Endpoint Security for Small Business

In this review:

Although it is hardly news that businesses face a variety of evolving threats to the security of their networks and computers, it might not be clear what they should do about those threats. Most decision-makers know they need desktop antivirus software — but today's proliferation of sophisticated malware means that such software is not sufficient by itself. In fact, only a combination of features, including anti-spyware techniques, behavior-based protection, and desktop firewalls, can provide comprehensive endpoint security.

Putting the correct combination together presents a particular challenge to small businesses. On the one hand, these businesses need more-centralized visibility and coordination than standalone, consumer-oriented products typically provide. On the other hand, these businesses rarely have the time or expertise required to manage complex security software designed for large enterprises.

The Ideal Security Suite

The ideal security suite for small businesses is one that supplies a broad array of effective protection to all the relevant endpoints — in other words, to all the laptops, desktops, and servers that are running Microsoft Windows and, increasingly, Mac OS X.

"On the one hand, these businesses need more-centralized visibility and coordination than standalone, consumer-oriented products typically provide."

The protection must guard against the entire spectrum of threats, which include not only the known viruses, but also new attacks that exploit vulnerabilities in operating systems and applications (sometimes known as day-zero threats); new variants of known viruses; and potentially unwanted applications (PUAs), including adware and spyware.

"On the other hand, these businesses rarely have the time or expertise required to manage complex security software designed for large enterprises."

The ideal security suite must also be easy to install and configure, with sensible defaults that do not require extensive tinkering to achieve full protection. Furthermore, the suite must be simple to manage and monitor so that out-of-date signatures and out-of-compliance machines do not inadvertently place chinks in a company's armor (After all, a security solution that has been inappropriately configured or poorly maintained will not provide consistent protection). Administrators must have the ability to schedule scans and monitor protection status, and individual users should have an on-access scan interface that alerts them to threats in real time.

Finally, the ideal security suite unifies all these capabilities into a useful deployable package on each endpoint — with the smallest possible demands on the computer's processor and memory so as not to interfere with core business tasks.

The Evaluated Security Suites

Security software vendors offer a great number of choices: single-function products as well as integrated ones; suites that have been designed for consumers, small businesses, or large enterprises; and software that you manage locally on your network or that is delivered as a managed service.

For this review, we evaluated the locally-managed endpoint security software packages from Sophos and Symantec, as well as the managed service from McAfee; all three of which target small businesses. The packages we evaluated contain integrated protection against viruses,

RATINGS TABLE

Category	McAfee Total Protection for Small Business	Sophos Computer Security SBE 2.0	Symantec Client Security 3.1
Installation & Deployment	▲▲▲	▲▲▲▲▲	▲
Usability & Management	▲▲▲	▲▲▲▲	▲▲
Visibility	▲▲▲	▲▲▲▲	▲▲▲
Effectiveness *(Signature-Based)*	▲▲▲▲	▲▲▲▲	▲▲▲▲
Effectiveness *(Day-Zero)*	▲▲▲	▲▲▲▲	▲▲
Performance	▲▲	▲▲▲	▲▲
OVERALL	▲▲▲	▲▲▲▲	▲▲
Quick Summary	With management done through a web service rather than a management server, Total Protection provides adequate protection with fewer components to install and manage.	Ideally suited for a small business, the product provides good protection including excellent behavioral protection with easy installation and intuitive management.	While protection against known malware was on par with the other products, we just can't see typical small businesses choosing this product given its complexity.
Platforms Supported	Windows 98, 2000, XP, 2003	Windows 98, Me, 2000, XP, 2003, Mac OS X	Windows 2000, XP, 2003
Technical Support	24/7	24/7	Business Hours
Price 5 Users/1 Year	$175	$241.50	$320

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

When we tested the McAfee, Sophos, and Symantec products in our security lab — using a representative small-business network consisting of Microsoft Windows Server 2003, ten Windows XP Professional workstations, and an Apple Macintosh — we found substantial differences in how they fared.

The differences became apparent as soon as we began installing the products. Sophos Computer Security SBE 2.0 used a straightforward, wizard-driven interface that selected reasonable defaults and required just 15 minutes to install and deploy. At the opposite end of spectrum, Symantec Client Security 3.1 posed more than three times as many questions as the Sophos product did — and most of the questions were relevant only to large enterprises, rather than to a small business comprised of one location and containing fewer than 50 personal computers.

spyware, and day-zero threats. We did not evaluate the products or components that each company offers to scan ingoing and outgoing e-mail at the mail server — an option that businesses hosting their own e-mail servers, such as Exchange servers, should consider.

Each of the products that we evaluated is sold according to a subscription model. You pay for a minimum of five users and for at least one year of periodic updates, which ensure that you are protected against emerging threats. The McAfee and Sophos products are backed by 24/7 support; for the Symantec product, such round-the-clock support is a premium option. The Sophos and Symantec suites allow you to install the management component on a single, existing server on your network, while the McAfee managed service hosts the management component and server.

Our Findings

As explained earlier, two factors are essential in an endpoint security suite that is targeted at small businesses.

> "When we tested the McAfee, Sophos, and Symantec products in our security lab...we found substantial differences in how they fared."

First, the suite must provide effective protection against an array of threats. Second, the suite must be easy to install and, over time, to administer.

We observed differences in effectiveness, as well. We evaluated the ability of each product to detect both known and unknown viruses, spyware, and adware. The products blocked many viruses on access, which is the ideal behavior, but for some adware and new viruses, the products often didn't take action until an installation had begun or an attack had started. When a signature or pattern-based detection was not available, we observed the ability of each product to use behavioral techniques to mitigate the damage done.

Although none of the products preemptively blocked every threat that we posed, each product used its own, unique techniques to block or mitigate the threats. When we tested using the default configurations, the Sophos product used its Behavioral

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

Activity	McAfee Total Protection for Small Business	Sophos Computer Security SBE 2.0	Symantec Client Security 3.1
Install the product and deploy to 10 endpoints	23 Steps 11 minutes	18 Steps 14 minutes	104 Steps 33 minutes
Identify an out-of-date endpoint	3 Steps 4 seconds	0 Steps Immediate	4 Steps 9 seconds
Identify an endpoint out-of-compliance with policy	Feature Not Available	0 Steps Immediate	Feature Not Available
Identify an unprotected computer	Feature Not Available	0 Steps Immediate	5 Steps 1 minute
Generate a report (All malware detections in past 24 hrs for a single computer)	4 Steps 6 seconds	6 Steps 28 seconds	10 Steps 48 seconds
Schedule a full system scan (including PUAs)	16 Steps 1:07 minutes	6 Steps 17 seconds	15 Steps 35 seconds
Scan a system and authorize a single PUA for all endpoints (not including scan time)	26 Steps 1:20 minutes	15 Steps 35 seconds	27 Steps 1:45 minutes
Authorize a list of 3 PUAs for all endpoints	20 Steps 41 seconds	15 Steps 28 seconds	17 Steps 1:20 minutes
Protect new endpoint	9 Steps 4 minutes	9 Steps 5 minutes	10 Steps 11 minutes
Authorize outbound Internet access for an application	7 Steps 35 seconds	10 Steps 34 seconds	27 Steps 2:32 minutes
Configure signature/engine update frequency	6 Steps 26 seconds	3 Steps 11 seconds	10 Steps 30 seconds
Enable application patches in updates	Feature Not Available	0 Steps Default Setting	Feature Not Available

Note: A step is defined as any mouse gesture or keystroke(s) requiring a human decision – for example, logging in, making a menu or sub-menu selection, clicking a button, checking a box, or expanding a menu. The steps are measured starting from the default view in the main page of each product's management console.

Genotype Protection and Sophos Client Firewall to block unknown threats better than either the McAfee or Symantec product did. For example, the Sophos Client Firewall successfully blocked viruses that existed on a machine we deliberately infected from spreading further across the network. Also, Behavioral Genotype Protection blocked some executable files after they were downloaded but before they began running.

The McAfee product successfully detected and removed adware setup files before they could be installed. The Symantec product worked successfully against viruses and virus variants, although its default behavioral protection did not prove effective in our testing. Additionally, we preferred the McAfee and Sophos practice of delivering intra-day malware definition updates, as opposed to the Symantec practice of delivering weekly updates, since a timely update can provide protection against a brand-new virus or variant.

The Verdict

After we tested the McAfee, Sophos, and Symantec products extensively, Sophos Computer Security SBE 2.0 stood out by clearly meeting the needs of small businesses. McAfee Total Protection for Small Business provided adequate features and usabilty, but failed to match Sophos in several key areas. We found Symantec Client Security 3.1 to be essentially unsuitable for a small-business environment because of its complex configuration requirements, lack of a dashboard containing actionable options, and poor performance when confronted with malware during a scan.

McAfee Total Protection for Small Business

McAfee Total Protection for Small Business is a relatively low-cost endpoint security solution that is provided as a managed service. As such, administrators install the endpoint software on computers they wish to protect, organize those computers into groups, and manage a security policy for each group, but do not install a mangement consle or have to worry about managing a server. Instead, adminstrators manage security policy with a Web browser through the McAfee SecurityCenter, an online service hosted by McAfee. Our testing shows McAfee Total Protection for Small business is easy to install and manage, adequate at protecting against malware, and a good value for small business. Our complaints are a lack of some visibility, alerting, remote cleanup, and reporting features, as well as noticeably slow performance.

Getting Started

Installation of Total Protection for Small Business is fast and simple. In fact, it is the fastest of all the products we tested – the network push install time was about 11 minutes

PERFORMANCE RESULTS - Comparision of scanning performance

Activity *See Note 1*	McAfee Total Protection for Small Business	Sophos Computer Security SBE 2.0	Symantec Client Security 3.1
On-Demand Scan of c: drive (No infections) *see Note 2*	11:29 minutes	5:59 minutes	12:34 minutes
On-Demand Scan of c: drive (Infected with adware)	16:26 minutes	10:17 minutes	15:11 minutes
On-Demand Scan (Single folder - 5696 files 653 MB)	3:21 minutes	1:54 minutes	3:48 minutes
On Access Scan (Folder copy - 444 files totaling 554 MB)	Off: 2:39 minutes On: 2:54 minutes Again: 2:48 minutes	Off: 2:00 minutes On: 2:18 minutes Again: 1:59 minutes	Off: 2:20 minutes On: 3:07 minutes Again: 2:28 minutes

Note 1: Results shown are averages of 3 individual measurements.

Note 2: The test data represents a minimal but realistic desktop computer (c: drive with ~13,000 files) including Windows system files. We excluded the endpoint protection software folder, Windows temp folder, and memory and registry scanning for a more consistent cross-comparison.

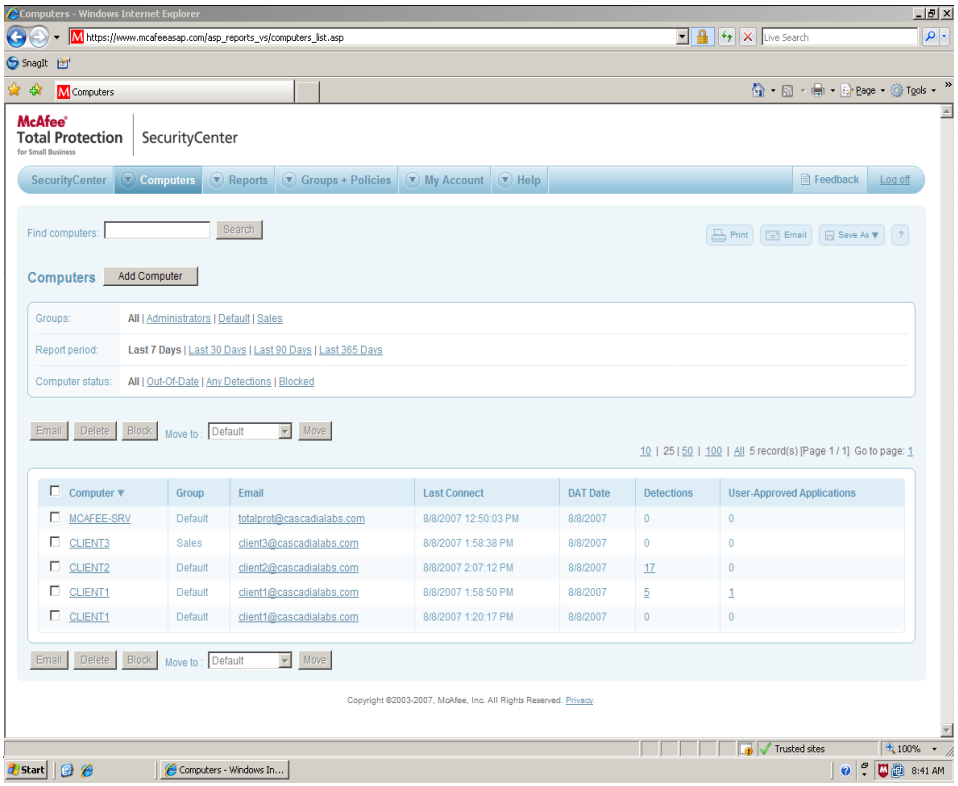
– due to the absence of installed server and console components. Administrators have three installation options: e-mailing users a link to the Total Protection for Small Business Installation Web page, running a network push installation, or using a command-line-activated install package. The e-mail-initiated option is the simplest option: users click a link in the e-mail message to open the install Web page, enter an e-mail address that serves as a username, and click the install button. However, this option requires user intervention and administrator privilege, so administrators may find themselves visiting each computer to install the product. The network push option installs Total Protection for Small Business to selected computers (similar to the other products), but only if the endpoints are joined to a common domain, which may not be the case for a small business network. The command-line option is too complicated for most small businesses as it requires integration with a network operating system login script.

McAfee provides anti-virus protection, application-specific buffer overflow protection, and firewall technology. These components provide adequate protection and deliver a good value to users, who receive the benefits of endpoint security with fewer components to manage, all at a lower cost per endpoint.

Management and Visibility

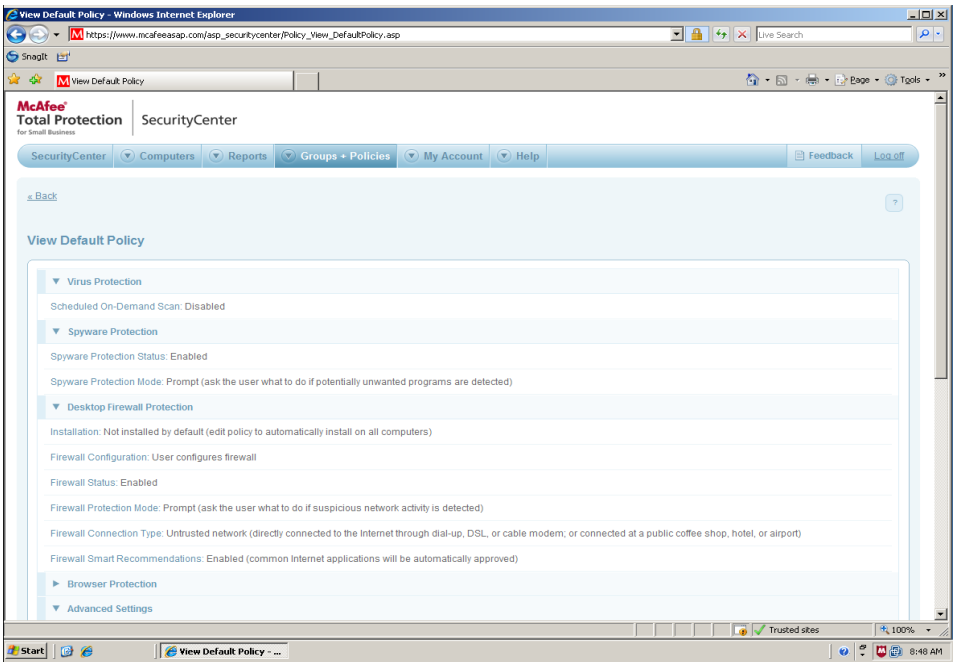
The SecurityCenter Web page contains a dashboard that displays basic information such as "Security Status," the percentage of managed endpoints with anti-virus and firewall installations, and the number of available licenses. Information such as unresolved virus infections and out-of-date computers are listed in the "Security Status" pane as clickable "Action Items," but the provided information does not reference a specific computer, so users need to navigate to a separate page to get detailed information. Navigation between pages is accomplished with a single menu bar that links to four management pages with a short pulldown menu for common actions, so users can quickly reach these areas.

McAfee hosts the SecurityCenter and the update server, and controls most of the scan settings for Total Protection for Small Business, but administrators must



The SecurityCenter allows users to quickly perform tasks and gather essential information.

Cascadia Labs



Total Protection for Small Business's Default Policy provides adequate and flexible protection.

deploy the product, organize computers into groups, and manage group policy. Policy settings are intuitively divided among four areas, similar to the Sophos Control Center, but they are a layer deeper in the management page. Management is easier than with Symantec, as is evidenced by the fewer steps required for common tasks; however, overall, the interface is not as efficient as that of Sophos. Performing a one-time scan is awkward, some useful visibility features are missing, and alerting and remote cleaning are absent, as we discuss below.

To perform a one-time scan, the group containing the target computer must be identified, and its associated policy must be edited to perform a scan at the desired date and time. Once the scan occurs, the policy must be changed back to its original settings. Remote scanning should be easier, and this approach introduces the possibility for administrators to forget to reset the scan leaving the network vulnerable. Also, an administrator will not know if a scan completes, due to the lack of any reporting for this event.

Total Protection for Small Business does provide useful pre-configured and flexible reporting on numerous events, and, like Sophos, makes these reports available through e-mail. However, reporting cannot be automated, so a user will have to set aside time to generate reports. And unlike the other products we tested, there is no tool for detecting unprotected endpoints that are not in a domain, there are no alerting features, and there is no record of completed on-demand scans for endpoints. This combination allows outbreaks to go unnoticed, with no means to confirm if scheduled scans actually execute. This scenario is mitigated by the fact that only an administrator can disable on-access scanning, so it's likely that an outbreak would originate from an unprotected or out-of-date endpoint on the network. Total Protection for Small Business is the only product that lacks remote cleaning capabilities for quarantined threats. As a result, an administrator will need to set time aside to visit each endpoint to manage the threats in quarantine.

Effectiveness

Our testing showed Total Protection for Small Business to be adequate in detecting threats with additional PUA and firewall management features. The product also includes application-specific buffer overflow protection. Overall, its scanning performance is significantly slower when compared to Sophos, and there was no way to configure or optimize the settings.

The PUA handling and the interactive firewall configuration features of Total Protection for Small Business are comparable to those offered by Sophos. Users may authorize detected PUAs and grant applications Internet access without administrator intervention. Detected applications can then be managed in the "Spyware Protection" and "Desktop Firewall" section of a group's policy. PUA handling and firewall policy can also be set to block the application or report the application and authorize its activity

Total Protection for Small Business's firewall technology is manageable, but still lacks the effectiveness of a full-fledged firewall like Sophos Client Firewall. The default firewall configuration blocks all traffic from computers outside the local network to prevent targeted hacker or incoming malware attacks. Further configuration is limited to allowing an application unlimited outbound access and opening specific ports for inbound access from local or specified remote addresses. Total Protection for Small Business does not have the application specific rules and stateful inspection features offered by Sophos or Symantec, so computers are vulnerable to application hijacking and more sophisticated hacking techniques.

Total Protection for Small Business typically makes a definition update, which we found to be as large as 5MB, available each weekday evening. Engine updates may also be included, but software updates and patches must be downloaded and installed separately. Administrators are notified at their username e-mail address when patches or software updates are available and

they will need to deploy them using the same methods as installing the product. The interval that endpoints check for updates can be set from 4 to 24 hours, users can initiate an update manually, and each computer automatically checks for an update five minutes after it is turned on. This combination of options assures administrators that computers will be kept up-to-date.

Total Protection for Small Business is supported on Windows 98, Windows 2000, Windows XP, and Windows 2003 Server editions. A version is not currently available for Macintosh, so users will need to purchase and manage a separate product for these computers. McAfee also offers Total Protection for Small Business – Advanced, for companies that want additional security protection for e-mail servers.

Conclusion

McAfee Total Protection for Small Business offers small businesses endpoint security with fast and easy installation and without an update server to manage and maintain. However, users will still need to manage product deployment, group computers, and security policy. We found the product delivered adequate protection, with some shortcomings in visibility, reporting, remote cleaning and alerting.

Price (5 endpoints, 1-year subscription): $174.90).

Sophos Computer Security Small Business Edition 2.0

For small businesses, Sophos Computer Security SBE 2.0 was easily the most suitable product that we tested. It is an effective, well-designed, and approachable endpoint security package. Its straightforward installation process and sensible default configuration make deployment easy and risk-free, and its informative dashboard simplifies ongoing monitoring and management. In terms of effectiveness, in our testing, Sophos leveraged its desktop firewall and Behavioral Genotype Protection to block and mitigate against unknown attacks better than Symantec and McAfee.

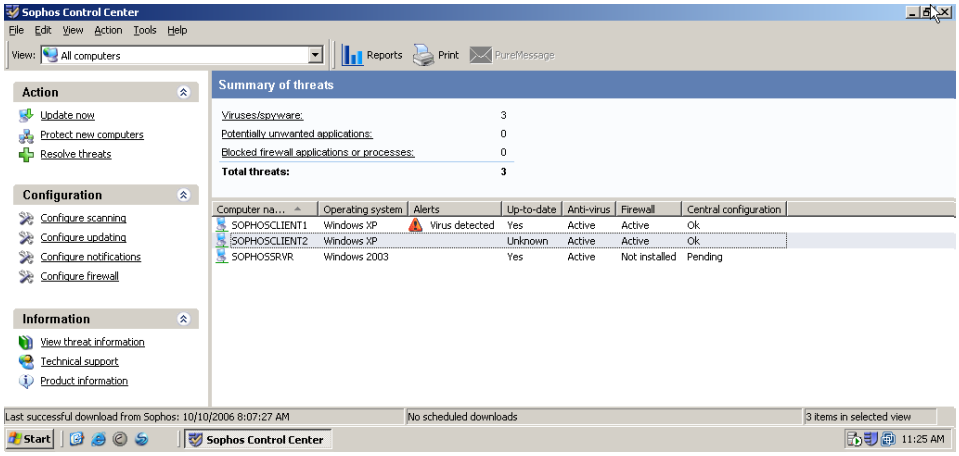
Getting Started

Sophos combines well-integrated product components with a setup wizard that limits the likelihood of making mistakes. The average small business owner can install and configure Sophos to provide effective endpoint security – unlike Symantec's product, which requires more technical acumen and patience to configure properly. We installed and deployed Sophos Computer Security SBE 2.0 to ten desktops and servers in just 15 minutes, Symantec's product took more than twice as long and the installation was far more error-prone.

Sophos Computer Security SBE 2.0 includes a complete spectrum of functionality: anti-virus, anti-spyware, desktop firewall, reporting tools, and alerting capabilities. Sophos integrates these components into a single server and a single management console, the Sophos Control Center, which gives administrators an easy-to-understand and effective dashboard that summarizes protection status of both Windows and Mac computers and present threats. The dashboard displays the state of all managed computers, indicating both out-of-compliance endpoints and endpoints not under management at all — the only product we tested that exposes this useful information at the top level of its interface.

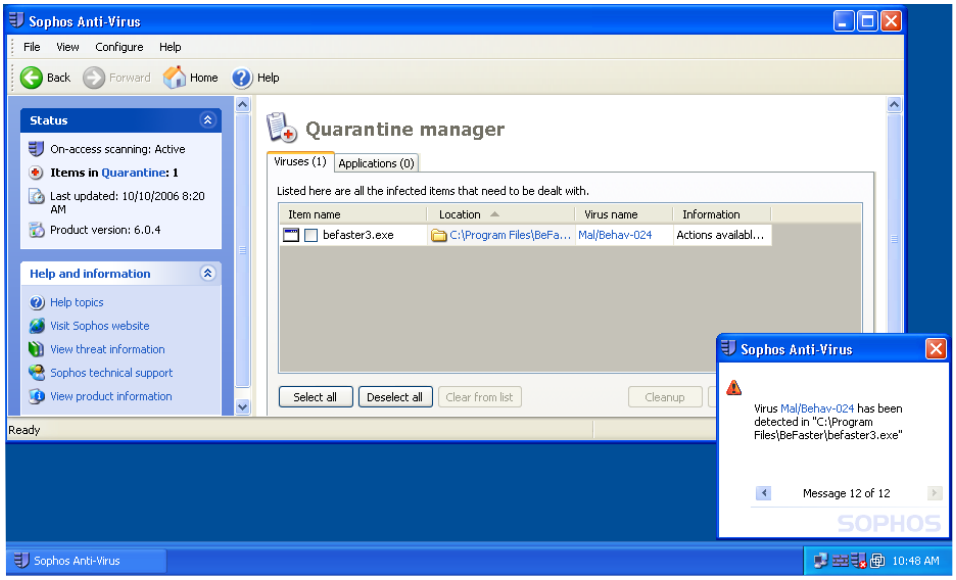
Management and Visibility

The dashboard also provides an entry point for performing essential tasks, from downloading updates and resolving threats to adding new endpoints on the network and configuring reporting and alerting. With Sophos, we were able to execute most tasks in just a few steps — managing the product would be well within the capabilities of non-expert users.



The Sophos dashboard provides a top-level overview and access to common tasks.

Aside from the effective console, Sophos offers a number of features that were unique or particularly suited to a small business. Sophos was the only product with a built-in ability to send a weekly threat summary by e-mail to individuals outside the network — a convenient way for a small business to keep an offsite IT consultant apprised of trends in the company's security situation. Sophos also handles firewall configuration and potentially unwanted application policy in an intuitive way: it presents the PUAs found and firewall breaches encountered so that administrator can easily make policy decisions with relevant data in hand.



Sophos Behavioral Genotype Protection blocks this adware that other products missed.

Specifically, a full system scan identifies potentially unwanted applications and gives administrators the option to either authorize all or selected PUAs or remove the PUAs using a remote cleanup option.

Sophos, like McAfee and Symantec, did struggle with handling exceptions for specific users. For example, although you can grant individual users authorization to use a specific PUA, you must do so on the individual machine's desktop. The administrator can tell from the dashboard that the user no longer is in compliance with the default policy, but we would prefer if the change could also be made centrally and propagated to the client.

Effectiveness

In our testing, the Sophos default security settings provided protection against a variety of threats. Like other products, Sophos blocked common viruses and variants using a combination of specific and generic pattern-based signatures. The Sophos product also had two differentiating features that proved effective during our testing – Behavioral Genotype Protection and the Sophos Client Firewall, features that provide additional protection against new and unknown malware attacks. Although both McAfee and Symantec have behavioral features, neither product demonstrated the same level of effectiveness in our testing.

In two malware test cases, an adware setup file and a keylogger, where Sophos lacked a signature, we noticed that the product applied its new Behavioral Genotype Protection to recognize suspicious behavior and block the program before it could execute and do harm. After blocking the threat, the interface prompted us to submit the file to the Sophos online security center for further analysis. Given the increasing velocity of day-zero attacks, the Behavioral Genotype Protection offers additional useful protection for endpoints.

Sophos included the most effective desktop firewall in the review. In its default configuration, the Sophos Client Firewall successfully blocked one virus from spreading over the network from machines we deliberately infected. The firewall component also includes an interactive setting, so more technically experienced users can choose to allow or deny processes that want to connect to or from their computers. While a client firewall is critical for laptops leaving the office, our testing showed it to be helpful in mitigating damage even on desktops within a protected network. By contrast, the Symantec firewall did not block this threat in its default configuration.

Sophos provides malware definition updates several times a day, more frequently than both McAfee (daily) and Symantec (weekly). In addition to the definitions and engine updates offered by all the vendors, Sophos includes application updates so small business users will be kept up-to-date automatically instead of having to sniff out software patches or updates that are often hard to find on the McAfee and Symantec Web sites. We consider these frequent and small (~250 KB) updates a benefit to businesses as they reduce the window of vulnerability between a new malware discovery and the provision of protection. McAfee sometimes releases multiple updates during a day, but Symantec normally releases updates only once a week (with exceptions under particularly volatile conditions). Sophos, by default, helps laptops remain up-to-date even while they're on the road. While endpoints first look for their parent management server for updates, they fall back to receiving their updates direct from the Sophos servers when they can't reach their default servers. And because the updates are typically very small, they work over even the slowest connections.

Sophos supports a more diverse choice of platforms than McAfee or Symantec including older versions of Windows and the Mac OS. Sophos Computer Security SBE 2.0 includes protection for workstations running Windows 98 or later or Mac OS X 10.2 or higher, and servers running Windows Server 2000, 2003, or Small Business Server. Sophos is the only product to integrate Macintosh protection directly into the console which becomes more important as the Mac OS is increasingly the target of malware attacks. Symantec and McAfee both manage Macs separately introducing an additional and separate product and management interface that administrators must contend with.

The client firewall provides protection only on workstations running Windows 2000 Professional or Windows XP.

Like the McAfee and Symantec products we reviewed, Sophos offers additional options for different deployment scenarios. Businesses with Microsoft Exchange e-mail servers may opt for the Sophos Security Suite SBE, while those wanting an anti-virus-only product may choose Sophos Anti-Virus SBE.

Conclusion

With its comprehensive scope, ease of use, and effectiveness at blocking and removing a variety of malware, Sophos Computer Security SBE 2.0 is clearly the most compelling small business solution in this test, outperforming both the McAfee and Symantec small-business endpoint security offerings.

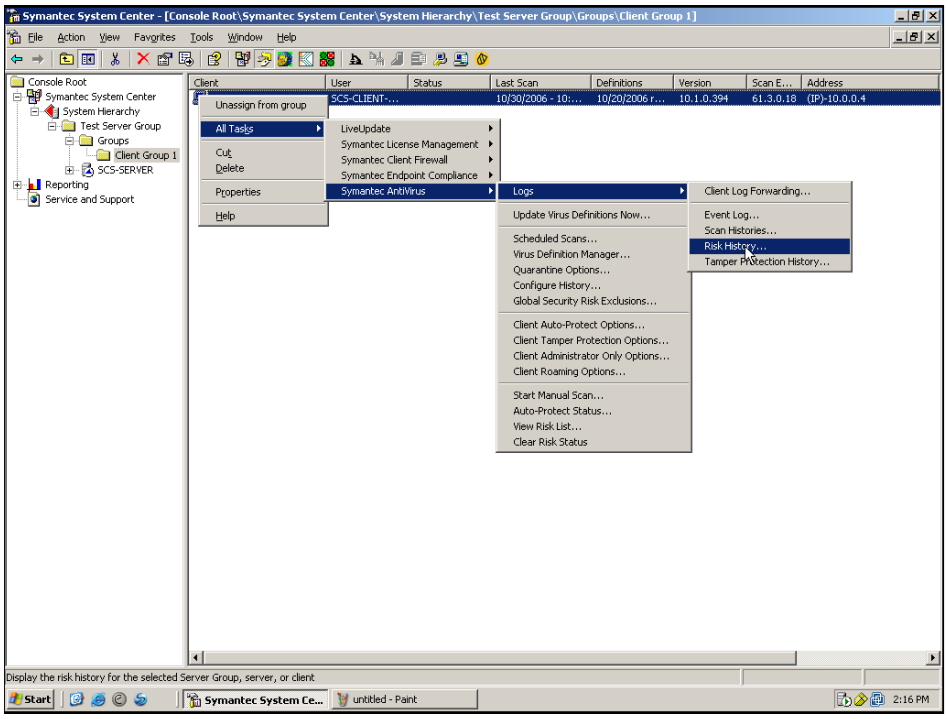
Pricing (5 endpoints, 1-year subscription): $241.50.

Symantec Client Security 3.1

Although Symantec offers Symantec Client Security 3.1 as a small businesses security solution, it's really more suitable for larger companies with more complexity to manage — and the experienced staff to manage it. We found the product more difficult to install and configure than both McAfee and Sophos; its default settings provided insufficient protection for some of the newer and previously-unknown threats we presented it with, and changing the settings is a complex task.

Getting Started

It takes a while to get Symantec up and running. A typical deployment consists of many components: the management server, a separate reporting server that runs with Microsoft Internet Information Server, two separate consoles for anti-virus management and firewall configuration, and some daunting initial configuration.



Symantec Client Security 3.1 has numerous options that present a configuration challenge for small-business users.

Performing a minimal installation and deployment of Symantec with patches entailed more than 100 steps — a far more involved process than setting up Sophos, the easiest installation of the products we tested. Symantec Client Security 3.1 lacks Active Directory integration, so administrators must select deployment targets either by using the Windows network browser or entering a list of IP addresses. Changing settings is almost always an involved affair and because such procedures require some technical ability, non-technical users should be aware that support may be required. The documentation is also very complex and in total, plan to spend a lot of time sifting through features and capabilities that are simply not appropriate for small business.

Management and Visibility

Once Symantec is installed, administrators have a multiplicity of consoles to use — a stark contrast with the more integrated tool sets provided by Sophos and to some extent, McAfee. Two of the key interfaces are an MMC (Microsoft Management Console) plug-in for managing the anti-virus component and reporting server interface and a separate, non-MMC application for creating firewall policy files. Anti-virus policy is integrated into the anti-virus MMC console, but since firewall policy distribution involves attaching policy files to objects in the anti-virus management console, administrators must store and organize these firewall policy files directly from the operating system.

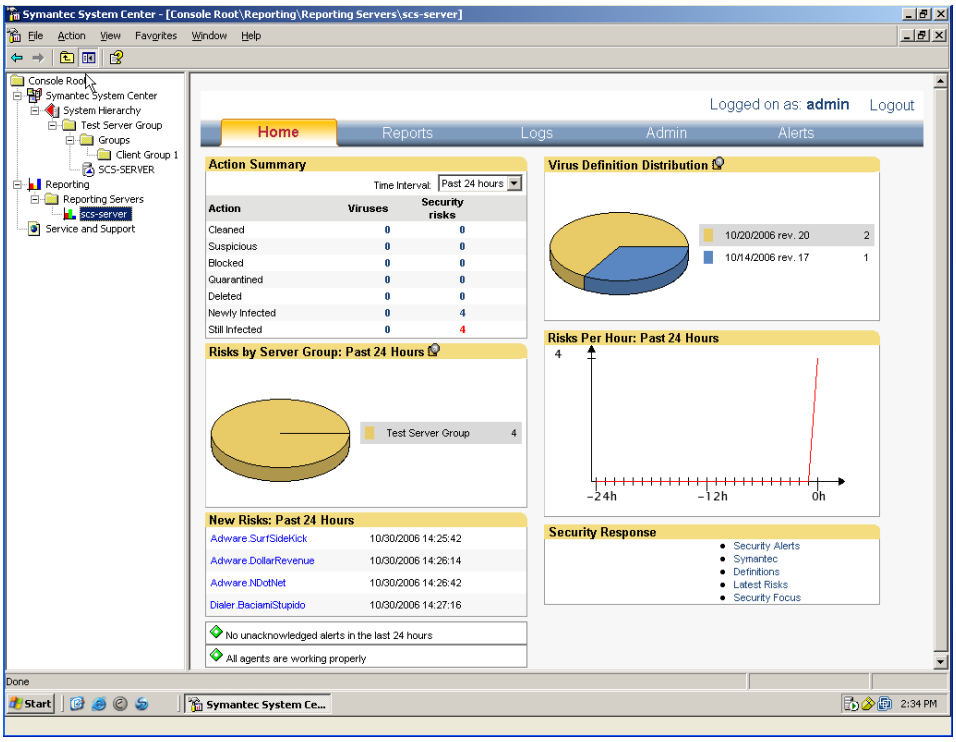
Symantec allows multiple anti-virus and firewall configurations to co-exist in one domain by dividing the domain into server groups to accommodate multiple individually configured sites. Each server group can, in turn, contain multiple client configuration groups. While a multi-level hierarchy like this is indisputably useful in enterprise environments with multiple locations, it adds unnecessary complexity for typical small-business users.

Other Symantec consoles include a quarantine management console, an update hosting console, and an additional alerting console. Then there's a set of administrative tools and utilities for creating, viewing, and managing anti-virus policies and client deployments. Symantec's grab-bag approach will be daunting for less technical sites and complexity like this invites misconfiguration which can result in compromised security. In particular, two tasks that can be crucial in some environments – setting exclusions for potentially unwanted applications and changing the default firewall policy – are among the least intuitive and most error-prone aspects of managing Symantec Client Security 3.1.

Symantec does include sophisticated reporting and alerting capabilities, though the product lacks the ability to schedule reports for automatic delivery by e-mail. The reporting server's home page provides a nice overview of threat conditions, but it doesn't have the action links or buttons of the dashboards in the McAfee and Sophos products.

Effectiveness

In our testing, Symantec was effective in protecting against common viruses and new virus variants using its signature and pattern-based approaches but fared less well with potentially unwanted applications. Although the Symantec Firewall is feature-rich, the typical small business customer won't have the technical ability to configure it properly. The default firewall configuration failed to prevent a malicious program from downloading code over the Internet. Nor did it prevent an infected desktop from becoming a mass-mailing zombie. It is possible to make firewall policy more effective by manually adding restrictions, but again, this is a difficult task for small businesses and contrasts sharply with the high level of default protection provided by the Sophos product.



Symantec's reporting server home page provides informative oversight but, unlike the other products' dashboards, lacks the ability to initiate context-sensitive actions.

Like the other products, a full scan pegged the endpoint CPU utilization at 100% making other work difficult, but further aggravating the problem, Symantec took longer to perform these scans. In our performance tests, Symantec performed around 50% slower than Sophos, and slightly slower than McAfee. During our testing timeline, we found that Symantec downloaded updates about once per week. Each of the updates was around 14 MB. While Symantec occasionally releases updates more frequently, we prefer Sophos and McAfee's approach of more frequent intra-day or daily updates.

Symantec Client Security 3.1 is supported on Windows 2000, Windows XP and Windows 2003 Server. Should you need to protect an e-mail server, a Symantec Client Security with Groupware Protection package is available, and if just anti-virus is preferred then Symantec AntiVirus with or without Groupware Protection is available. Symantec offers a Macintosh anti-virus package, it is managed separately from the Windows products.

Additionally, Symantec offers its Norton Internet Security suite, which might be a tempting alternative to small business users — but which, as a standalone product, does not provide crucial business-oriented features such as the ability to manage definition distribution, report on activity, and identify and clean infected systems remotely.

Conclusion

Because of its complexity, unless a knowledgeable consultant with Symantec experience is available, we recommend small business customers look elsewhere for their integrated endpoint security suite.

Pricing (5 endpoints, 1-year subscription): $320.

What the Ratings Signify

We installed each of these products on our test network, 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 six 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. We favored truly integrated products, those with straightforward installation wizards, and those that auto-discover endpoints through Active Directory (included in Microsoft Windows Small Business Server) or Windows NetBIOS discovery.

Usability & 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, 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 sensible default configurations that minimize configuration required to achieve reasonable protection levels.

Visibility covers the 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.

Effectiveness (Signature-Based) rates the products' ability to block an assortment of malware, including viruses, virus variants, spyware, adware, and other potentially unwanted applications using specific signatures or patterns. To provide a level playing field, our testing was conducted 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 new or unknown viruses, spyware and other malware. We evaluated anti-virus, anti-spyware, desktop firewall, buffer overflow protection, behavior-based variant protection, and other behavioral techniques. We set basic settings but otherwise tested the products in their default configuration. To provide a level playing field, our testing was conducted 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. ▲

Cascadia Labs

Independent evaluations of technology products

Contact: inquiry@cascadialabs.com
www.cascadialabs.com

SOPHOS

This comparative review, conducted independently by Cascadia Labs in October and November 2006, was sponsored by Sophos. Cascadia 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 Cascadia Labs' test plan and feedback on findings.