AberdeenGroup

The Financial Value of Symantec's Security Solutions

An Executive White Paper

March 2003

Aberdeen Group, Inc.
260 Franklin Street, Suite 1700
Boston, Massachusetts 02110 USA
Telephone: 617 723 7890
Fax: 617 723 7897
www.aberdeen.com

The Financial Impact of Symantec's Security Solutions

Executive Summary

Financial benefit and electronic security for the enterprise are not normally associated with each other. After all, the common wisdom about security, for many people, is that it is believed — a priori — to be decidedly light on benefits and heavy on the cost side of the financial ledger.

However, when electronic security policies, procedures, and products are not deployed and maintained to avoid, mitigate, and prevent disruption to make-the-money missions of an organization, the financial implications become obvious: lost productivity, wages, revenues, and customers, and an impaired brand, among others. Conversely, when policies, people, and security products are appropriately aligned to reinforce business procedures, security products actually automate business productivity that, in turn, empowers higher levels of revenue growth and profit.

The success of any security product is the result of its ability to solve business — not just technology — problems for its buyers. As a result, security products that are appropriately selected, deployed, integrated, and maintained can be a tool for improving revenue while reducing marginal cost for core business operations. Unfortunately, total cost of ownership (TCO) has proven to be inadequate because it only portrays cost without showing the beneficial financial impact of a technology. To truly understand the financial value and impact of any technology — security included — one must analyze its financial components to arrive at a credible return on investment (ROI).

Financial value:

- Return on investment (ROI)
- Internal rate of return (IRR)
- Discounted cash flow (DCF)

Financial value components:

- Revenue impact
- Total cost of ownership (TCO)
- Cost avoidance and reduction

Aberdeen was asked to research the financial value components of some of Symantec's products among its customers. For this research, Aberdeen relied on findings from thousands of previous interviews that were conducted among IT buyers from 2000 through 2002, hundreds of interviews conducted with users of Symantec products during 2001 and 2002, and about fifty additional interviews that were conducted during the fourth quarter of 2002 to verify the currency of existing and prior financial value research findings.

This *Executive White Paper* provides IT buyers with insight into some of the findings that resulted from this primary research project and sheds light on a sorely lacking area of security-related research; namely, the financial value of security. A few of the findings from this research project are contained herein as specific examples that illustrate the financial value of Symantec's security products. Instead

of trying to shoehorn buying decisions based upon fictitious magic quadrants, and hyper-inflated cost-of-ownership numbers, this *White Paper* provides IT buyers with an overview of how to think about the financial value of security by using Symantec's security products as examples.

Symantec's Security Products

During the past year, Symantec acquired a number of best-of-breed security suppliers and technologies that are centered on: (1) separating the problems from the benign; (2) protecting the enterprise's IT infrastructure; and (3) making it possible for IT managers to stay on top of security more cost-effectively. Symantec's new lineup of products and services clearly indicates that it has spread its security wings into complementary areas that were heretofore not available from a single supplier (Table 1).

Symantec's product and service lineup now falls under a new mantra — Alert, Protect, Manage, and Respond — that is used to communicate its value proposition

Table 1: Symantec's Security Product Lineup

Alert	
Symantec DeepSight Threat Management System	Consolidates worldwide security incidents to provide a view of specific threats against an enterprise network, enabling IT to focus.
Symantec Man Trap	Camouflaged deception IDS (honeypot) that captures and traps intruders in decoy networks
Protect	
Symantec Host IDS	Monitors network and user activity against policy, in real-time, using host-based agents
Symantec Man Hunt	High speed detection and correlation of intrusions, using network sensors
Symantec Client Security	Integrated PC-based firewall with intrusion detection and virus prevention
Symantec Gateway Security	Network gateway appliance combining firewall, VPN, anti-virus, IDS, filtering, and scanning
Symantec Enterprise Firewall	Software-based network firewall
Symantec Antivirus	PC-based virus prevention and scanning of malicious code
Manage	
Symantec Incident Manager	Security incident identification, classification, tracking, resolution, and management system
Symantec Enterprise Security Manager (ESM)	Security, policy management, and vulnerability system for use with major IT computing and application systems

Source: Aberdeen Group, March 2003

260 Franklin Street, Suite 1700
Boston, Massachusetts 02110
Telephone: 617 723 7890
Fax: 617 723 7897
www.aberdeen.com

for IT buyers. Symantec's products and services clearly show that it is no longer "just your father's antivirus software supplier." Rather, it is emerging as a leading powerhouse for protecting business operations, revenue, profits, operations, and intellectual property by shielding the electronic infrastructure from security-related problems and events.

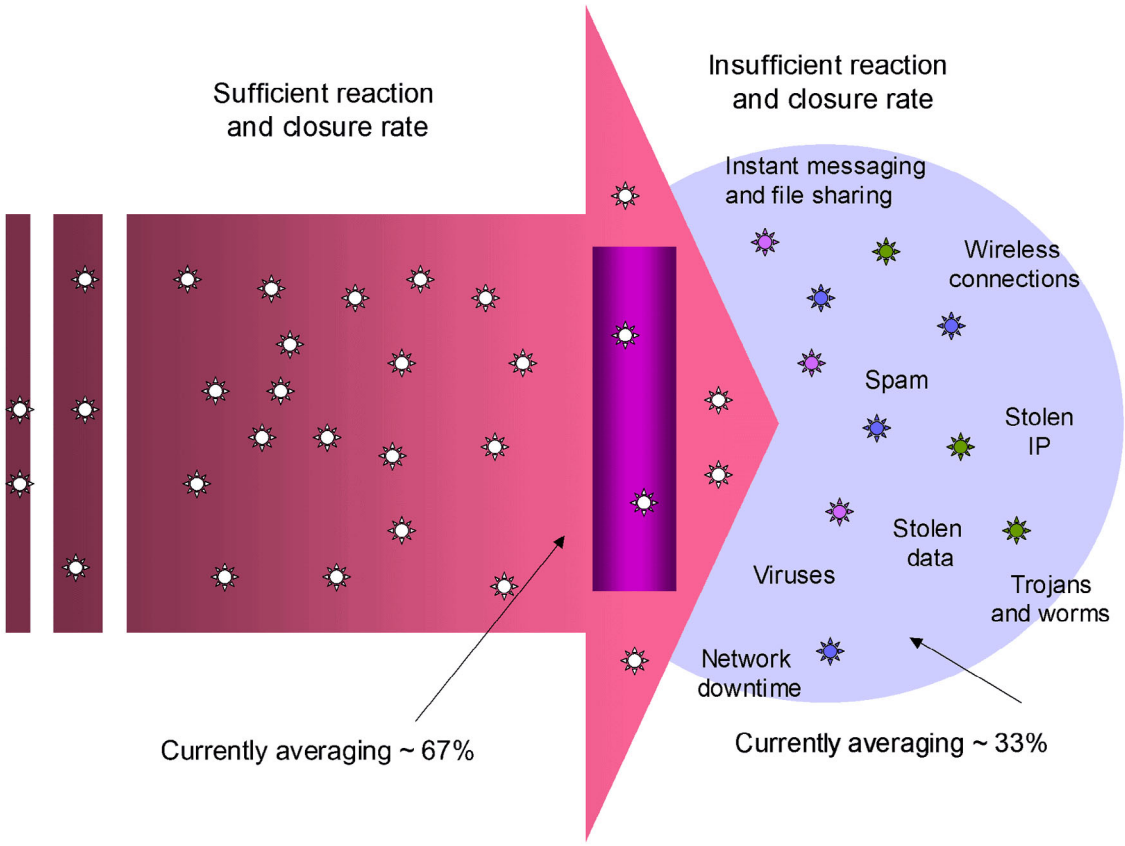
Financial Impact of Symantec's Alerting and Warning Products

Symantec DeepSight Threat Management System

Symantec's solutions for alerting IT about impending danger are unlike common intrusion detection systems that deliver lots of chatter-and-noise and after-the-fact notification. According to its users, the Symantec DeepSight Threat Management System is identifying most threats before they occur and providing IT managers with sufficient time and recommendations to respond (Figure 1).

However, not all of the threat warnings issued by Symantec are acted on and resolved in time by IT managers. Many IT managers report that they are able to

Figure 1: Symantec's Threat Management System at Work



Source: Aberdeen Group, March 2003

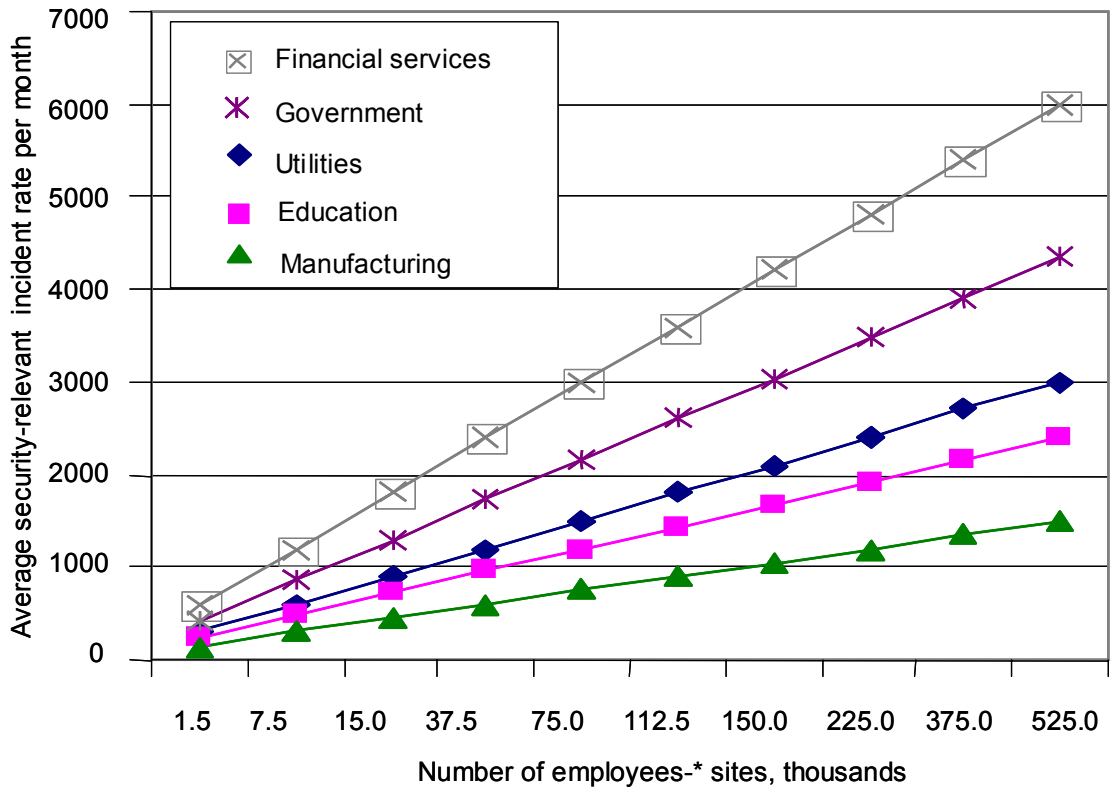
successfully respond to about two-thirds of these warnings — before attacks occur. Conversely, about 33% of the advanced threat warnings issued are not acted on by IT organizations. Despite this, IT managers also say that Symantec's Threat Management System enables them to safely ignore a lot of data that is picked up by their overly-chatty network intrusion detection tools. As a result, IT managers who currently use the Threat Management System say that their next objective is to reorganize IT response teams to take better advantage of all of the early warnings to close the remaining 33% response gap.

Not all industries are equal opportunity targets for security intrusions and events. The unresolved impact of security events differs markedly by firm, size of company, vertical industry, and the complexity of the enterprise's network, which includes the number of independently interconnected sites (Figure 2).

For example, IT managers tell Aberdeen that the damages wrought by security intrusions are spread across a very wide impact-spectrum, including:

- Individual PCs being trashed by new forms of blended threats
- E-mail systems that must be taken down and/or restored

Figure 2: Average Monthly Security Relevant Incidents, By Industry



Source: Aberdeen Group, March 2003

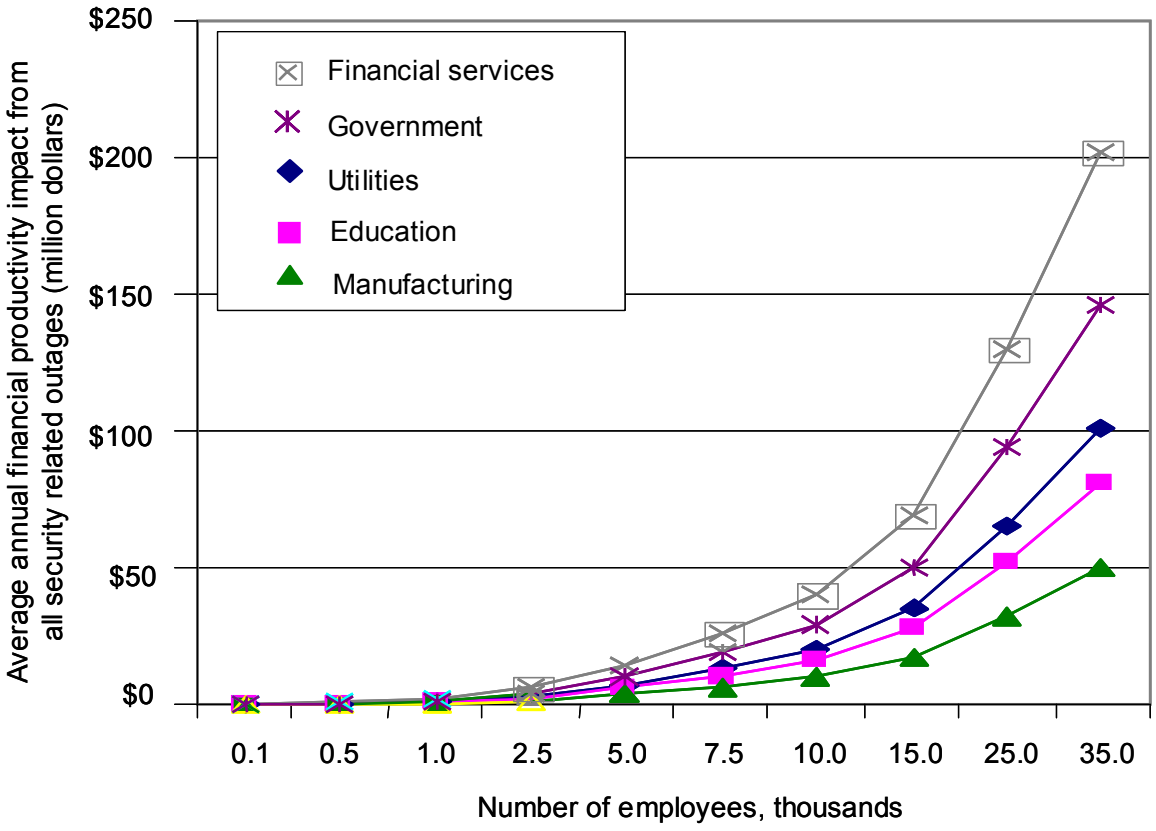
260 Franklin Street, Suite 1700
Boston, Massachusetts 02110
Telephone: 617 723 7890
Fax: 617 723 7897
www.aberdeen.com

- Web sites that are tampered with, defaced, and surreptitiously taken over
- Unauthorized access to confidential information

Firms in financial services, telecommunications, government, and other sectors are at or near the top, whereas firms in agriculture and mining industries are at or near the bottom. As a numbers game, security intrusions that result in actual damage directly affect finances in the form of lost productivity, lost wages, and loss of revenues. As if this were not enough, security intrusions create a double financial-whammy for most firms in the form of added expenses for recovering IT systems, applications and data that are used to service customers (Figure 3).

IT managers interviewed by Aberdeen say that the ability to avoid, respond, and resolve electronic security breaches directly influences the financial results of their

Figure 3: Annual Financial Impact, All Security Related Outages



Source: Aberdeen Group, March 2003

260 Franklin Street, Suite 1700
Boston, Massachusetts 02110
Telephone: 617 723 7890
Fax: 617 723 7897
www.aberdeen.com

organizations. Based on their current experiences with Symantec's Threat Management System, IT buyers say that their ability to respond to about 67% of early security threats delivers a positive financial impact by avoiding impaired revenue and additional costs incurred for recovery. This nearly one-to-one mapping of electronic security threats to financial results is why the early users of the Threat Management System are keen to close the remaining 33% gap.

For example, a firm in the financial services industry with 2,500 employees using Symantec DeepSight Threat Management can realize savings of $57 per user for each dollar of revenue generated by employees. Likewise, a similar-sized manufacturing firm will realize smaller financial benefits; namely, $14 per user for each dollar of revenue generated by employees.

Firms with larger user populations and with larger revenues per employee will realize better results. The data indicate financial savings — though low to start with — increase over time, primarily due to an organization's ability to act on the data being provided by this early warning security threat system. Other methods of valuing the financial impact would also include profit-per-employee in for-profit firms, and budget-per-employee among non-profits and government agencies.

Symantec ManTrap

Symantec ManTrap is an electronic decoy that is used to capture and trap digital intruders from outside or inside an organization, and to prevent these intruders from causing harm. According to customers, the savings realized through the use of ManTrap results from two factors: (1) the reduced rate of unauthorized access to enterprise IT resources, and (2) the avoidance of financial loss associated with unauthorized access to data and computing resources.

Users of ManTrap consistently cite loss prevention rates — between 40% and 85% — that are directly attributed to use of the product.

Enterprises in financial services, utilities, telecommunications, entertainment, and publishing are among those employing electronic resources and data that are more easily converted into cash equivalents. Firms in these industries report that their businesses are more susceptible to electronic theft and they are, therefore, more interested in using ManTrap to avoid financial loss. Likewise, IT buyers in manufacturing, healthcare, and government agencies say that ManTrap is employed to prevent the theft of critical data that can be subsequently converted to a cash equivalent.

ManTrap customers would not identify actual loss rates experienced by their firms, but consistently cite loss prevention rates — between 40% and 85% — that are directly attributed to the use of the product.

260 Franklin Street, Suite 1700
Boston, Massachusetts 02110
Telephone: 617 723 7890
Fax: 617 723 7897
www.aberdeen.com

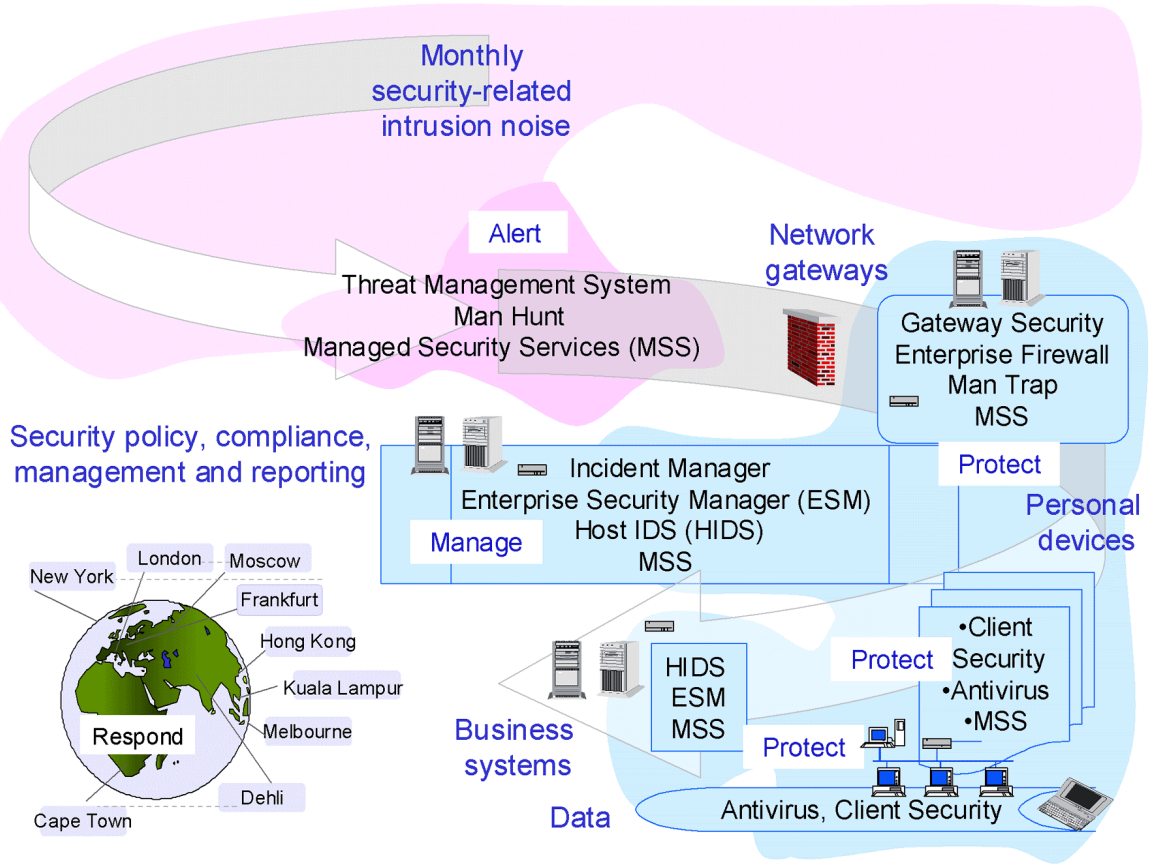
Financial Impact of Symantec's Protection Products

IT managers say that it is unrealistic to expect that any security supplier's products will be prescient about every security threat, 100% of the time, day in and day out. As a result, most IT buyers place a great deal of time and money on deploying and maintaining a variety of electronic security systems that are used to mitigate against threat and risk that cannot always be predicted. Symantec's current product line-up — focused on protecting and managing security threats across the IT infrastructure — includes Host IDS, ManHunt, Client Security, Antivirus, Gateway Security, Firewall, Incident Manager, and Enterprise Security Manager (Figure 4).

Symantec Host IDS

Symantec Host IDS provides IT managers with real-time notification of unauthorized access occurring across a variety of IT systems deployed throughout an

Figure 4: Symantec's Security Products



Source: Aberdeen Group, March 2003

enterprise network. Host IDS monitors and identifies suspicious activity that occurs in software-based business systems, applications, operating systems, e-mail systems, Web sites, and departmental computing resources, among others.

Although the technology underlying Host IDS is different from ManTrap, IT managers using Host IDS share a similar rationale: the ability to obtain notification about unauthorized access to corporate resources. IT managers using Host IDS say that it helps them to avoid financial loss while meeting corporate governance, compliance, and auditing requirements. Organizations characterize the financial value of Host IDS as an aid in reducing financial loss rates, with savings in the range of 50% to 70% loss reductions. For example, the IT decision-makers of one firm interviewed by Aberdeen said that the product enabled them to pinpoint and eliminate an ongoing insider theft-ring that had been siphoning more than $2 million in goods and services each month.

Symantec ManHunt

Symantec ManHunt is a new generation of IT tool that examines high-speed network data for anomalous activity and automatically correlates, aggregates, prioritizes, responds, and notifies IT staff, who can then respond more appropriately. According to IT buyers who use the product, ManHunt automatically reduces a mountain of intrusion data — in real time — to simplify incident management and intrusion prevention. Financially, these IT buyers say that ManHunt enables them to proactively monitor and stay on top of electronic network security-related events that would otherwise take legions of highly-skilled people.

One IT buyer said ManHunt eliminated the need for three IT analysts and $4 million on software development.

A financial return on ManHunt will vary by industry. IT buyers in industries whose assets are more readily exchanged for cash equivalents say the return on ManHunt is usually experienced after about six months, depending on the losses that it prevents. These same buyers say that the product helped them avoid significant costs for staffing and customized software development for analyzing intrusion data. For example, one IT buyer said that the use of ManHunt eliminated the need for three highly-skilled IT analysts and a $4 million software development expense. In addition to tangible financial savings, ManHunt customers also cite intangible benefits that include better control over: (1) intellectual property, (2) design data, (3) improved business cycle times, and (4) lowered costs for work-in-process.

Symantec Client Security and Antivirus

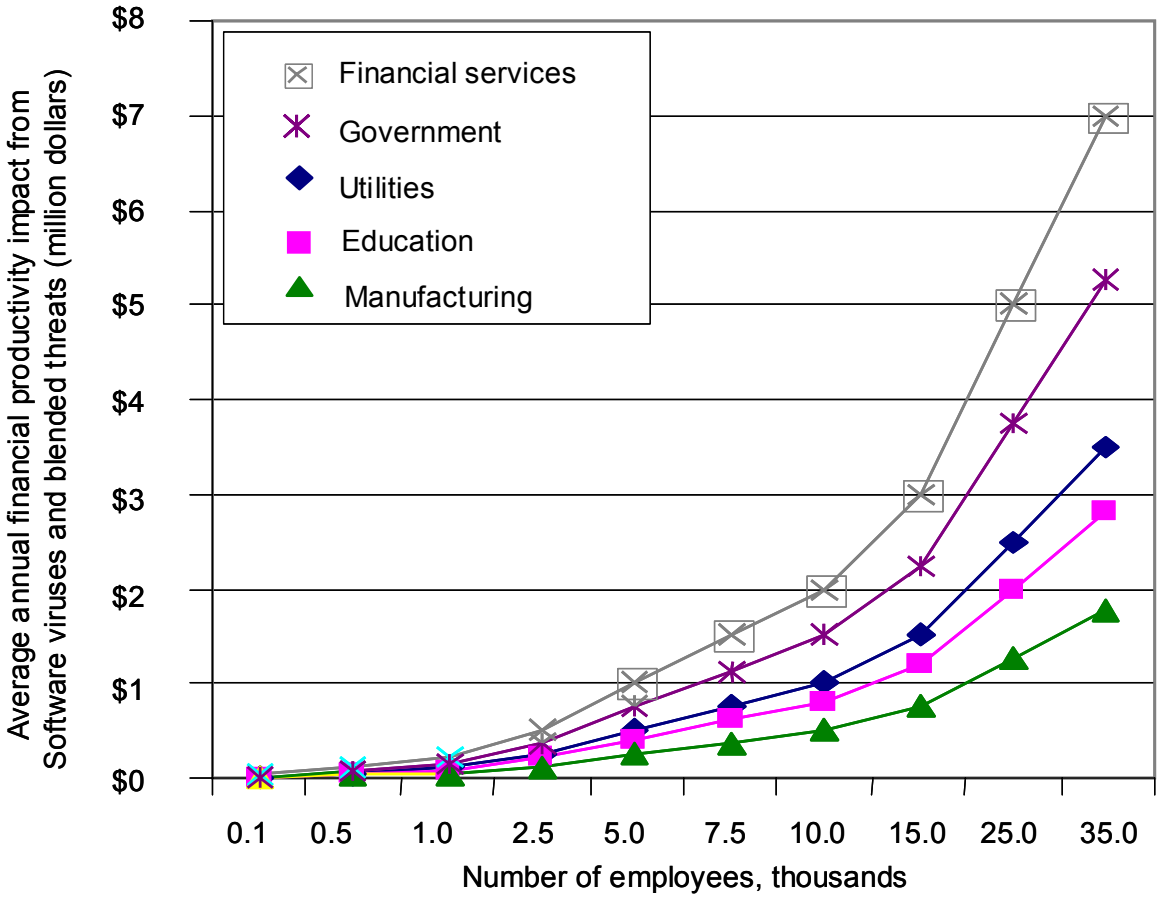
According to senior IT buyers, Symantec Client Security and Antivirus software are deployed to protect and recover PCs, e-mail servers, and departmental systems

260 Franklin Street, Suite 1700
Boston, Massachusetts 02110
Telephone: 617 723 7890
Fax: 617 723 7897
www.aberdeen.com

from software viruses and blended threats, thus reducing business disruption. For some IT buyers, Symantec Antivirus is sufficient to meet their needs. For others, the additional features offered by Symantec Client Security — a built-in firewall with mobile-code blocking, e-mail address privacy blocking, client-based IDS, and a range of other features — is absolutely essential. The integration of these four security capabilities — antivirus, firewall, IDS and filtering — is often cited as a significant reason for using the product.

According to IT managers, annual downtime caused by viruses and blended threats quickly adds up to lost employee productivity. For example, in manufacturing industries the financial loss due to software viruses and blended threats averages $80-per-employee per year in lost productivity. At the high end, the financial services industry averages more than $200 annually per employee due to downtime (Figure 5). In addition to regaining productivity, Symantec is generally credited by its customers with minimizing — and in some cases

Figure 5: Financial Impact of Software Viruses and Blended Threats



Source: Aberdeen Group, March 2003

260 Franklin Street, Suite 1700
Boston, Massachusetts 02110
Telephone: 617 723 7890
Fax: 617 723 7897
www.aberdeen.com

eliminating — recovery costs that are incurred when antivirus software is not deployed or updated.

Symantec Gateway Security and Symantec Enterprise Firewall

Symantec Gateway Security is a blend of multiple security technologies, all rolled-up into an appliance package. This network security appliance delivers the combined capabilities of a network firewall, virtual private network, gateway-based antivirus software, a network intrusion and vulnerability detection scanning engine, and software that filters for nuisance URL and newsgroup traffic. In addition, the Gateway appliance delivers the capability to filter e-mail and Web-based traffic for incoming blended software threats. Load balancing and redundancy capabilities are built into this appliance, which is augmented by alerting, reporting, and centralized administrative capabilities.

The Enterprise Firewall differs from the Gateway in two ways. First, the product is delivered as software that can be deployed on a variety of network servers. Second, compared with the Swiss Army-like capabilities of the Gateway, the Enterprise Firewall contains only firewall, VPN software, reporting, and centralized management software.

The financial savings realized from Symantec Gateway range from $10,000 to more than $2.5 million.

The financial savings realized by IT buyers who are using the Symantec Gateway appliance differs by industry, ranging from a low of $10,000 annually to a reported high that topped more than $2.5 million annually. Most of the savings comes from reductions (and redirections) of IT staff needed to deploy, maintain, and update these necessary guardians of the enterprise network. In addition to staff reductions and redirection onto more important projects, the other significant factor cited by IT buyers is the ability to deploy new security technologies without the overhead associated with having to purchase, deploy, and maintain different products from multiple suppliers.

According to some IT buyers, staff increases — that would have been required to maintain and manage security products from multiple suppliers — are avoided and generally offsets increases coming from staff reassignments. An additional financial benefit — reduced telecommunication costs — is cited by the IT buyers who use VPN capabilities that are embedded in these two products. IT buyers using the Internet for a variety of business purposes — remotely connecting employees, replacing private networks for automated teller machines, connecting remote operating sites with headquarters, etc. — say that, on average, their telecommunication expenses are reduced by 20% per month. This savings is consistent across industries and occurs after the products support mainstream organizational processes.

260 Franklin Street, Suite 1700
Boston, Massachusetts 02110
Telephone: 617 723 7890
Fax: 617 723 7897
www.aberdeen.com

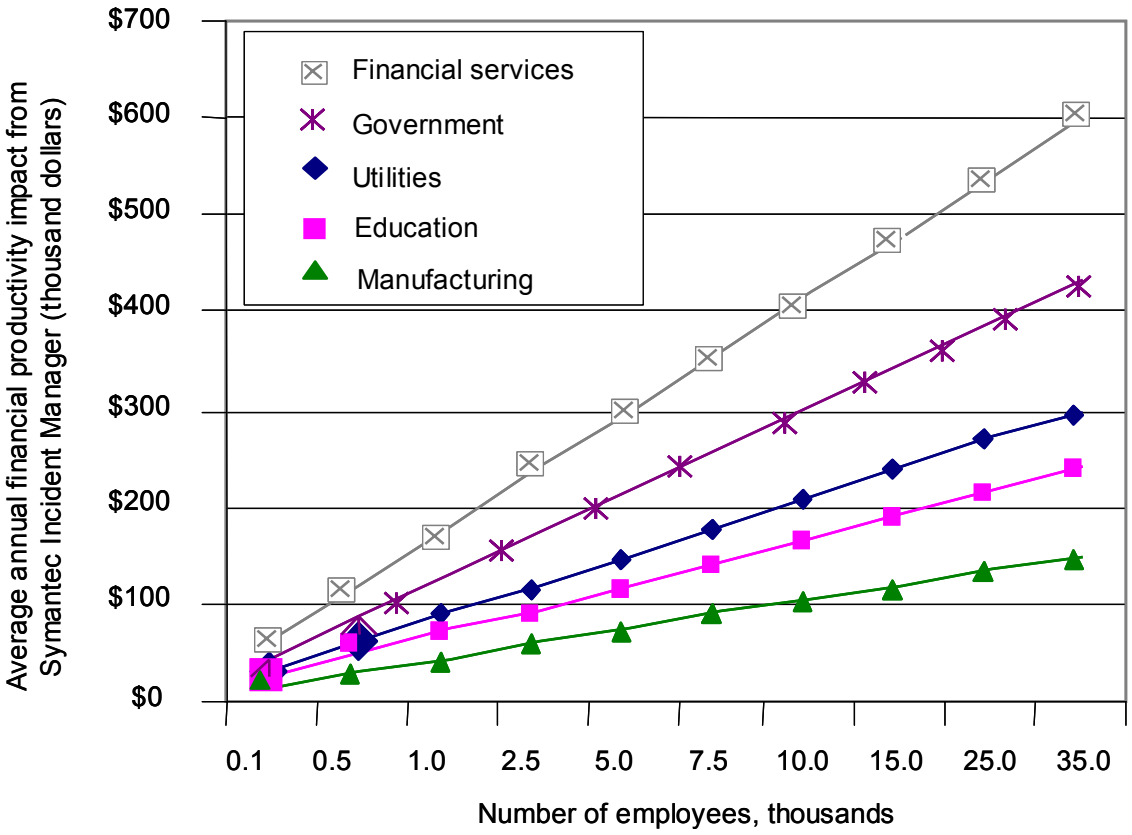
Financial Impact of Symantec's Management Products

At the heart of Symantec's security solutions are its two flagship security management products, Incident Manager and Enterprise Security Manager (ESM). Both of these products are similar in that they automate security processes that would otherwise take an army of administrators to manage. However, the products differ in their focus: Incident Manager focuses on automating the process of managing security incidents throughout their life cycle; ESM automates security policy, vulnerability assessment and configuration management tasks used to comply with company best-practices and industry-specific security policies.

Symantec Incident Manager

Incident Manager delivers immediate financial relief by eliminating costs from staff build-out. According to its customers, the financial impact of Incident Manager includes an average savings of more than two hours of IT staff time per security incident — by eliminating time spent on investigation, research, correlation, prioritization, and life-cycle tracking (Figure 6).

Figure 6: Annual Financial Impact of Symantec Incident Manager



Source: Aberdeen Group, March 2003

260 Franklin Street, Suite 1700
Boston, Massachusetts 02110
Telephone: 617 723 7890
Fax: 617 723 7897
www.aberdeen.com

Incident Manager is credited with this financial benefit by automating the correlation of seemingly unrelated security events into incidents that are worthy of human attention, and then by tracking these incidents to resolution. In addition, savings also result from IT staff not spending time on the false-positive incidents that detract from available staff time to investigate real problems. For example, IT managers in financial service industries cite financial savings that range from more than about $60,000 to about $6 million per year, whereas savings in manufacturing firms range from more than about $15,000 to about $1.5 million per year. Of course, financial savings depend on a number of factors, including the incident rate, the vertical industry, the complexity of the IT environment, the number of networked connections maintained by the enterprise, and the proficiency of IT administrators and security staff.

Moreover, the financial return on Incident Manager depends on how many data feeds are connected with it: more input results in faster returns. For example, the product's interaction with Symantec DeepSight Threat Management provides a continually updated database of security vulnerabilities from external sources, including CERT, SANS, and others. In addition, organizations using the product with internal incident data sources — such as ESM for IT systems and third-party software product vulnerability logs — report faster returns.

Symantec Enterprise Security Manager

Symantec ESM is an automated security policy compliance and vulnerability assessment tool. It delivers a combination of industry-specific security and compliance policies — ISO 17799, GLBA, and HIPAA — with an automated process that continually checks for vulnerabilities within a variety of applications, databases, firewalls, software operating environments, departmental servers, and PCs. Working in tandem with most other Symantec security products, ESM also takes feeds from Symantec's Security Response centers, providing integrity-checks to determine whether or not something has changed in a specific IT system.

Enterprise Security Manager duplicates the work of one IT staff member for every 100 computing platforms in the enterprise.

IT buyers say the impetus for purchasing and deploying Enterprise Security Manager comes from a number of factors, including meeting compliance and audit requirements, as well as direction from senior managers. According to its customers, the financial impact of ESM averages a ten-fold reduction in the time needed to check, verify, and correct security configurations against policy. For example, in the past, organizations with 100 systems platforms that are checked for vulnerabilities and conformance to policy spent more than 2,000 staff hours annually prior to using ESM. These same firms now spend a little more than 240 hours when using ESM.

In effect, ESM is replacing the workload of one IT staff member for every 100 computing platforms in the enterprise. Based on customer experiences, the intangible benefit of ESM is that it enables their firm to better document compliance while using fewer — and less-skilled — staff resources.

Financial Impact of Symantec's Managed Security Services

In addition to its security products that are licensed by customers, Symantec also delivers security alerting, protection, and management over the Internet through a number of managed security services (MSS). These services include Symantec Managed Firewall Service, Managed Intrusion Detection and Response Service, Managed Internet Vulnerability Assessment Service, Managed Security Policy Compliance Service, and Managed Virus Protection Service, among others.

IT buyers interviewed by Aberdeen state that although they generally pay more for MSS over a licensed product, the price of MSS is usually less than the total cost of ownership for the equivalent combination of products, including the cost of hiring staff to deploy and maintain security for the enterprise. Few, if any, of the IT buyers that Aberdeen interviewed are purchasing MSS to cover all of their security needs. Rather, most of them appear to be augmenting internally maintained security products with MSS to meet all of their overall requirements. For some IT buyers, the incentive to purchase MSS is higher when using it for more mature, well-understood security technologies. For others, MSS provide an opportunity to inexpensively learn about the benefits of new security technologies without having to make major financial commitments.

The most common and salient financial reason cited by IT buyers for purchasing MSS: It improves cash flow. By offloading one-time and ongoing staff expenses to MSS, IT managers are finding:

The most common financial reason cited by IT buyers for purchasing security as a managed service: It improves cash flow.

- Better financial control due to predictable cash flow and budgeting
- Improved financial flexibility for reacting to general and administrative budget change
- The ability to offload needed security to experts
- The ability to stay on top of changing security threats and technologies

Aberdeen Conclusions

The success of any security product is the result of its ability to solve business — not just technology — problems for its buyers. As a result, security products — appropriately selected, deployed, integrated, and maintained — are a tool for improving revenue while reducing marginal cost for core business operations. Unfortunately, the overuse of TCO is an inadequate metric for making decisions

260 Franklin Street, Suite 1700
Boston, Massachusetts 02110
Telephone: 617 723 7890
Fax: 617 723 7897
www.aberdeen.com

about technology purchases, because TCO only portrays cost without showing the beneficial financial impact of a technology. To truly understand the impact of any technology — security included — one must analyze its ROI. Unfortunately, few IT organizations can dedicate the staff and systems needed to arrive at "the five-nines of ROI."

Despite this inability — and the lack of staff — to accurately measure financial performance to the last penny, most IT managers can quantify staffing levels, time spent on specific activities, and costs that are avoided. Likewise, IT managers can easily and anonymously identify lost productivity and revenue, as well as impaired good will. This *White Paper* provides some insight into the financial value of Symantec's security products and services. However, by itself, this report cannot cover every industry, enterprise, and IT buyer's specific environment. However, it does provide a framework for thinking about the financial value of Symantec's security products and services.

According to its users, Symantec's products are delivering financial value.

It should be noted that the actual financial impact of any of Symantec's products will differ, based on a number of factors. Furthermore, financial benefits that result from staff reductions may not be fully realized, as some IT staff is reassigned to other more important projects. Nevertheless, according to its customers, Symantec's products are delivering financial value, including improved revenue, improved cash flow, better productivity, downstream cost avoidance, and cost reduction, among others. Beyond the financial benefits and values of specific security products and services provided by Symantec, IT buyers say that Symantec's ability to deliver multiple security technologies is a considerable intangible when looking to protect the enterprises electronic infrastructure in a financially prudent manner.

Aberdeen Group, Inc.
260 Franklin Street, Suite 1700
Boston, Massachusetts
02110-3112
USA

Telephone: 617 723 7890
Fax: 617 723 7897
www.aberdeen.com

Aberdeen Group is a computer and communications research and consulting organization closely monitoring enterprise-user needs, technological changes and market developments.

Based on a comprehensive analytical framework, Aberdeen provides fresh insights into the future of computing and networking and the implications for users and the industry.

Aberdeen Group performs projects for a select group of domestic and international clients requiring strategic and tactical advice and hard answers on how to manage computer and communications technology. This document is the result of research performed by Aberdeen Group, which was underwritten by Symantec. Aberdeen Group believes its findings are objective and represent the best analysis available at the time of publication.

To provide us with your feedback on this research, please go to www.aberdeen.com/feedback.