McAfee, Inc.
Form 10-K
March 01, 2006

Table of Contents

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

Form 10-K

þ **ANNUAL REPORT PURSUANT TO SECTION 13 OR 15(d) OF THE SECURITIES EXCHANGE ACT OF 1934**
For the Fiscal Year Ended December 31, 2005

or

o **TRANSITION REPORT PURSUANT TO SECTION 13 OR 15(d) OF THE SECURITIES EXCHANGE ACT OF 1934**
For the Transition Period from to

Commission File Number: 001-31216

McAfee, Inc.
(Exact name of registrant as specified in its charter)

Delaware *(State or other jurisdiction of incorporation or organization)*	**77-0316593** *(I.R.S. Employer Identification Number)*
3965 Freedom Circle **Santa Clara, California** *(Address of principal executive offices)*	**95054** *(Zip Code)*

Registrant s telephone number, including area code:
(408) 988-3832

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

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

Common Stock, $0.01 Par Value, together with associated Rights

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

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

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

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

Indicate by check mark whether the registrant is a large accelerated filer, an accelerated filer, or a non-accelerated filer. See definition of accelerated filer and large accelerated filer in Rule 12b-2 of the Exchange Act. (Check one):

Large accelerated filer o Accelerated filer þ Non-accelerated filer o

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

The aggregate market value of the voting stock held by non-affiliates of the issuer as of the last business day of the Registrant s most recently completed second fiscal quarter (June 30, 2005) was approximately $4.3 billion. The number of shares outstanding of the issuer s common stock as of February 22, 2006 was 166,315,976.

DOCUMENTS INCORPORATED BY REFERENCE

Items 10, 11, 12, 13 and 14 of Part III are incorporated by reference from the Registrant s Proxy Statement for the Annual Meeting of Stockholders to be held on May 25, 2006.

McAFEE INC.

FORM 10-K
For the fiscal year ended December 31, 2005

TABLE OF CONTENTS

PART I

Item 1. *Business*

General

This Annual Report on Form 10-K contains forward-looking statements that involve risks and uncertainties. These statements include, without limitation, statements regarding our expectations, beliefs, intentions or strategies regarding the future. All forward-looking statements included in this Report on Form 10-K are based on information available to us on the date hereof. These statements involve known and unknown risks, uncertainties and other factors, which may cause our actual results to differ materially from those implied by the forward-looking statements. In some cases, you can identify forward-looking statements by terminology such as may, will, should, could, expects, p anticipates, believes, estimates, predicts, potential, targets, goals, projects, continue, or variations of similar expressions, or the negative of these terms or other comparable terminology. Although we believe that the expectations reflected in the forward-looking statements are reasonable, we cannot guarantee future results, levels of activity, performance or achievements. Therefore, actual results may differ materially and adversely from those expressed in any forward-looking statements. Neither we nor any other person can assume responsibility for the accuracy and completeness of forward-looking statements. Important factors that may cause actual results to differ from expectations include, but are not limited to, those discussed in Risk Factors included in Item 1A of this document. We undertake no obligation to revise or update publicly any forward-looking statements for any reason.

We were incorporated in 1992. In 1999, our subsidiary McAfee.com sold to the public its Class A common stock as a part of its initial public offering. In September 2002, we repurchased the 25% minority interest in McAfee.com and merged McAfee.com with and into us. In June 2004, we changed our name to McAfee, Inc. from Network Associates, Inc. We previously changed our name from McAfee Associates, Inc. to Network Associates, Inc. in conjunction with our December 1997 merger with Network General Corporation.

This report includes registered trademarks and trade names of McAfee and other corporations. Trademarks or trade names owned by McAfee and/or its affiliates include: McAfee, Network Associates, ePO, ePolicy Orchestrator, VirusScan, IntruShield, Entercept, and Foundstone.

We file registration statements, periodic and current reports, proxy statements, and other materials with the Securities and Exchange Commission, or SEC. You may read and copy any materials we file with the SEC at the SEC s Office of Public Reference at 450 Fifth Street, NW, Room 1300, Washington, DC 20549. You may obtain information on the operation of the Public Reference Room by calling the SEC at 1-800-SEC-0330. The SEC maintains a web site at www.sec.gov that contains reports, proxy and information statements and other information regarding issuers that file electronically with the SEC, including our filings.

We are headquartered at 3965 Freedom Circle, Santa Clara, California, 95054, and the telephone number at that location is (408) 988-3832. Our internet address is www.mcafee.com. We make available, free of charge, through the investor relations section of our website, our annual reports on Form 10-K, quarterly reports on Form 10-Q and current reports on Form 8-K, and any amendments to those reports filed pursuant to Section 13(a) or 15(d) of the Securities Exchange Act of 1934, as amended, as soon as reasonably practicable after they are electronically filed with or furnished to the SEC. The contents of our website are not incorporated into, or otherwise to be regarded as part of this Annual Report on Form 10-K.

OVERVIEW

We are a worldwide supplier of computer security solutions designed to proactively prevent intrusions on networks and secure computer systems and other digital devices from a large variety of known and unknown threats and attacks. We apply business discipline and a pragmatic approach to security that is based on four principles of security risk management (identify and prioritize assets; determine acceptable risk; protect against intrusions; enforce and measure compliance). We have one business and operate in one industry, developing, marketing, distributing and supporting computer security solutions for large enterprises, governments, small and medium-sized business and consumers through a network of qualified partners. We operate our business in five geographic regions: North America; Europe, Middle East and Africa, collectively referred to as EMEA; Japan; Asia-Pacific, excluding Japan; and Latin America. See Note 19 to our consolidated financial statements for a description of revenues, operating income and assets by geographic region.

We offer a comprehensive set of security solutions. The solutions include anti-virus, anti-spyware, anti-spam, intrusion prevention, secure messaging, web filtering and vulnerability management. We offer policy management tools to keep threat-protection systems up-to-date and allow companies to enforce security policies.

The majority of our net revenue has historically been derived from our McAfee Security anti-virus products and, until the sale of the Sniffer product line in July 2004, our Sniffer Technologies network fault identification and application performance management products. We have also focused our efforts on building a full line of complementary network and system protection solutions. On the system protection side, we strengthened our anti-virus lineup by adding complementary products in the anti-spam and host intrusion prevention categories, and through our June 2005 Wireless Security Corporation acquisition, we have strengthened our solution portfolio in our consumer and small business segments. On the network protection side, we have added products in the network intrusion prevention and detection category, and through our October 2004 Foundstone acquisition, vulnerability management products and services.

In 2005, our net revenue was $987.3 million and net income was $138.8 million. See Management s Discussion and Analysis of Financial Condition and Results of Operations.

Our two product groups, which are defined below, are McAfee System Protection Solutions and McAfee Network Protection Solutions.

McAfee System Protection Solutions

McAfee system protection solutions help large enterprises, small and medium-sized businesses, consumers, government agencies and educational organizations assure the availability and security of their computer desktops, digital devices, application servers and web service platforms. The McAfee system protection solutions portfolio features a range of products including anti-virus, anti-spyware, managed services, application firewalls and host intrusion prevention. Each is backed by McAfee AVERT Labs, a leading threat research organization. A substantial majority of our net revenue has historically been derived from our McAfee System Protection Solutions.

McAfee system protection solutions also include McAfee consumer security products, offering both traditional retail products and on-line subscription services. Consumer retail and on-line subscription applications allow users to protect their personal computers, or PCs, from malicious code and other attacks, repair PCs from damage caused by viruses and spyware and block spam and other undesirable content. Our retail products are sold through retail outlets, including Best Buy, CompUSA, Costco, Dixons, Fry s, Office Depot, Office Max, Staples, Wal-Mart and Yamada to single users and small home offices in the form of traditional boxed product. These products include for-fee software updates and technical support services. On-line subscription services are delivered through the use of an internet browser at our McAfee Consumer Online web site, through multiple on-line service providers, such as AOL and Comcast, and through original equipment manufacturers, or OEMs, such as Apple, Dell, Gateway/eMachines, NEC and Toshiba, North America.

Our McAfee system protection solutions previously included our Magic Service Solutions product line, offering management and visibility of desktop and server systems. In January 2004, we sold our Magic Solutions product line to BMC Software.

McAfee Network Protection Solutions

McAfee network protection solutions help enterprises, small businesses, government agencies, educational organizations and service providers maximize the availability, performance and security of their network infrastructure. The McAfee network protection solutions portfolio features a range of products including IntruShield for network intrusion detection, Secure Content Management solutions for complete e-mail and web security and prevention, and Foundstone for intrusion detection and prevention and vulnerability management.

Table of Contents

We acquired Foundstone on October 1, 2004. We continue to integrate Foundstone s products with our intrusion prevention technologies and systems management capabilities to deliver enhanced risk management of prioritized assets, automated shielding and risk remediation, and automated policy enforcement and compliance.

Our McAfee network protection solutions previously included our Sniffer Technologies product line, offering network fault identification and application performance management products. In July 2004, we sold our Sniffer Technologies product line to Network General Corporation.

Policy Management

Policy management tools keep threat-protection systems up-to-date and enforce security policies. Policy management includes live threat information and identifying and dealing with rogue systems, and is a key element of complete security protection.

Expert Services and Technical Support

We have established Professional Services and McAfee Technical Support to provide professional assistance in the design, installation, configuration and support of our customers networks and acquired products. We offer a range of consulting and educational services under both the McAfee and Foundstone banners.

McAfee Consulting Services provide product design and deployment with an array of standardized and custom offerings. This business is organized around our major product groupings and also offers a range of classroom education courses designed to enable customers and partners to successfully deploy and operate McAfee s security products. Services are also available to help customers deal with security outbreaks and plan for the upgrade or replacement of key parts of the security infrastructure.

Foundstone Consulting Services assist clients in the early assessment and design of their security and risk architectures. Through research and innovation, the Foundstone Security Practice is able to advise government and commercial organizations on the most effective counter measures required to meet business and legislative targets for security and privacy. Foundstone Consulting Services are augmented by a range of classroom-based training courses including the Ultimate Hacking Series.

The McAfee Technical Support program provides our customers on-line and telephone-based technical support in an effort to ensure that our products are installed and working properly. During the first quarter of 2005, we reorganized our technical support offerings to better meet our customers varying needs. McAfee Technical Support offers a choice of Gold or Platinum support for our customers. In addition, for our legacy support customers only, we offer the on-line ServicePortal or the telephone-based Connect. The services in these offerings have been incorporated into the current Gold and Platinum Technical Support offerings. All Technical Support programs include software updates and upgrades. Technical Support is available to all customers worldwide from various regional support centers.

McAfee Technical Support ServicePortal Consists of a searchable knowledge base of technical solutions and links to a variety of technical documents such as product FAQs and technical notes and the ability to submit and track support cases online.

McAfee Gold Technical Support Provides unlimited, toll-free (where available) telephone access to technical support 24 hours a day, 7 days a week and access to the McAfee Technical Support ServicePortal.

McAfee Platinum Technical Support Offers proactive, personalized service and includes an assigned Technical Account Manager, or TAM. Customers receive proactive support contact (telephone or e-mail) with customer-defined frequency, election of five designated customer contacts, access to all the services in McAfee Gold Technical Support and the McAfee Technical Support ServicePortal.

In addition, we also offer our consumer users technical support services made available at our www.mcafee.com website on both a free and fee-based basis, depending on the support level selected.

Table of Contents

Research and Development

We are committed to malicious code and vulnerability research through our McAfee AVERT Labs organization. McAfee AVERT Labs conducts research in the areas of host intrusion prevention, network intrusion prevention, wireless intrusion prevention, malicious code defense, security policy and management, high-performance assurance and forensics and threats, attacks, vulnerabilities and architectures.

In April 2005, we sold the assets of McAfee Labs, our research and development organization focused on performing research for government agencies, to SPARTA, Inc. McAfee will remain as the general contractor on certain of its government contracts until government approval is obtained for SPARTA to be the general contractor.

Strategic Alliances

From time to time, we enter into strategic alliances with third parties to support our future growth plans. These relationships may include joint technology development and integration, research cooperation, co-marketing activities and sell-through arrangements. Strategic alliance partners include AOL, Cable and Wireless, Comcast, Dell, Gateway, Telecom Italia, Telefonica and Wanadoo, among others. As part of our NTT DoCoMo alliance, we have jointly developed technology to provide integrated anti-virus protection against mobile threats to owners of 3G FOMA handsets.

Product Licensing Model

We typically license our products to corporate and government customers on a perpetual basis. Most of our licenses are sold with maintenance contracts, and typically these are sold on an annual basis. As the maintenance contracts near expiration, we contact customers to renew their contracts, as applicable. We typically sell perpetual licenses in connection with sales of our hardware-based products in which software is bundled with the hardware platform.

For our largest customers (over 2,000 nodes) and government agencies, we also offer two-year term-based licenses. Our two-year term licensing model also creates the opportunity for recurring revenue through the renewal of existing licenses. By offering two-year licenses, as opposed to traditional perpetual licenses, we are also able to meet a lower initial cost threshold for customers with annual budgetary constraints. We also offer one-year licensing arrangements in Japan. The renewal process provides an opportunity to cross-sell new products and product lines to existing customers. Term-based licenses for our customers with over 2,000 nodes accounts for less than 2% of our total revenues in 2005.

On-Line Subscriptions and Managed Applications

For our on-line subscription services, customers essentially rent the use of our security services for a defined period of time. Because our on-line subscription services are version-less, or self-updating, customers subscribing to these services are capable of using the most recent version of the software application without the need to purchase product updates or upgrades. Our on-line subscription consumer products and services are found at our www.mcafee.com web site where consumers download our anti-virus application using their internet browser which allows the application to detect and eliminate viruses on their PCs, repair their PCs from damage caused by viruses, optimize their hard drives and update their PCs virus protection systems with current software updates and upgrades. Our www.mcafee.com website also offers customers access to McAfee Personal Firewall Plus, McAfee SpamKiller and McAfee Privacy Service, as well as combinations of these services. Our on-line subscription services are also available to customers and small business through various relationships with internet service providers, or ISPs, such as AOL and Comcast, and available through PC OEMs, such as Dell and Gateway. Our business model allows for ISPs to make McAfee subscription services available as either a premium service or as a feature included in the ISP s service. At

December 31, 2005, we had approximately 17.2 million McAfee consumer on-line subscribers, which includes on-line customers obtained through our alliances with ISPs and OEMs.

Similarly, our small and medium-sized business on-line subscription products and services, or our Managed VirusScan offerings, provide these customers the most up-to-date anti-virus software. Our Managed VirusScan service provides anti-virus protection for both desktops and file servers. In addition, McAfee Managed Mail

Table of Contents

Protection screens emails to detect and quarantine viruses and infected attachments, and spam. Our McAfee Desktop Firewall blocks unauthorized network access and stops known network threats.

We also make our on-line subscription products and services available over the internet in what we refer to as a managed environment. Unlike our on-line subscription service solutions, these managed service providers, or MSP, solutions are customized, monitored and updated by networking professionals for a specific customer.

Sales and Marketing

Our sales and marketing activities are directed at large corporate and government customers, small and medium-sized accounts and consumers, as well as resellers, distributors, system integrators, internet service providers and OEMs worldwide through the channels listed below.

Resellers and Distributors

The majority of our products are sold through partners, including corporate resellers, retailers, service providers, original equipment manufacturers, or OEMs, and, indirectly, through distributors in all of our geographic regions. In addition, our channel efforts include strategic alliances with complementary manufacturers and publishers to expand our reach and scale. We currently utilize corporate resellers, including ASAP Software, CDW, Dell, Insight, Softmart, Software House International and Software Spectrum, as well as network and systems integrators who offer our solutions and sell site licenses of our software to corporate, small business and government customers.

Independent software distributors who currently supply our products include GE Access, Ingram Micro Inc., MOCA and Tech Data Corp. These distributors supply our products primarily to large retailers, value-added resellers, or VARs, mail order and telemarketing companies. Both through our authorized distributors and directly with certain retail resellers either through a consignment model or a non-consignment model, we sell our retail packaged products to several of the larger computer and software retailers, including Best Buy, CompUSA, Costco, Dixons, Fry s, Office Depot, Office Max, Staples, Wal-Mart and Yamada. Members of our channel sales and marketing force work closely with our major reseller and distributor accounts to manage demand generating activities, training, order flow, and affiliate relationship management.

Our top ten distributors typically account for between 50% to 65% of our net revenues in any quarter. Our agreements with our distributors are not exclusive and may be terminated by either party without cause. Terminated distributors may not continue to sell our products. If one of our significant distributors terminated its relationship with us, we could experience a significant interruption in the distribution of our products.

We utilize a sell-through business model for distributors under which we recognize revenue on products sold through distributors at the time our distributors resell the products to their customers. Under this business model, our distributors are permitted to purchase software licenses at the same time they fill customer orders and to pay for hardware and retail products only when these products are resold to the distributors customers. In addition, prior to the resale of our products, our distributors are permitted rights of return subject to varying limitations. After sale by the distributor to its customer, there is generally no right of return from the distributor to us with respect to such product, unless we approve the return from the final customer to the distributor.

Original Equipment Manufacturers

OEMs license our products for resale to end users or inclusion with their products. For example, we are a security services provider for PC hardware manufacturers such as Apple, Dell, Gateway/eMachines and Toshiba. Depending on the arrangement, OEMs may sell our software bundled with the PC or related services, pre-install our software and allow us to complete the sale, or sublicense a single version of our products to end users who must register the product with us in order to receive updates.

United States Sales

Our United States sales force is organized by product line and customer segment. The majority of our customers are served through reseller partners, while some of our largest accounts are handled by a direct sales organization. The sales organizations supporting our partners are also organized by product line. One set of sales representatives focuses on the McAfee anti-virus installed base. A second focuses on our newer intrusion prevention products and risk management. Small business customers are served exclusively through our reseller partners with a channel organization responsible for lead generation and a channel support team responsible for partner training and contract management.

International Sales

We have sales and support operations in EMEA, Japan, North America, Asia-Pacific (excluding Japan) and Latin America. In 2005, 2004, and 2003 based on net revenue in our regions, revenues outside of North America accounted for approximately 42%, 39% and 35% of our net revenues, respectively. Within our international sales regions, sales forces are organized by country when and where local demand and sales force considerations make it advisable.

Other Marketing Activities

Channel marketing is the means by which we market, promote, train and incentivize our resellers and distributors to promote our products to their end-user customers. We offer our resellers and distributors technical and sales training classes and marketing and sales assistance kits. We also provide specific cooperative marketing programs for end-user seminars, catalogs, demand creation and sales events.

One of the principal means of marketing our products and services is through the internet. Our website, www.mcafee.com, supports marketing activities to our key customer and prospect segments, including home and home office users, small and medium-sized businesses, large enterprises and our partner community. Our website contains various marketing materials and information about our products and our customers can download and purchase products. We also promote our products and services through advertising activities in trade publications, direct mail campaigns and strategic arrangements. In addition, we attend trade shows, sponsor conferences and publish a quarterly newsletter, which is mailed to existing and prospective customers.

We also market our products through the use of rebate programs. Within most countries we typically offer two types of rebate programs, volume incentive rebates to strategic channel partners and promotional rebates to end-users. The strategic channel partner earns a volume incentive rebate primarily based upon its sale of our products to end-users.

Customers

We primarily market our products to large corporate and government customers through resellers and distributors, except for a very small number where we sell direct. Our two largest distributors, Ingram Micro Inc. and Tech Data Corp., together accounted for approximately 33% of our net revenue in 2005.

We market our products to individual consumers directly through on-line distribution channels and indirectly through traditional distribution channels, such as retail stores and OEMs. McAfee Consumer is responsible for on-line distribution of our products sold to individual consumers over the internet or for internet-based products, including products distributed by our on-line partners, and for the licensing of technology to strategic distribution partners for sale to individual consumers, with certain exceptions.

Product Development, Investments, and Acquisitions

We believe that our ability to maintain our competitiveness depends in large part upon our ability to successfully enhance existing products, develop and acquire new products and develop and integrate acquired products. The market for computer software includes low barriers to entry, rapid technological change, and is highly competitive with respect to timely product introductions. As part of our growth strategy, we have made and expect to continue to make acquisitions of, or investments in, complementary businesses, products and technologies.

In addition to developing new products, our internal development staff is focused on developing upgrades and updates to existing products and modifying and enhancing any acquired products. Future upgrades and updates may

Table of Contents

include additional functionality to respond to user problems or address compatibility problems with new or changing operating systems and environments.

For 2005, 2004 and 2003, we expensed $176.4 million, $172.7 million and $184.6 million, respectively, on research and development as incurred. We also expensed in-process research and development totaling $4.0 million related to the acquisition of Wireless Security Corporation in 2005, $5.7 million of related to IntruVert in 2003 and $0.9 million related to Entercept in 2003. See Management s Discussion and Analysis of Financial Condition and Results of Operations.

Manufacturing

We employ an outsourced manufacturing strategy that relies on contract manufacturers for manufacturing services. Our manufacturing operations primarily consist of quality assurance of materials and components, subassemblies, final assembly, and testing of products. We presently use a limited number of independent third-party companies to provide manufacturing and fulfillment services related to assembly, test, and product repair. Our arrangements with contract manufacturers generally provide for quality, cost, and delivery requirements, as well as manufacturing process terms, such as continuity of supply, inventory management, flexibility regarding capacity, quality and cost management, oversight of manufacturing, and conditions for use of our intellectual property. These arrangements generally do not commit us to purchase any particular amount or any quantities beyond certain amounts covered by orders or forecasts that we submit covering discrete periods of time.

Competition

The markets for our products are intensely competitive and are subject to rapid changes in technology. We also expect competition to increase in the near-term. We believe that the principal competitive factors affecting the markets for our products include, but are not limited to:

- performance,
- quality,
- breadth of product group,
- integration of products,
- introduction of new products,
- brand name recognition,
- price,
- market presence,
- functionality,
- innovation,
- customer support,

frequency of upgrades and updates,

reduction of production costs,

manageability of products and

reputation.

We believe that we compete favorably against our competitors in each of these areas. However, some of our competitors have longer operating histories, greater brand recognition, stronger relationships with strategic channel partners, larger technical staffs, established relationships with hardware vendors and/or greater financial, technical and marketing resources. These factors may provide our competitors with an advantage in penetrating markets with their network security and management products.

Table of Contents

System Protection Market. Our principal competitors in the anti-virus market are Symantec Corp., Computer Associates International Inc. and Microsoft Corp., which expects to have its consumer security solution, that may offer system and network protection products as enhancements to their operating systems, generally available in June 2006. Trend Micro Inc. remains the strongest competitor in the Asian anti-virus market and recently entered the U.S. market. F-Secure Corporation, Dr. Ahn s Anti-Virus Lab, Panda Software and Sophos are also showing growth in their respective markets.

Network Protection Market. Our principal competitors in the network protection market are Cisco Systems Inc., Computer Associates International Inc., Internet Security Systems Inc., Juniper Networks, Inc., Symantec Corp., Check Point Software Technologies Ltd. and 3Com Corporation. Qualys, Inc. and Internet Security Systems Inc. are the strongest competitors for our Foundstone products and solutions.

Other Competitors. In addition to competition from large technology companies such as EMC Corp., Hewlett-Packard Co., IBM, Novell Inc. and Microsoft Corp., we also face competition from smaller companies and shareware authors that may develop competing products.

Proprietary Technology

Our success depends significantly upon proprietary software technology. We rely on a combination of patents, trademarks, trade secrets and copyrights to establish and protect proprietary rights to our software. However, these protections may be inadequate or competitors may independently develop technologies or products that are substantially equivalent or superior to our products. Often, we do not obtain signed license agreements from customers who license products from us. In these cases, we include an electronic version of an end-user license in all of our electronically distributed software and a printed license in the box for our products. Since none of these licenses are signed by the licensee, many legal authorities believe that such licenses may not be enforceable under the laws of many states and foreign jurisdictions. In addition, the laws of some foreign countries either do not protect these rights at all or offer only limited protection for these rights. The steps taken by us to protect our proprietary software technology may be inadequate to deter misuse or theft of this technology. For example, we are aware that a substantial number of users of our anti-virus products have not paid any license or support fees to us.

Employees

As of December 31, 2005, we employed approximately 3,290 individuals worldwide. With limited exceptions, none of our employees are represented by a labor union. We consider the relationships with our employees to be positive. Competition for qualified management and technical personnel is intense in the software industry. Our continued success depends in part upon our ability to attract, assimilate and retain qualified personnel. To date, we believe that we have been successful in recruiting qualified employees, but there is no assurance that we will continue to be successful in the future.

Special Note Regarding Forward-Looking Statements in This Report

This Annual Report on Form 10-K contains forward-looking statements that involve risks and uncertainties. All forward-looking statements included in this Report on Form 10-K are based on information available to us on the date hereof. These statements involve known and unknown risks, uncertainties and other factors, which may cause our actual results to differ materially from those implied by the forward-looking statements. Although we believe that the expectations reflected in the forward-looking statements are reasonable, we cannot guarantee future results, levels of activity, performance or achievements. Therefore, actual results may differ materially and adversely from those expressed in any forward-looking statements. Neither we nor any other person can assume responsibility for the accuracy and completeness of forward-looking statements. Important factors that may cause actual results to differ from expectations include, but are not limited to, those discussed in "Risk Factors" beginning immediately hereafter. We undertake no obligation to revise or update publicly any forward-looking statements for any reason.

Table of Contents

These statements include, without limitation, statements regarding our expectations, beliefs, intentions or strategies regarding the future. Forward-looking statements in the Report include, but are not limited to, statements about the following matters:

- future investments in complementary businesses, products and technologies;
- our expectation that our financial results will continue to fluctuate;
- our expectation that international revenue will remain a significant percentage of our net revenue;
- our expectation that both product and pricing competition will increase;
- our expectation that product-related expenses will increase;
- expectations about future sales to our top ten distributors and our sales efforts through the channel and other partners;
- our future dividend policy;
- the expected geographic composition of our future revenues;
- our expected future revenue mix;
- the anticipated future trend of specific categories of expenses;
- the expected future impact of the adoption of Statement of Financial Accounting Standard No. 123R *Share-Based Payment* on our results or operations;
- our expected future level of DSOs; and
- our expected ability to meet our obligations through available cash and internally generated funds, our expectation of generating positive working capital through operations, and our belief as to working capital being sufficient to meet our cash requirements in future periods.

In some cases, you can identify other forward-looking statements in the Report by terminology such as may, will, should, could, expects, plans, anticipates, believes, estimates, predicts, potential, targets, goals, variations of such words, similar expressions, or the negative of these terms or other comparable terminology.

Item 1A. *Risk Factors*

Investing in our common stock involves a high degree of risk. The risks described below are not the only ones facing our company. Additional risks not presently known to us or that we deem immaterial may also impair our business operations. Any of the following risks could materially adversely affect our business, operating results and financial condition and could result in a complete loss of your investment.

Our Financial Results Will Likely Fluctuate, Making It Difficult for Us to Accurately Estimate Operating Results.

Our revenues and operating results have varied significantly in the past. We expect fluctuations in our operating results to continue. Also, we believe that period-to-period comparisons of our financial results should not be relied upon as an indicator of our future results. Our expenses are based in part on our expectations regarding future revenues, making expenses in the short term relatively fixed. We may be unable to adjust our expenses in time to compensate for any unexpected revenue shortfall.

Factors that may cause our revenues, gross margins and operating results to fluctuate significantly from period to period, include, but are not limited to:

- introduction of new products, product upgrades or updates by us or our competitors;

- revenue recognition which may be influenced by volume, size, timing and contractual terms of new licenses and renewals of existing licenses;

the mix of products we sell and services we offer and whether (i) our products are sold directly by us or indirectly through distributors, resellers, ISPs such as AOL, OEMs such as Dell, and others, (ii) the product is hardware or software based and (iii) in the case of software licenses, the licenses are perpetual licenses or time-based subscription licenses;

changes in our supply chains and product delivery channels, which may result in product fulfillment delays;

personnel limitations, which may adversely impact our ability to process the large number of orders that typically occur near the end of a fiscal quarter;

costs or charges related to our acquisitions or dispositions, including our acquisition of Wireless Security Corporation in June 2005 and the dispositions of our McAfee Labs assets;

the components of our revenue that are deferred, including our on-line subscriptions and that portion of our software licenses attributable to support and maintenance;

stock-based compensation expense, which we will begin recognizing for our stock-based compensation plans in the first quarter of 2006;

costs and charges related to certain events, including Sarbanes-Oxley compliance efforts, litigation, relocation of personnel and previous financial restatements;

changes in generally accepted accounting principles;

our ability to effectively manage our operating expense levels; and

factors that lead to substantial declines in estimated values of long-lived assets below their carrying value.

Although a significant portion of our revenue in any quarter comes from previously deferred revenue, a meaningful part of our revenue in any quarter depends on contracts entered into or orders booked and shipped in that quarter. Historically, we have experienced more product orders, and therefore, a higher percentage of revenue shipments, in the last month of a quarter. Some customers believe they can enhance their bargaining power by waiting until the end of a quarter to place their order. Any failure or delay in the closing of new orders in a given quarter could have a material adverse effect on our quarterly operating results. For example, during the fourth quarter of 2005, we failed to meet our previously issued revenue and earnings guidance due in part to incorrect assumptions regarding in-period realization of fourth quarter bookings, a higher proportion of sales involving ratable revenue or multi-year support and more large, multi-product, multi-year enterprise transactions that resulted in lower recognition of up-front revenue. In addition, a significant portion of our revenue is derived from product sales through our distributors. We recognize revenue on products sold by our distributors when distributors sell our products to their customers. To determine our business performance at any point in time or for any given period, we must timely and accurately gather sales information from our distributors information systems at an increased cost to us. Our distributors information systems may be less accurate or reliable than our internal systems. We may be required to expend time and money to ensure that interfaces between our systems and our distributors systems are up to date and effective. As our reliance upon interdependent automated computer systems continues to increase, a disruption in any one of these systems could interrupt the distribution of our products and impact our ability to accurately and timely recognize and report revenue. Further, as we increasingly rely upon third-party manufacturers to manufacture our hardware-based products, our reliance on their ability to provide us with timely and accurate product cost information exposes us to risk. A failure of our third-party manufacturers to provide us with timely and accurate product cost information may impact our costs of goods sold and negatively impact our ability to accurately and timely report revenue.

Because we expect these trends to continue, it is difficult for us to accurately estimate operating results prior to the end of a quarter.

We Face Risks in Connection With the Material Weakness Resulting From Our Sarbanes-Oxley Section 404 Management Report and Any Related Remedial Measures That We Undertake.

In conjunction with (i) our ongoing reporting obligations as a public company and (ii) the requirements of Section 404 of the Sarbanes-Oxley Act that management report as of December 31, 2005 on the effectiveness of our

Table of Contents

internal control over financial reporting and identify any material weaknesses in our internal control over financial reporting, we engaged in a process to document, evaluate and test our internal controls and procedures, including corrections to existing controls and additional controls and procedures that we may implement. As a result of this evaluation and testing process, our management identified a material weakness in our internal control over financial reporting relating to the financial close process. See Item 9A in the Annual Report on Form 10-K for the year ended December 31, 2005 for additional disclosure about the material weakness. In response to the material weakness in our internal control over financial reporting, we have implemented and will continue to implement, additional controls and procedures, including automating many of our controls and financial reporting processes, re-engineering our close process, standardizing our worldwide policies and procedures and continuing to hire accounting and finance personnel where appropriate. In addition, in connection with the settlement of the SEC s formal investigation into our accounting practices, we are required to appoint an independent consultant to conduct a one-time, comprehensive review of our internal accounting and financial reporting controls, among other matters. These efforts could result in increased cost and could divert management attention away from operating our business. As a result of the identified material weakness, even though our management believes that our efforts to remediate and re-test our internal control deficiencies have resulted in the improved operation of our internal control over financial reporting, we cannot be certain that the measures we have taken or we are planning to take will sufficiently and satisfactorily remediate the identified material weakness in full.

In future periods, if the process required by Section 404 of the Sarbanes-Oxley Act reveals further material weaknesses or significant deficiencies, the correction of any such material weakness or significant deficiency could require additional remedial measures which could be costly and time-consuming. In addition, the discovery of further material weaknesses could also require the restatement of prior period operating results. If a material weakness exists as of a future period year-end (including a material weakness identified prior to year-end for which there is an insufficient period of time to evaluate and confirm the effectiveness of the corrections or related new procedures), our management will be unable to report favorably as of such future period year-end to the effectiveness of our control over financial reporting. If we are unable to assert that our internal control over financial reporting is effective in any future period (or if our independent auditors are unable to express an opinion on the effectiveness of our internal controls), or if we continue to experience material weaknesses in our internal control over financial reporting, we could lose investor confidence in the accuracy and completeness of our financial reports, which would have an adverse effect on our stock price and potentially subject us to litigation.

If We Fail to Effectively Upgrade Our Information Technology System, We May Not Be Able to Accurately Report Our Financial Results or Prevent Fraud.

As part of our efforts to continue improving our internal control over financial reporting, we plan to upgrade our existing SAP information technology system during 2006 in order to automate certain controls that are currently performed manually. We may experience difficulties in transitioning to new or upgraded systems, including loss of data and decreases in productivity as personnel become familiar with new systems. In addition, our management information systems will require modification and refinement as we grow and as our business needs change, which could prolong difficulties we experience with systems transitions, and we may not always employ the most effective systems for our purposes. If we experience difficulties in implementing new or upgraded information systems or experience significant system failures, or if we are unable to successfully modify our management information systems and respond to changes in our business needs, our operating results could be harmed or we may fail to meet our reporting obligations. In addition, as a result of the automation of these manual processes, the data produced may cause us to question the accuracy of previously reported financial results.

We Face Risks Related to Our International Operations.

During 2005, net revenue in our operating regions outside of North America represented approximately 42% of our net revenue. We intend to continue our focus on international growth and expect international revenue to remain a significant percentage of our net revenue.

Risks related to international operations include:

longer payment cycles and greater difficulty in collecting accounts receivable;

increased costs and management difficulties related to the growth and operation of our international sales and support organization;

our ability to successfully establish, manage and staff shared service centers for worldwide sales finance and accounting operations centralized from locations in the U.S. and Europe;

our ability to adapt to sales and marketing practices and customer requirements in different cultures;

our ability to successfully localize software products for a significant number of international markets;

compliance with more stringent consumer protection and privacy laws;

currency fluctuations, including weakness of the U.S. dollar relative to other currencies, or the strengthening of the U.S. dollar that may have an adverse impact on revenues, financial results and cash flows and risks related to hedging strategies;

enactment of additional regulations or restrictions on the use, import or export of encryption technologies, which would delay or prevent the acceptance and use of encryption products and public networks for secure communication;

political instability in both established and emerging markets;

tariffs, trade barriers and export restrictions;

a high incidence of software piracy in some countries; and

international labor laws and our relationship with our employees and regional work councils.

We Are Subject to Intense Competition in the System and Network Protection Markets, and We Expect to Face Increased Competition in the Future.

The markets for our products are intensely competitive and we expect both product and pricing competition to increase. As competition increases, we expect increases in our product-related expenses, including increased product rebates, marketing development funds and strategic channel partner revenue-sharing agreements. Some of our competitors have longer operating histories, have more extensive international operations, greater name recognition, larger technical staffs, established relationships with hardware vendors and/or greater financial, technical and marketing resources. We face competition in specific product markets. Principal competitors include:

in the system protection market, which includes our anti-virus and risk assessment and vulnerability management solutions, Symantec Corp., Computer Associates International Inc. and Microsoft Corp. Trend Micro Inc. remains the strongest competitor in the Asian anti-virus market and has recently entered the U.S. market. F-Secure Corporation, Dr. Ahn s Anti-Virus Lab, Panda Software and Sophos are also showing growth in their respective markets; and

in the network protection market, which includes our other intrusion detection and protection products, Cisco Systems Inc., Computer Associates International Inc., Internet Security Systems Inc., Juniper Networks, Inc., Symantec Corp. and 3Com Corporation. Qualys and Internet Security Systems Inc. are the strongest competitors for our Foundstone products and solutions.

Other competitors for our various products could include large technology companies. We also face competition from numerous smaller companies and shareware authors that may develop competing products.

A significant portion of our revenue comes from our consumer business. We will continue to focus on growth in this segment both directly and through relationships with ISPs such as AOL and Comcast, and PC OEMs, such as Dell and Gateway. As competition in this market increases, we may experience pricing pressures from both our competitors and partners which may have a negative effect on our ability to sustain our revenue and market share growth. In addition, as our consumer business becomes more dependent upon the ISP model, our direct on-line revenue may suffer and our retail box business may also continue to decline. Furthermore, as penetration of the consumer anti-virus market through the ISP model increases, this market may become saturated.

Table of Contents

Increasingly, our competitors are large vendors of hardware or operating system software. These competitors are continuously developing or incorporating system and network protection functionality into their products. For example, in the first quarter of 2006 Microsoft announced that it intends to releases its consumer security solution in June 2006 and continues to execute on its announced plans to boost the security functionality of its Windows platform through its acquisition of managed service provider FrontBridge Technologies, anti-virus provider Sybari Software, Inc. and anti-spyware provider GIANT Company Software. Through its acquisitions of Okena, Inc., Riverhead Networks and NetSolv, Cisco Systems Inc. may incorporate functionality that competes with our content filtering and anti-virus products. In addition, Juniper Networks, Inc. acquired Netscreen Technologies.

The widespread inclusion of products that perform the same or similar functions as our products within computer hardware or other companies software products could reduce the perceived need for our products or render our products obsolete and unmarketable. Furthermore, even if these competitors incorporated products are inferior or more limited than our products, customers may elect to accept the incorporated products rather than purchase our products. Or, if our competitors products are offered at significant discounts to our prices or for free, we may be unable to respond competitively, or may have to significantly reduce our prices which would negatively impact our revenue. In addition, the software industry is currently undergoing consolidation as firms seek to offer more extensive suites and broader arrays of software products, as well as integrated software and hardware solutions. This consolidation may negatively impact our competitive position.

We Rely Heavily on Our Intellectual Property Rights Which Offer Only Limited Protection Against Potential Infringers.

We rely on a combination of contractual rights, trademarks, trade secrets, patents and copyrights to establish and protect proprietary rights in our software. However, the steps taken by us to protect our proprietary software may not deter its misuse, theft or misappropriation. Competitors may independently develop technologies or products that are substantially equivalent or superior to our products or that inappropriately incorporate our proprietary technology. We are aware that a substantial number of users of our anti-virus products have not paid any registration or license fees to us. Certain jurisdictions may not provide adequate legal infrastructure for effective protection of our intellectual property rights. Changing legal interpretations of liability for unauthorized use of our software or lessened sensitivity by corporate, government or institutional users to avoiding infringement of intellectual property could also harm our business.

We Face Risks Related to Our Strategic Alliances.

Through our strategic alliances we may from time to time license technology from third parties to integrate or bundle with our products or we may license out our technology for others to integrate or bundle with their products. We may not realize the desired benefits from our strategic alliances on a timely basis or at all. We face a number of risks relating to our strategic alliances, including the following:

Strategic alliances require significant coordination between the parties involved. To be successful, our alliances may require the integration of other companies products with our products, which may involve significant time and expenditure by our technical staff and the technical staff of our strategic allies.

Our agreements with our strategic alliances are terminable without cause with no or minimal notice or penalties. We may expend significant time, money and resources to further relationships with our strategic alliances that are thereafter terminated.

The integration of products from different companies may be more difficult than we anticipate, and the risk of integration difficulties, incompatible products and undetected programming errors or bugs may be higher than that normally associated with new products.

Our sales force and our marketing and professional services personnel may require additional training to market products that result from our strategic alliances. The marketing of these products may require additional sales force efforts and may be more complex than the marketing of our own products.

We may be required to share ownership in technology developed as part of our strategic alliances.

We Face Product Development Risks Associated with Rapid Technological Changes in Our Market.

The markets for our products are highly fragmented and characterized by ongoing technological developments, evolving industry standards and rapid changes in customer requirements. Our success depends on our ability to timely and effectively:

- offer a broad range of network and system protection products;
- enhance existing products and expand product offerings;
- extend security technologies to additional digital devices such as mobile phones and personal digital assistants;
- respond promptly to new customer requirements and industry standards;
- provide frequent, low cost upgrades and updates for our products;
- maintain quality; and
- remain compatible with popular operating systems such as Linux, Windows XP, and Windows NT, and develop products that are compatible with new or otherwise emerging operating systems.

We may experience delays in product development as we have at times in the past. Complex products like ours may contain undetected errors or version compatibility problems, particularly when first released, which could delay or harm market acceptance. The widespread inclusion of products that perform the same or similar functions as our products within the Windows platform could reduce the perceived need for our products. For example, in the first quarter of 2006 Microsoft announced that it intends to release its consumer security solution in June 2006 and continues to execute on its announced plans to boost the security functionality of its Windows platform. Even if these incorporated products are inferior or more limited than our products, customers may elect to accept the incorporated products rather than purchase our products. The occurrence of these events could negatively impact our revenue.

We Face Risks Associated with Past and Future Acquisitions.

We may buy or make investments in complementary companies, products and technologies. For example, in October 2004 we acquired Foundstone to bolster our risk assessment and vulnerability management capabilities and in June 2005 we acquired Wireless Security Corporation to continue to develop their patent-pending technology, to introduce a new consumer wireless security offering, and to integrate the technology into our small business managed solution. We may not realize the anticipated benefits from the Foundstone and Wireless Security Corporation acquisitions.

Integration

Integration of an acquired company or technology is a complex, time consuming and expensive process. The successful integration of an acquisition requires, among other things, that we:

- integrate and retain key management, sales, research and development and other personnel;
- integrate the acquired products into our product offerings both from an engineering and sales and marketing perspective;

integrate and support preexisting supplier, distribution and customer relationships;

coordinate research and development efforts; and

consolidate duplicate facilities and functions and integrate back-office accounting, order processing and support functions.

The geographic distance between the companies, the complexity of the technologies and operations being integrated and the disparate corporate cultures being combined may increase the difficulties of integrating an acquired company or technology. Management s focus on the integration of operations may distract attention from our day-to-day business and may disrupt key research and development, marketing or sales efforts. In addition, it is common in the technology industry for aggressive competitors to attract customers and recruit key employees away from companies during the integration phase of an acquisition.

Internal Controls, Policies and Procedures

Acquired companies or businesses are likely to have different standards, controls, contracts, procedures and policies, making it more difficult to implement and harmonize company-wide financial, accounting, billing, information and other systems.

Open Source Software

Products or technologies acquired by us may include so-called open source software. Open source software is typically licensed for use at no initial charge, but imposes on the user of the open source software certain requirements to license to others both the open source software as well as the software that relates to, or interacts with, the open source software. Our ability to commercialize products or technologies incorporating open source software or otherwise fully realize the anticipated benefits of any such acquisition may be restricted because, among other reasons:

- open source license terms may be ambiguous and may result in unanticipated obligations regarding our products;

- competitors will have improved access to information that may help them develop competitive products;

- open source software cannot be protected under trade secret law;

- it may be difficult for us to accurately determine the developers of the open source code and whether the acquired software infringes third-party intellectual property rights; and

- open source software potentially increases customer support costs because licensees can modify the software and potentially introduce errors.

Use of Cash and Securities

Our available cash and securities may be used to acquire or invest in companies or products, possibly resulting in significant acquisition-related charges to earnings and dilution to our stockholders. For example, in June 2005 we used approximately $20.2 million to acquire Wireless Security Corporation. Moreover, if we acquire a company, we may have to incur or assume that company s liabilities, including liabilities that may not be fully known at the time of acquisition.

We Face Manufacturing, Supply, Inventory, Licensing and Obsolescence Risks Relating to Our Products.

Third-Party Manufacturing

We rely on a small number of third parties to manufacture some of our hardware-based network protection and system protection products. We expect the number of our hardware-based products and our reliance on third-party manufacturers to increase as we continue to expand our portfolio of hardware-based network protection and system protection products. Reliance on third-party manufacturers, including software replicators, involves a number of risks, including the lack of control over the manufacturing process and the potential absence or unavailability of adequate capacity. If any of our third-party manufacturers cannot or will not manufacture our products in required volumes on a cost-effective basis, in a timely manner, at a sufficient level of quality, or at all, we will have to secure additional manufacturing capacity. Even if this additional capacity is available at commercially acceptable terms, the qualification process could be lengthy and could cause interruptions in product shipments. The unexpected loss of any of our manufacturers would be disruptive to our business. Furthermore, supply disruptions or cost increases could increase our costs of goods sold and negatively impact our financial performance. For example, if the price to us of our hardware-based products increased and we were unable to offset the price increase, then the increased cost to us of selling the product could reduce our overall profitability.

Table of Contents

Sourcing

Our products contain critical components supplied by a single or a limited number of third parties. Any significant shortage of components or the failure of the third-party supplier to maintain or enhance these products could lead to cancellations of customer orders or delays in placement of orders.

Third-Party Licenses

Some of our products incorporate software licensed from third parties. We must be able to obtain reasonably priced licenses and successfully integrate this software with our hardware. In addition, some of our products may include open source software. Our ability to commercialize products or technologies incorporating open source software may be restricted because, among other reasons, open source license terms may be ambiguous and may result in unanticipated obligations regarding our products.

Obsolescence

Hardware-based products may face greater obsolescence risks than software products. We could incur losses or other charges in disposing of obsolete inventory.

Product Fulfillment

We typically fulfill delivery of our hardware-based products from centralized distribution centers. We have in the past and may in the future make changes in our product delivery network. Changes in our product delivery network may disrupt our ability to timely and efficiently meet our product delivery commitments, particularly at the end of a quarter. As a result, we may experience increased costs in the short term as temporary delivery solutions are implemented to address unanticipated delays in product delivery. In addition, product delivery delays may negatively impact our ability to recognize revenue if shipments are delayed at the end of a quarter.

False Detection of Viruses and Actual or Perceived Security Breaches Could Adversely Affect Our Business.

Our anti-virus software products have in the past, and these products and our intrusion protection products may at times in the future, falsely detect viruses or computer threats that do not actually exist. These false alarms, while typical in the industry, may impair the perceived reliability of our products and may therefore adversely impact market acceptance of our products. In addition, we have in the past been subject to litigation claiming damages related to a false alarm, and similar claims may be made in the future. An actual or perceived breach of network or computer security at one of our customers, regardless of whether the breach is attributable to our products, could adversely affect the market s perception of our security products.

We Face a Number of Risks Related to Our Product Sales Through Intermediaries.

We sell a significant amount of our products through intermediaries such as distributors, PC OEMs, ISPs and other strategic channel partners, referred to collectively as distributors. Our top ten distributors typically represent approximately 50% to 65% of our net sales in any quarter. We expect this percentage to increase as we continue to focus our sales efforts through the channel and other partners. Our two largest distributors, Ingram Micro Inc. and Tech Data Corp., together accounted for approximately 33% of our net revenue in 2005.

Sale of Competing Products

Our distributors may sell other vendors products that are complementary to, or compete with, our products. While we have instituted programs designed to motivate our distributors to focus on our products, these distributors may give greater priority to products of other suppliers, including competitors. Our ability to meaningfully increase the amount of our products sold through our distributors depend on our ability to adequately and efficiently support these distributors with, among other things, appropriate financial incentives to encourage pre-sales investment and sales tools, such as online sales and technical training as product collateral needed to support their customers and

Table of Contents

prospects. Any failure to properly and efficiently support our distributors may result in our distributors focusing more on our competitors products rather than our products and thus in lost sales opportunities.

Loss of a Distributor

The agreements with our distributors, such as Dell, Ingram Micro Inc., Tech Data Corp. and AOL, are generally terminable by either party without cause with no or minimal notice or penalties. We may expend significant time, money and resources to further relationships with our distributors that are thereafter terminated. If one of our significant distributors terminates its agreement with us, we could experience a significant interruption in the distribution of our products. In addition, our business interests and those of our distributors may diverge over time, which might result in conflict, termination or a reduction in collaboration. For example, our relationship with Internet Security Systems Inc. was terminated following the announcement of our acquisitions in 2003 of Entercept and IntruVert.

Payment Difficulties

Some of our distributors may experience financial difficulties, which could adversely impact our collection of accounts receivable. Our allowance for doubtful accounts was approximately $2.4 million as of December 31, 2005. We regularly review the collectibility and credit-worthiness of our distributors to determine an appropriate allowance for doubtful accounts. Our uncollectible accounts could exceed our current or future allowances.

We Face Risks Related to Customer Outsourcing to System Integrators.

Some of our customers have outsourced the management of their information technology departments to large system integrators. If this trend continues, our established customer relationships could be disrupted and our products could be displaced by alternative system and network protection solutions offered by system integrators. Significant product displacements could impact our revenue and have a material adverse effect on our business.

Critical Personnel May Be Difficult to Attract, Assimilate and Retain.

Our success depends in large part on our ability to attract and retain senior management personnel, as well as technically qualified and highly-skilled sales, consulting, technical, finance and marketing personnel. Other than executive management who have at will employment agreements, our employees are not typically subject to an employment agreement or non-competition agreement. For example, in January 2006, Gene Hodges, our former president, resigned to pursue other opportunities. In the past we have experienced significant turnover in our finance organization worldwide and replacing these personnel remains difficult given the competitive market for these skill sets.

It could be difficult, time consuming and expensive to replace any key management member or other critical personnel. Integrating new management and other key personnel also may be difficult and costly. Changes in management or other critical personnel may be disruptive to our business and might also result in our loss of unique skills and the departure of existing employees and/or customers. It may take significant time to locate, retain and integrate qualified management personnel.

Other personnel related issues that we may encounter include:

Competition for Personnel; Need for Competitive Pay Packages

Competition for qualified individuals in our industry is intense. To attract and retain critical personnel, we believe that we must maintain an open and collaborative work environment. We also believe we need to provide a competitive compensation package, including stock options and restricted stock. Increases in shares available for issuance under our stock option plans require stockholder approval. Institutional stockholders, or our other stockholders, may not approve future requests for option pool increases. For example, at our 2003 annual meeting held in December 2003, our stockholders did not approve a proposed increase in shares available for grant under our employee stock option plans. Additionally, as of January 2006 we are required to include compensation expense in our consolidated statement of income and comprehensive income relating to the issuance of employee stock options. We are currently evaluating our compensation programs and in particular our equity compensation philosophy. In the future, we may decide to issue fewer stock options, possibly impairing our ability to attract and retain necessary personnel. Conversely, issuing a comparable number of stock options could adversely impact our results of operations when compared with periods prior to the effectiveness of these new rules.

Reduced Productivity of New Hires; Senior Management Additions

Notwithstanding our ongoing efforts to reduce our general personnel levels, we continue to hire in key areas and have added a number of new employees in connection with our acquisitions. We have also increased our hiring in Bangalore, India in connection with the relocation of a significant portion of our research and development operations to India.

Several members of our senior management were only added in the last year, and we may add new members to senior management. In January 2005, we hired Eric Brown as our new executive vice president and chief financial officer, in July 2005 we hired Richard Decker as our new senior vice president and chief information officer and in the second quarter of 2005, we promoted William Kerrigan to the position of executive vice president of consumer brands.

For new employees or management additions, there may be reduced levels of productivity as recent additions or hires are trained or otherwise assimilate and adapt to our organization and culture.

Product Liability and Related Claims May Be Asserted Against Us.

Our products are used to protect and manage computer systems and networks that may be critical to organizations. Because of the complexity of the environments in which our products operate, an error, or a false positive, failure or bug in our products, including a security vulnerability, could disrupt or cause damage to the networks of our customers, including disruption of legitimate network traffic by our products. Failure of our products to perform to specifications (including the failure of our products to identify or block a virus), disruption of our customers network traffic or damages to our customers networks caused by our products could result in product liability damage claims by our customers. Our license agreements with our customers typically contain provisions designed to limit our exposure to potential product liability claims. It is possible, however, that the limitation of liability provisions may not be effective under the laws of certain jurisdictions, particularly in circumstances involving unsigned licenses.

Intellectual Property Litigation in the Network and System Security Market Is Common and Can Be Expensive.

Litigation may be necessary to enforce and protect trade secrets, patents and other intellectual property rights that we own. Similarly, we may be required to defend against claimed infringement by others.

In addition to the expense and distractions associated with litigation, adverse determinations could:

- result in the loss of our proprietary rights;
- subject us to significant liabilities, including monetary liabilities;
- require us to seek licenses from third parties; or
- prevent us from manufacturing or selling our products.

The litigation process is subject to inherent uncertainties. We may not prevail in these matters, or we may be unable to obtain licenses with respect to any patents or other intellectual property rights that may be held valid or infringed upon by our products or us.

If we acquire a portion of software included in our products from third parties, our exposure to infringement actions may increase because we must rely upon these third parties as to the origin and ownership of any software being acquired. Similarly, notwithstanding measures taken by our competitors or us to protect our competitors intellectual property, exposure to infringement claims increases if we employ or hire software engineers previously employed by competitors. Further, to the extent we utilize open source software we face risks. For example, the

Table of Contents

scope and requirements of the most common open source software license, the GNU General Public License, or GPL, have not been interpreted in a court of law. Use of GPL software could subject certain portions of our proprietary software to the GPL requirements. Other forms of open source software licensing present license compliance risks, which could result in litigation or loss of the right to use this software.

Computer Hackers May Damage Our Products, Services and Systems.

Due to our high profile in the network and system protection market, we have been a target of computer hackers who have, among other things, created viruses to sabotage or otherwise attack our products and services, including our various websites. For example, we have seen the spread of viruses, or worms, that intentionally delete anti-virus and firewall software. Similarly, hackers may attempt to penetrate our network security and misappropriate proprietary information or cause interruptions of our internal systems and services. Also, a number of websites have been subject to denial of service attacks, where a website is bombarded with information requests eventually causing the website to overload, resulting in a delay or disruption of service. If successful, any of these events could damage users or our computer systems. In addition, since we do not control compact disk, or CD, duplication by distributors or our independent agents, CDs containing our software may be infected with viruses.

Pending or Future Litigation Could Have a Material Adverse Impact on Our Results of Operation and Financial Condition.

In addition to intellectual property litigation, from time to time, we have been subject to other litigation. Where we can make a reasonable estimate of the liability relating to pending litigation and determine that it is probable, we record a related liability. As additional information becomes available, we assess the potential liability and revise estimates as appropriate. However, because of uncertainties relating to litigation, the amount of our estimates could be wrong. In addition to the related cost and use of cash, pending or future litigation could cause the diversion of management s attention and resources.

We Face Risks Related to the Settlement Agreement with the Securities and Exchange Commission.

On February 9, 2006, the United States District Court for the Northern District of California entered a final judgment permanently enjoining us and our officers and agents from future violations of the securities laws. This final judgment resolved the charges filed against us in connection with the SEC s investigation of our financial results. As a result of the judgment, we will forfeit for three years the ability to invoke the safe harbor for forward-looking statements provision of the Private Securities Litigation Reform Act or the Reform Act. This safe harbor provided us enhanced protection from liability related to forward-looking statements if the forward-looking statements were either accompanied by meaningful cautionary statements or were made without actual knowledge that they were false or misleading. While we may still rely on the bespeaks caution doctrine that existed prior to the Reform Act for defenses against securities lawsuits, without the statutory safe harbor, it may be more difficult for us to defend against any such claims. In addition, due to the permanent restraint and injunction against violating applicable securities laws, any future violation of the securities laws would be a violation of a federal court order and potentially subject us to a contempt order. For instance, if, at some point in the future, we were to discover a fact that caused us to restate our financial statements similar to the restatements that were the subject of the SEC action, we could be found to have violated the final judgment. Further, any collateral criminal or civil investigation, proceeding or litigation related to any future violation of the judgment, such as the compliance actions mandated by the judgment, could result in the distraction of management from our day-to-day business and may materially and adversely affect our reputation and results of operations.

We Face Risks Related to Our Anti-Spam and Anti-Spyware Software Products.

Our anti-spam and anti-spyware products may falsely identify emails or programs as unwanted spam or potentially unwanted programs, fail to properly identify unwanted emails or programs, particularly as spam emails or spyware are often designed to circumvent anti-spam or spyware products, or, in the case of our anti-spam products, incorrectly identify legitimate businesses as users of phishing technology. Parties whose emails or programs are blocked by our products, or whose websites are incorrectly identified as utilizing phishing techniques, may seek redress against us for labeling them as spammers or spyware, or for interfering with their business. In

Table of Contents

addition, false identification of emails or programs as unwanted spam or potentially unwanted programs may reduce the adoption of these products.

Cryptography Contained in Our Technology is Subject to Export Restrictions.

Some of our computer security solutions, particularly those incorporating encryption, may be subject to export restrictions. As a result, some products may not be exported to international customers without prior U.S. government approval. The list of products and end users for which export approval is required, and the regulatory policies with respect thereto, are subject to revision by the U.S. government at any time. The cost of compliance with U.S. and international export laws and changes in existing laws could affect our ability to sell certain products in certain markets and could have a material adverse effect on our international revenues.

Our Business Strategy Exposes Us to Significant Risks.

In 2005, we continued executing our business strategy to, among other things, streamline our business, better leverage the McAfee brand, better position us as the leading provider of intrusion prevention solutions, and help accelerate profit and growth. Risks related to these activities include:

- increasing direct competition from larger, more established competitors, such as Microsoft Corp. and Cisco Systems Inc.;
- dependence on our channel and other partners to sell our products;
- business decisions by our competitors may change the dynamics of the market in which we compete; and
- there may be customer confusion around our strategy.

Business Interruptions May Impede Our Operations and the Operations of Our Customers.

We are continually updating or modifying our accounting systems. Modifications of these types of systems are often disruptive to business and may cause us to incur higher costs than we anticipate. Failure to properly manage this process could materially harm our business operations.

In addition, we and our customers face a number of potential business interruption risks that are beyond our respective control. Natural disasters or other events could interrupt our business or the business of our customers, and each of us is reliant on external infrastructure that may be antiquated. Our corporate headquarters are located near a major earthquake fault. The potential impact of a major earthquake on our facilities, infrastructure and overall operations is not known. Despite safety precautions that have been implemented, there is no guarantee that an earthquake would not seriously disturb our entire business process. We are largely uninsured for losses and business disruptions caused by an earthquake and other natural disasters.

Our Stock Price Has Been Volatile and Is Likely to Remain Volatile.

During 2005, our stock price was highly volatile ranging from a per share high of $33.24 to a low of $20.35. On December 30, 2005, our stock s closing price per share price was $27.13. Announcements, business developments, such as a material acquisition or disposition, litigation developments and our ability to meet the expectations of investors with respect to our operating and financial results, may contribute to current and future stock price volatility. In addition, third-party announcements such as those made by our partners and competitors may contribute to current and future stock price volatility. For example, future announcements by Microsoft Corp. related to its consumer security solution may contribute to future volatility in our stock price. Certain types of investors may choose not to invest in stocks with this level of stock price volatility.

We Face the Risk of a Decrease in Our Cash Balances and Losses in Our Investment Portfolio.

Our cash balances are held in numerous locations throughout the world. A portion of our cash is invested in marketable securities as part of our investment portfolio. We rely on third-party money managers to manage our investment portfolio. Among other factors, changes in interest rates, foreign currency fluctuations and macro economic conditions could cause our cash balances to fluctuate and losses in our investment portfolio. Most

Table of Contents

amounts held outside the United States could be repatriated to the United States, but, under current law, would be subject to U.S. federal income tax, less applicable foreign tax credits.

Our Charter Documents and Delaware Law and Our Rights Plan May Impede or Discourage a Takeover, Which Could Lower Our Stock Price.

Our Charter Documents and Delaware Law

Pursuant to our charter, our board of directors has the authority to issue up to 5.0 million shares of preferred stock and to determine the price, rights, preferences, privileges and restrictions, including voting rights, of those shares without any further vote or action by our stockholders. The issuance of preferred stock could have the effect of making it more difficult for a third-party to acquire a majority of our outstanding voting stock.

Our classified board and other provisions of Delaware law and our certificate of incorporation and bylaws, could also delay or make a merger, tender offer or proxy contest involving us more difficult. For example, any stockholder wishing to make a stockholder proposal (including director nominations) at our 2006 annual meeting, must meet the qualifications and follow the procedures specified under both the Exchange Act of 1934 and our bylaws.

Our Rights Plan

Our board of directors has adopted a stockholders rights plan. The rights will become exercisable the tenth day after a person or group announces acquisition of 15% or more of our common stock or announces commencement of a tender or exchange offer the consummation of which would result in ownership by the person or group of 15% or more of our common stock. If the rights become exercisable, the holders of the rights (other than the person acquiring 15% or more of our common stock) will be entitled to acquire in exchange for the rights exercise price, shares of our common stock or shares of any company in which we are merged with a value equal to twice the rights exercise price.

Item 1B. ***Unresolved Staff Comments***

None.

Item 2. ***Properties***

Our worldwide headquarters currently occupy approximately 135,000 square feet in facilities located in Santa Clara, California under leases expiring through 2013. Worldwide, we lease facilities with approximately 900,000 total square feet, with leases that expire at various times. Our primary international facilities are located in Germany, India, Ireland, Japan, the Netherlands, the United Kingdom and Singapore. In the first quarter of 2005, we moved our European headquarters from the Netherlands to a 25,000 square foot facility in Cork, Ireland. Significant domestic sites include California, Oregon and Texas. We believe that our existing facilities are adequate for the present and that additional space will be available as needed.

We own our regional office located in Plano, Texas. The 170,000 square feet facility opened in January 2003 and is located on 15.6 acres of owned land. This facility supports approximately 700 employees working in our customer support, engineering, accounting and finance, information technology, internal audit, legal and telesales groups.

Item 3. ***Legal Proceedings***

Information with respect to this item is incorporated by reference to Note 20 to the notes to consolidated financial statements included in this Form 10-K.

Item 4. ***Submission of Matters to a Vote of Security Holders***

No matters were submitted to a vote of stockholders during the quarter ended December 31, 2005.

PART II

Item 5. *Market for the Registrant s Common Equity and Related Stockholder Matters*

Price Range of Common Stock

In June 2004, we changed our name to McAfee, Inc., and our common stock began trading under the symbol MFE. Our common stock began to trade on the New York Stock Exchange effective February 12, 2002, and traded under the symbol NET from February 12, 2002 until we changed our name to McAfee in June 2004. Prior to February 12, 2002, our common stock traded on the NASDAQ National Market. From December 1, 1997, our common stock traded under the symbol NETA, and prior thereto, under the symbol MCAF.

The following table sets forth, for the period indicated, the high and low sales prices for our common stock for the last eight quarters, all as reported by NYSE. The prices appearing in the table below do not reflect retail mark-up, mark-down or commission.

	High	Low
Year Ended December 31, 2005		
First Quarter	$ 29.15	$ 21.94
Second Quarter	28.71	20.35
Third Quarter	33.24	26.00
Fourth Quarter	32.59	25.35
Year Ended December 31, 2004		
First Quarter	$ 18.90	$ 14.90
Second Quarter	19.75	15.60
Third Quarter	20.42	15.79
Fourth Quarter	33.55	20.09

Dividend Policy

We have not paid any cash dividends since our reorganization into a corporate form in October 1992. We intend to retain future earnings for use in our business and do not anticipate paying cash dividends in the foreseeable future.

Holders of Common Stock

As of January 31, 2006, there were 767 record owners of our common stock.

Common Stock Repurchases

The table below sets forth all repurchases by us of our common stock during the fourth quarter of 2005, all of which were pursuant to a publicly announced plan or program:

	Total Number of	Approximate Dollar Value of Shares

Period	Total Number of Shares Purchased	Average Price Paid per Share		Shares Purchased as Part of Publicly Announced Plan or Repurchase Program	That May yet be Purchased Under Our Stock Repurchase Program	
	(in thousands, except price per share)					
October 1, 2005 through October 31, 2005					$	251,245
November 1, 2005 through November 30, 2005	345	$	27.47	345	$	241,767
December 1, 2005 through December 31, 2005	420	$	27.50	420	$	230,217
Total	765	$	27.49	765		

Table of Contents

In November 2003, our board of directors authorized the repurchase of up to $150.0 million of our common stock in the open market from time to time over the following two years, depending upon market conditions, share price and other factors. In 2003, we purchased 350,000 shares for a total of $4.7 million. In August 2004, our board of directors authorized an additional $200.0 million in stock repurchases over the following two years. In 2004, we purchased approximately 12.6 million shares for a total of $221.8 million. In April 2005, our board of directors authorized the repurchase of an additional $175.0 million of our common stock in the open market from time to time until August 2006. In 2005, we repurchased approximately 2.8 million shares for a total of $68.4 million. As of December 31, 2005, we had authorization from our board of directors to repurchase an additional $230.2 million of our common stock. In February 2006, we repurchased approximately 4.1 million shares for a total of $97.3 million.

Retirements of Common Stock

In 2004, we retired the approximately 13.0 million treasury shares we had repurchased on the open market in 2003 and 2004.

In 1998, we deposited approximately 1.7 million shares of our common stock with a trustee for the benefit of the employees of our Dr. Solomon s acquisition to cover the stock options assumed in our acquisition of this company. These shares, which have been included in our outstanding share balance, were to be issued upon the exercise of stock options by Dr. Solomon s employees. We determined in June 2004 that Dr. Solomon s employees had exercised approximately 1.6 million options, and that we had issued new shares in connection with these exercises rather than using the trust shares to satisfy the option exercises. The trustee returned the 1.6 million shares to us in June 2004, at which time we retired them and they were no longer included in our outstanding share balance. In December 2004, the trustee sold the remaining 133,288 shares in the trust for proceeds of $3.8 million, and remitted the funds to us. The terms of the trust prohibited the trustee from returning the shares to us and stipulated that only employees could benefit from the shares. We distributed these funds to all employees below the level of vice president through a bonus which was recognized as expense in 2004.

Table of Contents

Item 6. *Selected Financial Data*

You should read the following selected financial data with our consolidated financial statements and related notes and Management s Discussion and Analysis of Financial Conditions and Results of Operations . Historical results may not be indicative of future results.

	Years Ended December 31,				
	2005(1)	2004(2)	2003	2002(3)	2001
	(In thousands, except for per share amounts)				
Statement of Operations Data					
Total net revenue	$ 987,299	$ 910,542	$ 936,336	$ 1,043,044	$ 1,071,660
Income from operations	158,129	322,671	64,402	124,028	153,483
Income before provision for income taxes, minority interest and cumulative effect of change in accounting principle	181,534	316,471	73,125	129,933	148,136
Income before cumulative effect of change in accounting principle	138,828	225,065	59,905	128,312	83,253
Cumulative effect of change in accounting principle, net of taxes			10,337		
Net income	138,828	225,065	70,242	128,312	83,253
Income per share, before cumulative effect of change in accounting principle, basic	$ 0.84	$ 1.40	$ 0.37	$ 0.86	$ 0.60
Income per share, before cumulative effect of change in accounting principle, diluted	$ 0.82	$ 1.31	$ 0.36	$ 0.80	$ 0.53
Cumulative effect of change in accounting principle, basic	$	$	$ 0.07	$	$
Cumulative effect of change in accounting principle, diluted	$	$	$ 0.07	$	$
Net income per share, basic	$ 0.84	$ 1.40	$ 0.44	$ 0.86	$ 0.60
Net income per share, diluted	$ 0.82	$ 1.31	$ 0.43	$ 0.80	$ 0.53