Case Study of Symantec Endpoint Security deployed at a Federal Government Agency

White Paper

31 July 2007
Executive Summary

Dynamics of Endpoint Security

Analyzing a Federal Government Agency as a Test Case

The Federal Government Agency

Security Requirements

Compliance with FISMA and Agency Security Requirements

Endpoint Security Issues

Improving the Productivity of Scientists While Remaining Compliant

Centralizing Security Policy Management

Long Issue Remediation Time

Technology Requirements

Increased Complexity from Heterogeneous Endpoints Environment

Automated Security Patch Management

Solution Deployment

Selecting an Endpoint Security Product

Project Milestones

Implementing the Endpoint Security Solution

Network Architecture Diagram

Lessons Learned

Areas of Potential Business Value

Reduction in Help Desk Calls

Figure 1: Reduction in FTEs Resulting From Fewer Help Desk Tickets

Figure 2: Labor Savings Resulting From a Reduction in Help Desk Tickets

Increase in IT Staff Time Savings

Figure 3: Critical Incidents, Lost Hours, and Lost Productivity Dollars

Reduction in Audit Costs

Figure 4: Initial Audit Time, Reduction in Audit Time, and Savings

Conclusion
Executive Summary

Dynamics of Endpoint Security
According to a 2006 survey\(^1\), the following four categories account for 74% of business and government financial losses:

- Virus attacks (67%)
- Unauthorized access
- Losses related to laptop
- Theft of proprietary information

Yet, 97% of the companies surveyed have deployed firewalls and 98% use antivirus software. What would explain this discrepancy? Why were the countermeasures ineffective?

The most glaring system vulnerability stems from users—internal, remote, and mobile—who fail to patch their systems, update virus definitions, or neglect other security protection measures. These users can turn around and infect an entire population of other users or unintentionally create weaknesses and reveal vulnerabilities that an attacker can later leverage. Meanwhile, the security team spends the bulk of its time responding to requests from internal and external auditors, the daily barrage of support calls from frustrated end users, an ever-evolving and expanding threat landscape, and a constantly varying disclosure of vulnerabilities on systems and applications.

Organizations can achieve efficiency gains by automating the execution of security policies. This is particularly important for ensuring the security of all endpoints—desktops, laptops, servers, guest systems, and embedded devices.

Analyzing a Federal Government Agency as a Test Case
The Alchemy Solutions Group engaged a large federal government agency to research the area of endpoint security. The situation for the federal government agency is unique in that it involves a privately operated company subject to stringent regulatory requirements. It must comply with a complex security policy that includes:

- A large user population, including guest, mobile, internal, and remote users
- Local and remote offices
- Client and server deployments
- Multiple platforms and a variety of external devices that can be attached to them

With the help of an endpoint security solution from Symantec, which included Symantec Sygate Enterprise Protection, Symantec Network Access Control, and Symantec On-Demand Protection software, IT security engineers at the agency have been able to realize gains in security efficiency and effectiveness. They can now enforce and refine their host security policy for the entire enterprise from a centralized management console, regardless of the location of the end user or the type of device being used.

---

\(^1\)2006 CSI/FBI Computer Crime and Security Survey
The Federal Government Agency

In addition to a headquarters, the agency has two remote offices with approximately 100 employees each, and a number of smaller field offices scattered around the United States. They employ a total of 4,200 staff, bringing together scientists from many disciplines to solve complex problems in energy, national security, the environment, and life sciences.

There are three different groups that implement the policies at the federal government agency. An unclassified computer security department, formed by a small group of employees, is responsible for defining the security policy. This group is responsible for developing the plan for the deployment of security policies throughout the lab. Once the policies and roadmap are determined, the IT network services team implements the program. The IT services team is then chartered not only with maintaining the systems that allow scientists at the federal agency to do their jobs but with developing new and innovative IT services and products that can be used to advance their agency research initiatives.

Security Requirements

Compliance with FISMA and Agency Security Requirements
The federal government agency is subject to FISMA, which provides a framework for annual IT security reviews, reporting, and remediation planning. Following National Institute of Standards and Technology guidelines, the federal government agency is required to submit an annual report to the Office of Management and Budget (OMB) to show how effectively it is managing IT security and meeting FISMA regulations. If any IT security weaknesses are identified, they must be resolved within a timely manner. OMB provides economic incentives for compliance, as well as disincentives for noncompliance. In addition, there are internal and external pressures to ensure that the agency’s security policies and procedures, systems, data, applications, and networks satisfy agency requirements.

Endpoint Security Issues
The federal government agency seeks to provide its scientists with continuous and unfettered access to information they need to do their jobs. At the same time, they need to protect its IT systems against security threats, malicious attacks, and configuration vulnerabilities that could enter the network through a variety of endpoints which include laptops, desktops workstations, and PDAs.

Under the agency’s prior security environment, too much responsibility for security was in the hands of its scientists. For example, when users were traveling with their laptops, they were disconnected from the controls and security provided by the federal government agency network. Upon returning from a trip, scientists were personally responsible for ensuring that their security software and patches were up-to-date and their registry settings were correct. In addition, they were responsible for compliance with other other security policies before they could obtain system access via the LAN. As a result, they needed to bring their system into compliance themselves or request assistance from the IT Help Desk. Lacking strong endpoint security management and remediation controls, the agency’s network was exposed to a variety of risk, threats, and attacks. User productivity was also impacted. The agency needed a way to automate and centralize threat detection and remediation controls in order to mitigate security risks and increase user productivity.
Improving the Productivity of Scientists While Remaining Compliant

When the IT staff set out to establish effective security policies and procedures and find appropriate tools to help implement and manage their security, they were faced with some key challenges. At the forefront, the security solution needed to both comply with FISMA and federal agency security requirements while meeting the needs of the scientists by not impacting their research.

As scientists at the federal government agency are allowed to install applications on their desktops that further their research, a balance had to be struck between this and the need to maintain host security. The IT staff needed a solution that would both accommodate new laptop and desktop applications while ensuring compliance with security policies.

Centralizing Security Policy Management

With facilities dispersed across the country and a variety of users—scientists, management and administrative personnel, among others—the federal government agency needed a security solution that could be centrally managed. To establish a clear division of privileges, the security staff needed to apply security controls such as separation of duties and the principle of least privilege. The latter means that users are given access to those functions or applications needed to perform a job.

Due to the diversity of research conducted at the federal government agency, the IT team sought a solution that would allow for business units to set their own policies while still providing a global security view. The rollout also needed to support multiple access methods: remote access IPSec VPN, dialup, SSL VPN, wireless LAN, DHCP, 802.1x, web access, etc.

Overall, they required a solution that would provide the appropriate degree of security for each endpoint device with the ability to centrally manage and maintain security levels without impacting users. Faced with a wide array of possibilities, the federal government agency sought to minimize costs by consolidating the functionality of numerous countermeasures into a customizable, automated solution.

These countermeasures included:

- Antivirus
- Antispyware
- Personal firewall
- Host and network intrusion prevention
- File and disk encryption
- Network access control
- Application control
- Patch management
- Host integrity checking
- Peripheral device control
**Long Issue Remediation Time**
The current process for addressing security problems was inefficient, incurring lost end-user productivity and less than optimal use of IT support resources. Typical endpoint security problems included:

- Interaction with the IT Help Desk
- Quarantine
- Application of security updates
- Remediation
- Security scanning
- Lead time to gain network access

Systems that were compromised or identified as vulnerable and required remediation were frequently quarantined for lengthy periods of time. To improve their efficiency, the processes needed to be automated in order to fix problems quickly, improve user downtime, and eliminate the need to involve the IT Help Desk and the IT Desktop Support groups.

**Technology Requirements**

**Increased Complexity from Heterogeneous Endpoints Environment**
Providing network access without compromising network security was a growing concern. The complexity of the challenge was compounded by a heterogeneous workstation environment that included desktops and laptops running Microsoft Windows, Linux, UNIX, and Mac OS operating environments.

In certain laboratory areas, the federal government agency needed to closely control access to, and removal of, sensitive information. Overseeing the use of media devices such as USB keys, CD/DVD burners, and PCMCIA hard drives presented another security challenge. In addition, the IT security team needed to block unauthorized device usage such as USB, infrared, firewire, SCSI, and serial and parallel ports and to regulate the ability to read, write, or execute data on specific devices.

In short, to allow its scientists, other employees, and subcontractors secure access to information at any time, from anywhere, and from virtually any kind of access device, the agency needed a flexible endpoint security policy and a software solution that could address a diversity of devices and platforms.

**Automated Security Patch Management**
As the number of malicious code attacks throughout the world increases, the need of applying security patches becomes more critical for protection. Threats released before a vendor patch—also known as “zero-day” threats—reduce the window of security between the discovery of vulnerability and the threat on which it is based. As a result, the federal government agency realized that relying on its users to manually update their devices with the latest security updates did not provide an adequate level of protection. The federal government agency required a way to automate patch management and antivirus software updates, which provided a proactive stance in enforcing security policies with minimal or no impact to end-user performance.
Solution Deployment

Selecting an Endpoint Security Product
The previous security infrastructure at the federal government agency consisted of Cisco-based firewall protection and intrusion prevention devices for access control, as well as Symantec AntiVirus Enterprise Edition software to identify, thwart, and eliminate computer viruses and other malicious software. In 2003, faced with increasingly stringent regulatory requirements and inadequate security protection at its endpoints, the federal government agency began its search for a more complete endpoint solution. The federal government agency evaluated several different solutions, including Symantec Sygate Enterprise Protection software. As functionality in the product closely corresponded with endpoint technical requirements specified by the IT security team, they decided to run a 60-day proof-of-concept pilot across the organization’s heterogeneous environment. Their primary goal was to evaluate the ease of installation and operation, as well as the potential impact on end users.

Project Milestones

- June 2003–Decision taken to evaluate endpoint security solutions
- December 2003–60-day proof of concept conducted based on Symantec Enterprise Security
- May 2004–Selection of Symantec Sygate Enterprise Security as foundation for enterprise security
- June 2004–Symantec Consulting Services helped define security policies and implement Symantec Sygate Enterprise Protection
- February 2005–Deployment of Symantec Network Access Control and Symantec Sygate On-Demand

The federal government agency team ultimately selected Symantec Sygate Enterprise Protection software as the foundation for endpoint security for three primary reasons:

- Support for heterogeneous computing environments
- Engineering and technical support
- Ability to deploy across managed clients and servers as well as unmanaged nodes

In 2005, needing to deploy preconfigured security agents to unmanaged systems and to protect the network from dangerous endpoints by enforcing compliance and contact with the enterprise LAN, the agency selected Symantec Sygate On-Demand Protection Solution and Symantec Network Access Control, respectively. Symantec On-Demand Protection Solution prevents eavesdropping and theft of data from unmanaged devices and unprotected or compromised devices from connecting to the enterprise via the web. It also allows the federal government agency to deliver endpoint security to unmanaged devices (e.g., kiosks, contractors, home machines, etc.). Symantec Network Access Control enables the discovery of endpoints and its compliance with security policies, leverage existing networks to detect and control access for connected devices, and remediate non-compliant endpoints.
Implementing the Endpoint Security Solution

In June 2004, the federal government agency engaged Symantec Consulting Services to help define the security policies and implement the Symantec Sygate Enterprise Protection software. After meeting with the network team, the desktop services team, and other staff involved with the project, the Symantec consultants had a good understanding of the diverse environment, as well as the security and technical requirements. Symantec security experts assisted the federal government agency with its security policy development, software testing, and problem resolution. Within two weeks, the software implementation—including the installation, configuration, testing, and approval of security policies—was completed with no impact to employees. The software was rolled out across three independent security networks: unclassified, internet secret, and top secret. Each of these networks must remain physically separated and operated independently. Symantec Sygate Enterprise Protection software allows the federal government agency to comply with these requirements while centrally managing endpoint security.

Throughout the project, a team of technical experts from Symantec responded to various issues the federal government agency encountered. And the ability to leverage one software solution across all of its different operating systems and server platforms—Microsoft Windows, UNIX, and Linux—helped the agency team to reduce time to deployment as well as overall costs.

In early 2005, the federal government agency deployed Symantec Network Access Control and Symantec On-Demand Protection Solution. Symantec Network Access Control allows the enforcement of security settings and software running on hosts connected to its enterprise network. Symantec On-Demand Protection Solution enables the agency to eliminate the exposure resulting from unprotected devices and provides integrated endpoint security technologies that help ensure compliance with security policies, prevent unauthorized data transfer, and protect confidential information.
Symantec Sygate On-Demand Protection software helps prevent the compromise of enterprise information assets caused by unprotected network access through Web-enabled applications, wireless LANs, and SSL VPNs via unmanaged devices including home computers, kiosks, and guest laptops.

Symantec Sygate Enterprise Protection software provides advanced endpoint protection and seamless integration with Symantec Network Access Control software in a single management architecture.

Symantec Consulting Services helped define the security policies and implemented the Symantec Sygate Enterprise Protection software.

Symantec Network Access Control software enables PNNL to discover endpoints, assess compliance with security policies, and remediate noncompliant machines.

As many as 2,000 remote and mobile users

Total deployment: 5,000 Windows-based desktops and laptops 500 Macintosh desktops and laptops 1,000 Linux and UNIX workstations

Main office

Field offices

Internet

The Federal Government Agency Endpoint Protection Architecture
Lessons Learned
One of the early adopters of Symantec Sygate Enterprise Protection software, the federal government agency’s IT security team has subsequently worked with Symantec product engineers to identify new product requirements and expand upon its functionality. In addition, the team identified a number of lessons learned as a result of their experience. The following are ten top lessons the team pinpointed during interviews with The Alchemy Solutions Group:

1. Before beginning, it is important to have a clear understanding of the software, especially when implementing it in a heterogeneous operating environment.

2. Know what is going on in the network. Don’t jump to conclusions.

3. Do adequate planning to ensure a smooth implementation.

4. Make sure all parties—particularly end users—are aware of the implementation plans and the impact.

5. Minimize the impact on end users while maximizing the security of the endpoints.

6. Take your time. Don’t push out a policy update before you understand all the implications to the end user. Phase in new rules. Refine existing security policies.

7. Enlist the support of the software vendor during implementation and rollout—and keep your account executive updated.

8. Create a separate “sandbox” environment to test the solution and gain valuable insights.


10. Use the pilot to fine-tune your product knowledge. Be sure you are ready before going live.

Areas of Potential Business Value
The Alchemy Solutions Group pinpointed three areas where the federal government agency should experience potential business value:

- Reduction in calls to the IT Help Desk
- Increase in IT employee productivity
- Reduction in audit costs

The following assumptions were made:

- IT Help Desk receives weekly calls from 25% of users once a month
- 90% of IT Help Desk calls are resolved within 10 minutes or less
- 10% of IT Help Desk calls are resolved in 11 minutes to 4 hours
- IT Help Desk availability is equal to 2,080 hours per year
Reduction in Help Desk Calls

Lack of an automated endpoint security solution necessitates manual intervention when end users change endpoints or require changes to their access. However, Symantec Sygate Enterprise Protection and Symantec Network Access Control enable automated remediation, which results in a reduction of calls into the IT Help Desk. The Alchemy Solutions Group compiled a number of different scenarios ranging from a 5% reduction in IT Help Desk calls up to a reduction of 50%. For example, an annual reduction in IT Help Desk calls of 20% in an organization of 2,000 users would produce a reduction in 14.33 full-time equivalents (FTE). For an organization with 500 weekly calls, this translates into a reduction of 3.58 FTEs; for an organization with 1,000 weekly calls, this translates into a reduction of 7.17 FTEs; and for an organization with 1,500 weekly calls, this translates into a reduction of 10.75 FTEs.

Figure 1: Reduction in FTEs Resulting From Fewer Help Desk Tickets

Assuming an annual salary of $43,380, a reduction of 14.33 FTEs (20%) would equate to an annual labor savings of $155,445 in an organization with 2,000 weekly calls. For an organization with 500 weekly calls, this translates into an annual labor savings of $38,861; for an organization with 1,000 weekly calls, this translates into an annual labor savings of $77,723; and for an organization with 1,500 weekly calls, this translates into an annual labor savings of $116,584.

Figure 2: Total Labor Savings Resulting From a Reduction in Help Desk Tickets
Increase in IT Staff Time Savings

Assuming that 0.16% of security incidents per year are critical and that 25% of endpoints are affected by these incidents, an organization with 15,000 employees and 20,000 security incidents per year would experience 120,000 critical incidents per year. A normal endpoint critical incident typically involves the following actions:

- Detect incident
- Quarantine
- Generate IT Help Desk ticket
- Report incident
- Remediate policy conflict
- Provide technical support
- Resolve conflict
- Scan endpoint
- Approve endpoint

Assuming that it takes 1.4 hours to go through all of the above actions, an organization experiencing 120,000 critical incidents per year would lose 168,000 IT production hours.

An organization that loses 168,000 in IT production hours at an annual salary for a computer operator of $43,380 would see an annual loss in productivity dollars of $8.08 million. The lost employee productivity savings for smaller organizations are just as impressive, ranging from $.27 million annually for an organization with 500 employees, to $.54 million annually for an organization with 1,000 employees, to $2.69 million annually for an organization with 5,000 employees.

---

**Figure 3: Critical Incidents, Lost Hours, and Lost Productivity Dollars**

3. - See footnote 2
Reduction in Audit Costs
For an organization of 15,000 employees, assuming 120,000 critical incidents per year and an audit time for each incident of 1 minute, it would take an average of 250 days to complete an audit. Symantec Sygate Enterprise Protection eliminates unwelcome audit findings by keeping endpoints patched and required applications running. This measure enforces policy compliance when contact is made at any and every endpoint. The Alchemy Solutions Group estimates that Symantec Sygate Enterprise Protection reduces the total number of incidents and, for an organization of 15,000 employees, would result in a 75% decrease in security audit time. This equates to a reduction of 187.5 days and annual savings of $276,000. And, per Figure 4, the benefits to an organization dramatically increase with the number of employees (with a dramatic parallel growth in incidents).

### Figure 4: Initial Audit Time, Reduction in Audit Time, and Savings

<table>
<thead>
<tr>
<th>Number of Employees</th>
<th>Number of Incidents</th>
<th>Security Audit Time Savings Based upon 75% Reduction in Audit Time</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>5,000</td>
<td>10,000</td>
</tr>
<tr>
<td>500</td>
<td>Days</td>
<td>0.5</td>
</tr>
<tr>
<td>1,000</td>
<td>Days</td>
<td>1.0</td>
</tr>
<tr>
<td>5,000</td>
<td>Days</td>
<td>5.2</td>
</tr>
<tr>
<td>10,000</td>
<td>Days</td>
<td>10.4</td>
</tr>
<tr>
<td>15,000</td>
<td>Days</td>
<td>15.6</td>
</tr>
<tr>
<td>20,000</td>
<td>Days</td>
<td>20.8</td>
</tr>
<tr>
<td>25,000</td>
<td>Days</td>
<td>26.0</td>
</tr>
<tr>
<td>30,000</td>
<td>Days</td>
<td>31.3</td>
</tr>
<tr>
<td>35,000</td>
<td>Days</td>
<td>36.5</td>
</tr>
<tr>
<td>50,000</td>
<td>Days</td>
<td>52.1</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Number of Incidents</th>
<th>Security Audit Savings</th>
</tr>
</thead>
<tbody>
<tr>
<td>5,000</td>
<td>$2,300</td>
</tr>
<tr>
<td>10,000</td>
<td>$4,600</td>
</tr>
<tr>
<td>15,000</td>
<td>$6,900</td>
</tr>
<tr>
<td>20,000</td>
<td>$9,200</td>
</tr>
<tr>
<td>25,000</td>
<td>$11,500</td>
</tr>
<tr>
<td>30,000</td>
<td>$13,800</td>
</tr>
<tr>
<td>35,000</td>
<td>$16,100</td>
</tr>
<tr>
<td>50,000</td>
<td>$18,400</td>
</tr>
</tbody>
</table>
Conclusion

There is little question that endpoint security is a required component of an overall enterprise security strategy. On the one hand, the frequency of endpoints being exposed directly to the Internet will continue to increase with the various trends that are fostering more and more movement to mobile computing. One the other hand, even when users are operating on the LAN, endpoints are being exposed to a growing number of threats, both from other internal sources as well as from external sources.

Per this federal government agency case study, establishing an endpoint security solution is a complicated undertaking. Based on the opinion of The Alchemy Solutions Group, the federal government agency was successful in its endpoint security implementation for several different reasons, including:

- Clear delineation of technology/solution requirements
- Development of an implementation plan with precise areas of responsibility, both for the customer’s IT team and for the Symantec team
- Leveraging Symantec Consulting Services as well as Symantec engineering resources throughout the various phases of the deployment
- Development of a phased-implementation approach
The Alchemy Solutions Group

www.alchemygroupinc.com
The Alchemy Solutions Group provides global consulting services for organizations with a high client-touch ratio. These client groups typically include enterprise wide sales, marketing, and customer support organizations. Utilizing significant intellectual capital developed through years of experience, Alchemy has the resources and industry knowledge to positively impact overall corporate performances.

Business Value Analysis (BVA) is a public research deliverable under the Total Operational and Economic Impact (TOEI) practice. Its charter is to define, discover, develop and document the TOEI of a client’s solution in a post implementation environment. The resulting BVA provides a clear description of the ultimate value of the client’s delivered solution, which can be repurposed into a variety of industry-specific communication and education mediums.

Alchemy is committed to leveraging deep industry expertise, proven business process experience, and formal research to understand the key attributes and constraints to corporate performance. Our professionals have strong execution capabilities to help our clients drive value-based process changes quickly and effectively.

Skip King – Principal and Corporate Officer
As principal and corporate officer of The Alchemy Solutions Group, Skip is responsible for establishing strategic relationships with executives that are committed to understanding the impact their products and services are having on their customers. The TOEI was established specifically to research the deployment of products and services in pre and post implementation environments. This independent and objective approach used to determine the economic impact, is key to providing industry executives the candid insight required to help educate and transform client-facing organizations. From product development to sales and marketing, the repurposing of the research findings have always proven valuable to Alchemy clients.

Prior to founding The Alchemy Solutions Group, Skip served in the software industry for 19 years in sales, sales management, field operations, executive management, and M&A positions. Skip’s global experience in large companies like Oracle and smaller firms, including technology start ups, allows him to bring a wealth of insight to support the continued Research and Publishing efforts at Alchemy.

stanleyking@alchemygroupinc.com