily in short-term, interest-bearing investment grade securities.

Repurchases of Equity Securities During 2012

Repurchases are made under the terms of our 2007 Stock Incentive Plan. Under this plan, we award shares of restricted stock to our non-employee directors. These shares of restricted stock are subject to a lapsing right of repurchase by us. We may exercise this right of repurchase in the event that a restricted stock recipient’s service to us is terminated. If we exercise this right, we are required to repay the purchase price paid by or on behalf of the recipient for the repurchased restricted shares, which typically is the par value per share of $0.001. Repurchased shares are returned to the 2007 Stock Incentive Plan and are available for future awards under the terms of that plan.

These were the no repurchases of equity securities made by us during the fiscal quarter ended December 31, 2012. We do not have a stock repurchase program.

Item 6. SELECTED FINANCIAL DATA

The consolidated statement of operations data for the three years ended December 31, 2012, 2011 and 2010 and the consolidated balance sheet data as of December 31, 2012 and 2011 have been derived from our audited consolidated financial statements appearing elsewhere in this report. The consolidated statement of operations data for the years ended December 31, 2009 and 2008 and the consolidated balance sheet data as of December 31, 2010, 2009 and 2008 have been derived from our audited consolidated financial statements that do not appear in this report. The selected consolidated financial data set forth below should be read in conjunction with Item 7. Management's Discussion and Analysis of Financial Condition and Results of Operations set forth below and our consolidated financial statements and related notes included elsewhere in this report. The historical results are not necessarily indicative of the results to be expected in any future period.

	Year Ended December 31,				
	2012	2011	2010	2009	2008
	(in thousands, except share and per share data)				
Consolidated statement of operations data:					
Revenue:					
Products	$135,490	$98,166	$78,436	$62,585	$45,245
Services	87,600	67,480	52,136	40,880	30,428
Total revenue	223,090	165,646	130,572	103,465	75,673
Cost of revenue:					
Products	40,695	28,368	20,000	15,641	12,408
Services	11,321	8,841	6,828	6,379	4,952
Total cost of revenue	52,016	37,209	26,828	22,020	17,360
Gross profit	171,074	128,437	103,744	81,445	58,313
Operating expenses:					
Research and development	41,570	33,145	18,789	16,256	12,620
Sales and marketing	86,759	64,589	48,735	36,498	33,169
General and administrative	28,194	19,709	18,814	16,761	18,713
Depreciation and amortization	5,187	3,917	3,375	3,647	2,627
Total operating expenses	161,710	121,360	89,713	73,162	67,129
Income (loss) from operations	9,364	7,077	14,031	8,283	(8,816)
Other income (expense), net	20	(351)	125	926	3,064
Income (loss) before income taxes	9,384	6,726	14,156	9,209	(5,752)
Provision for (benefit from) for income taxes	4,357	536	(5,821)	331	319
Net income (loss)	$5,027	$6,190	$19,977	$8,878	$(6,071)
Net income (loss) per common share:					
Basic	$0.17	$0.22	$0.72	$0.34	$(0.24)
Diluted	$0.16	$0.21	$0.69	$0.32	$(0.24)
Shares used in per common share calculations:					
Basic	29,787,100	28,607,013	27,670,356	26,458,273	25,379,791
Diluted	30,929,210	29,529,525	28,896,246		