SOURCEFIRE INC
Form 424B4
March 09, 2007

Table of Contents

Filed Pursuant to Rule 424(b)(4)
Registration Statement No. 333-138199

PROSPECTUS

5,770,000 Shares

COMMON STOCK

Sourcefire, Inc. is offering 5,320,000 shares of its common stock and the selling stockholders are offering 450,000 shares. We will not receive any proceeds from the sale of shares by the selling stockholders. This is our initial public offering and no public market exists for our shares.

Our shares of common stock have been approved for quotation on the Nasdaq Global Market under the symbol FIRE.

Investing in our common stock involves risks. See Risk Factors beginning on page 9.

PRICE $15.00 A SHARE

	Price to Public	*Underwriting Discounts and Commissions*	*Proceeds to Sourcefire*	*Proceeds to Selling Stockholders*
Per share	$15.00	$1.05	$13.95	$13.95
Total	$86,550,000	$6,058,500	$74,214,000	$6,277,500

We have granted the underwriters the right to purchase up to an additional 865,500 shares of common stock to cover over-allotments.

The Securities and Exchange Commission and state securities regulators have not approved or disapproved these securities, or determined if this prospectus is truthful or complete. Any representation to the contrary is a criminal offense.

Morgan Stanley & Co. Incorporated expects to deliver the shares of common stock to purchasers on March 14, 2007.

MORGAN STANLEY *LEHMAN BROTHERS*

UBS INVESTMENT BANK ***JEFFERIES & COMPANY***

March 8, 2007

Table of Contents

TABLE OF CONTENTS

You should rely only on the information contained in this prospectus. We have not authorized anyone to provide you with information different from that contained in this prospectus. We are offering to sell, and seeking offers to buy, shares of common stock only in jurisdictions where offers and sales are permitted. The information contained in this prospectus is accurate only as of the date of this prospectus, regardless of the time of delivery of this prospectus or of any sale of shares of common stock.

Until and including April 2, 2007, 25 days after the commencement of this offering, all dealers that buy, sell or trade shares of our common stock, whether or not participating in this offering, may be required to deliver a prospectus. This delivery requirement is in addition to the dealers obligation to deliver a prospectus when acting as underwriters and with respect to their unsold allotments or subscriptions.

For investors outside the United States. Neither we nor any of the underwriters have done anything that would permit this offering or possession or distribution of this prospectus in any jurisdiction where action for that purpose is required, other than in the United States. You are required to inform yourselves about, and to observe any restrictions relating to, this offering and the distribution of this prospectus.

Table of Contents

PROSPECTUS SUMMARY

This summary highlights selected information contained elsewhere in this prospectus and does not contain all of the information you should consider in making your investment decision. You should read the following summary together with all of the more detailed information regarding us and our common stock being sold in the offering, including our financial statements and the related notes, appearing elsewhere in this prospectus. Unless we state otherwise, Sourcefire, the Company, we, us, and our refer to Sourcefire, Inc., a Delaware corporation, and its subsidiaries as a whole.

SOURCEFIRE, INC.

Overview

We are a leading provider of intelligence driven, open source network security solutions that enable our customers to protect their computer networks in an effective, efficient and highly automated manner. We sell our security solutions to a diverse customer base that includes more than 25 of the Fortune 100 companies and over half of the 30 largest U.S. government agencies. We also manage one of the security industry s leading open source initiatives, Snort.

Our family of network security products forms a comprehensive Discover, Determine and Defend, or 3D, approach to network security. Using this approach, our technology can automatically:

Discover potential threats and points of vulnerability;

Determine the potential impact of those observations to the network; and

Defend the network through proactive enforcement of security policy.

Our Sourcefire 3D approach is comprised of three key components:

RNA. At the heart of the Sourcefire 3D security solution is Real-time Network Awareness, or RNA, our network intelligence product that provides persistent visibility into the composition, behavior, topology (the relationship of network components) and risk profile of the network. This information provides a platform for the Defense Center s automated decision-making and network policy compliance enforcement. The ability to continuously discover characteristics and vulnerabilities of any computing device, or endpoint, communicating on a network (such as a computer, printer or server), or endpoint intelligence, along with the ability to observe how those endpoints communicate with each other, or network intelligence, enables our Intrusion Prevention products to more precisely identify and block threatening traffic and to more efficiently classify threatening and/or suspicious behavior than products lacking network intelligence.

Intrusion Sensors. The Intrusion Sensors utilize open source Snort® and our proprietary technology to monitor network traffic. These sensors compare observed traffic to a set of Rules , or a set of anomalous network traffic characteristics, which can be indicative of malicious activity. Once the Intrusion Sensors match a Rule to the observed traffic, they block malicious traffic and/or send an alert to the Defense Center for further analysis, prioritization and possible action.

Defense Center. The Defense Center aggregates, correlates and prioritizes network security events from RNA Sensors and Intrusion Sensors to synthesize multipoint event correlation and policy compliance analysis. The Defense

Center s policy and response subsystems are designed to leverage existing IT infrastructure such as firewalls, routers, trouble ticketing and patch management systems for virtually any task, including alerting, blocking and initiating corrective measures.

The traffic inspection engine used in our intrusion prevention products is the open source technology called Snort. Martin Roesch, our founder and Chief Technology Officer, created Snort in 1998. Our employees, including Mr. Roesch, have authored all major components of Snort, and we maintain control over the Snort project, including the principal Snort community forum, Snort.org. Snort, which has become a de facto industry standard, has been downloaded over 3 million times. We believe that a majority of the Fortune 100 companies and all of the 30 largest U.S. government agencies use Snort technology to monitor network traffic and that Snort is the most widely

Table of Contents

deployed intrusion prevention technology worldwide. The ubiquitous nature of the Snort user community represents a significant opportunity to sell our proprietary products to customers that require a complete enterprise solution.

For the year ended December 31, 2006, we generated approximately 81% of our revenue from customers in the U.S. and 19% from international customers. We increased our revenue from $32.9 million in 2005 to $44.9 million in 2006, representing a growth rate of 37%.

Our Industry

We believe, based on our review of various industry sources, that the network security industry was estimated to be a $18.4 billion market in 2006 and is projected to grow to $26.9 billion in 2009, representing a compound annual growth rate of over 13%. Our addressable markets include intrusion prevention, vulnerability management and unified threat management, which were collectively projected to total $2.9 billion in 2006 and are expected to grow at a compound annual growth rate in excess of 21% to $5.2 billion in 2009, according to industry sources we reviewed. We expect that this growth should continue as organizations seek solutions to various growing and evolving security challenges, including:

Greater Sophistication, Severity and Frequency of Network Attacks. The growing use of the Internet as a business tool has required organizations to increase the number of access points to their networks, which has made vast amounts of critical information more vulnerable to attack. Theft of sensitive information for financial gain motivates network attackers, who derive profit through identity theft, credit card fraud, money laundering, extortion, intellectual property theft and other illegal means. These profit-motivated attackers, in contrast to the hobbyist hackers of the past, are employing much more sophisticated tools and techniques to generate profits for themselves and their well-organized and well-financed sponsors.

Increasing Risks from Unknown Vulnerabilities. Unknown vulnerabilities in computer software that are discovered by network attackers before they are discovered by security and software vendors represent a tremendous risk. These uncorrected flaws can leave networks largely defenseless and open to exploitation. According to Computer Emergency Response Team Coordination Center, or CERT-CC, data as of October 2006, the trends in the rate of vulnerability disclosure are particularly alarming, with approximately 3,780 disclosed in 2004 and more than 5,990 disclosed in 2005, representing a growth rate of approximately 58%.

Potential Degradation of Network Performance. Many security products degrade network performance and are, therefore, disfavored by network administrators who generally prioritize network performance over incremental gains in network security. For example, the use of active scanners that probe networks for vulnerabilities often meets heavy resistance from administrators concerned about excessive network noise, clogged firewall logs and disruption of network assets that are critical to business operations.

Diverse Demands on Security Administrators. The proliferation of targeted security solutions such as firewalls, intrusion prevention systems, URL filters, spam filters and anti-spyware solutions, while critical to enhancing network security, create significant administrative burdens on personnel who must manage numerous disparate technologies that are seldom integrated and often difficult to use. Most network security products require manual, labor intensive incident response and investigation by security administrators, especially when false positive results are generated.

Heightened Government Regulation. Rapidly growing government regulation is forcing compliance with increased requirements for network security, which has escalated demand for security solutions that meet both compliance requirements and reduce the burdens of compliance, reporting and enforcement. Examples of these laws include The Health Insurance Portability and Accountability Act of 1996, or HIPAA, The Financial Services Modernization Act of 1999, commonly known as the Gramm-Leach-Bliley Act, The Sarbanes-Oxley Act of 2002 and The Federal

Information Security Management Act.

Table of Contents

Our Competitive Strengths

We believe that our leading market position results from several key competitive strengths, including:

Real-Time Approach to Network Security. Our solution is designed to support a continuum of network security functions that span pre-attack hardening of assets, high fidelity attack identification and disruption and real-time compromise detection and incident response. In addition, our ability to confidently classify and prioritize threats in network traffic and determine the composition, behavior and relationships of network devices, or endpoints, allows us to reliably automate what are otherwise manual, time-intensive processes.

Comprehensive Network Intelligence. Our innovative network security solution incorporates RNA, which provides persistent visibility into the composition, behavior, topology and risk profile of the network and serves as a platform for automated decision-making and network security policy enforcement. RNA performs passive, or non-disruptive, network discovery. This enables real-time compositional cataloging of network assets, including their configuration, thereby significantly increasing the network intelligence available to IT and security administrators. By integrating this contextual understanding of the network s components and situational awareness of network events, our solution is effective across a broad range of security domains, especially in the area of threat identification and impact assessment.

The Snort Community. The Snort user community, with over 100,000 registered users and over 3 million downloads to date, has enabled us to establish a market footprint unlike any other in the industry. We believe the Snort open source community provides us with significant benefits, including a broad threat awareness network, significant research and development leverage, and a large pool of security experts that are skilled in the use of our technology. We believe that Snort s broad acceptance makes us one of the most trusted sources of intrusion prevention and related security solutions.

Leading-Edge Performance. Our solutions have the ability to process multiple gigabits of traffic with latency as low as 100 microseconds. Our intrusion prevention 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. The Defense Center supports event loads as high as 1,300 events per second, which we believe meets or exceeds the requirements of the most demanding enterprise customers.

Significant Security Expertise. We have a highly knowledgeable management team with extensive network security industry experience gained from past service in leading enterprises and government organizations including Symantec, McAfee, the Department of Defense and the National Security Agency. Our founder and CTO, Martin Roesch, invented Snort and our core RNA technology and is widely regarded as a network security visionary. Our senior management team averages 16 years of experience in the networking and security industries. In addition, our Vulnerability Research Team, or VRT, is comprised of highly experienced security experts who research new vulnerabilities and create innovative methods for preventing attempts to exploit them.

Broad Industry Recognition. We have received numerous industry awards and certifications, including recognition as a leader in the network intrusion prevention systems market, supporting our position as one of a select few companies that best combines completeness of vision with ability to execute. RNA is one of only five network security products to receive the NSS Gold award, which is awarded by The NSS Group only to those products that are distinguished in terms of advanced or unique features, and which offer outstanding value. In addition, our technology has achieved Common Criteria Evaluation Assurance Level 2, or EAL2, which is an international evaluation standard for information technology security products sanctioned by, among others, the International Standards Organization, the National Security Agency and the National Institute for Standards and Technology.

Table of Contents

Our Growth Strategy

We intend to become the preeminent provider of network security solutions on a global basis. The key elements of our growth strategy include:

Continue to Develop Innovative Network Security Technology. We will continue to invest significantly in internal development and product enhancements and to hire additional network security experts to broaden our proprietary knowledge base. We believe our platform is capable of expanding into new markets such as unified threat management, security management and compliance and network management.

Grow our Customer Base. With over 3 million downloads of Snort and over 100,000 registered users, we believe Snort is the most ubiquitous network intrusion detection and prevention technology. We seek to monetize the Snort installed base by targeting enterprises that implement Snort but have not yet purchased any of the components of our Sourcefire 3D security solution. We will continue to target large enterprises and government agencies that require advanced security technology and high levels of network availability and performance in sectors including finance, technology, healthcare, manufacturing and defense.

Further Penetrate our Existing Customer Base. As of December 31, 2006, over 1,300 customers have purchased our Intrusion Sensors and Defense Center products. We intend to sell additional Intrusion Sensors to existing customers and expand our footprint in the networks of our customers to include branch offices, remote locations and data centers. In addition, we believe we have a significant opportunity to up-sell our higher margin RNA product to existing customers because of the significant incremental benefit that increased network intelligence can bring to their security systems.

Expand our OEM Alliances and Distribution Relationships. As part of our ongoing effort to expand our OEM alliances, we recently entered into a relationship with Nokia whereby Nokia Enterprise Solutions will market to its enterprise customers network security solutions that utilize our proprietary software and technology. In addition, we seek to expand our strategic reseller agreements and increasingly use this channel to generate additional inbound customer prospects. We also intend to utilize our relationships with managed security service providers such as Verizon, VeriSign and Symantec, to derive incremental revenue. In 2006, we generated approximately 11% of our revenue from governmental organizations and, in the future, we believe we will generate an increasing amount of revenue from government suppliers such as Lockheed Martin, Northrop Grumman and Immix Technology.

Strengthen Our International Presence. We believe the network security needs of many enterprises located outside of the United States are not being adequately served and represent a significant potential market opportunity. In 2006, we generated only approximately 19% of our revenue from international customers. We are expanding our sales in international markets by adding distribution relationships and expanding our direct sales force, with plans in the next year to double the number of personnel in Europe and to hire a country manager for Japan.

Selectively Pursue Acquisitions of Complementary Businesses and Technologies. To accelerate our expected growth, enhance the capabilities of our existing products and broaden our product and service offerings, we intend to selectively pursue acquisitions of businesses, technologies and products that could complement our existing operations.

Certain Risk Factors

Investing in our common stock involves substantial risk. You should carefully consider all the information in this prospectus prior to investing in our common stock. These risks and uncertainties include, but are not limited to, the following:

As we have had operating losses since our inception and we expect operating expenses to increase in the foreseeable future, we may never reach or maintain profitability.

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

Table of Contents

New competitors could emerge or our customers or distributors could internally develop alternatives to our products and either development could impair our sales.

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.

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 to technological and market developments and changing customer needs, our competitive position and prospects will be harmed.

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

Our Corporate Information

We were incorporated as a Delaware corporation in December 2001. Our principal executive office is located at 9770 Patuxent Woods Drive, Columbia, Maryland 21046. Our telephone number at that location is (410) 290-1616. Our website address is *www.sourcefire.com.* We also operate *www.snort.org.* These are textual references only. We do not incorporate the information on, or accessible through, any of our websites into this prospectus, and you should not consider any information on, or that can be accessed through, our websites as part of this prospectus.

Table of Contents

THE OFFERING

Common stock offered by Sourcefire	5,320,000 shares
Common stock offered by the selling stockholders	450,000 shares
Total	5,770,000 shares
Over-allotment option to be offered by Sourcefire	865,500 shares
Common stock to be outstanding after this offering	23,113,892 shares
Use of proceeds	We intend to use the net proceeds from this offering for working capital and other general corporate purposes. We may also use a portion of the net proceeds to repay our equipment facility or acquire other businesses, products or technologies. However, we do not have agreements or commitments for any specific repayments or acquisitions at this time. We will not receive any proceeds from the sale of common stock by the selling stockholders. See Use of Proceeds.
Nasdaq Global Market symbol	FIRE

The number of shares to be outstanding after this offering is based on 17,793,892 shares outstanding as of December 31, 2006, and excludes:

- 3,199,903 shares that may be issued upon the exercise of options outstanding as of December 31, 2006 under our stock option plan;
- 36,944 shares that may be issued upon the exercise of warrants outstanding as of December 31, 2006;
- 181,934 shares that were reserved for issuance pursuant to our stock option plan as of December 31, 2006; and
- 27,709 shares that are subject to repurchase by us.

Unless we specifically state otherwise, all information in this prospectus reflects or assumes:

- a 1-to-1.624 reverse split of our common stock, which was effected on February 22, 2007;
- the conversion of all outstanding shares of our preferred stock into shares of our common stock immediately prior to the completion of this offering pursuant to a written consent executed by the holders of the requisite number of shares of each class of our preferred stock to voluntarily convert their shares of our preferred stock into shares of our common stock; and
- the underwriters over-allotment option to purchase up to an additional 865,500 shares of common stock is not exercised.

Table of Contents

SUMMARY CONSOLIDATED FINANCIAL DATA

The table below summarizes our consolidated financial information for the periods indicated and has been derived from our audited consolidated financial statements. You should read the following information together with the more detailed information contained in Selected Consolidated Financial Data, Management s Discussion and Analysis of Financial Condition and Results of Operations and our consolidated financial statements and the accompanying notes appearing elsewhere in this prospectus.

	Year ended December 31,			
	2003	2004	2005	2006
	(in thousands, except share, per share and other operating data)			
Consolidated statement of operations data:				
Revenue:				
Products	$ 8,153	$ 12,738	$ 23,589	$ 30,219
Services	1,328	3,955	9,290	14,707
Total revenue	9,481	16,693	32,879	44,926
Cost of revenue:				
Products	2,570	4,533	6,610	8,440
Services	436	872	1,453	2,632
Total cost of revenue	3,006	5,405	8,063	11,072
Gross profit	6,475	11,288	24,816	33,854
Operating expenses:				
Research and development	3,751	5,706	6,831	8,612
Sales and marketing	9,002	12,585	17,135	20,652
General and administrative	2,141	2,905	5,120	5,017
Depreciation and amortization	441	752	1,103	1,230
Total operating expenses	15,335	21,948	30,189	35,511
Loss from operations	(8,860)	(10,660)	(5,373)	(1,657)
Other income (expense), net	16	164	(85)	792
Loss before income taxes	(8,844)	(10,496)	(5,458)	(865)
Income tax expense				(67)
Net loss	(8,844)	(10,496)	(5,458)	(932)
Accretion of preferred stock	(1,262)	(2,451)	(2,668)	(3,819)
Net loss attributable to common stockholders	$ (10,106)	$ (12,947)	$ (8,126)	$ (4,751)
Net loss attributable to common stockholders per common share:				
Basic and diluted	$ (4.69)	$ (4.97)	$ (2.54)	$ (1.40)

Pro forma (unaudited)[1]				(0.06)
Shares used in per common share calculations:				
Basic and diluted	2,156,725	2,602,743	3,200,318	3,389,527
Pro forma (unaudited)[1]				16,885,981
Other operating data:				
Number of sales in excess of $500,000	2	5	9	14
Number of new 3D customers	161	136	149	273
Cumulative number of Fortune 100 3D customers at end of period	10	17	24	26
Number of full-time employees at end of period	84	107	135	182

(footnotes on following page)

Table of Contents

	As of December 31, 2006		
	Actual	Pro forma[2]	Pro forma As Adjusted[3]
		(unaudited) (in thousands)	
Consolidated balance sheet data:			
Cash and cash equivalents	$ 13,029	$ 13,029	$ 84,793
Held-to-maturity investments	13,293	13,293	13,293
Total assets	49,952	49,952	121,716
Long-term debt	1,312	1,312	1,312
Total liabilities	22,104	22,104	22,104
Total convertible preferred stock	66,747		
Total stockholders equity (deficit)	(38,899)	27,848	99,612

(1) Pro forma to give effect to the conversion of all outstanding shares of our preferred stock into shares of our common stock immediately prior to the completion of this offering.

(2) The pro forma balance sheet data reflect the conversion of all outstanding shares of our preferred stock into shares of our common stock immediately prior to the completion of this offering.

(3) The pro forma as adjusted balance sheet data reflect the conversion of all outstanding shares of our preferred stock into shares of our common stock immediately prior to the completion of this offering and our receipt of estimated net proceeds of $71.8 million from our sale of 5,320,000 shares of common stock that we are offering at the initial public offering price of $15.00 per share, after deducting estimated underwriting discounts and commissions and estimated offering expenses payable by us.

Table of Contents

RISK FACTORS

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

Risks Related to Our Business

We have had operating losses since our inception and we expect operating expenses to increase in the foreseeable future and we may never reach or maintain profitability.

We have incurred operating losses each year since our inception in 2001. Our net loss was approximately $10.5 million for the year ended December 31, 2004, $5.5 million for the year ended December 31, 2005 and $0.9 million for the year ended December 31, 2006. Our accumulated deficit as of December 31, 2006 is approximately $38.9 million. Becoming profitable 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 and our losses have generally been decreasing when compared to prior periods, you should not assume that we will become profitable in the near future or at any other time. We may never achieve profitability and, even if we do, we may not be able to maintain or increase our level of profitability. We expect that our operating expenses will continue to increase in the foreseeable future as we seek to expand our customer base, increase our sales and marketing efforts, continue to invest in research and development of our technologies and product enhancements and incur significant new costs associated with becoming a public company. These efforts may be more costly than we expect and we may not be able to increase our revenue enough to offset our higher operating expenses. In addition, if our new products and product enhancements fail to achieve adequate market acceptance, our revenue will suffer. If we cannot increase our revenue at a greater rate than our expenses, we will not become and remain profitable.

We face intense competition in our market, 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 network security monitoring, detection, prevention and response solutions 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 include large software companies, software or hardware network infrastructure companies, smaller software companies offering relatively limited 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.

Mergers or consolidations among these competitors, or acquisitions of our competitors by large companies, present heightened competitive challenges to our business. For example, Symantec Corporation, Cisco Systems, Inc., McAfee, Inc., 3Com Corporation and Juniper Networks, Inc. have acquired during the past several years smaller companies, which have intrusion detection or prevention technologies and Internet Security Systems, Inc. has recently been acquired by IBM. These acquisitions will make these combined entities potentially more formidable competitors to us if such products and offerings are effectively integrated. 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 be able to adapt more quickly to new or emerging technologies and changes in customer requirements. They also have greater resources to devote to the promotion and sale of their products than we have. In addition, these companies have reduced and could continue to reduce, the price of their security monitoring, detection, prevention and response products and managed security services, which intensifies pricing pressures within our market.

Several companies currently sell software products (such as encryption, firewall, operating system security and virus detection software) 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. The widespread inclusion of comparable features 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 or our customers or distributors could internally develop alternatives to our products and either development could impair our sales.

We may face competition from emerging companies as well as established companies who have not previously entered the market for network security products. Established companies may not only develop their own network intrusion detection and prevention products, but they may also acquire or establish product integration, distribution or other cooperative relationships with our current competitors. Moreover, our large corporate customers and potential customers could develop network security software internally, which would reduce our potential revenue. New competitors or alliances among competitors may 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. For example, one of our competitors, Internet Security Systems, Inc., has recently been acquired by IBM and the combined company, if successfully integrated, could become a formidable competitor to us. In addition, the acquisition could result in a loss of our current sales to IBM if IBM were to discontinue reselling our products and services. If these new competitors are successful, we would lose market share and our revenue would likely decline.

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;
- the timing, size and contract terms of orders received, which have historically been highest in the fourth quarter (representing more than one-third of our total revenue in recent years), but may fluctuate seasonally in different ways;
- the level of perceived threats to network security, which may fluctuate from period to period;
- the level of demand for products sold by original equipment manufacturers, or OEMs, resellers and distributors that incorporate and resell our technologies;

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;

Table of Contents

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. 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 will likely 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 any period. If we fail to meet or exceed such expectations for these or any other reasons, the market price of our shares could fall substantially and we could face costly securities class action suits. 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.

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 will be harmed.

The market for network security products is relatively new and 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 new 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, while not 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, we may in the future 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 will suffer.

We spend substantial amounts of time and money to research and develop new products and enhanced versions of Snort, the Defense Center and our Intrusion Sensors and RNA products to incorporate additional features, improved functionality or other enhancements in order to meet our customers rapidly evolving demands for network 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 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.

Table of Contents

Our new products or enhancements could fail to attain sufficient market acceptance for many reasons, including:

- 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 intrusion prevention or other 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, which problems are more likely due to our just-in-time manufacturing and inventory practices.

If our new products or enhancements (including, but not limited to, version 4.0 of RNA, which we plan to introduce in the next several months) do not achieve adequate acceptance in the market, our competitive position will 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 if our relationships with our largest customers are impaired, our revenue could decline.

In 2004, 2005 and 2006, 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 for each respective period. Part of our growth strategy is to sell additional products to our existing customers and, in particular, to up-sell our RNA products to customers that previously bought our Intrusion Sensor products. 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 Snort, Intrusion Sensors and RNA 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. Approximately 82% of our customers renewed their maintenance and support agreements upon expiration in the year ended December 31, 2006. No single customer contributed greater than 10% of our recurring maintenance and support revenues in 2005 or in 2006. If customers choose not to continue their maintenance service, our revenue may decline.

If we cannot attract sufficient government agency customers, our revenue and competitive position will suffer.

Contracts with the U.S. federal and state and other national and state government agencies accounted for 17% of our total revenue for the year ended December 31, 2004, 16% for the year ended December 31, 2005 and 11% for the year ended December 31, 2006. We lost many government agency customers when a foreign company tried unsuccessfully to acquire us in late 2005 and early 2006. Since then, we have been attempting to regain government customers, which subjects us to a number of risks, including:

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;

Budgetary Constraints and Cycles. Demand and payment for our products and services are impacted by public sector budgetary cycles and funding availability, with funding reductions or delays adversely impacting public sector demand for our products, including delays caused by continuing resolutions or other temporary funding arrangements resulting from the current congressional transition;

Table of Contents

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 cancelled 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 cancelled because of default, we may only be able to collect for products and alternative products and services delivered to the customer;

Governmental Audits. National governments and other 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 if the audit uncovers improper or illegal activities.

Replacing Existing Products. After we announced in October 2005 that we had agreed to be acquired by a foreign company, many government agencies were unwilling to buy products from us and instead purchased and installed products sold by our competitors. The proposed acquisition was terminated in April 2006 following objections from the Committee on Foreign Investment in the United States. Since that time, we have been attempting to retain government agency customers. Many government agencies, however, 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 are subject to risks of operating internationally that could impair our ability to grow our revenue abroad.

We market and sell our software in North America, South America, Europe, Asia and Australia and we plan to establish additional sales presence in these and other parts of the world. Therefore, we are subject to risks associated with having worldwide operations. Sales to customers located outside of the United States accounted for approximately 18% of our total revenue in the year ended December 31, 2004, approximately 18% of our total revenue in the year ended December 31, 2005 and approximately 19% of our total revenue in the year ended December 31, 2006. 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;

unexpected changes in regulatory requirements;

difficulties and costs of staffing and managing foreign operations;

import and export controls;

the uncertainty of protection for intellectual property rights in some countries;

costs of compliance with foreign laws and laws applicable to companies doing business in foreign jurisdictions;

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

multiple and possibly overlapping tax structures; and

foreign currency exchange rate fluctuations.

To date, a substantial portion of our sales have been denominated in U.S. dollars, and we have not used risk management techniques or hedged the risks associated with fluctuations in foreign currency exchange rates. In the future, if we do not engage in hedging transactions, our results of operations will be subject to losses from fluctuations in foreign currency exchange rates.

Table of Contents

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

We expect that the net proceeds from this offering together with current cash, cash equivalents, borrowings under our credit facility and short-term investments should be sufficient to meet our anticipated cash needs for working capital and capital expenditures for at least the next 24 months. However, our business and operations may consume resources faster than we anticipate. In the future, we may need to raise additional funds to expand our sales and marketing and research and development efforts or to make acquisitions. Additional financing may not be available on favorable terms, if at all. If adequate funds are not available on acceptable terms, we may be unable to fund the expansion of our sales and marketing and research and development efforts or take advantage of acquisition or other opportunities, which could seriously harm our business and operating results. If we issue debt, the debt holders would 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 will experience dilution, and the new equity securities could have rights senior to those of our common stock.

Our inability to acquire and integrate other businesses, products or technologies could seriously harm our competitive position.

In order to remain competitive, we intend to acquire additional businesses, products or technologies. If we identify an appropriate acquisition candidate, we may not be successful in negotiating the terms of the acquisition, financing the acquisition, or effectively integrating the acquired business, product or technology into our existing business and operations. Any acquisitions we are able to complete may not be accretive to earnings. Further, completing a potential acquisition and integrating an acquired business will significantly divert management time and resources.

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

While we created a majority of the current Snort code base, a portion of the current Snort code was created by the combined efforts of the Company and the open source software community and a portion was created solely by the open source community. We believe that the portions of the Snort code base created by anyone other than by us are required to be licensed by us pursuant to the GNU General Public License, or GPL, which is how we currently license Snort. There is a risk, however, that a third party could claim some ownership rights in Snort, and attempt to prevent us from commercially licensing Snort in the future (rather than pursuant to the GPL as it is currently licensed) and 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 and result in our having to pay substantial compensation to the party claiming ownership.

Our products contain third party 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.

Our products are distributed with software programs licensed to us by third party authors under open source licenses, which may include the GPL, the GNU Lesser Public License, or LGPL, the BSD License and the Apache License. These open source software programs include, without limitation, Snort®, Linux, Apache, Openssl, Etheral, IPTables, Tcpdump and Tripwire. These third party open source programs are typically licensed to us for a minimal fee or no fee at all, and the underlying license agreements generally require us to make available to the open source user community the source code for such programs, as well as the source code for any modifications or derivative works we create based on these third party open source software programs. With the exception of Snort, we have not created any modifications or derivative works to any other open source software programs referenced above. We regularly release updates and upgrades to the Snort software program under the terms and conditions of the GNU GPL

version 2. Included with our software and/or appliances are copies of the relevant source code and licenses for the open source programs. Alternatively, we include instructions to users on how to obtain copies of the relevant open source code and licenses. Additionally, if we combine our proprietary software with third party open source software in a certain manner, we could, under the terms of certain of these open source license agreements, be required to release the source code of our proprietary software. This could also allow our competitors to create similar products, which would result in a loss of our product sales. We do not provide end users a copy of the source

code to our proprietary software because we believe that the manner in which our proprietary software is aligned with the relevant open source programs does not create a modification or derivative work of that open source program requiring the distribution of our proprietary source code. Our ability to commercialize our products by incorporating third party open source software may be restricted because, among other reasons:

- the terms of open source license agreements may be unclear and subject to varying interpretations, which could result in unforeseen obligations regarding our proprietary products;
- it may be difficult to determine the developers of open source software and whether such licensed software infringes another party s intellectual property rights;
- competitors will have greater access to information by obtaining these open source products, which may help them develop competitive products; and
- open source software potentially increases customer support costs because licensees can modify the software and potentially introduce errors.

The software program Linux is included in our products and is licensed under the GPL. The GPL is the subject of litigation in the case of The SCO Group, Inc. v. International Business Machines Corp., pending in the United States District Court for the District of Utah. It is possible that the court could rule that the GPL is not enforceable in such litigation. Any ruling by the court that the GPL is not enforceable could have the effect of limiting or preventing us from using Linux as currently implemented.

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.

When we undertake actions to protect and maintain ownership and control over our proprietary intellectual property, including patents, copyrights and trademark rights, our standing in the open source community could be diminished which could result in a limitation on our ability to continue 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.

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

We rely primarily on copyright, trademark, patent and trade secrets laws, confidentiality procedures and contractual provisions to protect our proprietary rights. As of the date hereof, we had 25 patent applications pending for examination in the U.S. and foreign jurisdictions. We also hold numerous registered United States and foreign trademarks and have a number of trademark applications pending in the United States and in foreign jurisdictions. Valid patents may not be issued from pending applications, and the claims allowed on any patents may not be sufficiently broad to protect our technology or products. Any issued patents may be challenged, invalidated or circumvented, and any rights granted under these patents may not actually provide adequate protection or competitive advantages to us. Despite our efforts to protect our proprietary rights, unauthorized parties may attempt to copy aspects of our products or to obtain and use information that we regard as proprietary. Policing unauthorized use of our technologies or products is difficult. Our products incorporate open source Snort software, which is readily available to the public. 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. It is possible that we may have to resort to litigation to enforce and protect our copyrights, trademarks, patents and trade secrets, which litigation could be costly and a diversion of

management resources. If we are unable to protect our proprietary rights to the totality of the features in our software and products (including aspects of our software and products protected other than by patent rights), we may find ourselves at a competitive disadvantage to others who need not incur the additional expense, time and effort required to create the innovative products that have enabled us to be successful to date.

In limited instances we have agreed to place, and in the future may place, source code for our software in escrow, other than the Snort source code which is publicly available. In most cases, the source code may be made available to certain of our customers and OEM partners in the event that we file for bankruptcy or materially fail to support our products. This may increase the likelihood of misappropriation or other misuse of our software. We

have agreed to source code escrow arrangements in the past only rarely and usually only in connection with prospective customers considering a significant purchase of our products and services.

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

Technology products such as ours, which interact with multiple components of complex networks, are increasingly subject to infringement claims as the functionality of products in different industry segments overlaps. In particular, our RNA technology is a new technology for which we have yet be issued a patent. It is possible that other companies have patents with respect to technology similar to our technology, including RNA. Ten of our 25 pending patent applications relate to our RNA technology and were filed in 2003, 2004 and 2005. If others filed patent applications before us, which contain allowable claims within the scope of our RNA technology, then we may be found to infringe on such patents, if and when they are issued. We are aware of at least one company that has filed an application for a patent that, on its face, contains claims that may be construed to be within the scope of the same broad technology area as our RNA technology. That company, PredatorWatch, has filed suit against us for misappropriation and incorporation in our RNA technology of its proprietary rights (see discussion in next risk factor). PredatorWatch has separately notified us that it believes that our RNA technology is covered by claims in a pending patent application filed by PredatorWatch. Unless and until the U.S. Patent and Trademark Office, or PTO, issues a patent to an applicant, there can be no way to assess a potential patentee s right to exclude. Depending on the timing and substance of these patents and patent applications, our products, including our RNA technology, may infringe the proprietary rights of others, and we may be subject to litigation with respect to any alleged infringement. The application of patent law to the software industry is particularly uncertain as the PTO has only recently begun to issue software patents in large numbers and there is a backlog of software related patent applications pending claiming inventions whose priority dates may pre-date development of our own proprietary software. Additionally, in our customer contracts we typically agree to indemnify our customers if they incur losses resulting from a third party claim that their use of our products infringes upon the intellectual property rights of a third party. Any potential intellectual property claims against us, with or without merit, could:

- be very expensive and time consuming to defend;
- require us to indemnify our customers for losses resulting from such claims;
- cause us to cease making, licensing or using software or products that incorporate the challenged intellectual property;
- cause product shipment and installation delays;
- require us to redesign our products, which may not be feasible;
- divert management s attention and resources; or
- require us to enter into royalty or licensing agreements in order to obtain the right to use a necessary product or component.

Royalty or licensing agreements, if required, may not be available on acceptable terms, if at all. A successful claim of infringement against us and our failure or inability to license the infringed or similar technology could prevent us from distributing our products and cause us to incur great expense and delay in developing non-infringing products.

We have been sued by a company claiming that we misappropriated and incorporated its proprietary rights into our 3D product line and our defense of these claims is costly, diverts the attention of our management and may be unsuccessful.

On April 25, 2006, we were served with a complaint filed by PredatorWatch (now named NetClarity) in the Superior Court for Suffolk County, Massachusetts. The plaintiff alleges that we, Martin F. Roesch, our Chief Technology Officer, and Inflection Point Associates, L.P., the general partner of one of our stockholders, Inflection Point Ventures, L.P. (i) misappropriated and incorporated the plaintiff s trade secrets; (ii) breached an oral agreement of confidentiality; (iii) breached a covenant of good faith and fair dealing owed to the plaintiff;

Table of Contents

(iv) were unjustly enriched; (v) misrepresented certain material facts to the plaintiff, upon which the plaintiff relied to its detriment; and (vi) engaged in unfair and deceptive acts in violation of Massachusetts state law. The plaintiff has sought to recover amounts to be ascertained and established, as well as double and treble damages and attorney s fees.

Litigation is subject to inherent uncertainties, especially in cases like this where sophisticated factual issues must be assessed and complex technical issues must be resolved. In addition, these types of cases involve issues of law that are evolving, presenting further uncertainty. Our defense of this litigation, regardless of the merits of the complaint, has been, and will likely continue to be, time consuming, extremely costly and a diversion of time and attention for our technical and management personnel. Through December 31, 2006, we have spent approximately $198,000 in legal fees and expenses on this litigation and expect to incur substantial additional expenses even if we ultimately prevail. Publicity related to this litigation could likely have a negative impact on our sales of our 3D product line and a negative impact on the price of our common stock. Sales of our 3D product line amounted to $21.7 million and $26.9 million for 2005 and 2006, respectively, or 66% and 60% of our total sales for 2005 and 2006, respectively.

A failure to prevail in the litigation could result in one or more of the following:

- our paying substantial monetary damages, which could be tripled if any misappropriation is found to have been willful, and which may include paying an ongoing significant royalty to PredatorWatch or compensation for lost profits to PredatorWatch;
- our paying substantial punitive damages;
- our having to provide an accounting of all revenue received from selling our 3D product line in its current form;
- the issuance of a preliminary or permanent injunction requiring us to stop selling our 3D product line in its current form;
- our having to redesign our 3D product line, which could be costly and time-consuming and could substantially delay our 3D product line shipments, assuming that a redesign is feasible;
- our having to reimburse PredatorWatch for some or all of its attorneys fees and costs, which would be substantial;
- our having to obtain from PredatorWatch a license to use its technology, which might not be available on reasonable terms, if at all; or
- our having to indemnify our customers against any losses they may incur due to the alleged infringement.

Additionally, PredatorWatch has separately notified us that they believe that our RNA technology and 3D security solutions are covered by claims contained in a pending patent application. This pending patent application has not issued as a patent, but in the event it does issue, PredatorWatch could file an additional complaint to include a patent infringement claim against us.

If we are enjoined from selling our 3D product line in its current form, we may be required to redesign our 3D product line to avoid infringing on the intellectual property rights of others. If we are unable to efficiently redesign commercially acceptable products, our sales will decline substantially. This litigation is at an early stage, so we cannot predict its course or its costs to us. We do, however, expect to continue to incur significant costs in defending against this litigation and these costs could increase substantially if this litigation approaches or enters a trial phase. It is

possible that these costs could substantially exceed our expectations in future periods. For a more detailed description of this litigation, please see Business Legal Proceedings.

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

We utilize various types of software licensed from unaffiliated third parties. For example, we license database software from MySQL that we use in our Intrusion Sensors, our RNA Sensors and our Defense Centers. Our

Table of Contents

Agreement with MySQL permits us to distribute MySQL software on our products to our customers worldwide until December 31, 2010. We amended our MySQL agreement on December 29, 2006 to give 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 for our products, we would be required to expend resources to implement a replacement database in our products, and there would be no guarantee that we would be able to procure the replacement on the same or similar commercial terms.

In addition to MySQL, we rely on other open source software, such as the Linux operating system, the Apache web server and OpenSSL, a secure socket layer implementation. These open source programs are licensed to us under various open source licenses. For example, Linux is licensed under the GNU General Public License, while Apache and OpenSSL are licensed under other forms of open source license agreements. If we could no longer rely on these open source programs, the functionality of our products would be impaired and, we would be required to expend significant resources to find suitable alternatives.

Our business would be disrupted if any of the software we license from others or functional equivalents of this software were either no longer available to us or no longer offered to us on commercially reasonable terms. In either case, we would be required to either redesign our products to function with software available from other parties or develop these components ourselves, which would 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.

Defects, errors or vulnerabilities in our software products would harm our reputation and divert 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, eliminate or work-around errors or defects or to address and eliminate vulnerabilities;
- loss of existing or potential customers;
- delayed or lost revenue;
- delay or failure to attain market acceptance;
- increased service, warranty, product replacement and product liability insurance costs; and
- negative publicity, which will 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 security measures could misappropriate the confidential information or other valuable property of customers using our products, or interrupt their operations. If that happens, affected customers or others may sue us. In addition, we may face liability for breaches of our product warranties, product failures or damages caused by faulty installation of our products. Provisions in our contracts relating to warranty disclaimers and liability limitations may 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. 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 are vulnerable to, and may be targeted by, hackers.

Like other companies, our websites, networks, information systems, products and services may be targets for sabotage, disruption or misappropriation by hackers. As a leading network security solutions company, we are a

high profile target and our networks, products and services may have vulnerabilities that may be targeted by hackers. Although we believe we have sufficient controls in place to prevent disruption and misappropriation, and to respond to such situations, we expect these efforts by hackers to continue. If these efforts are successful, our operations, reputation and sales could be adversely affected.

We utilize a just-in-time contract manufacturing and inventory process, which increases our vulnerability to supply disruption.

Our ability to meet our customers demand for certain of our products depends upon obtaining adequate hardware platforms on a timely basis, which must be integrated with our software. We purchase hardware platforms through our contract manufacturers from a limited number of suppliers on a just-in-time basis. In addition, 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 depend on a single source to manufacture our enterprise class intrusion sensor product; if that sole source were to fail to satisfy our requirements, our sales revenue would decline and our reputation would be harmed.

We rely on one manufacturer, Bivio Networks, to build the hardware platform for two models of our intrusion sensor products that are used by our enterprise class customers. These enterprise class intrusion sensor products are purchased directly by customers for their internal use and are also utilized by third party managed security service providers to provide services to their customers. Revenue resulting from sales of these enterprise class intrusion sensor products accounted for approximately 3.8% of our product revenue in the year ended December 31, 2005 and approximately 21% of our product revenue in the year ended December 31, 2006. The unexpected termination of our relationship with Bivio Networks would be disruptive to our business and our reputation which could result in a decline in our revenue as well as shipment delays and possible increased costs as we seek and implement production with an alternate manufacturer.

Our inability to hire and retain key personnel would slow our growth.

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

Our future success will depend to a significant extent on the continued services of Martin Roesch, our founder and Chief Technology Officer, and E. Wayne Jackson, III, our Chief Executive Officer. The loss of the services of either of these or other individuals could adversely affect our business and could divert other senior management time in searching for their replacements.

We depend on resellers and distributors for our sales; if they fail to perform as expected, our revenue will suffer.

Part of our business strategy involves entering into additional agreements with resellers and distributors that permit them to resell our products and service offerings. Revenue resulting from our resellers and distributors accounted for approximately 46% of our total revenue in the year ended December 31, 2004, approximately 48% of our total revenue in the year ended December 31, 2005 and approximately 49% of our total revenue in the year ended December 31, 2006. For the year ended December 31, 2005 and for the year ended December 31, 2006, no single reseller, distributor, customer or OEM accounted for more than ten percent of our total revenue. There is a risk that our pace of entering into such agreements may slow, or that our existing agreements may not produce as much business as we anticipate. There is also a risk that some or all of our resellers or distributors may be acquired,

may change their business models or may go out of business, any of which could have an adverse effect on our business. For example, IBM, our current reseller, recently completed its acquisition of Internet Security Systems, Inc., one of our competitors. Sales of our products to IBM or where IBM helped influence the sales process as a percentage of our total revenue were 3.1% and 1.2% for the year ended December 31, 2006 and the year ended December 31, 2005, respectively. While we have received oral assurances from IBM that it does not expect any material change to our reseller relationship solely on account of its acquisition of Internet Security Systems, Inc., we cannot currently anticipate how our relationship with IBM may change. IBM may decide to discontinue reselling our products and services.

If we do not continue to establish and effectively manage our OEM relationships, our revenue could decline.

Our ability to sell our network security software products in new markets and to increase our share of existing markets will be impaired if we fail to expand our indirect distribution channels. Our sales strategy involves the establishment of multiple distribution channels domestically and internationally through strategic resellers, system integrators and OEMs. We have alliances with OEMs such as IBM and Nokia and we cannot predict the extent to which these companies will be successful in marketing or selling our software. These agreements could be terminated on short notice and they do not prevent our OEMs, systems integrators, strategic resellers or other distributors from selling the network security software of other companies, including our competitors. IBM and Nokia or any other OEM, system integrator, strategic reseller or distributor could give higher priority to other companies software or to their own software than they give to ours, which could cause our revenue to decline. Additionally, IBM recently completed its acquisition of Internet Security Systems, Inc., one of our competitors. Our ability to sell our network security software products through IBM as a reseller or have our product sales influenced by them as a partner could be materially diminished.

Our inability to effectively manage our expected headcount growth and expansion and our additional obligations as a public company could seriously harm our ability to effectively run our business.

Our historical growth has placed, and our intended future growth is likely to continue to place, a significant strain on our management, financial, personnel and other resources. We will likely not continue to grow at our historical pace due to limits on our resources. We have grown from 84 employees at December 31, 2003 to 182 employees at December 31, 2006. Since January 1, 2005, we have opened additional sales offices and have significantly expanded our operations. This rapid growth has strained our facilities and required us to lease additional space at our headquarters. In several recent quarters, we have not been able to hire sufficient personnel to keep pace with our growth. In addition to managing our expected growth, we will have substantial additional obligations and costs as a result of being a public company. These obligations include investor relations, preparing and filing periodic SEC reports, developing and maintaining internal controls over financial reporting and disclosure controls, compliance with corporate governance rules, Regulation FD and other requirements imposed on public companies by the SEC and the Nasdaq Global Market. Fulfilling these additional obligations will make it more difficult to operate a growing company. Any failure to effectively manage growth or fulfill our obligations as a public company could seriously harm our ability to respond to customers, the quality of our software and services and our operating results. To effectively manage growth and operate a public company, we will need to implement additional management information systems, improve our operating, administrative, financial and accounting systems and controls, train new employees and maintain close coordination among our executive, engineering, accounting, finance, marketing, sales and operations organizations.

Risks Related to Your Investment

The price of our common stock may be subject to wide fluctuations and may trade below the initial public offering price.

Before this offering, there has not been a public market for our common stock. The initial public offering price of our common stock was determined by negotiations between us and representatives of the underwriters, based on numerous factors, including those that we discuss under Underwriters. This price may not be indicative of the market price of our common stock after this offering. We cannot assure you that an active public market for our common stock will develop or be sustained after this offering. The market price of our common stock also could be

subject to significant fluctuations. As a result, you may not be able to sell your shares of our common stock quickly or at prices equal to or greater than the price you paid in this offering.

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;
- 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 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 and may dilute your voting power and your ownership interest in us.

After the completion of this offering, we will have 23,113,892 outstanding shares of common stock (23,979,392 shares of common stock if the underwriters exercise in full their option to purchase additional shares). This number is comprised of all the shares of our common stock that we are selling in this offering, which may be resold immediately in the public market. Subject to certain exceptions described under the caption Underwriters, we and all of our directors and executive officers and certain of our stockholders and option holders have agreed not to offer, sell or agree to sell, directly or indirectly, any shares of common stock without the permission of the underwriters for a period of 180 days from the date of this prospectus. When this period expires we and our locked-up stockholders will be able to sell our shares in the public market. Sales of a substantial number of such shares upon expiration, or early release, of the lock-up (or the perception that such sales may occur) could cause our share price to fall.

Sales of substantial amounts of our common stock in the public market following our initial public offering, 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.

We also may issue our shares of common stock from time to time as consideration for future acquisitions and investments. If any such acquisition or investment is significant, the number of shares that we may issue may in turn be significant. In addition, we may also grant registration rights covering those shares in connection with any such

acquisitions and investments.

Investors purchasing common stock in this offering will experience immediate and substantial dilution.

The initial public offering price of our common stock is substantially higher than the net tangible book value per outstanding share of our common stock immediately after this offering. As a result, you will pay a price per share that substantially exceeds the book value of our tangible assets after subtracting our liabilities. Purchasers of our common stock in this offering will incur immediate and substantial dilution of $10.69 per share in the net tangible book value of our common stock from the initial public offering price of $15.00 per share. If the underwriters exercise in full their option to purchase additional shares, there will be dilution of $10.34 per share in the net tangible book value of our common stock.

Table of Contents

As a result of becoming a public company, we will be obligated to develop and maintain proper and effective internal controls over financial reporting and will be subject to other requirements that will be burdensome and costly. We may not complete our analysis of our internal controls over financial reporting in a timely manner, or these internal controls may not be determined to be effective, which may adversely affect investor confidence in our company and, as a result, the value of our common stock.

We will be required, pursuant to Section 404 of the Sarbanes-Oxley Act of 2002 (Section 404), to furnish a report by management on, among other things, the effectiveness of our internal control over financial reporting for the first fiscal year beginning after the effective date of this offering. This assessment will need to include disclosure of any material weaknesses identified by our management in our internal control over financial reporting, as well as a statement that our auditors have issued an attestation report on our management s assessment of our internal controls.

We are just beginning the costly and challenging process of compiling the system and processing documentation before we perform the evaluation needed to comply with Section 404. We may not be able to complete our evaluation, testing and any required remediation in a timely fashion. During the evaluation and testing process, if we identify one or more material weaknesses in our internal control over financial reporting, we will be unable to assert that our internal control is effective. If we are unable to assert that our internal control over financial reporting is effective, or if our auditors are unable to attest that our management s report is fairly stated or they are unable to express an opinion on the effectiveness of our internal control, we could lose investor confidence in the accuracy and completeness of our financial reports, which would have a material adverse effect on the price of our common stock. Failure to comply with the new rules might make it more difficult for us to obtain certain types of insurance, including director and officer liability insurance, and we might be forced to accept reduced policy limits and coverage and/or incur substantially higher costs to obtain the same or similar coverage. The impact of these events could also make it more difficult for us to attract and retain qualified persons to serve on our board of directors, on committees of our board of directors, or as executive officers.

In addition, as a public company, we will incur significant additional legal, accounting and other expenses that we did not incur as a private company, and our administrative staff will be required to perform additional tasks. For example, in anticipation of becoming a public company, we will need to create or revise the roles and duties of our board committees, adopt disclosure controls and procedures, retain a transfer agent, adopt an insider trading policy and bear all of the internal and external costs of preparing and distributing periodic public reports in compliance with our obligations under the securities laws. In addition, changing laws, regulations and standards relating to corporate governance and public disclosure, and related regulations implemented by the Securities and Exchange Commission and the Nasdaq Global Market, are creating uncertainty for public companies, increasing legal and financial compliance costs and making some activities more time consuming. These laws, regulations and standards are subject to varying interpretations, in many cases due to their lack of specificity, and, as a result, their application in practice may evolve over time as new guidance is provided by regulatory and governing bodies. We intend to invest resources to comply with evolving laws, regulations and standards, and this investment may result in increased general and administrative expenses and a diversion of management s time and attention from revenue-generating activities to compliance activities. If our efforts to comply with new laws, regulations and standards differ from the activities intended by regulatory or governing bodies due to ambiguities related to practice, regulatory authorities may initiate legal proceedings against us and our business may be harmed.

Table of Contents

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

We intend to amend and restate our certificate of incorporation and bylaws, both of which will become effective upon the completion of this offering, to add provisions that may delay or prevent an acquisition of us 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 the ability of our board of directors to issue preferred stock without stockholder approval. In addition, because we are incorporated in Delaware, we are governed by the provisions of Section 203 of the Delaware General Corporation Law, which prohibits stockholders owning in excess of 15% of our outstanding voting stock from merging or combining with us. Although we believe these provisions collectively provide for an opportunity to receive higher bids by requiring potential acquirors to negotiate with our board of directors, they would apply even if the offer may be considered beneficial by some stockholders. 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.

Table of Contents

SPECIAL NOTE REGARDING FORWARD-LOOKING STATEMENTS

This prospectus 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 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 network security products;
- our plans to continue to invest in and develop innovative technology and products for our existing markets and other network security markets;
- the timing of expected introductions of new or enhanced products;
- our expectation of growth in our customer base and increasing sales to existing customers;
- our plans to increase revenue through more relationships with original equipment manufacturers, resellers, distributors, government suppliers and co-marketers;
- our plans to grow international sales;
- our plans to acquire and integrate new businesses and technologies;
- our plans to hire more network security experts 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 prospectus are made only as of the date of this prospectus. 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, the following:

- the market for network security products is rapidly evolving and the complex technology incorporated in our products makes them difficult to develop, and 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 will be harmed;
- defects, errors or vulnerabilities in our software products would harm our reputation and divert resources;
- in the future, we may not be able to secure financing necessary to operate and grow our business as planned;

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

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

new competitors could emerge or our customers or distributors could internally develop alternatives to our products and either development could impair our sales;

if our new products and product enhancements do not achieve sufficient market acceptance, our results of operations and competitive position will suffer;

if existing customers do not make subsequent purchases from us or if our relationships with our largest customers are impaired, our revenue could decline;

Table of Contents

if we cannot attract sufficient government agency customers, our revenue and competitive position will suffer;

if we do not continue to establish and effectively manage our OEM relationships, our revenue could decline;

we are subject to risks of operating internationally that could impair our ability to grow our revenue abroad;

our inability to acquire and integrate other businesses, products or technologies could seriously harm our competitive position;

our inability to hire and retain key personnel would slow our growth; and

our inability to effectively manage our headcount growth and expansion could seriously harm our ability to effectively run our business.

We operate in an industry in which it is difficult to obtain precise industry and market information. Although we have obtained some industry data from outside sources that we believe to be reliable, in certain cases we have based certain statements contained in this prospectus regarding our industry and our position in the industry on our estimates concerning, among other things, our customers and competitors. These estimates are based on our experience in the industry, conversations with our principal suppliers and customers and our own investigations of market conditions. The statistical data contained in this prospectus regarding the network security software industry are our statements, which are based on data we obtained from industry sources.

SOURCEFIRE®, SNORT®, the Sourcefire logo, the Snort and Pig logo, SECURITY FOR THE REAL WORLD™, SOURCEFIRE DEFENSE CENTER™, SOURCEFIRE 3D™, RNA™ and certain other trademarks and logos are trademarks or registered trademarks of Sourcefire, Inc. in the United States and other countries. This prospectus also refers to the products or services of other companies by the trademarks and trade names used and owned by those companies.

Table of Contents

USE OF PROCEEDS

We estimate that we will receive net proceeds from this offering of approximately $71.8 million, based on the initial public offering price of $15.00 per share and after deducting underwriting discounts and commissions and other estimated expenses of $2.5 million payable by us. If the underwriters option to purchase additional shares in this offering is exercised in full we estimate that our net proceeds will be approximately $83.8 million. We will not receive any proceeds from the sale of shares of our common stock by the selling stockholders, one of which is our Chief Executive Officer. See Principal and Selling Stockholders for more information.

We intend to use the net proceeds to us from this offering for working capital and other general corporate purposes, including financing our growth, developing new products and funding capital expenditures. We may seek to finance our growth by, for example, expanding our direct sales force in international markets and by hiring additional personnel beyond our current plans to bring products to market sooner. Some possible capital expenditures include, without limitation, (i) procuring and installing an enterprise resource planning system, (ii) purchasing additional development and testing equipment for our security lab and (iii) acquiring additional security-related technology for further development. In addition, we may choose to repay the equipment line portion of our credit facility with Silicon Valley Bank or expand our current business through acquisitions of other businesses, products or technologies. However, we do not have agreements or commitments for any specific repayments nor do we have any plans, proposals or arrangements with respect to any specific acquisitions at this time. As of December 31, 2006, the outstanding balance under the equipment line portion of our Silicon Valley Bank credit facility was $1,312,000, bearing interest at annual rates from 6.5%, fixed, to 8.75%, variable based on prime plus 0.5% at December 31, 2006, and maturing between February 2007 and December 2009. The outstanding balance, if any, under the working capital portion of the credit facility must be repaid on March 28, 2007. The proceeds of the equipment line portion of the credit facility were used for furniture, leasehold improvements, personal computers and equipment for our network security lab.

Pending any use, as described above, we plan to invest the net proceeds in short-term, interest-bearing investment grade securities.

DIVIDEND POLICY

We intend to retain all future earnings, if any, for use in the operation of our business and to fund future growth. We have never declared or paid any dividend on our capital stock and do not anticipate paying any dividends for the foreseeable future and the loan and security agreement governing our working capital line of credit restricts our ability to pay dividends or other distributions on our capital stock. The decision whether to pay dividends will be made by our board of directors in light of conditions then existing, including factors such as our results of operations, financial condition and requirements, business conditions and covenants under any applicable contractual arrangements.

Table of Contents

CAPITALIZATION

The following table sets forth our cash and cash equivalents and our capitalization (including long-term debt) as of December 31, 2006:

- on an actual basis;
- on a pro forma basis, giving effect to the conversion of all of the outstanding shares of our preferred stock into 14,302,128 shares of our common stock immediately prior to the completion of this offering pursuant to a written consent executed by the holders of the requisite number of shares of each class of our preferred stock to voluntarily convert their shares of our preferred stock into shares of our common stock; and
- on a pro forma as adjusted basis, giving effect to the conversion of all of the outstanding shares of our preferred stock into 14,302,128 shares of our common stock immediately prior to the completion of this offering and our sale of 5,320,000 shares of common stock in this offering at the initial public offering price of $15.00, and after deducting the underwriting discounts and commissions and estimated offering expenses payable by us.

The numbers of shares of common stock shown as issued and outstanding exclude:

- 3,199,093 shares that may be issued upon the exercise of options outstanding as of December 31, 2006;
- 36,944 shares that may be issued upon the exercise of warrants outstanding as of December 31, 2006;
- 181,934 shares that are reserved for issuance pursuant to our stock option plan as of December 31, 2006; and
- 27,709 shares that are subject to repurchase by us.

You should read this table in conjunction with the consolidated financial statements and the related notes, Management s Discussion and Analysis of Financial Condition and Results of Operations, and Description of Capital Stock included elsewhere in this prospectus.

Table of Contents

	As of December 31, 2006		
	Actual	Pro forma (unaudited)	Pro forma As Adjusted
	(dollars in thousands)		
Cash and cash equivalents	$ 13,029	$ 13,029	$ 84,793
Long-term debt, including current portion	$ 1,312	$ 1,312	$ 1,312
Series A Convertible Preferred Stock, par value $.001 per share: 2,495,410 shares authorized, 2,475,410 shares issued and outstanding, actual; no shares authorized, no shares issued and outstanding, pro forma and pro forma as adjusted	10,308		
Series B Convertible Preferred Stock, par value $.001 per share: 7,132,205 shares authorized, 7,132,205 shares issued and outstanding, actual; no shares authorized, no shares issued and outstanding, pro forma and pro forma as adjusted	14,265		
Series C Convertible Preferred Stock, par value $.001 per share: 5,404,043 shares authorized, 5,404,043 shares issued and outstanding, actual; no shares authorized, no shares issued and outstanding, pro forma and pro forma as adjusted	18,270		
Series D Convertible Preferred Stock, par value $.001 per share: 3,264,449 shares authorized, 3,264,449 shares issued and outstanding, actual; no shares authorized, no shares issued and outstanding, pro forma and pro forma as adjusted	23,879		
Warrants to purchase Series A Convertible Preferred Stock	25		
Total convertible preferred stock and warrants	66,747		
Stockholders equity (deficit):			
Common Stock, par value $.001 per share: 36,500,000 authorized, 3,491,764 issued and outstanding, actual; 36,500,000 shares authorized, 17,793,892 shares issued and outstanding, pro forma; 240,000,000 shares authorized, 23,113,892 shares issued and outstanding, pro forma as adjusted	3	18	23
Preferred Stock, par value $.001 per share: no shares authorized, no shares issued and outstanding, actual and pro forma; 20,000,000 shares authorized, no shares issued and outstanding, pro forma as adjusted			
Unearned compensation			
Additional paid-in capital		66,732	138,491
Accumulated deficit	(38,902)	(38,902)	(38,902)
Total stockholders equity (deficit)	(38,899)	27,848	99,612
Total capitalization (including long-term debt)	$ 29,160	$ 29,160	$ 100,924

28

Table of Contents

DILUTION

Dilution is the amount by which the offering price paid by the purchasers of the common stock sold in the offering exceeds the net tangible book value per share of common stock after the offering. Net tangible book value per share is determined at any date by subtracting our total liabilities from the total book value of our tangible assets and dividing the difference by the number of shares of common stock deemed to be outstanding at that date.

Our pro forma net tangible book value as of December 31, 2006 was $27.8 million, or $1.57 per share, which gives effect to the conversion of all outstanding shares of our preferred stock into 14,302,128 shares of our common stock immediately prior to the completion of this offering. After giving effect to the receipt and our intended use of approximately $71.8 million of estimated net proceeds from our sale of 5,320,000 shares of common stock in this offering at the initial public offering price of $15.00 per share, our pro forma as adjusted net tangible book value as of December 31, 2006 would have been approximately $99.6 million, or $4.31 per share. This represents an immediate increase in pro forma net tangible book value of $2.74 per share to existing stockholders and an immediate dilution of $10.69 per share to new investors purchasing shares of common stock in the offering. The following table illustrates this substantial and immediate per share dilution to new investors:

Initial public offering price per share		$ 15.00
Pro forma net tangible book value per share before this offering	$ 1.57	
Increase per share attributable to investors in this offering	2.74	
As adjusted pro forma net tangible book value per share after this offering		4.31
Dilution per share to new investors		$ 10.69

The following table summarizes on an as adjusted pro forma basis as of December 31, 2006:

- the total number of shares of common stock purchased from us by our existing stockholders and by new investors purchasing shares in this offering;
- the total consideration paid to us by our existing stockholders and by new investors purchasing shares in this offering at the initial public offering price of $15.00 per share (before deducting the estimated underwriting discounts and commissions and estimated offering expenses payable by us in connection with this offering); and
- the average price per share paid by existing stockholders and by new investors purchasing shares in this offering:

	Shares purchased		Total consideration		Average price
	Number	Percent	Amount	Percent	per share
Existing stockholders	17,793,892	77%	$ 56,878,184	42%	$ 3.20
Investors in the offering	5,320,000	23	79,800,000	58	15.00

Total	23,113,892	100%	$ 136,678,184	100%

The tables and calculations above assume no exercise of:

- stock options outstanding as of December 31, 2006 to purchase 3,199,903 shares of common stock at a weighted average exercise price of $2.96 per share; or
- the underwriters over-allotment option.

To the extent any of these options are exercised, there will be further dilution to new investors.

Table of Contents

SELECTED CONSOLIDATED FINANCIAL DATA

The consolidated statement of operations data for the five years ended December 31, 2006 and the consolidated balance sheet data as of December 31, 2002, 2003, 2004, 2005 and 2006 have been derived from our audited consolidated financial statements. The selected consolidated financial data set forth below should be read in conjunction with 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 prospectus. The historical results are not necessarily indicative of the results to be expected in any future period.

	Year ended December 31,				
	2002	2003	2004	2005	2006
	(in thousands, except share, per share and other operating data)				
Consolidated statement of operations data:					
Revenue:					
Products	$ 1,704	$ 8,153	$ 12,738	$ 23,589	$ 30,219
Services	197	1,328	3,955	9,290	14,707
Total revenue	1,901	9,481	16,693	32,879	44,926
Cost of revenue:					
Products	448	2,570	4,533	6,610	8,440
Services	155	436	872	1,453	2,632
Total cost of revenue	603	3,006	5,405	8,063	11,072
Gross profit	1,298	6,475	11,288	24,816	33,854
Operating expenses					
Research and development	1,261	3,751	5,706	6,831	8,612
Sales and marketing	3,179	9,002	12,585	17,135	20,652
General and administrative	1,234	2,141	2,905	5,120	5,017
Depreciation and amortization	153	441	752	1,103	1,230
Total operating expenses	5,827	15,335	21,948	30,189	35,511
Operating loss	(4,529)	(8,860)	(10,660)	(5,373)	(1,657)
Other income (expense), net	22	16	164	(85)	792
Loss before income taxes	(4,507)	(8,844)	(10,496)	(5,458)	(865)
Income tax expense					(67)
Net loss	(4,507)	(8,844)	(10,496)	(5,458)	(932)
Accretion of preferred stock	(356)	(1,262)	(2,451)	(2,668)	(3,819)
Net loss attributable to common stockholders	$ (4,863)	$ (10,106)	$ (12,947)	$ (8,126)	$ (4,751)

Net loss per common share:					
Basic and diluted	$ (2.61)	$ (4.69)	$ (4.97)	$ (2.54)	$ (1.40)
Pro forma (unaudited)[1]					$ (0.06)
Shares used in per common share calculations:					
Basic and diluted	1,865,663	2,156,725	2,602,743	3,200,318	3,389,527
Pro forma (unaudited)[1]					16,885,981
Other operating data:					
Number of sales in excess of $500,000	1	2	5	9	14
Number of new 3D customers		161	136	149	273
Cumulative number of Fortune 100 3D customers at end of period	3	10	17	24	26
Number of full-time employees at end of period	46	84	107	135	182

(footnotes on following page)

Table of Contents

	As of December 31,				
	2002	2003	2004	2005	2006
Consolidated balance sheet data:					
Cash and cash equivalents	$ 2,991	$ 5,315	$ 3,563	$ 1,106	$ 13,029
Held-to-maturity investments			5,751	2,005	13,293
Total assets	4,928	10,316	20,016	21,250	49,952
Long-term debt	580	345	461	990	1,312
Total liabilities	2,031	5,166	10,177	16,340	22,104
Total convertible preferred stock	7,716	19,958	37,339	40,007	66,747
Total stockholders equity (deficit)	(4,819)	(14,808)	(27,500)	(35,097)	(38,899)
Dividends declared per share					

(1) On a pro forma basis, giving effect to the conversion of all of the outstanding shares of our preferred stock into shares of our common stock immediately prior to the completion of this offering.

Table of Contents

MANAGEMENT S DISCUSSION AND ANALYSIS OF FINANCIAL CONDITION AND RESULTS OF OPERATIONS

The following discussion and analysis of our financial condition and results of operations should be read in conjunction with our consolidated financial statements and related notes that appear elsewhere in this prospectus. In addition to historical consolidated financial information, the following discussion contains forward-looking statements that reflect our plans, estimates and beliefs. Our actual results could differ materially from those discussed in the forward-looking statements. Factors that could cause or contribute to these differences include those discussed below and elsewhere in this prospectus, particularly in Risk Factors.

Overview

Sourcefire is a leading provider of intelligence driven, open source network security solutions that enable our customers to protect their computer networks in an effective, efficient and highly automated manner. We apply a comprehensive Discover, Determine and Defend, or 3D, approach to network security through which we: 1) discover potential threats and vulnerabilities, 2) determine the potential impact of those observations to the network and 3) defend the network through aggressive enforcement of security policies. We sell our security solutions to a diverse customer base that includes over 25 of the Fortune 100 companies and over half of the 30 largest U.S. government agencies. We also manage one of the security industry s leading open source initiatives, Snort.

Our Sourcefire 3D approach is comprised of three key components:

RNA. At the heart of the Sourcefire 3D security solution is Real-time Network Awareness, or RNA, our network intelligence product that provides persistent visibility into the composition, behavior, topology (the relationship of network components) and risk profile of the network. This information provides a platform for the Defense Center s automated decision-making and network policy compliance enforcement. The ability to continuously discover characteristics and vulnerabilities of any computing device communicating on a network such as a computer, printer or server, or endpoint intelligence, enables our Intrusion Prevention products to more precisely identify and block threatening traffic and to more efficiently classify threatening and/or suspicious behavior than products lacking network intelligence.

Intrusion Sensors. The Intrusion Sensors utilize open source Snort® and our proprietary technology to monitor network traffic. These sensors compare observed traffic to a set of Rules , or a set of network traffic characteristics, which can be indicative of malicious activity. Once the Intrusion Sensors match a Rule to the observed traffic, they block malicious traffic and/or send an alert to the Defense Center for further analysis, prioritization and possible action.

Defense Center. The Defense Center aggregates, correlates and prioritizes network security events from RNA Sensors and Intrusion Sensors to synthesize multipoint event correlation and policy compliance analysis. The Defense Center s policy and response subsystems are designed to leverage existing IT infrastructure such as firewalls, routers, trouble ticketing, and patch management systems for virtually any task, including alerting, blocking and initiating corrective measures.

Historical Development of our Business

We were organized as a Delaware corporation and began operations in January 2001, and we sold our first commercial product, a Sourcefire Intrusion Sensor, in the summer of 2001. In 2002, we released the first version of

the Defense Center product, closed our first round of institutional financing, raising approximately $7.5 million from the sale of Series A convertible preferred stock, and hired senior executives including our CEO, COO, VP of Sales and VP of Business Development. In 2003, we closed our second round of institutional financing, raising $11 million from the sale of Series B convertible preferred stock, released our RNA product and hired our CFO and VP of Engineering. In 2004, we completed our third round of institutional financing, raising $15 million from the sale of Series C convertible preferred stock, exceeded 100 total employees, hired our chief marketing officer and introduced the Sourcefire 3D suite of products. In 2005, we leased approximately 40,000 square feet of office space

for our corporate headquarters including a 4,000 square foot state-of-the-art security lab, received NSS gold certification for our intrusion detection product and released our enterprise class intrusion sensor product.

In October 2005 we entered into a definitive merger agreement to be acquired by Check Point Software Technologies Ltd., an Israeli company, for $225.0 million. As a result of the merger announcement and during the period following the announcement, our U.S. government business was curtailed as certain government agencies apparently became unwilling to buy products from a company being acquired by a foreign entity and instead purchased and installed products sold by our competitors. In April 2006, the proposed acquisition was mutually terminated in response to objections from the Committee on Foreign Investment in the United States. Our business, including our business with the U.S. government, continued to grow following the termination. We believe that, other than the curtailment of government business described above, the announcement, pendency and termination of the merger have not had a material adverse effect on our business or plans for this offering.

In 2006, we closed our fourth round of institutional financing, raising $23 million from the sale of Series D convertible preferred stock, and achieved our first quarter of cash flow positive results.

Key Financial Metrics and Trends

Pricing and Discounts

We maintain a standard price list for all our products and we have not changed our list pricing during the past. Additionally, we have a corporate policy that governs the level of discounting our sales organization may offer on our products based on factors such as transaction size, volume of products, federal or state programs, reseller or distributor involvement and the level of technical support commitment. Our total product revenue and the resulting cost of revenue and gross profit percentage are directly affected by our ability to manage our product pricing policy. Although we have not experienced pressure to reduce our prices, competition is increasing and, in the future, we may be forced to reduce our prices to remain competitive.

Revenue

We currently derive revenue from product sales and services. Product revenue is principally derived from the sale of our network security solutions. Our network security solutions include a perpetual software license bundled with a third-party hardware platform. Services revenue is principally derived from technical support and professional services. We typically sell technical support to complement our network security solutions. Technical support entitles a customer to product updates, new Rules releases and both telephone and web assistance for using our products. Our professional services revenue includes optional on-site network security deployment consulting, and classroom and online training for managing a network security solution.

Product sales are typically recognized as revenue at shipment of the product to the customer, whether sold directly or through resellers. For sales made through distributors and original equipment manufacturers, or OEMs, we do not recognize revenue until we receive the monthly sales report which indicates the sell-through volume to end user customers. Revenue from services is recognized when the services are performed. For technical support services, revenue is recognized ratably over the term of the support arrangement, which is usually a 12-month agreement providing for payment in advance and automatic renewals.

We sell our network security solutions globally. However, over 80% of our revenue for 2006 was generated by sales to U.S.-based customers. We expect that our revenue from customers based outside of the United States will increase in amount and as a percentage of total revenue as we execute our strategy to strengthen our international presence. We also expect that our revenue from sales through OEMs and distributors will increase in amount and as a percentage of

total revenue as we execute our strategy to expand such relationships. We manage our operations on a consolidated basis for purposes of assessing performance and making operating decisions. Accordingly, our business does not have reportable segments.

Revenue from product sales has been highly seasonal, with more than one-third of our total product revenue in recent fiscal years generated in the fourth quarter. The timing of our year-end shipments could materially affect our fourth quarter product revenue in any fiscal year and sequential quarterly comparisons. Revenue from our government customers has occasionally been influenced by the September 30th fiscal year-end of the U.S. federal

Table of Contents

government, which has historically resulted in our revenue from government customers being highest in the third quarter. Although we do not expect these general seasonal patterns to change substantially in the future, our revenue within a particular quarter is often affected significantly by the unpredictable procurement patterns of our customers. Our prospective customers usually spend a long time evaluating and making purchase decisions for network security solutions. Historically, many of our customers have not finalized their purchasing decisions until the final weeks or days of a quarter. We expect these purchasing patterns to continue in the future. Therefore, a delay in even one large order beyond the end of the quarter could materially reduce our anticipated revenue for a quarter. Because many of our expenses must be incurred before we expect to generate revenue, delayed orders could negatively impact our results of operations for the period and cause us to fail to meet the financial performance expectations of securities industry research analysts or investors.

On April 20, 2006, we received a complaint filed by PredatorWatch, Inc. in Suffolk County, Massachusetts, alleging, among other things, that we misappropriated and incorporated the plaintiff s trade secrets and confidential information into our RNA technology. The plaintiff has sought to recover amounts to be ascertained and established, as well as double and treble damages and attorneys fees. While this litigation is at an early stage and we cannot reliably estimate the amount, if any, that the Plaintiff could recover, the potential range of remedies available to the Plaintiff, if successful, could include royalties on past and future sales of RNA and/or a permanent injunction prohibiting us from selling any products containing RNA technology.

Cost of Revenue

Cost of product revenue includes the cost of the hardware platform bundled into our network security solution, royalties for third-party software included in our network security solution, materials and labor that go into the quality assurance of our products, logistics, warranty, shipping and handling costs and, in the limited instance where we lease our network security solutions to our customers, depreciation and amortization. For both the year ended December 31, 2006 and the year ended December 31, 2005, cost of product revenue was 28% of total product revenue. Hardware costs, which are our most significant cost items, generally have not fluctuated materially as a percentage of revenue in recent years because competition among hardware platform suppliers has remained strong and, therefore, our hardware cost has remained consistent. Because of the competition among hardware suppliers and our outsourcing of the manufacture of our products to four separate domestic contract manufacturers, we currently have no reason to expect that our cost of product revenue as a percentage of total product revenue will change significantly in the foreseeable future due to hardware pricing increases. However, hardware or other costs of manufacturing may increase in the future. We incur labor and associated overhead expenses, such as occupancy costs and fringe benefits costs, as part of managing the manufacturing process. These costs are included as a component of our cost of product revenue, but they have not been material.

Cost of service revenue includes the direct labor costs of professionals and outside consultants engaged to furnish those services, as well as their travel and associated direct material costs. Additionally, we include in cost of service revenue an allocation of overhead expenses such as occupancy costs, fringe benefits and supplies. For the years ended December 31, 2006 and 2005, cost of service revenue was 18% and 16% of total service revenue, respectively, and, although we anticipate incurring additional costs in the future for increased personnel to support and service our growing customer base, we do not expect the cost of service revenue as a percentage of service revenue to change materially in the future.

Gross Profit

Our gross profit is affected by a variety of factors, including competition, the mix and average selling prices of our products, our pricing policy, technical support and professional services, new product introductions, the cost of hardware platforms, the cost of labor to generate such revenue and the mix of distribution channels through which our

products are sold. Although we have not had to reduce the prices of our products or vary our pricing policy in recent years, our gross profit would be adversely affected by price declines if we are unable to reduce costs on existing products and to continue to introduce new products with higher margins. Currently, product sales typically have a lower gross profit as a percentage of revenue than our services due to the cost of the hardware platform. Our gross profit for any particular quarter could be adversely affected if we do not complete sales of higher margin products by the end of the quarter. As discussed above, many of our customers do not finalize purchasing decisions

until the final weeks or days of a quarter, so a delay in even one large order of a higher-margin product could reduce our total gross profit percentage for that quarter. For both the year ended December 31, 2006 and the year ended December 31, 2005, gross profit was 75% of total revenue. Based on current market conditions, we do not expect these percentages to change significantly in the foreseeable future, although unexpected pricing pressures or an increase in hardware or other costs would cause our gross profit percentage to decline.

Operating Expenses

Research and Development. Research and development expenses consist primarily of payroll, benefits and related costs for our engineers, occupancy costs and other overhead, costs for sophisticated components used in product and prototype development and costs of test equipment used during product development.

We have significantly expanded our research and development capabilities and expect to continue to expand these capabilities in the future. All of our research and development is performed in the United States. We are committed to increasing the level of innovative design and development of new products as we strive to enhance our ability to serve our existing commercial and federal government markets as well as new markets for security solutions. To meet the changing requirements of our customers, we will need to fund investments in several development projects in parallel. Accordingly, we anticipate that our research and development expenses will continue to increase in absolute dollars for the foreseeable future, but should decline moderately as a percentage of total revenue as we expect to grow our sales more rapidly than our research and development expenditures. For the years ended December 31, 2006 and 2005, research and development expense was $8.6 million and $6.8 million, or 19% and 21% of total revenue, respectively.

Sales and Marketing. Sales and marketing expenses consist primarily of salaries, incentive compensation, benefits and related costs for: sales and marketing personnel; trade show, advertising, marketing and other brand-building costs; marketing consultants and other professional services; training, seminars and conferences; travel and related costs; and occupancy and other overhead costs.

As we focus on increasing our market penetration, expanding internationally and continuing to build brand awareness, we anticipate that selling and marketing expenses will continue to increase in absolute dollars, but decrease as a percentage of our revenue, in the future.

For the years ended December 31, 2006 and 2005, sales and marketing expense was $20.7 million and $17.1 million, or 46% and 52% of total revenue, respectively.

General and Administrative. General and administrative expenses consist primarily of: salaries, incentive compensation, benefits and related costs for executive, finance, information system and administrative personnel; legal, accounting and tax preparation and advisory fees; travel and related costs; information systems and infrastructure costs; and occupancy and other overhead costs.

We expect our general and administrative expenses to increase due to our preparations to become and to operate as a public company, including costs associated with compliance with Section 404 of the Sarbanes-Oxley Act, directors and officers liability insurance, increased professional services and a new investor relations function.

For the years ended December 31, 2006 and 2005, general and administrative expense was $5.1 million and $5.0 million or 11% and 16% of total revenue, respectively.

Stock-Based Compensation. Prior to January 1, 2006, our stock-based compensation expense consisted primarily of the amortization of unearned compensation related to grants of restricted shares of our common stock to certain

officers and employees in 2002 and 2003, as well as the modification of certain fixed stock option awards subsequent to their grant date. Total stock-based compensation expenses recorded in our statements of operations for 2003, 2004 and 2005 were $72,000, $177,000 and $470,000, respectively.

Effective January 1, 2006, the Company adopted the fair value recognition provisions of the Financial Accounting Standards Board s SFAS No. 123(R), Share-Based Payment, using the prospective transition method, which requires the Company to apply its provisions only to awards granted, modified, repurchased or cancelled

Table of Contents

after the effective date. Under this transition method, stock-based compensation expense recognized beginning January 1, 2006 is based on the grant date fair value of stock awards granted or modified after January 1, 2006.

As a result of adopting SFAS No. 123(R) on January 1, 2006, based on the estimated grant-date fair value of employee stock options subsequently granted or modified, the Company recognized aggregate stock-based compensation expense of $703,000 for the year ended December 31, 2006. The Company uses the Black-Scholes option pricing model to estimate the calculated value of granted stock options. The use of option valuation models requires the input of highly subjective assumptions, including the expected term and the expected stock price volatility.

The grant date fair value of options not yet recognized as expense as of December 31, 2006 aggregated approximately $3.4 million, net of estimated forfeitures, which will be recognized over a weighted-average period of approximately four years. We expect to record aggregate amortization of stock-based compensation of approximately $1,251,000, $1,026,000, $791,000 and $321,000 during fiscal years 2007, 2008, 2009 and 2010, respectively, from these outstanding awards, subject to continued vesting.

Critical Accounting Policies and Estimates

Our consolidated financial statements are prepared in accordance with accounting principles generally accepted in the United States of America. The preparation of these consolidated financial statements requires us to make estimates and assumptions that affect the reported amounts of assets, liabilities, revenue, costs and expenses and related disclosures. We evaluate our estimates and assumptions on an ongoing basis. Our actual results may differ from these estimates.

We believe that, of our significant accounting policies, which are described in Note 2 to the notes to our consolidated financial statements, the following accounting policies involve a greater degree of judgment and complexity. Accordingly, we believe that the following accounting policies are the most critical to aid in fully understanding and evaluating our consolidated financial condition and results of operations.

Revenue Recognition. We recognize substantially all of our revenue in accordance with Statement of Position No. 97-2, Software Revenue Recognition, or SOP 97-2, as amended by SOP 98-4 and SOP 98-9. We establish persuasive evidence of an arrangement for each type of revenue transaction based on:

- in the case of direct sales or indirect sales through some resellers or distributors, either a signed contract with the end user customer or a click-wrap contract embedded in the product, whereby the end user customer agrees to our standard terms and conditions,
- in the case of indirect sales through OEMs or some resellers or distributors, a signed distribution contract with OEMs and other resellers; or
- in the case of services, including support, training and other professional services, through the execution of a separate services arrangement.

For each arrangement, we defer revenue recognition until all of the following criteria have been met:

- persuasive evidence of an arrangement exists (*e.g.*, a signed contract);
- delivery of the product has occurred and there are no remaining obligations or substantive customer acceptance provisions;

the fee is fixed or determinable; and

collection of the fee is probable.

We allocate the total value of the arrangement among each deliverable based on its fair value as determined by vendor-specific objective evidence, such as standard product discount levels, daily service rates and consistent support level renewal pricing. If vendor-specific objective evidence of fair value does not exist for each of the deliverables, all revenue from the arrangement is further deferred until the earlier of the point at which sufficient vendor-specific objective evidence of fair value can be determined or all elements of the arrangement have been delivered. However, if the only undelivered elements are technical support and/or professional services, elements

for which we currently have established vendor specific objective evidence of fair value, we recognize revenue for the delivered elements using the residual method. Changes in judgments and estimates about these assumptions could materially impact the timing of revenue recognition.

Accounting for Stock-Based Compensation. Prior to January 1, 2006, we accounted for stock-based compensation using the intrinsic value method prescribed in Accounting Principles Board Opinion No. 25, Accounting for Stock Issued to Employees, or APB No. 25, and related interpretations. Accordingly, compensation cost for stock options generally was measured as the excess, if any, of the estimated fair value of our common stock over the amount an employee must pay to acquire the common stock on the date that both the exercise price and the number of shares to be acquired pursuant to the option are fixed. We had adopted the disclosure-only provisions of SFAS No. 123, Accounting for Stock-Based Compensation, and SFAS No. 148, Accounting for Stock-Based Compensation Transition and Disclosure, which was released in December 2002 as an amendment to SFAS No. 123, and used the minimum value method of valuing stock options as allowed for non-public companies.

In December 2004, the Financial Accounting Standards Board issued SFAS No. 123(R), Share-Based Payment, which revised SFAS No. 123 and superseded APB No. 25. SFAS 123(R) focuses primarily on transactions in which an entity obtains employee services in exchange for share-based payments. Under SFAS 123(R), an entity is generally required to measure the cost of employee services received in exchange for an award of equity instruments based on the grant date fair value of the award, with such cost recognized over the applicable requisite service period. In addition, SFAS 123(R) requires an entity to provide certain disclosures in order to assist in understanding the nature of share-based payment transactions and the effects of those transactions on the financial statements. The provisions of SFAS No. 123(R) are required to be applied as of the beginning of the first interim or annual reporting period of the entity s first fiscal year that begins after December 15, 2005.

Effective January 1, 2006, we adopted the fair value recognition provisions of SFAS No. 123(R) using the prospective transition method, which requires the Company to apply the provisions of SFAS No. 123(R) only to awards granted, modified, repurchased or cancelled after the effective date. Under this transition method, stock-based compensation expense recognized beginning January 1, 2006 is based on the grant date fair value of stock awards granted or modified after January 1, 2006. As the Company had used the minimum value method for valuing its stock options under the disclosure requirements of SFAS 123, all options granted prior to January 1, 2006 continue to be accounted for under APB No. 25.

In determining the grant date fair value of share-based payments, we conducted contemporaneous valuations relying on the guidance prescribed by the American Institute of Certified Public Accountants in its practice aid, Valuation of Privately-Held-Company Equity Securities Issued as Compensation, or the Practice Aid. In each instance where we made such a valuation determination, and as more fully described below, we generally first determined a fair value of the enterprise using one or both of the market approach or the income approach. Once we determined an estimated fair value of the enterprise, we then allocated that enterprise value to each of our classes of stock based upon a consideration of those classes relative economic and control rights, using a methodology consistent with the Practice Aid, as discussed in further detail below.

We did not obtain contemporaneous valuations by an unrelated valuation specialist that we could rely on during the periods outlined below. Instead, we relied on the experience of our management team and our board of directors, which includes several venture capitalists who have considerable experience in the valuation of emerging companies and one member with extensive experience as a chief financial officer of a publicly traded company who joined our board in August 2006.

For the Period August 2005 through September 2005. We did not grant any share-based payments during the period from August 2005 through September 2005. The primary reason for not granting any share-based compensation

during this period was because we believed that the fair value of our enterprise was not easily determinable due to our ongoing merger discussions with Check Point Software Technologies Ltd., or Check Point.

October 2005. On October 5, 2005 our ongoing discussions with Check Point resulted in the signing of a definitive merger agreement to be acquired for approximately $225.0 million in cash. Later that month, we granted an option to purchase 6,157 shares of our common stock at an exercise price of $8.36 per share to one employee. In connection with that grant, we determined that the fair value of our common stock was also $8.36 per share and

therefore, in accordance with APB No. 25, did not record any compensation expense since the award had no intrinsic value on the measurement date. In concluding that $8.36 was the fair value of our common stock, we followed the methodology outlined above by first determining our enterprise value and then allocating that value to each of our classes of stock. We calculated an enterprise value of $225.0 million using the market approach. We concluded that the market approach was the most appropriate methodology at this time since it relied on data generated by an actual market transaction. Immediately prior to this grant, we executed a merger agreement with Check Point, which proposed a definitive arm s length transaction between willing parties. We arrived at the $225.0 million enterprise value using the aggregate consideration that Check Point had agreed to pay for us. In addition to doing the foregoing analysis, we also reviewed market data provided by our investment advisors for comparable acquisition transactions that had occurred in the previous several months to ascertain the fairness of the Check Point offer.

In allocating the $225.0 million enterprise value to each of our classes of stock, we used the current-value method since we believed at the time of the valuation that a liquidity event in the form of an acquisition was imminent. Using the current-value method, we first allocated the proceeds to each of our series of preferred stock based upon their respective liquidation preferences and dividend rights. Specifically, we allocated approximately $56.8 million in the aggregate to our preferred stock, representing the liquidation preferences plus all accrued but unpaid dividends. In accordance with our Charter, we then allocated the remaining $168.2 million to all equity securities assuming conversion of all securities into shares of common stock. This resulted in a value of approximately $8.85 per share of common stock. We then applied a discount of approximately five percent to reflect the risk that the proposed merger with Check Point would not be consummated, and we arrived at fair value per common share of $8.36. We used a five percent discount based upon advice received from our financial advisors that such a discount was typical at similar stages of similar transactions, as well as based on our own opinions formed in negotiating the merger agreement with Check Point.

For the Period November 2005 to March 2006. In January 2006 we granted options to purchase a total of 171,489 shares of our common stock to our employees at an exercise price of $8.36 per share. In accordance with SFAS 123(R), we measured share-based compensation expense with respect to these grants using the Black-Scholes option pricing model using a per share fair value of our common stock of $8.36 per share. In concluding that $8.36 was the fair value of our common stock, we followed the same methodology used in October 2005 because we were still a party to the proposed merger agreement with Check Point for which we believed that consummation was imminent and therefore no adjustment to the market approach previously used was warranted. In late March 2006 we made a public announcement concerning the withdrawal of our merger agreement with Check Point because we could not obtain approval from the Department of Homeland Security s Committee on Foreign Investment in the United States, or CFIUS.

April 2006. During April 2006, we cancelled the 6,157 options previously granted in October 2005 as well as the options to purchase 159,175 shares of our common stock we granted in January 2006, all at an exercise price of $8.36 per share, and we reissued them at an exercise price of $5.26 per share. Additionally, we granted new options to employees to purchase an aggregate of 287,846 shares of our common stock at $5.26 per share. In accordance with SFAS 123(R), we measured the share-based compensation expense with respect to these grants using the Black-Scholes option pricing model using a per share fair value of our common stock of $5.26 per share. In concluding that $5.26 was the fair value of our common stock, we again followed the methodology outlined above by first determining our enterprise value and then allocating that value to each of our classes of stock.

In April 2006, we calculated an enterprise value of $205.0 million using both a market approach and an income approach. One fundamental factor that affected the enterprise fair value calculated under both approaches, and resulted in an enterprise value that was lower than the amount calculated during the period from October 2005 through March 2006, was the March 2006 withdrawal of our merger agreement from consideration for approval by CFIUS. We considered valuations derived using both approaches because we believed that neither approach, on its own,

would necessarily result in the best evidence of fair value based on the status of our business. For example, we did not believe that the market approach alone would be the most appropriate methodology as a result of our inability to consummate the Check Point transaction. Similarly, we believed that relying solely on the income approach would not have resulted in the best evidence of fair value because of the inherent limitations of that approach in accounting for risk.

Table of Contents

Under the market approach, we considered the merger agreement with Check Point as one data point; however, we assigned less probative value to that transaction in light of the termination of that agreement due to the failure of the CFIUS approval process. We also considered comparable recent acquisition transactions that had occurred in the previous several months. In deciding which companies and transactions were sufficiently similar to us to result in a meaningful comparison, we looked to the merger and acquisition market for security software companies and specifically both public and private target companies within that group that were similar to us in terms of size (revenue and growth rates), industry, profitability (or net loss experience), stage of development, enterprise valuations, growth patterns, business model, and experience of the management team. Examples of companies within this group, or the Peer Group, included Abridean (acquired by nCipher), Cyberguard (acquired by Secure Computing), Sygate (acquired by Symantec), Omnipod (acquired by MessageLabs) LODOGA Security (acquired by Transdigital), iDefense (acquired by Verisign), JP Mobile (acquired by Good Technology) and GuardedBet (acquired by Micromuse). We chose these companies because they best matched the comparison criteria listed above without the need to make further assumptions or adjustments to arrive at a meaningful comparison.

In arriving at an enterprise fair value under this approach, we placed significant emphasis on the enterprise value of companies within the Peer Group expressed as a multiple of those respective companies trailing revenues. We believe that focusing on revenue multiples of trailing revenue was the best evidence of fair value because the merger and acquisition market for security software companies most commonly uses this approach to measure valuation. Based on that assumption, in reviewing companies within the Peer Group, we observed a range of revenue multiples from 4.5 to 14.3 resulting in a mean revenue multiple of 5.88. From this analysis and rounding to the nearest whole number, we determined that an appropriate revenue multiple that marketplace participants used to value companies within the Peer Group was six times their 2005 revenues. Six times our 2005 revenues yielded an enterprise value of approximately $197.0 million.

Under the income approach, we calculated our enterprise value using the discounted cash flow method, which determines the present value of the expected future economic benefit to an equity holder by application of an appropriate discount rate. Our EBITDA projections, working capital requirements and capital expenditure requirements, all of which affect our cash flows, were calculated through our fiscal year ending December 31, 2008. We did not use estimated cash flows for periods beyond our fiscal year 2008 for two primary reasons. First, the projections we used internally to manage our business included only detailed results of our operations through our fiscal year ending December 31, 2008. Second, the fact that we had limited and variable historical data due to our establishment as an enterprise in 2001 and our belief that the assumptions necessary to determine cash flows from our business beyond 2008 were highly speculative in nature and could have caused us to place an inaccurate enterprise valuation on our business. To arrive at a present value of these projected cash flows, we discounted each year s cash flows using a 20.8% weighted average cost of capital. To these discounted cash flows we added the present value of our estimated enterprise terminal value in early 2009. Based on a review of comparable company market multiple data, we determined this terminal value to be three times our estimated 2008 revenues, or $320.0 million. Taking into account the discounted cash flows and this estimated terminal value, we arrived at an enterprise value of $205.0 million. We used this enterprise value to calculate the fair value of our common stock since it did not differ materially from the estimated enterprise value using the market approach.

In allocating the $205.0 million enterprise value to each of our classes of stock, we again used the current-value method since we still believed at the time that the most likely outcome for our business was an acquisition transaction. We also considered that if we had used the probability-weighted expected return method of allocation, we believed the allocation results would have been the same as those achieved using the current-value method because in April 2006, we assigned a zero probability to an IPO scenario. Accordingly, we allocated approximately $57.8 million in the aggregate to our preferred stock, representing the liquidation preferences plus all accrued but unpaid dividends. We then allocated the remaining $151.2 million, which included estimated option exercise proceeds of $4.0 million, to all equity securities assuming conversion of all securities into shares of common stock. This resulted in a per share gross

fair value of approximately $8.25 per share of common stock. We then applied a discount of fifteen percent (15%) to account for the lack of marketability of our equity securities. In arriving at a fifteen percent (15%) marketability discount, we considered the following factors: our expectations of a ready market for our securities in the future, the number, extent and terms of existing contractual arrangements requiring us to purchase or sell our securities, the restrictions on transferability of our equity securities by our stockholders,

the existence of potential acquirors, the costs associated with bringing equity securities to market, the risk and volatility of our business, the size and timing of any projected dividends, the difficulty in assigning a value to our equity interest and the concentration of our ownership. In addition to the marketability discount, we further discounted this value by twenty-five percent (25%) to reflect the absence of any strategic or synergistic benefits that would justify a valuation premium for our common stockholders. Because our common stockholders controlled significantly less than a 50% interest, we considered that class a minority interest. In arriving at this twenty-five percent (25%) discount, we considered the following factors: the concentration of our ownership in individual stockholders, the number of common stockholders and the relative size of their holdings, the existence of potential acquirors, the degree of influence a minority shareholder has, patterns of historical liquidation of stockholders interests, how control is exercised and the average change-of-control premium realized in other comparable merger and acquisition transactions. We relied on studies performed by merger and acquisition data tracking service providers, such as Mergerstat and Pratt s Stats, to determine the appropriate marketability and minority interest discounts. Applying both discounts to the value of $8.25 per share yielded a fair value of $5.26 per share. In determining that the result obtained under this approach was the best evidence of our fair value, our board also considered the negative impact that the withdrawal of our Check Point merger agreement due to the CFIUS approval process had on our business. Prior to entering into the merger agreement, we had planned to generate both net income and positive cash flow for 2006. As a result of the termination of the merger agreement, we revised our 2006 operating plan downward to reflect operational difficulties and uncertainties associated with existing and potential government agency customers, which had in some cases refrained from doing business with us during the CFIUS review process. Although we had increased our revenue and customer penetration substantially over the previous few years, we still operated at a net loss and had to use cash proceeds from private placements to fund our operations. Thus, in April 2006, our board of directors considered the foregoing analyses and concluded that $5.26 was the best estimate of the fair value of our common stock for purposes of granting options at that time.

For the Period May 2006 to September 2006. We did not grant any share-based compensation to our employees during the period from May 2006 until September 2006, and thus recorded no expense with respect to share-based compensation to our employees during that period.

October and November 2006. In October 2006 we granted options to purchase a total of 399,603 shares of our common stock to our employees at an exercise price of $9.48 per share. In accordance with SFAS 123(R), we measured share-based compensation expense with respect to these grants using the Black-Scholes option pricing model using a per share fair value of our common stock of $9.48 per share. In concluding that $9.48 was the fair value of our common stock, we again followed the methodology outlined above by first determining our enterprise value and then allocating that value to each of our classes of stock. In addition to the allocation of the enterprise value to each of our classes of stock, we also considered the impact of two significant potential liquidity events: the successful consummation of a public offering of our common stock, or the IPO scenario, and the sale of the company in a merger or acquisition transaction, or the M&A scenario. We took into account the probability of each outcome in making our evaluation.

In October 2006, we calculated an enterprise value of $226.0 million using a market approach, which we corroborated using an income approach that considered discounted cash flows. In conducting our analysis using the market approach, we followed the same methodology that we used in calculating fair value under that approach in April 2006, except that we used a multiple of six times our revenues for the trailing four quarters ended September 30, 2006 instead of six times our 2005 revenues.

In allocating the $226.0 million enterprise value to each of our classes of stock, we recognized that the methodology to follow would differ from past periods because we faced the two potential liquidity scenarios described above. In allocating the enterprise value under the M&A scenario, we followed closely the allocation methodology used in past periods whereby we first allocated a portion of the enterprise fair value to our preferred stock based upon its rights and

preferences. Accordingly, we allocated approximately $75.0 million in the aggregate to our preferred stock based upon liquidation preferences and accrued but unpaid dividends. We then allocated the remaining $151.0 million to all equity securities assuming conversion of all securities into shares of common stock. This resulted in a per share value of approximately $7.55 per share of common stock.

Table of Contents

In allocating the enterprise value under the IPO scenario, we assumed that all of our preferred stock would automatically convert to common stock based on the definition of a qualified public offering contained in our Charter. Thus under the IPO scenario allocation, we did not first allocate a portion of the enterprise value to our preferred stock, but rather calculated the value of approximately $11.42 per share assuming conversion of all securities into shares of common stock.

Under this dual allocation approach, we then assigned a probability to the M&A scenario and another probability to the IPO scenario to arrive at a composite allocation. In October 2006, because of the relative uncertainty surrounding the likelihood of an M&A scenario versus an IPO scenario, we ascribed a 50% probability to the M&A scenario and 50% probability to the IPO scenario, resulting in a fair value of $9.48 per share. Thus, in mid-October 2006, our board of directors considered the foregoing analyses and concluded that $9.48 was the best estimate of the fair value of our common stock for purposes of granting options at that time.

In November 2006 we granted options to purchase a total of 56,955 shares of our common stock to our employees at an exercise price of $10.41 per share. In accordance with SFAS 123(R), we measured share-based compensation expense with respect to these grants using the Black-Scholes option pricing model using a fair value of our common stock of $10.41 per share. In concluding that $10.41 was the fair value of our common stock, we performed an analysis identical to the one we performed in October 2006 using the same enterprise value of $226.0 million. Because there was not a substantial difference in our trailing four quarters of revenue as measured in October and November, we determined that using an enterprise value of $226.0 million for our analysis in both periods was appropriate. The difference in the resultant valuation, however, was in our assessment of an M&A scenario versus the relative likelihood of an IPO scenario. In November 2006, we determined that the IPO event scenario was more likely than it had been in October because we had filed our initial registration statement with the Securities and Exchange Commission on October 25, 2006.

In allocating the $226.0 million enterprise value, we followed the probability-weighted expected return method. Thus we assigned a 75% probability to the $11.42 per share value arrived under the IPO scenario and a 25% probability to the $7.55 per share value arrived under the M&A scenario, given our increased expectation of completing our initial public offering. This probability-weighted expected return methodology resulted in a per share fair value of our common stock of $10.41. Thus, in November 2006, our board of directors considered the foregoing analysis and concluded that $10.41 was the best estimate of the fair value of our common stock for purposes of granting options at that time.

December 2006. In December 2006 we granted options to purchase a total of 38,484 shares of our common stock to our employees at an exercise price of $11.34 per share. In accordance with SFAS 123(R), we measured share-based compensation expense with respect to these grants using the Black-Scholes option pricing model using a per share fair value of our common stock of $11.34 per share. In concluding that $11.34 was a fair value of our common stock, we followed an analysis similar to the ones that we performed in October and November 2006.

We used an enterprise value of $250.0 million that we determined based upon valuation discussions that we conducted with our underwriters with respect to other recent technology initial public offerings, and our perceptions of the then-current market conditions. Additionally, in December 2006, we determined that the IPO event scenario was just as likely as it had been in November.

In allocating the $250.0 million enterprise value, we followed the probability-weighted expected return method. Thus, we assigned a 75% likelihood that the IPO scenario would occur and a 25% likelihood that the M&A scenario would occur. In allocating the enterprise value under the M&A scenario, we followed closely the allocation methodology used in past periods whereby we first allocated a portion of the enterprise fair value to our preferred stock based upon its rights and preferences. Accordingly, we allocated approximately $79.0 million in the aggregate to our preferred

stock based upon liquidation preferences and accrued but unpaid dividends. We then allocated the remaining $171.0 million to all equity securities assuming conversion of all securities into shares of common stock. Under the IPO scenario, we calculated the fair value of approximately $12.26 per share assuming conversion of all securities into shares of common stock. By assigning a 25% probability to the $8.53 per share fair value arrived under the M&A scenario and assigning a 75% probably to the $11.34 per share fair value arrived under the IPO scenario, this probability-weighted expected return methodology resulted in a per share fair value of our common

Table of Contents

stock of $11.34. Thus, in December 2006, our board of directors considered the foregoing analysis and concluded that $11.34 was the best estimate of the fair value of our common stock for purposes of granting options at that time.

Based on the initial public offering price of $15.00, the intrinsic value of the options outstanding at December 31, 2006 was $38.6 million, of which $23.9 million related to vested options and $14.7 million related to unvested options.

As noted above, we use the Black-Scholes option pricing model to estimate the calculated value of granted stock options. The use of option valuation models requires the input of highly subjective assumptions, including the expected term and the expected stock price volatility. Additionally, the recognition of expense requires the estimation of the number of options that will ultimately vest and the number of options that will ultimately be forfeited. Accordingly, the use of different estimates and assumptions can have a significant impact on the amount of stock-based compensation that is measured and recognized.

Accounting for Income Taxes. Deferred taxes are determined based on the difference between the financial statement and tax basis of assets and liabilities using enacted tax rates in effect in the years in which the differences are expected to reverse. Valuation allowances are provided if, based upon the weight of available evidence, it is more likely than not that some or all of the deferred tax assets will not be realized.

To date, for U.S. federal income tax purposes, we have operated in a loss position. We have $28.1 million of net operating loss carry-forwards as of December 31, 2006, although the use of these net operating loss carry-forwards may be significantly limited by changes in our ownership. As of December 31, 2006, we recorded a full valuation allowance against net deferred tax assets, including deferred tax assets generated by net operating loss carry-forwards. These carry-forwards will begin to expire in 2022. We expect that, to the extent we have taxable income in years before their expiration, these net operating loss carry-forwards will impact our effective tax rate.

Warranty. We provide a one-year warranty against defects in materials and workmanship and will either repair the goods or provide replacement products at no charge to the customer. We record estimated warranty costs, currently at less than 1.0% of product revenue, based on historical experience by product, at the time we recognize product revenue. As the complexity of our products increases, we could experience higher warranty claims relative to sales than we have previously experienced, and we may need to increase these estimated warranty reserves.

Bad Debt Reserve. We have historically used a rate of 1.0% of outstanding accounts receivable to estimate our reserve for bad debts based on analysis of past due balances and historical experiences of write-offs. As we expand our business, we expect our accounts receivable balance to grow. If our future experience of actual write-offs for bad debts exceeds 1.0% of our accounts receivable balance, we will have to increase our reserve accordingly.

Inventory Valuation. We outsource our manufacturing and our products are generally drop-shipped directly to our customers by the manufacturers. Therefore, we usually carry relatively little inventory. The inventory on our balance sheet also includes products that we use for demonstration purposes at customer locations. We value our inventory at the lower of the actual cost of our inventory or its current estimated market value. We write down inventory for obsolescence or lack of marketability based upon condition of the inventory and our view about future demand and market conditions. Because of the seasonality of our product sales, obsolescence of technology and product life cycles, we generally write down inventory to net realizable value based on forecasted product demand. Actual demand and market conditions may be lower than those that we project and this difference could have a material adverse effect on our gross profit if inventory write-downs beyond those initially recorded become necessary.

Table of Contents

Results of Operations

The following table sets forth our results of operations for the periods shown:

	Year ended December 31,			
	2003	2004	2005	2006
	(in thousands)			
Revenue:				
Products	$ 8,153	$ 12,738	$ 23,589	$ 30,219
Services	1,328	3,955	9,290	14,707
Total revenue	9,481	16,693	32,879	44,926
Cost of revenue:				
Products	2,570	4,533	6,610	8,440
Services	436	872	1,453	2,632
Total cost of revenue	3,006	5,405	8,063	11,072
Gross profit	6,475	11,288	24,816	33,854
Operating expenses:				
Research and development	3,751	5,706	6,831	8,612
Sales and marketing	9,002	12,585	17,135	20,652
General and administrative	2,141	2,905	5,120	5,017
Depreciation and amortization	441	752	1,103	1,230
Total operating expenses	15,335	21,948	30,189	35,511
Operating loss	(8,860)	(10,660)	(5,373)	(1,657)
Other income (expense), net	16	164	(85)	792
Loss before income taxes	(8,844)	(10,496)	(5,458)	(865)
Income tax expense				(67)
Net loss	$ (8,844)	$ (10,496)	$ (5,458)	$ (932)

Table of Contents

The following table sets forth our results of operations as a percentage of total revenue for the periods shown:

	Year ended December 31,			
	2003	2004	2005	2006
	(% of revenue)			
Revenue:				
Products	86%	76%	72%	67%
Services	14	24	28	33
Total revenue	100	100	100	100
Cost of revenue:				
Products	27	27	20	19
Services	5	5	5	6
Total cost of revenue	32	32	25	25
Gross profit	68	68	75	75
Operating expenses:				
Research and development	39	34	21	19
Sales and marketing	95	75	52	46
General and administrative	22	18	16	11
Depreciation and amortization	5	5	3	3
Total operating expenses	161	132	92	79
Operating loss	(93)	(64)	(17)	(4)
Other income (expense), net		1		2
Loss before income taxes	(93)	(63)	(17)	(2)
Income tax expense				
Net loss	(93)%	(63)%	(17)%	(2)%

Comparison of Years Ended December 31, 2006 and 2005

Revenue. Our total revenue increased 37% to $44.9 million in the year ended December 31, 2006 from $32.9 million in the year ended December 31, 2005. Product revenue increased 28% to $30.2 million in the year ended December 31, 2006 from $23.6 million in the year ended December 31, 2005. We did not introduce any new products during 2006 nor did we change the prices of our products from 2005 to 2006. The increase in product revenue was driven primarily by higher demand for our network security solutions throughout both periods, specifically sales of our enterprise class Intrusion Sensors which increased $5.5 million during 2006. Our services revenue increased 58% to $14.7 million in the year ended December 31, 2006 from $9.3 million in the year ended December 31, 2005. The increase in service revenue resulted primarily from support services being provided to a larger installed customer base in the 2006 period.

Cost of Revenue. Our total cost of revenue increased 36% to $11.1 million in the year ended December 31, 2006, compared to $8.1 million in the year ended December 31, 2005. Our product cost of revenue increased 28% to $8.4 million in the year ended December 31, 2006, compared to $6.6 million in the year ended December 31, 2005. During these periods, we did not experience a material increase in our cost per unit of hardware platforms, which is the largest component of our product cost of revenue. The increase in product cost of revenue was driven primarily by higher volume demand for our network security solutions for which we must procure and provide the hardware platform to our customers. Our services cost of revenue increased 81% to $2.6 million in the year ended December 31, 2006, compared to $1.5 million in the year ended December 31, 2005. Of this increase, $620,000 was attributable to our hiring of additional personnel to both service our larger installed customer base

and to provide training and professional services to our customers, and $190,000 was attributable to extending the service contracts with the manufacturers for the hardware platform included with our products for our installed base of customers.

Gross Profit. Gross profit increased 36% to $33.9 million in the year ended December 31, 2006, from $24.8 million in the year ended December 31, 2005. Gross profit as a percentage of total revenue was 75% in both the years ended December 31, 2006 and December 31, 2005. This percentage did not vary between the periods because our product mix, the selling prices of our products and our hardware platform costs remained relatively stable throughout both periods. The increase of $9.1 million in gross profit was primarily due to an increase in product sales and an increase in the number of customers that contracted with us for support arrangements.

Research and Development. Research and development expenses increased 26% to $8.6 million, or 19% of total revenue, in the year ended December 31, 2006 from $6.8 million, or 21% of total revenue, in the year ended December 31, 2005. The increase in the amount of research and development expenses was primarily due to an increase in payroll and benefits of $1.8 million in the year ended December 31, 2006, which resulted from adding personnel in our research and development department to support the release of updates and enhancements to RNA, Intrusion Sensor, and Defense Center products. In addition, at the beginning of 2006, we began product development work on a new release of the Snort intrusion detection engine.

Sales and Marketing. Sales and marketing expenses increased 21% to $20.7 million, or 46% of total revenue, in the year ended December 31, 2006 from $17.1 million, or 52% of total revenue, in the year ended December 31, 2005. The increase in the amount of sales and marketing expenses was primarily due to an increase of $2.1 million in salaries and incentive compensation expense for additional sales personnel, as well as an increase of $0.4 million for stock compensation expense and $0.3 million in advertising and promotion expenses in support of our 3D marketing message for our network security solutions.

General and Administrative. General and administrative expenses decreased 2% to $5.0 million, or 11% of total revenue in the year ended December 31, 2006 from $5.1 million, or 16% of total revenue in the year ended December 31, 2005. During 2006, payroll and benefits increased $180,000 for personnel hired in our accounting, information technology, human resources and legal departments, stock compensation increased $280,000 for the adoption of FAS 123R, and audit and tax consulting increased $110,000; however, these increases were offset by a reduction of $620,000 in legal fees associated with the planned merger with Check Point Software Technologies, Inc. that was negotiated in the summer and autumn of 2005 and withdrawn in March 2006

Depreciation and Amortization. Depreciation and amortization expenses increased 12% to $1.2 million in the year ended December 31, 2006 from $1.1 million in the year ended December 31, 2005. These expenses increased principally because of additional personal computers purchased for personnel hired during 2006.

Comparison of Years Ended December 31, 2005 and 2004

Revenue. Our total revenue increased 97% to $32.9 million in the year ended December 31, 2005 from $16.7 million in the year ended December 31, 2004. Product revenue increased 85% to $23.6 million in 2005 from $12.7 million in 2004. The increase in product revenue was primarily driven by increasingly strong demand for our 3D security solutions, particularly by Fortune 100 companies, of which we added seven as customers during 2005. During the fourth quarter of 2005 we introduced our enterprise class Intrusion Sensors which resulted in $900,000 of incremental sales over 2004. Additionally, the Company experienced further demand for its RNA product during 2005 resulting in incremental sales of $2.3 million. We made no material changes in the selling prices of our products in 2004 or 2005. Our services revenue increased 135% to $9.3 million in 2005 from $4.0 million in 2004. The $5.3 million increase resulted primarily from an additional $4.4 million in revenue generated from support services being provided to a

larger installed customer base in 2005 than in 2004, and a $880,000 increase in professional and training services revenue resulting from our increase in the number of training programs and the personnel to provide these services in 2005 over 2004. During 2005, we created the Sourcefire Certification Program to provide training for network security professionals.

Cost of Revenue. Our total cost of revenue increased 49% to $8.1 million in the year ended December 31, 2005 from $5.4 million in the year ended December 31, 2004. Our product cost of revenue increased 46% to

Table of Contents

$6.6 million in 2005, compared to $4.5 million in 2004. The increase in product cost of revenue was primarily attributable to additional hardware platform costs for the approximately 550 incremental units shipped in 2005 over the amount shipped in 2004, as well as the shipment of our more costly enterprise class intrusion sensors, which were introduced in August 2005. Our cost for hardware platforms and manufacturing did not change materially between 2004 and 2005. Additionally our royalty cost of providing third party software in our products increased by approximately $400,000. Our services cost of revenue increased 67% to $1.5 million in the 2005, compared to $872,000 in 2004. Of this increase, approximately $310,000 was attributable to salaries, bonuses and associated employee benefits and overhead costs for our hiring of additional training and professional service personnel in 2005, with a further $270,000 attributable to travel, facilities and consulting costs incurred in the provision of training and services in 2005 over 2004.

Gross Profit. Our gross profit increased 120% to $24.8 million in 2005, from $11.3 million in 2004. Gross profit as a percentage of total revenue increased to 75% in 2005 from 68% in 2004. This increase in gross profit, as a percentage of total revenue, was principally due to a change in product mix between the periods, with a larger percentage of higher margin products being sold in 2005, and significant growth in our customer support revenue of $4.5 million, which did not require an equivalent incremental expense for support personnel.

Research and Development. Research and development expenses increased 20% to $6.8 million, or 21% of total revenue, in the year ended December 31, 2005 from $5.7 million, or 34% of total revenue, in the year ended December 31, 2004. In 2005, we increased our research and development staff to support the development of enhancements to our 3D product line and the introduction of our enterprise class intrusion sensor, which resulted in an approximate increase of $500,000 in compensation and benefits for additional research and development personnel. Additionally we submitted our products to multiple independent security testing processes in 2005, which cost us an additional $420,000 in testing and certification.

Sales and Marketing. Sales and marketing expenses increased 36% to $17.1 million, or 52% of total revenue, in the year ended December 31, 2005 from $12.6 million, or 75% of total revenue, in the year ended December 31, 2004. The reduction in the percentage of sales and marketing costs to total revenue resulted primarily from an increase in support revenue as well as an increase in sales efficiency against higher sales quotas. The increase of $4.5 million in 2005 resulted primarily from $1.7 million in additional compensation and benefits for personnel added to the sales force, $1.6 million in additional incentive compensation earned on significantly higher sales volume and an increase of $700,000 in marketing expenses to support the company s growth and product brand recognition programs.

General and Administrative. General and administrative expenses increased to $5.1 million, or 16% of total revenue in the year ended December 31, 2005 from $2.9 million, or 17% of total revenue in the year ended December 31, 2004. The significant increase in 2005 resulted from $1.1 million in legal fees, including $750,000 of one-time fees resulting from our planned acquisition by Check Point Software Technologies, Ltd., and approximately $900,000 in additional compensation and benefits for additional general and administrative personnel.

Depreciation and Amortization. Depreciation and amortization expenses increased 47% to $1.1 million in the year ended December 31, 2005 from $752,000 in the year ended December 31, 2004. These expenses increased principally because of additional amortization of leasehold improvements made to our principal place of business into which we moved in April 2005.

Comparison of Years Ended December 31, 2004 and 2003

Revenue. Our total revenue increased 76% to $16.7 million in the year ended December 31, 2004, from $9.5 million in the year ended December 31, 2003. Product revenue increased 56% to $12.7 million in 2004 from $8.2 million in 2003. The increase in product revenue in 2004 resulted primarily from an increase in demand for our network security

products, the first full year of sales for both our RNA product, which was introduced in December 2003, and our enterprise class Defense Center, which was introduced in September 2003. Sales of RNA increased by $2.1 million and incremental sales of the enterprise class Defense Center were $550,000. Our services revenue increased 198% to $4.0 million in 2004 from $1.3 million in 2003. The increase in services revenue resulted

primarily from a $2.5 million increase in our support services for our growing customer base as well as the first year of professional training and service revenues of $160,000, which programs were initiated in early 2004.

Cost of Revenue. Our total cost of revenue increased to $5.4 million, or 32% of total revenue in 2004, from $3.0 million, or 32% of total revenue, in 2003. Our product cost of revenue increased 76% to $4.5 million in 2004, compared to $2.6 million in 2003. The increase in product cost of revenue is primarily due to the increase in product revenue of $4.5 million and the resulting increase in our cost of hardware of $1.5 million. The cost of the hardware platforms as a percentage of the selling price remained relatively static at 29% and 27% for 2004 and 2003, respectively. Our services cost of revenue increased 100% to $872,000 in 2004 from $436,000 in 2003. This increase was attributable to the addition in 2004 of personnel to perform training services, which contributed $440,000 of additional compensation, benefits and associated supplies and overhead expenses.

Gross Profit. Gross profit increased to $11.3 million in 2004 from $6.5 million in 2003. Gross profit as a percentage of total revenue was 68% for both 2004 and 2003. The $4.8 million increase was achieved primarily by increasing the volume of products sold while maintaining a consistent hardware platform cost per unit relative to revenue of 29% and 27% in 2004 and 2003, respectively.

Research and Development. Research and development expenses increased 52% to $5.7 million, or 34% of total revenue, in the year ended December 31, 2004 from $3.8 million, or 40% of total revenue, in the year ended December 31, 2003. The increase of $1.9 million resulted primarily from the addition of hired personnel and outside consultants to our research and development team to support the development of our RNA product, which contributed an increase of $1.4 million in compensation and benefits expenses and $550,000 of consulting costs in 2004.

Sales and Marketing. Sales and marketing expenses increased 40% to $12.6 million, or 75% of total revenue, in the year ended December 31, 2004 from $9.0 million, or 95% of total revenue in the year ended December 31, 2003. The reduction in the percentage of sales and marketing costs to total revenue resulted primarily from an increase in support revenue as well as an increase in sales efficiency against higher sales quotas. The increase of $3.6 million in 2004 was primarily due to approximately $1.3 million for salary and benefits for the addition of personnel to the sales force, approximately $900,000 in additional incentive compensation earned on significantly higher sales volume and an increase of $800,000 in marketing expenses to support the company s growth and product brand recognition.

General and Administrative. General and administrative expenses increased to $2.9 million, or 17% of total revenue, in the year ended December 31, 2004 from $2.1 million, or 23% of total revenue in the year ended December 31, 2003. The increase in 2004 resulted primarily from additional personnel in finance and information technology, which added approximately $600,000 of compensation and benefits expenses.

Depreciation and Amortization. Depreciation and amortization expenses increased 71% to $752,000 in the year ended December 31, 2004 from $441,000 in the year ended December 31, 2003. These expenses increased principally because of an increase in purchases of testing equipment for our research and development lab as well as personal computers for additional personnel hired during 2004.

Table of Contents

Quarterly Results of Operations

You should read the following tables presenting our unaudited quarterly results of operations in conjunction with the consolidated financial statements and related notes contained elsewhere in this prospectus. We have prepared the unaudited information on the same basis as our audited consolidated financial statements. You should also keep in mind, as you read the following tables, that our operating results for any quarter are not necessarily indicative of results for any future quarters or for a full year.

The following table presents our unaudited quarterly results of operations for the eight fiscal quarters ended December 31, 2006. This table includes all adjustments, consisting only of normal recurring adjustments, that we consider necessary for fair statement of our operating results for the quarters presented.

	Three months ended							
	March 31, 2005	June 30, 2005	Sept. 30, 2005	Dec. 31, 2005	March 31, 2006	June 30, 2006	Sept. 30, 2006	Dec. 31, 2006
	(unaudited) (in thousands)							
Revenue:								
Products	$ 4,890	$ 4,019	$ 5,980	$ 8,700	$ 5,423	$ 6,040	$ 6,927	$ 11,829
Services	1,862	2,076	2,397	2,955	3,109	3,495	3,940	4,163
Total revenue	6,752	6,095	8,377	11,655	8,532	9,535	10,867	15,992
Cost of revenue:								
Products	1,375	1,082	1,772	2,381	1,397	1,721	1,813	3,509
Services	290	332	359	472	610	681	725	616
Total cost of revenue	1,665	1,414	2,131	2,853	2,007	2,402	2,538	4,125
Gross profit	5,087	4,681	6,246	8,802	6,525	7,133	8,329	11,867
Operating expenses	6,547	6,466	8,021	9,155	8,440	8,485	8,420	10,166
Income (loss) from operations	(1,460)	(1,785)	(1,775)	(353)	(1,915)	(1,352)	(91)	1,701
Other income (expense)	(1)	(10)	(39)	(35)	(10)	156	296	350
(Loss) income before income taxes	(1,461)	(1,795)	(1,814)	(388)	(1,925)	(1,196)	205	2,051
Income tax expense								67
Net (loss) income	$ (1,461)	$ (1,795)	$ (1,814)	$ (388)	$ (1,925)	$ (1,196)	$ 205	$ 1,984
Net cash (used in) provided by operations	680	(1,316)	(2,086)	(1,736)	2,701	(1,205)	416	156

48

Table of Contents

The following table sets forth our results of operations as a percentage of total revenue for the periods shown:

	Three months ended							
	March 31, 2005	June 30, 2005	Sept. 30, 2005	Dec. 31, 2005	March 31, 2006	June 30, 2006	Sept. 30, 2006	Dec. 31, 2006
	(unaudited) (% of revenue)							
Revenue:								
Products	72%	66%	71%	75%	64%	63%	64%	74%
Services	28	34	29	25	36	37	36	26
Total revenue	100	100	100	100	100	100	100	100
Cost of revenue:								
Products	21	18	21	20	16	18	17	22
Services	4	5	4	4	7	7	7	4
Total cost of revenue	25	23	25	24	23	25	24	26
Gross profit	75	77	75	76	77	75	76	74
Operating expenses	97	106	96	79	99	89	77	64
Income (loss) from operations	(22)	(29)	(21)	(3)	(22)	(14)	(1)	10
Other income (expense)			(1)		(1)	1	3	2
(Loss) income before income tax expense	(22)	(29)	(22)	(3)	(23)	(13)	2	12
Income tax expense								
Net (loss) income	(22)%	(29)%	(22)%	(3)%	(23)%	(13)%	2%	12%

Seasonality

Our product revenue has tended to be seasonal. In our third quarter, we have historically benefited from the Federal government s fiscal year end purchasing activity. This increase has been partially offset, however, by European sales, which have tended to decline significantly in the summer months due to the practice by many Europeans of taking extended vacation time and delaying capital purchase activities until their return in the fall. We have historically generated a significant portion of product revenue in the fourth quarter due to the combination of increased activity in Europe coupled with North American enterprise customers who often wait until the fourth quarter to extract favorable pricing terms from their vendors, including Sourcefire. The timing of these shipments could materially affect our year-end product revenue. Currently, we do not see any indication that these seasonal patterns will change significantly in the foreseeable future.

Quarterly Timing of Revenue

On a quarterly basis, we have usually generated the majority of our product revenue in the final month of each quarter. We believe this occurs for two reasons. First, many customers wait until the end of the quarter to extract favorable pricing terms from their vendors, including Sourcefire. Second, our sales personnel, who have a strong incentive to meet quarterly sales targets, have tended to increase their sales activity as the end of a quarter nears, while their participation in sales management review and planning activities are typically scheduled at the beginning of a quarter.

Liquidity and Capital Resources

At December 31, 2006 and December 31, 2005, our principal sources of liquidity were cash and cash equivalents totaling $13.0 million and $1.1 million, respectively, held-to-maturity investments of $13.3 million and

Table of Contents

$2.0 million, respectively, and accounts receivable of $16.5 million and $12.9 million, respectively. We have funded our growth primarily with proceeds from the issuance of convertible preferred stock for aggregate net cash proceeds of $56.5 million through December 31, 2006, occasional borrowings under a working capital line of credit and cash generated from operations.

We manufacture and distribute our products through contract manufacturers and OEMs. We believe that this approach gives us the advantages of relatively low capital investment and significant flexibility in scheduling production and managing inventory levels. By leasing our office facilities, we also minimize the cash needed for expansion. Our capital spending is generally limited to leasehold improvements, computers, office furniture and product-specific test equipment. The majority of our products are delivered to our customers directly from our contract manufacturers. Accordingly, our contract manufacturers are responsible for purchasing and stocking the components required for the production of our products and they invoice us when the finished goods are shipped.

Our product sales are, and are expected to continue to be, highly seasonal. This seasonality typically results in a significant amount of cash provided by our operating activities during the first half of the year with lower to negative cash flow during the second half of the year. We have cash reserves and a working capital line of credit that can be utilized to cover any short-term cash needs resulting from the seasonality of our business.

Discussion of Cash Flows

Net cash provided by our operating activities in 2006 was $2.1 million compared to net cash used in our operating activities in 2005, 2004 and 2003 of $4.5 million, $9.8 million and $7.6 million, respectively.

The cash provided by our operations in 2006 resulted primarily from an increase in deferred revenue of $3.5 million, an increase in accounts payable and accrued expenses of $1.6 million, and depreciation and amortization of $1.3 million and stock based compensation of $806,000, both of which are non-cash charges, offset by an increase in accounts receivable of $3.6 million and a net loss of $932,000. Deferred revenue increased primarily due to an increase of $4.4 million in support services provided to customers. The increase in accounts payable and accrued expenses resulted primarily from additional legal costs associated with this offering and additional contract manufacturing costs associated with increased sales volume. The increase in accounts receivable resulted primarily from our seasonally significant fourth quarter product sales that are invoiced and recorded as revenue but not collected as of the end of the calendar year.

The cash used in our operating activities in 2005 resulted primarily from a net loss of $5.5 million and an increase of $5.1 million in accounts receivable and $1.1 million in inventory, offset by an increase in deferred revenue of $5.0 million, and depreciation and amortization of $1.1 million and stock-based compensation of $470,000, both of which are non-cash charges. The increase in accounts receivable resulted primarily from our seasonally significant fourth quarter product sales that are invoiced and recorded as revenue but not collected as of the end of the calendar year, while the increase in inventory was primarily due to the expansion of our number of evaluation, or demonstration, products, especially the enterprise class intrusion sensors. Deferred revenue increased primarily due to an increase of $3.6 million for support services to customers, which are usually paid for in advance but recorded as revenue ratably throughout the term of the service contract.

The cash used in our operating activities in 2004 resulted primarily from a net loss of $10.5 million and an increase of $4.7 million in accounts receivable and $409,000 in inventory, offset by an increase in deferred revenue of $3.1 million, an increase in accounts payable and accrued expenses of $1.7 million and depreciation and amortization of $756,000 and stock-based compensation of $177,000, both of which are non-cash charges. The increase in accounts receivable resulted primarily from our seasonally significant fourth quarter product sales that are invoiced and recorded as revenue but not collected as of the end of the calendar year, while the increase in inventory was primarily

due to the expansion of our number of evaluation, or demonstration, products. Deferred revenue increased primarily due to an increase of $2.4 million for support services to customers and $480,000 for products.

Historically, we have incurred significant losses, largely attributable to our investment in internally funded research and development and the rapid expansion of our sales force. Based on our historical product development efforts, we launched our first commercial products in November 2001. Since November 2001, our revenue has

significantly increased, our investment in internally-funded research and development has declined as a percentage of revenue, but not for any subsequent period. We have not invested significantly in property, plant and equipment, and we have established an outsourced approach to manufacturing that provides significant flexibility in both managing inventory levels and financing our inventory. Our revenue has been highly seasonal. This seasonality tends to result in the generation of cash in the first quarter of the year, due to the collection of accounts receivable from significant fourth quarter billings, and the net use of cash during the remaining nine months of the year. Given the recent success of our products and resulting growth in revenue, we believe that the proceeds of this offering, existing cash, cash equivalents, cash provided by operating activities and funds available through our bank line of credit will be sufficient to meet our working capital and capital expenditure needs for at least the next 24 months.

Credit Facility. In March 2005, we renewed our loan and security agreement with Silicon Valley Bank, under which we increased our working capital line of credit with Silicon Valley Bank so that we can borrow up to $5.0 million. This agreement also provides for an additional $1.0 million equipment facility for capital expenditure financing and we obtained a supplemental $1.0 million equipment facility in July 2006, for a total of $2.0 million. Interest on the working capital line of credit accrues at a variable rate of prime plus 0.5%. The line expires on March 28, 2007, at which time all advances will be immediately due and payable. We intend to renew this credit facility for a minimum period of one year. As of December 31, 2006, we had no amounts outstanding and $4.8 million available under our working capital line of credit. Any borrowings we may make under the working capital line of credit would be secured by substantially all of our assets, other than our intellectual property. We have issued a $201,000 standby letter of credit which reduces the available borrowings under the agreement by that amount. For the equipment facility, we were allowed to request advances through January 31, 2007. Each advance is collateralized into a note payable at a fixed rate of 9.0% or prime plus 0.5% over a term of 36 months. As of December 31, 2006, we had $1,312,000 outstanding and $113,000 remaining available under the equipment facility. The $113,000 remaining availability was fully utilized as of January 31, 2007. The working capital line of credit restricts our ability to:

incur or guaranty additional indebtedness;

create liens;

enter into transactions with affiliates;

make loans or investments;

sell assets;

pay dividends or make distributions on, or repurchase, our stock; or

consolidate or merge with other entities.

In addition, we are required to maintain a monthly adjusted quick ratio (unrestricted cash plus accounts receivable to current liabilities, excluding deferred revenue, plus long-term debt) of 1.5 to 1.0 and we must achieve a positive earnings before interest, taxes, depreciation and amortization by the calendar quarter ending March 31, 2007. These thresholds are based on our stockholders equity, assuming conversion of all of our convertible preferred stock into shares of common stock. These operating and financial covenants may restrict our ability to finance our operations, engage in business activities or expand or pursue our business strategies. As of December 31, 2006, we were in compliance with all covenants under the credit facility. To the extent we are unable to satisfy those covenants in the future, we will need to obtain waivers to avoid being in default of the terms of either of our credit facilities. In addition to a covenant default, other events of default under our credit facilities include the filing or entry of a tax lien, attachment of funds or material judgment against us, or other uninsured loss of our material assets. If a default occurs,

the bank may require that we immediately repay all amounts of principal and interest then outstanding. After this offering, we expect that we will have sufficient resources to fund any amounts which may become due under this credit facility as a result of a default by us or otherwise. Any amounts which we may be required to repay prior to a scheduled repayment date, however, would reduce funds that we could otherwise allocate to other opportunities that we consider desirable.

Working Capital and Capital Expenditure Needs

Except as disclosed in the Contractual Obligations table below, we currently have no material cash commitments, except for normal recurring trade payables, expense accruals and operating leases, all of which we

Table of Contents

anticipate funding through our existing working capital line of credit, our available working capital and funds expected to be provided by operating activities. In addition, we do not currently anticipate significant investment in property, plant and equipment, and we believe that our outsourced approach to manufacturing provides us significant flexibility in both managing inventory levels and financing our inventory. In the event that our revenue plan does not meet our expectations, we may eliminate or curtail expenditures to mitigate the impact on our working capital. Our future capital requirements will depend on many factors, including our rate of revenue growth, the expansion of our marketing and sales activities, the timing and extent of spending to support product development efforts, the timing of introductions of new products and enhancements to existing products, the acquisition of new capabilities or technologies, and the continuing market acceptance of our products and services. Moreover, to the extent that existing cash, cash equivalents, cash from operations, cash from short-term borrowing and the net proceeds from this offering are insufficient to fund our future activities, we may need to raise additional funds through public or private equity or debt financing. In the years ended December 31, 2006 and 2005 we spent $1.3 million and $2.2 million, respectively, on capital equipment. Our capital expenditure budget for 2007 totals approximately $2.5 million, which is expected to include approximately $400,000 for leasehold improvements, $1.2 million for additional testing equipment for our research and development lab, $600,000 for additional network systems and $300,000 for personal computers for additional personnel we anticipate hiring.

Although we are currently not a party to any agreement or letter of intent with respect to potential investments in, or acquisitions of, businesses, services or technologies, we may enter into these types of arrangements in the future, which could also require us to seek additional equity or debt financing. Additional funds may not be available on terms favorable to us or at all. We currently have no plans, proposals or arrangements with respect to any specific acquisition.

Contractual Obligations

Our principal commitments consist of obligations under our equipment facility, leases for office space and minimum contractual obligations for services. The following table describes our commitments to settle contractual obligations in cash as of December 31, 2006:

	Payments due by period				
	Total	Less than 1 year	1-3 years	3-5 years	More than 5 years
			(in thousands)		
Equipment Line of Credit Facility	$ 1,312	$ 675	$ 637	$	$
Operating Leases	5,511	1,576	2,604	1,290	41
Purchase Commitments[(1)]	1,655	1,388	267		

(1) We entered into a purchase commitment with a hardware manufacturing vendor with whom we have a current arrangement. Under the terms of this commitment, we have agreed to purchase a set quantity of new appliance inventory over an 18-month period. The approximate value of the purchase commitment is $800,000 and we expect to commence making payments under this commitment beginning in April 2007 once the new appliance configuration is accepted. Additionally, we have entered into a purchase commitment with a vendor to license database software that is used in our products. Under the terms of the commitment, we are permitted to distribute the vendor s software in our products through December 31, 2010 in exchange for an up front payment, plus annual maintenance fees. The approximate aggregate value of the purchase commitment is $855,000, which was paid in January 2007.

As of December 31, 2006, our total contractual obligations were $6.8 million or a net increase of $2.8 million over the amount due at December 31, 2005, due to increased borrowings under our equipment facility with Silicon Valley Bank, our off-balance sheet arrangement with ePlus, and new leases of office space.

Off-Balance Sheet Arrangements

As of December 31, 2006, we had an off-balance sheet arrangement with ePlus, a supplier and financier of computer equipment and furniture. The arrangement provides financing that does not meet the requirement of generally accepted accounting principles for treatment as capitalized equipment and furniture due to the short

Table of Contents

length of the term of the financing versus the useful life of the equipment and furniture. As of December 31, 2006 we had utilized approximately $845,000 of this arrangement which has no set expiration date, but can be terminated by either party providing the other party notice of the intent to discontinue.

Recent Accounting Pronouncement

On July 13, 2006, the FASB issued FIN 48, Accounting for Uncertainty in Income Taxes. FIN 48 clarifies the accounting for uncertainty in income taxes recognized in an enterprise s financial statements in accordance with FASB Statement No. 109, Accounting for Income Taxes. FIN 48 prescribes a recognition threshold and measurement attribute for the financial statement recognition and measurement of a tax position taken or expected to be taken in a tax return. FIN 48 also provides guidance on derecognition, classification, interest and penalties, accounting in interim periods, disclosure and transition. FIN 48 is effective for fiscal years beginning after December 15, 2006. An enterprise is required to disclose the cumulative effect of the change on retained earnings in the statement of financial position as of the date of adoption and such disclosure is required only in the year of adoption. We are currently evaluating the effect that FIN 48 will have on our consolidated balance sheets, consolidated statements of operations or consolidated statements of cash flows.

Quantitative and Qualitative Disclosures about Market Risk

Foreign Currency Risk

Nearly all of our revenue is derived from transactions denominated in U.S. dollars, even though we maintain sales and business operations in foreign countries. As such, we have exposure to adverse changes in exchange rates associated with operating expenses of our foreign operations, but we believe this exposure to be immaterial at this time. As we grow our international operations, our exposure to foreign currency risk could become more significant.

Interest Rate Sensitivity

We had unrestricted cash, cash equivalents and held-to-maturity investments totaling $26.3 million at December 31, 2006. The unrestricted cash and cash equivalents are held for working capital purposes while investments, made in accordance with our low-risk investment policy, take advantage of higher interest income yields. In accordance with our investment policy, we do not enter into investments for trading or speculative purposes. Some of the securities in which we invest, however, may be subject to market risk. This means that a change in prevailing interest rates may cause the principal amount of the investment to fluctuate. To minimize this risk in the future, we intend to maintain our portfolio of cash equivalents and long-term investments in a variety of securities, including commercial paper, money market funds, debt securities and certificates of deposit. Due to the nature of these investments, we believe that we do not have any material exposure to changes in the fair value of our investment portfolio as a result of changes in interest rates.

Our exposure to market risk also relates to the increase or decrease in the amount of interest expense we must pay on our outstanding debt instruments, primarily certain borrowings under our bank working capital line of credit and equipment facility. Any advances under the working capital line of credit and certain advances under our equipment facility bear a variable rate of interest determined as a function of the prime rate at the time of the borrowing and is adjusted monthly based on changes in the prime rate. Other advances under our equipment facility bear interest at a fixed rate of interest. At December 31, 2006, there were no amounts outstanding under our working capital line of credit and $1,312,000 outstanding under the equipment facility. The interest rates paid on this balance at December 31, 2006 were: a fixed rate of 6.5% on $18,000; a fixed rate of 7.0% on $458,000; and a variable rate of 8.75% on $836,000.

53

Table of Contents

BUSINESS

Overview

We are a leading provider of intelligence driven, open source network security solutions that enable our customers to protect their computer networks in an effective, efficient and highly-automated manner. We sell our security solutions to a diverse customer base that includes over 25 of the Fortune 100 companies and over half of the 30 largest U.S. government agencies. We also manage one of the security industry s leading open source initiatives, Snort.

Our family of network security products forms a comprehensive Discover, Determine and Defend, or 3D, approach to network security. Using this approach, our technology can automatically:

- Discover potential threats and points of vulnerability through use of our Intrusion Sensors coupled with our Real-time Network Awareness, or RNA, Sensors;
- Determine the potential impact of those observations to the network by aggregating threat and network intelligence, including potential attacks and points of vulnerabilities at the Defense Center; and
- Defend the network through proactive enforcement of security policy, substantially reducing the need for manual investigation and intervention by information technology, or IT, administrators.

At the heart of the Sourcefire 3D security solution is RNA, our network intelligence product that provides persistent visibility into the composition, behavior, topology (the relationship of network components) and risk profile of the network. This information provides a platform for automated decision-making and network policy compliance enforcement. The ability to continuously discover characteristics and vulnerabilities of any computing device, or endpoint, communicating on a network (such as a computer, printer or server) or endpoint intelligence, along with the ability to observe how those endpoints communicate with each other, or network intelligence, enables our Intrusion Prevention products to more precisely identify and block threatening traffic and to more efficiently classify threatening and/or suspicious behavior than products lacking network intelligence.

Using a broad range of analysis, reporting and automated response capabilities, the Defense Center aggregates, correlates and prioritizes network security events from RNA Sensors and Intrusion Sensors to synthesize multipoint event correlation and policy compliance analysis. The Defense Center s policy and response subsystems are designed to leverage existing IT infrastructure such as firewalls, routers, trouble ticketing and patch management systems for virtually any task, including alerting, blocking and initiating corrective measures.

The traffic inspection engine used in our intrusion prevention products is the open source technology called Snort®. Martin Roesch, our founder and Chief Technology Officer, created Snort in 1998, and assigned his rights in Snort to us when we were formed. Our employees, including Mr. Roesch, have authored all major components of

Table of Contents

Snort, and we maintain control over the Snort project, including the principal Snort community forum, Snort.org. Snort, which has become a de facto industry standard, has been downloaded over 3 million times. We believe that a majority of the Fortune 100 companies and all of the 30 largest U.S. government agencies use Snort technology to monitor network traffic and that Snort is the most widely deployed intrusion prevention technology worldwide. The ubiquitous nature of the Snort user community represents a significant opportunity to sell our proprietary products to customers that require a complete enterprise solution.

For the years ended December 31, 2005 and 2006, we generated approximately 82% and 81% of our revenue from customers in the United States and 18% and 19% from customers outside of the United States respectively. We have expanded our international and indirect distribution channels and, in the future, we expect to increase sales outside of the United States and to source additional customer prospects and generate an increasing portion of product revenue through alliances with original equipment manufacturers, or OEMs, such as Nokia Inc. We increased our revenue from $32.9 million in 2005 to $44.9 million in 2006, representing a growth rate of 37%. For the year ended December 31, 2006, product revenue represented 67% of our total revenue and services revenue represented 33% of our total revenue.

Our Industry

We believe, based on our review of various industry sources, that the network security industry was estimated to be a $18.4 billion market in 2006 and is projected to grow to $26.9 billion in 2009, representing a compound annual growth rate of over 13%. Our addressable markets include intrusion prevention, vulnerability management and unified threat management, which were collectively projected to total $2.9 billion in 2006 and are expected to grow at a compound annual growth rate in excess of 21% to $5.2 billion in 2009, according to industry sources we reviewed. We expect growth should continue as organizations seek solutions to various growing and evolving security challenges, including:

Greater Sophistication, Severity and Frequency of Network Attacks. The growing use of the Internet as a business tool has required organizations to increase the number of access points to their networks, which has made vast amounts of critical information more vulnerable to attack. Theft of sensitive information for financial gain motivates network attackers, who derive profit through identity theft, credit card fraud, money laundering, extortion, intellectual property theft and other illegal means. These profit-motivated attackers, in contrast to the hobbyist hackers of the past, are employing much more sophisticated tools and techniques to generate profits for themselves and their well-organized and well-financed sponsors. Their attacks are increasingly difficult to detect and their tools often establish footholds on compromised network assets with little or no discernable effect, facilitating future access to the assets and the networks on which they reside.

Increasing Risks from Unknown Vulnerabilities. Vulnerabilities in computer software that are discovered by network attackers before they are discovered by security and software vendors represent a tremendous risk. These uncorrected flaws can leave networks largely defenseless and open to exploitation. According to CERT-CC data as of October 2006, the trends in the rate of vulnerability disclosure are particularly alarming, with approximately 3,780 disclosed in 2004 and more than 5,990 disclosed in 2005. During 2006, Microsoft alone issued 49 patches designated as critical for its various software products. Many vulnerabilities have existed since the original release of the affected software products some dating back to the 1990s but were not corrected until recently.

Potential Degradation of Network Performance. Many security products degrade network performance and are, therefore, disfavored by network administrators who generally prioritize network performance over incremental gains in network security. For example, the use of active scanners that probe networks for vulnerabilities often meet heavy resistance from administrators concerned about excessive network noise, clogged firewall logs, and disruption of network assets that are critical to business operations.

Diverse Demands on Security Administrators. The proliferation of targeted security solutions such as firewalls, intrusion prevention systems, URL filters, spam filters and anti-spyware solutions, while critical to enhancing network security, create significant administrative burdens on personnel who must manage numerous disparate technologies that are seldom integrated and often difficult to use. Most network security products require manual, labor intensive incident response and investigation by security administrators, especially when false

Table of Contents

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 the growing number of start-up security companies.

Heightened Government Regulation. Rapidly growing government regulation is forcing compliance with increased requirements for network security, which has escalated demand for security solutions that both meet compliance requirements and reduce the burden of compliance reporting and enforcement. Examples of these laws include

The Health Insurance Portability and Accountability Act of 1996, or HIPAA, and its related rules, which establish requirements for safeguards to protect the confidentiality, integrity and availability of electronic protected health information.

The Financial Services Modernization Act of 1999, commonly known as the Gramm-Leach-Bliley Act, which includes provisions to protect consumers personal financial information held by financial institutions.

The Sarbanes-Oxley Act of 2002, which mandates that public companies demonstrate due diligence in the disclosure of financial information and maintain internal controls and procedures for the communication, storage and protection of such data.

The Federal Information Security Management Act, which requires federal agencies, including contractors and other organizations that work with the agencies, to develop, document and implement an agency-wide information security program.

Our Competitive Strengths

We are a leading provider of intelligence driven, open source network security solutions that enable our customers to protect their computer networks in an effective, efficient and highly automated manner. We apply the Sourcefire 3D security solution Discover, Determine, Defend to network security through our comprehensive family of products, which consists of our RNA, Intrusion Sensors and the Defense Center products. Our competitive strengths include:

Real-Time Approach to Network Security. Our approach to network security enables our customers to secure their networks by providing real-time defense against both known and unknown threats. Our solution is designed to support a continuum of network security functions that span pre-attack hardening of assets, high fidelity attack identification and disruption and real-time compromise detection and incident response. In addition, our ability to confidently classify and prioritize threats in network traffic and determine the composition, behavior and relationships of network devices, or endpoints, allows us to reliably automate what are otherwise manual, time-intensive processes. For example, our Intrusion Sensor may trigger an alert upon identifying a Microsoft Windows-specific threat. The Defense Center would collect this alert, or security event, and classify and prioritize the event based upon a number of factors including, whether any other Intrusion Sensor generated the same alert, whether the network endpoints are vulnerable to that specific attack (based on intelligence collected by RNA Sensors and whether the threat is against a high-priority target (e.g., an e-commerce server). The response to any given security event is predicated upon this automated, real-time intelligent analysis and could range from no action (as in the case where the Defense Center has determined that the network or the individual asset is not vulnerable to the observed threat) to blocking the threat in real time, dynamically modifying firewall policy, and/or launching configuration management software to correct a vulnerability condition.

Comprehensive Network Intelligence. Our innovative network security solution incorporates RNA, which provides persistent visibility into the composition, behavior, topology and risk profile of the network and serves as a platform for automated decision-making and network security policy enforcement. RNA performs passive, or non-disruptive,

network discovery. This enables network behavior analysis and real-time compositional cataloging of network assets, including their configuration, thereby significantly increasing the network intelligence available to IT and security administrators. By integrating this contextual understanding of the network s components and situational awareness of network events, our solution is effective across a broad range of security domains, especially in the area of threat identification and impact assessment. In the intrusion prevention and vulnerability

management markets, we believe that our solution s ability to gather this network intelligence has made our products difficult to evade, easy to tune or calibrate, and efficient, in terms of network performance as measured by aggregate throughput and latency reduction.

The Snort Community. The Snort user community, with over 100,000 registered users and over 3 million downloads to date, has enabled us to establish a market footprint unlike any other in the industry. We believe that a majority of the Fortune 100 companies and all of the top 30 U.S. government agencies (as measured by total annual budgets) use Snort technology to monitor network traffic and that Snort is the most widely deployed intrusion prevention technology worldwide. We believe the Snort open source community provides us with significant benefits, including a broad threat awareness network, significant research and development leverage, and a large pool of security experts that are skilled in the use of our technology. The Snort user community enables us to cost-effectively test new algorithms and concepts on a vast number of diverse networks and significantly expedites the process of product innovation. We believe that Snort s broad acceptance makes us one of the most trusted sources of intrusion prevention and related security solutions.

Leading-Edge Performance. Our solutions are built to maintain high performance across the network while also providing high levels of network security. Specifically, our solutions have the ability to process multiple gigabits of traffic with latency as low as 100 microseconds. Our intrusion prevention 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. The Defense Center supports event loads as high as 1,300 events per second, which we believe meets or exceeds the requirements of the most demanding enterprise customers.

Significant Security Expertise. We have a highly knowledgeable management team with extensive network security industry experience gained from past service in leading enterprises and government organizations including Symantec, McAfee, the Department of Defense and the National Security Agency. Our founder and CTO, Martin Roesch, invented Snort and the core RNA technology and is widely regarded as a network security visionary. In addition, our senior management team averages 16 years of experience in the networking and security industries. Our employees have authored all major components of the Snort source code and maintain the Snort project. In addition, our Vulnerability Research Team, or VRT, is comprised of highly experienced security experts who research new vulnerabilities and create innovative methods for preventing attempts to exploit them. By combining the strengths of our VRT with the tremendous breadth of the Snort community, we believe our aggregate industry knowledge places us at the leading edge of the network security industry.

Broad Industry Recognition. We have received numerous industry awards and certifications including recognition as a leader in the network intrusion prevention systems market, supporting our position as one of a select few companies that best combines completeness of vision with ability to execute. RNA is one of only five network security products to receive the NSS Gold award, which is awarded by The NSS Group only to those products that are distinguished in terms of advanced or unique features, and which offer outstanding value. In addition, our technology has achieved Common Criteria Evaluation Assurance Level 2, or EAL2, which is an international evaluation standard for information technology security products sanctioned by, among others, the International Standards Organization, the National Security Agency and the National Institute for Standards and Technology.

Our Growth Strategy

We intend to become the preeminent provider of network security solutions on a global basis. The key elements of our growth strategy include:

Continue to Develop Innovative Network Security Technology. We intend to maintain and enhance our technological leadership position in network security. We will continue to invest significantly in internal development and product enhancements and to hire additional network security experts to broaden our proprietary knowledge base. We believe our platform is capable of expanding into new markets such as unified threat management, security management, network behavior analysis and compliance and network management and, over time, we expect to penetrate these markets with innovative products and technologies.

Table of Contents

Grow Our Customer Base. We have a substantial opportunity to grow our customer base as our products become more widely adopted. With over 3 million downloads of Snort and over 100,000 registered users, we believe Snort is the most ubiquitous network intrusion detection and prevention technology and represents a significant customer conversion and up-sell opportunity for Sourcefire. We seek to monetize the Snort installed base by targeting enterprises that implement Snort but have not yet purchased any of the components of our Sourcefire 3D security solution. We will continue to target large enterprises and government agencies that require advanced security technology and high levels of network availability and performance in sectors including finance, technology, healthcare, manufacturing and defense. Furthermore, we may attempt to create new customer conversion and up-sell opportunities by releasing select future product developments and enhancements under an open source licensing scheme, similar to the up-sell opportunities for our current products created by releasing Snort under the GNU General Public License.

Further Penetrate Our Existing Customer Base. We believe our strong customer relationships provide us the opportunity to sell additional quantities of existing products and up-sell new products. Through December 31, 2006, over 1,300 customers have purchased our Intrusion Sensors and Defense Center products. We intend to sell additional Intrusion Sensors to existing customers and expand our footprint in the networks of our customers to include branch offices, remote locations and data centers. In addition, we believe we have a significant opportunity to up-sell our higher margin RNA product to existing customers because of the significant incremental benefit that increased network intelligence can bring to their security systems.

Expand Our OEM Alliances and Distribution Relationships. We believe we have a significant opportunity to drive revenue growth through our OEM and distribution relationships. As part of our ongoing effort to expand our OEM alliances, we recently entered into a relationship with Nokia, Inc. whereby Nokia Enterprise Solutions will market to its enterprise customers network security solutions that utilize our proprietary software and technology. In addition, we seek to expand our strategic reseller agreements and increasingly use this channel to generate additional inbound customer prospects. For example, we have reseller agreements with True North Solutions, which has been acquired by American Systems Corporation, and Pentura Limited, a UK information technology security company, through which we expect to derive additional revenue growth in the future. We also intend to utilize our relationships with managed security service providers such as Verizon, VeriSign and Symantec, to derive incremental revenue. In 2006, we generated approximately 11% of our revenue from governmental organizations and, in the future, we believe we will generate an increasing amount of revenue from government suppliers such as Lockheed Martin, Northrop Grumman and Immix Technology, who resell our products to government agencies. In addition, we believe we have a significant opportunity to drive revenue growth by expanding our relationships with other network security vendors. For example, Crossbeam Systems, Inc. currently offers the Sourcefire 3D security solution as a blade, or server component, in its unified threat management appliance.

Strengthen Our International Presence. We believe the network security needs of many enterprises located outside of North America are not being adequately served and represent a significant potential market opportunity. In 2006, we generated approximately 19% of our revenue from international customers. We have distribution agreements with several resellers having significant foreign presence, through which we now offer the Sourcefire 3D security solution. We are expanding our sales in international markets by adding distribution relationships and expanding our direct sales force, with plans in the next year to double the number of personnel in Europe and to hire a country manager for Japan. We believe that the addition of more sales personnel will lead to increased international sales.

Selectively Pursue Acquisitions of Complementary Businesses and Technologies. To accelerate our expected growth, enhance the capabilities of our existing products and broaden our product and service offerings, we intend to selectively pursue acquisitions of businesses, technologies and products that could complement our existing operations. We continually seek to enhance and expand the functionality of our offerings and in the future we may pursue acquisitions that will enable us to better satisfy our customers rigorous and evolving network security needs.

We currently have no plans, proposals or arrangements with respect to any specific acquisition.

Table of Contents

Products

Our key products consist of RNA Sensors, Intrusion Sensors and the Defense Center. When deployed in a customer s network, these three products work together to produce an automated, unified intrusion prevention solution. The RNA Sensors and the Intrusion Sensors report network information and intelligence back to the central management center, known as the Defense Center. The Defense Center then aggregates, contextualizes, analyzes, prioritizes and acts on the event information generated by the RNA Sensors and the Intrusion Sensors. By aggregating the events from these sources, the Defense Center is designed to offer a comprehensive view of security events on a customer s network and can identify suspicious activity that is undetectable through traditional intrusion detection/prevention products. While our customers can purchase and use the Intrusion Sensors without necessarily purchasing the Defense Center (as in the case where the customer is using a different kind of management console or where the customer can manage the sensor directly), a customer deploying an Intrusion Sensor without a corresponding Defense Center loses a significant amount of capability available when the products are used together.

Our approach to network security enables our customers to secure their networks by providing real-time defense against both known and unknown threats. For example, our Intrusion Sensor may trigger an alert upon identifying a Microsoft Windows-specific threat. The Defense Center would collect this alert, or security event, and classify and prioritize the event based upon a number of factors, including whether any other Intrusion Sensor generated the same alert, whether the network endpoints are vulnerable to that specific attack (based on intelligence collected by an RNA sensor) and whether the threat is against a high-priority target (e.g., an e-commerce server). The response to any given security event is predicated upon this automated, real-time intelligent analysis and could range from no action (as in the case where the Defense Center has determined that the network or the individual asset is not vulnerable to the observed threat) to blocking the threat in real time, dynamically modifying firewall policy, and/or launching configuration management software to correct a vulnerability condition.

Our products are generally sold as dedicated hardware appliances that are pre-configured with our proprietary network security technology, along with open source software, including Snort. By offering our products as turn-key solutions, our customers benefit from:

Ease of Installation and Interoperability. RNA and the Intrusion Sensors can be shipped to various locations, plugged in by any network or systems administrator and configured remotely, usually in less than 30 minutes, and are easy to install across geographically dispersed organizations. In addition, our products are typically interoperable with the diverse range of IT infrastructures used by our customers.

Ease of Management and Maintenance. Because our appliances are pre-configured with our proprietary technology, open source software, a secure operating system and a self-maintaining database, each appliance can be managed and maintained from a central console.

Table of Contents

High Degree of Performance and Scalability. Our products exhibit high levels of performance in network environments with line speeds of up to eight gigabits per second with latency as low as 100 microseconds, ideal for latency-sensitive services such as voice over internet protocol. Additionally, depending upon the volume of network traffic, the Defense Center can support up to 120 RNA Sensors and/or Intrusion Sensors, making the Sourcefire 3D security solution scalable for the most demanding customer environments. By way of comparison, a network that would require 120 RNA sensors would be one that is of significant size and complexity, and would be consistent with a network used by our largest customers. Additionally, multiple Defense Centers may be deployed on a single network.

In addition, RNA can be separately licensed as a standalone software solution for installation on a qualified Linux distribution environment (*e.g.*, Red Hat Enterprise Linux).

We charge our customers a one-time, up-front fee for each of our appliances, which includes a perpetual license to use our proprietary technology installed on that appliance. We license the standalone software version of RNA based upon the number of nodes, or devices, on the network segment monitored by the software. We also charge our customers for annual maintenance and support, which includes the right to receive our VRT certified Rules and updates to the vulnerability database. The ability to receive up-to-date Rules and vulnerabilities is critical to the successful performance of the Sourcefire 3D security solution. Of the customer maintenance and support revenues up for renewal in the year ended December 31, 2006, we renewed approximately 82% of this value. Such services are typically paid for in advance, and recognized ratably as revenue over the period of the agreement.

As of December 31, 2006, the list prices of our Intrusion Sensors ranged from $3,995 to $119,500; the list prices for our RNA Sensors ranged from $1,195 to $11,995; the list prices for our RNA nodes ranged from $3 to $30; and the list prices for our Defense Center ranged from $16,995 to $41,995. Pricing for our products varies based on performance capabilities.

Real-Time Network Awareness, or RNA

RNA, available either as a software product or as an appliance, was invented to solve a very basic problem with traditional network security technologies: they have limited knowledge about the networks that they are defending. Even at the most basic level, firewalls, intrusion detection and prevention systems, patch management systems, vulnerability management systems and IT compliance solutions have limited knowledge about the assets and network they are protecting at any given point in time. Correspondingly, most of these enterprise network security technologies operate with little real-time information about composition, behavior or change within the network environment. As a result, these technologies are often blind to obvious critical security events and are unable to respond without human intervention.

As illustrated below, traditional intrusion prevention and detection technologies provide little automation and require IT professionals to manually perform event analysis and response. By incorporating network intelligence, the Sourcefire 3D security solution increases the amount of automated response to actionable and dismissible events, and reduces the number of security events requiring human analysis and response.

RNA Sensors are deployed at strategic points on the network to provide visibility into traffic passing that point. If RNA can observe the traffic of devices in the network, it can determine the operating system of those devices, the network, transport and application layer protocols (including tunneled protocols and protocols on non-standard ports) they are using, and the services and clients employed by those devices. Once RNA has gathered this information it can determine the topology of the network and the vulnerability state of any individual device.

60

Table of Contents

In addition to determining network behavior and device composition, RNA, coupled with the Defense Center, is capable of identifying potentially threatening or abnormal traffic that would be undetectable through traditional detection techniques and intrusion prevention products. RNA and the Defense Center accomplish this by collecting, aggregating and analyzing traffic flow information. These flow records contain a wide variety of information about the observed network traffic, and anomalies in these flow records can be indicative of malicious or abnormal activity. The Defense Center uses this information to build models of normal network traffic behavior. Divergence from traffic norms, especially when correlated with other network events, enables the Defense Center to identify and trigger responses to threats posed by unknown vulnerabilities, newly released exploits, worms, stealth scans, distributed denial of service and other attacks.

While RNA was originally invented to accumulate intelligence about the network environment and behavior, it has a number of other applications. For example, RNA can (i) inform network access control about device changes that are not compliant with network policy or user roles; (ii) drive real-time patch management by informing those systems of the presence and composition of network end-points; and (iii) inform vulnerability management systems of new hosts and their composition, enabling surgical scanning of those devices on a basis consistent with network security policy. Beyond network security, RNA is also proving to be beneficial in purely administrative tasks. For example, IT administrators use RNA inventory information to assist in asset and license management functions.

RNA 4.0, which we intend to release in the next several months, will allow customers to define and set compliance policies for endpoints, subnetworks or networks with the click of a mouse. Once defined, any change outside of policy would result in immediate notification followed by an array of possible corrective actions, including the sending of an alert, redirection of the asset into a sandbox or quarantined network, blocking some or all traffic to or from the asset, and corrective measures such as patch and configuration management. RNA 4.0 will also include a sophisticated compliance dashboard that will allow administrators to monitor and report on compliance in real-time.

Intrusion Sensors

Intrusion Sensor appliances include proprietary Sourcefire components and open source Snort technology. They monitor network traffic and compare observed traffic to a set of Rules, or a set of network traffic characteristics, indicative of malicious activity. These Rules are created by our Vulnerability Research Team and are updated two to three times per month, depending on the rate that new vulnerabilities and/or exploits are discovered and disclosed. Once the Intrusion Sensors match a Rule to the observed traffic, they send an alert to the Defense Center for further analysis and prioritization.

The Intrusion Sensors can be used either as an intrusion prevention system, configured as an in-line solution, or as an intrusion detection system, passively monitoring traffic and providing alerts. The in-line configuration allows IT administrators to proactively and automatically protect their networks by, for example, blocking sessions containing malicious traffic. We offer several different models of Intrusion Sensors depending on the network traffic volume and inspection performance desired.

Defense Center

The Defense Center enables the central management of critical network security functions, including event monitoring, event correlation and prioritization, policy definition and enforcement, forensic analysis, network behavior analysis, trends analysis, management reporting, and system administration.

The Defense Center can also accept data from legacy Snort sensors, which are sensors built by a customer who has downloaded the open source Snort engine from www.snort.org.

The Defense Center, with its intuitive and easy-to-navigate web-based user interface, includes an integrated high performance database capable of correlating and analyzing events received from RNA Sensors, the Intrusion Sensors and/or Intrusion Agents in real-time to determine the:

relevance of an event to a specific network asset;

potential impact an event will have on the network asset; and

criticality of an event based on the business sensitivity of the targeted network.

Table of Contents

Automated event prioritization allows IT administrators to focus their time and resources on real security events that represent the most critical threats based upon the customer s actual, point-in-time network exposures and threats.

Designed to scale to virtually any size deployment, from remote site to global enterprise, the Defense Center s data management solution is capable of handling extremely high event loads while also preserving those events for both high-level security trends analysis and in-depth forensic analysis down to the individual packet level. The forensic analysis interface features customizable workflows that enable users to tailor the graphical user interface to fit the way they prefer to monitor their networks and investigate and analyze security events. In addition, users can easily create standard or customized reports in PDF, HTML and CSV formats that can be automatically emailed for easy distribution.

The Defense Center also excels as an administrative platform. A flexible scheduling subsystem allows the automation of tasks including system backup, report generation, software update downloading, policy update downloading and the application of intrusion prevention policies. The Defense Center also supports high-availability deployment for management redundancy and dynamic load balancing of our Intrusion Sensors where required.

Services

Maintenance and Support. We offer our customers ongoing product support services for both hardware and software. These maintenance programs are typically sold to customers for a one-year term at the time of the initial product sale and typically automatically renew for successive one-year periods. As part of our maintenance and support, we provide telephone and web-based support, documentation and software updates, error corrections and Rules and vulnerability updates. Additionally, we provide expedited replacement for any defective hardware under warranty.

The ability to receive an accurate and up-to-date set of Rules with which our sensors inspect network traffic is a part of our maintenance and support program. Because the sophistication and methods of attacks are constantly changing, our Vulnerability Research Team, or VRT, is continually crafting, refining and updating our set of Rules so that, when deployed, Intrusion Sensors can detect the most recently discovered vulnerabilities and exploits in addition to existing vulnerabilities and exploits. We typically release new and updated Rules two to three times per month; however, that rate can increase or decrease depending on the rate that new vulnerabilities and exploits are discovered and disclosed. Of the customer maintenance and support revenues up for renewal in the year ended December 31, 2006, we renewed approximately 82% of this value.

We make available all updates, upgrades, patches and new Rules to our customers through our web site. Our maintenance and support team is located at our corporate headquarters in Columbia, Maryland.

Professional Services and Training. Our technical consultants assist our customers in the configuration of our appliances and software. These fee-based services, provided by our technical consultants, include providing advice on optimal sensor deployment strategies within the customer s network, customization, or tuning of, Rules and configuration of appliances for the particular characteristics of the customer s network. Additionally, we provide our customers with fee-based, hands-on training classes on subjects such as sensor deployment, Rule creation, tuning and configuration and security assessment. Our professional services and training are sold directly to our customers as well as indirectly through our resellers and can be delivered by our personnel or authorized training and service partners.

Technology

The Sourcefire 3D security solution provides our customers with a unified intrusion, vulnerability management and compliance enforcement capability. By combining the intelligence gathered by RNA and the Intrusion Sensor, along with the central management of the Defense Center, our customers can better prepare for, defend and remediate attacks on their networks.

Real-time Network Awareness. RNA acquires intelligence about the network passively; that is, it listens to network traffic to determine the key characteristics of the devices on the network. For example, by watching the

Table of Contents

creation and termination of a transmission control protocol, or TCP, connection, RNA can determine, among other things, the operating systems and versions running on the devices communicating with each other, as well the identity of those devices, or their IP addresses. Active network discovery, by contrast, works by sending out probative traffic in order to stimulate a response from accessible devices. It then interprets the responses so that it can draw conclusions about those devices. Because active scanners rely on a pinging model of stimulus and response, they are noisy, have the potential to disrupt or degrade overall network performance, and sometimes disturb the potentially sensitive assets that they seek to interrogate. RNA s passive network discovery methods do not generate traffic on the network and are designed not to disrupt or degrade network performance.

Once RNA has established a host profile for a specific device, it will update that profile dynamically as it observes traffic to or from that device. The types of information that could be updated include routing changes, new services, new protocols on existing service ports, OS vendor or version changes, changed hop count to the device, and changed vendor and version data of services.

In addition to determining network and device composition, RNA, coupled with the Defense Center, is capable of identifying traffic anomalies. RNA and the Defense Center accomplish this by collecting, aggregating and analyzing traffic flow information. These flow records can contain a wide variety of information about the observed network traffic, including a timestamp for the flow start and finish time, the number of bytes and packets observed in the flow, their sequence, the flow s source and destination IP addresses, source and destination port numbers, IP protocol, the application layer protocol and, in the case of TCP flows, all TCP flags observed over the life of the flow. The Defense Center leverages this information to build models of normal network traffic behavior. Divergence from traffic norms, especially when correlated with other network events, can enable critical protection against threats posed by unknown vulnerabilities, newly released exploits, zero-learning worm detection, stealth scans, and fine-grained distributed denial of service attacks, as well as network system malfunctions and misconfigurations.

Defense Center. The Defense Center is a high performance management system suited for large, complex and distributed enterprise networks. It simplifies the complicated issues usually associated with intrusion detection and prevention deployments by incorporating policy management, data aggregation, correlation, analysis and reporting into a single centralized solution that enables our customers to take advantage of a distributed sensor infrastructure. The Defense Center is delivered with a built-in high performance database capable of handling millions of events and supporting in-depth forensic analysis for identification of both discrete occurrences and long-term security trends. Packaged as a complete, preconfigured system and including an intuitive, efficient interface, the Defense Center is easy to install and easy to use on a daily basis.

Table of Contents

The Defense Center also allows IT administrators to build customized policies that combine threat, network and vulnerability management, so that IT administrators can define responses in advance to anomalous observations, including any combination of alerting, blocking or correcting the non-normal condition. Examples include alerting via email, Simple Network Management Protocol, or SNMP, traps or SYSLOG events, blocking by dynamically modifying router, firewall, switch, or IPS policies, and correcting via interaction with trouble ticketing, patch management, or configuration management systems. For maximum flexibility, the Defense Center provides a fully documented remediation application programming interface, or API, that allows the creation of customized responses with third-party technologies.

We also separately license a visualization module to the Defense Center that provides our customers a real-time map of their network using the intelligence gathered by RNA. This visualization module provides a unique, intuitive graphical interface for IT professionals to manage their network assets and enforce policy compliance.

Intrusion Sensors. The Intrusion Sensors are sold as turn-key networking appliances that are composed of highly optimized proprietary Sourcefire components and open source Snort technology. The Intrusion Sensor s threat detection algorithms are governed by a rules-based language that combines the benefits of signature, protocol and anomaly-based inspection methods. The highly flexible Snort rules language also allows administrators to write their own custom rules or to tailor existing rules to their specific networking environment. Once the Intrusion Sensor matches observed traffic with one of the many Rules deployed on the Intrusion Sensor, an alert is generated and sent to the Defense Center for additional analysis and prioritization.

Awards and Certifications. We have received numerous industry awards and certifications, including:

Gartner Magic Quadrant. We were recognized by Gartner, Inc. as being a Leader in the Network Intrusion Prevention System Appliances category.

NSS Gold Award. Our product is one of only five network security products to be awarded the NSS Gold award. NSS is a world leader in benchmarking and independent product evaluations, and the NSS Gold Award is awarded only to those products that are distinguished in terms of advanced or unique features, and which offer outstanding value.

EAL2. Common Criteria Evaluation Assurance Level 2 is an international evaluation standard for information technology security products sanctioned by, among others, the International Standards Organization, the National Security Agency and the National Institute for Standards and Technology.

National Security Agency Systems and Network Attack Center. We have met the classified testing standards of the National Security Agency Systems and Network Attack Center, which are required in order to sell security products to certain agencies of the U.S. Government.

DISA FAO STIG. We have met the classified testing standards of the Defense Information Security Agency, Finance and Accounting Office Security Technical Implementation Guide, which are required in order to sell security products to certain agencies of the U.S. Government.

FIPS 140-2. Federal Information Processing Standard 140-2 is a standard that describes US Federal government requirements that IT products should meet for Sensitive, but Unclassified, or SBU, use. The standard was published by the National Institute of Standards and Technology (NIST). FIPS 140-2 evaluation is required for sale of products implementing cryptography to the Federal Government. In addition, the financial community increasingly specifies FIPS 140-2 as a procurement requirement and is beginning to embrace it.

NEBS. Network Equipment-Building System requirements are used by service providers to qualify equipment that will provide a high level of reliability and safety to their network. These requirements are designed to ensure that products are safe and do not interfere with the reliable operation of a network. NEBS compliance is a critical issue to service providers evaluating the suitability of products for use in their networks.

OSEC. Open Security Evaluation Criteria is a framework for evaluating the security functionality of networked products. OSEC defines a core set of tests for any networked security product, and then adds tests

Table of Contents

for security and performance to each product space, such as network intrusion detection systems. OSEC criteria are open to view and critique, and are formulated with input from vendors, end-users, and many representatives from the security community that actively work in the product spaces for which criteria have been developed.

Customers

We provide products and services to a variety of end users worldwide, including some of the world s largest banks, defense contractors, hospitals, IT companies and retailers, as well as U.S. and other national, state and local government agencies. We view our primary customers as enterprise, service provider and risk management enterprises, but we have also developed products and services for the consumer and small office market. Our enterprise market customers generally have annual revenue exceeding $500 million.

In 2003, Northrop Grumman, a federal government reseller, accounted for 15% of our revenues. In 2004, Immix Technologies, a federal government reseller, accounted for 10% of our revenues. In 2005 and 2006, no customer accounted for over 10% of our revenues. If we failed to retain either Northrop Grumman or Immix Technologies as a reseller customer, we believe that we would find another federal government reseller through which we could sell our products. Our customers represent a broad spectrum of organizations within diverse sectors, including financial services, technology, telecommunications and government and information technology services.

For the years ended December 31, 2005 and 2006, we generated approximately 82% and 81% of our revenue from customers in the United States and approximately 18% and 19% from customers outside of the United States, respectively.

Sales and Marketing

We market and sell our appliances, software and services directly to our customers through our direct sales organization and indirectly through our resellers, distributors and original equipment manufacturers.

Sales. As of December 31, 2006, our sales organization was comprised of approximately 75 full-time individuals organized into two groups: North America and International. We maintain sales offices in Columbia, Maryland; Vienna, Virginia; Livonia, Michigan; and Reading, United Kingdom. As of December 31, 2006, our international sales force was made up of 17 individuals, and our North America sales force was made up of 58 individuals divided into three geographic regions: East, West and Federal. Our sales personnel are responsible for market development, including managing our relationships with resellers, assisting resellers in winning and supporting key customer accounts and acting as liaisons between the end customers and our marketing and product development organizations. We expect to continue to expand our International direct sales group in Europe, the Middle East, Asia/Pacific and Latin America. We are expanding our sales in international markets by adding distribution relationships and expanding our direct sales force, with plans in the next year to double the number of personnel in Europe and to hire a country manager for Japan.

Each sales organization is supported by experienced sales engineers who are responsible for providing pre-sales technical support and technical training for the sales team and for our resellers and distributors. 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 dedicated sales force with broad experience in selling network security products to resellers. We maintain a broad network of value-added resellers throughout the United States and Canada, and distributors in Europe, Latin America and Asia/Pacific. Our arrangements with our resellers are non-exclusive, territory-specific, and generally cover all of our products and

services and provide for appropriate discounts based on a variety of factors including volume purchases. These agreements are generally terminable at will by either party by providing the other party at least 90 days written notice. Our arrangements with distributors also are non-exclusive and territory-specific and provide distributors with discounts based upon the annual volume of their orders. We provide our resellers and distributors with marketing assistance, technical training and support.

Table of Contents

Strategic Relationships. We have established commercial relationships with networking and security companies to provide alternative distribution channels for our products.

We executed an OEM agreement with Nokia Inc. on July 14, 2006 under which Nokia is permitted to incorporate our RNA and Intrusion Sensor technology into Nokia Enterprise Solutions hardware platform for direct and indirect sales to its enterprise customers. In addition, Nokia has the ability to resell the Defense Center. This agreement expires on July 14, 2009. We have no other relationship with Nokia, other than this OEM agreement and there exists no material dependencies on Nokia.

Marketing. Our marketing activity consists primarily of product marketing, product management and sales support programs. Marketing also includes advertising, our Web site, trade shows, direct marketing and public relations. Our marketing program is designed to build the Sourcefire and Snort brands, increase customer awareness, generate leads and communicate our product advantages. We also use our marketing program to support the sale of our products through new channels and to new markets. We have eight full-time employees in our marketing department.

Research and Development

Our research and development efforts are focused primarily on improving and enhancing our existing network security products as well as developing new 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.

Vulnerability Research Team. Our Vulnerability Research Team is a group of leading edge network security experts working to proactively discover, assess and respond to the latest trends in network threats and security vulnerabilities. By gathering and analyzing this information, our Vulnerability Research Team creates and updates Snort Rules and security tools that are designed to identify, characterize and defeat attacks.

This team comprises eight full time employees and operates from our corporate headquarters in Columbia, Maryland. Our Vulnerability Research Team participates in extensive collaboration with hundreds of network security professionals in the open source Snort community to learn of new vulnerabilities and exploits. The Vulnerability Research Team also coordinates and shares information with other security authorities such as The SANS Institute, CERT-CC (Computer Emergency Response Team), iDefense (Verisign), SecurityFocus (Bugtraq; Symantec) and Common Vulnerabilities and Exposures (Mitre). Because of the knowledge and experience of our personnel comprising the Vulnerability Research Team, 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 vulnerability and threats on a real-time basis.

As of December 31, 2006, we had approximately 55 employees dedicated to research and development. Our research and development expense was $5.7 million, $6.8 million and $8.6 million for the years ended December 31, 2004, 2005 and 2006, respectively.

Manufacturing and Suppliers

We rely primarily on contract equipment manufacturers to assemble, integrate and test our appliances and to ship those appliances to our customers. We typically hold little inventory, relying instead on a just-in-time manufacturing philosophy. We rely on four primary integrators. We have contracted with Avnet, Inc., a leading distributor of enterprise network and computer equipment, to manufacture all of our appliances built on IBM hardware. Avnet is our sole supplier of IBM-based hardware appliances. We have also contracted with Patriot Technologies, Inc. and Intelligent Decisions Inc., or IDI, to assemble, integrate and test all our product offerings operating on an Intel

platform. Our agreement with Patriot expires on December 12, 2007, and will automatically renew for successive one year periods unless either we or Patriot notify the other of an intent not to renew at least 90 days prior to expiration. We entered into a conditional purchase commitment with Patriot pursuant to which we have agreed to purchase a set quantity of new appliance inventory over an 18-month period provided that the new appliance meets certain specifications on or before November 15, 2006. The approximate value of the purchase commitment is $800,000. Our agreement with IDI expires on January 31, 2008 and will automatically renew unless

Table of Contents

either party notifies the other party of its intent not to renew at least 30 days prior to the end of the term. Finally, we have contracted with Bivio Networks, Inc. to manufacture select high performance models of our appliances. Bivio is our sole supplier of these high performance models, such as our IS3800 and IS5800, which are the highest priced Intrusion Sensors that we offer. Our agreement with Bivio expires on February 10, 2008. All of these agreements are non-exclusive. 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 terminate or expire 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. As of the date hereof we had 25 patent applications pending for examination in the U.S. and foreign jurisdictions. We currently hold no issued patents. The claims for which we have sought patent protection relate to methods and systems we have developed for intrusion detection and prevention used in our RNA, Intrusion Sensor and Defense Center products. In addition, we utilize contractual provisions, such as non-disclosure and non-compete agreements, as well as 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 Management s Discussion and Analysis of Financial Condition and Results of Operations Seasonality.

Competition

The market for network security monitoring, detection, prevention and response solutions is intensely competitive and we expect competition to increase in the future. Our chief competitors generally fall within the following categories:

- large companies, including Symantec Corporation, Cisco Systems, Inc., Internet Security Systems, Inc. (which has recently been acquired by IBM), Juniper Networks, Inc., 3Com Corporation, Check Point Software Technologies, LTD and McAfee, Inc., that sell competitive products and offerings, as well as other large software companies that have the technical capability and resources to develop competitive products;

- software or hardware network infrastructure companies, including Cisco Systems, Inc., 3Com Corporation and Juniper Networks, Inc., that could integrate features that are similar to our products into their own products;

- smaller software companies offering relatively limited applications for network and Internet security monitoring, de