WHITE PAPER: ENDPOINT SECURITY

Symantec™ Endpoint Protection

A unified, proactive approach to endpoint security

White Paper: Endpoint Security

Symantec Endpoint Protection

A unified, proactive approach to endpoint security

Contents

Executive summary **4**

An integrated approach to endpoint protection **5**

Simplifying endpoint protection—multiple technologies, one product **6**

Single endpoint protection agent 6

Single, unified management console 7

Lower total cost of ownership 8

Highest level of comprehensive endpoint security **8**

Antivirus and antispyware 8

Network threat protection 10

Proactive threat protection 13

Network access control ready 14

Raising the bar on endpoint security **14**

Summary **16**

Executive summary

Organizations today face a threat landscape that involves stealthy, targeted, and financially motivated attacks that exploit vulnerabilities in endpoint devices. Many of these sophisticated threats can evade traditional security solutions, leaving organizations vulnerable to data theft and manipulation, disruption of business-critical services, and damage to corporate brand and reputation. To stay ahead of this emerging breed of stealthy and resilient security threats, organizations must advance their endpoint protection.

Symantec Endpoint Protection enables organizations to take a more holistic and effective approach to protecting their endpoints—laptops, desktops, and servers. It combines five essential security technologies to proactively deliver the highest level of protection against known and unknown threats, including viruses, worms, Trojan horses, spyware, adware, rootkits, and zero-day attacks. This offering combines industry-leading antivirus, antispyware, and firewall with advanced proactive protection technologies in a single deployable agent that can be administered from a central management console. Also, administrators can easily disable or enable any of these technologies based on their particular needs. Through its seamless and multilayered endpoint protection, Symantec Endpoint Protection delivers:

- **Advanced threat prevention—**Exceeding traditional signature-based file scanning methods, it provides comprehensive endpoint protection against known and unknown threats from inside or outside the organization. Symantec Endpoint Protection provides advanced proactive protection via best-of-breed technologies that automatically analyze application behavior and network communications, with additional tools to restrict high-risk device and application behavior.

- **Simplified, holistic approach to endpoint protection—**The consolidation of essential endpoint security technologies into a single agent makes Symantec Endpoint Protection easy to install, maintain, and update, saving organizations time and money while protecting their assets and business. Its automated security updates provide hassle-free protection from the latest threats. And it gives administrators comprehensive endpoint visibility with its unified management console, which includes graphical reporting, centralized logging, and threshold alerting.

An integrated approach to endpoint protection

The IT threat landscape has changed dramatically over the past few years. In the past, the majority of attacks were meant simply to make headline news. Today, attacks have become more sophisticated and stealthy, targeting specific organizations to reap financial gain. Professional hackers continuously develop new tactics to gain unauthorized, undetected, and ongoing access to an organization's systems and information. One gauge of the growing sophistication of attacks is the appearance of blended threats, which integrate multiple attack methods such as worms, Trojan horses, and zero-day threats.

Antivirus, antispyware, and other signature-based protection measures, which are primarily reactive, may have been sufficient to protect an organization's vital resources a few years ago, but not so today. Organizations now need proactive endpoint security measures that can protect against zero-day attacks and even unknown threats. They need to take a structured approach to endpoint security, implementing a comprehensive solution that not only protects from threats on all levels, but also provides interoperability, seamless implementation, and centralized management.

Symantec Endpoint Protection fulfills this need through its comprehensive and multilayered approach to endpoint protection. It combines Symantec AntiVirus™ with advanced threat prevention to deliver unmatched defense against malware for laptops, desktops and servers from known and unknown malware, including viruses, worms, Trojan horses, spyware, and adware. It even protects against sophisticated attacks that evade traditional security measures such as rootkits, zero-day attacks, and mutating spyware.

Symantec Endpoint Protection delivers more than world-class, industry-leading antivirus and antispyware signature-based protection. It also provides proven proactive technologies that protect endpoints from targeted attacks and attacks not previously seen. It includes turnkey, proactive technologies that automatically analyze application behaviors and network communications to detect and block suspicious activities, as well as administrative control features that allow administrators to deny specific device and application activities deemed to be high risk for their organization. They can even block specific actions based on the user's location.

The multilayered approach of the Symantec solution significantly lowers risks and gives organizations confidence that their business assets are protected. It is a comprehensive product that gives organizations the capabilities they need with the ability to customize the solution according to their needs. Whether the attack emanates from a malicious insider or an external intruder, endpoints are protected.

Simplifying endpoint protection—multiple technologies, one product

To combat the ever-growing threats against their IT infrastructures, administrators understand the importance of endpoint protection technologies. However, this often translates into making sure each endpoint has installed on it an antivirus, antispyware, desktop firewall, intrusion prevention, and device control technology. Deploying these security products individually on each endpoint is not only time-consuming, but it also increases IT complexity and costs. Organizations then need to provide management, training, and support for a variety of different endpoint security solutions. Also, differing technologies can often work against one another or impede system performance due to high resource consumption.

To reduce the complexities and costs associated with deploying and managing multiple solutions, Symantec has consolidated best-in-breed endpoint protection technologies into a single integrated agent that can be administered from a single, unified management console. Symantec Endpoint Protection increases endpoint protection while eliminating the administrative overhead and costs associated with multiple security products. Furthermore, it gives administrators the flexibility to scale their protection over time. They can start with a limited set of protection technologies and then enable additional technologies as needed. Symantec Endpoint Protection can even be configured to work alongside other vendors' technologies, such as desktop firewalls or antivirus solutions. This makes it easy for organizations to implement and configure the solutions that they need to address their requirements.

Single endpoint protection agent

Unlike competing solutions, Symantec Endpoint Protection integrates antivirus, antispyware, firewall, device control, and state-of-the-art intrusion prevention into a single agent that empowers organizations to customize the level of endpoint protection with technologies that work together. Symantec Endpoint Protection requires less memory and consumes fewer resources, while increasing protection. Also, administrators can tune the agent to maintain endpoint performance, so that it uses fewer resources during periods of high user activity.

The consolidation of capabilities into a single endpoint security agent enables operational efficiencies such as a single communication method and content delivery system across all of its security technologies. Service configuration and exclusions can be performed globally at a single point on the client or at the management server. Furthermore, automated security updates to the agent provide hassle-free protection from the latest threats.

Symantec Endpoint Protection provides a single, simplified user interface on the client. Administrators can customize the interface, allowing them to decide which technologies can run at the client and which configuration options will not be available to the end user. Administrators also have the option to completely hide the interface from users. These features give administrators flexibility and control to protect endpoint devices in a manner that meets their organization's unique requirements. Also, features and options can be easily turned on or off by the administrator at any time.

Single, unified management console

The ability to manage all of the services provided by Symantec Endpoint Protection from a single, unified console enables administrators to take a holistic approach to endpoint security management. With the Symantec Endpoint Protection Manager, console administrators can create and manage policies, assign them to agents, view logs, and run reports for endpoint security activities. It provides comprehensive endpoint visibility through graphical reporting, centralized logging, and threshold alerting. The unified console simplifies endpoint security administration and enables operational efficiencies, including centralized software updates, policy updates, reporting, and licensing maintenance.

The console's enterprise-class management architecture can scale to meet the most demanding environments. It can provide granular control over administrative tasks, while simplifying and unifying management efforts to reduce total cost of ownership. Its flexible management structure allows different administrators to be granted different levels of access to the management system based on their roles and responsibilities. It also supports the import of Organization Units from Active Directory and works with leading software deployment tools such as SMS to further enhance administrators' management capabilities.

Unlike competing solutions, this multilayered approach to endpoint security offers proven world-class protection in a single agent deployment that significantly lowers risks without added resource overhead so that organizations can efficiently manage security and gain confidence that their corporate assets and business are protected.

Lower total cost of ownership

By offering the benefit of essential endpoint security technologies in one, Symantec Endpoint Protection lowers total cost of ownership, enabling organizations to reduce administrative overhead and the costs associated with managing multiple endpoint security products. It also leverages existing IT investments.

- **Reduces administrative overhead—**Reduces head count and hours associated with managing multiple point solutions
- **Reduces costs—**Reduces the effort associated with managing endpoint security, user and network downtime, and remediation efforts
- **Leverages existing IT investments—**Works with leading software deployment tools, patch management tools, SIM tools, databases, and operating systems

Highest level of comprehensive endpoint security

Symantec Endpoint Protection seamlessly combines best-in-breed protection mechanisms into a single agent to deliver the highest level of comprehensive endpoint security:

- Antivirus/antispyware
- Network threat protection
- Proactive threat protection

In addition, Symantec Endpoint Protection is network access control ready. The agent can be enabled to provide network access control capabilities that allow organizations to ensure endpoints comply with corporate security policy before gaining access to the network. Symantec Endpoint Protection eliminates the need to deploy additional network access control software on an organization's endpoint devices.

Antivirus and antispyware

Antivirus and antispyware solutions generally employ traditional scan-based technologies to identify viruses, worms, Trojan horses, spyware, and other malware on an endpoint device. Typical antivirus and antispyware solutions detect these threats by searching the system for files that match characteristics, or threat signatures, of a known threat. Once it detects the threat, the solution remediates it, typically by deleting or quarantining it. For many years, this methodology

has been effective for protecting endpoints against known threats. Although it's inadequate for protecting against unknown and zero-day threats, it is still an essential element of overall endpoint security.

With the industry's increased attention on endpoint security, a variety of products have recently entered the antivirus and antispyware market. While many of these first- and second-generation solutions provide a level of protection, they often fall short of full protection. Many technologies only work on one operating system. Others lack the ability to interoperate with other essential endpoint security technologies, such as personal firewall, device control, and intrusion prevention.

The quality and level of protection provided by Symantec Endpoint Protection rivals that of competing solutions. Symantec Endpoint Protection provides higher levels of real-time protection than other first-generation and packaged solutions, and Symantec outperforms many long-time security solution providers. For example, since 1999 Symantec is the only vendor to obtain over 30 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. According to AV-Comparatives, the polymorphic test determines the flexibility of an antivirus scan engine, as well as how good it is at detecting complex viruses. AV-Comparatives also considers any polymorphic test score below 100 percent as failed or not reliable detection since even one missed replicant can cause a reinfection.

A study conducted by Thompson Cyber Security Labs in September 2006 showed that Symantec provided superior rootkit detection and removal over competing vendors. Rootkits are stealth applications or scripts that a hacker uses to gain an undetectable presence on a system, which also provides the hacker administrator-level access to that system. Ready-to-use rootkit applications are widely available on the Internet, giving inexperienced hackers the ability to use a rootkit without having to understand how it works. Rootkits are often used to collect confidential information such as user IDs, account numbers, and passwords. To detect and remove rootkits, a thorough analysis and repair needs to be performed on an operating system. Toward this end, Symantec Endpoint Protection includes Veritas Raw Disk Scan to provide a deeper inspection into the file system than any other solution, enabling the analysis and repair necessary to remove even the most difficult rootkit attacks.

Furthermore, Symantec Endpoint Protection is backed by the Symantec Global Intelligence Network—an integrated service that provides organizations with the critical intelligence they need to reduce security risks, improve regulatory compliance, and strengthen their overall security posture. Symantec Global Intelligence Services provide insight into the latest global, industry, and local threats and attacks so an organization can respond proactively to emerging threats. Through a combination of early threat warning notifications and Symantec Managed Security Services, Symantec Global Intelligence Services delivers real-time analysis of malicious activity against an entire enterprise, helping organizations protect their critical information assets.

Network threat protection

Network threat protection on endpoints is critical to protect from blended threats and to inhibit outbreaks. To be effective, it must encompass more than a firewall. Network threat protection should include a blend of state-of-the-art protection technologies, including intrusion prevention and sophisticated capabilities to control network communications.

In the past, security experts debated whether firewalls needed to be placed only on the perimeters of an organization's network or on individual desktops as well. With the current threat landscape and the mobile workforce extending the perimeters of organizations' computing infrastructures, endpoints have become a primary target for exploits and attacks. A threat often first infects a single laptop while outside the network perimeter, and then when the laptop connects to the internal network, the threat spreads to other endpoints. Endpoint firewalls can be leveraged not only to block internal network attacks from breaching any endpoint connected to the network, but also to prevent these threats from ever leaving the initially infected endpoint.

The Symantec Endpoint Protection endpoint security agent incorporates a best-in-breed firewall solution that combines features of the Symantec client firewall and the Sygate™ firewall. These include:

- Rule-based firewall engine
- Predefined antivirus, antispyware, and personal firewall checks
- Firewall rule triggers on applications, host, services, and time
- Full TCP/IP support (TCP, UDP, ICMP, Raw IP Protocol)
- Option to allow or block support of network protocols, including Ethernet, Token Ring, IPX/SPX, AppleTalk, and NetBEUI

- Ability to block protocol drivers such as VMware and WinPcap
- Adapter-specific rules
- Ability to inspect encrypted and clear text network traffic
- Packet and stream intrusion prevention system (IPS) blocking, custom IPS signatures blocking, and generic exploit blocking for proactive threat protection
- Self-enforcement for network access control

Intrusion prevention plays a critical role in the solution's network threat protection scheme, especially if the intrusion is vulnerability based using generic signatures. Vulnerability-based intrusion prevention systems can use one generic signature to block the hundreds of potential exploits that attack a vulnerability—halting the attack at the network layer so it never has a chance to infect an endpoint.

While traditional IPS solutions can detect a specific, known exploit, they are inadequate for protecting published software vulnerabilities from the barrage of exploit variants that dominate today's threat landscape. According to the Internet Security Threat Report (ISTR Vol XI), it takes 47 days on average for an operating system or application provider to release a patch for a published vulnerability. 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 windows of opportunity for sophisticated attackers. Considerable damage can be inflicted on an organization with the first wave of exploits that occurs before the release of an exploit signature. Even after the exploit signature is released, it will prove ineffective against variants of that exploit that may be polymorphic or self-mutating. Furthermore, these reactive, exploit-based signatures cannot protect against yet-to-be-seen, unreported, or unknown threats, such as stealthy exploits targeted at specific companies that often go undetected. To combat mutating and unseen threats, more proactive measures in the form of a vulnerability-based IPS are required.

While an exploit-based signature detects only a specific exploit, a vulnerability-based signature operates at a higher level, detecting not only a specific exploit for a vulnerability, but 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 operating system or application vendors announce new vulnerabilities that can potentially place organizations at great risk, Symantec engineers study the characteristics of that vulnerability and create and release a generic signature based on that study. This helps protect organizations before exploits begin to surface.

The power of vulnerability-based intrusion prevention derives from the fact that a single vulnerability definition is not only protecting against one type of threat, but perhaps hundreds or thousands (see table). Since it looks for vulnerability characteristics and behavior, it can protect against a wide range of threats, even those that are not yet known or developed.

Generic exploit blocking protects against thousands of exploit variants.

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

Vulnerability-based protection is also useful for protecting against exploits that target a specific business or organizations. Targeted attacks are generally stealthy, since their goal is not to be discovered while they steal confidential information and then erase themselves from the system. As a result, there is no way to create an exploit signature for these targeted exploits, since organizations have no way of knowing about them until the damage is done. Vulnerability-based protection 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, blocking yet-to-be-seen exploits or exploit variants from

entering and infecting the endpoint. Since they don't have a chance to infect the endpoint, they don't do damage or need to be remediated.

Symantec Endpoint Protection also gives administrators the ability to create custom intrusion prevention signatures. This allows them to define rule-based signatures, tailored to the needs of their unique environment and custom applications. Signatures can be created that block a few specific actions or more complex actions. By eliminating the need to wait for an operating system or application vendor to create patches for known vulnerabilities, Symantec Endpoint Protection provides administrators with comprehensive, proactive control over the security and protection of their endpoints.

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. These are referred to as proactive threat protection technologies.

Symantec Endpoint Protection includes Proactive Threat Scan, a proactive threat protection technology that protects against the multitude of variant and yet-to-be-seen threats that exploit known vulnerabilities. Its unique host intrusion prevention capabilities empower organizations to protect themselves against unknown or zero-day threats. Proactive Threat Scan is based on heuristics technology that analyzes the behavior of processes running in a system to detect potential threats. Most host-based IPSs only examine what they consider to be "bad behavior." As a result, they 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 of applications, providing more accurate threat detection and significantly reducing the number of false positives. As a result, Symantec Endpoint Protection allows organizations to detect unknown threats that cannot be detected by any signature-based technology.

Symantec Endpoint Protection also incorporates device and application control capabilities that allow administrators to deny specific device and application activities deemed as high risk, enabling organizations to block specific actions based on the location of the user. Device control technology allows administrators to determine and control what devices are allowed to attach to an endpoint. It can lock down an endpoint, for example, preventing thumb drives, CD burners,

printers, and other USB devices from connecting to the system to keep confidential data from being copied from the system. Its ability to block device connections can also help prevent endpoints from being infected by viruses spread from these types of devices and others.

Application control technology 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 DLL control. This advanced capability is useful for administrators who want to restrict certain activities deemed as suspicious or high risk.

Network access control ready

The endpoint security agent in Symantec Endpoint Protection is network access control ready, meaning that network access control technology has been integrated into the agent and can be easily enabled through the purchase of a Symantec Network Access Control license. So when Symantec Endpoint Protection is deployed, no additional agent software needs to be deployed on the endpoint device to implement network access control.

When network access control is enabled through the purchase of an additional license, it controls access to corporate networks, enforces endpoint security policy, and easily integrates with existing network infrastructures. Regardless of how endpoints are connected to the network, Symantec Network Access Control discovers and evaluates endpoint compliance status, provisions the appropriate network access, provides automated remediation capabilities, and continually monitors endpoints for changes in compliance status. Additionally, to simplify and streamline management, administrators manage all functionality using the same management console for Symantec Endpoint Protection and Symantec Network Access Control.

Raising the bar on endpoint security

Symantec Endpoint Protection raises the bar on comprehensive and secure endpoint security that delivers advanced threat prevention and is easy to manage. It's the only endpoint security solution to offer the benefits of essential best-in-breed technologies in one integrated agent that can be administered from a single management console and is network access control ready.

Symantec believes that effective endpoint security requires endpoint protection technologies to be coupled with endpoint compliance technologies. Accordingly, Symantec Endpoint Protection (endpoint protection) is tightly integrated with Symantec Network Access Control (endpoint compliance), enabling organizations to take a more holistic approach to endpoint security. These offerings interoperate seamlessly to provide a comprehensive and unified multilayered

endpoint security solution that enables IT administrators to strike a balance between end-user productivity and security, while simplifying endpoint security administration (see Figure 1).

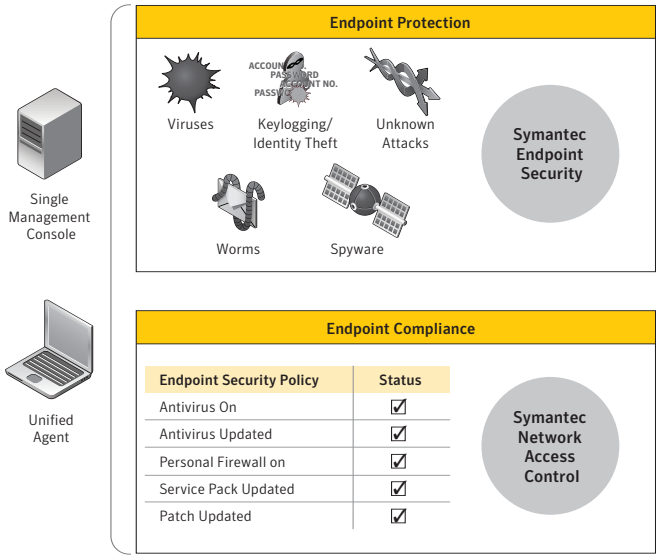

Figure 1. Symantec's approach to endpoint security

Organizations that have deployed other market-leading security offerings from Symantec can realize increased system protection, simplified management, and cost savings by taking advantage of this integrated endpoint security offering. And to make it easier to realize the benefits of Symantec Endpoint Protection, Symantec provides existing customers with a full range of services and offerings to facilitate the move to this latest offering, including a wizard to migrate policies from Symantec AntiVirus™, best practices guides, knowledge base articles, and online training.

Engineered to operate with an organization's existing security and IT investments, Symantec Endpoint Protection is easy to implement and deploy. But to help speed the return on an organization's investment, Symantec also provides a full range of consulting, technical education, and support services that help maximize the benefits and capabilities inherent in Symantec Endpoint Protection.

To provide customer assistance and guidance on how best to deploy, manage, and maximize the benefits and features provided by Symantec Endpoint Protection, Symantec Enterprise

Support Services offers three levels of protection designed to meet the needs of organizations ranging from small businesses to large enterprises. Symantec Education has a portfolio of training courses designed to get users and administrators up to speed quickly. The Symantec Consulting Service starts with antivirus deployment and migration assistance. Symantec can also provide a Residency Service, in which Symantec consultants work side by side with customers' IT staff, or an Operational Service, in which the entire endpoint security function can be outsourced to Symantec, the security experts.

Summary

To combat the sophisticated, stealthy, and targeted attacks that plague today's threat landscape, organizations can no longer rely solely on traditional antivirus and antispyware solutions. Effective endpoint security requires organizations to implement additional layers of security that can proactively protect against zero-day threats. They need to take a holistic approach to endpoint security that effectively protects their organization from threats at all levels, while providing seamless interoperability that simplifies management and lowers total cost of ownership.

Symantec Endpoint Protection delivers an unmatched, comprehensive, and integrated endpoint security solution that serves as a foundation for secure endpoint computing. It combines essential best-in-breed security technologies to deliver advanced threat prevention from known and unknown threats. It increases protection and reduces the administrative overhead and costs associated with managing multiple endpoint security products by providing a single agent that is administered via a single management console. As a result, this seamless and multilayered endpoint protection simplifies security administration, saving organizations time and money while protecting their assets and business.

Symantec is a global leader in infrastructure software, as well as endpoint security, enabling businesses and consumers to have confidence in a connected world. It offers the industry's deepest portfolio of security solutions to help organizations protect endpoint systems and corporate information from a broad spectrum of internal and external security risks. Symantec helps organizations protect their infrastructure, information, and interactions by delivering software and services that address risks to security, availability, compliance, and performance.

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.

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

Copyright © 2007 Symantec Corporation. All rights reserved. Symantec, the Symantec Logo, Sygate, and Symantec AntiVirus are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners. Printed in the U.S.A. 05/07 12516469