

Endpoint Security for Enterprises

The enterprise security landscape continues to change as companies expand their conceptual models of security. Whereas “security” once meant anti-virus—and later evolved to include capabilities like firewalls, host intrusion prevention, and anti-spyware—it’s now growing broader again as a new decade begins.

Forward-looking companies, and those operating under regulatory and compliance mandates, know that security increasingly demands they control the points at which data enters and leaves their trusted networks. Companies are justifiably worried that employees may knowingly or inno-

cently transfer confidential data—like customers’ Social Security numbers—out of the organization.

Of course, enterprise endpoint security vendors are adapting to this changing landscape, albeit in different ways. Many of the leading endpoint security players have, through acquisitions, extended product lines with separate products that perform various aspects of data protection. Many smaller companies have sprung up to provide data loss prevention and device control products, too. But these data-protection solutions can be complex and intrusive. And given the complexity of managing multiple

Security increasingly demands that companies control the points at which data enters and leaves their trusted networks.

In This Review

- **McAfee** Total Protection for Endpoint 8.7i (ePO 4.5)
- **Sophos** Endpoint Security and Data Protection 9.0
- **Symantec** Endpoint Protection 11.0
- **Trend Micro** OfficeScan Client-Server Suite Advanced 10 SP1

products in an enterprise environment, it’s natural that companies should expect their chosen endpoint security suites to provide the first line of data protection.

How is data protection implemented in practice? One approach is to control access to removable devices, like USB drives; another is to closely track files and data that are being exchanged.

OVERALL RATINGS

Category	McAfee Total Protection for Endpoint 8.7i (ePO 4.5)	Sophos Endpoint Security and Data Protection 9.0	Symantec Endpoint Protection 11.0	Trend Micro OfficeScan Client-Server Suite Advanced 10 SP1
Installation & Configuration	▲▲▲	▲▲▲▲	▲▲▲▲	▲▲
Policies & Management	▲▲▲	▲▲▲▲	▲▲▲▲	▲▲
Data Protection	▲▲	▲▲▲▲	▲▲▲	▲▲▲
Visibility & Threat Awareness	▲▲▲▲	▲▲▲▲	▲▲▲▲	▲▲▲
Performance	▲	▲▲▲▲	▲▲▲	▲▲▲▲
Technical Support	▲▲▲	▲▲▲▲	▲▲	▲▲
OVERALL	▲▲▲½	▲▲▲▲	▲▲▲½	▲▲▲½

Quick Summary	McAfee Total Protection for Endpoint is complex to set up and use. Despite strong reporting and policy management, it provides only basic device control and was slow in our performance testing.	Sophos Endpoint Security and Data Protection 9.0 combines ease of use with excellent performance and very good support. It’s the only product in the group to integrate data loss prevention capabilities, but the default firewall settings could have been more effective out of the box.	Symantec Endpoint Protection 11.0 delivered a solid experience from the start and provides robust policy management and reporting. Tech support, however, was very disappointing.	Trend Micro OfficeScan Client-Server Suite Advanced 10 (Service Pack 1) has too many confusing components, making for difficult installation and policy management. Scan speeds were good but Trend Micro’s built-in reporting is limited, and tech support was poor.
---------------	---	---	---	---

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

Now that several vendors are providing at least some of these functions within their core packages, we've undertaken to rate them in the context of a complete endpoint security solution.

For all this, of course, the fundamentals of enterprise security haven't disappeared: endpoint security products must protect desktops, laptops, and servers, in a way that's easy to deploy and manage. What's really new is that some vendors are addressing the expanding needs of customers by integrating data protection into the endpoint—building on traditional anti-malware measures and providing a more powerful tool set for today's security administrators.

What to Look For

Choosing an enterprise security product can be complex not just because your enterprise itself is complex, but

because there are so many factors to consider. Ultimately, though, the ideal security suite provides this set of capabilities:

- Easy installation and configuration, with the ability to install prerequisites and synchronize with your existing Active Directory infrastructure.
- Sensible policy management organized by capability and task, rather than following arbitrary divisions in the product's architecture, with straightforward configuration that simplifies things for the IT administrator and is informed by vendor intelligence e.g. sample policies or pre-defined application lists or rules.
- Data protection capabilities to ensure your PCs and network are secured not just against malware, but also against misappropriation of sensitive data.

- Visibility and threat reporting capabilities that let you know your enterprise is protected, rapidly take action when it isn't, and get clear indications of compromised endpoints so you can take appropriate action.
- Good performance so your users maintain their productivity.
- Responsive technical support that gets you clear answers with minimal wait times and limited gate-keeping.

On top of all this, the suite should be cohesive and integrated so you don't have to manage a myriad of disparate products.

Our overall matrix provides a summary of each product's capabilities in these areas, and individual product reviews address each factor in further detail.

Performance Spotlight

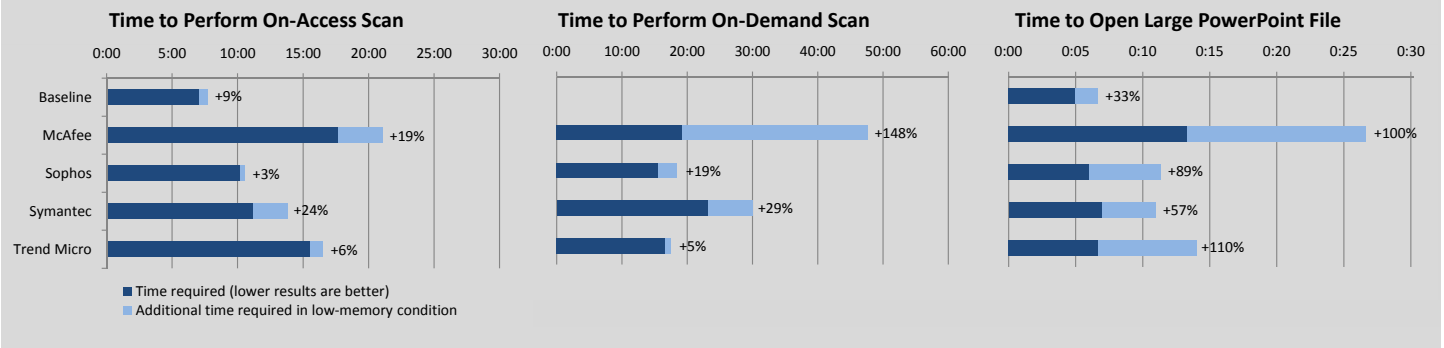
Performance remains an important consideration in choosing a security suite: Products that impose too much overhead can slow down users, reducing their productivity and leading to frustration. Our testing demonstrated significant differences in the performance costs products impose on users, with Sophos being fastest overall, Symantec and Trend Micro turning in good results, and McAfee disappointingly slow.

We first tested performance in a best-case scenario, on desktop machines with 2GB of RAM and no other applications running. Then, to simulate more heavily loaded systems running multiple applications, we depleted memory so that only 256MB remained. Trend Micro and Sophos were affected relatively little by the reduction in memory, as the charts below illustrate.

We also analyzed the impact of endpoint security programs

on system reboot time. In general, we found that the endpoint security software packages added 20 to 60 seconds to the time required to shut down and restart a system. We did not include this data in our performance charts, though, because we found a fundamental inconsistency in how products behaved after they rebooted.

When we added the EICAR test "virus" to the startup folder, Sophos and Symantec successfully detected and blocked its execution during the boot process. McAfee and Trend Micro, though, both missed the test virus and allowed it to execute. Neither Trend nor McAfee enable their on-access scanning capabilities until after the machine completes booting, which makes boot up faster but leaves a potential window of opportunity for malware to infect a machine. This inconsistency made it impractical to do any meaningful comparison as it is difficult for us to accurately determine when we could really consider a reboot complete.



The Suites We Reviewed

We tested the latest versions of the four leading enterprise endpoint security products, as indicated by Gartner's 2009 Magic Quadrant for the category, from McAfee, Sophos, Symantec, and Trend Micro targeted at midsize and large enterprises.

McAfee Total Protection for

Endpoint 8.7i (ePO 4.5) is all about control. If you take the time to master its complex interface, it can provide you with deep control over detailed security settings. But installation and configuration and policy management are challenging, and the client was the slowest we tested.

Sophos Endpoint Security and Data

Protection 9.0 is the one package that truly combines malware and data protection. It earned high ratings in all categories. It stands out for its simplicity, speed and the most extensive device control and data loss prevention capabilities. It lacks the granular reporting capabilities some administrators will demand, however, and the firewall requires a little customizing before deployment.

Symantec Endpoint Protection 11.0

is a solid product all-around, with good ratings in most categories. It lacks integrated data loss prevention, and our experience with Symantec technical support was below average.

Trend Micro OfficeScan Client-Server Suite Advanced 10

Service Pack 1 is a confusing tangle of products in its current state. The core OfficeScan product by itself is capable, but adding components for reporting, server protection, and other features not included in OfficeScan makes the suite unwieldy to manage.

Our Findings

To determine which products best meet the security needs of enterprises, we evaluated them on six key criteria: installation and configuration; policies and management; data protection; vis-

ibility and threat management; performance; and technical support.

Installation and configuration may be a one-time affair, but it sets the tone for administrators' ongoing relationship with the product. We find that products that are complex and confusing to install are often difficult to manage on an ongoing basis.

Sophos Endpoint Security and Data

Protection 9.0 had both the fastest overall average setup time and fewest overall steps. Symantec also fared well. In comparison to Symantec and Sophos, McAfee Total Protection for

Endpoint proved to be complicated, requiring longer to install than any other product. Trend Micro's OfficeScan suite was ultimately complex and confusing even though the base product is relatively simple. Trend Micro's own technical support staff struggled to give us clear answers to questions about server protection and the intrusion prevention firewall.

Policies and management addresses how each product handles establishing protection policies. Sophos and Symantec were a pleasure to use in this regard, with clear and logical interfaces. McAfee had many granular options available but they were often nested many layers down into the interface. Trend Micro OfficeScan policy management made sense but was less flexible than other products and didn't have centralized management for its server protection product.

Data protection rates integrated device control and data loss prevention capabilities. Sophos stood out as the only product in our roundup to include true real-time data monitoring capabilities. This feature enables an administrator to configure policies to identify sensitive data in files being used by employees. Symantec, McAfee,

and Trend Micro each have standalone point products for data loss prevention functions that must be separately purchased, set up, and maintained. All of the products we looked at include some form of device control, but some were more full-featured than others; McAfee, for one, doesn't include the device control necessary for implementing realistic and effective security policies in this area.

Visibility and threat awareness

encompasses dashboards, reporting, and alerting tools, as well as the products' behavior when they detect threats on clients. Since no product can realisti-

cally be 100% effective in blocking every security threat, many companies take the position that machines must be re-imaged once any malicious activity is detected. Therefore, we focused our analysis not on raw threat detection effectiveness but on the qualitative indicators that products provide to help administrators stay abreast of individual threats and the overall protection status of their networks.

McAfee, Sophos, and Symantec all posted strong results in this area, though for different reasons. McAfee's dashboard is excellent, allowing extensive customization and providing actionable information about out-of-compliance endpoints. Sophos has a clear dashboard and, not surprisingly, better visibility into device and data breaches; for example, the dashboard includes a filter view to instantly find out-of-date endpoints so there's no need to run a report to get to the detail for such essential information. Symantec offered monitors and reports that gave useful information and access to logs that could provide great detail when necessary.

In contrast, Trend Micro doesn't include reporting in its basic OfficeScan

Sophos Endpoint Security and Data Protection 9.0 is the one package that truly combines malware and data protection.

USABILITY RATINGS

Task	McAfee	Sophos	Symantec	Trend Micro
Total installation and configuration steps and time to complete	166 steps, 5 hours	93 steps, 2.5 hours	123 steps, 3.5 hours	107 steps, 3 hours*
Add a scheduled scan	9	7	9	6
Enable scanning of potentially unwanted applications	7	7	5	6
Create read-only access for removable storage	Feature unavailable†	4	Feature unavailable†	8
Add an exception for particular device classes (e.g., encrypted USB keys)	Feature unavailable†	4	7	Feature unavailable†
Block access to application	10	5	12	Feature unavailable
View out-of-date endpoints	7 (add to dashboard)	0 (on dashboard)	0 (on dashboard)	0 (on dashboard)
Send e-mail when virus detected	13	7	8	Feature unavailable
View users/workstations overridden by application control rules	7	0 (on dashboard)	5	Feature unavailable
View users/workstations blocked by device control rules	Feature unavailable	0 (on dashboard)	5	Feature unavailable
View users/workstations that have overridden data loss prevention rules	Feature unavailable	0 (on dashboard)	Feature unavailable	Feature unavailable

Lower numbers are better, as they indicate number of steps to complete a task. The number of steps assumes that e-mail server has already been configured.

*—Includes steps to protect client endpoints, but not to install the ServerProtect component on servers.

†—While product has device control, this particular feature is not available.

suite; it requires a separate component, called Control Manager, to produce even prepackaged reports. Trend Micro was further hobbled by having multiple components—each with its own administration interface—and a design that lends itself more to monitoring log files and less to action.

Performance is important, too, since you don't want user productivity to be unduly impacted by their security software. (See the "Performance Spotlight" sidebar.) Sophos was faster than the Symantec, McAfee and Trend Micro products we tested, and particularly excelled in low-memory situations simulating desktops in active use. Trend Micro followed close behind, Symantec provided serviceable performance while McAfee was much slower than the other products across the board.

Technical support is an important aspect of the enterprise security suite, since deploying and managing these products in heterogeneous enterprise environments often involves surprises. All the companies in the review offer phone, e-mail, and Web support 24 hours a day, 7 days a week in their basic support plan, which is what we evaluated. (Premium support is available for an additional cost.) We found that Sophos' technical support stood out for its minimal gate-keeping and clear answers for most questions. McAfee's support was also good; Symantec and Trend Micro were less responsive and helpful.

Overall Ratings

In the final analysis, each product we looked had different strengths and weaknesses. Only one delivered solid

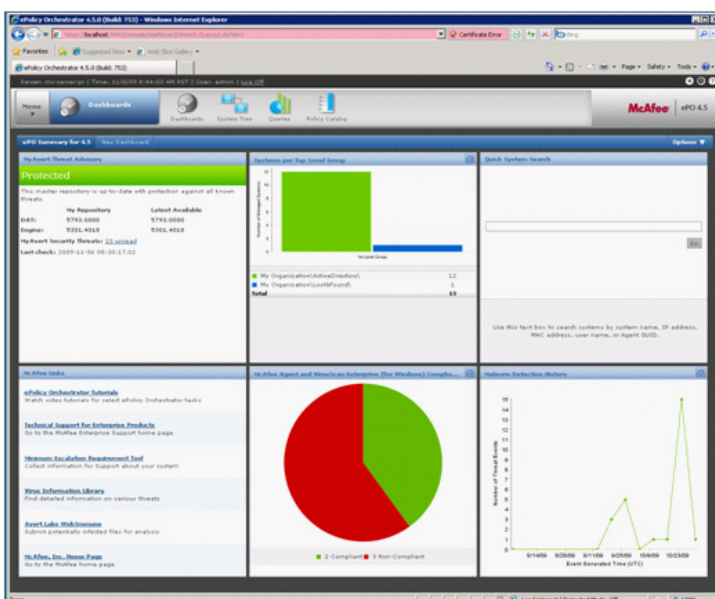
marks across our full battery tests: Sophos Endpoint Security and Data Protection 9.0.

Sophos excelled on setup, configuration, and management and delivered the fastest performance and best technical support experience. Combine this with meaningful data protection and you have a product that delivers superior protection and has the potential to reduce expenditure on security products and recurring management costs too.

Symantec Endpoint Protection offered good setup, management, and reporting features and a solid product overall but weaker performance and technical support must be considered; McAfee and Trend Micro both delivered only fair results overall mostly due to their

TECHNICAL SUPPORT RATINGS

Task	McAfee	Sophos	Symantec	Trend Micro
Rating	▲▲▲	▲▲▲▲	▲▲	▲▲
Included Support Level	Gold	Standard	Essential	Standard
Availability	24/7	24/7	24/7	Mon-Fri 8am-8pm EST
Responsiveness				
Average Wait Time (min)	22	2	12	14
Average Escalation Time (min)	0	0	10	2
Total Non-value-adding Time (min)	22	2	22	16
Easy Questions Answered by Tier 1	Yes	Yes	Yes	Yes
Difficult Questions Answered by Tier 1	Yes	Yes	No	No



McAfee's dashboards are easy to configure, with different monitors or even multiple pages of monitors.

complexity. McAfee also suffered from poor performance and a lack of included data protection capabilities. Trend Micro makes reporting a chore and struggles with multiple disconnected components.

McAfee Total Protection for Endpoint 8.7i (ePO 4.5)

The latest version of McAfee's enterprise security suite, like its predecessors, suffers from all-around complexity and poor usability. Administrators who want intensive control over every last detail of their endpoint protection may prefer it, but other products we tested provide a more approachable set of capabilities for most businesses.

McAfee took longer than any other product to install and configure—about 5 hours—and McAfee's policy management features make administrators jump through hoops to accomplish even basic tasks. The product was the slowest we tested on every test but one, and by a wide margin. The upside: If you can master its complexity, McAfee Total Protection provides detailed control over client policies and a slick, customizable dashboard that lets you take corrective action quickly.

Installation and Configuration

Installing and configuring McAfee Total Protection is a challenging affair. You first must install the prerequisite Microsoft SQL Server database, then install McAfee's ePO (ePolicy Orchestrator) platform, then "check in" individual packages for anti-virus, anti-spyware, and so on. It doesn't help that McAfee's documentation is light on practical,

how-to information, though it does provide context by explaining why things are done.

Policies and Management

The complexity continues when it comes to managing policies. McAfee's fundamental difficulty is that it organizes capabilities based on the McAfee component that happens to provide them, rather than in any sort of intuitive grouping by function. McAfee's policy management is more complex than most—the benefit of this approach being that McAfee offers highly granular control over policies and over what features users can see and change in their clients. McAfee also offers sensible default policies and in some cases, other sample policies, such as its "Typical Corporate Environment" firewall policy,

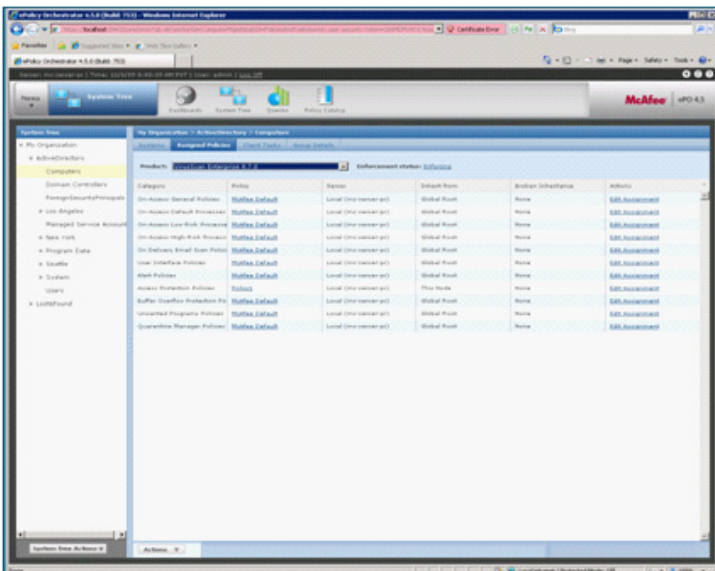
to help administrators wade through the many settings.

Data Protection

McAfee Total Protection doesn't include data protection to the extent that other products do—at least, not without buying additional products. The suite comes with no integrated data loss prevention capabilities, and what device access control it has is comparatively difficult to set up.

McAfee does offer sophisticated application control, including the ability to block the creation or hooking of applications. As McAfee says in its documentation, companies must apply this capability with care, as it can lead to users being blocked when attempting to use unknown but legitimate applications.

For device control, McAfee has limited built-in capabilities. It provides only AutoRun blocking, and we found that preventing AutoRun on USB devices was more difficult than in the other products we tested. Also, while you can



McAfee's 11 anti-virus policies make it challenging to find the settings you're looking for.

create a custom rule to block write access to a specific drive, we found that it was easy to defeat by simply assigning a different drive letter.

Visibility and Threat Management

McAfee's reporting and alert tools are powerful, and its dashboard is eye-catching, but here again administrators may find themselves struggling with complexity. An appealing feature of the dashboard is that it lets you take direct action on information, providing a fast path to correct a problem. For example, if an endpoint is out of compliance, you can immediately deploy a new agent or signature update. The dashboard also does offer a large number of charts that you can display on as many different tabs as you desire. But this flexibility comes at a price: Finding the right monitor can be time consuming, often forcing administrators to navigate through a large collection of queries organized by product component rather than functional area.

McAfee Total Protection can send any of more than 100 predefined reports, or custom reports, at hourly, daily, weekly, or monthly intervals. You can add any of more than 200 threat events to a report, and add filters to narrow results to specific groups or systems, but sending reports automatically is a cumbersome process. You can't, for example, create an ad-hoc report and then simply schedule it for repeated sending; instead, you must visit a different part of the interface.

On the client, McAfee's signature-based and behavioral protections are augmented by its SiteAdvisor capability, which provides blocking of Web sites that McAfee has assessed as risky. As with Trend Micro's Smart Protection Network, browser-based blocking provides an additional layer of security while browsing.

Performance

If you're looking for a product that won't slow your users down, then McAfee isn't for you. McAfee turned in the slowest performance results of any product we tested. In most cases it was dead last in our tests, and its performance in low-memory conditions (simulating use on a loaded system)

was especially poor.

Technical Support

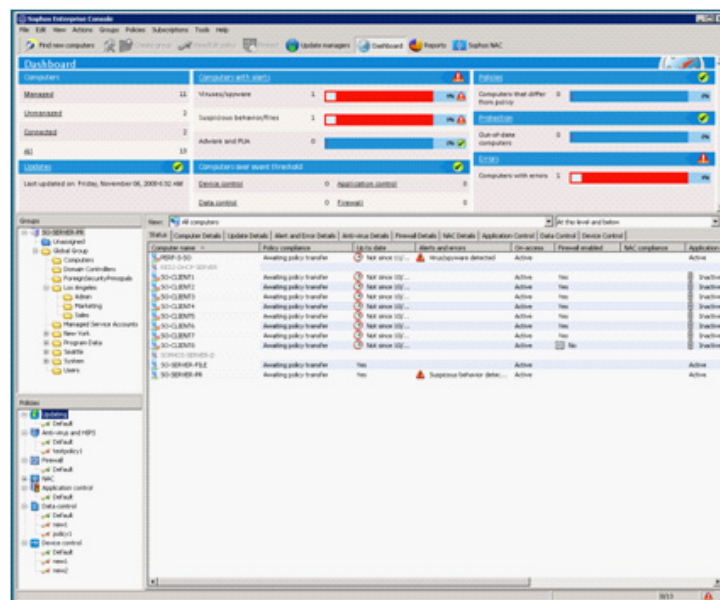
We found we needed to consult McAfee's manual more frequently than with other products. When it came time to contact live technical support, we had to endure long wait times and a painful authorization process on each call. That said, our experience overall was positive; representatives successfully answered all the questions we posed.

Conclusion

It takes a long time to install and to master the control of McAfee Total Protection, but administrators that have the time to fine-tune and want granular control over every aspect of client policy may find McAfee Total Protection an appealing option. Both the Sophos and Symantec products are faster and manage to do a better job of packaging enterprise security capabilities in a way that's easy to understand and manage.

Sophos Endpoint Security and Data Protection 9.0

The new version 9.0 of Sophos' endpoint security suite has the best installation experience, policy management, and threat visibility of any product in this review. And on data protection, Sophos stands out for its comprehensive, simple, and completely integrated approach that includes data loss prevention. It's all rounded out by fast performance and excellent technical support, making the Sophos Endpoint Security and Data Protection an appealing choice for organizations of all sizes.



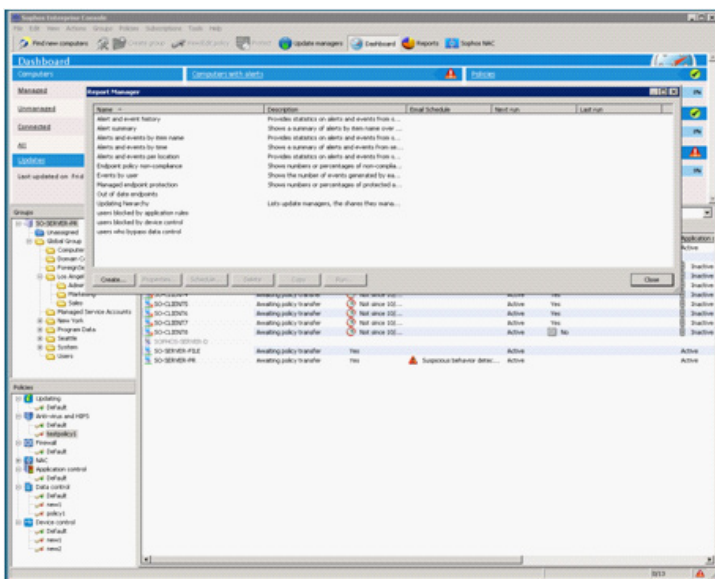
The Sophos home page shows everything the administrator needs to see in clear, easy-to-use sections.

Installation and Configuration

We found Sophos' installation and configuration on the whole to be remarkably uncomplicated for an enterprise security product, though like many suites its default firewall configuration requires some tuning. For those with mixed environments, administrators will appreciate that Sophos includes Windows, Mac, Unix, and Linux endpoint support in its base license. Sophos automatically installs the database required for the management server, and provides wizards that include compelling features, such as single-click import of an existing Active Directory structure. If you already have another security suite installed, Sophos includes the capability to uninstall and replace it.

One challenge we encountered when deploying Sophos is that its default firewall configuration stops common applications, including Internet Explorer and Windows Remote Desktop access. To deploy the firewall effectively, you should expect to spend some time running it in interactive mode and customizing it to fit your environment.

Sophos' clearly organized interface means administrators shouldn't need to refer to the Sophos documentation



Sophos includes a new report manager that is easier to use than previous versions.

often. For potentially complex tasks, such as first-time installation, upgrades, or removal of competing software products, Sophos offers PDF documentation that we found easy to follow.

Policies and Management

Sophos' Windows-based interface makes setting up groups and policies simple and transparent. The product uses multiple policies—but a manageable five, in contrast with McAfee's 11, and with fewer tabs on each. Sophos keeps everything in one window, so unlike with the Trend and McAfee products you don't need to go to multiple places in the interface or bring up additional menus. And unique among products in this review, Sophos allows you to create policies in the policies panel and then drag and drop to apply them to any given group in the groups panel.

For controlling application use in a company, Sophos takes a different approach than the other vendors. SophosLabs technicians maintain a large list of applications that is automatically updated. The product lets you select categories or individual applications to be blocked, so that blocking works even if the path or name of the application is changed. This is a useful

approach, taking the burden off the administrator to keep on top of the ever-changing details of applications that they might want to control the use of. On the downside, if an application is not on Sophos' extensive list, there is no way to add it manually; instead, a request to the Sophos technicians must be submitted.

Sophos handles intrusion prevention (HIPS) and data loss prevention in the same way with clear benefits to organizations that have limited security-focused resources and expertise.

Data Protection

Sophos' data protection capabilities are unsurpassed among the products in this review. They include data loss prevention, which lets an administrator create policies to identify sensitive data being copied onto removable storage, sent via e-mail or otherwise being transferred. Sophos make the process of identifying sensitive data simple by providing a constantly updated library of content definitions designed to locate Social Security numbers, credit or debit card numbers, and other types of personally identifiable information. Pre-defined rules reduce the learning curve and time required to manage this capability. In addition, administrators can create their own custom patterns which could be used to detect document markers or other intellectual property traits.

There are a few rough edges. For example, to monitor files copied onto USB keys the Sophos solution intercepts Windows Explorer file copies but blocks files being written direct to the

USB from within an application. When a data loss prevention rule is triggered, the product can block the transfer entirely, request end user confirmation, or allow the transfer—logging the attempt regardless of the action taken. An administrator can review logs or quickly scan activities using the event viewer, and if he notices a blocked activity that should be allowed in the future can make that change on the spot.

Sophos also includes device control with granular restrictions for specific devices. The device control includes the ability to log and to add exemptions. In addition, the product provides the ability to block access to online storage sites (e.g., Mozy), remote-access services (e.g., GotoMyPC) and mobile synchronization software (e.g., ActiveSync)—data loss channels that may not be covered by traditional data loss prevention solutions.

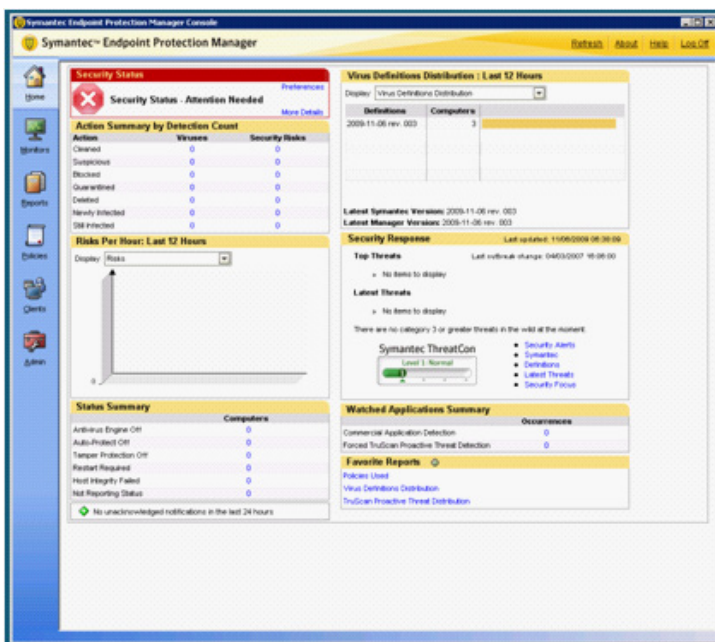
Visibility and Threat Management

Sophos' easy-to-use dashboard provides instant visibility into the areas administrators will care about on a daily basis—for example, policy exceptions, out-of-date computers, and computers that have generated threat alerts. When we tested Sophos against Web-borne exploits, its HIPS (Host Intrusion Prevention System) alerts often detected activity that would alert administrators that action is required. The new Sophos release also includes a much-improved reports manager, which makes it easier to create reports, as well as schedule and deliver them in different formats.

Setting up alerts is quick and easy. Also, when a problem is detected on an endpoint, Sophos includes links on its dashboard to navigate to the appropriate tab for fixing it. The product provides a useful set of reporting categories.

Performance

On performance, Sophos was fastest



The Symantec Home screen shows a clear representation of the overall security status for the domain.

and the clear leader, placing first or second on every test. Sophos' performance remained strong under memory constraints that simulate typical everyday use of a system. In this scenario, its on-access scan time increased just 3 percent, and its on-demand scan time by 19 percent, far better than other products.

Technical Support

Sophos' technical support was very good—the best of any we experienced in this review. We encountered short wait times, had no problems with gatekeepers (as we did with other companies), and quickly got answers to our questions.

Conclusion

Sophos Endpoint Security and Data Protection 9.0 is a well-rounded product that is fast, easy to use, and whose extensive built-in application control and data loss prevention capabilities set it apart from competitors.

Symantec Endpoint Protection 11.0

Symantec Endpoint Protection 11.0 provides a solid, effective solution for protecting corporate endpoint ma-

chines. Its management interface is sophisticated yet comprehensible. The suite offers sensible default settings that provide reasonable protection, while making installation easy. And Symantec includes device control for a large range of devices—though the granularity of its controls isn't as extensive as a typical enterprise administrator might need. We

encountered only a couple of shortcomings: Our experiences with basic Symantec technical support were frustrating, and we found some operations in the management interface awkward.

Installation and Configuration

Symantec Endpoint Protection 11.0 delivered a good experience from the outset. Thorough, easy-to-follow documentation starts things off on the right foot, preparing you with a higher-level understanding of how the product works so you can make more informed decisions

later. Symantec automatically installs the required database server, though you will need to install Microsoft IIS on the management server.

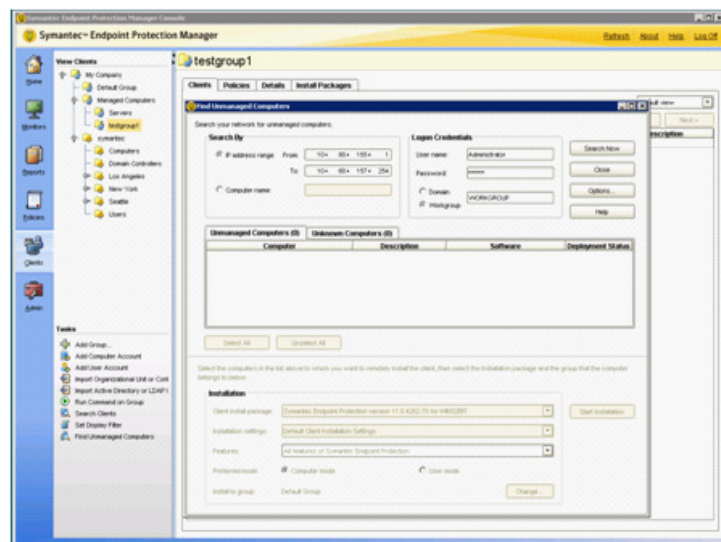
Synchronizing with Active Directory is straightforward, though not as easy as Sophos' single-click import. We found

a myriad of client deployment options, such as creating installation packages and deploying using Symantec's Altiris management application. Our chosen approach, pushing agents to clients, was a little tricky, though: push installation requires either client configuration or manual Group Policy changes documented only in Symantec's knowledge base, not the administrators' guide where you might look first.

Policies and Management

Administrators will find a clean interface for setting policies and managing endpoints. Symantec chooses reasonable default settings that will satisfy many administrators and, like McAfee, includes a number of sample policies that you can learn from and adapt to your own needs. Symantec's policy management interface is organized in a logical fashion. Symantec's interface also includes a list of recent changes in a pane, a capability we found helpful.

For application control, Symantec



With Symantec Endpoint Protection, searching for unmanaged computers not in the domain requires entering the administrator password and scanning an IP address range.

requires that you use pattern matching against process names—flexible, but also time consuming for an administrator and practically speaking unlikely to be effectively maintained day to day.

Data Protection

Symantec's device control covers a

broad range of device classes, including USB devices, floppy drives, tape drives, CD/DVD drives, printers, and generic Bluetooth devices. Attempts to access blocked devices can be logged (and reported on).

Symantec includes data loss prevention capabilities, focused on logging rather than actual prevention. Symantec logs files copied to devices, but cannot detect prohibited content within files and prevent those files from being copied at all. It's possible to restrict all drives to read-only access in the application control section of the interface. The fact that this option is located under application control is one example of how Symantec's interface can occasionally be non-intuitive.

Visibility and Threat Reporting

Symantec's dashboard is nicely organized and makes it easy to stay abreast of endpoint protection status and recent threat detections. Particularly appealing is Symantec's general overview of your enterprise, showing a red "X" if action is required or a green checkmark if all is well. If there's a problem, Symantec links to the details, but doesn't go as far as McAfee or Sophos to make it immediately correctable.

Reports are easily located under the reports tab; there's no need to search through names that don't seem to relate to what you're looking for, and it's easy to pick from a broad range of predefined reports, which allow for fine granularity (such as filtering by OS, protocol, severity, site, domain, and so on).

Symantec's threat detection and reporting is generally strong. Although it did not provide URL-level blocking to prevent loading of compromised pages in the first place, when we tested it with a selection of drive-by downloads, it often relocated dropped files before exploit code could actually execute them. And even in some cases where execution occurred, Symantec squelched the bulk of the exploit. Its

process for sending reports and alerts is simple and straightforward, and its alert system is complete and easy to use with effective dampers (throttles) for noisy alerts. But reports are only available in HTML format.

Symantec similarly provides a large variety of alerts, with many filters that parallel those in its reports. Custom reports are also easy to set up.

Performance

Although an improvement on previous versions, Symantec's speed is not a strength, and it returned average results overall. It had relatively strong performance for on-access scans when opening files or copying large folders, but its performance deteriorated in low-memory conditions designed to simulate everyday user activity—an area where Sophos excelled.

Technical Support

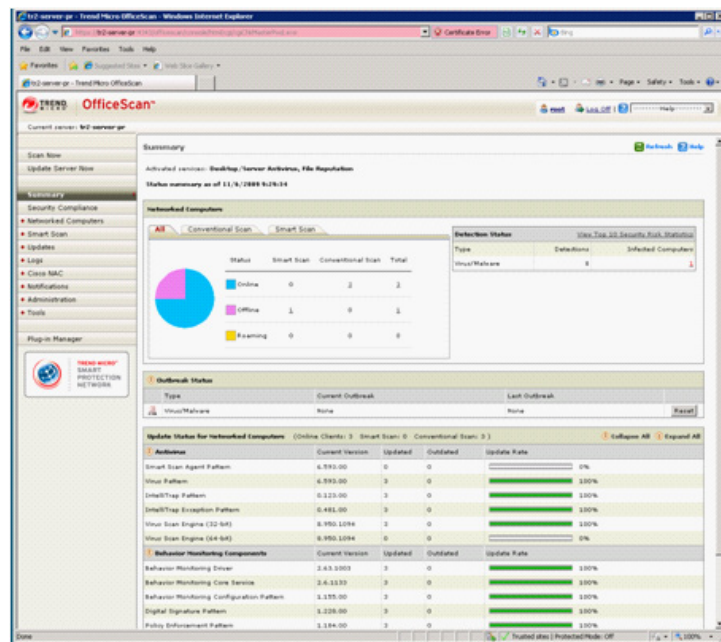
We found Symantec's technical support to be frustrating and not up to an adequate standard for busy and technically skilled enterprise administrators. The company ultimately succeeded in answering our questions, but first we had to spend a long time on hold on most calls, and then Symantec engaged in aggressive gate-keeping: The first representative often couldn't answer even basic questions, and it took us a while to get access to a more knowledgeable representative. Finding Web support for a specific product is also tricky because of Symantec's large product selection.

Conclusion

On the whole, Symantec Endpoint Security 11.0 is a well-rounded and capable product that will appeal to many enterprise buyers – that said, buyers need to consider the shortcomings in performance and technical support.

Trend Micro OfficeScan Client-Server Suite Advanced 10 SP1

Trend Micro OfficeScan, by itself, offers a simple way to manage desktop and laptop endpoints. But when you expand OfficeScan to manage the diverse array of endpoints using its full complement of components, the Trend OfficeScan Suite becomes a tangled web of complexity.



Trend Micro's dashboard shows a lot of information in a single Web-based console.

The OfficeScan client is speedy, and its use of Trend Micro's Smart Protection Network helps protect against today's Web threats by blocking malicious URLs known to Trend Micro before the malicious content is delivered to the endpoint computer. To deliver adequate protection, however, the OfficeScan suite requires ancillary components for firewall and behavioral protection, reporting, and server protection—a confusing proposition that will test the patience of many

administrators.

Installation and Configuration

The full OfficeScan installation with all of its components is an involved process—more so than a simple record

management is performed through OfficeScan domains (which are distinct from Active Directory domains), but all computers within an OfficeScan domain are in a single pool—there's no hierarchy—so administrators won't be

able to organize computers in flexible and logical ways.

As in installation, Trend Micro's component model adds complexity to management because it lacks sufficient integration. The new Intrusion Defense Firewall must be managed separately. For server protection, Trend Micro offers ServerProtect, which is not managed at all

you want reporting, you need to install a separate product, Trend Micro Control Manager, on a separate server. We installed Control Manager and found it to be little more than a log analysis tool.

A strong aspect of Trend Micro's threat management is its extensive use of URL-based blocking capabilities on clients in addition to traditional file-based blocking. During Web browsing, OfficeScan contacts Trend Micro's Smart Protection Network, a Web reputation database of potentially malicious URLs. Trend Micro also added behavioral monitoring in OfficeScan 10 Service Pack 1.

Performance

Trend Micro's performance was unremarkable and mixed—consistently better than McAfee but not usually as good as the overall performance leader, Sophos. Trend Micro's performance in low-memory on-access and on-demand scans (simulating a large number of open applications) held up well to its performance with full memory.

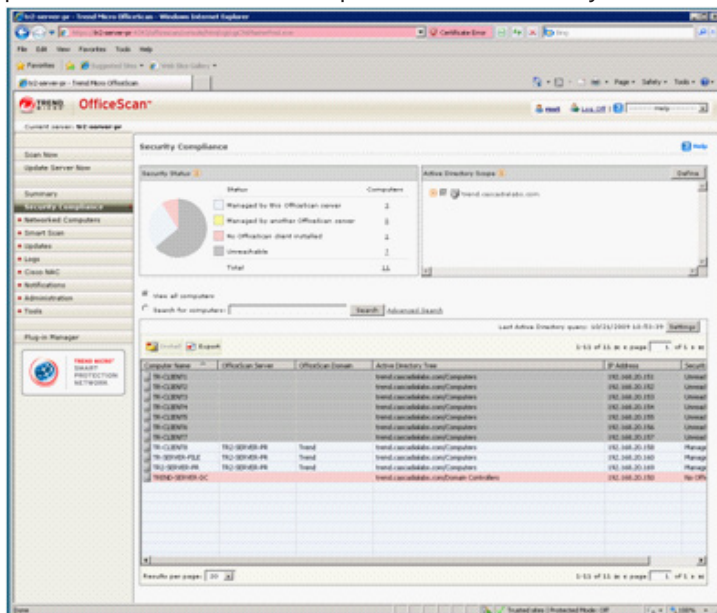
Technical Support

Our experience with Trend Micro's technical support was only fair. Wait times were long, but once we reached a representative, he or she was able to answer questions effectively and escalate issues quickly when necessary.

We found that some of the confusion in Trend Micro's product positioning leaked through to its technical-support staff. In our calls, we received conflicting answers about which of Trend Micro's two firewall products—Intrusion Defense Firewall or the native ServerProtect—was recommended. (We ultimately used Intrusion Defense Firewall.)

Conclusion

The complexity and poor integration of Trend Micro's suite, along with limited built-in reporting and inconsistent tech support, makes it a less than ideal



Reporting in the Trend Micro OfficeScan Console is limited to one on-screen compliance report that can't be sent by e-mail or exported to a file.

of steps and elapsed time adequately indicates. The product's component model allows for add-ons from Trend Micro or partners, but for administrators concerned with initial deployment, it just adds conceptual complexity. Some of the product's components, such as ServerProtect for server endpoints, require separate installation. A reporting component is not part of OfficeScan, requiring yet another piece of software to specify and install in most environments.

To add to this complexity, Trend Micro is changing its firewall strategy, transitioning from the native OfficeScan firewall to the Intrusion Defense Firewall—a completely different product. Even Trend Micro's own technical support found it challenging to provide clear insight to our firewall-related questions.

Policies and Management

Trend Micro's policy management doesn't feel fully developed. Policy

through OfficeScan.

Data Protection

Trend Micro includes device control but no data loss prevention. Setting up a policy is easy and requires little navigation of the interface: just select from a few drop-down options. Trend Micro supports fewer classes of devices than other products we tested, but offers a broad set of options to control each class of device—restricting it to read-only, read-and-execute, and so on.

Visibility and Threat Management

Trend Micro has a useful and well-organized dashboard that shows status of software and signature updates. But it provides very few alerts—just detection of virus or malware, virus or malware detected and not cleaned, and outbreak. The product's interface emphasizes events and log information rather than task-oriented goals; we found it insufficient to give a comprehensive view of an enterprise's protection status. It also lacks reporting; if

choice for most enterprises. Companies that have the patience to work with such a cumbersome product infrastructure will see solid performance and good URL-based Web-threat blocking, but adding all the components to the mix ultimately invites difficulty which is not ideal when you are trying to build a strong threat defense for your business.

How We Tested

Cascadia Labs aims to test products in meaningful, comparable, and reproducible ways. For areas such as technical support that invariably involve subjective judgments, we base those judgments on data we collect as impartially and objectively as possible.

At the time of our testing, companies were beginning to roll out their patches for Windows Server 2008 R2 and for Windows 7, so we didn't test products specifically on either of these platforms. All products were tested using Windows Server 2008 servers and Microsoft Windows XP SP2 client machines.

Installation, Configuration, and Administration Tasks

To quantify the ease or difficulty of installing and configuring a product, and then using various capabilities on an ongoing basis, Cascadia Labs counts the numbers of steps required for a knowledgeable administrator to successfully complete various specific usage scenarios. We consider a single "step" to be any of the following:

- Browsing or navigating to and

- opening an application or snap-in
- Opening the management console
- Clicking a button
- Entering data in a form field
- Selecting a checkbox or radio button
- Choosing an item from a menu (one step for each menu level)
- Responding to a dialog box
- Selecting an item from a pop-up menu

Performance

For performance testing, we automated specific tasks to ensure repeatable results and accurate timings, and we configured policies to ensure results are comparable between products. Typically, this meant enabling exceptions for our automation tools and leaving 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. Our on-access tests did not include compressed or archive 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. For on-demand, full-system scans, we scanned only the local hard drive and enabled scanning within compressed

and archive files.

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

We also repeated each test in a low-memory condition where machines were reconfigured with only 256 MB of total system RAM, simulating a typical desktop system running large numbers of applications simultaneously. Again, we ran each of these tests at least three times and averaged the results.

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.

Technical Support

During the course of our testing, Cascadia Labs made several calls to each company's technical-support staff with the explicit goal of evaluating their troubleshooting capabilities. We played the role of a typical IT staff member with no special perks. We recorded length of wait time before a vendor answered our call; how long it took to get what we needed once on the call and whether the first representative was able to answer our queries; and how well tech-support personnel were able to answer more difficult questions. We also noted whether the first representative was able to answer our questions or whether escalation was required. ▲



Independent evaluations of technology products

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

SOPHOS

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