Usability of Endpoint Security

An independent evaluation of enterprise-level endpoint security solutions for total cost of ownership and usability metrics
Contents

Executive Summary .................................................. 3
Introduction ......................................................... 4
What Usability Means .............................................. 5
Kaspersky Business Space Security 6 ......................... 6
McAfee Total Protection for Endpoint (ePO 4.6) .......... 8
Microsoft Forefront Endpoint Protection 2010 ........... 10
Sophos Endpoint Security and Data Protection 9.7… 12
Symantec Endpoint Protection 12.1 ......................... 14
Trend Micro OfficeScan 10.5 ................................. 16
Installation & Deployment ........................................ 18
Visibility & Reporting ............................................ 19
Policy & Management .............................................. 20
Overall Results ...................................................... 22
Test Methodology .................................................. 23
Products Tested ...................................................... 24
Executive Summary

Approaching endpoint security from a usability point of view casts a new light on how security software affects business. It’s no longer about how many tens of thousands of viruses a product can capture, or blocking host access with a firewall product.

Networks have grown to such complexity that efficient deployment and administration is a key concern.

Businesses need to secure sensitive data, so a product that provides a comprehensive feature set and streamlined workflow is important.

Of the six products evaluated in this report, only McAfee and Sophos delivered the breadth of features that we feel meets the needs of enterprises.

Beyond core malware, client firewall and host intrusion protection, it is the data loss protection, device protection and full-disk encryption functionality that singles these two products out, with Sophos also combining these with the best usability.

From a usability point of view, it’s interesting to note how the levels of interaction vary widely between the products depending on the approach to the workflow, interface design and their technical implementation.

<table>
<thead>
<tr>
<th>Summary</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Kaspersky</strong></td>
<td>★★★★</td>
</tr>
<tr>
<td>Completed tasks in good time, but involved a lot of steps</td>
<td></td>
</tr>
<tr>
<td><strong>McAfee</strong></td>
<td>★★★</td>
</tr>
<tr>
<td>Completed tasks in reasonable time, but required the most complex installation process</td>
<td></td>
</tr>
<tr>
<td><strong>Microsoft</strong></td>
<td>★★★</td>
</tr>
<tr>
<td>Required the most amount of time to perform common tasks and at least 200 more user actions than other competitors</td>
<td></td>
</tr>
<tr>
<td><strong>Sophos</strong></td>
<td>★★★★★</td>
</tr>
<tr>
<td>Offers the simplest management due to wizards for many tasks, intuitive policy management and a responsive console</td>
<td></td>
</tr>
<tr>
<td><strong>Symantec</strong></td>
<td>★★★</td>
</tr>
<tr>
<td>Provides lots of features, but too many common tasks took longer than the other products</td>
<td></td>
</tr>
<tr>
<td><strong>Trend</strong></td>
<td>★★★</td>
</tr>
<tr>
<td>Completes common tasks and initial deployment easily, but lack of comparable features let this product down</td>
<td></td>
</tr>
</tbody>
</table>
Information security is not a new concept. Most people are aware of the importance of security, but organizations trying to manage increasingly complex systems continue to make mistakes.

As threats become more sophisticated, security vendors often respond with increasingly sophisticated tools to counter them. From web filtering to device level security, this “pile-on” paradigm could potentially introduce more and more complexity into the equation.

With complexity comes a higher barrier to usage and increased risk of human error. In other words, the more complex you make something, the lesser the chance it will be used, and the greater the risk you make mistakes.

The dynamics of the threat landscape demand security products that are monitored and managed on a daily basis, and this can prove costly over the course of a year.

With the backdrop of the increased need for comprehensive protection, we have assembled this report which sets out to measure the usability of endpoint security products from an administrator’s points of view.

Endpoint security protection products are centralized security management solutions designed to help businesses tackle security across the entire organization.

This report focuses on the user element of security. It considers the following core areas of a security system, from the perspective of usability:

• Installation
• Administration
• Management
• Maintenance
• Visibility and reporting

Each of these features is common in some part to all the products evaluated in this test.

Testing of such different products was done by comparing the way a range of common tasks were completed in each product. Evaluation was possible by comparing the number of steps (clicks) required, the time taken for the task to be completed, as well as the logic, automation, sense and ease of completing each task.

Products under test

To provide a useful comparison, products were selected from well known business security industry vendors.

• Kaspersky Business Space Security 6
• McAfee Total Protection for Endpoint (ePO 4.6)
• Microsoft Forefront Endpoint Protection 2010
• Sophos Endpoint Security and Data Protection 9.7
• Symantec Endpoint Protection 12.1
• Trend Micro OfficeScan 10.5
Usability—The Overlooked Feature of Endpoint Security

In the security industry, usability drives both administrative cost and product effectiveness. In other words, reduce a product’s complexity, physical design and the number of steps it takes to make it work and the frequency of how often it’s used goes up.

Think of it this way: every mouse click a software product requires, every menu selection and extra option window that needs to be navigated, costs your business money. From a cost projection standpoint usability not only predicts positive, repeatable outcomes, but also affects and controls cost centers, either positively or otherwise.

As a result of the world’s changing threats, endpoint security must constantly evolve. In fact, a good security product should be able to provide protection against current as well as future threats.

In its purest form an endpoint solution provides a remotely administered firewall and anti-virus solution. In an enterprise environment, there are many additional endpoints and security “holes” that require attention.

While the importance of complete endpoint security is undisputed, selecting a product based on features or security features alone limits both choice and capabilities.

For example, a mature security application market means many vendors now offer products that closely match each other for functionality and security performance.

On paper, product offerings may seem similar, but the way each feature is implemented can vary dramatically between products. And the way each feature is implemented significantly impacts its security performance.

Moreover, how effectively features are arranged, organized and implemented is often just as important as what the features actually are.

The term usability is open to interpretation. For the purpose of this report we consider usability to mean:

• how easily tasks can be carried out
• how quickly the product responds as it is being used (i.e., the number of steps and time required to carry them out)
• how intuitive the user interface is
• whether tasks can be automated, or if they require intervention
• the degree of intervention required (e.g., additional resources, human capital)

Ultimately, configuration reinforces complexity while simplicity of design encourages operational and administrative usability.
Kaspersky Business Space Security 6

In many respects Kaspersky Business Space Security is a bridging product that spans the gap between a small-to-medium (SMB) business and enterprise-sized corporations.

While it is lacking in some areas, Kaspersky offers an easily deployed product that also includes features like smartphone protection. For companies seeking a comprehensive all-in-one product, its lack of encryption and data loss protection is a shortcoming.

In its favor Kaspersky does support a really wide range of client operating systems, especially legacy Windows options going as far back as Windows 98 SE. This is bettered only by Sophos’ product.

Installation and deployment

Requiring nine user actions and around seven minutes to install, Kaspersky’s product was the most streamlined of any tested. Only Sophos (22 steps and just over 10 minutes) came close to matching its automation.

The installer takes a lot of drudgery out of the initial settings, the administration kit comes with Windows security components already imported. Automation for Mac and Linux platforms still requires manual download and import.

A management console Wizard is helpfully to import any required components and settings. This includes license keys, up-to-date DAT files, scan engines and additional components. The wizard also encompasses network discovery and unusually offers to configure email alerts.

Despite claiming to be able to do so, during our testing Kaspersky was unable to remove the pre-installed old antivirus product, which increases the burden for an enterprise scale deployment.

After a 17-step wizard-based Active Directory import process, another 24 steps add the installation job to any user group. This was the most steps to find unmanaged computers and deploy to them of any of the products tested. Another point to note, during our test Kaspersky didn’t keep the Active Directory structure up to date.

Visibility and reporting

Visibility and reporting is reasonably good with Kaspersky. Its main dashboard provides a basic but clear overview of the deployed endpoints. Unfortunately the update period for this isn’t made clear. Six main areas are identified by green or red light: deployment, management, policy protection, antivirus status, updates and monitoring. If an alert is raised a direct link will be displayed alongside tasks related to the area of concern.

In our test visibility and reporting task Kaspersky required the lowest number of user interactions (14) and the second lowest time of around a minute. This was one and a half times faster than Symantec, who came last, taking just over two and a half minutes.

Kaspersky provides a clear reporting system based on 11 existing templates. It’s possible to modify these according to a number of set criteria and generate custom results exported as HTML, PDF or XML.

Policy and protection

Kaspersky Business Space Security starts to show shortcomings in some of its policy design and protection—or put simply, a lack of mature features. Its security components are grouped together in a single policy. This creates a problem when creating policies for a new group, it will need to be done manually, invariably becoming a burden and adding confusion for a larger deployment.

To complete the application of all our required policy settings during testing, Kaspersky required the third highest number of steps at 183. Even so, it was still able to post the second fastest time—approximately six minutes. This time looks favorable against the 25 minutes set by Microsoft.
Kaspersky Business Space Security 6

While device control is fully integrated, the available rules are lacking. We were unable to ban unencrypted devices or to specify levels of access to specific models or volumes.

Scanning of web traffic is possible but there is no URL site blocking or filtering capabilities. There also seems to be a lack of fine monitoring for specific information and applications on individual endpoints. There seemed to be no way of blocking credit card information, no ability to log files containing confidential information, or warning users before moving, transferring or emailing confidential documents.

Under Kaspersky’s system, deployment only works for managed endpoints. Any that exist in unassigned groups need to be moved into a managed group.

In a similar way to creating a report you’re able to create administrator-defined automated tasks from a set list of predefined tasks. This makes the job of updating and applying automatic tasks to various endpoints relatively simple, though it does lack some flexibility.

<table>
<thead>
<tr>
<th>Pros</th>
<th>Cons</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Easy-to-use installation wizard</td>
<td>• Some policy settings are lengthy and require many steps</td>
</tr>
<tr>
<td>• Good visibility and reporting</td>
<td>• Device control not as comprehensive as other products in the review</td>
</tr>
</tbody>
</table>

🌟🌟🌟🌟
McAfee Total Protection for Endpoint (ePO 4.6)

McAfee Total Protection for Endpoint has been an accomplished endpoint security suite for many years. However, like its predecessors, its ePolicy Orchestrator 4.6 remains complex in terms of both deployment and configuration. Complexity aside, there is no doubting its enterprise credentials and feature set. The McAfee and Sophos product suites are the only two that provide full-disk encryption, to protect files at a system level.

The ePolicy Orchestrator 4.6 also provides detailed facilities for the core protection areas, including standard malware scanning, email scanning, device control and comprehensive data loss protection. Some of the new features introduced to this version have a somewhat tacked-on feel; in particular its data loss protection component, which has a different interface.

Installation and deployment

McAfee has the most complex installation process, requiring 133 steps, compared to just 18 for Kaspersky. But its installation time was not the slowest, finishing ahead of Trend Micro. Despite the multitude of steps, the initial management installation incorporates other additional functions, such as SQL Server installation. The suite includes comprehensive data loss protection, but this requires separate installation, which almost doubled the number of steps required.

Logging into the McAfee ePolicy Orchestrator for the first time launches a guided configuration wizard. This starts a complex sequence of 98 installation steps (the most complex encountered in this usability test), which takes just over four minutes. The wizard forces the administrator to download and install various components for the endpoint security suite by repeatedly selecting and accepting various licenses for each one. The McAfee Device Control component requires a manual download and installation for correct integration into the deployment.

The same applies if at some later stage you want to deploy an updated or additional component. This is likely to add extra work where you need to test new software or computer build images before rolling out to a production environment.

Deployment in to the imported Active Directory is a more straightforward process, requiring 40 steps, which includes the ability to remove any existing endpoint client. Support for non-domain endpoints is supplied through a rogue system detection agent, which is installed on the network and reports any endpoint activity to the management server.

Visibility and reporting

Like most of its components, McAfee’s dashboard is nice and clear, but the instant overview of the network status is poor. By default, the dashboard gives snapshot at five minute intervals. It is possible, however to customize the dashboard to display any information to make it perform comparably to other suites. Reported results often host links that take you directly to the relevant agent or can directly deploy corrective action.

The reporting system is comprehensive, with 193 base queries available. These can be copied and modified, new queries can be created from scratch, and each query can be scheduled to run at any interval. The reporting system appears highly complex, requiring the largest number of steps to complete (41 user actions, twice that of the next highest, Symantec at 21). Despite this, it outperformed both Microsoft and Symantec, completing the task in one minute and 48 seconds.
McAfee Total Protection for Endpoint (ePO 4.6)

Policy and protection
McAfee, oddly, breaks its policy management system down by a per-category basis, so policies are set for every single McAfee module that has been installed. While this is highly flexible and configurable (a possible 193, compared to 11 for VirusScan 8.8) it makes it a potentially overly complex system. Installation, with 167 steps, took just less than eight minutes, and earned it a respectable third place, just a minute behind Kaspersky.

The device manager handled all our per-device, per-volume and encryption-only policies, but it generally required more steps to complete than the other packages. As well as monitoring HTTP transfer and blocking malicious URLs, it was also possible to scan and block credit card information. Disappointingly, there seemed to be no easy way to block all applications or to track application use over the network.

Pros
- Clear dashboard
- Offers full-disk encryption

Cons
- Requires a lot of user interaction
- Complex policy management in comparison with the other products in the review
In many ways Microsoft Forefront is a difficult product to review. The product itself does very well in comparison tables, but this doesn’t tell the whole story. It requires many other software packages to complement it and enable it to function properly. Aimed entirely at the enterprise segment, Microsoft Forefront Endpoint Protection is sold either as a stand-alone product, or as part of an enterprise license. Standing alone, it relies on existing infrastructure such as Microsoft Windows Server, Microsoft SQL Server, and so on.

More worrisome from a security point-of-view, it lacks features beyond base anti-malware, it won’t pass Payment Card Industry Compliance and it still risks the loss of personal data. Besides this, it also lacks flexibility and, typical of Microsoft, there’s no cross-platform support.

The figures for the installation of Microsoft Forefront are a little bit misleading. To even get to this installation stage takes a lot of effort. To fully install this product and the prerequisites can take two to three days. Raw installation in terms of the Forefront System Center Configuration Manager plugin is one of the least involved (just 18 steps) but it takes around a quarter of an hour to complete, which is slower than Sophos, Kaspersky and Trend Micro. Being a plugin, the usage model is tied entirely to Microsoft System Center Configuration Manager (SCCM), so if your business doesn’t use SCCM this represents a sizable deployment endeavor.

In a similar manner to McAfee, SCCM requires you to install an agent on the endpoints before Forefront can be deployed.

For deployment, the System Center Configuration Manager doesn’t import the Active Directory structure, it instead uses Collections to manage endpoints that then become members of Collections based on their attributes, such as operating system type or version. This in itself caused issues during testing.

The default Active Directory structure used repeated sub-directories for similar groups (such as sales) while the collection system requires unique names throughout. Pushing the installations out to the endpoints also shows the weakness of Microsoft’s system.

**Before installation occurs**

- Install Microsoft .NET Framework 3.5 SP1
- Add additional Windows Server 2008 Roles and Features
- Install Microsoft SQL Server 2005
- Install Microsoft SQL Server 2005 Management Objects Collection
- Install SP2 for Microsoft SQL Server 2005
- Install SQL Server 2005 Critical Update 934458
- Install Microsoft Report Viewer 2008 Redistributable
- Install Windows Software Update Services 3.0 SP2
- Extend Active Directory Schema
- Install Microsoft System Center Configuration Manager 2007 with SP2
- Install R2 for Microsoft System Center Configuration Manager 2007
- Install Microsoft System Center Configuration Manager Hotfix KB2271736
Microsoft Forefront Endpoint Protection 2010

Each time the management console is launched, there’s an annoying delay of up to 30 seconds. Preparing and pushing the Forefront client is a simple job, and during testing the old security product was automatically removed without issue, Microsoft provides automatic removal of Symantec, McAfee and Trend products.

Visibility and reporting
The System Center Configuration Manager includes the main dashboard. Its interface should be well to any administrator, which does have advantages but its main shortcoming is that it can’t be built as a dedicated security interface.

The dashboard provides a good default overview of the current network status every hour, although this is configurable. Even so, an endpoint can take up to seven days to report a status change.

The console includes status for deployment, protection, security, definitions, policy and protection baselines. It’s also possible to use a number of these as links directly to the relevant sections.

We felt reporting was very limited, largely because the product depends on other Microsoft or existing Windows components to fulfill elements of its security. This leaves just three standard reports: malware activity, malware protection and a computer list, with no option to create any reports of your own or produce any on a schedule.

This limitation extended to email and notification alerts. Only malware detection alerts were possible, which was disappointing, we’d expect to be able to apply an alert to any critical event.

The reports generated during testing took an average 15 steps and just under two minutes, which is similar to McAfee and Sophos, but it was only able to complete two of the three tasks.

Policy and protection
Where Microsoft provides the capability to apply policies, it does it well, with the previously mentioned delays caused by the SCCM interface. As with its reporting, we felt somewhat limited by Forefront, more by its lack of integrated features than the policy interface. For example, we were unable to implement any external device control for encrypted drives or on a per-device or per-volume basis. Configuring the built-in Windows firewall via the SCCM interface is possible, but it isn’t as accomplished as the group policy management console.

Applying our standard antivirus policy during testing required the fewest steps of any product (24 versus 32 for McAfee and 33 for Sophos). In its favor, Forefront uses the same SCCM distribution points and low-bandwidth drip-feed style update technology, so all updates to the client are made through the same Microsoft Update catalog that will work on- or off-site.

Of significance to note was the importing of an Active Directory structure. This took a staggering 249 steps and around eight and a half minutes—four times longer than any other product. Compared to Sophos and Kaspersky (both taking around 30 seconds with less than 20 steps) it seems overly complex. Its complexity is highlighted in the full policy task table. Forefront required 392 user interactions, nearly 200 more than its nearest competitor and taking 25 minutes overall, far slower than Sophos’ two minute benchmark.

Pros
• Good for enterprises that have a Microsoft infrastructure in place

Cons
• Long list of prerequisites
• Windows only
• Limited reporting
• No instant endpoint status in the console

★★★★
Sophos Endpoint Security and Data Protection 9.7

Sophos offers the most comprehensive suite of security and data protection in this report, although it is almost matched by McAfee. These are the only products to offer full-disk encryption. With a good mix of malware protection, client firewall, application and device control, and network access control, they provide complete data protection against the threat of lost or stolen laptops, USB drives or misappropriated data.

Sophos provides protection without increasing complexity and without hindering integration or usability of its product. Impressively, Sophos also offers client support for versions of Windows reaching back to 95, as well as Mac OS X, Linux and UNIX distributions, and Windows Mobile. Importantly, these are managed using the same policies, which eases any potential management burden.

Installation and deployment
Installation for an enterprise-level product was remarkably quick and uncomplicated. The only other product in the report to manage it faster was the much less capable Kaspersky product.

Initial installation is managed by a wizard that handles base requirements, such as SQL Server 2008, and also installs the console. When started for the first time the dashboard activates a wizard that allows you to select a specific family of products and versions of the required client operating systems and then downloads the necessary components.

We were pleasantly surprised to find that Sophos provides wizards for simple deployment to non-domain endpoints and those in Active Directory. You can import the existing Active Directory structure intact. Alternatively, it is possible to select a subset of Active Directory while maintaining synchronization capabilities. Deploying the protection components involves another wizard, which includes removal of any existing security products. With just 12 steps and a few seconds for deployment to new endpoints, only Kaspersky comes close.

Visibility and reporting
The enterprise console is a refreshing change from the complexities of the McAfee and Microsoft products. It has a good design that provides a clear view of the network status in real time. By default it provides the status for endpoints, updates, malware alerts, policies, protection, errors and device/data/application control, as well as firewall events. It also displays links offering quick access to the appropriate administration areas. Also available are lists of endpoints, a tree of defined groups including any imported from Active Directory, and all policies.

Reports are based on eight predefined templates which can be scheduled to run at any time or repeated interval. Reports include event history, and events by item name, time, location, policy compliance, user, endpoint protection and update hierarchy.

While we found that Sophos was unable to produce some of the statistical reports delivered by other products, our testing showed that Sophos was almost half a minute faster at reporting than its nearest rival Kaspersky.

Policy and protection
You can easily access a full list of policies from the main dashboard. It is relatively simple to use this list to duplicate, modify or create new policies from scratch. At just 118 steps (just over two minutes) to complete all the policy settings in our tests, Sophos was three times faster than Kaspersky, and over ten times faster than Microsoft Forefront.
Sophos Endpoint Security and Data Protection 9.7

The main dashboard also includes a tree of defined groups, including any imported from Active Directory. This allows you to easily implement policies via the main dashboard to entire or individual groups. The layout works logically, involving no unnecessary steps or dialogs.

The breadth and scope of protection is impressive. Importantly with data loss protection, the level of control of information is reassuringly tight. We successfully implemented policies to block credit card numbers, log the movement of confidential files and warn users before they attempted to email specified documents. Control over devices was just as flexible, including the ability to block access to unencrypted storage, mark types of devices as read-only and block Bluetooth devices entirely.

This flexibility permeates all of Sophos’ protection components. During testing, application control enabled blocking of all unspecified applications, logging of applications being used on the network, and blocking of older versions of specific applications. This worked from a pre-supplied list of applications rather than requiring generation of a hash or specification of an executable path.

<table>
<thead>
<tr>
<th>Pros</th>
<th>Cons</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Most intuitive and responsive interface</td>
<td>• Missing some of the minor reports</td>
</tr>
<tr>
<td>• Broad feature set and platform coverage</td>
<td></td>
</tr>
</tbody>
</table>

★ ★ ★ ★ ★
Symantec Endpoint Protection 12.1 provides a well-rounded set of core enterprise-level security features. It addresses aspects including malware, client firewall, intrusion protection, and application and device control. It has a well-designed management console which includes cross-platform support for Mac OS X, many distributions of Linux, and Windows going back to XP SP3.

It does miss some of the more robust security features we’d hope for, primarily full-disk encryption and detailed data loss protection. These are offered as additional options. Importantly, the installation is conducted via a well devised workflow.

**Installation and deployment**

Symantec has done an excellent job with the basic install process, which employs a wizard that takes care of installing SQL Server and configures the management server. This requires 21 steps, and only Kaspersky and Forefront managed this in less.

Even though the installer is easy to use, it is time consuming, taking over 22 minutes to complete. Only McAfee took longer. The installation includes 32 and 64 bit packages for Windows and one for Mac. Oddly, no check is made at this stage for updated clients or malware signatures, which still have to be downloaded and imported manually. Starting the Endpoint Protection Manager for the first time initiates a welcome window which guides you through a number of first-time tasks: license status, tour, updates and deployment. If you’re unfamiliar with the product it’s easy to miss adding the Directory Server configuration at this point, but once that’s done importing the Active Directory structure takes just 22 steps.

For non-domain endpoints, the wizard can be pointed at a Windows Network Workgroup, a range of IP addresses or computer names. The only concern we noted was the removal of any previous client, which isn’t done automatically, although unsupported scripts are provided for.

**Visibility and reporting**

Symantec has a well laid out dashboard, which delivers a clear overview of the status of the systems deployed—updated at 15 minute intervals (this is configurable).

The dashboard provides information relating to endpoint status, definition version, virus and risk activity, as well as an overview of security status as a whole. Some of the results provided also act as links that enable an administrator to view further information. Five quick-links run down the side of the interface, providing access to monitors, reports, policies, clients and administration tools. Also of note is this being a Java-based interface which we feel put a minor extra burden on the management server.

Symantec offers a comprehensive system that’s based on 64 unique reports split into eight groups. Custom reports are possible via a filter that provides options for various customizations. The report query can also be scheduled to run at any interval. Although comprehensive, the Symantec product required the second largest number of steps to set up. But at 21 steps it is still only half of McAfee’s. It also took the longest time (over two and a half minutes) to produce the reports for these tasks. We also noticed that email notifications are limited to just a few events predefined by Symantec, and only two relate to malware risks.

**Policy and protection**

A clear policy link is provided on the main management dashboard and Symantec has done a good job of providing a system for modifying and creating policies. The client list also provides a logical way to implement user-created policies.

Annoyingly, policy inheritance is enforced globally on sub-groups. Changing one policy means all policies on a sub-group from then on have to be managed manually—so applying a policy takes just 35 steps, but it could then require repeated application on sub-groups. Taking a minute and a half, (second slowest) this may add up significantly.
Symantec Endpoint Protection 12.1

The flexibility of its policies is good, and we were able to add exceptions for USB devices on a per-model and per-volume basis, along with blocking Bluetooth devices. The steps required to do this were higher than the other tested products, and we were unable to specify alternative treatment for encrypted devices versus non-encrypted devices.

Application control is also available, but this was implemented in a somewhat complex manner. Effectively, you need to manually generate a checksum for the specific executable you wish to block or allow.

No data loss protection is provided. Although it is possible to specify a general file extension to monitor file types, that’s a somewhat blunt instrument. We were also unable to block credit card numbers, emailing of documents or log the transfer of confidential documents. These functions are available as optional components.

The Symantec Endpoint Security product posted the second slowest time to complete the policy and protection tasks in this test. Taking around a quarter of an hour, it was still half the time of Microsoft Forefront, but around eight times slower than Sophos.

Pros
- Feature rich, if additional modules are installed
- Intuitive interface

Cons
- Although requiring few user interactions was slow to respond for several tasks
- Was unable to remove existing antivirus product
**Trend Micro OfficeScan 10.5**

The enterprise level offering from Trend Micro, called OfficeScan, has a strong emphasis on virtual machines and on Windows. So strong in fact that, other than Microsoft, it's the only product that doesn't provide a Linux or Unix client option. A Mac client option is available, so cross-platform support isn't completely overlooked. OfficeScan also offers an optional smartphone component (as does Symantec, Microsoft and Sophos) for Android, iOS, Windows Mobile and Symbian devices.

Broadly speaking, OfficeScan provides a good range of enterprise protection, including anti-malware, client firewall, intrusion protection, web protection and device control.

Its key weaknesses when compared with the other packages here is its lack of full-disk encryption or data loss protection, and it does take an unconventional approach to policies.

**Installation and deployment**

Despite having a slick-looking installer, OfficeScan took more interactions (37) to install than any other product, but was one of the quickest at around 11 minutes.

After completing the basic installation, a plugin manager downloads each separate component needed from the Trend download site. While this ensures up-to-date engines, it's a laborious process because each component required a manual step to initiate the download and installation.

A concern we quickly identified during testing was that OfficeScan cannot import any existing Active Directory hierarchy, so while it's happy to scan the network and log discovered endpoints, it's up to the administrator to recreate any groups and hierarchy manually.

In its favor we were glad to see that any previously installed security software is automatically removed, and once the grouping is set up OfficeScan provides an easy and swift remote installation.

Interestingly, there doesn’t appear to be any way to automatically deploy to non-domain endpoints. We were forced to do manual client installs on our test systems.

**Visibility and reporting**

A browser-based dashboard keeps its resource usage low. It provides a clear overview of the network status and systems deployed. It provides information relating to online status, detections, outbreaks, updates and versions.

Unfortunately, we were not really able to determine what the update intervals actually were from looking at the dashboard. Some of the results it provides include links that enable the administrator to quickly drill down into the data using the client manager.

Overall, reporting is a very weak aspect of the OfficeScan product. Nevertheless, it was still able carry out the tasks we set for this report. Requiring 16 user interactions, and taking just over a minute, OfficeScan completed the tasks in a respectable manner.

Its graphical interface, outbreak listing, update status and client connections are nice and clear, but it does lack the depth of reporting of any other package here. An added component—Trend Micro Control Manager—is required to address this.

We were equally frustrated trying to set automated notifications for outbreaks and other behavior. It was possible (11 steps) to create email alerts for malware detection but little else.

**Policy and protection**

OfficeScan seems to depart from normal work patterns in a number of areas, one of those being its handling of policies.
Trend Micro OfficeScan 10.5

There’s no centralized policy store where each group is assigned a policy. Rather, every group has its own settings, which are inherited by subgroups. This is fine initially, but once you go down the road of breaking that inheritance, you’re left with the task of manually managing all of the (now independent) settings—greatly increasing the workload.

As an example, to apply a new policy takes 34 steps and just over a minute (about average). But even mildly complex scenarios, such as when groups have different settings, means management quickly becomes a burden. Furthermore, there’s no way to keep track of which groups have which settings.

Device protection is implemented in OfficeScan at a basic level. We were able to configure the application to block all removable devices, but couldn’t get it to allow encrypted devices or other attributes.

It also appeared to lack any level of application control. We were unable to block applications or monitor those run across the network. As a result, we expected OfficeScan to lag in the results table. Surprisingly, it holds a respectable fourth place, posting just under 10 and a half minutes.

<table>
<thead>
<tr>
<th>Pros</th>
<th>Cons</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Easy installation</td>
<td>• Limited features</td>
</tr>
<tr>
<td>★★★</td>
<td>• Setting policies can add extra work</td>
</tr>
</tbody>
</table>
Installation & Deployment

Microsoft’s Forefront has, by far, the most involved and lengthy installation. This is due to all the prerequisites you have to install before you can even think about Forefront itself—despite showing as second in the performance table.

As the table shows, Kaspersky was both the fastest and most direct. In second was Sophos, followed by Trend Micro in third. Even though there is a large range between the number of steps and time involved, all the installers were intuitive and generally allowed easy deployment.

<table>
<thead>
<tr>
<th>Task: Import AD Structure</th>
<th>Kaspersky</th>
<th>McAfee</th>
<th>Microsoft</th>
<th>Sophos</th>
<th>Symantec</th>
<th>Trend Micro</th>
</tr>
</thead>
<tbody>
<tr>
<td>STEPS</td>
<td>249</td>
<td>29</td>
<td>13</td>
<td>22</td>
<td>74</td>
<td>48</td>
</tr>
<tr>
<td>TIME (IN SECONDS)</td>
<td>515</td>
<td>32</td>
<td>17</td>
<td>45</td>
<td>24</td>
<td>88</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Task: Identify and force an update on out-of-date endpoints</th>
<th>Kaspersky</th>
<th>McAfee</th>
<th>Microsoft</th>
<th>Sophos</th>
<th>Symantec</th>
<th>Trend Micro</th>
</tr>
</thead>
<tbody>
<tr>
<td>STEPS</td>
<td>24</td>
<td>30</td>
<td>10</td>
<td>64</td>
<td>29</td>
<td>30</td>
</tr>
<tr>
<td>TIME (IN SECONDS)</td>
<td>64</td>
<td>48</td>
<td>24</td>
<td>88</td>
<td>29</td>
<td>48</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Task: Find endpoints where malware has been detected</th>
<th>Kaspersky</th>
<th>McAfee</th>
<th>Microsoft</th>
<th>Sophos</th>
<th>Symantec</th>
<th>Trend Micro</th>
</tr>
</thead>
<tbody>
<tr>
<td>STEPS</td>
<td>24</td>
<td>30</td>
<td>10</td>
<td>64</td>
<td>29</td>
<td>30</td>
</tr>
<tr>
<td>TIME (IN SECONDS)</td>
<td>64</td>
<td>48</td>
<td>24</td>
<td>88</td>
<td>29</td>
<td>48</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Task: Import AD Structure</th>
<th>Kaspersky</th>
<th>McAfee</th>
<th>Microsoft</th>
<th>Sophos</th>
<th>Symantec</th>
<th>Trend Micro</th>
</tr>
</thead>
<tbody>
<tr>
<td>STEPS</td>
<td>24</td>
<td>30</td>
<td>10</td>
<td>64</td>
<td>29</td>
<td>30</td>
</tr>
<tr>
<td>TIME (IN SECONDS)</td>
<td>64</td>
<td>48</td>
<td>24</td>
<td>88</td>
<td>29</td>
<td>48</td>
</tr>
</tbody>
</table>
Visibility & Reporting

Our tests only show a small percentage of the true reporting capability of the products under test. Our focus was on common and important everyday reports that would run frequently. Sophos was able to complete the selected tasks the fastest, ahead of Kaspersky. Symantec was the slowest, taking five times longer.

<table>
<thead>
<tr>
<th>Visibility &amp; Reporting</th>
<th>Kaspersky</th>
<th>McAfee</th>
<th>Microsoft</th>
<th>Sophos</th>
<th>Symantec</th>
<th>Trend Micro</th>
</tr>
</thead>
<tbody>
<tr>
<td>List out-of-date endpoints</td>
<td>1  0:17</td>
<td>5  0:29</td>
<td>4  0:59</td>
<td>1  0:09</td>
<td>6  1:04</td>
<td>4  0:25</td>
</tr>
<tr>
<td>Configure email notification on any virus detections</td>
<td>9  0:25</td>
<td>26  0:47</td>
<td>11  0:55</td>
<td>13  0:13</td>
<td>9  0:46</td>
<td>11  0:35</td>
</tr>
<tr>
<td>Identify all endpoints that are connected/online</td>
<td>4  0:16</td>
<td>10  0:32</td>
<td>n/a  n/a</td>
<td>1  0:06</td>
<td>6  0:45</td>
<td>1  0:18</td>
</tr>
<tr>
<td>Totals to perform once</td>
<td>14  0:58</td>
<td>41  1:48</td>
<td>15  1:54</td>
<td>15  0:28</td>
<td>21  2:35</td>
<td>16  1:18</td>
</tr>
</tbody>
</table>
Policy creation and management was where we saw the biggest divide between products. Keep in mind that we have only looked at features available in all products. The biggest feature differences to note are around importing of an Active Directory structure. Most products handle this with ease, but Microsoft Forefront requires four times longer than its nearest rival. Sophos was the outstanding performer, three times faster than any other product, and 12 times faster than Microsoft.

Different products perform differently depending on which policies are being administered, so speed and simplicity for those policies you are going to use frequently are a good starting point.

An interesting find was that a specific implementation for some products could cause more issues than the policy creation itself. For example, when policy creation deviated from the norm, the Trend Micro product began creating issues for itself, requiring repeat workloads. On complex deployments this will become a major irritation. Similarly Kaspersky and Symantec had weaknesses in their implementation which incur repeated workflows, especially when dealing with groups. Microsoft, McAfee and Sophos offer what we would consider classic policy implementation.

---

### Task: Identify and force an update on out-of-date endpoints

<table>
<thead>
<tr>
<th>Steps</th>
<th>12</th>
<th>9</th>
<th>9</th>
<th>5</th>
<th>7</th>
</tr>
</thead>
<tbody>
<tr>
<td>Time (in seconds)</td>
<td>24</td>
<td>29</td>
<td>10</td>
<td>64</td>
<td>30</td>
</tr>
</tbody>
</table>

### Task: Find endpoints where malware has been detected

<table>
<thead>
<tr>
<th>Steps</th>
<th>5</th>
<th>3</th>
<th>4</th>
<th>2</th>
<th>1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Time (in seconds)</td>
<td>17</td>
<td>21</td>
<td>6</td>
<td>30</td>
<td>21</td>
</tr>
</tbody>
</table>
### Policy & Management

<table>
<thead>
<tr>
<th>Policy &amp; Management</th>
<th>Kaspersky Steps</th>
<th>Time (mm:ss)</th>
<th>McAfee Steps</th>
<th>Time (mm:ss)</th>
<th>Microsoft Steps</th>
<th>Time (mm:ss)</th>
<th>Sophos Steps</th>
<th>Time (mm:ss)</th>
<th>Symantec Steps</th>
<th>Time (mm:ss)</th>
<th>Trend Micro Steps</th>
<th>Time (mm:ss)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Apply new antivirus policy to endpoints in the Sales subgroup in the London, Paris and New York groups, and the Admin subgroup in the London group</td>
<td>44</td>
<td>1:19</td>
<td>32</td>
<td>1:06</td>
<td>24</td>
<td>1:56</td>
<td>33</td>
<td>0:14</td>
<td>35</td>
<td>1:24</td>
<td>34</td>
<td>1:06</td>
</tr>
<tr>
<td>Identify and force an update on out-of-date endpoints</td>
<td>12</td>
<td>0:24</td>
<td>9</td>
<td>0:29</td>
<td>9</td>
<td>1:20</td>
<td>5</td>
<td>0:10</td>
<td>13</td>
<td>1:04</td>
<td>7</td>
<td>0:30</td>
</tr>
<tr>
<td>Find endpoints that have not communicated with the management server within the last seven days</td>
<td>3</td>
<td>0:16</td>
<td>4</td>
<td>0:21</td>
<td>4</td>
<td>1:10</td>
<td>3</td>
<td>0:08</td>
<td>6</td>
<td>1:38</td>
<td>3</td>
<td>0:22</td>
</tr>
<tr>
<td>Find endpoints where malware has been detected</td>
<td>5</td>
<td>0:17</td>
<td>3</td>
<td>0:21</td>
<td>4</td>
<td>1:02</td>
<td>1</td>
<td>0:06</td>
<td>2</td>
<td>0:30</td>
<td>1</td>
<td>0:21</td>
</tr>
<tr>
<td>Perform full scan on endpoint W7-SA</td>
<td>8</td>
<td>0:24</td>
<td>22</td>
<td>0:57</td>
<td>8</td>
<td>1:07</td>
<td>4</td>
<td>0:07</td>
<td>11</td>
<td>0:51</td>
<td>7</td>
<td>0:28</td>
</tr>
<tr>
<td>Perform full scan on all endpoints in the London group</td>
<td>17</td>
<td>0:27</td>
<td>11</td>
<td>0:34</td>
<td>10</td>
<td>1:10</td>
<td>6</td>
<td>0:08</td>
<td>9</td>
<td>0:46</td>
<td>9</td>
<td>0:41</td>
</tr>
<tr>
<td>Change rights of user2 from read-only to full</td>
<td>7</td>
<td>0:20</td>
<td>9</td>
<td>0:26</td>
<td>13</td>
<td>1:27</td>
<td>14</td>
<td>0:08</td>
<td>42</td>
<td>1:09</td>
<td>7</td>
<td>0:24</td>
</tr>
<tr>
<td>Allow use of PUA IE-SetSearchPage.exe (SpyCar)</td>
<td>15</td>
<td>0:28</td>
<td>8</td>
<td>0:30</td>
<td>12</td>
<td>1:25</td>
<td>9</td>
<td>0:10</td>
<td>11</td>
<td>0:52</td>
<td>10</td>
<td>0:26</td>
</tr>
<tr>
<td>Exclude C:\Enex from on-access scanning</td>
<td>13</td>
<td>0:28</td>
<td>11</td>
<td>0:37</td>
<td>12</td>
<td>1:28</td>
<td>10</td>
<td>0:11</td>
<td>14</td>
<td>0:52</td>
<td>12</td>
<td>0:28</td>
</tr>
<tr>
<td>Check on which server updates are retrieved from</td>
<td>8</td>
<td>0:29</td>
<td>5</td>
<td>0:29</td>
<td>13</td>
<td>1:30</td>
<td>1</td>
<td>0:06</td>
<td>10</td>
<td>0:55</td>
<td>3</td>
<td>0:21</td>
</tr>
<tr>
<td>Configure endpoints to update every 15 minutes</td>
<td>9</td>
<td>0:22</td>
<td>7</td>
<td>0:26</td>
<td>10</td>
<td>1:23</td>
<td>7</td>
<td>0:09</td>
<td>8</td>
<td>0:42</td>
<td>7</td>
<td>0:28</td>
</tr>
</tbody>
</table>
Overall Results

From a technical point of view, Sophos delivers the product that is not only user friendly and well designed, but executes common tasks faster and with fewer steps than other products.

Sophos is more than three times faster than many of its competitors at completing the tasks in our test. Kaspersky was the only other product to come close, but still required 55% more steps for common policy and management tasks.

Considering that the tasks in our test typically need to be completed on a daily or weekly basis, your administration time could be cut by 60%. This amounts to a significant saving.

Only two products can be considered able to meet all of the various enterprise protection demands in a single package, Sophos and McAfee.

Each of these is also well designed and efficient.

Of these three, in terms of ultimate usability, Sophos stands to save you the greatest amount of time—which naturally means money too.
Test Methodology

To provide context for this usability test, we wanted to evaluate the products as if they were deployed in a live scenario.

To ensure that a reliable comparison could be made between products, tests needed to be repeatable, timely, recordable and accurate.

We actually tested over 100 different tasks, but only a small number of these were consistent between all products. To make this a fair comparison, the evaluation focuses only on these comparable tasks.

We acknowledge that different products offer different ranges of features. The tasks chosen for this review were selected to enable a comparison of like with like.

We focused on the usability of the management console since this is the tool that administrators use regularly. We did not measure usability of the client software on the endpoint.

The test focused purely on management tasks. We did not measure the functionality of specific features. For example, when we measured how to initiate a scan from the console we did not consider how long the scan took or what the result was.

The test environment included deploying each endpoint security product over a simulated company’s world-wide network structure, consisting of a number of remote locations and specific workforce groups such as sales, administration, marketing and directors.

The test environment

The deployment for each product included a server running Microsoft Windows Server 2008 configured as an Active Directory Domain Controller using default group policies. In addition, DHCP and DNS services were also configured on this server.

A Windows Server 2008 Management Server was also deployed with a static IP address, joined to the Active Directory domain. This server was used as the host for running the client administration console and tools.

We configured five endpoints to test the feature sets, compatibility and usability of each product.

Two endpoints were configured with Windows XP Professional SP3 and connected to the network via IP addresses obtained using DHCP—one joined to the Active Directory domain and the other not. Another two endpoints (3 and 4) were deployed running Windows 7 Enterprise and connected to the network in an identical manner (only one joined to the Active Directory domain).

A management server was used as the final endpoint (endpoint 5).

An unrelated, pre-existing security product was installed on two of the endpoints to create a scenario where installation of the test product included removal of existing security software.

To evaluate the usability of each product we structured a range of basic scenarios—including installation, visibility and policy that required the use of consistent features across all products. This ensured that a fair comparison could be made.
# Products Tested

<table>
<thead>
<tr>
<th>Products</th>
<th>Kaspersky Business Space Security 6</th>
<th>McAfee Total Protection for Endpoint (ePO 4.6)</th>
<th>Microsoft Forefront Endpoint Protection 2010</th>
<th>Sophos Endpoint Security and Data Protection 9.7</th>
<th>Symantec Endpoint Protection 12.1</th>
<th>Trend Micro OfficeScan Client-Server Advanced Suite (OfficeScan 10.5)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Features</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Antivirus</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>Web protection</td>
<td>✔</td>
<td>✔</td>
<td>✗</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>Firewall</td>
<td>✔</td>
<td>✔</td>
<td>✗</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>Cross platform</td>
<td>✔</td>
<td>✔</td>
<td>✗</td>
<td>✔</td>
<td>✔</td>
<td>✗</td>
</tr>
<tr>
<td>App control</td>
<td>✔</td>
<td>✔</td>
<td>✗</td>
<td>✔</td>
<td>✔</td>
<td>✗</td>
</tr>
<tr>
<td>Device control</td>
<td>✔</td>
<td>✔</td>
<td>✗</td>
<td>✔</td>
<td>✔</td>
<td>✗</td>
</tr>
<tr>
<td>Data protection</td>
<td>✔ (Smartphone only so not tested)</td>
<td>✔</td>
<td>✗</td>
<td>✔</td>
<td>✔</td>
<td>✗</td>
</tr>
<tr>
<td>Network control</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>Encryption</td>
<td>✔ (Smartphone only so not tested)</td>
<td>✔</td>
<td>✗</td>
<td>✔</td>
<td>✔</td>
<td>✗</td>
</tr>
<tr>
<td>Virtual machine</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>Email</td>
<td>✔</td>
<td>✔</td>
<td>✗</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>HIPS</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
</tbody>
</table>

Features may vary due to license or product

- ✔ Included with installation
- ✗ Smartphone only so not tested
- ✗ Not included with installation