SYMANTEC ENDPOINT PROTECTION: A UNIFIED, PROACTIVE APPROACH TO ENTERPRISE SECURITY

BY LAUREN DUDA

Enterprises must constantly guard against stealthy, targeted, financially motivated attacks that can exploit vulnerabilities in endpoint devices to allow data theft and other damage. Through a seamless, multilayered approach, Symantec® Endpoint Protection helps provide advanced threat prevention and simplified, holistic endpoint protection across notebooks, desktops, and servers.

Related Categories:

Antivirus

Firewalls

Security

Symantec

Threat management

*Visit **DELL.COM/PowerSolutions** for the complete category index.*

IT threats have changed dramatically over the past few years, as attacks with the simple goal of making headline news have given way to a relentless wave of financially motivated attacks against unsuspecting enterprises. With this goal in mind, professional hackers continuously develop sophisticated new tactics to escape detection and discover new entry points that allow them unauthorized and ongoing access to an organization's systems and valuable information.

Antivirus, anti-spyware, and other signature-based protection measures may have been sufficient to protect an organization's vital resources a few years ago, but not today. Although these primarily reactive methodologies can still play a vital role in protecting notebooks, desktops, and servers, they are only part of the solution. To help protect these endpoints against a comprehensive array of sophisticated threats—including unknown threats and zero-day attacks—organizations must augment their traditional security approach with proactive endpoint security.

However, for many organizations, adding proactive endpoint security can translate into installing discrete antivirus, anti-spyware, desktop firewall, intrusion prevention, and other types of software from multiple vendors. Deploying this software individually on each endpoint not only is time-consuming, but also increases IT costs and complexity, and typically requires providing management, training, and support for each application. In addition, these different applications can actually work against one another to create security gaps, and may require high resource consumption that can impede system performance.

To help eliminate security gaps, increase endpoint system performance, and reduce the costs and complexities associated with deploying and managing multiple endpoint protection solutions, Symantec Endpoint Protection consolidates multiple endpoint protection technologies into a single integrated agent that administrators can control from a unified management console. Symantec Endpoint Protection combines industry-leading antivirus and anti-spyware signature-based protection with firewall, device control, and proactive intrusion prevention software, and employs state-of-the-art threat prevention to help protect against known and unknown malware, including viruses, worms, Trojan horses, spyware, and adware. It even helps protect against sophisticated attacks that evade traditional security measures such as rootkits, zero-day attacks, and mutating spyware.

Advanced antivirus and anti-spyware technology

Although typically inadequate for protecting against unknown threats and zero-day attacks, antivirus and anti-spyware software is still essential to endpoint security. This software typically uses traditional scan-based technologies to identify viruses, worms, Trojan horses, spyware, and other

> “Symantec Endpoint Protection consolidates multiple endpoint protection technologies into a single integrated agent that administrators can control from a unified management console.”

malware on an endpoint device—searching the system for files that match the characteristics, or threat signatures, of a known threat. Once these technologies detect a threat, they remediate it, typically by deleting or quarantining it. For many years, this type of software has been effective in helping protect endpoints against known threats.

With the IT industry’s increased focus on endpoint security, a variety of antivirus and anti-spyware products have become available. Although many of these first- and second-generation solutions provide some protection, they can fall short of comprehensive protection—only working on one OS, for example, or lacking the ability to interoperate with other essential endpoint security elements such as personal firewalls, intrusion prevention systems (IPSs), and device control.

Antivirus and anti-spyware software may also be unable to detect polymorphic threats or detect and remove rootkits. For example, in a February 2007 study conducted by AV-Comparatives, of 15 antivirus products tested with 12 highly polymorphic viruses, only Symantec and one other vendor received a score of 100 percent for all polymorphic viruses tested.[1] According to the report, these tests help determine the flexibility of an antivirus scan engine as well as how good it is at detecting complex viruses.

Rootkits—stealth applications or scripts that hackers can use to gain undetectable administrator-level access to a system—are widely available on the Internet, giving inexperienced hackers easy access to these tools without having to understand how they work. Rootkits are often used to collect confidential information such as user IDs, account numbers, and passwords. Detecting and removing rootkits typically requires thoroughly analyzing and repairing the OS, something many antivirus solutions may be unable to do. To this end, Symantec Endpoint Protection 11.0 is designed to provide a deeper inspection into the file system than many other solutions, enabling the analysis and repair processes necessary to remove even highly difficult rootkit attacks.

State-of-the-art network threat protection

Network threat protection is critical to defending endpoints against blended threats and inhibiting outbreaks. To be effective, it must encompass more than just a firewall: it should combine state-of-the-art protection technologies, including intrusion prevention and sophisticated capabilities for controlling network communications.

In the past, security experts have debated whether organizations should place firewalls only on the perimeters of their networks, or on individual desktops as well. As threats have multiplied and mobile workforces have extended the perimeters of organizations’ network infrastructures, however, endpoints have become a primary target for attacks: an exploit may first infect a single notebook outside the network perimeter, then spread to other endpoints when the notebook connects to the internal network. Endpoint firewalls have become key not only to blocking internal network attacks from breaching endpoints connected to the network, but also to helping prevent these threats from leaving the initially infected endpoint.

The Symantec Endpoint Protection single-endpoint security agent incorporates a state-of-the-art firewall that includes the following key components:

- Rule-based firewall engine
- Predefined antivirus, anti-spyware, and personal firewall checks
- Firewall rule triggers based on applications, hosts, services, and time periods
- Comprehensive TCP/IP support, including User Datagram Protocol (UDP) and Internet Control Message Protocol (ICMP)
- An option to allow or block support of network protocols, including the Ethernet, Token Ring, Novell® IPX/SPX™, Apple AppleTalk, and NetBIOS Extended User Interface (NetBEUI) protocols
- The ability to block protocol drivers such as those for VMware® virtualization software and Windows Packet Capture Library (WinPcap)
- Adapter-specific rules
- Encrypted and clear-text network traffic inspection
- Packet and stream IPS blocking, custom IPS signature blocking, and generic exploit blocking for proactive threat protection
- Self-enforcement for network access control

Because intrusion prevention is vital to helping protect against vulnerability-based intrusions that utilize generic signatures, it must play a critical role in network threat protection. However, although traditional IPSs can detect a specific known exploit, they are typically inadequate against the barrage of exploit variants that exist today. According to the March 2007 *Symantec Internet Security Threat Report*, from July to December 2006 it took 47 days on average for an OS or application

[1] “Anti-virus Comparative No. 13: On-Demand Detection of Malicious Software,” by AV-Comparatives, February 2007, www.av-comparatives.org/seiten/ergebnisse/report13.pdf.

Threat	Single GEB signature	Number of variants blocked
Blaster	MS RPC DCOM BO	814
W32.Mytob.IM@mm	MS_RPC_NETDDE_BO	426
Sasser	MS LSASS BO	394
W97M.Invert.B	RPC_NETAPI32_BO	250
W32.Gaobot.AAY	NetBIOS MS NO (TCP)	121
Welchia	MS IIS Webdav Exploit	55
W32.Zotob.A	MS Plug and Play BO	51
W32.Welchia.C	MS Locator Service BO	43

Figure 1. *Multiple exploit variants blocked through generic exploit blocking signatures*

provider to release a patch for a published vulnerability.[2] Attacks that exploit these vulnerabilities before a patch becomes available are often referred to as unseen or zero-day attacks. A few hours after the first vulnerability exploit is detected, IPS vendors typically can release a signature to protect against further attacks from the specific exploit.

These reactive measures create significant opportunities for sophisticated attackers. Considerable damage can be inflicted on an organization with the first wave of exploits before the release of an exploit signature. Even after the exploit signature is released, it may prove ineffective against polymorphic or self-mutating variants of that exploit. Furthermore, these reactive, exploit-based signatures cannot protect against unseen, unreported, or unknown threats, such as stealthy exploits targeted at specific organizations, which often go undetected. Combating these types of threats requires proactive measures through a vulnerability-based IPS.

While an exploit-based signature detects only a specific exploit, a vulnerability-based signature operates at a higher level—it can detect not only a specific exploit for a vulnerability, but potentially any exploit that attempts to attack that vulnerability. Symantec Endpoint Protection includes generic exploit blocking (GEB), a vulnerability-based IPS technology that uses generic signatures. When OS or application vendors announce new vulnerabilities, Symantec engineers study the characteristics of that vulnerability, then create and release a generic signature based on that study. The power of vulnerability-based IPSs derives from the fact that a single vulnerability definition can protect simultaneously against multiple types of threats (see Figure 1). Because these definitions are based on vulnerability characteristics and behavior, they can help protect organizations against a wide range of threats—even those that are not yet known or developed.

Vulnerability-based IPSs are also useful for protecting against exploits that target a specific organization. Targeted attacks are generally stealthy, because the attackers' goal is to steal confidential information and then erase themselves from the system without being discovered. Because organizations have no way of knowing about these targeted exploits until the damage is done, there is no way to create an exploit signature that could have prevented the attack. Vulnerability-based IPSs can detect and block the exploit by recognizing the high-level characteristics of the vulnerability that the targeted attack is attempting to exploit. The endpoint security agent in Symantec Endpoint Protection incorporates vulnerability-based protection at the network layer, helping prevent even unseen exploits and exploit variants from entering and infecting the endpoint—avoiding damage and the need for remediation.

> "Targeted attacks are generally stealthy, because the attackers' goal is to steal confidential information and then erase themselves from the system without being discovered."

Symantec Endpoint Protection also enables administrators to create custom rule-based intrusion prevention signatures tailored to the needs of their specific environment. They can create signatures that block a few specific actions or multiple complex actions. By helping eliminate the need to wait for an OS or application vendor to create patches for known vulnerabilities, Symantec Endpoint Protection provides administrators with comprehensive, proactive control over endpoint security.

Proactive threat protection

While signature-based file and network scanning technologies address key areas of protection, non-signature-based approaches are also necessary to address the growing number of unknown threats used in stealth attacks. These approaches are referred to generally as proactive threat protection technologies.

Symantec Endpoint Protection includes Proactive Threat Scan, which is based on heuristics technology that analyzes the behavior of system processes to help protect against the

[2] *Symantec Internet Security Threat Report, Volume XI: Trends for July–December 06,* by Symantec, March 2007, eval.symantec.com/mktginfo/enterprise/white_papers/ent-whitepaper_internet_security_threat_report_xi_03_2007.en-us.pdf.

multitude of variant and unseen threats that exploit known vulnerabilities. Its host intrusion prevention capabilities also enable organizations to protect themselves against unknown or zero-day threats.

Many host-based IPSs only examine what they consider to be "bad behavior" by applications. As a result, they can often falsely identify acceptable applications as threats and shut them down, causing productivity problems for users and help-desk nightmares for administrators. Proactive Threat Scan, however, scores both good and bad behavior, helping increase the accuracy of threat detection and reduce the number of false positives.

Symantec Endpoint Protection also incorporates device and application control capabilities that allow administrators to deny specific activities deemed high risk and to block specific actions based on user location. Device control allows administrators to determine which devices are allowed to attach to an endpoint—for example, it can lock down an endpoint to keep USB drives, CD burners, printers, and other USB devices from connecting to help prevent confidential data from being copied off of the system. Its ability to block device connections can also help prevent endpoints from being infected by viruses spread from these and other types of devices.

Application control allows administrators to control access to specific processes, files, and folders by users and other applications. It provides application analysis, process control, file and registry access control, and module and dynamic-link library (DLL) control. These advanced capabilities are useful for administrators who want to restrict certain activities deemed suspicious or high risk.

Integrated network access control

The Symantec Endpoint Protection agent integrates network access control, which administrators can easily enable by purchasing a Symantec Network Access Control license. After deploying Symantec Endpoint Protection, administrators do not need to deploy additional agent software on endpoint devices to implement network access control.

Convergent security and management

Effective client management is key to reducing costs and providing a quality, stable, and secure computing environment. Dell Client Manager™ software, powered by Altiris, can enhance security configurations to help make well-managed endpoints into secure endpoints as well. Incorporating security functionality into their management console helps organizations increase productivity while reducing endpoint management costs.

The Symantec Endpoint Protection Integration Component, which Altiris plans to include in all Dell Client Manager versions, facilitates migration to Symantec Endpoint Protection–based clients using remote delivery mechanisms. This component provides detailed reporting, broad dashboard deployment views, multicasting technology, advanced client discovery, and the ability to scale for both LAN-connected and remote endpoints. Integrating this component into their endpoint management system enables administrators to easily migrate client systems and manage rollout activities using Dell Client Manager, initiate scans and other troubleshooting- and health-related tasks from the Dell Client Manager console, and view Symantec Endpoint Protection–based environments from a single console to help simplify reporting and remediation tasks.

Comprehensive, cost-effective, easy-to-manage endpoint protection

Symantec Endpoint Protection enables organizations to implement an integrated solution that protects from threats on multiple levels. And even though it provides a comprehensive array of endpoint protection features, Symantec Endpoint Protection still gives administrators the flexibility to scale their protection over time. They can start with a limited set of features and then enable additional capabilities as needed. Symantec Endpoint Protection can even be configured to work alongside other vendors' technologies, so that organizations can implement and configure the solutions they need to address specific requirements.

In addition, the integrated Symantec Endpoint Protection agent is designed for low memory and resource usage on notebooks, desktops, and servers, helping eliminate the administrative overhead and costs associated with multiple security products. Administrators can tune the agent to help maintain endpoint performance, reducing its resource usage during periods of high user activity.

To combat sophisticated, stealthy, and targeted attacks, organizations can no longer rely solely on traditional antivirus and anti-spyware software. Effective endpoint security requires implementing a holistic solution that can proactively protect against threats at multiple levels while providing seamless interoperability, simplifying management, and reducing total cost of ownership. Through its integration of advanced security technologies into a single multilayered agent, Symantec Endpoint Protection can meet all of these requirements—helping simplify security administration, save time and money, and provide high levels of endpoint security to protect critical enterprise assets.

Lauren Duda *is a product marketing manager for the Endpoint Security team at Symantec. Lauren currently has global product marketing responsibility for Symantec AntiVirus™ and Symantec Client Security software. She has a B.A. from the University of California, Los Angeles, and an M.B.A. from California State University, Long Beach.*

MORE ONLINE
DELL.COM/PowerSolutions

QUICK LINK

Symantec Endpoint Protection:
www.symantec.com/endpoint