

Endpoint Security for Enterprises

In this review:

- **McAfee Total Protection for Enterprise (page 5)**
- **Sophos Endpoint Security and Control 7.0 (page 7)**
- **Symantec Endpoint Protection 11.0 (page 10)**

Most medium and large enterprises already recognize that they need more than traditional anti-virus software to keep their notebooks, desktops, and servers secure. McAfee, Sophos, and Symantec have all released new endpoint security suites that integrate several endpoint security technologies and include significant changes from prior versions. This changing landscape of products from the major vendors gives companies a chance to re-evaluate their endpoint security choices taking into account how these new products match up with the company's requirements. No matter which direction they go, companies are in for some major changes and a migration effort to one of the new products.

Given that most companies assess their endpoint security on an annual or bi-annual basis due to existing contracts, these recent changes will impact product selection inside organizations over the next couple of years.

Endpoint security is so important because corporate networks no longer have a clearly delineated perimeter where a secure boundary can thwart attacks. Wireless users come and go.

Notebook users connect their machines to insecure networks at home and on the road, putting them at risk when they are completely unprotected by corporate perimeter security devices. These same notebooks connect back

“In a very practical sense, companies must rely on their endpoint security vendors to build products that provide effective protection right out of the box.”

to the corporate network over virtual private networks (VPNs) or are simply reconnected to the corporate network when an employee returns to work. Without proper protection, these laptops can be carriers of malware. At the same time, desktops are under attack from harmful content masquerading inside download bundles, exploits found on Web sites,

“In our testing, Sophos clearly beat McAfee and Symantec in detecting threats that included a large percentage of day-zero malware.”

and new threats that ride in on e-mail and instant messaging applications. Endpoint security software on file and application servers can protect these

critical computers as well as scan the content that resides on them.

Given the ever-changing landscape of old and new (day-zero) threats, medium and large enterprises must enter into a close marriage with their chosen endpoint security suite. The anti-virus, anti-spyware, and host intrusion protection components in these suites present the last (and sometimes only) line of defense against increasingly sophisticated threats.

Handling New Threats

New and more sophisticated threats are appearing everywhere on the Internet. E-mail messages continue to bring in harmful content. Even though many companies do restrict attachments, these threats can be carried in embedded HTML or pointed to through links included in the e-mail. Web sites, either intentionally or through hacks, can contain harmful downloads and exploits. For example, many of the social networking sites have fallen prey to malware that can find its way onto your corporate endpoints. The new Storm worm and all of its variants have received a lot of press and represent a new type of blended threat that organizations must address.

To assess these new types of threats, we turned up the heat on endpoint security products, testing each of them with a number of common security threats including Storm and its variants and a large variety of day-zero attacks including targeted exploits. To perform our assessment of these new threats, we installed and enabled all behavioral

RATINGS TABLE			
Category	McAfee Total Protection for Enterprise	Sophos Endpoint Security and Control 7.0	Symantec Endpoint Protection 11.0
Installation & Deployment	▲▲	▲▲▲▲	▲▲▲
Usability & Management	▲▲▲	▲▲▲▲	▲▲▲
Visibility	▲▲▲▲	▲▲▲▲	▲▲▲▲
Effectiveness (Basic)	▲▲▲▲	▲▲▲▲	▲▲▲
Effectiveness (Day-Zero)	▲▲▲	▲▲▲▲▲	▲▲▲
Performance	▲▲▲	▲▲▲▲	▲▲▲
OVERALL	▲▲▲	▲▲▲▲	▲▲▲
Quick Summary	McAfee Total Protection for Enterprise provides innovative features around Active Directory synchronization and a solid reporting engine, but remains complex and demonstrated poor day-zero protection.	Sophos Endpoint Security and Control is an exceptionally well-designed product. A natural choice for enterprises looking for a well-integrated endpoint security suite that is effective against day-zero threats out-of-the-box.	Symantec Endpoint Protection 11.0 has much-improved management and integration over previous versions but we found its day-zero or behavior-based capabilities lacking. Users will also face a difficult migration from previous versions.
Technical Support	24/7	24/7	Business Hours (24/7 license upgrade available)

Key: ▲ - Poor ▲▲ - Fair ▲▲▲ - Average ▲▲▲▲ - Good ▲▲▲▲▲ - Excellent

detection in the products but did not make any attempt to create more-involved HIPS-based rules. Gone are the days when you can judge a product's effectiveness based on its signature database – the environment is changing too fast now, and the products are up against real-time challenges.

As in previous testing, we were able to find many examples of malicious software or potentially unwanted applications that were not found in the vendors' signature databases. This allowed us to tax their behavioral capabilities. The products differed greatly in how they blocked threats and the points at which they blocked them.

Of course, from our standpoint, the sooner a threat is blocked the better. Ideally, a threat would be blocked on-access (pre-execution). For most

“The Sophos management interface remains more intuitive than both Symantec and McAfee, and its new Active Directory synchronization worked well in our testing.”

adware and some newer threats, however, the products we tested often didn't take action until an installation (on-execution) or an attack had already begun. In cases where detection via signatures or patterns was ineffective, we monitored the ability of each product to use behavioral techniques to prevent or mitigate damage. Finally, we performed on-demand scans after

the fact (post-execution) to give the products one last chance to detect and stop the threats.

The Ideal Security Suite

It's simple: the ideal endpoint security suite should provide complete protection with minimal management.

- It should be invisible to both administrators and end users until it is needed.
- The administrator should have the ability to implement security policies through an intuitive interface, and once configured, the product should sit in the background watching for malicious binaries and behaviors without negatively impacting end-user performance.
- Each and every threat should be handled either through a match in the signature database or by other protection designed to handle variants and new threats based on their patterns or behaviors.
- The product should notify the administrator when necessary about computers that need attention and about the threats it has uncovered.

In other words, the ideal endpoint security suite should take ownership of the endpoint security problem and not overly complicate the life of the security administrator or end-user. Security is a complex topic and our philosophy is that the products you pay for should handle this complexity behind the scenes whenever possible. But it's not just idealism; it's a practical consideration for most companies. Most organizations have neither the expertise nor the budgets to outthink or stay ahead of the bad guys. In a very practical sense, companies must rely on their endpoint security vendors to build products that provide effective protection right out of the box.

The Suites We Reviewed

Cascadia Labs evaluated how three leading enterprise endpoint security products fared in meeting enterprises' needs.

USABILITY RESULTS - Comparison of steps & time to perform important tasks

Activity	McAfee	Sophos	Symantec
Install the product and deploy to 10 endpoints using NetBIOS	115 Steps 38 min 35 sec	39 Steps 20 min 43 sec	53 Steps 23 min 35 sec
Install the product and deploy to 10 endpoints using Active Directory	115 Steps 37 min 50 sec	41 Steps 20 min 39 sec	Feature Not Available
Identify an out-of-date endpoint	1 Step 3 sec	0 Steps Immediate	6 Steps 30 sec
Identify an endpoint out-of-compliance with policy	Feature Not Available	0 Steps Immediate	4 Steps 23 sec
Identify an unprotected endpoint	Feature Not Available	8 Steps 12 sec	6 Steps 48 sec
Create a new policy to detect and block all PUAs	16 Steps 40 sec	11 Steps 16 sec	11 Steps 24 sec
Identify an endpoint that missed a scan or identify last successful on-demand scan	9 Steps 43 sec	2 Steps 4 sec	7 Steps 22 sec
Generate a report of all malware detections in the past 24 hrs for a single endpoint	15 Steps 1 min 10 sec	5 Steps 15 sec	7 Steps 17 sec
Schedule a full system scan, including checks for potentially unwanted applications (PUAs)	27 Steps 1 min 30 sec	9 Steps 20 sec	15 Steps 38 sec
Scan a single system and then authorize a single PUA for all endpoints (scan time not included)	38 Steps 2 min 45 sec	6 Steps 30 sec	6 Steps 9 sec
Authorize a list of 3 PUAs for all endpoints	14 Steps 1 min 20 sec	12 Steps 40 sec	22 Steps 1 min 18 sec
Protect 5 new endpoints	16 Steps 21 min 35 sec	14 Steps 1 min 2 sec	10 Steps 1 min 21 sec
Protect 5 new endpoints automatically using Active Directory	20 Steps 1 min 47 sec	11 Steps 33 sec	Feature Not Available
Authorize outbound Internet access for an application for a management group	18 Steps 1 min 25 sec	6 Steps 10 sec	16 Steps 44 sec
Block execution of well known consumer P2P, VoIP, IM and toolbar applications for a group	27 Steps 1 min 12 sec	6 Steps 16 sec	46 Steps 1 min 57 sec
Configure signature/engine updating frequency	6 Steps 16 sec	11 Steps 37 sec	7 Steps 28 sec

The packages, from McAfee, Sophos, and Symantec, all integrate protection against viruses, spyware, adware, and day-zero threats. We did not include products or components that each

company also offers to scan incoming and outgoing messages at the mail server in this evaluation.

McAfee Total Protection for Enterprise

includes the new ePolicy Orchestrator 4.0 (ePO) with an overhauled user interface and an administrator-configurable dashboard along with a new 7.0 version of its Host Intrusion Prevention client.

Sophos Endpoint Security and Control 7.0 maintains its simplicity of design but now has new application control and improved day-zero capabilities.

Symantec Endpoint Protection 11.0 finally has an integrated management console and includes new advanced threat protection.

Our Findings

Our testing uncovered some major differences in effectiveness from previous tests, which perhaps isn't surprising given the overhauls in the Symantec and McAfee products. Sophos Endpoint Security and Control, which changed visibly the least, showed some very impressive results in handling day-zero threats indicating to us that substantial work has clearly been going on at its core.

For common, well-known malware, all the products performed as expected – catching nearly all of the viruses, Trojans and spyware we threw at them before execution. As we've found in previous tests, bundled adware was typically not blocked until or after execution.

However, we found very interesting results with newer threats. In our testing, Sophos clearly beat McAfee and Symantec in detecting threats that included a large percentage of day-zero malware. Sophos detected 86 of our 100 malware samples prior to execution compared to 43 and 51 for McAfee and Symantec respectively. Much of this success can be attributed to the Sophos pre-execution HIPS capabilities including its Behavioral Genotype Protection. Its run-time HIPS protection also caught 11 more samples at execution through detection of malicious registry, process, and

PERFORMANCE RESULTS - Comparison of scanning performance

Task	McAfee	Sophos	Symantec
Scan of c: drive (No infections)	7 min 33 sec	6 min 50 sec	7 min 49 sec
Scan of c: drive (second run showing impact of caching)	7 min 19 sec	3 min 26 sec	6 min 52 sec
Scan of c: drive (infected with adware)	9 min 12 sec	7 min 38 sec	11 min 9 sec
On-Access Scan of specific folder (contains 3443 files totaling 450 MB with no zip files and no infections)	1 min 37 sec	1 min 26 sec	1 min 33 sec

file system modifications. Finding 97 out of our 100 fresh threats overall is impressive compared to the 82 and 58 caught by Symantec and McAfee respectively.

We were disappointed with McAfee's effectiveness. It only caught 43 of our 100 files pre-execution. Although 28 of these were caught with signatures, McAfee's pattern-based recognition and other pre-execution capabilities couldn't keep up with Sophos. McAfee caught 13 more malware samples at execution but none of these could be attributed to its run-time HIPS capabilities. It should be possible to improve McAfee's protection by configuring HIPS rules, but it takes a lot of expertise and time to configure the rule-based HIPS and we conducted our testing with basic HIPS settings in place.

Like McAfee, Symantec did not fare

that well in protecting against the new threats we threw at it. It caught 51 of these new threats pre-execution using specific signatures or generic pattern signatures but didn't show any effective HIPS or behavior-based protection in real-time. Symantec's new Proactive Threat Scan is included to bring additional protection against some malware, but it only runs hourly by default. This default configuration leads to a window of vulnerability where malware is not detected and can inflict damage. Although Proactive Threat Scan can be configured to run when a process starts, it places a heavy burden on the system according to Symantec's documentation and confirmed in our testing. Symantec did play catch up in detecting 18 more threats post-execution bringing its total to 82. Overall, we found Symantec's protection to often come too late in the cycle.

The Sophos management interface remains more intuitive than both Symantec and McAfee, and its new Active Directory synchronization worked well in our testing. McAfee ePO 4.0 has a new look and feel, and we liked the ability to create our own custom dashboards. This is a big improvement in visibility over the previous version of ePO. However, the tie between view and do is still absent, and we found ourselves constantly wishing we could more easily take action on information that was presented to us. Policy configuration remains complex. Symantec has made major improvements in its management tools. Prior to this version, Symantec required multiple consoles for policy management, but Endpoint Protection brings those together although other servers and consoles are still used for quarantine and updates. And although Symantec users will face a difficult migration given major foundational changes in the product, policy management is much improved over prior versions.

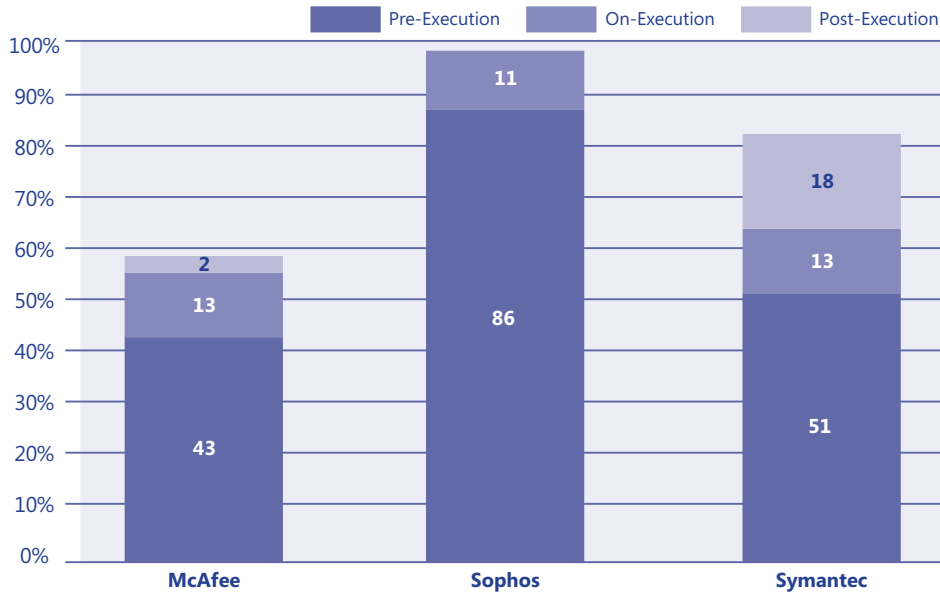
The Verdict

With major changes afoot in the endpoint security arena, Sophos has emerged in our tests as the best choice out-of-the-box for handling day-zero attacks. Coupled with its intuitive policy and management interface, Sophos is an excellent choice for most companies. McAfee's flexible Active Directory synchronization, strong reporting capabilities, and uber-configurable product might fit the bill for very large enterprises with the time and expertise to combat its complexity. Symantec has made a major leap forward with an improved and integrated policy management interface but didn't provide sufficient day-zero protection in our testing. It's clear to us that the products were born out of different philosophies: McAfee provides a lot of granular capabilities that can be useful to highly qualified security experts; Symantec seems to favor application lock-down to mitigate against day-

EFFECTIVENESS RESULTS - Common Threats

Task	McAfee		Sophos		Symantec	
	Virus/Spyware	Adware	Virus/Spyware	Adware	Virus/Spyware	Adware
Pre-Execution	8	2	9	0	9	2
On-Execution	0	3	0	2	0	0
Post-Execution	1	0	1	3	0	3
Total Detected	9	5	10	5	9	5
Total Undetected	1	0	0	0	1	0

EFFECTIVENESS RESULTS - 100 New Threats



Catching threats before execution provides the best protection for endpoints.

zero threats; while Sophos strives to minimize configuration and handle day-zero threats right out of the box. While no single viewpoint works for all companies, our report should provide enough insight in helping you choose the right product and philosophy for your enterprise.

and basic usability and management features are clearly more complicated than those of Sophos and Symantec. In our effectiveness testing using default configurations, although McAfee had decent signature-based detection rates,

its day-zero protection was very poor. Some of this poor performance can be attributed to the need to configure rules when using its run-time HIPS configuration, a difficult and time-consuming task for even seasoned security administrators.

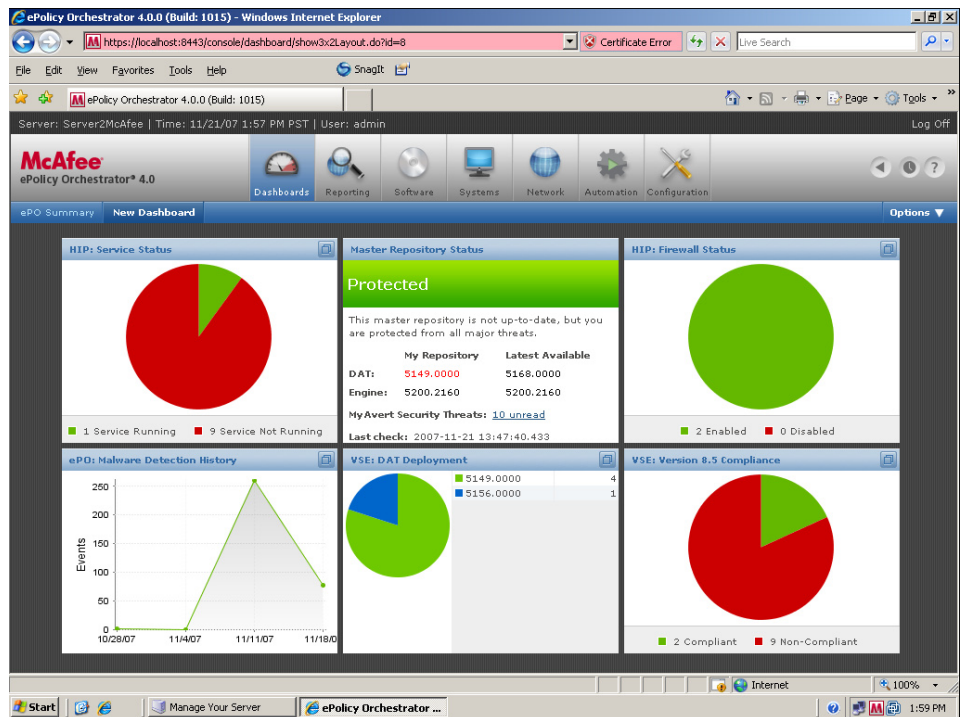
Getting Started

Installing McAfee Total Protection for Enterprise is an arduous, time-consuming task. The offering actually comprises a number of different McAfee products that must be checked into the management server separately. In the end, the McAfee installation process took 115 steps and more than twice as long as the 41 steps necessary for Sophos deployment. We installed the ePO server, VirusScan Enterprise 8.5i (the anti-virus client), AntiSpyware Enterprise Module 8.5 (an add-on to the anti-virus client), and Host Intrusion Prevention 7.0 (a separate desktop firewall, HIPS, and application control component). Additional tasks must also be created to acquire and push out the most current patches and signature updates.

McAfee Total Protection for Enterprise

McAfee Total Protection for Enterprise is a comprehensive suite targeted at very large enterprises. Its flexible Active Directory support, robust reporting engine, and multi-server database roll-up features are useful for companies with thousands of users and multiple locations. The most recent version includes a significant change to the management console, ePolicy Orchestrator 4.0 (ePO 4.0), that incorporates several improvements including a user-configurable dashboard built around McAfee's reporting engine.

However, as with previous versions, McAfee's installation, deployment,



The McAfee ePO dashboard lets administrators customize six panels leveraging the same robust query building system used to generate reports.

On a positive note, McAfee ePO provides robust Active Directory synchronization. Administrators have the unique option of choosing whether to mirror their AD structure exactly or to create a different management structure more amenable to their security policy. This capability should be especially valuable in large network environments where the AD structure may not be the most logical way to manage protection.

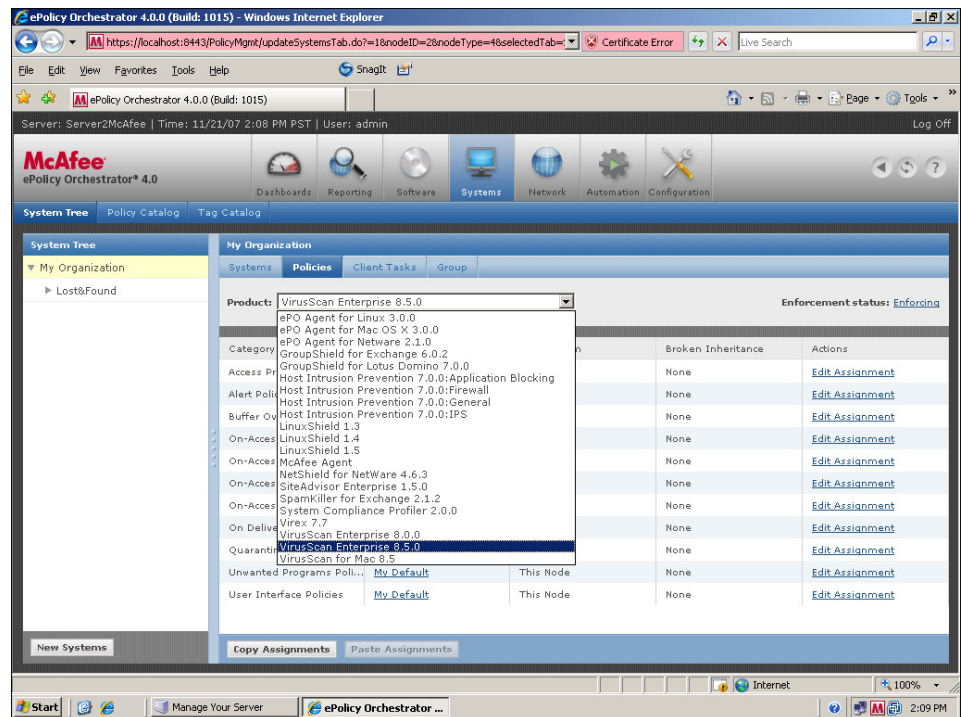
McAfee Total Protection for Enterprise provides support for Windows XP, Windows 2003, Windows 2000, Windows NT 4.0, and NetWare. McAfee does offer products for Macintosh and Linux, but they are separate purchases, and only basic settings can be managed via ePO.

Migration

Upgrading from ePO 3.6 is very similar to performing a new installation and involves many of the same tasks. Administrators must back up their existing reporting databases before upgrading to ePO 4.0 and must perform the policy migration and upgrade tasks in the proper order. For example, administrators must upgrade from HIP 6.x to HIP 7.0 in the ePO 3.6 environment and run the included migration utility before upgrading to ePO 4.0 because migration from HIP 6.x to HIP 7.0 is not supported on ePO 4.0. Following the upgrade to ePO 4.0, the current version of the McAfee agent must be manually checked into the master repository and deployed with a client task. Unlike a first-time installation, the most current agent is not checked in automatically.

Usability and Management

The ePO console is the central administration point for the Total Protection suite. ePO's configurable dashboard, which ties directly into McAfee's powerful reporting engine, allows administrators to configure six different panels that can display the output from any query they can perform within the reporting engine.



Policy creation and management is complicated by the need to configure separate settings for each product and OS, and the need to navigate multiple configuration screens for a single product.

Administrators also use ePO to deploy agents, manage policy configuration, automate tasks, and generate reports.

Common actions such as scheduling updates to endpoints, generating reports, and distributing policy configurations across the network are spread across seven distinct sections: Dashboards, Reporting, Software, Systems, Network, Automation, and Configuration. In testing, we found the ePO console to be far more difficult to use than either the Sophos Enterprise Console or the Symantec Endpoint Protection Manager console. This is primarily due to a distinct separation between the process of gathering information and taking actions and the frequent need to navigate several layers deep into a section to locate and change the desired settings.

McAfee does a good job of exposing an inheritance model to deploy policy settings across different groups in the enterprise, and it provides the most granular set of configuration options for deploying products. This can be useful in the right hands. On the

other hand, the policy configuration information is presented in a confusing manner. For example, policies are distinct for products and OSs and are often further subdivided into separate feature pages. For example, VirusScan Enterprise 8.5i has 11 different policy categories to manage, Host Intrusion Prevention 7.0 has 12 different policy categories, and many categories have multiple pages of features to navigate through, which makes policy management daunting.

McAfee continues to provide the strongest reporting capabilities of the products reviewed. A large number of canned reports are available, and administrators can use the Query Builder to create and save reports on an almost limitless range of data. Each graphical chart links to a customizable and drillable table. While the reporting interface was somewhat difficult to use, properly configured queries are easily saved and can be scheduled to run automatically.

Effectiveness

The McAfee product was the least effective overall in protecting against the malware threats used in our testing.

We found mixed results in its detection of common threats. The on-access scanner detected most common viruses and spyware and blocked adware better than the other products, but it let a recent Storm worm variant install a rootkit on the client, and the anti-virus engine failed to terminate the malicious process it detected. McAfee was the only product that completely missed detecting a Trojan dropper, even after restarting the infected machine and completing an on-demand scan. It was late in its detection and blocking of a Trojan Keylogger during installation that Sophos and Symantec deleted during the on-access scan. On the positive side, it was the only product to catch and quarantine one of our adware applications during the install process.

With VirusScan Enterprise, AntiSpyware module, and the Host Intrusion Prevention client installed, it detected or blocked only 43 out of a possible 100 newer threats pre-execution – much lower than the 86 by Sophos and somewhat lower than the 51 by Symantec. More surprising was the complete lack of effectiveness of McAfee's run-time HIPS component when we executed the malware. The results would presumably be better upon configuring its run-time HIPS but this process requires a lot of expertise to at once block threats and avoid false positives. The McAfee Host Intrusion Prevention client bundles a firewall with both signature-based and behavioral-based system monitoring and provides application control features. During our testing the default firewall configuration did provide some mitigation by blocking the download of additional malicious code from remote hosts and in preventing spamming.

McAfee provides application blocking capabilities to prevent the execution of unwanted client

applications, but McAfee's approach to application blocking requires multiple disconnected steps compared to Sophos' simple approach. McAfee requires administrators to configure each executable separately, while Sophos allows administrators to block applications by selecting from a database of legitimate applications.

During our performance tests, McAfee lagged somewhat behind Sophos. The scanning engine was generally slower in completing on-demand scans and was the only product that does not include caching features, so a second-pass run took essentially the same amount of time as the first one. McAfee's client memory usage was about 75MB in our testing.

McAfee, just like Symantec, delivers malware definition updates on a daily basis. However, McAfee was the only product in our tests that did not receive definition updates during weekends of the test period.

Conclusion

The McAfee Total Protection for Enterprise suite provided less than adequate out-of-the-box endpoint protection in our testing but does give a wide range of configuration options for enterprises. Companies with dedicated security teams and very specific policy requirements may find the McAfee solution compelling, but companies looking to simplify their overall security approach will likely find the McAfee environment daunting.

Sophos Endpoint Security and Control 7.0

Sophos Endpoint Security and Control is a well-designed security package that combines effective multi-layered endpoint protection with exceptional manageability and ease of use. Its straightforward installation process, along with its intuitive user interface and management dashboard, makes

the process of deploying and managing endpoint security easy and painless. It also performed exceptionally well in our effectiveness tests by blocking more new and unknown threats than the McAfee and Symantec products. On the downside, we found the Sophos reporting capabilities fairly minimal compared to those of the other products in this review.

Getting Started

We found Sophos Endpoint Security and Control to be far easier to install than both Symantec and McAfee. All of the Sophos capabilities are bundled together in a single, well-integrated package that made installation and configuration quick and painless. It took just over twenty minutes to install and deploy Sophos Endpoint Security and Control in our test lab, with a large portion of the installation time devoted to waiting for repository packages and signatures to finish updating from the Sophos Web site. By comparison, McAfee required multiple manual package installations and required substantial advance preparation and expertise to configure correctly, with roughly three times the number of steps to install, and up to an hour more to successfully deploy all of the protection components and updates to the clients.

During the installation process, we were able to discover endpoints automatically using Microsoft Active Directory. As with the other products, Sophos Endpoint Security and Control supports Active Directory both via one-time directory import and via automatic synchronization. With automatic synchronization, administrators can protect new endpoints automatically when they are added to the Active Directory tree, without any additional work in the Sophos console. However, Sophos, unlike Symantec, does not include synchronization based on AD users or synchronization without mirroring the AD structure as McAfee does.

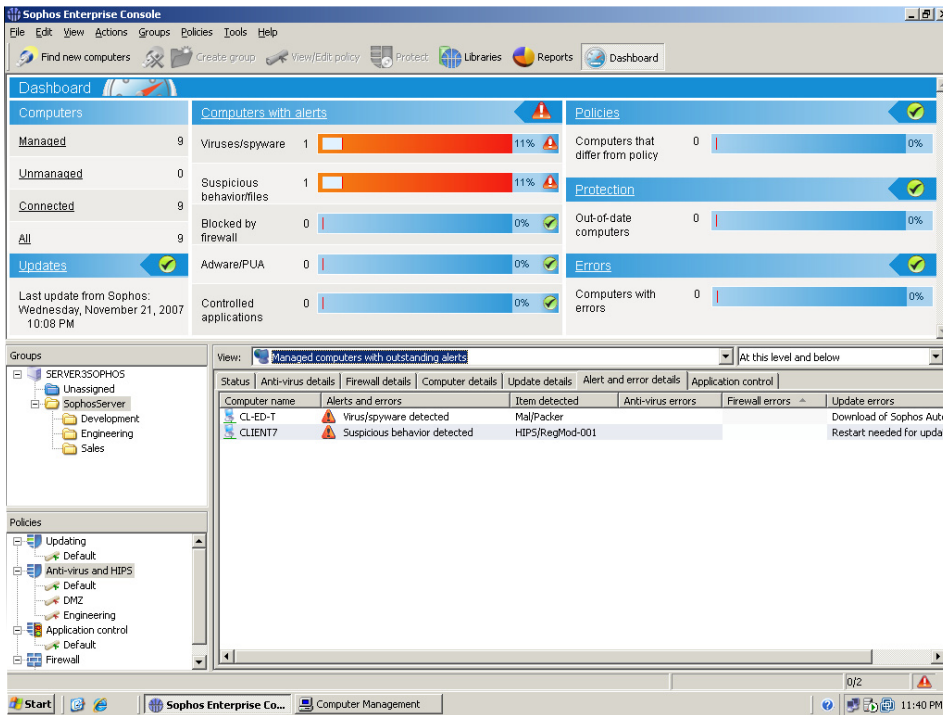
Sophos Endpoint Security and Control provides support for a wider range of platforms than either the McAfee or Symantec offerings, with one license covering all platforms. It supports workstations running Windows 95 or later (including Windows Vista), Mac OS X 10.2 or higher, servers running Windows Server 2000 or 2003, and NetWare, Linux, UNIX, NetApp Storage

Usability and Management

The Sophos Enterprise Console collects information from all the security components and presents it in a well-integrated interface. The centerpiece is a dashboard that summarizes the important, actionable pieces of information that an administrator needs to know. It shows new detected threats, nodes out-of-compliance

category across the endpoint groups that we created in our deployment. Sophos Enterprise Console can manage Macintosh and Linux as well as Windows platforms, a feature that brings benefits to heterogeneous environments and is absent in Symantec's console.

In our usability tests, most common administrative tasks took fewer steps and less time with Sophos than with the Symantec and McAfee products, a benefit which should reduce the recurring management costs in any size enterprise. Both Symantec and McAfee were more difficult to navigate and required more intricate and sometimes counterintuitive steps to perform a given task. In instances where the number of steps were similar, we often found Sophos to take less time, due to better integration, fewer layers to navigate, and better overall design.



Sophos guards against more threats by employing signatures, Behavioral Genotype Protection, and effective run-time HIPS - all with minimal administrator configuration.

Systems, OpenVMS and Windows Mobile devices. Firewall protection is provided for Windows 2000 and later.

Migration

Unlike the processes required by McAfee and Symantec, a migration from the previous Sophos version is relatively painless. A migration guide walks administrators through the process which comes down to just backing up the database and installing the new management server over the old with all existing policies kept intact. New client software can then be deployed to groups of clients when desired.

with policy, as well as the number of managed and unmanaged nodes across the network. In comparing Sophos with Symantec, we found the Sophos dashboard view more helpful, and although McAfee's dashboard provides flexible views, it requires administrators to configure it beforehand and to go elsewhere to take action.

We also used the Sophos Enterprise Console to create, deploy, and enforce policies. Sophos maintains separate policy configurations for anti-virus/HIPS, firewall, application control, and updating. We found it very easy to manage and identify policy configurations within each

Overall, the reporting capabilities in Sophos Endpoint Security and Control are adequate but less extensive than those in the other products. The Enterprise Console provides a wizard which creates a number of pre-built reports for display in either table or graphical chart format. Sophos can also generate daily, weekly, monthly, and annual reports for alerts and threats, and it has options to automatically purge old data from the reporting database. However, we would like to see more powerful capabilities for custom ad-hoc reporting to accommodate the needs of enterprises that may have specific reporting requirements not met by the provided canned reports.

The Enterprise Console allows management of adware and other "potentially unwanted applications (PUAs)" in a straightforward way. It presents the PUAs found during anti-virus scans and security breaches from firewall logs so that the administrator can easily make policy decisions with relevant data in hand. Specifically, a full system scan identifies all potentially unwanted applications and gives

administrators the option to either authorize all or selected PUAs or remove the PUAs using a remote cleanup option, a feature unavailable in either McAfee or Symantec's console.

Sophos has integrated strong application blocking capabilities into its management product and anti-virus client. Administrators can use Sophos Enterprise Console to either authorize or block the installation and execution of legitimate (non-spyware/adware) applications. Unlike Symantec and McAfee, Sophos maintains a list of well-known legitimate applications, such as file sharing clients, browser plug-ins, and instant messaging clients. Symantec and McAfee's products require administrators to lock down the environment and add in allowed applications, which requires constantly updating the rules of the executables when they are patched or updated. By having Sophos maintain the database of applications to control, administrators can be assured of continued protection, without the burden of having to maintain a separate allowlist, blocklist, and fingerprints of applications, even when vendors apply patches that update their applications. Enterprises can request Sophos to add unsupported applications to the regularly updated list.

Effectiveness

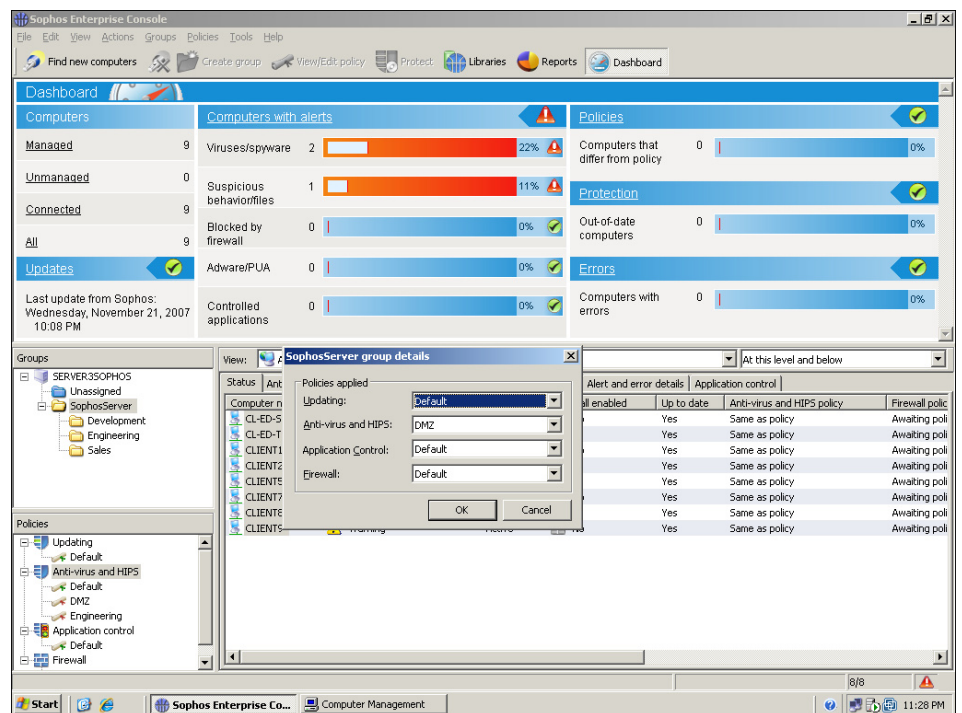
Sophos beat Symantec and McAfee in our day-zero effectiveness tests, providing better protection against our set of new and unknown threats. Using a combination of signature-based and behavioral-based HIPS techniques, Sophos was able to detect fully 86 of the unknown threats pre-execution, double the number detected by McAfee (43) and 35 more than Symantec (51).

Two features contributed to Sophos significantly higher blocking rates, its Behavioral Genotype Protection (BGP) and run-time HIPS. BGP is a "pre-execution" HIPS technology which

recognizes a suspicious or malicious file before it executes on the client. Sophos' run-time HIPS capability was able to block an additional 11 malware binaries through detection of the modification of files, processes, and registry values during execution. All told, Sophos detected 97 of the 100 new threats we tested compared to 58 for McAfee and 82 for Symantec.

Sophos also did a good job at finding the set of known common viruses,

detected that threat before installation. When we examined adware threats, we found Sophos' effectiveness to be on-par with that of the other products. Like Symantec and McAfee, Sophos detected most bundled adware on or after installation, but was successful in blocking one adware's attempt to modify registry values using its run-time HIPS capabilities and another's attempt to download the full adware payload from a remote host using its firewall functionality.



Sophos has a well integrated policy management approach that lets administrators assess and change settings for management groups quickly and easily.

spyware, and adware in our test. When we challenged the products with a recent Storm worm variant, Sophos was the only product to detect the threat on-access with its Behavioral Genotype Protection. Unlike Sophos, both McAfee and Symantec failed to block the malware and allowed it to install a rootkit on the client. Sophos was the only product that was able to detect or block all of the viruses and spyware we used in testing, although in one instance a keylogger was only detected by an on-demand scan after complete installation. Symantec and McAfee

Sophos also fared very well in our scanning performance tests. It was a close winner in our on-access folder-based tests and finished our on-demand folder scan significantly faster than Symantec and McAfee. Furthermore, the Sophos scanning engine (like Symantec's) implements a caching algorithm, which led to about a 50% speed improvement in a second-pass run. Sophos memory usage was approximately 80MB for its agent and scanner during our testing.

Sophos delivers malware definition

updates in a streamlined fashion. Unlike Symantec and McAfee, which deliver updates on a daily basis, Sophos delivers updates on an intra-day basis. Sophos updates are still much smaller than both Symantec and McAfee updates, which is an advantage for companies concerned about limiting the impact on network resources when responding rapidly with updates for new threats. Sophos also includes automatic application updates in its update engine in addition to malware definition and engine updates.

Conclusion

Sophos Endpoint Security and Control provides effective malware detection and strong performance and is easier to use and more streamlined than both Symantec and McAfee. It is an exceptionally well-designed product, combining architectural simplicity with highly effective pre-execution detection of malware threats. Sophos Endpoint Security and Control is a natural choice for enterprises looking for a simple and well-integrated endpoint security suite that is effective out of the box.

Symantec Endpoint Protection 11.0

Symantec Endpoint Protection 11.0 (SEP 11.0) finally brings together the necessary components for an effective endpoint security suite. For the last few years, enterprises using Symantec products had to cobble together multiple packages and management consoles to create a complete solution. Symantec now has a single, integrated solution to manage policies although larger organizations will want to use separate Quarantine and LiveUpdate servers which must be managed independently. SEP 11.0 makes it much easier to create and manage policies than previous Symantec products and the current McAfee Total Protection product, but doesn't match Sophos Endpoint Security and Control in terms of day-zero effectiveness, usability &

management, or scanning performance on infected machines.

Getting Started

For companies using Active Directory synchronization, administrators can import organizational units/containers or users. Administrators have the option of managing users separate from the Organizational Unit (OU) structure. Importing OUs results in a direct mirror of this structure in the console. However, if users are brought in from the LDAP server, they may be copied to different groups that are configured by the administrator. This user-based synchronization provides added flexibility in managing security policy since a user (such as an engineer with permission to use a larger set of applications) can be given appropriate permissions no matter which computer they are using. The downside of Symantec's Active Directory integration is that, unlike McAfee and Sophos, there is no way to automate deployment after a successful synchronization.

Non-Active Directory deployment is simplified by the Migration and Deployment Wizard which quickly identifies the endpoints that need to be protected and deploys the appropriate installation package to them. The only cumbersome part of the wizard-driven process is lack of support for group logon credentials which requires administrators to type in credentials for each machine, an arduous task. For large deployments, administrators may choose to use the Find Unmanaged Computers wizard in the Clients tab of the management console.

Administrators managing a large number of endpoints will also likely want to deploy separately-managed Quarantine server and LiveUpdate servers to better manage bandwidth usage. Quarantine server is especially useful during a virus outbreak, and LiveUpdate server will lessen the load on the management server generated by signature updates. Each LiveUpdate server handles distributing updates

from the central management server to the clients to relieve any potential bandwidth issues that may occur in large deployments. However, these consoles are not integrated with the Symantec Endpoint Protection Manager console.

Symantec Endpoint Protection supports Windows XP, Windows 2000, Windows 2003, Linux, and NetWare platforms. Symantec also offers Macintosh support, but like its Linux product, must be managed separately from the Windows products.

Migration

Given the workload involved in migrating to SEP 11, because of the extensive architecture changes, administrators will have difficulty choosing whether to migrate or perform a fresh install. Although a migration will preserve anti-virus/anti-spyware policies, groupings, and reporting events, the time invested in pre-migration steps such as removing components that block migration, such as the Symantec Reporting Server and Symantec Client Firewall, and then properly migrating servers and clients in order to preserve the appropriate policies, may not be worth it. Companies that use Symantec's previous firewall won't be able to migrate these rules over to the new product. In addition, administrators should note that the new behavior-based Proactive Threat Scan will be turned off during the migration.

Usability and Management

The primary management interface is the Symantec Endpoint Protection Manager, which provides access to the monitoring, reporting, client management, and policy management capabilities. Policies are divided between six components and are easily edited and applied to management groups. A simple-to-use inheritance check box allows policies to be acquired from a parent group. Administrators use named policies which are easily copied,

edited, and applied to specified groups by right clicking, and matching policies to groups is as simple as double clicking and viewing the policy detail window.

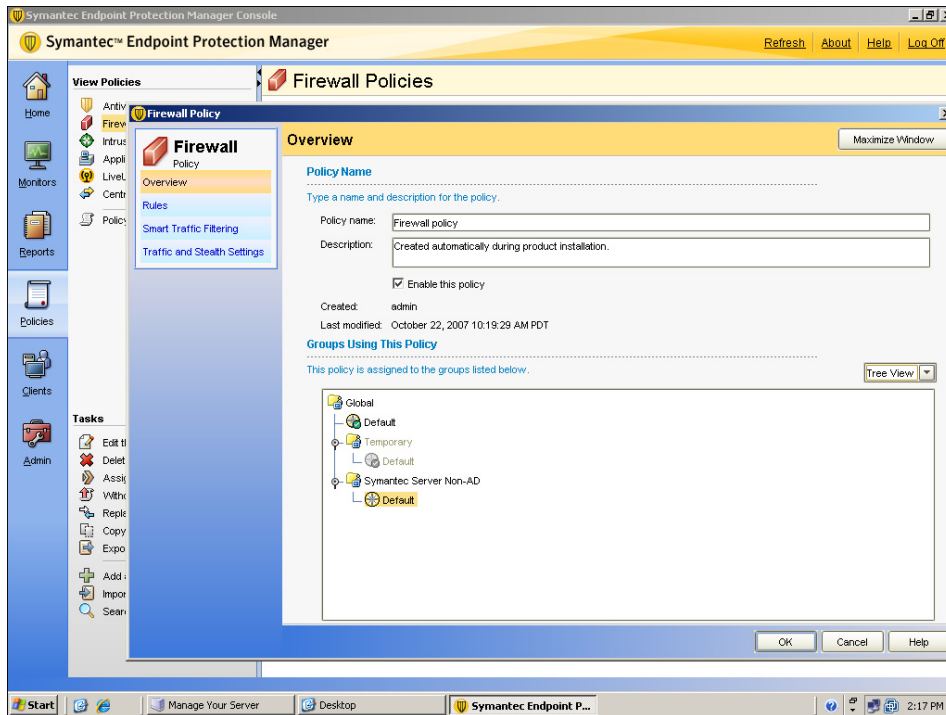
We found Symantec's application control features to be poorly integrated and cumbersome to use. Unlike Sophos, which maintains an up-to-date list

file to be updated. The same results can be achieved by Sophos with much fewer steps.

Firewall and IPS features are now fully integrated into the single Symantec client. Firewall rules are easily created through a wizard that includes applications learned by the client and

granular as those of McAfee, but they are easier to use and provide a wider variety of useful information than what is available with Sophos' limited reporting features.

Symantec Endpoint Protection Manager is the only console in this review that cannot manage clients other than Windows. Symantec's updates includes client software updates and can update virus signatures on a daily basis on par with the McAfee product.



Symantec's mostly usable policy management interface can still perplex administrators who want to display the policies for a given group.

of applications that can be blocked, Symantec lets administrators generate a fingerprint for each specific executable and paste the checksum into the application control policy by hand. The feature is geared more towards environments where IT personnel maintain a set of workstation images with a defined set of applications that are installed. The fingerprint file of all executables is created through accessing an application through the Windows command prompt. Manually uploading this file into the Endpoint Protection Manager console allows the administrator to effectively lock down the environment allowing only these programs to run. Adding or upgrading an application requires the fingerprint

reported to the server. Administrators familiar with client firewall management will find the process easy to navigate. Likewise, the signature-based IPS settings are straightforward and provide additional options for protecting against DoS and other network attacks.

Reporting and system monitoring provide administrators with granular tools for assessing the status of the environment. Canned reports are spread across eight areas and administrators can configure and save filters to apply to any of the reporting areas. A scheduled report feature allows any of these outputs to be emailed on a flexible schedule. The reporting and monitoring features are not as

Effectiveness

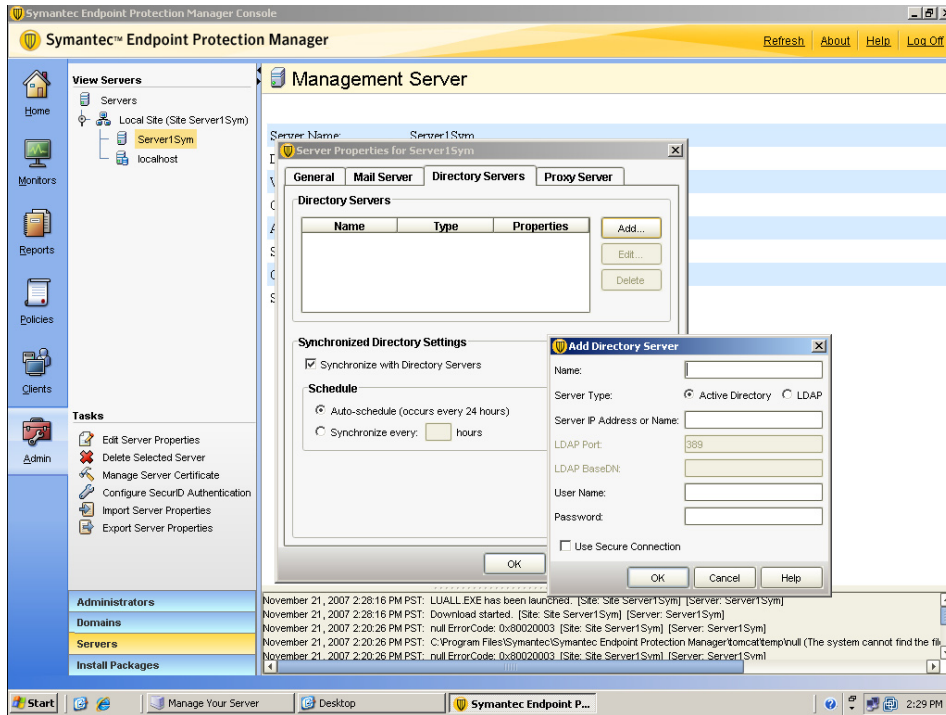
In our testing, Symantec performed reasonably well in protecting against new and unknown virus threats but much of the protection came late in the cycle. Using its signature and pattern-based approaches, it detected 51 of our 100 threats pre-execution, more than McAfee, but considerably less than the 86 detected by Sophos. Symantec caught another 13 on-execution, 11 of which were caught with signatures and 2 of which were caught using behavioral heuristics, and another 18 post-execution, after malware has taken control of the system, bringing its total to 82 compared to 97 for Sophos and 58 for McAfee.

SEP 11.0 returned mixed results in identifying our set of known viruses, spyware, and adware. In the virus testing, it allowed a Storm worm variant to install a rootkit and failed to terminate the malicious process on detection – similar to what happened with McAfee. It did detect all of the other threats of this class during the on-access scan. In our adware and spyware tests, Symantec's results were on par with the other products. In several cases, it identified some or all of the bundled adware components only after installation and a full system scan.

While Sophos' HIPS protection significantly increased detection rates, we were unable to identify any significant impact of Symantec's behavioral or HIPS-based protection

component. We did see a number of binaries identified by their association with a family of threats, but in the absence of a signature or pattern, Symantec, like McAfee, failed to block the execution of the malware. Symantec does include a new Proactive Threat Scan capability

improvement in scan time. During our testing, Symantec's memory usage ranged from 40-60MB when accounting for its agent, scanner, firewall components, and Proactive Threat Scan processes. We also saw high CPU usage when Proactive Threat Scan ran.



Symantec offers the unique ability to synchronize the Active Directory environment such that security policies can be managed on a user basis rather than an endpoint basis.

that scans running processes on an hourly basis. This Proactive Threat Scan detection did manage to detect 1 malware during our tests. An administrator can override the default setting with a specific frequency or can change the product to scan every process upon creation, but this setting can significantly impact system performance.

Its on-demand scan of the system drive was nearly identical in performance to McAfee, but performance slowed significantly when we had it scan an infected drive - a full 3.5 minutes behind Sophos and 2 minutes behind McAfee. Repeated scanning of the uninfected drive did show some caching effects, with a 12%

Conclusion

Symantec Endpoint Protection 11.0 provides adequate protection against a diverse range of threats and is a reasonable choice for large enterprises. Management and integration of protection is much improved from the previous product, but we found its pre-execution and behavior or HIPS-based day-zero capabilities lacking in effectiveness against our malware corpus. Users of previous Symantec products will face a painful and time-consuming migration process moving to Symantec Endpoint Protection 11.0

What the Ratings Signify

We installed each of these products on our test network of Windows Server

2003 and ten Windows XP machines, configured it, and then assaulted it with a variety of threats ranging from well-known malware to new and obscure threats selected to exercise products' behavioral blocking, firewalls, and other protective abilities. We also performed representative administrative tasks such as adding new machines to the network, granting exceptions for particular applications running on individual machines, and exercising alerting and reporting capabilities. We then scored each product in the following five categories.

Installation & Deployment

rates the experience of installing the server software and management console and deploying the endpoint security software to client and server machines on the network. For products that have undergone a significant upgrade, we examine the ease of migrating existing policies and events to the new version. We favored truly integrated products, those with straightforward installation wizards, and those that auto-discover endpoints through full Active Directory integration, NetBIOS, or via IP addresses.

Usability & Management

covers both initial product configuration and ongoing management. We included administrative tasks such as configuring security policies, protecting a new endpoint, scheduling tasks, running an on-demand scan, configuring a firewall, removing a malware infestation, and granting access to a potentially unwanted application. We also included end-user tasks such as scanning files received through e-mail and other means, performing updates on a laptop while on the road, and using the interface to gather information about applications or files that were blocked. We also awarded higher scores to products with enterprise-oriented features such as Active Directory integration.

Visibility covers the dashboard, monitoring, reporting, and alerting capabilities offered by the product.

We considered the availability of a dashboard that provides an easy-to-comprehend overview of client protection status, recent events, and task-based activities to be a major benefit. However, a dashboard must be augmented by reporting and alerting tools to identify critical information such as detected malware, out-of-date signatures, and computers without endpoint protection across hundreds or even thousands of endpoints.

Effectiveness (Basic) rates a product's ability to block an assortment of common malware, including viruses, virus variants, spyware, adware, and other potentially unwanted applications using specific signatures, patterns, or detection on execution. We systematically examine how the product

handles the threat including changes to the registry, file system, and running processes that occur on installation. Network traffic is analyzed alongside the product's firewall logs to determine if further malicious activity occurs beyond the local host. To provide a level playing field, we conducted testing using samples from our own malware corpus without input from the vendors.

Effectiveness (Day-Zero) assesses the breadth of protection available to stop or mitigate against unknown or recently discovered viruses, spyware, exploits, and other malware. We evaluate anti-virus, anti-spyware, desktop firewall, buffer overflow protection, behavioral techniques, and run-time HIPS techniques. Detection is examined on-access, on-demand, during installation

and then with a final on-demand scan following installation. We enable basic settings but otherwise test the products in their default configuration. To provide a level playing field, we conducted tests using samples from our own malware corpus without input from the vendors.

Performance measures how well each product minimizes impact on users while performing common tasks such as on-access scans, full system scans on both clean machines and those infected with adware and viruses, and signature updates. ▲



Independent evaluations of technology products

Contact: inquiry@cascialabs.com
www.cascialabs.com

SOPHOS

This comparative review, conducted independently by Casadia Labs in November 2007, was sponsored by Sophos. Casadia Labs aims to provide objective, impartial analysis of each product based on hands-on testing in its security lab, and gives each company whose products are included the opportunity to participate by providing input on Casadia Labs' test plan and feedback on findings.