



Confidence in a connected world.

## **Symantec™ Endpoint Protection 11.0—Value Delivery Research Study**

Proving how integrated endpoint security management can lower operating costs and reduce security risk at small, midsize, and large organizations

# Symantec Endpoint Protection 11.0—Value Delivery Research Study

## Contents

<b>Executive summary</b> . . . . .	4
About Symantec Endpoint Protection 11.0 . . . . .	4
The Value Delivery Research study . . . . .	4
Key findings . . . . .	4
<b>Understanding the true value of an integrated approach to endpoint security</b> . . . . .	5
<b>About Symantec Endpoint Protection 11.0</b> . . . . .	6
<b>Results overview</b> . . . . .	7
<b>Methodology and demographics</b> . . . . .	10
<b>Detailed results—large customers</b> . . . . .	10
State government . . . . .	10
<i>About the organization</i> . . . . .	11
<i>Security challenges</i> . . . . .	12
Large county government . . . . .	13
<i>About the organization</i> . . . . .	13
<i>Security challenges</i> . . . . .	13
<b>Detailed results—small and midsize customers</b> . . . . .	14
High-tech solution provider . . . . .	14
<i>About the organization</i> . . . . .	14
<i>Security challenges</i> . . . . .	15

**Contents** *(cont'd)*

Regional bank ..... 16

*About the organization*..... 16

*Security challenges* ..... 17

Professional union ..... 19

*About the organization*..... 19

*Security challenges* ..... 19

Landscaping service provider ..... 20

*About the organization*..... 20

*Security challenges* ..... 21

Healthcare provider ..... 21

*About the organization*..... 21

*Security challenges* ..... 22

**Conclusion** ..... **23**

**For more information**..... **23**

**About Symantec** ..... **24**

## Executive summary

### About Symantec Endpoint Protection 11.0

Symantec Endpoint Protection 11.0 is an integrated security application that provides a centralized solution for organization-wide endpoint management. It integrates antivirus, antispyware, desktop firewall, intrusion prevention, device and application control, and optional network access control capabilities. It lets IT security managers monitor and protect all critical endpoints—including desktops, laptops, and servers—from a single, easy-to-use management console.

### The Value Delivery Research study

The Alchemy Solutions Group, a leading global services consulting firm, designed the Value Delivery Research (VDR) study to show that Symantec Endpoint Protection 11.0 can deliver substantial cost and performance benefits to businesses of different sizes and in a wide variety of security-conscious industries. Working closely with Symantec, the Alchemy team identified seven qualified Symantec customers with end-user populations ranging from 170 to 30,000. Industries represented were broad, including healthcare, financial services, the public sector, and others.

The next step was a series of detailed interviews with each organization to better understand their IT security operations, spending patterns, and management challenges. After the first round of interviews, all participating customers installed a beta version of Symantec Endpoint Protection 11.0. Following the evaluation period, Alchemy worked closely with each customer to project the total operational and economic impact (TOEI) of Symantec Endpoint Protection 11.0 based on an organization-wide implementation.

### Key findings

All customers, regardless of industry and size, anticipated that Symantec Endpoint Protection 11.0 would deliver significantly lower security administration costs while helping them transition from reactive to proactive security. Participants' projected annual TOEI varied from \$24,000 to \$5.3 million, with average savings across all participants of over \$280 per end user. In-depth discussions identified additional value associated with Symantec Endpoint Protection 11.0 advanced technologies.

Projected annual total operation and economic impact varied from \$24,000 to \$5.3 million, with average savings across all participants of over \$280 per end user.

Highlights include:

- Centralized security management through the Symantec Endpoint Protection 11.0 console could potentially reduce management hours by approximately 75 percent.
- Automated user and account administration makes it significantly easier to add, remove, and update user security profiles.
- Device control capabilities help IT security operations more rapidly detect and secure unprotected devices such as USB thumb drives and other peripheral components.
- Proactive endpoint monitoring combined with device control lets businesses detect and contain threats before significant damage is done.
- The client user interface allows end users to perform basic support functions themselves. For some organizations, this feature could dramatically reduce help desk calls relating to antivirus and antispymware issues.
- Taken together, all these capabilities can help organizations operationalize endpoint security by making basic day-to-day activities more simple, streamlined, automated, and measurable. This, in turn, makes it easier for security to work with IT risk management and address critical issues, such as preventing data loss.

Centralized security management through the Symantec Endpoint Protection 11.0 console could potentially reduce management hours by approximately 75 percent.

## **Understanding the true value of an integrated approach to endpoint security**

Most IT organizations today rely on fragmented endpoint security measures. Different types of security software may run on desktops, laptops, and servers. Antivirus, antispymware, network threat protection, and proactive threat protection may be managed independently at different locations. This piecemeal approach often leads to higher administrative costs. It can also mean increased risk as hackers develop new tactics to gain unauthorized and undetected access to an organization's systems and information with blended threats.

To address threats more proactively and be more cost-effective, a growing number of businesses are developing a structured approach to endpoint security that integrates all types of endpoints in a single, centralized management framework. Symantec Endpoint Protection 11.0 is the first solution to provide a fully automated environment for centralized endpoint security management via a single agent. It allows businesses to manage endpoints of all types and control access to applications from a single console—regardless of location. Initial analysis suggests that

Symantec Endpoint Protection 11.0 could help organizations of all sizes dramatically reduce IT administration costs associated with security while significantly reducing security risks.

The VDR study proves that Symantec Endpoint Protection 11.0 delivers these benefits and more.

Symantec Endpoint Protection 11.0 is the first solution to provide a fully automated environment for centralized endpoint security management.

### **About Symantec Endpoint Protection 11.0**

Symantec Endpoint Protection 11.0 is designed to help businesses implement proactive security management by providing a comprehensive and multilayered approach to endpoint protection. It combines industry-leading antivirus capabilities with advanced threat prevention to deliver unmatched defense against malware for laptops, desktops, and servers. It even protects against sophisticated attacks—such as rootkits, zero-day attacks, and mutating spyware—that evade traditional security measures. And it offers a single integrated agent and a single console for managing all endpoints.

Symantec Endpoint Protection 11.0 seamlessly combines best-of-breed protection mechanisms into a single solution to deliver the highest level of comprehensive endpoint security. It integrates:

- **Antivirus/Antispyware.** Symantec Endpoint Protection 11.0 provides the industry-leading antivirus and antispyware protection of Symantec AntiVirus. Since 1999 Symantec is the only vendor to obtain more than 35 consecutive VB100 awards. In a February 2007 test study conducted by AV-Comparatives, of 15 antivirus solutions tested for polymorphic threats, only Symantec and one other vendor received a score of 100 percent in all categories. Symantec is also a leader in the detection and removal of rootkits—stealth applications or scripts that a hacker uses to gain an undetectable presence on a system as well as administrator-level access to that system.
- **Network threat protection.** Network threat protection on endpoints is critical to protect them from blended threats and to inhibit outbreaks. Symantec Endpoint Protection 11.0 offers comprehensive network protection, including a desktop firewall as well as a blend of state-of-the-art protection technologies, such as intrusion prevention and sophisticated capabilities to control network communications.

- **Proactive threat protection.** While signature-based file scanning and network scanning technologies cover key areas of necessary protection, nonsignature-based technologies are needed to address the growing number of unknown threats used in stealth attacks. Symantec Endpoint Protection 11.0 includes TruScan™ proactive threat scan technology, which protects against the multitude of variant and yet-to-be-seen threats that exploit known and unknown vulnerabilities. It also incorporates device and application control capabilities that allow administrators to deny specific device and application activities deemed as high-risk.
- **Network Access Control option.** Through seamless integration with Symantec™ Network Access Control, it provides a centralized way of ensuring that endpoints comply with the corporate security policy before gaining access to the network, eliminating the need to deploy additional Network Access Control software on an organization's endpoint devices.

Customers reported significant improvements in endpoint security and lower attack-related risks.

By offering multiple endpoint security technologies in a single agent, Symantec Endpoint Protection 11.0 enables organizations to reduce administrative overhead and the costs associated with managing multiple endpoint security products. It also leverages existing IT investments, such as software deployment tools, patch management tools, SIM tools, databases, and operating systems, leading to lower total cost of ownership (TCO)—all while providing proactive security that minimizes the potential impact of unexpected attacks.

## Results overview

The Symantec Endpoint Protection 11.0 VDR project looked at how Symantec Endpoint Protection 11.0 could benefit seven Symantec customers participating in this Symantec Endpoint Protection 11.0 beta program. Overall, the study concluded that the operational and economic impact to the IT security of these organizations will be immediate and significant. In most instances, the current effort required to manage endpoint security will be reduced across the board by 75 percent and for some application areas will be completely eliminated. At the same time, customers also reported significant improvements in endpoint security and lower attack-related risks. The focus of this study was Symantec Endpoint Protection; this study did not measure Symantec Network Access Control TOEI savings by customers.

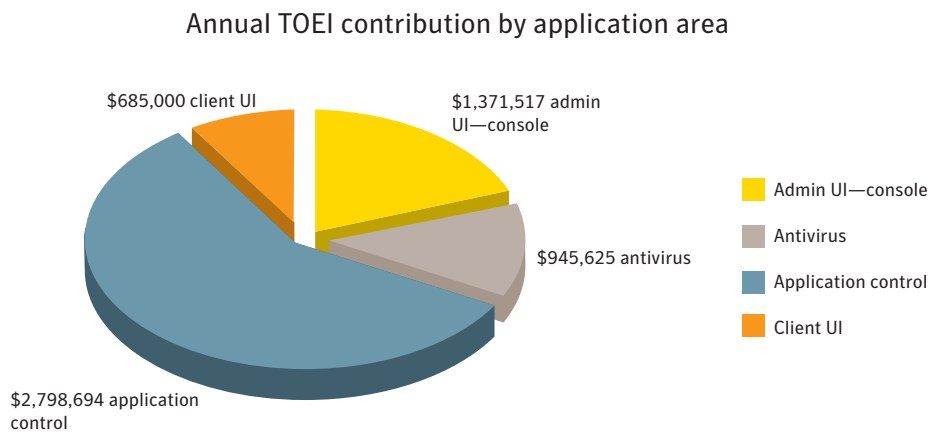
On the next page is a table that summarizes benefits of Symantec Endpoint Protection 11.0 by feature.

**Table 1. Symantec Endpoint Protection 11.0 value by feature (as defined by the customer)**

<b>Feature</b>	<b>Value</b>
Client user interface	Several participating beta customers found that calls to the IT help desk could be reduced by up to 65 percent because of Symantec Endpoint Protection 11.0 features. With over 80 percent of IT support calls logged by the IT help desk related to antivirus and antispymware issues, allowing end users to perform some support tasks themselves could offer significant cost and labor savings for certain organizations.
Antispymware, antivirus, and desktop firewall	Centralized security management through the Symantec Endpoint Protection 11.0 console could potentially reduce management hours by approximately 75 percent. Also, the automatic deployment of antispymware, antivirus, and desktop firewall software and updates will drastically reduce the threats currently experienced by these customers.
Device control	Symantec Endpoint Protection 11.0 can prevent sensitive information from being downloaded to storage devices such as USB sticks, protecting the company from the risk associated with losing sensitive data and also protecting the systems from the risk of introducing malicious code from externally connected peripherals.
Application control	End users tend to install applications that undermine the performance of the network, such as Skype, Kazaa (peer-to-peer file sharing), or iTunes (music downloads). These applications impact network performance, causing general slowdowns. Symantec Endpoint Protection 11.0 can help IT security operations maintain control over the applications that are installed on end-user systems.
Admin user interface (UI)—threat monitoring	The Symantec Endpoint Protection 11.0 graphical user interface greatly simplifies the process of monitoring possible threats. For antivirus issues, it simplifies the process of identifying and classifying potential workstation-based threats, prioritizing the threat, and dispatching the recovery against that threat.  On the network, firewall, and IDS side, reviewing daily and hourly reports allows visibility into unusual activity at the endpoint. This allows immediate detection and prevention of potential network intrusions and data loss. Threat monitoring combined with device control allows IT departments to deal with potential threats and security issues on a timely, proactive basis instead of dealing with the negative impact after the fact.
Admin UI—report generation	For most IT departments, generating reports on network security is a manual and time-consuming process. Symantec Endpoint Protection 11.0 can automatically produce a wide variety of security reports, which not only provides visibility into unusual activity at the endpoint, but it also helps businesses meet auditing and compliance requirements associated with regulations, such as SOX, GLBA, HIPAA, etc.
Admin UI—creating accounts and roles-based administration	Symantec Endpoint Protection 11.0 can create, deploy, and update accounts and security policies. This is done at the console and does not involve traveling to the user location. The procedure using Symantec Endpoint Protection 11.0 is performed in the background and deployed in real time. When end users change jobs or roles within the organization, the changes needed to update end users and their access rights can be performed right at the console, saving thousands of hours for these organizations.



The figure below shows annual aggregate TOEI for all participating customers according to Symantec Endpoint Protection 11.0 feature.



**Figure 1. Customer estimates of annual TOEI by feature**

The following table shows estimated TOEI for each participating customer.

**Table 2. Symantec Endpoint Protection 11.0 value by customer**

Customer	Number of end users	Projected savings for Symantec Endpoint Protection 11.0 from 2007–08
High-tech solution provider	1,100	\$5.3 million
State government	30,000	More than \$3.4 million
Regional bank	1,500	\$2.0 million
Landscaping service provider	1,550	More than \$325,000
Professional union	300	\$315,000
Large county government	6,000	Approximately \$300,000
Healthcare service provider	170	More than \$24,000

## Methodology and demographics

The Symantec Endpoint Protection 11.0 VDR study was designed to compare the endpoint security challenges that organizations faced before trying a beta version of Symantec Endpoint Protection 11.0 with their experiences afterwards. The study was also structured to estimate potential operational savings associated with each key feature of Symantec Endpoint Protection 11.0. Alchemy and Symantec agreed to quantify these savings as the total operational and economic impact (TOEI) of Symantec Endpoint Protection 11.0.

Alchemy began the study by working with Symantec to identify 40 potential customers that could benefit from testing Symantec Endpoint Protection 11.0. To qualify for the study, which would include access to Symantec Endpoint Protection 11.0 beta software and support from Symantec, customers had to agree to:

- Provide resources to participate in two interviews ranging from four to six hours each
- Install and extensively test the beta software immediately upon release
- Make technical and business resources available throughout the process
- Share with Symantec and Alchemy the potential TOEI impact that Symantec Endpoint Protection 11.0 would have on their respective organizations

After preliminary discussions with 40 customers, Alchemy identified seven with the time and resources available to participate. At these organizations, end user counts ranged from 170 to 30,000, and remote support locations varied from two to more than 100 globally.

In addition, participating customers' IT support organizations had differing levels of size, sophistication, and familiarity with Symantec data availability and security products. In each case, the tactical level fire-fighting required to maintain adequate service levels was extremely labor-intensive, with little or no automation to help manage the complexities of endpoint security.

Participating customers have from 170 to 30,000 end users and from 2 to 100 remote support locations.

## Detailed results—large customers

Of the seven participating customers, two qualified as large organizations, with end-user communities of 30,000 and 6,000 respectively.

### State government

#### *About the organization*

This state government organization supports more than 100 state government agencies. Its IT organization has 1,000 employees. This number includes a staff of 300 in the centralized corporate IT functions and 700 staff members working at the divisional or other department levels. A total of 400 of these staff members—or an average of three people per agency—are focused on security functions. This organization supports 30,000 end users with a wide variety of skills and specific functions, working at all state executive-level offices and all state-funded agencies as well as hospitals, libraries, and other local state offices.

#### *Security challenges*

Processes and best practices are inconsistent from one agency to another. Each agency recognizes the importance of creating a secure environment, but delays in communication or the execution of security-related actions have an impact on overall readiness. In 2005, the organization was struck by the Nimda virus. They experienced no data loss, but impact on the end users' ability to function on the job was significant. In 2006, the organization was hit by a spybot that slowed network traffic. This year, two phishing incidents were detected early and stopped.

#### **Symantec Endpoint Protection 11.0 anticipated benefits**

- A TOEI of more than \$3.4 million from 2007 to 2008
- Centralized management of many tasks that are decentralized today, including application control, location awareness, and log file monitoring of the multiple levels of government agencies and offices
- Improved ability to detect attacks early

Table 3. State government: Symantec Endpoint Protection 11.0 value summary

Symantec Endpoint Protection 11.0 beta TOEI summary	2007	2008
<b>Admin UI—monitoring</b>		
<b>Agency log file monitoring.</b> For more than 100 agencies, this is a once-a-week task performed by about 80 employees that takes four hours to complete. It will be automated by Symantec Endpoint Protection 11.0.	\$552,500	\$566,313
<b>Admin UI—reporting</b>		
<b>Audit and general reporting.</b> Once a year, preparing an audit report takes four hours per day for two weeks to collect the information. An additional two weeks is needed for one person to collect and produce the report. Symantec Endpoint Protection 11.0 can automate many of these reporting processes, thereby reducing labor costs.	\$17,500	\$17,938
<b>Admin UI—policies</b>		
<b>Creating and maintaining policies.</b> Currently it takes eight hours per month to audit policies and keep them current. With Symantec Endpoint Protection 11.0, once policies are set, they can be easily updated through a single management console.	\$3,000	\$3,075
<b>Admin UI—location awareness.</b> Each department has laptop/remote users that must be updated each month. Symantec Endpoint Protection 11.0 can automate and streamline this process for approximately 5,000 laptop users today.	\$318,750	\$326,719
<b>Application control.</b> Recreational network usage is an issue. With Symantec Endpoint Protection 11.0 application control capabilities, each agency could eliminate the cost of one server per year.	\$798,000	\$798,000
<b>Projected savings</b>	\$1,689,750	\$1,712,044
<b>Total savings</b>		\$3,401,794

Notes: Estimate includes a 2.5% inflation increase from 2007 to 2008.

Hours indicated are person-hours.

## Large county government

### About the organization

This county government serves nearly one million citizens. It provides a variety of public services, including court and prison systems, health and human services, and tax and collection services. The organization supports a total of 6,000 end users in approximately 70 locations. The security budget is included in the overall \$28.2 million IT budget, but is not a separate line item and is not fully justified for each purchase. Today, there are 145 IT staff members in the central IT organization, of whom eight are dedicated to security operations. Firewall management, spam email filtering, and management of the county Web site are all outsourced.

### Security challenges

The areas of great security concern include keeping track of changes to end-user access rights as users move from department to department and access control issues regarding unmanaged PCs that can enter the organization's network.

Symantec Endpoint Protection 11.0 anticipated benefits
<ul style="list-style-type: none"><li>• A TOEI of almost \$300,000 for 2007 and 2008</li><li>• More efficient—and effective—security administration</li><li>• Fewer security management tools to manage</li></ul>

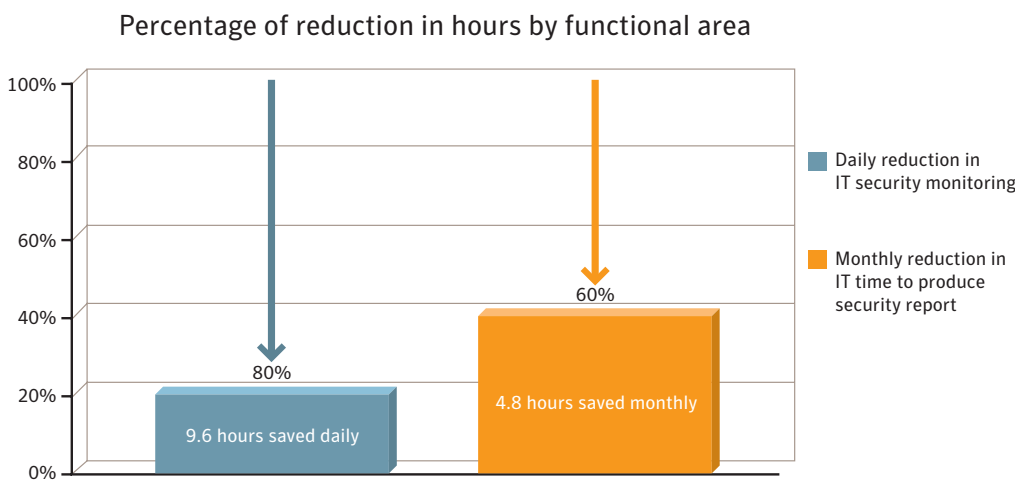


Figure 2. Large county government: annual reduction in hours by functional area

**Table 4. Large county government: Symantec Endpoint Protection 11.0 value summary**

<b>Symantec Endpoint Protection 11.0 beta TOEI summary</b>	<b>2007</b>	<b>2008</b>
<b>Admin UI—monitoring.</b> Today, an average of six technicians take one hour twice a day for monitoring. Symantec Endpoint Protection 11.0 promises to reduce this time by 80%. or 9.6 hours saved daily.	\$71,596	\$73,386
<b>Admin UI—patch deploy and validate.</b> Today, the process of deploying updates is performed on average four times per month, with each occurrence taking two hours. With Symantec Endpoint Protection 11.0, at least a 60% time savings or 4.8 hours are expected to be saved monthly.	\$2,354	\$2,413
<b>Antivirus and antispyware.</b> By allowing this organization to eliminate other security applications, Symantec Endpoint Protection 11.0 offers an estimated annual savings of about \$75,000.	\$75,000	\$75,000
<b>Projected savings</b>	\$148,950	\$150,799
<b>Total savings</b>		\$299,749

Notes: Estimate includes a 2.5% inflation increase from 2007 to 2008.

Hours indicated are person-hours.

### **Detailed results—small and midsize customers**

Of the seven participating customers, five qualified as small and medium organizations. These organizations include a variety of industries, such as healthcare, high tech, and banking.

#### **High-tech solution provider**

##### ***About the organization***

This organization has 1,100 total end users, of whom a very high percentage work remotely with laptops and travel throughout Asia and Europe. The IT staff totals 33 globally, and eight of those resources have direct responsibility for security operations.

### Security challenges

Because of its international presence and fast-moving operations, this organization has had several threats to its environment: virus and malware, laptops stolen or compromised, and receipt of an unwelcome threat that entered the organization's network through an external endpoint without being detected. Downtime related to recreational use of the company network is also a major concern.

Symantec Endpoint Protection 11.0 anticipated benefits
<ul style="list-style-type: none"><li>• TOEI of more than \$5.3 million for 2007 and 2008</li><li>• Greater application and device control</li><li>• Less help desk support time necessary to resolve support issues</li><li>• Fewer security-related calls to IT support</li></ul>

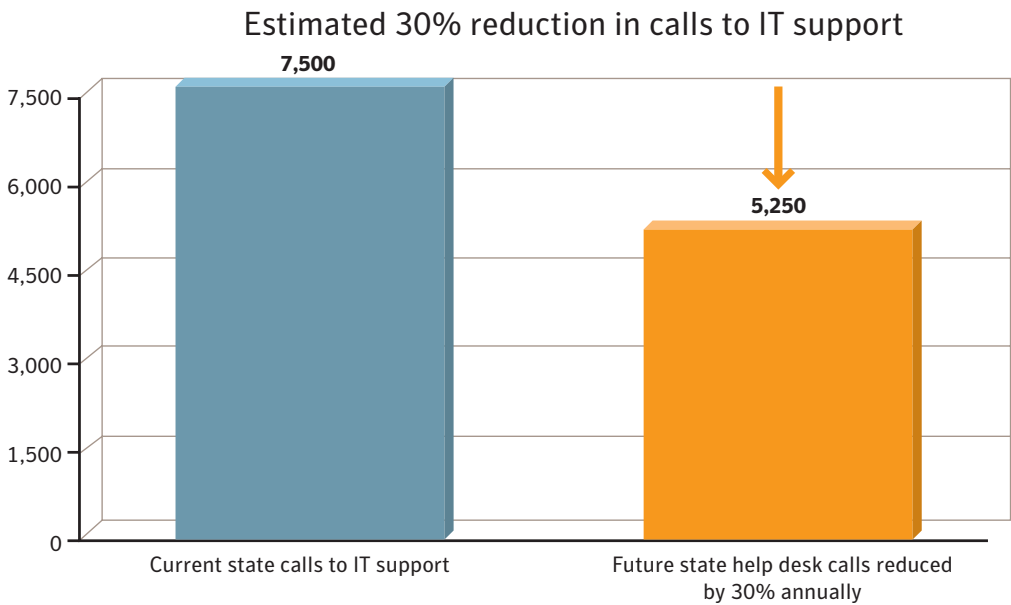


Figure 3. High-tech solution provider: estimated annual reduction in IT support calls typically related to antivirus and antispyware issues

**Table 5. High-tech solution provider: Symantec Endpoint Protection 11.0 value summary**

<b>Symantec Endpoint Protection 11.0 TOEI beta summary</b>	<b>2007</b>	<b>2008</b>
<b>Application control.</b> Symantec Endpoint Protection 11.0 will help this organization reduce network downtime due to recreational application usage. Savings will be global.	\$1,996,631	\$2,046,547
<b>Admin UI—reporting.</b> With Symantec Endpoint Protection 11.0, hours required to create custom reports for IT security operations audit compliance will drop from six hours to 10 minutes, monthly.	\$4,153	\$4,257
<b>Admin UI—roles-based administration.</b> Symantec Endpoint Protection 11.0 will allow this organization to avoid PC rework by establishing roles-based access rights.	\$38,774	\$39,744
<b>Client UI—self diagnostics.</b> With Symantec Endpoint Protection 11.0, this company could reduce the time required to resolve help desk issues by 50% annually.	\$600,000	\$615,000
<b>Projected savings</b>	\$2,639,558	\$2,705,547
<b>Total savings</b>		\$5,345,105

Notes: Estimate includes a 2.5% inflation increase from 2007 to 2008.

Hours indicated are person-hours.

## **Regional bank**

### **About the organization**

This regional bank offers consumer and commercial banking products and services, including online products. Its IT department supports a total of 1,500 end users with a staff of 74 IT employees, who are augmented by 24 contractors. The total IT budget for security tools is approximately \$1.0 million, which also includes the cost of any contractors or outside resources. They currently support end users in more than 80 branch bank locations, and four business and administration locations.



### Security challenges

This regional bank applies best practices to building and maintaining a security-focused business environment. For example, the assistant vice president of information security is responsible for overseeing individual and network data security. The primary IT-related security issues the bank faces are:

- 1) Managing security systems
- 2) Preserving data privacy issues by ensuring that non-public information does not leave the environment
- 3) Protecting against internal security breaches
- 4) Protecting against external security vulnerabilities

However, the bank's most critical security concern is the potential for bad publicity related to a security breach of its information systems.

Symantec Endpoint Protection 11.0 anticipated benefits
<ul style="list-style-type: none"><li>• TOEI of \$2.0 million from 2007 to 2008</li><li>• Centralized management of many tasks</li><li>• More efficient endpoint PC scanning for virus and malware</li></ul>

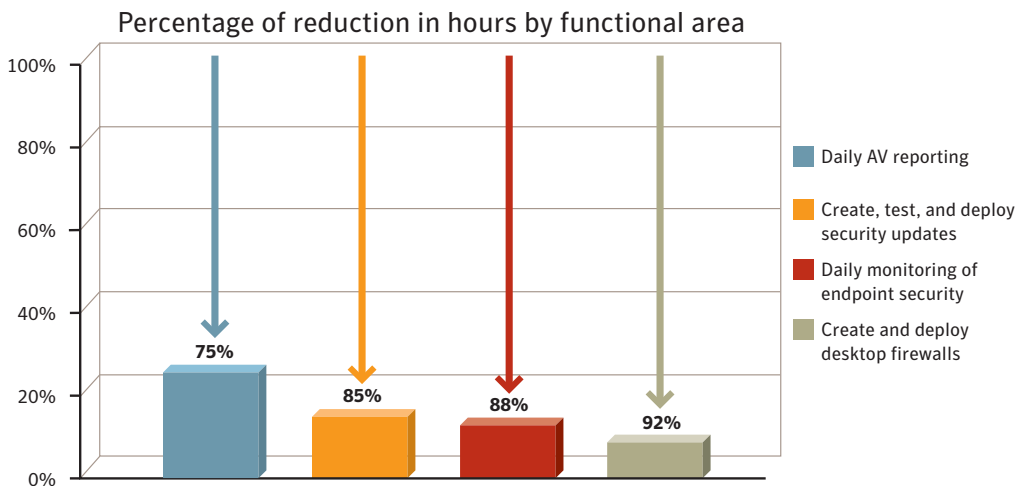


Figure 4. Regional bank: annual reduction in hours by functional area

Table 6. Regional bank: Symantec Endpoint Protection 11.0 value summary

Symantec Endpoint Protection 11.0 beta TOEI summary	2007	2008
<b>Admin UI—reporting</b>		
<b>Audit preparation.</b> Symantec Endpoint Protection 11.0 will automate audit report preparation. The audit report takes 30 minutes per screenshot (19 screenshots) to prepare. It is prepared three times per year.	\$891	\$913
<b>Daily reporting on desktop firewall.</b> Currently this takes one hour per day. With Symantec Endpoint Protection 11.0, it could be reduced to 10 minutes per day	\$9,467	\$9,704
<b>Admin UI—patch and update deployment</b>		
<b>Antivirus and firewall management.</b> Currently this takes one hour per day for each task. With Symantec Endpoint Protection 11.0, this would be reduced to 15 minutes per day for both tasks.	\$16,539	\$16,953
<b>Admin UI—clients</b>		
<b>Creating accounts and deploying major security software updates.</b> Previously it took 20 hours to create, test, and deploy an update. This happens twice annually. It should take only three hours with Symantec Endpoint Protection 11.0.	\$5,625	\$5,766
<b>Admin UI—install packages.</b> Today it takes approximately 60 hours to create a suitable package to deploy a desktop firewall for the first time. With the Symantec Endpoint Protection 11.0 console, this same function will take less than five hours to complete.	\$10,000	\$10,250
<b>Antivirus/Antispyware</b>		
<b>Find and remove rootkits.</b> This is a non-centralized process taking one hour per PC on an average of five PCs per week. Symantec Endpoint Protection 11.0 will centralize and automate this process.	\$8,125	\$8,328
<b>PC scan tuning.</b> Each endpoint PC is virtually unusable for one hour every other week, per end user. Symantec Endpoint Protection 11.0 could dramatically reduce this downtime.	\$937,500	\$960,938
<b>Projected savings</b>	\$988,147	\$1,012,851
<b>Total savings</b>		\$2,000,997

Notes: Estimate includes a 2.5% inflation increase from 2007 to 2008.

Hours indicated are person-hours.

## Professional union

### About the organization

This union provides healthcare benefits and pension services to workers and their dependents. The organization processes more than 700,000 pension and healthcare claims each year. There are a total of 25 IT staff members, including management. With such a small team, there is no dedicated IT security staff. However, network engineers spend 30 to 40 percent of their time on security, and other network or data administrators spend an average of 25 percent on security-related issues. This includes Microsoft® Exchange administration, which—due to manual log-tracking—consumes 20 percent of their time on mail security-related issues. They support approximately 300 end users at two different business sites.

### Security challenges

Management is security-minded, especially with regard to protecting its members' personal health and financial information. Information leakage from unsecured endpoints is a major issue. Other security challenges include implementing desktop encryption, USB lockdown, researching an email security encryption solution, and researching network access control.

#### Symantec Endpoint Protection 11.0 anticipated benefits

- TOEI of more than \$315,000 from 2007 to 2008
- Centralized and streamlined administration
- Improved device and application control

Percentage of reduction in hours by functional area

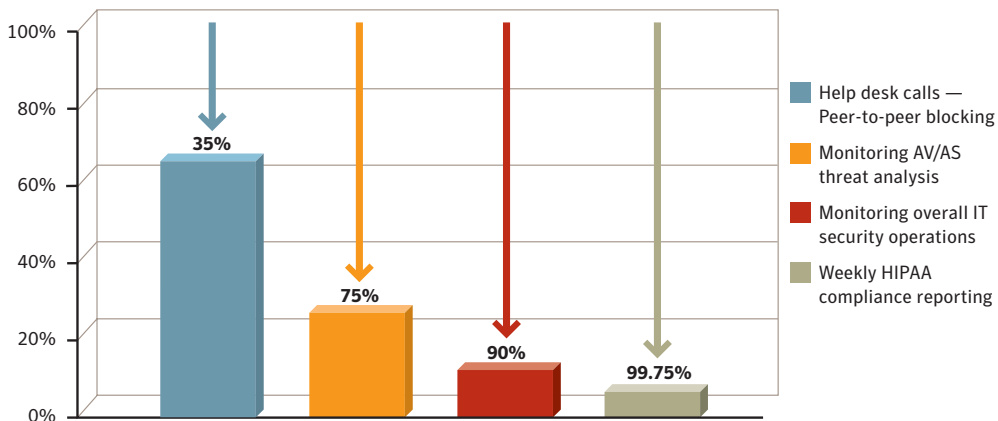


Figure 5. Professional union: Estimated annual reduction in hours by functional area

**Table 7. Professional union: Symantec Endpoint Protection 11.0 value summary**

<b>Symantec Endpoint Protection 11.0 beta TOEI summary</b>	<b>2007</b>	<b>2008</b>
<b>Admin UI—monitoring</b>		
<b>Daily audit reporting.</b> Currently the organization spends 20 hours per week complying with HIPAA security policy reporting. This could be reduced to 30 minutes or less with Symantec Endpoint Protection 11.0.	\$31,688	\$32,480
<b>Daily monitoring.</b> Reviewing current endpoint security status takes one hour each day. With Symantec Endpoint Protection 11.0, this could be reduced to 10 minutes.	\$9,581	\$9,821
<b>Issue resolution.</b> Currently an average of ten issues arise each week. On average, it takes eight hours to resolve four of these. The affected end user is idle for the same amount of time. Symantec Endpoint Protection 11.0 could dramatically reduce time to resolution.	\$84,000	\$86,100
<b>Re-imaging PC.</b> Currently, IT spends one hour per day on this task. With Symantec Endpoint Protection 11.0, this could fall to 15 minutes per day. Savings includes a reduction in end-user down time.	\$26,250	\$26,906
<b>Application control.</b> Rogue applications require 2.5 hours per week to remediate individual occurrences. Symantec Endpoint Protection 11.0 could dramatically reduce this requirement.	\$4,063	\$4,164
<b>Projected savings</b>	\$155,582	\$159,471
<b>Total savings</b>		\$315,053

Notes: Estimate includes a 2.5% inflation increase from 2007 to 2008.

Hours indicated are person-hours.

## **Landscaping service provider**

### **About the organization**

This company operates through a national network of 120 branch offices, providing landscape services to a wide variety of customers. The IT organization supports a total of 1,550 end users with a budget of \$8.0 million annually. Today the IT team totals 36 employees. One employee is dedicated to security and is generally in reactive mode. IT contractors are added as needed.

**Security challenges**

Security challenges include growing a secure network infrastructure to support business growth, and safely managing a Microsoft Exchange upgrade.

Symantec Endpoint Protection 11.0 anticipated benefits
<ul style="list-style-type: none"> <li>• More than \$326,000 TOEI from 2007 to 2008</li> <li>• Automated upgrade management</li> </ul>

**Table 8. Landscaping service provider: Symantec Endpoint Protection 11.0 value summary**

Symantec Endpoint Protection 11.0 beta TOEI summary	2007	2008
<b>Admin UI—update deployment</b>		
<b>Onsite upgrades.</b> Most business locations require hands-on support to complete software upgrades. Each location has an average of 30 clients. The upgrade process includes three support analysts per location. Symantec Endpoint Protection 11.0 could eliminate an average of 200 hours for each upgrade event and 140 individual trips to these locations.	\$160,000	\$160,500
<b>Antispyware.</b> Symantec Endpoint Protection 11.0 could recapture 600 support analyst and senior technician hours per week by reducing support center calls and the need for PC re-imaging.	\$2,769	\$2,838
<b>Projected savings</b>	\$162,769	\$163,338
<b>Total savings</b>		\$326,108

Notes: Estimate includes a 2.5% inflation increase from 2007 to 2008.

Hours indicated are person-hours.

**Healthcare provider**

**About the organization**

This healthcare provider firm’s IT team supports a total of 170 end users, of which 70 percent use laptops and are continually moving between clinic and office locations. The current IT budget is less than \$250,000 per year, of which 30 percent is directed to security solutions. The IT team today is composed of four cross-trained staff members, including the director.

**Security challenges**

With a large mobile work force, endpoint control is major security risk. The IT team needs a more effective way to encrypt hard drives and improve device control at mobile endpoints to address risks associated with the prevalence of thumb drives. Current goals include improving security awareness while controlling IT-related security costs.

Symantec Endpoint Protection 11.0 anticipated benefits
<ul style="list-style-type: none"> <li>• More than \$24,000 TOEI from 2007 to 2008</li> <li>• Improved endpoint control, including more effective remote device management</li> <li>• Centralized security management</li> </ul>

**Table 9. Healthcare service provider: Symantec Endpoint Protection 11.0 value summary**

Symantec Endpoint Protection 11.0 beta TOEI Summary	2007	2008
<b>Admin UI—monitoring</b>		
<b>Virus definition status.</b> Daily monitoring of status takes one hour. This could be reduced to only 10 minutes per day with Symantec Endpoint Protection 11.0.	\$7,665	\$7,857
<b>Issue remediation.</b> Currently, issues that require onsite action arise about once a month. 50% of these are four-hour tasks; the remaining 50% are eight-hour tasks. Issue remediation would take considerably less time with Symantec Endpoint Protection 11.0.	\$1,800	\$1,845
<b>Admin UI—reporting</b>		
<b>Automated reports.</b> This currently takes two weeks per reporting cycle, six times per year. With Symantec Endpoint Protection 11.0, this cost is eliminated.	\$2,769	\$2,838
<b>Projected savings</b>	\$12,234	\$12,540
<b>Total savings</b>		\$24,774

Notes: Estimate includes a 2.5% inflation increase from 2007 to 2008.

Hours indicated are person-hours.

## **Conclusion**

Symantec Endpoint Protection 11.0 combines Symantec AntiVirus™ with new advanced threat prevention technologies to protect against a variety of new threats, going beyond traditional antivirus and antispyware prevention to stop rootkits, bots, zero-day attacks, blended network-based intrusions, and data loss.

While enhanced security and lower costs are the primary benefits of Symantec Endpoint Protection 11.0, the VDR study reveals that Symantec Endpoint Protection 11.0 offers this and much more to a broad spectrum of companies, including the following highlights:

- Businesses of all sizes, across many industries, can benefit from Symantec Endpoint Protection 11.0.
- Symantec Endpoint Protection 11.0 can help businesses reduce IT security operations costs while they implement proactive security strategies.
- Security administration savings can reach millions of dollars a year.
- Security benefits include better threat monitoring, endpoint management, and dramatically improved device and application control.

## About Symantec

Symantec is a global leader in infrastructure software, enabling businesses and consumers to have confidence in a connected world.

The company helps customers protect their infrastructure, information, and interactions by delivering software and services that address risks to security, availability, compliance, and performance. Headquartered in Cupertino, Calif., Symantec has operations in 40 countries.

More information is available at [www.symantec.com](http://www.symantec.com).

For specific country offices and contact numbers, please visit our Web site. For product information in the U.S., call toll-free 1 (800) 745 6054.

Symantec Corporation  
World Headquarters  
20330 Stevens Creek Boulevard  
Cupertino, CA 95014 USA  
+1 (408) 517 8000  
1 (800) 721 3934  
[www.symantec.com](http://www.symantec.com)

Copyright © 2008 Symantec Corporation. All rights reserved. Symantec, the Symantec logo, and Symantec AntiVirus are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. Microsoft is either a registered trademark or trademark of Microsoft Corporation in the United States and/or other countries. Other names may be trademarks of their respective owners.  
01/08 13509087