Practical Business Endpoint Security

In This Review

- **ESET** Smart Security 4 Business Edition
- **Kaspersky** Lab Business Space Security 6.0 (Admin Kit 8.0)
- **McAfee** Total Protection for Endpoint v 8.7i (ePO 4.5)
- **Sophos** Endpoint Security and Control 8
- **Symantec** Endpoint Protection 11.0
- **Trend Micro** Worry-Free Business Security 6.0 Standard Edition

The business endpoint security market is changing at a surprisingly rapid clip, especially considering how relatively mature it is. While established brand names may provide subjective reassurance, buyers who look beyond the brands to products' quantitative capabilities may discover less-familiar options that are a better fit for their enterprises.

In our continued testing of security products, Cascadia Labs has found significant differences in how well products meet various corporate goals for security suites, from effectiveness at blocking threats to performance to integration with enterprise infrastructure.

To evaluate the true capabilities of endpoint security suites, we put six of them to the test in our enterprise security lab. We gathered detailed quantitative and qualitative data about their capabilities in a variety of areas important to small and midsize enterprises.

We started by looking at the end-user experience with some quantitative measures of effectiveness and performance—a product needs to protect users against Web threats and stay out of users way as much as possible. Then we changed vantage points to the IT administrator and explored how the product integrates with Active Directory and Windows 2008 Server, and what the product is like to manage and use. We continue to believe that products that are easy to manage and that provide excellent visibility into their workings will ultimately contribute to a better security policy.

Summary

We found that the products were more different than similar—leading to the conclusion that companies should carefully consider the choice they make.

Kaspersky, Symantec, and Trend Micro Worry-Free made installation and

OVERALL RATINGS

Category	ESET Smart Security 4 Business Edition	Kaspersky Lab Business Space Security 6.0 (Admin Kit 8.0)	McAfee Total Protection for Endpoint 8.7i (ePO 4.5)	Sophos Endpoint Security and Control 8	Symantec Endpoint Protection 11.0	Trend Micro Worry-Free Business Security 6.0 Standard Edition
Installation & Configuration	▲▲	▲▲▲▲▲	▲▲	▲▲▲	▲▲▲▲	▲▲▲▲
Policies & Management	▲▲	▲▲▲▲	▲▲▲	▲▲▲▲	▲▲▲▲	▲▲▲▲
Visibility & Reporting	▲▲	▲▲▲	▲▲▲▲	▲▲▲	▲▲▲▲	▲▲▲
Performance	▲▲▲▲	▲▲▲▲▲	▲▲▲	▲▲▲▲▲	▲▲▲	▲▲
Effectiveness	▲▲▲	▲▲▲▲	▲▲▲	▲	▲▲	▲▲▲▲
OVERALL	▲▲½	▲▲▲▲	▲▲▲	▲▲▲	▲▲▲½	▲▲▲½
Quick Summary	A fast product best suited to smaller companies given its poor AD integration, lack of a dashboard, and little polish relative to other products in this review.	Nice choice for companies of all sizes given great AD integration, speed, excellent protection against Web threats, and solid management. Reporting and documentation can be improved.	A complex product best suited for large organizations that can handle its complexity. We found slow performance throughout our tests.	Very clean and well-designed product with default settings that do little to block Web threats. Reporting needs some work.	A solid product with good management and great reporting, but with some real struggles against our live Web threats.	A good choice for small companies, offering solid protection against Web threats. Performance can be a drag.

Key: ▲ – Poor ▲▲ – Fair ▲▲▲ – Good ▲▲▲▲ – Very Good ▲▲▲▲▲ – Excellent

INSTALLATION & CONFIGURATION SUMMARY REPORT

Product	Steps and Time to Complete	Rating	Pros	Cons
ESET Smart Security	131 steps, 3-4 hours	▲▲	• Very well documented: easy to follow, included GPO changes	• Poor Active Directory integration • Uses Microsoft Access database by default (not documented in wizard)
Kaspersky Lab Business Space Security	78 steps, 3 hours	▲▲▲▲▲	• No manual GPO changes required • Manual firewall changes clearly documented • Provides extensive list of product removals • Automatically installs database for management server	• Installation documentation could be clearer
McAfee Total Protection for Endpoint	166 steps, 4-6 hours	▲▲	• Good detection of Active Directory clients and other domains on the network • AD sync task is easy to perform and use later	• Process is complex • Product required a comparatively large number of downloads and was poorly integrated • Poor documentation, with disjointed topics
Sophos Endpoint Security and Control	183 steps, 3-4 hours	▲▲▲	• Great Active Directory integration: importing the AD structure is easy to find and perform	• Requires pre-install of SQL Server 2005/2008 • Requires server reboot after disabling UAC, forcing restart from beginning of wizard • Custom install of "SQL Server" component is confusing
Symantec Endpoint Protection	123 steps, 3-4 hours	▲▲▲▲	• Documentation very thorough, easy to follow • Auto-installs database for management server • AD sync well documented and easy to perform	• Manual GPO or client configuration required to open network for agent install
Trend Micro Worry-Free Business Security	72 steps, 3 hours	▲▲▲▲	• Least number of steps during installation • Auto-installs a database for management server	• Requires manual GPO configuration to push client • IIS-specific components not documented until after initial IIS install is completed

configuration easy, with Kaspersky edging out the others thanks to its Active Directory integration. These same products and Sophos provided the best policies and management experience; McAfee lagged due to complexity, and ESET needs Active Directory integration to be a viable player in larger companies.

Symantec and McAfee had the best visibility and reporting, with many options to make the administrator and compliance officer happy. In terms of performance, Kaspersky, Sophos, and ESET all fared well, with McAfee and Trend Micro slowing down a user's experience significantly. In terms of effectiveness, Kapsersky and Trend Micro Worry-Free got the best scores, with Symantec and Sophos not fully blocking enough of our Web threats.

In the end, companies will need to make a choice based on their individual requirements and to configure them suitably, so it pays to look at individual ratings and reviews and not simply the products' overall scores.

Rating the Products

The ratings are determined based on the tests run in our labs with highlights shown as Pros and Cons in our summary reports. The ratings are intended for use in comparing the products and should not be used as an absolute measure of the products' capabilities in a given area. If a product truly stands out against the other products, it can receive 5 triangles.

We installed each product on our test network of Windows Server 2008 and Windows XP and Windows 7 machines, configured it, and then tested its performance and effectiveness against a set of Web threats to exercise the product's countermeasures including URL and Web content filtering, 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 testing alerting and reporting capabilities. We then scored each product in the following five categories.

Installation & Configuration 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. We favored truly integrated products, those with straightforward installation wizards, and those that auto-

POLICIES & MANAGEMENT SUMMARY REPORT

Product	Rating	Pros	Cons
ESET Smart Security	▲▲	• Policy editor includes unique "default" button to set any value back to the default	• No Active Directory integration Doesn't handle groups well; default view returns to view without groups when restarted
Kaspersky Lab Business Space Security	▲▲▲▲	• Clear, easy-to-use interface • Allows for separate workstation, server, and mobile policies in each group • Uses one policy per group • MMC interface is easier, faster than Web-based interfaces	• Only one active policy of each type allowed in each container
McAfee Total Protection for Endpoint	▲▲▲	• Provides very granular control over policies and what users see	• Complex: uses 11 separate anti-virus policies, plus one for the agent • Default install leaves clients unprotected; updates not enabled • Default firewall install disables all network connectivity
Sophos Endpoint Security and Control	▲▲▲▲	• Nice clear interface; everything you need is in one window	• Uses five policies (Agent, Anti-Virus, Application Control, Firewall, and NAC), making creating and deploying policies cumbersome
Symantec Endpoint Protection	▲▲▲▲	• Interface is simple and straightforward • Default policies have the settings most administrators will want • Firewall works with enterprise apps without modification	• Multiple policies make client administration more complex than single-policy products
Trend Micro Worry-Free Business Security	▲▲▲▲	• Clean, simple interface • All policy changes can be made in one tab • Easy to determine which policy applies to any group, to create new policies or groups	• Default configuration leaves login Web console with security certificate error

discover endpoints through full Active Directory integration, NetBIOS, or IP addresses. Many of these products require a database and Web server. The best ones make administrators' lives easier by automatically installing necessary pre-requisites.

Policies & Management covers both initial product configuration and ongoing management. We included administrative tasks such as setting default endpoint configuration, adding a new desktop, scheduling scans, running an on-demand scan, and configuring a firewall. We also awarded higher scores to products with enterprise-oriented features such as Active Directory integration and location awareness. All of the products support some type of push install to clients in a domain, as well as inheritance of policies from parent

VISBILITY & REPORTING SUMMARY REPORT

Product	Rating	Pros	Cons
ESET Smart Security	▲▲	• Lots of pre-defined reports	• No dashboard • Custom reports and alerts are difficult to set up • No PDF format option for reports
Kaspersky Lab Business Space Security	▲▲▲	• Excellent extensible dashboard • Flexible system for both pre-defined and custom reports and alerts • Easy to e-mail alerts and reports	• Finding the report you're looking for can take a while • "Custom" reports limited to pre-defined queries
McAfee Total Protection for Endpoint	▲▲▲▲	• Large set of pre-defined reports and alerts • Nice dashboard, with a huge number of optional graphs that can be displayed on as many different tabs as desired	• Complex process to create reports • Must navigate through multiple sections of the interface
Sophos Endpoint Security and Control	▲▲▲	• Clean interface for dashboards and reports • Setup of e-mail alerts is quick and easy	• Reporting functionality is limited to a few categories • No way to automatically generate weekly reports
Symantec Endpoint Protection	▲▲▲▲	• Informative, well-organized dashboard • Process of sending reports and alerts is simple and straightforward • Alert system is complete and easy to use with dampers	• Admin console can result in very high utilization levels on the server • Limited to HTML reports
Trend Micro Worry-Free Business Security	▲▲▲	• Dashboard is well organized and customizable • Alerts and reports are simple to schedule and send via e-mail	• Canned reports a bit awkward to use • Reporting is limited to 14 pre-defined reports

container to children. We preferred fewer policies to manage and products that could ably handle laptops, desktops, and servers together.

Visibility & Reporting examines the dashboard, 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 lacking endpoint protection across hundreds or even thousands of endpoints.

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. An endpoint security solution shouldn't noticeably slow end-users down. The cream of the crop will add only minimal overhead on client computers for on-access and on-demand scans.

Effectiveness rates the products' ability to block Web-based threats. To provide a level playing field, we conducted testing using samples from our own independently-created corpus without input from the vendors. We set basic settings but otherwise test the products in their default configuration allowing the products to use their full set of countermeasures against threats. We measure the products ability to halt threats before they initiate processes or otherwise modify the computer.

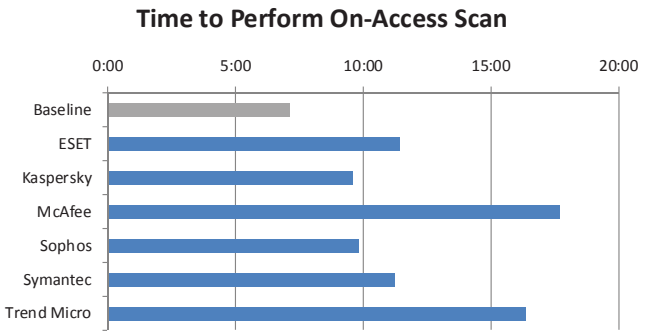
Performance Results

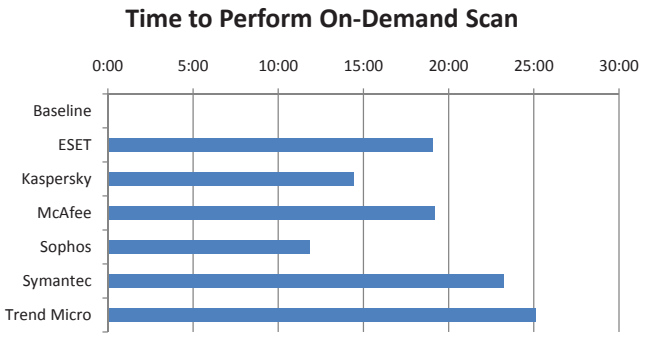
The Sophos and Kaspersky products were the fastest we tested. They minimized the overhead of on-access scans, and turned in by far the shortest times to perform full-system on-demand scans. By contrast, the McAfee and Trend Micro products imposed a significant impact on everyday activities—they needed more than double the time to copy folders and open a large PowerPoint file as our baseline system (with no endpoint security product). Symantec and Tend Micro took the longest to perform on-demand scans.

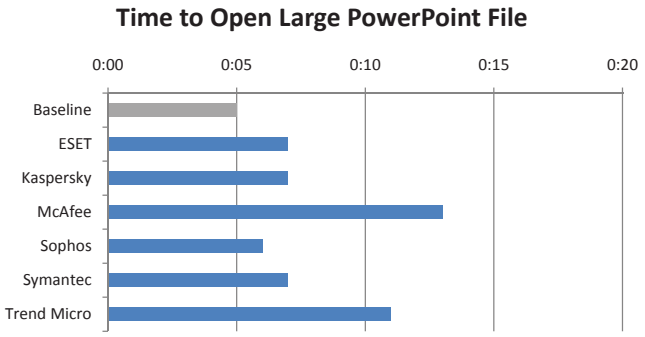
In addition, we performed a second on-demand scan to determine the maximum potential benefit of a product's caching mechanisms. The Kaspersky product showed a much larger improvement than other products—but it's important to note that this test shows the maximum possible benefit, in conditions where no files had changed and no intervening signature updates were performed before. Because this second on-demand scan is so unrepresentative of real-world usage, we did not include it in our calculatinos of the products' performance ratings.

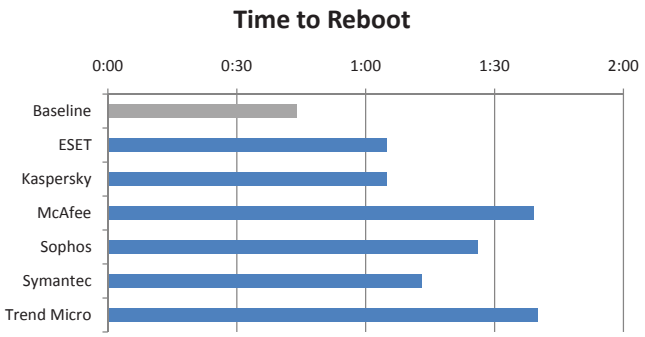
Effectiveness Results

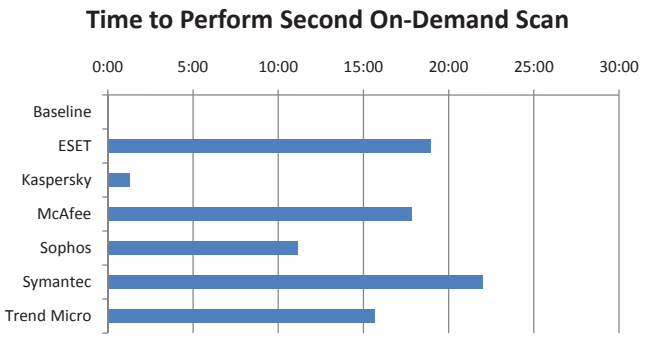
The products showed wide variation in effectiveness at blocking the effects of drive-by downloads and browser-borne exploits, a dominant mode of threat delivery today. Kaspersky and edged out Trend Micro tied for the best outcome, each completely blocking 80 percent of the exploit campaigns we tested with, and with Kaspersky substantively blocking one more. In Trend Micro's case, the

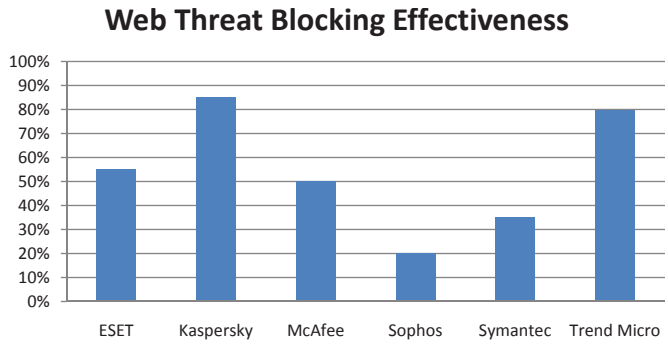










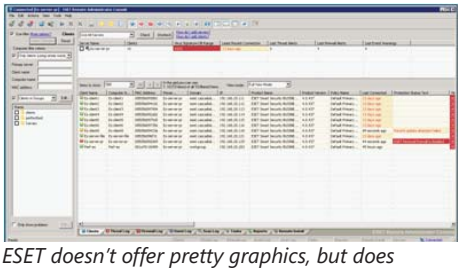


product achieved this effectiveness via URL-based blocking, reporting that it was preventing numerous malicious URLs from downloading at all. Kaspersky's product used a variety of techniques, including heuristics identifying malicious iframes embedded in a Web page's HTML, that in most cases completely thwarted the exploits. Even in the cases where Kaspersky did not completely block the exploit, it did at least report that it had detected Trojans.

ESET and McAfee were in the second tier, each blocking half of the exploits, and with ESET also blocking all but some file system activity in one additional case. Symantec followed, with Sophos last, fully blocking only 20 percent of the exploits. Sophos' HIPS capability frequently reported suspicious behavior and resulted in partial but incomplete blocking of the malicious activity. We score incomplete protection—where any rogue process still runs on the compromised system—as a "miss".

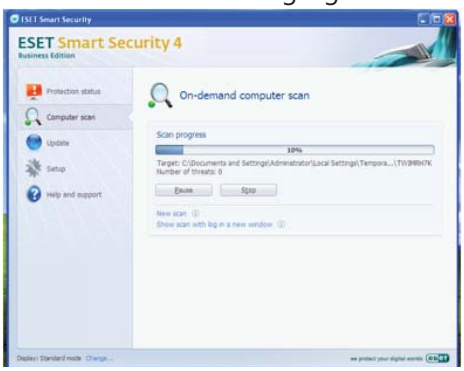
ESET Smart Security 4 Business Edition BRIEF

While the ESET product delivered good performance numbers and installation was fairly straightforward—albeit with poor Active Directory integration—it conspicuously lacks a dashboard interface and other aspects desirable for companies. The package also has somewhat limited policy-management features, and it was a chore to generate custom reports and alerts.



ESET doesn't offer pretty graphics, but does provide visibility into the status of all installed clients, as well as the ability to quickly narrow down a search for specific systems.

Like Kaspersky Business Space Security, the ESET product does not require an administrator to manually install either a database or Web server prior to installation and agent deployment. However, before deploying the agent, several modifications to Windows Firewall settings in the GPO will need to be made. One challenge came when attempting to locate the appropriate security components to download from ESET's extensive multi-language and multi-platform list that uses abbreviations rather than product names. This process could be simplified by splitting the language and platform option into separate drop down lists with better naming,



The ESET client offers a clean, simple interface with everything in a single window and most administrative options hidden from the end user.

ESET doesn't do anything fancy with Active Directory. It uses a flat initial structure, and all workstations and servers are imported into a single group, with one default policy—it's up to you to sort things out. Needless to say, in a large organization, this is a big disadvantage.

Creating custom reports and alerts is complex, due to a nearly impenetrable interface, although the product does offer 17 useful canned reports and matching alerts.

ESET turned in speedy on-demand scan results, but the product took longer to perform full-system scans than the fastest products. Its effectiveness against Web threats was middle-ofth-road in our tests.

Kaspersky Lab Business Space Security 6.0 BRIEF

The Kaspersky endpoint security suite excelled on our performance and effectiveness tests and was a breeze to install. Its deployment required among the fewest steps of the products we tested, and it provides flexible management and reporting capabilities.

The product uses several wizards to simplify the installation of the server and management components, and provides administrators with the option to deploy the security agent via a Windows Group Policy object (GPO) or via a remote push once file and print sharing ports are opened. It was the only product we reviewed that lets an administrator silently deploy agents via an automatically created GPO, and it was among the least complicated and fastest products to deploy in an Active Directory environment.

The Kaspersky suite does not require the installation of a Web server, and unlike Sophos and McAfee, it does not require the manual installation of a database. Our only complaint: some sections of the deployment documentation and administrator's guide could be organized better and more clearly presented.

Kaspersky Business Space Security allows three active policies per group—workstation, server, and mobile—whereas the other products we looked at generally require separate groups for servers, workstations, and mobile systems in each geographic or functional group.

Kaspersky offers an easy-to-follow tree structure that mirrors your Active Directory architecture, along with quick access to all the tools you need.

The product's default policy settings are very effective and generally just what an administrator would want: its default medium settings provide a balance between the highest security and the least impact on performance. Another plus is that workstation or server settings for all aspects of anti-virus, file, and application scanning, Web browsing, and firewall are in a single policy, whereas the products from McAfee, Symantec and Sophos require the configuration of multiple separate policies.

The product uses the Microsoft Management Console (MMC) to manage the

The Kaspersky client is straightforward and easy to navigate, with few options.

server, rather than a Web app, making tasks easier and faster to execute. The first time the admin console is launched, AD info is populated in the system, but computers had to be manually selected and added before they could be managed.

McAfee Total Protection for Endpoint 8.7i BRIEF

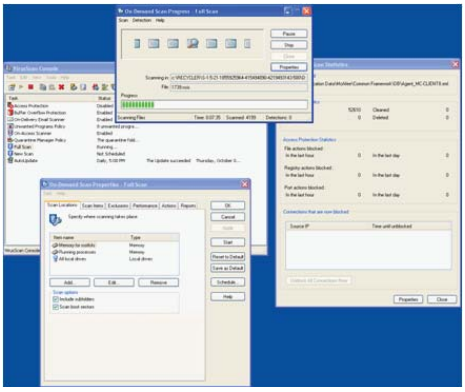
The McAfee product was saddled with a complicated installation process, and had among the poorest performance results in our testing. While it offers powerful and flexible reporting features, they can be difficult to use.

We found the McAfee installation and deployment to be among the more complex and time-consuming of the products we tested. This was primarily because the product requires the manual installation of a database, as well as needing to manually download and check in the anti-virus and anti-spyware components. We also ran into agent deployment issues from the lack of clear documentation on which ports

The McAfee main dashboard offers access to tutorials, a view of the most recent signature and engine update files, and the threat level for the all managed systems.

needed to be opened in the Windows Firewall. Another downside is that clients aren't set to automatically download updates by default; this has to be manually configured.

Importing the Active Directory structure with McAfee Total Protection for Endpoint was more cumbersome than most. The system separates tasks and policies, and requires you to create a task to download updates to server and another task to push new signa-



By default, the McAfee client gives the end user complete access to all options and configuration details through a variety of windows.

tures to clients—McAfee doesn't provide a way to execute an automated task more than once a day. In addition, creating a task to deploy patches is cumbersome; there's no way to create task as template and apply it later.

The product's strongest suit was its powerful reporting and alerting tools, which include 14 prebuilt dashboard consoles and the capability to build your own. However, while the features were powerful, administrators may struggle with the complexity of having to configure numerous settings on different menus to complete a single task. Expect to consult the manual more frequently than with other products.

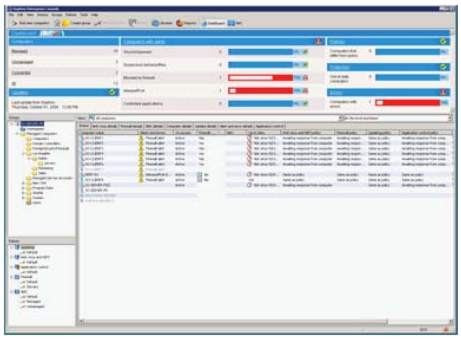
As for performance, McAfee was no speed demon, placing last on our on-access scan time test and returning middle-of-the-pack on-demand scan results. Its effectiveness was middle of the pack against Web threats.

Sophos Endpoint Security and Control 8 BRIEF

Armed with stellar performance, relatively simple setup, and a nicely designed management interface, Sophos Endpoint Security and Control fared well in the software side of security. Its performance was top notch but its effectiveness against Web threats was not good.

The Sophos product was the only package reviewed that allowed the creation of groups within its interface and the ability to synchronize those back into Active Directory. That lets an enterprise maintain the same directory structure in AD and the Sophos app—which, in the right settings, can be extremely useful for maintaining a consistent structure.

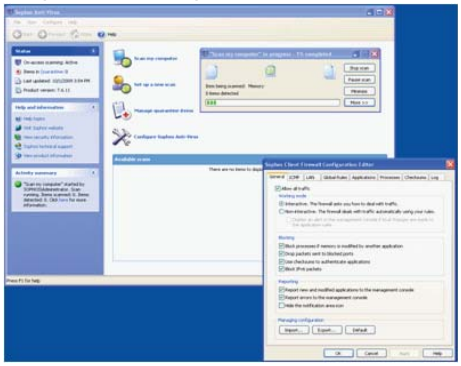
The Endpoint Security and Control suite was among the easiest products to install. Unfortunately, administrators need to manually install a database if they intend to install the server and console on Windows Server 2008. An additional server reboot is also required if UAC is running. Once those hurdles are overcome, Sophos' multiple wizards make the installation and deployment process quick and easy to navigate. It also features an Active



Sophos gives you a nice graphical overview of threats detected along with an organized view of the directory structure and policies.

Directory synchronization wizard that greatly simplifies locating clients in an AD environment.

In general, Sophos featured a clean interface; like Kaspersky Business Space Security, it uses the Windows MMC. We found setting up groups and policies simple and transparent. In addition,



Sophos provides separate client management tools for the Anti-Virus and Firewall applications.

the product uses five policies making creating and deploying policies a bit more cumbersome.

The product's dashboard has easy-to-read bar graphs, and allows for useful configuration of limits for warning and critical thresholds. E-mail alerts can be configured directly from the dashboard configuration window. But there's no mechanism to send reports at a regular interval, such as once a week—the system sends alerts only when a threshold is exceeded. In addition, reporting functionality is very limited although it does provide control over the reporting period.

Performance was a standout: Sophos delivered the fastest results on nearly all of our tests, although it scored poorly on reboot time, adding 40 seconds to our test systems. Effectiveness was unimpressive—although the Sophos product would sometimes warn us of suspicious content, most exploits were at least partially successful at launching rogue processes.

Symantec Endpoint Protection 11.0 BRIEF

The Symantec product's mixed performance results and lack of effectiveness against Web threats were offset by generally very good reporting and alerting features and robust policy management.

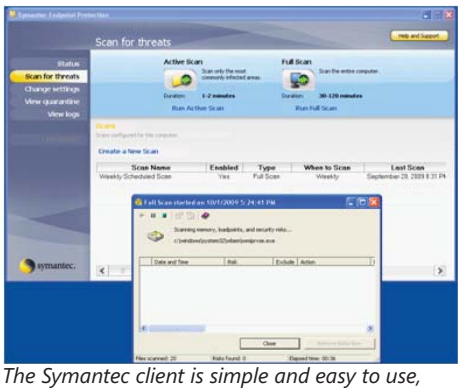
Before installing the Symantec management console and server, administrators must install a Web server. The two primary challenges we encountered during installation were locating the documentation listing the open ports needed for agent deployment to succeed as well as properly identifying our clients using the "Find Unmanaged Computers" wizard. Once the product is installed, Symantec includes one of the easier-to-use AD synchronization wizards. We found Symantec's documentation to be a tremendous help and among the best structured of all the products.

Symantec allows the creation of policies to control every aspect of the anti-virus, anti-spyware, firewall, intrusion prevention, application and device control, LiveUpdate and exception

The Symantec dashboard gives a clear picture of the current virus threat level along with status of recently deployed signature files and the status of clients.

categories, including which days of the week and/or times of day scans should run.

The product's home page is a nicely organized dashboard, which can show activity over the last 12 or 24 hours. Administrators can configure the dashboard to auto-refresh every 3, 5, 10, or 15 minutes as well as set thresholds for alerts (although the product doesn't allow thresholds other than number of events in a given time). Symantec Endpoint Protection provides a very broad range of pre-defined reports, with fine granularity on time periods (from last day to last month) and filtering by OS, protocol, direction (in or outbound), severity and other metrics. On the



The Symantec client is simple and easy to use, with no unnecessary options.

downside, it provides reports only in HTML format.

While Symantec demonstrated reasonable speed on our on-access scan and large-file-load tests, it was one of the slowest products on the on-demand scan, placing well behind Kaspersky and Sophos. Its lack of effectiveness against Web threats was surprising based on previous testing we've done on Symantec's consumer product.

Trend Micro Worry-Free Business Security 6.0 Standard Edition BRIEF

Trend Micro can boast very good effectiveness against Web threats and a simple, usable interface. It was, however, the slowest product overall that we tested, and its reporting capabilities are limited.

Like Symantec's product, Trend Micro Worry-Free Business Security requires the administrator to install a Web server, such as IIS or Apache, prior to product installation. The installation wizard automatically installs a database on either Windows Server 2003 or 2008. Trend Micro's documentation on deploying the security agent was slightly confusing; it listed specific requirements for Windows Vista workstations but not the steps for Windows XP workstations.

Viewing and creating policies worked well and was easy to do. Trend Micro provides a simple way to start with a template and easily modify it for any given group, as well as to easily determine which policy applies to a specific group.

Trend Micro makes it simple to identify unprotected clients, deploy the anti-virus software, and manage the overall process of protecting PCs in an organization.

The product's Live Status dashboard provides threat status for all clients along with several other security-health indicators, as well as server system status showing smart scan, component updates, unusual system events, and license status.

Alerts are limited to 24 events—most with thresholds, including client status and virus detected. Building reports

The Trend Micro client software provides a good basic interface for starting scans and other basic tasks.

using Trend Micro's templates is simple, and uses the same 24 event triggers as alerts. Reports can be run daily, weekly on any day, or monthly on day of month.

But the product's reporting features are a bit stunted. First, the reports folder initially is empty: You have to create a new report using one of the 14 templates, which can't be modified, to run a report. In a sense this is the worst of both worlds, in that Trend Micro provides nothing you can just run to start with, but no way to customize what you create. For example, the product lacks a way to generate a report showing endpoints that are out of date.

Finally, Trend Micro came in at or near the bottom of our performance tests. It took the longest to complete the on-demand scan—nearly twice as long as the two fastest packages, Kaspersky and Sophos. Trend Micro's product also added substantially to reboot time.

How We Tested Performance

For performance testing, we configured policies to make results comparable between products. For on-demand, full-system scans, we scanned only the local hard drive and enabled scanning within compressed and archive files. Our on-access tests did not include compressed or archive files. We enabled exceptions for our automation tools and left most other settings at their defaults.

We ran each individual test at least three times, restarting from a clean installation each time, and averaged the results. We computed the overall performance ranking by totaling each product's results for our on-access scan, on-demand scan, open PowerPoint file, and reboot-time tests.

On-Access Scan: Time to copy and paste a very large folder of non-archive file types, including Windows system files, documents, spreadsheets, pictures, PDFs, movies and music files.

On-Demand Scan: Time to complete a full system scan of an uninfected computer with default scan settings, but in all cases configuring products to scan all files and scan archives.

Open Large PowerPoint File: Time to open a PowerPoint file (8.7 MB PowerPoint photo album), demonstrating the impact of on-access scanning components.

Reboot Time: Reboot time, from specifying a reboot request through power on to fully-booted Windows desktop with idle CPU.

Second On-Demand Scan: Time to complete a subsequent full system scan of an uninfected computer with default scan settings. This test shows the maximum benefit that can be achieved by a product's caching abilities, and did not contribute to the overall rating.

For these performance tests, Cascadia Labs used a set of identically configured Dell desktop PCs with Intel Core 2 Duo E4500 2.2-GHz processors, 2 GB RAM, 160 GB hard disk, and Microsoft Windows XP Professional Service Pack 2. Test tasks were automated for maximum repeatability.

How We Tested Effectiveness

These effectiveness tests reflect the products' effectiveness against realistic, live threats using the products' full set of features—including Web reputation, anti-virus and anti-malware engines, and behavioral protection capabilities, among others. Cascadia Labs believes these tests to be a much more appropriate way to measure product effectiveness than simply pointing the products' signature engines against a large number of malicious binaries. However, this approach also requires readers to consider the following three factors when interpreting results.

Product Configuration: Business endpoint products provide many configuration options, both in the protection components they offer and the settings chosen for each component. Companies may choose different configurations based on the strictness of their security policy, their level of expertise, or other specific considerations. For these tests, we used products in their default configurations.

Samples Chosen: Threats can come from many places. For these tests, we focused on Web threats—specifically, drive-by downloads, as we believe they represent the largest and most prevalent threat to companies today. Cascadia Labs captures hundreds of threats per day; instead of choosing a random sample of Web threats, leading to tests with a large number of very similar underlying attacks, Cascadia Labs chose a single sample from 10 different campaigns with distinct exploit mechanisms to provide more threat diversity.

Scoring Mechanism: Defining a successful detection and creating a fair

scoring algorithm is harder than it may seem. Most would agree that stopping a threat before it exploits a computer, drops files, or runs processes is best. However, shouldn't products that stop the threat from running—even if they allow an exploit and some dropped files score better than a product that doesn't detect the threat at all? For this report, products that stop a threat completely are scored as a complete block and those that stop the threat from running score half of a block.

Most threats to company endpoints now come from the Web—specifically, from "drive-by" downloads that attack vulnerabilities in Web browsers and third-party applications. Cascadia Labs captures hundreds of threats per day, and we tested each of the products against ten different and timely Web threat campaigns that use distinct exploit mechanisms.

We used our proprietary exploit capture-and-replay technology to ensure that each product was tested against identical threats. For each exploit, we logged system activity and gave the highest scores to products that blocked exploits from starting new processes or dropping any files on the system; partial credit to those products that blocked all unwanted processes; and no points to those products that let the attack succeed, in full or in part, by successfully launching rogue processes on our test systems. ▲

Cascadia Labs

Independent evaluations of technology products

Contact: info@cascadialabs.com
www.cascadialabs.com

KASPERSKY lab

This comparative review, conducted independently by Cascadia Labs in November 2009, was sponsored by Kaspersky Lab. Cascadia Labs aims to provide objective, impartial analysis of each product based on hands-on testing in its security lab.