# IT Security Products for Business Users



# comparatives

# Review of IT Security Suites <u>for Business Users, 2</u>013

Language: English September 2013 Last revision date: 16<sup>th</sup> October 2013

www.av-comparatives.org

# Contents



About this review	3
Reviewed products	6
Management Summary	7
Avira Endpoint Security	8
Bitdefender Cloud Security for Endpoints	13
ESET Endpoint Security	17
F-Secure Client Security	22
G Data AntiVirus Business with Patch Management	28
IKARUS security.manager	32
Kaspersky Endpoint Security for Business Advanced	36
Sophos Endpoint Security and Control	40
Symantec Endpoint Protection	44
Webroot SecureAnywhere Endpoint Protection	49
Feature lists	53

# About this review

Our scenario for AV-Comparatives' 2013 Business Software Review is a single-site company network with a domain controller/file server running Windows Server 2012, and 25 client PCs, running a mix of Windows 8, Windows 7 and Windows XP. A company of this size may well not have a full-time IT manager, so we have considered the management and monitoring of the security software from the point of view of someone who is not highly trained or experienced in IT administration, and only looks after the system part-time. We do however assume that the initial installation/deployment of the software will be carried out by an IT professional who is familiar with small business networks. The increasing availability of hosted Microsoft Exchange services, combined with the fact that Windows Server 2012 has no counterpart to Small Business Server, means that we have not looked at antivirus software for Microsoft Exchange in this year's review.

Although it is a minor point, we start our review of each product by considering how easy it is for the administrator to find the right software components and documentation on the manufacturer's website. It can be time-consuming and frustrating to have to search for all the items needed, or to find that deployment has to be interrupted because a necessary component is missing. The next task for the administrator is to look at the documentation and find the sections relevant to installing the console (where applicable) and deploying the client software. We note here that "quick start guides" can be ideal for these tasks, providing they contain all the necessary details. Comprehensive manuals covering all the features, functions and options of the software need to be properly indexed and bookmarked if the reader is to find a particular section quickly and easily. Regarding installation of the management console on the server (where applicable), we would expect an IT professional to be able to install or update additional components (e.g. SQL Server), open firewall ports or create shares etc. without any assistance. However, should such actions be necessary, we feel that the console's setup program (or the manual) should make very clear exactly what needs to be done.

Even with a network of only 25 client PCs, deploying antivirus software by push installation should be considerably quicker than manually installing on each individual computer. We therefore consider how easy it is to do this with each of the reviewed products; suitable instructions in the manual, describing how to prepare the client PCs for remote installation, are invaluable here. We also look very briefly at installing the antivirus software for the server, which we would expect to be very quick and straightforward.

Once the antivirus software has been deployed, we consider how easy it is to monitor the state of the network using the console. We would expect to be warned clearly of any malware discoveries or potential security risks (e.g. the antivirus software not running or out-of-date on a client PC), and to easily find a means of rectifying any problems. Next we consider carrying out everyday maintenance tasks such as updating and scanning, and (where applicable) how to schedule such jobs.

We then shift our attention to the client antivirus software installed on the PCs. We look at warnings displayed in the event that malware is discovered or that there is a malfunction in the software, and what, if anything, the user is able to do with the program when logged on with a standard user account. We also consider whether the program makes more features available when an administrator account is used. Finally we take a very brief look at the antivirus software that protects the server.



Full details of the points we have looked at for each program are given below:

# Introduction and Software version reviewed

- Overview of the manufacturer's business products, and details of the product reviewed
- Main product version number of each of the components used

# System requirements

• Operating systems supported

# Downloading the software and documentation

• How easy is it to find everything on the website?

# Documentation

- The range of manuals available, scope of each
- How easy is it to find the right document for the job?
- How well is the documentation prepared?
- How easy is it to use?
- Which manuals were used in this test?

# Installing the console

• Are there any difficulties or points of interest?

# **Client/server antivirus management interface**

• Description of layout and features

# Deploying the antivirus software

- Deployment to clients by push installation
- Are there other installation methods, such as local installation from the client?
- Server protection installation

# **Client/server antivirus monitoring**

- Status of real-time protection
- Status of signatures (date and time of last update)
- Status of firewall if applicable
- Program version installed
- Malware discovered and result (e.g. deleted/quarantined) tested by running AMTSO Feature Settings Check on client
- Software vulnerabilities detected
- Any other relevant information
- Licensing information

# **Client/server antivirus tasks (from console)**

- Run scans: full, quick, custom once/automated
- Run a vulnerability scan once/automated

- Update signatures once/automated
- Update program version
- Enable/disable components such as real-time protection or firewall
- Add/remove components such as firewall if applicable
- Add scan exclusion
- USB device control

# **Client antivirus software**

- What is visible to the user?
- Are scan/update options available?
- Is there a status display that would alert the user in the event of a problem? If so, can the user easily fix the problem?
- By default, can components be disabled/enabled locally using (1) a Windows domain administrator account (2) a standard domain user account? If the answer to (2) is yes, can configuration options be password protected?
- What happens on malware discovery (AMTSO Feature Settings Check)?
- Is it clear to the user what, if anything, they need to do?

# Server antivirus software

- Brief description of window
- What functions are available?
- What happens on malware discovery?
- Is there a warning if e.g. real-time protection is disabled?



# **Reviewed products**

The following manufacturers participated in this review:



The products listed below were reviewed for this report. The manufacturers either provided us with the newest versions of their respective products, or confirmed that the latest version was available from their website (as at September 2013).

- AVIRA Endpoint Security 13.0
- Bitdefender Cloud Security for Endpoints 5.1
- ESET Endpoint Security 5.0
- F-Secure Client Security 11.0
- G DATA AntiVirus Business with Patch Management 12.0
- Ikarus security.manager 4.2
- Kaspersky Endpoint Security for Business Advanced 10.1
- Sophos Endpoint Security and Control 10.2
- Symantec Endpoint Protection 12.1
- Webroot SecureAnywhere Endpoint Protection 8.0

As no major flaws or problems were encountered while reviewing the products, we are pleased to be able to give our Approved Business Product Award to all the participating products.





# Management Summary

**Avira**'s mmc-based console and client software will feel very familiar and comfortable to IT professionals, and non-expert administrators will require minimal training. Documentation and client software interface are also of a very high standard. The suite impressed us with its reliable and trouble-free operation in our test.

**Bitdefender** could be deployed by a non-expert administrator due to its cloud-based console and simple local installation process for the endpoint software. The console is simple and straightforward to use.

**ESET** scores very highly with documentation and client software interface. The console is very powerful and can be customised to the administrator's needs. Non-expert administrators may initially require just a little practice to find their way around it.

**F-Secure** allows very detailed monitoring and has an excellent software update monitor to keep track of potential vulnerabilities. We feel that it could be comfortably used by non-expert administrators if some initial configuration is carried out by an IT professional.

**G Data**'s clearly laid-out console makes deploying and monitoring client software very straightforward, even if status reporting is not perfect. The minimalist interface to the client software has some obvious advantages for the administrator.

**IKARUS** is very easy to deploy and we liked the ability to reproduce the client software window on the server. The console is essentially fairly practical to use. However, we would say that there are one or two quirks to the software, which may make it more suitable for confident administrators.

**Kaspersky Lab** use the familiar mmc format and good graphic design to produce a powerful but easy-to-use console. Documentation is generally good, albeit with a couple of minor omissions. Deployment is very straightforward and the real-time progress display is excellent. The client software interface is oriented towards information display for the admin, with no user interaction available by default.

**Sophos**' business software could be used to protect larger networks but is equally well-suited to small business. Installation and deployment should not present a professional administrator with any problems, and the straightforward design of the console makes important tasks and information easy to find. The software worked very efficiently and reliably in our test.

**Symantec**'s management console is clear and simple, and good graphic design makes it particularly user-friendly. Client software is practical and familiar, and the deployment process is so simple that a non-expert administrator should be able to do it comfortably. Installation of the console itself is also very easy. In our test, we found the software to be very reliable and unproblematic.

**Webroot** is in many ways ideal for a small business without a full-time system administrator. The cloud-based console requires no installation and enables very simple deployment of client software by local installation on each PC. There are some obvious advantages to the default minimalist user interface.



# Avira Endpoint Security

		Avira Endpoint	Security				- 🗆 X
File Action View Help							
♦ ♦ 2	6 15						
<ul> <li>Avira Endpoint Security</li> <li>Avira Anagement Console Frontend</li> <li>Software Repository</li> <li>Avira Professional Security 13 (Windows), EN</li> <li>Avira Server Security 13 (Windows), EN</li> <li>Clients</li> <li>Servers</li> <li>Network neighborhood</li> <li>Events</li> <li>Reports</li> <li>Configuration</li> <li>User Management</li> <li>Info Center</li> <li>Avira Update Manager</li> </ul>	Name '\$ Eight \$ Seven \$ XP	Operating system Microsoft Windows Microsoft Windows	Computer status Offline, pending Online Online, pending	Hostnam 172.20.1.101 172.20.1.102 172.20.1.103	Config Inherited Inherited Inherited	Last notification 08/08/2013 16:42 09/08/2013 14:39 08/08/2013 16:29	Installed products Avira Professiona Avira Professiona Avira Professiona

### Introduction

Avira's small-business software for Windows consists of the Avira Management Console, Avira Professional Security client antivirus software, and Avira Server Security for protecting file servers. For larger and more complicated networks, gateway and Microsoft Exchange Server products are also available.

#### Software version reviewed

Avira Management Console 2.07 Avira Professional Security 13.0 Avira Server Security 13.0

# System requirements

According to the avira.com website, Windows Server 2008 and Windows Server 2008 R2, along with their respective Small Business Server variants, are supported server operating systems for the management console. Avira Server Security is additionally supported for Windows Server 2012. Clients can run Windows XP, Vista, and 7, all in 32 and 64-bit versions. In our test, the management console ran perfectly on Windows Server 2012. The antivirus component of Professional Security 2013 is fully compatible with Windows 8, but the firewall is not. The deployment wizard automatically deselects the Avira Firewall during installation on Windows 8, so that the Windows Firewall is used instead. Avira tell us that the upcoming 2014 version of Professional Security will be fully Windows 8 compatible.

#### Downloading the software

We found it very easy to locate the download page for Avira Endpoint Security on the Avira website, and were pleased to see that all the documentation relating not only to the console itself, but also to all possible client software packages, was available for download from the same page:

Avira Endpoint Security	Windows	Aug 1, 2013	EXE	281 MB	e
Documentation					
User Manual - Avira Professional Security		Jun 27, 2013	PDF	2 MB	e
User Manual - Avira Server Security		Jun 27, 2013	PDF	903 KB	e
User Manual - Avira AntiVir Windows Server		Aug 30, 2011	PDF	867 KB	e
User Manual - Avira Management Console		Dec 18, 2012	PDF	7 MB	e
HowTo - Avira Endpoint Security		Jun 14, 2013	PDF	839 KB	•
HowTo - Avira Management Console		Feb 12, 2013	PDF	4 MB	•
User Manual - Avira AntiVir Server (Unix)		Jan 23, 2013	PDF	430 KB	
HowTo - Avira Server Security (Windows)		Jan 16, 2012	PDF	1 MB	
HowTo - Avira Management Console for large networks		Feb 3, 2012	PDF	1 MB	
User Manual - Avira AntiVir Professional (Unix)		Sep 9, 2010	PDF	481 kB	
HowTo - Avira Professional Security (Windows)		Jul 18, 2012	PDF	3 MB	

We had assumed that the 281 MB would contain both the client and server software packages, and that we would not need to download these separately, although this turned out to be a mistake.

# Documentation

As can be seen in the screenshot in the previous section, Avira make a comprehensive range of manuals for their small business suite. Each of the three components we used (management console, client protection software, server protection software) has a full manual plus a succinct "How To" guide. We used the How-To guide for the Avira Management Console to assist with installing the console and deploying client software, and found it excellent for this task. There is just the right amount of information for an IT professional; for example, the quide does not go through all the details of installing the console, most of which are very obvious, but does explain how to configure the network settings for larger or more complicated networks. We found the instructions provided for preparing the clients, pushing out the endpoint security software, and carrying out scans and updates, to be clear and straightforward. There is a clickable table of contents at the beginning, and the document has been suitably bookmarked, providing easy access to any section through Adobe Reader's Bookmarks Bar. Screenshots are used to illustrate the instructions wherever necessary, and there is an explanation of the icons used in the software. We found the How-To guide to be an ideal companion for setting up Avira Endpoint Security.

# Installing the console

Installing the management console on our network was as quick and easy as installing iTunes. Steps included accepting the licence agreement, enter a licence key, choosing the installation folder, selecting a Windows domain account to use for management, and deciding whether to let the program automatically configure the Windows Server Firewall. Setup also asked us whether to include the client and server antivirus packages in the installation, which we accepted.

Select Features Select the features setup will install.	<b>RAVIRA</b>
Select the features you want to install, and deselect the Contemporation of the second second second (Windows) Avira Professional Security (Windows)	e features you do not want to install. Description Helps you to install and configure Avira products in your network.
286.00 MB of space required on the C drive 65224.11 MB of space available on the C drive tallShield	

**Client/server antivirus management interface** Avira Endpoint Security uses the Microsoft Management Console framework. The console tree in the left-hand pane displays the main configuration and monitoring items. These are the Software Repository (software packages to be deployed to client and server computers); Security Environment (custom-made groups to which the administrator assigns computers to managed); Network Neighbourhood be (displays the computers on the network using Microsoft's Active Directory schema); Events; Reports; Configuration; User Management; Info Center (displays news items about the product, e.g. version upgrades); Avira Update Manager, which helps the administrator keep the installed software up to date. Clicking on an item in the left-hand pane displays information and configuration options; rightclicking an item in the tree displays a menu which allows the administrator to go directly to specific tasks and configuration options. The use of the very familiar Microsoft Management Console means that IT professionals and computer enthusiasts will immediately feel at home.

# Deploying the antivirus software

We experienced one very minor glitch/misunderstanding right at the beginning of the deployment process. We had assumed that the security software packages for both the server and the clients had been already been downloaded and integrated into the console, ready for deployment. We were thus rather surprised that when we clicked on



Software Repository, no installation packages were to be seen. This was very easily rectified, however. The How To guide gave clear instructions for importing separate software packages, so we downloaded Avira Server Security and Avira Professional Security from the website, and were able to import these very quickly and easily as explained in the quide. After this minor hiccup, we found the remainder of the deployment process to be exceptionally guick and easy. First, we used the Security Environment to create two groups, one for the clients and one for the server. Next. we installed the Avira Management Console Agent on the clients this software provides communication between client and server for management and monitoring purposes. This is done by right-clicking the group (or an individual computer), pointing to Installation, AMC Agent, and then clicking Install. The status display in the main pane of the console briefly indicated that installation was underway, and then just a few moments later we could see that installation had successfully completed. We then repeated the process to install the actual security software. We note that once the agent had been installed, the client OS was recognised and the menu entry for the server software was greyed out:

Installation	•	AMC Agent	+
Configuration	•	Avira Professional Security 13 (Windows), EN	•
Commands	•	Avira Server Security 13 (Windows), EN	
Automatic update	•	Products	

Exactly the same process was used to install Avira Server Security on the server.

Once we had realised that we needed to import the software packages into the console, we found the remainder of the deployment process to be very intuitive, quick and unproblematic, and our network was protected within a few minutes.

It is possible to perform a local installation on a client PC using the .EXE setup file for Avira Professional Security. Avira do not recommend installing the agent locally, although their support staff can do this if necessary.

# **Client/server antivirus monitoring**

Clicking on a group of computers under Security Environment in the left-hand pane of the window displays the status of all the computers in that group. Details shown include computer name, OS, status, IP address, last notification, and products installed.

File Action View Help	<b>.</b>	<b>8</b> 5 3		
Avira Endpoint Security  Avira Endpoint Security  Avira Management Console Fronter  Bothware Repository  App Security Environment  App Clients  D D Eight	Name	Operating system	Com	Hostnam
	D Eight	Microsoft Windows 8 64 Bit (9200)	Online	172.20.1.101
	D Seven	Microsoft Windows 7 64 Bit Service Pack 1 (7601)	Online	172.20.1.102
	D XP	Microsoft Windows XP Professional Service Pack 3 (2600)	Online	172.20.1.103

We could not find a means of displaying the date of the signatures being used or the state of the real-time protection as such. However, if the latter is disabled, the status of the computer concerned will be shown as "Product Error", and a red exclamation mark will be displayed next to the computer's name:

Name	Operating system	Computer status
Eight	Microsoft Windows 8 64 Bit	Online, Product error
Seven	Microsoft Windows 7 64 Bit	Online
D XP	Microsoft Windows XP Prof	Online

Whilst the specific reason for this is not shown, expanding the computer's icon in the left-hand pane displays two further icons, for the AMC agent and Avira Professional Security. Clicking on the latter displays a list of events for the software, including (in this case) the fact that real-time protection had been disabled. We do not know what would be displayed here in the event that the service failed to start, or was disabled by malware.

It is also possible to change the view for the Avira Professional Security item, on a per-PC basis, so that it displays the installation/activation status of individual protection components, including real-time protection. If Avira's client firewall is installed, it is not mentioned separately in the status display, but events for it are listed along with those for real-time protection:

Avira Endpoint Security	Computer na	Level	Product	Actor	Message
Avira Management Console Fronter	A Eight	Warning	Avira Professio	Real-Time Prote	Service has been deactivated.
Software Repository	1 Eight	Warning	Avira Professio	Real-Time Prote	Service has been deactivated.
A 🛃 Security Environment	A Eight	Warning	Avira Professio	Real-Time Prote	Service has been deactivated.
4 L Clients	A Eight	Warning	Avira Professio	FireWall	Service has been deactivated.
a 🐉 Eight	A Eight	Warning	Avira Professio	FireWall	Service has been deactivated.
Mt AMC Agent	A Eight	Warning	Avira Professio	FireWall	Service has been deactivated.
🔀 Avira Professional Se	-	-			

Precise version numbers for each of the components of the client software can be found by right-clicking the Avira Professional Security icon for a particular PC, pointing to Views, and selecting Product Version.

Malware discoveries can be seen by clicking on Events in the left-hand pane, which shows all events relating to all computers on the network; alternatively, malware finds and other events for a particular computer can be seen by setting the view of that PC's Avira Professional Security icon to Events. Doubleclicking a malware event shows what action was taken (e.g. quarantining).

Avira Endpoint Security does not include a vulnerability scan. We could not find any means of displaying licensing information, other than the name of the licence file.

We feel that the simple layout of the Avira Management Console, combined with different views for many items, enables a great deal of information to be displayed without the interface becoming cluttered. However, we found that having to change views to display particular items of information, e.g. software version, was rather inconvenient. We wonder whether Avira might not allow greater customisation of the columns shown, so that it possible for the administrator to display a mix of status, version, event and task items simultaneously, without having to keep switching between views.

# **Client/server antivirus tasks**

The Avira Management Console allows a wide variety of tasks to be carried out on a single PC or an entire group by right-clicking the group and selecting an item from the contextmenu. As shown in the screenshot below, this can be used to run scans or updates, and install/uninstall or enable/disable components:

Avira Endpoint	Security	Name	Operating system	Computer st	tatus	Hostname / IP
<ul> <li>Avira Manag</li> <li>Software</li> <li>B Security</li> </ul>	ement Console Fronter Repository Environment	<ul> <li>Eight</li> <li>Seven</li> <li>XP</li> </ul>	Microsoft Windows 8 64 Bit Microsoft Windows 7 64 Bit Microsoft Windows XP Prof	Online Offline, ager Online	nt installed	172.20.1.101 172.20.1.102 172.20.1.103
▷ gHg Clien ▷ gHg Serve ▷ gHg Serve ▷ gHg Network ● Reports N Reports	Reset error state Views Installation Configuration	> > >				
Configu	Commands	•	AMC Agent	•		
👔 Info Cen	Automatic update Search Create report User permissions IP Address filter	•••	Avira Professional Security 13 (Windows) Avira Server Security 13 (Windows), EN	, EN 🕨	Start S Stop s Start u Install/ Enable	can can pdate /uninstall module /disable module:

To run a scheduled scan, the administrator selects Start Scan from the context menu shown above; the dialog box that then opens allows the scan to be scheduled. Scheduling updates works in exactly the same way.

Local client software access to is appropriately controlled by means of Windows administrator privileges, so there is no need for a password-protection feature in the management software. Scan exclusions can be set for all computers, specific groups, or individual computers, by selecting Configuration | Avira Professional Security | Configure from the context menu of the relevant item.

Avira Endpoint Security does not include any means of blocking USB devices.

We understand from reading the manual that the Avira Update Manager automatically updates both the client software already installed, and the software repository (from which the antivirus software is deployed to new clients). There is thus no need to manually update the software version installed on clients.

# **Client antivirus software**

Avira Professional Security provides the user with a fully featured window, almost identical to Avira's consumer antivirus interface. This even displays licence information:





The user is able to update signatures, run and schedule scans without restriction. There is a very obvious status display, which clearly shows if all is well by means of a suitable icon and text. A standard user is not able to deactivate real-time protection or restore quarantined items (unless administrator credentials are entered at the UAC prompt).

When an attempt is made to download the EICAR test file, Avira Professional Security displays the following alert:



Clicking on Details provides more information on the malware; the only possible action is to quarantine it. A scan is run automatically after malware has been found, and a restart is required after this.

We found Avira Professional Security's interface to be very good. Users can see the

program status and are warned in the event of a problem. They are able to update and scan themselves, but are prevented from taking any risky actions. We feel the alert on malware discovery is appropriate.

### Server antivirus software

Avira Server Security uses the MMC for its interface. Information and tasks displayed on the home page are very similar to the client software.

ile Action View Help			
• 🔿 🖄 🔛			
Console Root	Overview:	Enabled	
Statistics     Version information     About	Last full system scan	Not performed	Check system now
<ul> <li>Profile</li> <li>Quarantine</li> <li>Scheduler</li> <li>Reports</li> <li>Eventre</li> </ul>	Last update Scan engine: Virus definition file:	20/08/2013 V8.02.12.106, 14/08/2013 V7.11.97.96, 20/08/2013	<u>Start update</u>
Frence Settings	License valid until: Licensed to: Serial number:	08/08/2014 AV-Comparatives e.V. 2227008900-OEJIM- 0000003	<u>Renew</u>
	Notes:     Password is not set.     Password.     Email notification is n     go to "Settings - Ema	Please set a password under 'S ot configured. To configure the and take the desired configu	ettings - General - email notification, ration.

The status display icon and text warn in the event that e.g. real-time protection is deactivated. The EICAR test file was deleted silently when we attempted to download it. The log (Statistics) provides details of the detection.

# Summary

Avira Endpoint Security impressed us with its straightforward installation, clean verv interface using the familiar MMC console, and sensible client software. We found the suite to be entirely reliable and trouble-free in operation. Documentation is comprehensive and well produced. Our one suggestion for improvement would be to allow customisation of the client information displayed, in order to minimise the need to switch between views. Overall, we feel that experienced IT professionals should immediately feel at home with the software, and that with a little bit of training it could comfortably be used by nonexpert administrators too.



# **Bitdefender Cloud Security for Endpoints**

# Introduction

Bitdefender make a variety of business products, for companies of all sizes. Cloud Security for Endpoints uses a web-based console to manage antivirus software for client PCs and file servers.

#### Software version reviewed

Bitdefender Endpoint Security 5.1.4.227 Bitdefender Cloud Security Console as at 21<sup>st</sup> August 2013

# System requirements

Client operating systems: Windows XP, Vista, 7, 8 and 8.1, all 32 and 64-bit versions. We note that Bitdefender Cloud Security also supports Windows Embedded operating systems.

Server operating systems: Windows Server 2003, 2008, 2008 R2, 2012 and 2012 R2, along with Small Business Server variants of these.

#### Downloading the software

This is not applicable. Whichever deployment method is used, the software is automatically downloaded as part of the process.

# Documentation

Bitdefender Cloud Security has two manuals for the console, a comprehensive 119-page Administrator's Guide and a succinct 34-page Quick Start Guide. These can very conveniently be downloaded from the Help and Support page of the web console.

Both are clearly written, suitably bookmarked and have clickable contents pages. It is thus very easy to get to a particular page or section. Our one reservation about both documents is the complete lack of screenshots.

We used the Quick Start Guide to help us with the deployment of the client software. We were easily able to find clear instructions for the process in it.



### Installing the console

This is not applicable. The console is webbased, and so merely requires the administrator to open the URL and log in.

### **Client/server antivirus management interface**

The web console opens in Dashboard view. This shows key information in the form of six boxes: Network Status, Computer Status, Top 10 Most Infected Computers, Top 10 Detected Malware, Malware Activity, and Computer Malware Status. The Network Status box gives a broad overview of the protection status of all the registered computers in the form of a pie chart. Protected computers are shown as green, unprotected as red, offline as grey. This tells the administrator immediately if there are computers that need immediate attention. The Computer Status box provides details, displaying the more separate categories Updated, Antivirus, Licensed and Online, in the form of a bar chart.

#### Deploying the antivirus software

There are two methods of installing the client software on computers: local installation on individual computers, and push installation to a number of computers simultaneously. To install the software locally on a computer, the administrator merely has to log on to the web console and click on Installation Link in the Installation Area.

The installation of client PCs using push installation is clearly described in the Quick Start Guide. The section entitled "Network Discovery Requirements" details the necessary network configuration. We note that this involves setting up a WINS server and configuring clients to use it. Amongst other things, the Computer Browser Service and NetBIOS over TCP/IP have to be activated.

When the network configuration has been completed, the antivirus software has to be locally installed on one PC. Once this has been done, the client PCs to be installed will appear in the Computers view of the console. Uninstalled computers are distinguished by grey icons and lower-case names:

<ul> <li>AV-Comparatives</li> </ul>	Computer Name	▲ IP	05	Updated	Last Seen
	type here to search	type here to search	AI	AI	Al
	SERVER	172.20.2.200	Windows Server 2012 S	Yes	23 minutes ag
		172.20.2.103	Microsoft Windows XP	Yes	1 minute ag
	🗆 🛡 eight	172.20.2.101	Windows 8	never	neve
	seven	172.20.2.102	Windows 7	never	nev

Clients can then be installed from the console by selecting them and clicking Install Client from the Quick Tasks menu.

In our test, we had some difficulties with the push installation process, and noticed some inconsistencies with the status display of the clients once installed. Bitdefender inform us that this was a one-off glitch due to load issues with the servers used to host the service, and that this has now been resolved.

However, we found that local installation of the software on individual machines was a very quick and easy process, and suggest that this method is probably ideal for smaller networks.

Whether local or push installation used, there is no difference in the respective procedure for client and server computers.

# **Client/server antivirus monitoring**

The network status pie chart shows at a glance how many of the computers on the network are protected, how many are at risk, and how many are offline. Clicking on this pie chart opens a report with details for each machine, including the status of real-time protection:

Computer Name	IP 🔻	General Status	Update Status	Antimalware	License Status	Company Name
type here to search	type here to search	Al	All	All	Al	type here to search
SERVER	172.20.2.200	Vulnerable	Updated	Off	Licensed	AV-Comparatives
XP	172.20.2.103	Offline	Updated	On	Licensed	AV-Comparatives
SEVEN	172.20.2.102	Vulnerable	Updated	On	Not licensed	AV-Comparatives
EIGHT	172.20.2.101	Offline	Outdated	On	Not licensed	AV-Comparatives

When we disabled the firewall of one of our test PCs, we did not see any form of warning displayed, or any means of checking the firewall status.

We could not find a way of discovering the version number of the client software from the console, but we understand that the software is automatically kept up to date, so this is not necessary.

Of the six items displayed by default on the console Dashboard page, four relate to malware; together these surely provide enough information about malware attacks for any administrator.

Although we are expecting Bitdefender to add a vulnerability scanner to their business software very soon, we could not find any evidence of this in the version we tested.

Licensing information can be found by clicking on Account/My Account in the console.

# **Client/server antivirus tasks**

Scans can be run by selecting the machine(s) to be scanned in the Computers view, and clicking Scan in the Quick Tasks menu. A choice of Quick or Full Scan is then offered.

Scheduled scans can be set using a policy, to which a task with details and timing of the scan is added. Scan exclusions are also set here. The same process can be used to enable or disable individual components such as the firewall.

A product/signature update can be carried out by opening the About dialog, which automatically triggers an update.

Components can be installed or uninstalled from the Computers page, Quick Tasks menu, Configure Modules. We understand that Bitdefender Cloud Security for Endpoints automatically scans USB devices, but we could not find a means of blocking such devices altogether.

# **Client antivirus software**

When the main program window of the client software is opened, a minimalist interface, showing nothing more than a status display, appears:



Clicking on the double down-arrow in the centre opens up the interface:

Endpoint Security by Bitd	efender	- ×
		The system is protected. Last update 08/21/13 10:19:56
☐ Status	🗹 Security	≣ Events
- Endpoint		
Tasks		
Quick Scan Last run: N/A		Scan
Full System Scan Last run: 21.08.2013 10	09:45	Scan
Custom Scan		New
Quarantine		
Quarantine items: 0	View	Empty
-		
	*	
Bitdefender		

Scan options are clearly accessible on the Security tab. There is no update button.

In the event of a problem with the system, the status display changes to a warning:





The "Click to view issues" button opens up a page that explains why there is a warning. In this case, it was because no scan had been run in the last 7 days. There is no "Fix All" button provided, so users has to find a solution themselves.

Even with administrator credentials, the user cannot activate or deactivate components from the client interface; this can only be done from the console.

When we attempted to download the EICAR test file, Bitdefender quarantined the file and displayed the following very simple alert:



We found the essentially simple interface of Bitdefender's client software to be very suitable for a business environment, albeit with one exception: as the program warns the user in the event of a problem, we feel that a "Fix All" button would be useful, enabling the user to resolve the problem in a single click.

# Server antivirus software

The antivirus software installed on the server is identical to that for the clients, with the exception that only the Antimalware component is installed (not the Content Control or Firewall).

# Summary

Bitdefender Cloud Security for Endpoints could easily be deployed by a non-expert administrator. The web-based console requires no installation or configuration, and installing the client software individually on each PC is quick and simple. We found the console to be clear and easy to navigate, making it straightforward to find essential information and tasks. The client software is simple and secure but allows users to scan their PCs.

Whilst we experienced a few glitches with the product in our test, we understand that these were caused by a temporary issue with the hosting servers, which has since been resolved.



# **ESET Endpoint Security**

0		Co	nnecte	ed [Server] -	Adminis	strator - ES	ET Rem	ote Ad	ministrato	r Conso	ole				X
File Edit Actions	s View Tools	s Help													
🥰 🔮 🗳 🖬	P 🗣 📫	× × 🔒		👂 🔳 🖣	<b>67</b> □[			- 🚨							
Use All Servers	¥ [	Check Und	check	How do I add s How do I add d	ervers? lients?										
Server Name	Clients		1	Virus Signature	DB State	Least Rece	ent Conn	ection	Last Threat	Alerts		Last Firewa	II Alerts	Last	t Event Wai
Server	4		5	Some Old		1 week ag	0		0			0		0	
<						III									>
Items to show 500	¥ [	<< < >	In the gr 14 (4 it	rid you can see: tems) of all 4 ite	ms	Vie	w mode:	Custom	View Mode	~					
Client Name / 2	Primary Server	Domain	Produc	t Name			Product	Version	Last Con	nected	Prote	ction Status	Text / i	Virus Sigr	nature DB
Server 🔤	Server	avc.local	ESET Fi	le Security Mid	rosoft Win	ndows Server	4.5.1201	1	4 days ag	o				8795 (201	30913)
👺 Seven	Server	avc.local	ESET Er	ndpoint Securi	ty		5.0.2214	1	1 week ag	jo				8773 (201	30907)
🖾 Хр	Server	avc.local	ESET Er	ndpoint Securi	ty		5.0.2214	1	1 week ag	jo				8773 (201	30907)
墜 Eight	Server	avc.local	ESET Er	ndpoint Securi	ty		5.0.2214	4	4 days ag	0	Opera	ating system	is not u	8786 (201	30911)
<	ш														>
📮 Clients 🛛 😝 Tl	hr 📘 🖬 Fire	0 Eve	HIP	Dev	🍔 We	🛇 Anti	() Gre.	. Q s	ca 🛛 🛢 Me	) 📔	Qu	► Tas	h Re	@ Re	
	Client	s Threa Fire	ew Ev	vent HIPS	Devic	Web Ant	is Gre	yli Sca	n Mobil	Quar	Task	s Reports F	lemo Se	rvers 🐚 C	onnected

# Introduction

ESET's business security range includes client antivirus and endpoint protection, mobile security, file and mail server protection, gateway and collaboration security. For our review, we used ESET Endpoint Security client software, and ESET File Security for Windows Server, managed by the Remote Administrator console.

# Software version reviewed

ESET Remote Administrator 5.0 ESET File Security 4.5 ESET Endpoint Security 5.0

# System requirements

ESET Endpoint Security runs on 32 and 64-bit versions of Windows XP, Vista, 7 and 8. ESET File Security runs on 32 and 64-bit versions of Windows Server 2003, 2008, 2008 R2, and 2012, including Small Business Server variants. The ESET Remote Administrator Server and Console run on all of the client and server versions of Windows listed above.

# Downloading the software

The business downloads section of the ESET website presents a clear overview of all the products, making it easy to find the item you want. The individual download page for each product also includes links to all the relevant documentation for the product.

# Documentation

ESET produce two manuals for Remote Administrator, a very comprehensive 122-page User Guide, and a succinct 13-page Quick Start Guide. Both are produced to extremely high professional standards, being well written and organised, but also clearly illustrated, laid out and easily accessible. There are clickable contents pages and extensive bookmarking, making it very easy to get to a particular page or section. Both



documents are well illustrated with screenshots.

We were particularly impressed with the Quick Start Guide, aka Basic Setup Guide. It provides exactly the right amount of information needed to get the console and client software up and running – even starting with purchasing and downloading the software. We especially liked the way the guide integrates its instructions with the screenshots, using a translucent blue overlay to connect the text on the left with the screenshot on the right:



We note that ESET also state the estimated time needed for each particular configuration job, and provide clickable links within the .pdf document to the online knowledge base. We can only describe the Basic Setup Guide as outstanding. As it is only 13 pages long including cover and contents pages, we would recommend that administrators read the whole thing before starting installation and deployment.

# Installing the console

There are two steps to installing ESET Remote Administrator. The Server component provides the actual functionality, while the Console is the management interface. The Console can be installed on a different computer from the Server, or on multiple computers, or even run from a USB portable drive. Installing the Server component involves accepting a licence agreement, importing a licence key (provided by ESET), entering passwords for various functions, and entering the username and password required to download updates (also provided by ESET). Setting up the Console merely requires the location of the installation folder to be decided.

We found the installation process to be very straightforward.

**Client/server antivirus management interface** The layout of the ESET Remote Administrator console is fairly similar to Microsoft's MMC consoles. There is a menu bar and toolbar along the top, with a narrow left-hand pane and larger right-hand pane. Additionally, a row of tabs along the bottom of the window allows a wide variety of views to be shown in the main pane, including Clients, Threats, Quarantine, Tasks, Reports, Remote Install, and various logs. We initially found that it was not easy to obtain on overview, given the array of available tabs, buttons, menus and links. However, with a little practice, essential views and tasks can be found.

We note that the content of all the pages of the console can be customised extensively. The order of the columns can be changed easily by drag and drop, and the columns to be displayed can be added or removed:



We find this very useful, as it allows administrators to display exactly the information they consider most important.



As well as the standard Windows-based console, ESET also provide a web-based console. This does not allow administrative tasks to be carried out, but is very valuable for monitoring, especially as it is highly customisable. The content of each of the boxes shown can be chosen individually; the screenshot below shows a custom dashboard we made:



We feel the design of the web console is very clean, simple and modern, in contrast with the Windows-based console, which seems complicated and rather old-fashioned in comparison. We would suggest that if ESET could build administrative tasks into the web console, and allowed the display of these to be customised too, an unbeatably clear but powerful console might result.

# Deploying the antivirus software

Deployment of the client software involves creating installation packages from the 32 and 64-bit .MSI installers. This can be performed as a separate task, or as part of the first push installation (it only needs to be done once). The administrator then clicks Default Search Task in the Remote Install Pane, selects the client machine(s) to be installed, and selects Windows Push Installation from the Actions menu. Progress can be seen in the Tasks pane.

We would suggest that administrators new to ESET Remote Administrator might need a little assistance in finding their way around the console at first. However, the Basic Setup Guide provides exactly that; we used the guide to assist us with deployment, and found it to be a very straightforward procedure.

As an alternative to push installation, the administrator can create an installation package for local installation, which is then run on individual client PCs.

ESET produce a separate product to protect file servers, ESET File Security. The installation process is however identical to that of the client software, involving the creation of the relevant installation package and distribution by push install or local installation.

# **Client/server antivirus monitoring**

The Clients page of the ESET Remote Administrator console displays a great deal of information about monitored computers. Protection Status Text shows the state of important protection components such as real-time protection and firewall, as displayed in the window of the client software. We find this very good, as it tells the administrator not only that something is wrong, but also the exact nature of the problem. Other items shown in the window are the version of the virus signature database being used by each machine, along with its date; product name and version number of the software installed; and last malware discovery (further details can be seen in the threats pane).

The License Manager in the tools menu shows the licence being currently used, the number of client licences in total and those being used.

Both the Clients view of Remote Administrator console and the client software itself will indicate if important Microsoft updates are available (see main screenshot at the start of the section). There is however no other form of vulnerability scan.



#### **Client/server antivirus tasks**

Right-clicking one or more selected computers in the Clients tab allows a number of different tasks to be started from the New Task submenu. These include full or custom scans, updates, and activating or deactivating specific components such as real-time protection.

Client Name	Salast All	Chill. A		Product Version		
🖉 Eight	Select All	Ctn+A	curity	5.0.2214		
Server 🖉	Select by 'Seven'		Microsoft Windows Server	4.5.12011		
Seven	Inverse Selection	Ctrl+I	curity	5.0.2214		
Хр	Hide Selected	Ctrl+H	curity	5.0.2214		
	Hide Unselected	Ctrl+U				
	New Task	•	Configuration Task			
	Data For This Client	•	On-Demand Scan			
	Clear Info	•	On-Demand Scan (Cl	eaning Disabled)		
Set/Reset Flags Request Data Add to Group Set Policy	Set/Reset Flags	•	Update Now			
	Request Data	•	SysInspector Script Ta	sk		
	Add to Group		Protection Features			
	Set Policy		Run Scheduled Task			
	Remote Install		Restore/Delete From (	Quarantine Task		
	Firewall Rules Merge Wizard		Rollback Virus Databa	se Task		
	Show/Hide Columns		Clear Client's Update	Cache		
	Delete	Del	Generate Security Auc	lit Log		

The administrator can choose to deselect the ESET firewall during deployment and use Windows Firewall instead. Additionally, the Configuration Task dialog contains exactly the same range of options as is available in the client software itself; this includes completely disabling the firewall. The program version can be updated using the Upgrade Windows Client entry in the Remote Install Wizard.

Scheduling scan and signature updates, adding scanning exclusions, and USB control are all performed using the Configuration Editor:

ESET Configuration Editor - [C:\Users\vz\AppData\Local\Temp\RAC49DD.tmp] - Read-only
File Edit Profile Show Help
Reset
Windows desktop v5  Kernel  Settings  Advanced  Presentation mode  Long file  Long file
General Content of the second state state (the second state state (the second state state state (the second state states
Default user interface values
in- Email filter
🕀 🛢 Email client
Document protection
🕀 🖶 Personal firewall
🕀 🛢 Update
R- HIPS

#### **Client antivirus software**

ESET Endpoint Security uses the same interface as ESET's consumer antivirus software, which we regard as a model of simplicity and clarity.

۲	ESET Endpoint Security –						
ESET ENDPOINT SEC	CURITY	<b>~</b> .					
	Protection status						
Protection status	Maximum protection						
Computer scan	Computer V Maximum protection						
Update	Network         ✓ Maximum protection           Web and email         ✓ Maximum protection						
Setup	Frequently used						
🗙 Tools	Run Smart scan Statistics						
Help and support							
	Number of scanned objects: 2142 License valid until: 10/1/2014						
	(65	eT					

There is a very obvious status display in the form of a green text heading plus tick (checkmark) symbol when all is well; in the event of a problem, the text turns red and becomes a warning message, while the symbol changes to an exclamation mark. Update and scan options are easily accessible from the menu bar on the left-hand side. It is not possible to disable protection components such as real-time protection when using a



standard user account (unless administrator credentials are entered at the UAC prompt).

When we tried to download the EICAR test file, ESET blocked the download and displayed this warning message:



We feel this makes reasonably clear to the user that no further action is required.

# Server antivirus software

In terms of the user interface, the file server antivirus software can be regarded as identical to the client endpoint protection, except that the firewall and email protection are not included:



# Summary

We found many aspects of ESET's business product to be outstanding. We regard the client software, web console and documentation, especially the Basic Setup Guide, as exemplary. The Windows-based console is very powerful, and certainly quite useable with a little bit of practice; it seems well suited to larger business networks. However, for a small business, it appears complicated and rather old-fashioned in comparison with its web-based counterpart. We feel that if ESET could integrate management tasks into the web console (which can currently only be used for monitoring), an unbeatably clear and simple small-business package would result.



# **F-Secure Client Security**

Edit View Tools Help							
	X 🛍 📮 🗣		🛃 🛃 🗔				
Policy domains	Summary Settings	St	atus Software up	dates Alerts	Scanning reports	Installation	Operations
📮 Root	Root > Summary						
Computers	Summary						
	Summary						
seven	Policy Manager			Autoo	discover Windows hosts		
Domain Controllers	Policy distribution status:		Distributed				
Be bomain controllers	Virus definitions on the serv	er:	Recent: 2013-0	3-28_04			
			12 hours old				
	Spyware definitions on the s	erver:	2013-08-28_04				
			12 hours old				
	DeepGuard updates on the	server:	2013-08-23_01				
			5 days 12 hours	old			
	Software Updater database	elease date:	27 August 2013				
	New nosts:		0				
	Domain (3 hosts)						
	Hosts having latest policy:		66.6% of domain (2 h	osts) <u>View</u>	hosts' latest policy update	2	
	Disconnected hosts:		0 disconnected				
	New alerts summary:		3 4 security ale	ts <u>View</u>	alerts by severity		
			0 🔕 fatal error				
			0 🕕 errors				
			0 🕓 warnings				
			0 🛞 information	al			
	Virus protection for w	orkstation	s (3 hosts)				
	Real-time scanning enabled		0% of installations	(0 hosts) <u>View</u>	hosts' overall protection		
	Infections found:		0 infected object	s <u>View</u>	hosts' infection status		
	Virus definitions:		100% latest (3 hosts)				

# Introduction

F-Secure provide businesses with two protection models, a hosted security service and a self-managed business software suite. We tested the latter. It consists of a management server and console called Policy Manager, endpoint software called Client Security, and server antivirus software called Server Security.

# Software version reviewed

F-Secure Policy Manager 11.0 F-Secure Server Security 10.0 F-Secure Client Security 11.0

# System requirements

F-Secure Policy Manager runs on Windows Server 2003, 2008, 2008 R2 and 2012. F-Secure Client Security runs on Windows XP, Vista, 7 and 8; with the exception of Windows XP (32-bit only), both 32 and 64-bit versions are supported. Server Security runs on all versions of Windows Server from 2003 to 2012, with the latest version, 10.1, also supporting Windows Server 2012 R2.

# Downloading the software

The Business Downloads section of the F-Secure website provides a clear overview of the components of the Business Suite; clicking on the link for any component opens a details page with the respective system requirements and download links for the software and documentation.

# Documentation

F-Secure provide a comprehensive 157-page guide to the Policy Manager, which covers all aspects of installation, deployment and management. It has been produced to a high standard, is suitably bookmarked, and has a clickable contents page, making it easy to get to a particular section quickly. Unfortunately, it is completely lacking in screenshots.

There is also a 20-page Quick Installation Guide, covering installation of the console and deployment of the client software. This is also very well produced and has the advantage of being well illustrated with appropriate screenshots. We used this to help us with the installation and deployment processes, and found it excellent, with one exception; please see the note in the next section regarding Windows Server Firewall.

# Installing the console

Installation of the console is as quick and easy as installing iTunes. There is a choice of languages, a licence agreement to accept, the choice of installation folder location and ports to be used for the different console modules.

F-Secure.	POLICY MANAGER
onfigure the ports for the Policy Ma	mager Server modules.
osts need access to the Host mod	ule.
olicy Manager Console needs acco achine if you intend to run both at he Web Benotting module is option	ess to the Administration module, restrict its access to the local the same machine (recommended).
lost module	Administration module
Port number:	Port number: 8080 Restrict access to the local machine
Veb Reporting module	
Enable Port number	8081

We note that the standard ports used for the Policy Manager are not opened by default on Windows Server operating systems. Whilst an experienced administrator would realise this and take appropriate action, we note that there is no warning in the setup wizard that these ports will need to be opened manually. We were also unable to find anything about this in either of the relevant manuals.

However, F-Secure tell us that they are aware of this, and are taking steps to amend the manual accordingly.

# **Client/server antivirus management interface**

The F-Secure Policy Manager console uses a two-pane window similar in design to Microsoft's mmc consoles. The narrow lefthand pane displays computers in groups; individual computers or entire groups can be selected, the details of which are then shown in the right-hand pane.

There are a number of tabs along the top of the main right-hand pane. Summary (shown above) displays an overview of the state of the network, with red or yellow icons warning of problems. The Settings tab allows the client software to be configured, while the Status section provides very detailed information on the state of every component of every client. Software updates is a vulnerability monitor which checks for updates in Windows and other third-party software. Alerts shows malware detections, Scanning Reports displays scan logs, Installation allows endpoint protection software to be deployed to client PCs, and finally Operations allows update and scan tasks to be carried out. We found the layout of the console to be essentially clear and easy to navigate.

# Deploying the antivirus software

We found the deployment of the endpoint software to clients by push installation to be a very straightforward process. The wizard uses autodiscover to detect Windows PCs on the network, which can then be selected for installation. Appropriate software packages have to be imported the first time the wizard is used; there is one for clients, and one for both cover 32 and servers. 64-bit architectures. The individual components to be installed can easily be selected:





There is a choice of languages for the UI, and the option of automatically uninstalling any conflicting antivirus software. Finally, options for restarting the client PC after installation can be set. The installation process can be seen on client PCs:



A message box informing the user that the client PC should be restarted appeared at the end of the installation process, as we specified in the deployment wizard. The console also shows that installation is complete.

Alternative installation methods are available. The client security packages can also be installed by policy, or locally on each client PC, using an MSI installation package created in the console.

Server protection installation can be carried out locally with the MSI package, or by push installation from the console. The procedure is identical to clients but uses a different software package.

#### **Client/server antivirus monitoring**

The status of real-time protection can be seen in the Status tab under Overall Protection:

cuon			
Real-time scanning	Internet Shield security level	Incoming e-mail scanning	Outgoing e-n
Disabled	Office	Enabled	Enabled
Disabled	Office	Enabled	Enabled
Disabled	Office	Enabled	Enabled
	Real-time scanning Disabled Disabled Disabled	Real-time scanning         Internet Shield security level           Disabled         Office           Disabled         Office           Disabled         Office	Real-time scanning         Internet Shield security level         Incoming e-mail scanning           Disabled         Office         Enabled           Disabled         Office         Enabled           Disabled         Office         Enabled

The list of components monitored is comprehensive, with Internet Shield (firewall), ingoing and outgoing email protection, Exploit Shield and Software Updater all shown. We also liked the fact that it is possible to re-order or hide the columns, and sort the table by a particular column. In our test, we found that the status of real-time protection displayed in the console was slow to react, taking 10 minutes to react after the change had registered on the client. However, this setting can be changed to as little as 5 seconds.

The Automatic Updates view of the Status tab shows the time of the last signature update and the version installed.

The program version installed can be seen in the Installed Software view of the Status tab. This also indicates which components of the software (e.g. firewall) are installed.

Malware detections and action taken can be seen under the Alerts tab.

We were particularly impressed with F-Secure's Software Update monitor. This displays a complete list of available updates for the operating system and also third-party software.

Category	Software	Update description	CVE ID
Critical security	Adobe Flash 6 Gold	Security updates available for Adobe Flash Player	
Critical security	Windows Media Player 9.0 Gold	Vulnerability in Windows Media Format Runtime Could Allow Remote Co	CVE-2013-3127
Important security	Microsoft Visual C++ 2008 SP1 Redistributab	Vulnerability in Microsoft Foundation Class (MFC) Library Could Allow Re	CVE-2010-3190
Important security	Windows 7 Professional (x64) SP1	Vulnerabilities in Windows Kernel Could Allow Elevation of Privilege (285	CVE-2013-2556
Important security	Windows XP Professional SP3	Vulnerability in Windows Internet Printing Service Could Allow Remote C	CVE-2008-1446
Non-security	.NET Framework 4 Client (x64) Gold	Update for Microsoft .NET Framework: June 2013	
Non-security	.NET Framework 4 Client Gold	Reliability Update 2 for the .NET Framework 4	
Non-security	.NET Framework 4 Client Gold	Update for Microsoft .NET Framework: June 2013	
Non-security	Internet Explorer 8 Gold	Fix for issue: Array elements in very large loops may be returned as undefi	
Non-security	Windows 7 Professional (x64) SP1	Windows Media Player 12 displays scrambled DVD content in Windows 7	
Non-security	Windows 7 Professional (x64) SP1	An update is available that adds support for DTLS in Windows 7 SP1 and	
Non-security	Windows 7 Professional (x64) SP1	An enterprise hotfix rollup is available for Windows 7 SP1 and Windows S.,	
Non-security	Windows 7 Professional (x64) SP1	Update for Microsoft .NET Framework: June 2013	
Non-security	Windows 7 Professional (x64) SP1	Telugu characters are not displayed correctly in the Nirmala UI font in Wi	
Non-security	Windows 8 Professional (x64) Gold	Windows RT, Windows 8, and Windows Server 2012 update rollup: Augus	
Non-security	Windows 8 Professional (x64) Gold	A microcode update is available for Windows 8-based computers that us	
Non-security	Windows XP Professional SP3	Information about new Group Policy preferences in Windows Server 2008	
Non-security	Windows XP Professional SP3	When you disable and then re-enable the LAN-side network adapter on a	

There is a link to the configuration page for the Software Updater, which allows updates to be installed automatically. However, exclusions are possible in the event that the administrator needs to block the installation of a particular patch. Manual updates can also be made.

Licensing information is not displayed in the console; F-Secure inform us that it is not possible with the licence model they use for business products.

# **Client/server antivirus tasks**

Both updates and scans can be started from the extremely simply designed Operations tab. Policy Manager automatically checks for outdated software, so running a vulnerability scan is not necessary. The Software Updater in Settings can be used to automatically install software updates.

Individual components of the software, such as real-time protection or firewall, can easily be disabled from the Settings tab.

Components of the suite can be added or removed by rerunning the installation wizard. USB device control is configured by policy, using the table shown below:

Disalle	ow user changes		
Active	Display Name	HardwarelD	Access Level
Yes	USB Mass Stor	USB\Class_08	Full access
Yes	Wireless devices	USB\Class_E0	Full access
Yes	DVD/CD-ROM	gencdrom	Full access
Yes	Windows CE	{25dbce51-6	Full access
Yes	Floppy drives	{4D36E980-E	Full access
Yes	Modems	{4d36e96d-e	Full access
Yes	COM & LPT p	{4d36e978-e	Full access
Yes	Printers	{4d36e979-e	Full access
Yes	Smart Card Re	{50dd5230	Full access
Yes	Imaging Devic	{6BDD1FC6	Full access
Yes	IEEE 1394 Host	{6bdd1fc1-8	Full access
Yes	IrDA Devices	{6bdd1fc5-8	Full access
	Add	[	Edit

Clicking on an item and then clicking Edit allows the device type to be set to Block. We found this very simple and convenient.

The program version can be updated by creating a new installation package with the updated software, and then pushing it out by policy; this is done by clicking the Installation tab, and then Install under Policy-based installations.

Scanning exclusions for real-time protection and on-demand scans are set by policy:



# **Client antivirus software**

The client endpoint software has a System Tray icon and a fully featured interface, very similar to F-Secure's consumer security products:





The user can run updates and full or custom scans from the smaller buttons along the bottom of the window. There is a status display in the form of a text title and symbol at the top of the window; these change to display a very obvious warning in the event of a problem:



We note that no easy way is provided to correct any problems shown by the status display; there is no Fix-All button or equivalent. We also found that if the real-time protection is disabled from the console, the status display in the client software continues to show "Your computer is protected", even though Windows Action Center is warning that antivirus and antispyware protection is turned off. F-Secure tell us that this is by design, as the product is managed by the administrator and users should not be disturbed by security alerts.

We were pleased to see that the status display does warn of vulnerabilities, with the text "Critical software updates missing" below the main status text.

When we logged on to our test PC with a standard user account, we were able to deactivate the real-time protection of F-Secure Client Security without any form of

challenge. It is possible to prevent user changes in the console, by allowing only administrator accounts to make alterations to the settings; we suggest this would be a better default setting.

When an attempt was made to download the EICAR test file, F-Secure Client Security blocked the download and displayed the following pop-up:



This makes clear that the virus has been removed, so the user should not have to worry about taking any action. Clicking on the text shows more information:

Veb traffic scanning detected EICAR_Test_File. The content of the item view automatically.	ALDC
	103
What causes this?	
This can happen, for example, if you browse to a web site that tries to int your computer through a known vulnerability.	trude
What should I do?	
You do not have to do anything. If you were downloading a file, try from another location.	

The Details button additionally displays the name of the item, malware type, and web address from which it originated. We can only describe F-Secure's warnings on malware discovery as exemplary, starting with a very simple but clear message box, but allowing users to see more information if necessary.

# Server antivirus software

The server protection has a familiar F-Secure System Tray icon. This can be right-clicked to display a context menu of scanning options. There is no program window, however; other tasks are carried out by means of a web console. Whilst this provides the same functionality as a more standard Windowsbased interface, we did not find it very easy to use and suggest that it is more suited to IT professionals than non-expert administrators. F-Secure tell us that it was developed for use with the Windows Server Core configuration, which does not have a graphical user interface.

# Summary

F-Secure's business suite is in many ways very well designed. Installation and deployment are very straightforward, as long as the need to open firewall ports is understood. The console and client software are essentially well designed and easy to use. Monitoring of protection features in the clients is very detailed, and malware alerts on client PCs are excellent. The Software Update monitor is outstanding. We do however have some reservations about the default settings. We would suggest that a faster polling interval would provide a more accurate status display, and that user access to protection settings should be blocked as standard. We conclude that the software is essentially well designed, but could be made more suitable for nonexpert users if configured by an IT professional first. F-Secure tell us that they provide free training for partners and customers to assist with setting up and using the product.





# G Data AntiVirus Business with Patch Management

# Introduction

G Data make a variety of security software products for businesses of all sizes. We tested Antivirus Business, a straightforward antivirus solution for small businesses, managed by the G Data Administrator Console. The package we used also included the Patch Management feature, which is available as an add-on for any G Data business solution.

# Software version reviewed

G Data Administrator 12.0 G Data Security Client 12.0

# System requirements

G Data Antivirus Business is supported on clients with Windows XP (32-bit only), Windows Vista, 7 and 8, and servers with Windows Server 2003, 2008, 2008 R2, and 2012. We note that under some circumstances, a glitch related to SQL Server may occur if the console is installed on a Windows Server 2012 domain controller. This prevents the user from logging on to the management console, but is quickly and easily fixed by G Data Support.

# Downloading the software

The software and manual are downloaded by means of a link in an email sent by G Data.

# Documentation

G Data make one manual covering the installation, configuration and management of the entire suite, i.e. console and client software. It is comprehensive, at 181 pages, and produced to a very high standard. The contents page is very simple, listing only major sections of the document, but it is clickable. The manual has been extensively bookmarked, so it is easy to get to a specific page or section from Adobe Reader's Bookmarks Bar. There are appropriate screenshots to illustrate major features and tasks. We feel the manual is well written and sensibly organised.



We found the installation of G Data Administrator a very quick and easy process. Running the setup wizard involves accepting the licence agreement, choosing an installation folder, stating whether the machine being installed is a primary or secondary server, and installing SQL Server Express. The latter step is recommended for up to 1000 clients, and is carried out automatically by the wizard.

**Client/server antivirus management interface** 

The layout of the management console is similar to Microsoft's MMC consoles. A narrow left-hand pane shows the management server and its associated client/server machines. Clicking on an individual computer in this pane can display information about it in the right-hand pane, whilst clicking on the server at the top of the tree will display details of the whole network.

By default, the right-hand pane shows the Dashboard. This includes a summary of security details (real-time protection, update status, installation status of client software). Other panels show malware infections and client connections in the form of pie charts, while a fourth quadrant shows report status. We feel this provides a very clear overview of the most important security information.

Tabs along the top of the right-hand pane allow the view to be changed to show items such as detailed information about clients, configuration settings for the software, software updates available for Microsoft and other third-party vendors, and malware detections.

# Deploying the antivirus software

When the administrator logs in to the console for the first time, a deployment wizard starts automatically. This is remarkably simple, and merely involves selecting the machines to be installed from a list of computers found on the network:



We note that client PCs and servers can be installed together, there is one installation package used for both. After a few simple configuration steps, the wizard proceeds, and after just a couple of minutes, the status display informs the administrator that installation was successful:

<u>1</u>	Install G Data Security Client
SERVER: Installing G Data Security Client EIGHT: Installing G Data Security Client SEVEN: Installing G Data Security Client XP: Installing G Data Security Client EIGHT: Installation completed successfully. SEVER: Installation completed successfully.	

We found G Data's deployment process to be exceptionally quick and easy.

The G Data Security Client can also be installed locally on individual PCs, or by creating an installation package that is distributed by logon script.

# **Client/server antivirus monitoring**

The status of updates and real-time protection can be seen in the Security Status box of the Dashboard (home) page of the console. We note that if a PC's real-time protection is disabled from the console, or permanently disabled on from client, the Dashboard will immediately show that it is not running on the relevant machine. However, if it is "temporarily" disabled (up to 8 hours) from the System Tray icon of the client, this is not shown in the console, which continues to report that all is well. We are concerned that if malware were able to mimic this particular action, the administrator would not be made aware of it. Administrators may be best advised to leave RTP locked down on the client and only change it in the console.



The program version installed is shown in the Clients view.

Malware discoveries are individually listed in the Reports view, and an overview of infected machines is displayed on the Dashboard.

Available software updates, i.e. patches for vulnerabilities, are shown in detail in the Patch Manager view. This can be sorted according to patch, client, vendor or product:

Drag the column header to this area to group by this column.			
Patch	V Client V	Vendor	Y Pro
MS13-004 Security Update for Microsoft .NET Framework 3.5.1 on Windows 7 and Windows Server 2008 R2 x64 (K82742598)	EIGHT	Microsoft Corp.	Win
MS13-004 Security Update for Microsoft .NET Framework 3.5.1 on Win7 and 2008 R2 SP1 x64 (K82756921)	EIGHT	Microsoft Corp.	Wie
MS13-004 Security Update for Microsoft .NET Framework 4 on XP, 2003, Vista, Win7, 2008, 2008 R2 x64 (K82742595)	EIGHT	Microsoft Corp.	Win
MS13-005 Security Update for Windows 7 x64 (K82778930)	EIGHT	Microsoft Corp.	Win
MS13-006 Security Update for Windows 7 x64 (K82785220)	EIGHT	Microsoft Corp.	Win
MS13-007 Security Update for Microsoft .NET Framework 3.5.1 on Windows 7 and Windows Server 2008 R2 x64 (KB2736418)	EIGHT	Microsoft Corp.	Win
MS13-007 Security Update for Microsoft .NET Framework 3.5.1 on Win7 and 2008 R2 SP1 x64 (K82736422)	EIGHT	Microsoft Corp.	Win
MS13-008 Security Update for Internet Explorer 8 for Windows 7 x64 (KB2799329)	EIGHT	Microsoft Corp.	Win
MS13-007 Security Update for Microsoft .NET Framework 4 on XP, 2003, Vista, Win7, 2008, 2008 R2 x64 (K82736428)	EIGHT	Microsoft Corp.	Win
MS13-009 Cumulative Security Update for Internet Explorer 8 for Windows 7 x64 (KB2792100)	EIGHT	Microsoft Corp.	Win
MS13-009 Cumulative Security Update for Internet Explorer 9 for Windows 7 x64 (K82792100)	EIGHT	Microsoft Corp.	Win
MS13-010 Security Update for Internet Explorer 8 for Windows 7 x64 (KB2797052)	EIGHT	Microsoft Corp.	Win
MS13-015 Security Update for Microsoft .NET Framework 3.5.1 on Windows 7 and Windows Server 2008 R2 x64 (K82789644)	EIGHT	Microsoft Corp.	Win
MS13-010 Security Update for Internet Explorer 9 for Windows 7 x64 (KB2797052)	EIGHT	Microsoft Corp.	Win
MS13-015 Security Update for Microsoft .NET Framework 4 on XP, 2003, Vista, Win7, 2008, 2008 R2 x64 (K82789642)	EIGHT	Microsoft Corp.	Win
MS13-015 Security Update for Microsoft .NET Framework 4.5 on Windows 7, Vista, Win 2008, Win 2008 R2 for x64 (KB2789648)	EIGHT	Microsoft Corp.	Win
MS13-017 Security Update for Windows 7 x64 (K82799494)	EIGHT	Microsoft Corp.	Win
MS13-016 Security Update for Windows 7 x64 (K82778344)	EIGHT	Microsoft Corp.	Win

The available patches can be selected and installed, individually or en masse, from the Patch Manager. We found this to be a very simple but effective means of keeping software up to date.

Although there is a separate menu in the program window for licence management, we could not find a means of showing when our licence expired, only how many valid licences we had.

# **Client/server antivirus tasks**

Scans, both one-off and scheduled, can be set in the Tasks tab.

A vulnerability scan is not required as the Patch Manager constantly monitors software for available patches.

Updating both signatures and the software itself can be carried out from the Clients tab, by selecting the relevant computer(s) and right-clicking. This method can also be used to install or uninstall software. Real-time protection can be enabled/disabled from the Monitor section of the Client Settings tab, as can real-time exclusions.

Scan exclusions can be set in the General section.

USB device control is not available in the software version that we tested.

# **Client antivirus software**

By default, the G Data Security Client has a very minimalist interface. There is a System Tray icon, right-clicking which produces the following context menu:



Clicking Internet Update allows the user to update the signatures, and to choose between getting updates from the management server or G Data's Internet servers – for the benefit of mobile users. Other than displaying version information, no other functions are available to the user.

The administrator can optionally hide the G Data icon completely, or allow the users access to additional features:

Client functions	
The user can run virus checks	
The user can download virus signature up	dates
The user can change email and monitor o	ptions
Display local quarantine	
Protect options with a password	Change password

With all options enabled, the context menu is extended:





If the user is allowed to change email and monitor options, the real-time protection can be disabled; however, this can be password protected, so that only users authorised by the administrator are able to do this.

We note that when real-time protection is switched off, there is only a muted warning from Windows Action Center, i.e. the System Tray icon does not change, and there is no notification shown. Only if the Action Center window is opened is it obvious that virus protection is turned off. However, the G Data system tray does display a warning symbol:



When we attempted to download the EICAR test file, the download was blocked, and the following alert shown in the browser window:



We feel this makes reasonably clear that no further action is necessary.

#### Server antivirus software

The antivirus software for the server can be considered identical to that for the client.

#### **Summary**

G Data AntiVirus Business with Patch Management impressed us in many ways. Deployment is extremely simple, and the clearly designed console does a very good job of making important information and tasks easy to find. The option of a minimalist user interface for the client software may well appeal to many administrators. Documentation is very good.

#### 💠 IKARUS security.manager \_ 8 × File View Tools Help Management 0 Overview Page General Properties Charts ▼ A X ₹× °℃ 💭 🕶 🖓 🕶 Srvtwo.avc.local . Ŧ System Overview 😝 Infected 🔒 Warning This section aggregates general information about the server and statistical data about the hosts it administrates. All ISM Version: 4.2.27 Srvtwo.avc.local on Windows Server 2008 R2 x64 Service Pack 1 (Build 7601) Server: 🗉 🗐 localhost 5 Number of hosts: 🖃 🕼 avc.loca Administrated: 0 E D Computers Infected: 0 EIGHT.avc.local A Warning: 0 SEVEN.avc.local Total Number of Viruses: 0 SRVTWO.avc.local TR.avc.local License Information 🖃 📁 Domain Controllers Your license is valid until 11/29/2013 23:59. SERVER.avc.local You are administrating 0 host(s). With this license you are allowed to administrate up to 5 host(s) MANUAL Pending Active Waiting Processed 🔹 🝯 🥩 Update Interval 30s State ID Timestamp Information Next Scheduled Time: Pending Tasks Virus List Log File Change Log

# **IKARUS** security.manager

# Introduction

IKARUS produce endpoint protection and gateway protection products plus mail and web cloud-security services. For our review, we tested IKARUS anti.virus endpoint protection software, managed by the IKARUS security.manager console.

# Software version reviewed

IKARUS security.manager 4.2 IKARUS anti.virus 2.2

# System requirements

Both the console and the endpoint protection software can be installed on 32 and 64-bit versions of Windows XP, Vista, Windows 7, plus Windows Server 2003, 2008, and 2008 R2. The antivirus software can also be installed on 32 or 64-bit Windows 8. At the time of testing, the IKARUS website did not show Windows Server 2012 as being supported, so we installed security.manager under Windows Server 2008 R2.

# Downloading the software

Both components of the console (server/client software and user interface) and the accompanying manual can be downloaded from the relevant page of the download section of the IKARUS website.



# Documentation

IKARUS produce two manuals relevant to this test, one for the console, and one for the client antivirus software. Both are comprehensive, covering all relevant areas of their respective products. The instructions are essentially clear, although both documents show signs of having been imperfectly translated from German; the contents page of the console manual is still entitled "Inhalt", for example. Both manuals are well illustrated with screenshots. Sadly, neither is bookmarked, although the console guide does have a clickable contents page.

We used the security.manager manual to assist with installing the console and deploying the software.

# Installing the console

The console is installed in two parts, the server software and the user interface. The user interface can be installed on other computers, as well as or instead of the server. Installing the server software requires selecting a language, accepting a licence agreement, manually creating a shared folder, and choosing an SQL installation. If none is available, the setup wizard can install SQL Express 2005 or 2008 automatically. We chose the 2008 variant, which was installed for us without any problems.

The user interface also requires an additional component, in this case the .NET Framework 4; this was also installed automatically by the wizard. We found installing the console to be a very straightforward process.

# **Client/server antivirus management interface**

The security.manager console has a narrow left-hand column showing the computers on the network; this has tabs to show only infected PCs, or those with a warning. There are also two horizontal right-hand panes. The larger of these shows the details of either the group or individual computer (depending on the view). Tabs at the top allow the view to

be changed to General (a table of important system information for all PCs), Properties (a small selection of configuration items), and Charts (availability, administration and infection of clients, shown as pie charts). We found the General tab to be the most useful, and wonder why this is not the default when the console opens:

calho	ist								
umbe	r of hosts:	5							
otal N	lumber of Viruses:	0							
umbe	r of hosts online:	3							
umbe	r of Hosts Guarded:	1							
dmini	strated:	1							
dmink	strated:	1							
dminit fosts:	strated:	1							
footo:	strated: Name	1 Infections	Online	Service Installed	Administrated	Last Update	Last Time Online	[	
foots:	Name SERVER.avc.local	1 Infections 0	Online	Service Installed	Administrated	Last Update N/A	Last Time Online		 
footo:	Name SERVER.avc.local XP.avc.local	1 Infections 0 0	Online	Service Installed	Administrated	Last Update N/A N/A	Last Time Online N/A N/A	[	
fosts:	Name SERVER.avc.local XP.avc.local SRVTWO.avc.local	1 Infections 0 0 0 0	Online	Service Installed	Administrated	Last Update N/A N/A 9/2/2013 14:38	Last Time Online N/A N/A 9/2/2013 15:00		
dminit fosts: Still Still Control Still St	Name SERVER.avc.local XP.avc.local SRVTWO.avc.local SEVEN.avc.local	1 0 0 0 0 0	Online • •	Service Installed	Administrated	Last Update N/A N/A 9/2/2013 14:38 N/A	Last Time Online N/A N/A 9/2/2013 15:00 N/A		

We note that in most views, the main righthand pane uses the grey colour of the window frame. Whilst the writing on this is definitely legible, we would not describe it as eyecatching. The charts view, on the other hand, uses coloured pie charts on a white background, which we found much more striking.

The lower right-hand pane shows Pending Tasks by default, but can also display Virus List, Log File or Change Log.

# Deploying the antivirus software

Deployment of the antivirus software to clients by push installation could scarcely be simpler. The administrator right clicks on a computer or group, and clicks "Install IKARUS anti.virus". This applies to server computers as well as clients.

We could not find any alternative method of installing the endpoint software.

# **Client/server antivirus monitoring**

Whilst the status of real-time protection can be seen for individual computers, by selecting a computer in the left-hand pane and clicking the General tab, there is no means of displaying it for all computers or even a group. An administrator would thus have to click through all computers on the network



one by one to see if real-time protection was enabled. We feel that including RTP in the items displayed for groups/all computers would be a significant improvement.

We also found that the console reacted very slowly to changes in component activation or deactivation, failing to update for over 15 minutes in our test. Closing and re-opening the console immediately updated the display correctly, however. Client status can also be updated manually via the context menu. The date and time of the last update can be seen for groups/all computers under the General tab.

Detailed program information can be seen for each individual computer on the General tab. If malware is discovered on a client, this is shown very clearly in the console. The icon for the computer itself, as well as any groups of which it is a member, turns red with an exclamation mark:



By right-clicking an infected computer and then selecting "Start IKARUS anti.virus", the administrator can open an exact replica of the program window, exactly as it would appear on the client computer. The title bar indicates the name of the computer whose data is being shown:

File	Edit	Tools	Support	Help	
sc	AN			QUARANTINE	
scan				1 virus in quarantine	

The administrator can then see what has happened with the malware (in this case it can be seen to have been quarantined), and delete or restore files from quarantine, just as if working on the local machine.

Licensing information can be seen on the Overview Page of the console. This shows expiration date of the licence, number of licences purchased, and number being used, which we found helpful.

# **Client/server antivirus tasks**

The IKARUS security.manager window features a toolbar below the menu bar, which has one single icon, the Configurations button:

💠 IKARUS sec	urity.ma	nager
File View Too	ls Help	Management
Directory		
° <u>12</u> ° <u>12</u> 🛁 👻	₽ <b>-</b> s	rvtwo.avc.local 👻

Clicking on this opens the configuration dialog box, which can be used to enable or disable individual protection components, run scheduled scans, set exclusions, and change other settings.

Below the Configurations button is a group of four icons, the rightmost of which can be used to run one-off scans on individual machines (but not on groups of machines). We did not find the other icons in the group very clear, and would suggest that IKARUS could move them to the otherwise virtually empty toolbar and provide them with clear labels.

An individual computer or group of computers can be updated by right-clicking it and selecting "Update IKARUS anti.virus". Update scheduling can be changed on the Properties page. We could not find any means of updating the program version, controlling USB devices, or scanning for vulnerabilities.



#### **Client antivirus software**

IKARUS anti.virus has a fully featured interface similar to that of a consumer antivirus product. By default, the window opens on the Guard page, which provides a program status display.



Enabling or disabling individual protection features is extremely simple, as these are listed on the page with check boxes. A symbol and text line at the bottom indicate the overall status; "Your system is safely configured" in green with a tick (checkmark) are shown if all is well, but this changes to "Attention! Your system is not safe [sic] configured!" in red with an exclamation mark if the protection components are switched off. A "Fix-All" button is not necessary, given the component display/control on the same page.

In our test, we were able to deactivate the program's real-time protection using a nonadministrator account, without having to enter any additional credentials. However, access can be restricted to specific users/groups, and the administrator can also password protect the client settings.

When we attempted to download the EICAR test file, IKARUS quarantined the file and displayed the following alert:

<b>SCAN</b> Virus	UPDATE GUA 0 minutes ago Act	ARC
----------------------	---------------------------------	-----

We feel this makes very clear to the user that malware has been found, but does not indicate what, if anything, needs to be done. If no action is taken, the alert will reappear every few minutes. If the user clicks on SCAN, the program will open on the guarantine page; this recommends that the file should be deleted, and this is easy to do. However, if the user clicks on UPDATE or GUARD, the program opens at the relevant pages, providing no option to deal with the malware found. We feel that many users could be alarmed or confused by this, and may contact technical support; this is not necessary, given that the threat has already been successfully quarantined.

#### Server antivirus software

The server antivirus can be regarded as identical to that for the client.

#### Summary

We would describe IKARUS's business software as essentially straightforward and simple to use, but with room for improvement in some areas. The documentation is essentially good but would benefit from bookmarks and tidying up of the English translation. Installation of the console is unproblematic and deployment of the client software particularly quick and easy. We found the management console to be largely simple and effective in its layout, although it could be clarified and tidied up in some areas. Monitoring of real-time protection can only be viewed per machine, and is slow to react.

The main window of the client software is clear and easy to use, and we especially like the ability to reproduce the window of any client on the server, making monitoring and administration of individual PCs very simple. However, we are concerned that malware alerts may cause alarm and confusion with users, and suggest that IKARUS could improve this.

# Kaspersky Endpoint Security for Business Advanced



# Introduction

The Kaspersky Endpoint Security for Business range comprises three different packages: Core, Select and Advanced. We tested the Advanced package for our review, which includes endpoint protection for clients and file servers and vulnerability scanning/patch management. The suite also contains mobile device security and management features, and asset management, patch and vulnerability management, disk/file encryption, OS deployment, and network admission control features.

# Software version reviewed

Kaspersky Security Center 10.0 Kaspersky Endpoint Security for Windows 10.1

# System requirements

Both the console and the endpoint protection software can be installed on Windows XP, Vista, 7 and 8, plus Windows Server 2003, 2008, 2008 R2 and 2012, including Small Business Server variants. 32 and 64-bit architectures are supported, with one exception: only the 32-bit version of Windows XP is supported for the endpoint software.

Please note that 100 GB free disk space is needed for the patch management feature.

# Downloading the software

We found some confusion on the downloads page of Kaspersky Endpoint Security. There is a separate link for Kaspersky Anti-Virus for Windows Server, but it leads to exactly the same page/download as the link for Kaspersky Endpoint Security for Windows. We feel this could cause confusion and waste time. There are also two versions of the Security Center software available, Full and Lite, but no word of explanation as to what the difference is (the latter includes the client software). Again, we feel this could cause frustration, and suggest that a little more explanation of what is what would make it easier to



download the right software. Kaspersky Lab inform us that steps are being taken to rectify this.

### Documentation

There are no less than four manuals for Kaspersky Security Center. Unfortunately, we did not find the names very helpful in discerning the content of each one, and as noted last year, there are no details given on the website:

Kaspersky Security Center			
Kaspersky Security Center 10			
Administrator Guide For Version 10	English	¥	Download
Getting Started For Version 10	English	V	Download
Implementation Guide For Version 10	English	~	Download
User Guide For Version 10	English	¥	Download

We consequently still feel it is rather difficult to find the right manual for the job. The Implementation Guide is in fact the most useful document to help with installation and deployment. It is comprehensive at 92 pages, clear, well bookmarked and has a clickable contents page, making navigation easy. As with last year's version, there are no screenshots at all, which we feel is a shame.

# Installing the console

The setup wizard involves accepting a licence agreement, choosing typical or custom installation (we chose typical), and specifying the number of computers to be protected, in groups ranging from less than 100 to over 5,000. A progress display shows the required components, which of these are already there, which have to be installed; in our case, we needed SQL Server 2008 R2 Express SP2 and MSXML 4.0, but these were installed automatically by the wizard.

Kaspersky Security Center Administration Serv	er 🗕 🗆
stalling Kaspersky Security Center Administration S	erver
Please wait for the Kaspersky Security Center Administration Se complete.	rver installation to
Application name	Applicatio
PMCrosoft INET Framework 2:0 SP2 MCrosoft Windows Installer 4.5 MCrosoft SQL Server 2008 R2 Express SP2 MSXML 4.0 Kaspersky Security Center Administration Server	Prerequisite Prerequisite Prerequisite Prerequisite Main
< Back Next >	Cancel

After completion, the Quick Start Wizard runs. This requires the administrator to enter the licence key to activate the products, and allows some settings such as proxy server to be changed. Finally, the option is provided of starting the deployment wizard.

**Client/server antivirus management interface** Kaspersky Lab's administration console uses the familiar Microsoft Management Console (MMC) framework. This consists of a narrow left-hand pane with various options, and a much wider right-hand pane to display the chosen option. It opens with the main page of the Administration Server selected. This is divided into 6 sections: Deployment, Computer Management, Protection and Virus Scan, Update, Monitoring, and Administration Server. All but the last of these have their own status displays, in the form of a "traffic light" button, showing green, amber or red for problem/warning/safe states respectively. Each section has links to relevant tasks, e.q. the Deployment section has a link entitled "Install Kaspersky Anti-Virus". This page provides a simple, at-a-glance overview of the state of the network, with easy access to any important tasks that need doing.

The left-hand pane of the window, consistent with Windows, contains a folder tree with more detailed options. These include Managed Computers (displays status and allows everyday management), Reports and Notifications (protection, deployment and



update status as pie charts), Applications and Vulnerabilities (application control and update monitoring), Remote Installation, and Repositories (management of installation packages, updates and licences).

Kaspersky Security Center makes a wide variety of views and tasks available, but we feel the use of the familiar MMC console and good graphical design nonetheless make it very straightforward to find one's way around.

#### Deploying the antivirus software

Deployment to clients by push installation uses the Remote Installation Wizard. If the full Kaspersky Security Center has been downloaded, the client endpoint software is already integrated, so the administrator only has to select the computers for deployment:

Selecting computers for installation	
Manages computers     Manages computers     Manages computers     Manages computers     Seven     Seven     Seven     Seven     XP	Add If target computers are not displayed in the list, dick Add to type their names or IP addresses.

The wizard asks whether client PCs should be restarted automatically, not at all, or after a warning to users. Installation then proceeds, and a very clear pie chart shows the progress in real time:



Kaspersky Endpoint Security software can be installed on the server in the same way and at the same time as on the clients. It is automatically configured slightly differently from the clients, but deployment is identical. We found the remote push installation to be very quick and simple.

**Client/server antivirus monitoring** 

<b>N</b>			Kas	persky	Security Center					- 1-1	• ×
Elle Action Yew Help	51										
Kapenky Security Center Administration Server SIRVER Mininged computers Administration Server tables User accounts Computer and netficiations Computer insultations Computer ins	Groups Client comp Add computers Configure param Configure par	Policies Duters meters of computerns	Tasks ar status	discove	Compute	rs		Gen Comp Vi Vi O	tting started > star statues sist 2 ming 0 to 2	tanaged co	emputers
> 👸 Repositories	0					Statu		Computer name:			۹ 🖬
	Name BOHT SERVER	OS type Microsoft Win Microsoft Win Microsoft Win	AVC AVC AVC	Agen +/- +/- +/+	Visible 3 minutes ago 2 minutes ago 3 minutes ago	Last update 14 hours ago 15 hours ago 12 hours ago	Status Critica Critica OK/Vit	Critical	Visible ersky Anti-Virus i	s not installe	ed .
		Microsoft win	AVC	•/•	a minutes ago	14 hours ago	OIUVE	Domain name: IP addresse Protection status: Last update: Viruses found: Last visible time: Consection to Serv Operating system: Network Agent ver Anth-virus version: Encryption status:	eigl 273 141 141 111 111 No skore 20.	Lavc.local 25.1.304 sown ours ago nute ago osoft Windows 3.3361	5 8
<								Actions Install applica Reset Virus Co Create a task Perform task View virus act Display messo	tion suster Mty spe to the user		
Groups 0, computers 4	- 10 -		2	9						. 21	08:33

The overall status of real-time protection can be seen on the Statistics tab of Reports and Notifications as a pie chart. We note that a warning is only shown in the event that all the protection components are deactivated. The status of individual PCs is shown in the Computers tab of Managed Computers, with a traffic-light colour scheme:

							Getting started > Managed	computers
Clier + Add	nt computers figure paramete	ters	mputer status de	covery			Computer statusesi Oricali 1 Warning: 1 Oric 2	
O Add o O Refre	or remove columns esh				<u> </u>	Chahar 🔳 🔳	Computer name:	
Add o Refre	or remove columns esh	Dom	Anant/Anti-view	Virible	Last undate	Status: 🗮 💻	Computer name:	
Add o Refre	OS type Microsoft Win	Dom	Agent/Anti-virus	Visible 1 minute app	Last update 8 minutes app	Status: 📕 💻 Status ^ OK/Visible	Computer name: Status description Last connection to Administration Server 1	Info updat
Add o Refre	OS type Microsoft Win	Dom AVC AVC	Agent/Anti-virus + / + + / +	Visible 1 minute ago 8 minutes ago	Last update 8 minutes ago 20 hours ago	Status: 📕 💻 Status * OK/Visible OK/Visible	Computer name: Status description Last connection to Administration Server 1 Last connection to Administration Server 3	Info updat 1 minute a 14 minute
Add o Refre	OS type Microsoft Win Microsoft Win Microsoft Win	Dom AVC AVC AVC	Agent/Anti-virus + / + + / + + / -	Visible 1 minute ago 8 minutes ago 3 minutes ago	Last update 8 minutes ago 20 hours ago 20 hours ago	Status:	Conputer name: Status description Last connection to Administration Server 1 Last connection to Administration Server 3	Info updat 1 minute a 14 minute 3 minutes

The time of last update, database signature version, program version and number of malware detections can also be seen on the Computers tab of Managed Computers.

We could not find a means of monitoring the status of Kaspersky Lab's firewall on the client.

Outdated software is displayed in Application Vulnerabilities, a sub-item of Applications and Vulnerabilities.

Licensing information can be found in Repositories/Keys.



# **Client/server antivirus tasks**

Malware scans, vulnerability scans and updates can be run by right-clicking a computer or group and selecting All Tasks/Create a Task from the context menu. The program version can be updated by rerunning the deployment wizard.

Components such as real-time protection or firewall can be enabled or disabled by policy, under Managed Computers/Policies.

It is not possible to uninstall individual components such as the firewall. Kaspersky Lab informs us that this is due to the close integration of the protection components with each other.

We could not find out how to set scanning exclusions or control USB devices from the console, despite searching the Implementation Guide and Knowledge Base. We suggest that Kaspersky Lab should provide better documentation on how to access and configure these features.

# **Client antivirus software**

Kaspersky Endpoint Security's program interface is quite different from that of any of the other programs in this review. It provides the administrator with detailed information about the status of individual components and settings, but by default does not allow any actions to be carried out or the configuration to be changed.

Endpoint Security 10 for Windows	, dl Reports 🚱 Qua	rantin
Protection and Control	Settings AVC\Administra, you are working under a po	licy 🖥
Endpoint control disabled		0
Protection: there are activ	e threats	0
<ul> <li>File Anti-Virus</li> <li>Mail Anti-Virus</li> </ul>	A special disinfection procedure, which requires a computer restart, is necessary Disabled	
\Theta Web Anti-Virus	Disabled	
🧿 IM Anti-Virus	Disabled	
Firewall	incoming connections: 0, outgoing connections: 0	
Network Attack Blocker	Disabled	
😑 System Watcher	Disabled	
Tasks - 3 out of 3 tasks a	re scheduled	0
Next task: Full Scan starts 16/09	0/2013 at 19:00	

From the point of view of standard users, we would regard the interface as "minimalist", in the sense that they are not supposed to interact with it. Administrators could however enable some functionality, such as carrying out updates and scans, from the console.

By default, it is not possible to disable realtime protection from the program window, regardless of the type of Windows account being used.

By default, detected malware is blocked silently, but this can be configured by the administrator.

# Server antivirus software

The same software as for the clients is installed on the server, although it is configured differently by the setup wizard. For example, the Endpoint Control feature is not installed, and so this section is not displayed in the main program window. Otherwise, the interface of the server software is identical to that of the client.

# Summary

Kaspersky Lab's console is very powerful, but the use of the familiar mmc format means that administrators will easily find their way around the interface. The graphic design and use of e.g. pie charts to show deployment progress add to the user-friendliness. By default, the client software is minimalist from the point of view of the user, but provides the administrator with useful status information. Documentation is also good, once the right manual has been found. Our once concern is that it is very difficult to find exclusion and USB-device control settings.





# Sophos Endpoint Security and Control

# Introduction

Sophos specialise in security software for business and provide a wide range of products and services. For our review, we tested the Endpoint Security and Control client software, managed by the Sophos Enterprise Console.

# Software version reviewed

Sophos Endpoint Security and Control 10.2 Sophos Enterprise Console 5.2

# System requirements

Sophos Endpoint Security and Control is supported for Windows XP, Vista, 7 and 8, in 32 and 64-bit architectures; also for Windows Server 2003, 2008, 2008 R2, 2012, and Small Business Server versions of these, in 32 and 64-bit architectures where applicable. To simplify the installation of SQL Server, we tested the suite on Windows Server 2008 R2 64-bit.

# Downloading the software

Sophos provided us with a direct link to download the software. Documentation can easily be found in the Support section of the Sophos website.

# Documentation

installation То assist with the and deployment, we used the Sophos Enterprise Console Quick Startup Guide. This is relatively brief at 29 pages, though in some areas there are links to pages of the Sophos online knowledge base, which provide additional information. If the external knowledge base pages are included, the manual provides everything the administrator needs to know to install the console and deploy the client software. It is clearly laid out and well written, although there are unfortunately no screenshots at all. There is a clickable contents page and the document has been



well bookmarked, so it is easy to get to a particular page or section.

Other documentation is available, including a 57-page advanced startup guide, and a 123-page Help guide.

# Installing the console

The first step of installation is unpacking the setup software. This involves agreeing a licence agreement and selecting which components to install (the interface can be installed on additional computers for ease of access). The wizard provides a list of requirements and shows which of these have been fulfilled, which we found very helpful:



The actual installation process which then follows is straightforward; it requires the administrator to have created Sophos-specific user accounts in advance, but this is explained in the manual. An SQL Server installation is also required; the 2008 Express version can be installed automatically if desired, and we chose this option.

# **Client/server antivirus management interface**

The main pane of the console window shows either all managed computers or those in a specific group – this can be selected in the upper right-hand pane. Tabs along the top of the main pane allow different information to be shown in different views, including Status (= protection, the default view), Computer Details (OS, Service Pack, IP address, current user etc.), Update Details, Anti-virus Details, and status of various other protection components. A very wide variety of information can thus be seen simply by clicking through the tabs at the top.

The lower pane on the left-hand side shows the various configuration policies; rightclicking any of these allows the policy to be edited. The console also has a menu bar and toolbar.

Given that a considerable amount of information can be displayed, we found the layout of the Sophos Enterprise Console to be very straightforward.

# Deploying the antivirus software

The "Download Security Software Wizard" launches when the console is opened, and takes the administrator through the installation process. It asks for the client types to be protected – we note that older versions of Windows are still supported:

Select the platforms you will be p	protecting on your network.	Lat
Platforms:		
Windows NT		
Windows 9x		
Windows 2000 and above		
MAC OS X 10.4+		
Solaris 9/10 (SPARC)		
Solaris 9/10 (INTEL)		
Linux		
HP-UX (IA64) 11.23+		
AIX (PowerPC) 5.3+		
To make the initial download as quid need software now. You can chang	k as possible, select only the platforms e these settings later.	for which you

Next, computer groups have to be created; these can be imported from Active Directory, which we found very convenient. The administrator then right-clicks a group, and selects Protect Computers from the context menu. Servers can be installed along with clients, there is no need to run the process again. We found the deployment process to be very simple and unproblematic. The client software can also be installed manually on individual computers.



### **Client/server antivirus monitoring**

Amongst other things, the Status tab of the console shows whether signatures are up to date, if real-time protection is enabled, and the state of the Sophos firewall (if installed). We noticed that the status display responds very quickly (just a few seconds) when e.g. a computer is shut down or a protection components switched off.

The program version and virus signature database details can be seen under the Antivirus details. Malware detections are shown on both the Status tab and Alert and Error Details tab.

Double-clicking a computer from any view tab will open up a detailed report on that machine. We were impressed to see that in the event of an error (e.g. update failure), the report contains a hyperlink to a page on the Sophos website with potential causes of and solutions to the problem. In the case of a malware discovery, there is a similar link to the Sophos website, which will provide details of the malware concerned.

Sophos AutoUpdate	status				
Date/time	Code	Description			
10/09/2013 14:31:24	000006b	Download of RM	SNT failed from s	erver \\SRVTWO\	Sophc
History					
Sophos AutoUpdate	status				
Date/time	Code	Description			
10/09/2013 14:31:24	000006b	Download of RM	SNT failed from s	erver \\SRVTWO\	Sophc
10/09/2013 13:31:58	00000000	Updated success	sfully		
10/09/2013 11:47:41	000006d	Restart needed f	or updates to tak	e effect	
IDEs install	led				
	advalue a		a a base ide	and shalls	

Vulnerabilities can be seen under the Patch Details tab of the main pane.

The console has a Subscriptions menu, which makes it easy to access detailed licensing information.

# **Client/server antivirus tasks**

Updates and full scans can be carried out by right-clicking the computer group in the topleft pane, or one or more computers selected in the main pane; the commands Update Computers Now and Full System Scan are available on the context menu.

Scheduled scans and exceptions for these can be configured using the policy dialog for the Anti-virus and HIPS component.

Vulnerability scans (patch assessments) are run automatically according to a schedule defined in the relevant policy.

The automatic schedule can be changed by double-clicking the icon for the default updating policy in the lower-left pane of the console window.

We could not find a means of updating the program version, other than re-running the deployment wizard.

To enable or disable individual components such as the real-time protection or firewall, an appropriate policy can be created and assigned to the relevant clients. This is done by right-clicking the policy icon for the component concerned and selecting Create Policy.

Protection components such as the firewall can be added or removed by re-running the deployment wizard (right-click a computer or group and click Protect Computers). This provides a component choice page, from which any item can be added or removed.

Device control is carried out using the policy of the same name.

# **Client antivirus software**

The Sophos Endpoint Protection and Control software has a fully featured client interface, not unlike that of a consumer security



product. It is reminiscent of the Windows XP Explorer:



Scanning functionality is provided on the home page of the program: Scan My Computer runs a full scan, whilst Scans allows a custom scan to be run. There is no update button or menu item in the window, but right-clicking the system tray icon allows an update to be run.

The Status panel, in the top left-hand corner of the window, shows the status of real-time protection and updates. When we disabled real-time protection, there was no obvious warning in the window, although Sophos displayed a Windows 8 warning message (or System Tray message in earlier versions of Windows):



The same alert is shown when logging on to the computer. When logged on with a standard user account, we were not able to deactivate real-time protection, as the controls were greyed out.

When we attempted to download the EICAR test file, Sophos blocked the webpage and displayed the following alert:

Threat detected. A threat has been blocked and quarantined. We feel this makes clear that no further action is necessary.

# Server antivirus software

The interface of the server antivirus software can be considered identical to that for the clients.

# Summary

We found installing the Sophos console and client software deploying the to be unproblematic, with assistance from the Quick Startup Guide. Despite housing a wide range of functions, the console is straightforward to navigate. The client software is also clear and provides standard functionality. We feel that experienced IT professionals will feel entirely comfortable with the Sophos software, and that with minimal training it could be used by non-expert administrators too.



S



# **Symantec Endpoint Protection**

# Introduction

Symantec make a wide range of security products for businesses large and small. Endpoint Protection uses a locally installed management console to deploy and manage endpoint protection software for client PCs and file servers.

# Software version reviewed

Symantec Endpoint Protection Manager 12.1 Symantec Endpoint Protection 12.1

#### System requirements

Client operating systems: Windows XP, 32-bit; Windows Vista, 7, 8, in both 32 and 64-bit architectures.

Server operating systems: Windows Server 2003, 2008, 2008 R2, 2012, including all

Small Business Server variants, all 32 and 64bit.

# Downloading the software

Having completed the registration for the trial version, the user is taken to the download page. There are two items available in English (software and tools), both clearly marked and easy to find. When run, the main .exe file extracts not only the setup files but also the documentation, which we find very convenient.

#### Documentation

The documentation included in the downloaded package consists of a 132-page guide to the client software, a 28-page Getting Started guide, and a comprehensive 1,156 Installation and Administration Guide. All three are well organised and written, and

extensively bookmarked, but unfortunately completely lacking in screenshots. The Getting Started guide only covers client deployment using a link in an email, so we used the Installation and Administration Guide to assist us in deploying the client software.

# Installing the console

This is a very simple process, involving accepting the licence agreement, choosing the installation folder, and stating whether more or less than 100 clients will be protected. At the end of the process, a message box states that a database is being created and initialised, and that this "will take a few minutes"; this actually turned out to be 25 minutes, at the end of which we had started to wonder whether the process had hung.

# **Client/server antivirus management interface**

The Home page of Symantec Endpoint Protection Manager features boxes for overall and individual security status, license status and recent malware events. We feel this provides the administrator with a good overview of the state of the network and would highlight any problems immediately. A left-hand menu column provides links to Monitors, Reports, Policies, Clients and Admin. Monitors provides access to logs and other statistics; Reports enables the administrator to display highly customised summaries; Policies information allows specific client configuration to be applied to groups of client PCs; Clients displays a list of all the individual PCs on the network and allows a variety of monitoring and administration tasks to be carried out. Admin enables configuration of console users. We feel the layout of the console is clear and simple and enables the administrator to find relevant areas quickly and easily.

# Deploying the antivirus software

When the console is first opened, a welcome dialog is displayed:

Welc	OME ec Endpoint Protection	Symantec.
	License Status Your product has been activated. Add additional licenses	
	Product Tour Learn about Symattec Endpoint Protection features in 5 minutes or less. Start the four	
	LiveUpdate Last content download: Friday, 23 August 2013 12:48:32 o'clock CEST Run Now	
	Client Deployment Use the Client Deployment Wizard to install protection on your client comput Launch Client Deployment Wizard	ers.
	Server Settings You night want to customize settings for your email or proxy server. Change Server Settings	
Do not show	v this Welcome Page again	Close

The Client Deployment Wizard can also be started from the Common Tasks list in the console. Remote push installation requires an installation package and options to be selected from a single dialog box; the computers to be installed are then selected from a list:

allable Computers:	Install Protection Clier	nt on:	
httgure Network Timeout	 Computer	Type	Current Protection
rowse Network Search Network	S EIGHT	64-Bit	
Microsoft Windows Network	SEVEN	64-Bit	
E- J AVC	SXP (172.20.1.106)	32-Bit	
SEVEN			

Once installation has started, a real-time status report is provided. The client PCs have to be restarted after the software has been installed. There is no choice of components (such as the Symantec firewall) available during the installation process. However, a custom installation package can be made, allowing administrators to select or deselect whichever components they want.

We found deployment using remote push to be very quick and straightforward.

We installed the file server protection in exactly the same way as the client software. The process has to be run again for servers as



the software configuration for them is different.

There are two alternative installation methods for client PCs. The administrator can email users with a hyperlink to the client software. The user installing the software needs administrator credentials to carry out the procedure. Alternatively, an executable installation package can be saved to a file share on the server, so that the user or administrator can browse to the network share from the client PC.

# **Client/server** antivirus monitoring

The Security Status box in the top left-hand corner of the console window shows the state of important protection components, such as real-time protection and firewall. If all is well, the box is green and displays the text "Security Status – Good". In the event of a problem, even with a single client PC, the box turns red and warns "Attention Needed":



Clicking on View Details displays a comprehensive list of protection components, with any that are disabled marked in red; the hostname and IP address of all affected PCs are given.

The Endpoint Status box below Security Status shows how many PCs have up-to-date signatures, and how many are out of date; clicking on View Details opens a list of all the PCs on the network, showing OS, logged-on user, IP address, time of last scan, date and version of signatures, and status of individual protection components.

The version of the endpoint software installed can be found by clicking the Clients tab in the vertical menu column at the left-hand edge of the window. Malware discovered is clearly displayed in the Virus and Risks Activity Summary box on the Home page of the console. It is divided into two categories, Virus and Spyware/Risks, and the time period to be shown can be set to anything between an hour and a year.

We could not find any means of scanning for vulnerabilities.

Licensing information is shown in the License Status box in the top right-hand corner of the console window. This displays a warning in the event of a problem:



Clicking on Licensing Details opens a detailed information page; although this claims to provide licence expiration dates, this was the one bit of licensing information we were unable to find.

# **Client/server** antivirus tasks

A variety of tasks can be run from the Clients view of the console, including scans and updates:



Running the scan command opens a dialog box with a choice of quick, full or custom scans. The same context menu also allows individual protection components to be enabled or disabled, though it does not allow real-time protection to be deactivated. A command to restart the selected computer(s) is also available. A policy is used to schedule scanning of client PCs. The console allows the default scan to be edited, or new scans to be created.

Automated updates are also controlled by a policy. By default, this checks for new updates every four hours. The policy can easily be altered to make updates more or less frequent.

Components of the suite can be added or removed by rerunning the Client Deployment Wizard, and deploying a customised installation package. This worked very well in our test; the endpoint protection software on the client was stopped and then immediately restarted with the new configuration.

Rerunning the deployment process could also be used to update the version of the endpoint protection software.

Excluding a specific file or folder from scanning can be done by going to Policies and clicking Exceptions. This allows a wide variety of items, including applications and web domains, to be excluded from scanning:



Symantec Endpoint Protection Manager can block devices such as USB flash drives. This can be done by going to Policies, selecting Application and Device Control, editing the default policy, and adding the appropriate device type to the Device Control list. We found this very intuitive, and once we had clicked "Assign the policy", the USB flash drive plugged into one of our client PCs was almost immediately rendered invisible in Windows Explorer. The administrator can choose to display a message on the client PC when the device is blocked.

# **Client antivirus software**

The client software of Symantec Endpoint Protection has a similar interface to consumer antivirus products:

		Status - Symantec Endpoint Protection	- • 💌
	Status		Help
Status		Your computer is protected.	
Scan for Threats		No problems detected.	
Change Settings		Protection definitions are current	
View Quarantine View Logs	The follow	ing Symantec security components are installed on your computer:	
LiveUpdate	2	Virus and Spyware Protection Protects against viruses, malware, and spyware Definitons: 22 August 2013 r22	Options
/	<u> </u>	Proactive Threat Protection Provides zero-day protection against unknown threats Definitons: 16 July 2013 r11	Options
	<b>.</b>	Network Threat Protection Protects against Web and network threats Definitons: 22 August 2013 r11	Options
Symantec.			

There is a big and obvious status display at the top of the window. This uses text, an icon and colour to show whether all is well. In the event of a problem, a "Fix All" button appears in the status area; clicking this reactivates any disabled components.

Using the items in the menu column on the left, the user can update signatures, and run either a quick scan or a full system scan.

When logged on to the PC with a nonadministrator account, the menu items for disabling protection components are all greyed out and thus cannot be used.

When we attempted to download the EICAR test file, Symantec Endpoint Protection blocked the download and briefly displayed the following message:



As the message disappears after only 4 seconds, and does not link to any further

information, we are not convinced of its value.

# Server antivirus software

The server antivirus software can be regarded as identical to the client software in terms of interface. The deployment wizard provides the option of installing only "Basic" protection (without firewall), which we took. Only the Virus and Spyware Protection strip is then shown in the program window.

# Summary

We found protecting our network with Symantec Endpoint Security to be very convenient and trouble-free. The management console has been graphically well designed, displaying important information without overwhelming the user, and making everyday tasks easy to find and carry out. The software was very reliable and unproblematic in our test. We feel it should prove very easy for IT professionals to use, and only minimal training would be required for non-expert administrators.





# Webroot SecureAnywhere Endpoint Protection

# Introduction

Webroot's business security software uses a cloud-based console to manage endpoint security software on client and server computers.

# Software version reviewed

Webroot SecureAnywhere Endpoint Protection 8.0

Webroot SecureAnywhere Console as at  $4^{th}$  September 2014.

# System requirements

Webroot SecureAnywhere Endpoint Protection runs on Windows Server 2003, 2008, 2008 R2, and 2012, all in 32 and 64-bit versions where applicable. Supported Windows client operating systems are Windows XP, Vista, 7 and 8, again all in 32 and 64-bit versions. Additionally, Mac OS<sup>®</sup> X v.10.7 "Lion" and Mac OS X v.10.8 "Mountain Lion" are supported.

# Downloading the software

This is not applicable, as the console is webbased.

# Documentation

Webroot provide a comprehensive online help service, which could be described as an online manual. It covers all aspects of using the software, starting with creating a Webroot account. It is easy to navigate, due to a contents panel on the left-hand side of the page, and is illustrated with screenshots where necessary:

Getting Started Abort SecuriArywhere Endpoint Protection Creating a Watcot Account Logicity in the SecuritArywhere Endpoint Protection Using the Schap Witand Vatorice znanood endpoint status	Viewing ma The SecureAnyon Secure Home Co	anaged endpoin where Endpoint Protect Anywhere.	<b>it status</b> ion Status page gives	an overview of your man	laged endpoint		user@filienal.con +
About Deployment Downloading and Running the	Status Palcie	a Group Kanagement B	eperte   Overvies   Loga				
Security New Installer Ramiting using MS1 Installing using MS1 Installing using GPO Using the Security New Installing Displayment Isol Working with accounts Ecoling accounts all your account Configuring Junion	Alert Extension and the second						UL 2 0.0.100 0.0.000 0.0.000 0.0.000 0.0.000 0.0.000 0.0.000 0.0.0000 0.0.0
Managing Users	R Endpoint activ	ity over the Last IN hours	All Recently intected en	Appoints (Leal 7 days)			11.0
Creating a new user	Last 24 Hours	*	Postname	Peter	67040	Lest Infected	Docked Programe
Setting user permissions	See.	10	1 DIEARDA	Donanaged	Rutachines	Apr 19th 2012, 22:32	Vev
Editing user information	Not Seen	St View	2 R-64-1007	Domanaged	R_Machines	Apr 190 2012, 17:45	Vev
Managing License Keycodes Vewing locese keycodes Adding a locese keycode Adding Endpoints to Manage Adding endpoints to Manage	Tital	80,010					
Managing Policies About Policies About Policies Creating a new policy Editing a policy Remaining a Policy Copying a policy Copying a policy	The Status page - An alert n - A bar cha	shows: otification, if manage rt showing the numb	d endpoints need at er of endpoints that	tention. Click the notifi encountered threats in	cation to see a the last 7 day	list of endpoints that encou s. Click a bar to see a list of	ntered threats. endponts that encountered thre
Copying a policy Deleting a policy	<ul> <li>A pie cha</li> </ul>	t showing the Webro	et SecureAnywhere	software versions on	your managed	endpoints.	



A searchable online FAQ page is also available.

# Installing the console

This is not applicable, as the console is webbased.

**Client/server antivirus management interface** 

Logging on to the SecureAnywhere console involves entering two characters of a "Personal Security Code", a word or number at least six characters long, created when the Webroot account is set up.

The Home page of the console simply has links to the Endpoint Protection page and Webroot Community. We would regard the Endpoint Protection page, shown in the main screenshot above, as the main status display. It is made up of four main panels: Status; Endpoints Encountering Threats; Agent Version Spread (program version); and Recently Infected Endpoints. A row of tabs along the top of the console provides access to various tasks and information, including Policies (client configuration), Group Management (everyday administration tasks), Logs, and Resources (installation and deployment area). We found the layout of the console to be clear and straightforward.

# Deploying the antivirus software

Direct installation of the endpoint software from the client is extremely quick and easy. The administrator merely needs to log on to the console, go to the Resources page, click Windows Download, and then Run. No further action is necessary, and the software is installed in seconds. The same method is used for servers as for clients.

# **Client/server antivirus monitoring**

In our test, the console did not warn in any way when we disabled real-time protection on a client. However, Webroot inform us that program's entire functionality is contained within the WRSVC service/WRSA.exe, and that if this is switched off or fails to start, the endpoint protection will be shown as inactive in the console.

Due to the cloud-based nature of the product, there is no information shown about signature versions or time of last update; the client always uses the latest definitions from the cloud.

Details of the program version installed can be seen in overview on the Status page, or in detail for each individual client on the Group Management page.

Malware discoveries are shown in the Recently Infected Computers pane of the Status page. We did not find any sort of vulnerability scan in the software.

Licensing information can be displayed by running Agent Version Spread in the Reports section or in the Group View.

# **Client/server antivirus tasks**

A variety of tasks can be carried out from the Group Management page. Computers can be selected individually or by group, and the Agent Commands menu allows the administrator to scan, change scheduled scan times, or uninstall the software, amongst other things.

All E	ndpoints					ă H
Save	Changes   🔁 Uni	do Changes 丨 🌄 Mi	ove endpoints to another	group   📙 Apply policy to endpoints	Agent Commands - Deacti	vate
1 9 2 9	Hostname SERVER SEVEN	Policy UI visible UI visible	Group Default Group Default Group	C Scan Solder C Change scan time S Scan a Solder Clean up System Gleaner Unisstal Reset Reset	Agent     Clear Data     Clear Data     Krycode     Powrel User Access     Anfimalware Tools     Files & Processes     Monthly Sheld     downood     downood     Vew commands for selected of	b b b b b b b b b b b b b b b b b b b
					How to Use Agent Commands	

Additional commands available include logging off the current user, shutting down or restarting the PC, or even restarting in Safe Mode with Networking, which we found particularly thoughtful – this is very useful in the event of a malware infection.

Updating signatures is not relevant, due to the cloud-based nature of the program.



Enabling or disabling individual components can be done via policy. The administrator creates a new policy, which can be altered very easily from the configuration dialog box:

Section			
	Setting	Live	Draft
Basic Configuration	Realtime Shield Enabled	Off	
Scan Schedule	Enable Predictive Offline Protection from the central Secure	On	
Scan Settings	Remember actions on blocked files	On	
Self Protection	Automatically quarantine previously blocked files	On	
leuristics	Automatically block files when detected on execution	On	
Realtime Shield	Scan files when written or modified	On	
Behavior Shield	Block threats automatically if no user is logged in	On	
Core System Shield	Show realtime event warnings	Off	
Veb Threat Shield	Show realtime block modal alerts	Off	
dentity Shield	Show realtime block notifications	Off	
Firewall			
Jser Interface			
System Cleaner			

USB devices can be controlled by setting the highest level of heuristics in the policy. Webroot tell us that scan exclusions are not necessary, as all files and processes are already classified by the security software.

#### **Client antivirus software**

By default, Webroot's client software has a minimalist interface. There is a system tray icon; right-clicking this displays the following context menu:

Scan Now
Open
Help and Support
About
Refresh configuration
Save a Scan Log
 ▲ 🤎 记 04/09/2013

The only action available to the user is to start a pre-configured scan. Clicking "Open..." merely shows a message box, stating that the user should contact the administrator to access the user interface.

It is possible for the administrator to enable the full user interface, which has a program window identical to that of Webroot's consumer antivirus software:

Overv	ew PC Security Identity & Privacy System Tools My Account		
	You are protected! SecureAnywhere is protecting your computer. No active threats have been det There are 30 days remaining in your subscription.	ected.	
0	Last scanned 8 minutes ago. Next scan starts in 21 hours, 57 minutes, 23 seconds.	Scan Now	¢
0	Protection has been active for 9 minutes, 45 seconds.	Suspend	0
٢	4,402,882 system events have been inspected since installation.	View Details	-02-
0	3 secured sessions are currently active and being protected by the identity Shield.	Advanced	0
٢	System Cleaner has analyzed all installed applications and is ready to clean.	Cleanup Now	0
0	The SecureAnywhere firewall is monitoring 15 processes with 74 active network connections.	Disable	¢

However, most of the controls, including those for enabling or disabling individual components, are disabled; clicking any of them displays a message stating that the program is centrally managed. We feel that most administrators would regard such a program window as being merely a distraction, and that the default minimalist interface makes more sense.

When we attempted to download the EICAR test file, Webroot blocked the download and displayed the following message:

as been
as been
w

Clicking on Allow displays a further message: "Your administrator has blocked access to this function". We feel that whatever the user clicks, it is clear that the download has been blocked.

# Server antivirus software

The server software and its possible configurations are identical to those for the clients.



# Summary

Webroot SecureAnywhere Endpoint Protection is very straightforward to use. The console is clear, and deployment via individual installation on client machines could easily be carried out by non-expert administrators. The online help is also good.



Feature list	AVIRA	Bitdefender	ESET	F-Secure	G Data	IKARUS	Kaspersky Lab	Sophos	Symantec	Webroot
Recommended product for:										
up to 5 Clients, Server			ESET Endpoint Security		G Data SmallBusiness		Kaspersky Small Office	Sophos Endpoint	Symantec Endpoint	
		Cloud Security for Endpoints by Bitdefender	ESET Endpoint	F-Secure Client Security	G Data EndpointProtection		Security	Protection - Business	Protection Cloud	
up to 25 Clients and 1 Fileserver		chaponits by bitaerender	Protection Standard		Business		Security		Symantec Endpoint	
	Avira Small Business				G Data EndpointProtection	IKARUS security.manager			Protection Small Business Edition	Webroot SecureAnywhere Business - Endpoint
up to 25 Utents and Fileserver and Messaging Server	Security Suite	Cloud Security for	ECET Comune		Enterprise		Kaspersley Enterprise Conce	Protection - Advanced		Protection
more than 25 Clients, more than 1 Fileconer, more		+ Bitdefender Security for	Business	F-Secure Business Suite	G Data EndpointProtection		Security		Sumantos Protostion Suito	
than 1 Messaging server		Exchange			Enterprise plus				Enterprise Edition	
					Fatchmanagement					
Features Management Server										
What is the maximum number of clients overall?	1000	unlimited	unlimited	unlimited	unlimited	unlimited	unlimited	25000	unlimited	unlimited
Master-Slave-Server										
Multiple AV Servers	•		•		•		•		•	
Master server controls slave server in different	•		•		•	•	•		•	
offices	-	-		-		-	-			
stave server for distributing updates	0	0	0	•	0	8	0		0	
Client Installation										
support?										
Does the product include a mechanism that allows the administrator to push the software to the		•	•							•
clients?		-			-		-		-	-
Does the product include a mechanism that allows		•	•							
the end user to download and install the software?		-	-	-	-		-	-	-	-
General Capabilities										
Does the product allow administrators to assign										
anterent policies to different groups of computers (regardless of the person longed in)?	•	•	•	•	•	•	•	•	•	•
been also and out any sector of the sector o										
uses the product support static groups (i.e. user or computer are assigned manually to a group or are	•	•	•	•	•	•	•	•	•	•
imported from a third party system)?										
Group Import & Synchronisation										
Can changes in Active Directory be synchronized?						•			•	
Can computers/users he immorted from other LDAP										
server?	•		•	•		•	•		•	•
Can computers be imported by a GUI	•		•	•	•	•	•		•	
Can different actions be defined based on the	•		•		•	•	•		•	•
matware category: Microsoft Exchange										
Euchanne 2002 / 2007 / 2010	•	•	•	•	•	•	•		•	
Exchange 2003 / 2007 / 2010	•	• •		<b>-</b>		•				
Network shares		1	-	1		1		-		
entering a password?	•						•		•	•
Email Messages										
Microsoft Outlook	•	•	•	•	•	•	•		•	
Lotus Notes	•		•		•		•		•	
Thunderbird	•	•	•		•		•			
Archives		-	-		-					
7TP/PAP/AP1 & archived installer	•	•	•	•	•	•	•	•	•	
Contribution & alcinived instances	-	-	-		-	•	-	-	-	
Remediation										
Does the product provide remediation capabilities?		•	٠	•	•		•	•	•	•
General capabilities										
Firewall Rules										
Does the product come with default policies for	•	•	•	•	•	•	•	•	•	•
Does the product come with default policies for		•		•	•		•	•	•	•
server?		•		•	•	•	•	•	•	•
Client Management										
Client User Interface										
Lan the administrator limit or control configuration changes by the end-user?	•	•	•	•	•	•	•	•	•	•
Can different policies be applied for different	•	•	•	•	•	•	•	•	•	0
computers? Depending on the location of the device (i.e. Office.										
Hotel, Home, etc)	•		•		•	•	•		•	•
Depending on group membership of the computer	•	•	•		•	•	•		•	•
Depending on group membership of the user (i.e.				•	•	•			•	•
Administrator Management										
Rights / Access Control										
Does the product support multiple administrators										
and different access levels?	v	v	•	v	, v		v	•		v
Device Control										
Does the product allow administrators to limit the			•	•	•		•	•	•	•
use or external devices (USB sticks, printers, etc)?										
Can you lock										
DVD / USB / external media			•	•	•		•	•	•	•
Floppy			•	•	•		•	•	•	•
			All ports and all removable							
Ι.			media can be locked, but				multifunctional devicer		Firewire, Bluetooth, printers, modems, wi-6	
other			it's possible to add	Any PnP devices	Webcam		external network adapters,		CD/DVD/Blueray, card	
			individual ports or media				wi-fi, Bluetooth devices		readers	
r.u										
Fallover										
What if the AV Server (local) hangs up										
automatic switching to a second local server		•	•		•		•	•	•	
updates from vendor-server instead of local server	•	•	•	•	•	•	•	•	•	
										I and and as in the set
						It is not set by default but				always communicate with
other			Log and notifications	Multiple proxy servers and		you can define that if the server is not responding				the cloud, plus local
			- g and inserticutions	proxy chaining supported		the AV should use the				'offline' policy protects
						IKARUS online server				are lost.

		Avira		Bitdefende			ESET			F-Secure			G Data			lkarus			Kaspersky Lab			Sophos			Symantec		Webroot	
Supported Operating Systems	Management	Management	Protection	Management Managemen	t Protection	Management	Management	Protection	Management	Management	Protection	Management	Management	Protection	Management	Management	Protection	Management	Management	Protection	Management	Management	Protection	Management	Management	Protection	Management Management Pro	otection
Apple	Server	Lonsole	Client*	Server Console	Clerk	server	Lorisone	Csent	Server	Lonsore	Cient	Server	Lonsole	Cient	Server	Console	Client	server	Console	Uent	server	Lonsole	Lient	Server	Lonsole	Clent	Server Lonsole C	Cient
Mac OS		1									•		•	1						1		1	•			•	•	
Mac OS X								•			•		•							•			•			•	•	•
Mac OS X Server											•		•							•			•			•	•	
IPhone OS / IPod OS											•		•														•	
Windows 2000		r																										
Protessional / Server / Advanded Server						•	•																•					
Advanced Server 64 Bit Itanium						-		-															•					
Data Center Server / Data Center Server 64 Bit Intel						•	•	•															•				•	
Data Center Server 64 Bit Itanium																							•				•	
Windows XP																												
Home		•	•		•	•	•	•		•	•	•	•	•	•	•	•						•	•	•	•	•	•
Professional		•	•		•	•	•	•		•	•	•	•	•	•	•	•			•		•	•	•	•	•	•	•
Media Center / Tablet PC Edition					-	•	•	•			•	•	•	•	•	•	•			-			•			•		•
Windows Server 2003						•	•	•			•	•	•	•			•			•			•		,	•		•
Standard / Enterprise / Data Center / Small Business Server	•	•			•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•
Cluster Server / Storage Server						•	•	•			•	•	•	•	•	•	•				•	•	•	•	•	•	•	•
Web Edition						•	•	•	•	•	•	•	•	•	•	•	•				•	۰	•	۰	•	•	•	•
R2 Standard / Enterprise					0	0	•	0	0	0	•				•	•	0			•	0	0	•	0	0	•	•	•
Windows Vista					_			-																				
Home Basic / Home Premium		•	•		•	•	•	•		•	•	•	•	•	•	•	•						•		•	•	•	•
Business / Enterprise / Ultimate		U	•		•	•				U	0			•		U			•	•		•			U			•
Starter Edition										•		•		•			•	_	-						•			•
Home Premium		•	•			•	•	•		•	•	•	•			•	•				•	•	•	•	•	•	•	•
Professional / Ultimate / Enterprise		•	•		•	•	•	•		•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•
Windows 8																												
Professional / Enterprise			•		•	•	•	•			•	•	•	•						•						•		•
Windows 2012																												
Server 2012						•	•	•			•																	•
Windows Server 2008																												
Standard - Core Installation		•			•							•	•	•					•			•			•		•	
Enterorise								,				•												•				•
Server R2 (Standard/Enterprise)		-			•	•	•	•	•	•	•	0	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•
Data Center / Web Edition						•	•	•	•	•	•	•	•	•	•	•	•			•	•		•	•	•	•	•	
Foundation						•	۰	۰	•	•	۰	•	•	•	•	•	•				•		•	۰	•	•	•	
HPC						•	•	•				•	•	•	•	•	•								•	•	•	
Windows Mobile																												
Windows Mobile								•			•									•							•	
Works for Citrix		r																										
Works for Citrix						•	•	•	•	•	•	•	•	•						•	•	•	•			•	•	•
0590/91/93	_	r									•			<u> </u>	<u> </u>			<u> </u>		•		<u> </u>					•	
Series 60								•			•									•								
Linux					1																							
Redhat																												
Redhat Enterprise Linux 3.x 32 Bit / 64 Bit								•												•						•	•	
Redhat Enterprise Linux 4.x 32 Bit / 64 Bit								•	•	•	•							•	•	•			•			•	•	
Redhat Enterprise Linux 5.x 32 Bit / 64 Bit								•	•	•	•			•				•	•	•			•			•	•	
Redhat Enterprise Linux 6.x 32 Bit / 64 Bit								•	•	•	•									•						•		
SUSE	_	r	1		1																		•					
SUSE Linux Enterprise Desired p.3.2. Bit / 64 Bit								•			•												•			•		
SUSE Linux Enterprise Desktop 10.x 32 Bit / 64 Bit								0			0			•						•			0			0	•	
SUSE Linux Enterprise Server 10.x 32 Bit / 64 Bit								•	•	•	•			•				•	•	•			•			•	•	
SUSE Linux Enterprise Desktop 11.x 32 Bit / 64 Bit								•	•	•	•									•						•		
SUSE Linux Enterprise Server 11.x 32 Bit / 64 Bit								•	•	•	0									•						•		
Novell																												
Open Enterprise Server OES 32 Bit								•																		۰		
Open Enterprise Server UES 64 Bit																												
VMware					-													-	-	-								
ESX 4.x	•	•	•			•	•	•	•	•	•				1			•	•	•	•	•	•			•		•
ESX 5.x	•	•	•			•	•	•	•	•	•	•	•	•				•	•	•						•		•
											Server 2008,												Microsoft hyper-v,					
				Amazon Linux Manageme	ıt			Solaris, NetBSD,	CentOS, Ubun	tu, Debian,	Small Business Server 2011												FreeBSD, HP- UX.			Debian, Fedora,	Management console is	
Other supported OS				AMI, hosted in- the-cloud browser				Ubuntu, Free BSD, Android	openS	USE	(Standard),										Microsoft	hyper-v	OpenVMS,			Novell, Red Hat, Ubuntu	browser	
				based.							Debian,												Asianux,				based.	
											TurboLinux												Ubuntu					
Database																												
Does the product require a database	•			•		•					•	•			•			•			•			•				
For how many users/clients is the free database recommended				Unlimited		Unlimited			20000			<1000			Unlimited			≺ 100			25000			5000				
				MongoDB, database		Microsoft Access			H2 (embedded		Mirrosoft SOL	Microsoft SOJ			Nicrosoft SOL			Microsoft SQL			MS SOL Evolution			Subase SOL				
Which database is included (i.e. Microsoft SQL, Sybase, MySQL, etc)	MS Access			infrastructure stored in-the-		(Jet database) engine			database engine)		2008 R2 Express	2008 Express			2005			2005 Server Express Edition			2008			Anywhere				
				cloud					- , ~,								l l'											
Winch additional databases are supported Mirrosoft SOI Server																												
Microsoft SQL Server 2000															-				1					•	1			
Microsoft SQL Server 2005 / 2008 / 2008 R2						•					•	•			•			•			•			•				
	any ODPD					MUSOL E.O.												Microsoft SQL										
Other	database					Oracle 9i and											1	Express 2005 / 2008, MySQL						SQL 2012				
	possible					later												Enterprise										
Email Server																												
Microsoft Exchange					•			۰			•			•				•					۰			۰		
Domino								•										•					•			•		
Linux																												
Novell Netware Server																										Only via SMTP		
Dell NAS																										gateway		
Kerio								•															•					

Feature list	Avira	Bitdefender	ESET	F-Secure	G Data	Ikarus	Kaspersky Lab	Sophos	Symantec	Webroot
Recommended product for:			-	-	-		-			
up to 5 Clients, Server		Cloud Security for	ESET Endpoint Security	F-Secure Client Security +	G Data SmallBusiness Security	IKARUS anti.virus	Kaspersky Small Office Security	Sophos Endpoint Protection - Business	Symantec Endpoint Protection Cloud	
up to 25 Clients and 1 Fileserver	Avira Small Buciness	Endpoints by Bitdefender	ESET Endpoint Protection Standard	F-Secure Server Security	G Data EndpointProtection Business		Kaspersky Endpoint Security for Business SELECT		Symantec Endpoint	Webroot SecureAnywhere
up to 25 Clients and Fileserver and Messaging Server	Security Suite	Cloud Security for	ESET Socuro		G Data EndpointProtection Enterprise	IKARUS security.manager		Sophos Endpoint Protection - Advanced	Edition	Business - Enterprise Protection
more than 25 Clients, more than 1 Fileserver, more than 1 Messaging server		+ Bitdefender Security for Exchange	Business	F-Secure Business Suite	G Data EndpointProtection Enterprise plus PatchManagement		Kaspersky Total Security		Symantec Protection Suite Enterprise Edition	
Features Management Server										
What is the maximum number of clients overall?			unlimited	unlimited	unlimited		unlimited		unlimited	unlimited
What is the maximum number of clients that can be managed from a single management server under the following conditions: All necessary components (database, repositories, update mechanisms, reporting, etc.) are installed on this server and the Clients communicate with the server either continuously or at least once per hour	1000	unlimited	50000	20000	1000	unlimited	50000	25000	80000	20000
Required <u>minimum</u> hardware (CPU/RAM/free disk space)	1GHz, 1GB RAM, 5GB disk space	No server hardware required. The server is hosted in-the-cloud.	1GHz, 512 MB RAM, 1GB disk space	2GHz, 1GB RAM, 6GB disk space	Core 2 Duo, 2GB RAM, 2,5GB disk space	2GHz, 1GB RAM, 500MB disk space	1GHz, 512 MB RAM, 1GB disk space	1GHz, 512MB RAM, 500 MB disk space	3GHz, 4GB RAM, 300GB	No server hardware required. The server is hosted in-the-cloud.
Does the product provide a mechanism to limit the data transferred over WAN Links when updating clients in remote locations?			e	e	e		e	0	0	
By designating one client as local source for definition updates (Super Agent, Group Update Provider)	•	e	•	•	•	•	e	•	•	
Which options does the product provide to ensure that only authorized administrators can administer the product?	username and password for authentification	Role based user models enforced through passwords	Password protection (role based management), encrypted communication	Password-based user authentication in Policy Manager Console.	Role based user model enforced through passwords / AD Login/Windows based Login / password-protected client / encrypted communication between server and client and server and administrative console	Password protection of the server	Authentification username, password, password-protected client, system tray icon hide	Password protection, encrypted communication, role-based administration	Symantec Authentication, Windows Authentication, and RSA Authentication	Administrator access is limited to those with a username and password plus an up to six-digit PIN number. Individual access rights are also imposed.
Log out administrator if idle for a specified time	•	•	٠		•		•	•	•	•
Master-Slave-Server										
Multiple AV Servers	•		•		•		•		٠	
Master server controls slave server in different offices	•		•		•		•		•	
Slave server for distributing updates	•		•	•	•	•	•		•	

Notes		Management server infrastructure is hosted in- the-cloud, providing High Availability and unlimited scalability. Individual Update Servers can be installed into LAN. It is possible to install and configure more Update Servers in cascade.	Slave servers can be nested in multiple levels, each with its own credentials for access, which can be dependent on administrator's role (read-only/limited user/full privileges). Policies from upper level servers could be propagated to lower levels.		Different deployment possibilities, such as: All in one management server deployment, redundant server deployment (Main and Secondary ManagementServer), combination between management server and cascaded subnet servers (Update agent) and/or Peer-to- Peer update distribution between clients, multiple management servers based for example on their location and managed with the G Data Master Administrator	every workstation/server with a simple windows fileshare can be used as a "distributing update server"	Update agent can be used for distributing updates. An Update agent is a PC within the Administration server network dedicated to store and distribute database updates, installation packages, group tasks and policies.			
Client Installation										
Which client deployment methods does the product										
support?		1	1		1					
Does the product include a mechanism that allows the										
administrator to push the software to the clients?	•		-	-	-	-	-	-	-	
Can the installation of the clients be staggered over	•		•	•	•		٠	•	•	
time to ensure that the network is not over utilized?										
Can the administrator see the status of the										
deployment (i.e. Transfer, Installation in Progress,	•	•	•	•	•	•	•		•	•
Installation complete. etc.)?										
Does the product include a mechanism that allows the		_			_					
end user to download and install the software?		, v	w w	v	, v		¥	¥	· ·	¥
Can the admin send a link which allows the user to										
download and install the software?		٠	•	•	•	•	•	•	•	•
Does to product support the creation of MSI packages										
for deployment with 3rd party tools and Active			•	•			•		•	•
Directory (GPO)?										
Does the product support the creation of single file										
executable (.exe) installer (i.e. for logon scripts or CD		٠	•	•	•	•	•	•	•	•
distribution)										
Can computers be imported from a text file?	۵	1		1		•		۵	ė	1
can compare be imported from a text mer	-		-	_	_			-	-	-
Can computers be imported from Active Directory?			•	•	•		•	•	•	*
Keeping the OLL structure defined in Active Directory				6						
keeping the OO structure defined in Active Directory	*		*	*	-	*	•	*	*	*
Using other criteria to assign computers to groups	•		•	•	•	•	•		•	•
Can changes in Active Directory be synchronized?	0		•			0	•	•	•	•
Can the synchronisation schedule be defined?	•		0		•	é	•	0	0	
Can computers be imported from multiple Active		1		_	_		_		_	_
Directory server?				•	•		•		•	•
Can computers/users be imported from other LDAP				6			۵		ė	
server?	•		•	•		•	•		•	
Can computers be imported by a GUI	•		•	•	•	•	•		•	
can different actions be defined based on the malware			0		•	0	•	0	•	
Scan Location										
Can the administrator exclude/include files and folders					1					
from being scanned (by file extension)?	0	•	0	•	•	•	•	•	•	
By predefined lists of extensions provided by the										
product			•	*			•	•	•	
By filenames ("file tyt") regardless of folder or location				ė						
by menumes ( menue ) regardless of folder of focation				•	-		-			

By filenames & specific folder ("c·\Directory\file tyt")	•	•	۵	۵			•	•		
by menanies a specific folder ( c. (Directory (metax))	<b>_</b>			<b>_</b>						
By folder name Standard Windows folder (i.e. %WINDOW/S%	8	8	8	8	*		8	8	*	
%SYSTEM22%) regardless of the operating system										
	-	-	-	-		-	-		-	
Does the product provide preconfigured exclusions?	ė	e	÷	e			ė	ė	•	
Microsoft Exchange										
Microsoft Exchange	•	<b>e</b>	ė	0	ė		0	é	•	
Network shares										
Is scanning of network shares disabled by default?	8				e	•	•	÷	•	
Can a user or administrator scan network shares after	•						•			
entering a password?	•						•		•	
System memory / Processes		1	-			1			1	
Does the product scan processes in memory for	•	•	•	•	•	•	•	•	•	•
malware?										
Can the administrator define exceptions?	•	*	*	*	, in the second	*	*		*	*
Email Messages					•	<b>I</b>		•	I	•
Does the product scan existing email in the message										
stores of the following applications?					-					
International Outlook / Outlook Express	8		8	w w	×	*	w w		*	
Thunderbird	÷	•	÷		÷			÷	*	
Microsoft Windows Live Mail	ė	-	ė					ė	Only via SMTP gateway	
Microsoft Windows Mail	•	•	•		ė		•	•	,	
Dess the product contineering and outgoing emails									•	
and attachments in the following protocols?										
SMTP / POP3	•	*	•	•	•		•	•	•	
IMAP	•		\$	¢			<b>\$</b>		•	
Archives										
ZIP/RAR/ARJ & archived installers	ê		ê	¢	0	•	4	\$	•	
how doop at an domand (hy default)	00		10	E	100	0	unlimited	10	10	16
now deep at on demand (by default)	20	2	10	5	100	8	untilinteu	10	10	10
Does the product protect itself against Zip of Death and similar attacks?	20	2	10	5	100	8	untilinted	10	10	10
Does the product protect itself against Zip of Death and similar attacks? On Demand Scans	20	2	10	5	100	ŏ	antinitea	10	10	10
Does the product protect itself against Zip of Death and similar attacks? On Demand Scans Can the administrator define when scans should take	20		10		100	8	unninteu	10		
how deep at of neurand (by default) Does the product protect itself against Zip of Death and similar attacks? On Demand Scans Can the administrator define when scans should take place and which Scan locations should be included /	•	•	10	• •	•	•	¢	•	•	•
how deep at of hermatic by default? Does the product protect itself against Zip of Death and similar attacks? On Demand Scans Can the administrator define when scans should take place and which Scan locations should be included / excluded?	•	•	•	÷	•	ŏ ₽		•	•	•
Now deep at of hermatic (by default) Does the product protect itself against Zip of Death and similar attacks? On Demand Scans Can the administrator define when scans should take place and which Scan locations should be included / excluded? Can the system impact vs. scan speed be defined?	•	•	•	•	•	8 •	• •	•	•	•
Now deep at of neural d by default? Does the product protect itself against Zip of Death and similar attacks? On Demand Scans Can the administrator define when scans should take place and which Scan locations should be included / excluded? Can the system impact vs. scan speed be defined? On Access Scan	20 •	•	•	2 *	•	8 <b>8</b>	•	•	•	•
Now deep at of neurand (by default) Does the product protect itself against Zip of Death and similar attacks? On Demand Scans Can the administrator define when scans should take place and which Scan locations should be included / excluded? Can the system impact vs. scan speed be defined? On Access Scan Can the administrator define when a scan is triggered?	•	•	•	•	•	8 • •	•	•	•	•
Now deep at of Default (by default) Does the product protect itself against Zip of Death and similar attacks? On Demand Scans Can the administrator define when scans should take place and which Scan locations should be included / excluded? Can the system impact vs. scan speed be defined? On Access Scan Can the administrator define when a scan is triggered? Can the administrator specify which Scan Locations	20 	•	•	•	•	8 9	•	•	•	•
now deep at of neurand (by default) Does the product protect itself against Zip of Death and similar attacks? On Demand Scans Can the administrator define when scans should take place and which Scan locations should be included / excluded? Can the system impact vs. scan speed be defined? On Access Scan Can the administrator define when a scan is triggered? Can the administrator specify which Scan Locations (incl. Files / Directories) should be included /	20 	¢	•	¢		8 8 8		©	•	•
In the deep at of the definition (by definition) Does the product protect itself against Zip of Death and similar attacks? On Demand Scans Can the administrator define when scans should take place and which Scan locations should be included / excluded? Can the system impact vs. scan speed be defined? On Access Scan Can the administrator define when a scan is triggered? Can the administrator specify which Scan Locations (incl. Files / Directories) should be included / excluded?	20 *	•	•	•	•	8 9 9 9	• •	•	•	•
Now deep at of treatmand (by default) Does the product protect itself against Zip of Death and similar attacks? On Demand Scans Can the administrator define when scans should take place and which Scan locations should be included / excluded? Can the system impact vs. scan speed be defined? On Access Scan Can the administrator define when a scan is triggered? Can the administrator specify which Scan Locations (incl. Files / Directories) should be included / excluded? Log	20 * *	•	•	3 •	•	8	•	•	•	•
In the deep at of the definition of the definiti	20	•	10	•		8		•		•
In the deep at of the definited by definition of the definition of	20 *			•		8 9 9 9				•
In the deep at of the definition (by definition) Does the product protect itself against Zip of Death and similar attacks? On Demand Scans Can the administrator define when scans should take place and which Scan locations should be included / excluded? Can the system impact vs. scan speed be defined? On Access Scan Can the administrator define when a scan is triggered? Can the administrator define when a scan is triggered? Can the administrator specify which Scan Locations (incl. Files / Directories) should be included / excluded? Log Which information is logged? Date and time the infection was detected, the name of the infection and the original location where the Infection and the original location where the	20 • •	•	•	•	•	8 8 8 8 8		•		•
In the deep at of the definition (by definition) Does the product protect itself against Zip of Death and similar attacks? On Demand Scans Can the administrator define when scans should take place and which Scan locations should be included / excluded? Can the system impact vs. scan speed be defined? On Access Scan Can the administrator define when a scan is triggered? Can the administrator specify which Scan Locations (incl. Files / Directories) should be included / excluded? Log Which information is logged? Date and time the infection was detected, the name of the infection and the original location where the infection was found (incl. file name) De mahure actempoting in first Waren etch	20 * * * * * * * * * * * * * * * * * * *			2 0 0 0 0 0 0 0 0 0 0 0 0 0						•
In the deep at of the default (by default) Does the product protect itself against Zip of Death and similar attacks? On Demand Scans Can the administrator define when scans should take place and which Scan locations should be included / excluded? Can the system impact vs. scan speed be defined? On Access Scan Can the administrator define when a scan is triggered? Can the administrator specify which Scan Locations (incl. Files / Directories) should be included / excluded? Log Which information is logged? Date and time the infection was detected, the name of the infection and the original location where the infection was found (incl. file name) The malware category (i.e. Virus, Worm, etc)	20 20 20 20 20 20 20 20 20 20	2 0 0 0 0 0 0 0 0 0 0 0 0 0		2 2 2 2 2 2 2 2 2 2 2 2 2 2						•
In the deep at of the definition (by definition) Does the product protect itself against Zip of Death and similar attacks? On Demand Scans Can the administrator define when scans should take place and which Scan locations should be included / excluded? Can the system impact vs. scan speed be defined? On Access Scan Can the administrator define when a scan is triggered? Can the administrator specify which Scan Locations (incl. Files / Directories) should be included / excluded? Log Which information is logged? Date and time the infection was detected, the name of the infection and the original location where the infection was found (incl. file name) The malware category (i.e. Virus, Worm, etc) The computer on which the infection was found	20 20 20 20 20 20 20 20 20 20									* * * * * * * * * * * * * * * * * * *
In the deep at of the definition (by definition) Does the product protect itself against Zip of Death and similar attacks? On Demand Scans Can the administrator define when scans should take place and which Scan locations should be included / excluded? Can the system impact vs. scan speed be defined? On Access Scan Can the administrator define when a scan is triggered? Can the administrator specify which Scan Locations (incl. Files / Directories) should be included / excluded? Log Which information is logged? Date and time the infection was detected, the name of the infection and the original location where the infection was found (incl. file name) The malware category (i.e. Virus, Worm, etc) The computer on which the infection was found The user who was logged on at the time the infection was detected	20 20 20 20 20 20 20 20 20 20			2 0 0 0 0 0 0 0 0 0 0 0 0 0						* * * * * * * * * * * * * * * * * * *
In the deep at of the infection was found in the infection was found in the infection was found in the infection was found was lettered.										
In the deep at of the infected field (by default) Does the product protect itself against Zip of Death and similar attacks? On Demand Scans Can the administrator define when scans should take place and which Scan locations should be included / excluded? Can the system impact vs. scan speed be defined? On Access Scan Can the administrator define when a scan is triggered? Can the administrator define when a scan is triggered? Can the administrator specify which Scan Locations (incl. Files / Directories) should be included / excluded? Log Which information is logged? Date and time the infection was detected, the name of the infection and the original location where the infection was found (incl. file name) The malware category (i.e. Virus, Worm, etc) The computer on which the infection was found The user who was logged on at the time the infection was detected The action and current status of the infection (i.e. cleaned, deleted, quarantined, still infected)										
In the deep at of the infection was found in the infection was found inc. file name) The malware category (i.e. Virus, Worm, etc) The computer on which the infection was found the infection was detected The user was logged on at the time the infection was detected The action of the infection file infection the infection was logged on at the time the infection was detected The action of the infection file infection The user who was logged on at the time the infection was detected The action of the infection file infection The computer on which the infection infection The user who was logged on at the time the infection the action and current status of the infection (i.e. cleaned, deleted, auarantined, still infected) The current location of the infected file (i.e. local quarantine)										
In the deep at of the infection (i.e. of the article) of the infection was found (incl. file name) The and the original logged? Description and the original logged? Description and the original location was found the infection was found (incl. file article) The administrator specify which Scan Locations (incl. Files / Directories) should be included / excluded? Can the administrator specify which Scan Locations (incl. Files / Directories) should be included / excluded? Log Which information is logged? Date and time the infection was detected, the name of the infection and the original location where the infection was found (incl. file name) The malware category (i.e. Virus, Worm, etc) The computer on which the infection was found The user who was logged on at the time the infection was detected The action and current status of the infection (i.e. cleaned, deleted, quarantined, still infected) The carrent location of the infection (i.e. on Access, Manual, Start-up, etc)				2 0 0 0 0 0 0 0 0 0 0 0 0 0						
Internet of the infection of the infection was found infected file name infection was found infected file (i.e. local quarantine). The action and current status of the infection (i.e. cleaned, deleted, quarantined, still infected) The carnet hat detected the infection (i.e. on Access, Manual, Start-up, etc).										

Notify the end-user										
By displaying a pop up or balloon	0	e	•	0	•	ė	•	0	•	ė
Silen mode	ė	ė	ė		ė	ė	ė	ė	ė	
By adding a warning to an infected email body or					-	*				
subject (email) and by replacing an infected	•	•	•	•	•	•	•	•	•	
attachment					-					
Run a script or application after detection	•		٠				•		•	
Can a second or alternative action be defined (i.e. if		_	_	_						
the first action fails)?	•	•	٠	•	•		•	•	•	
Which file specific actions can the product perform?										
Clean / Delete	0	0	•	0	•	0	•	0	•	•
Can the product create a backup of the file before						_		_	_	
attempting to clean it?			*						÷	
Quarantine on the local system	•	0	•	•	<b>*</b>		•		•	•
Quarantine in a central location			•	•	<b>*</b>		•		•	
Deny Access	•	0	•	•	<b>÷</b>		•	•	•	•
Which processes specific actions can the product										
perform										
Terminate the process	•	0	٠	0	¢		0	0	•	•
Stop the service		•	٠		¢			0	•	•
Door to product provide proceeding and conditions?										
Does to product provide preconfigured conditions?										
Preconfigured Antivirus Check		0	٠			0	0	0	•	•
Preconfigured Firewall Check		•	٠				•	0	•	•
Preconfigured Patch Management Check			٠	•			•	0	•	
Other			Operating system patching				Databaca undata		Operating system patching	
other			status check				Database update		status check	
Remediation										
Door the product provide remediation conshilts										
Does the product provide remediation capabilities?		•	*	•	Ŧ	*	•	•	•	*
Which remediation action can be defined in the user										
interface (without resorting to scripts)?										
Registry remediation				\$			\$		•	•
File remediation										
Delete files / folders		¢	0			•	•	•	\$	\$
Download files							\$	•	\$	\$
Process remediation										
Run service / application in user / system security										•
context										
Software Remediation										
Download software and patches			0	•	•		•		•	•
Install / uninstall software and patches in user /				0			•	0	•	•
system security context				*	•		•			*
End-user interaction										
Inform user		0	0	•	•	•	•	•	•	0
Query user			•	0	•		•	•	*	
Enforcement										
Can the product prevent that a client failing the client										
health check connects to a network?										
Behaviour detection										
Behavior detection	•	0	0	•	•	•	•	•	•	0
Is this technology enabled by default?	•		٥	0		0	•	0	•	¢
General capabilities										
Is the firewall stateful for TCP and LIDP connections?		•								
is the mewall stateful for TCP and ODP connections?	*	¥	*	*	*				*	*
Can the firewall analyze VPN traffic	•	•	•				•	0	•	•
Firewall Rules										
Does the product come with default policies?										
For workstations	•	0	•	•	0		•	•	•	•
For server		0		•	0		•		•	•
Protocol										
TCP/UDP/ICMP	•	•	•	•	0		\$	•	•	•
Raw Ethernet		•	•						•	•
Other		Any other IP protocol is	IPv6-ICMP, IGMP, GRE,		IGMP GGP CUP IDP CPF					Processes and activity
		supported.	ESP, SMP		IGINIP, GGP, GOP, IDP, GRE					Frocesses and activity
Which Actions can be taken when a firewall rule is										
triggered?										

Allow / Block traffic / Ask / notify the end-user when traffic is blocked	8	\$	0	0	0		•		•	0
Log										
Log the incident	\$	\$	\$	\$	0		•	•	•	•
Include packet data in log	•		0	¢					•	
End-user Interaction				r					T	r
Can end-users be allowed to create firewall rules?			•	•	0		•	•	•	•
Can the administrator define rules that can not be	•	•	•	•	•		•	•	•	•
overridden by end-user rules?										
can the administrator define rules that can be overridden by end-user rules?			•	•			•	•	•	
Can the end-user be allowed to disable the firewall?			•	•	0		8	•	•	•
Can the firewall automatically be enabled after a defined time?			•				•		•	
Can the end-user easily block all network traffic?			•	٠					•	
Can the end-user be allowed to see the network traffic in real time?	•		•		٠		e	•	•	
Can the firewall rules be exported and imported?			•		•		•	•	•	
Firewall Logs										
Which logs are provided?		Log verbosity level can be set (Off, Low, Medium, High)	Critical warnings, Errors, Warnings, Informative records and/or Diagstic records. For troubleshooting, all blocked connections can be logged.	Alert log, packet log, HIPS log, full product log			Network attacks, Banned hosts, Application activity, Packet filtering	user defined	Traffic Logs, Packet Logs, Control Logs, Security Logs, System Logs, Tamper Protection Logs, Threat Logs, Scan Log, Risk Log	Outbound firewall logs
Client Management									•	
Client User Interface										
Can the administrator limit or control configuration changes by the end-user?	•	•	٠	•	0	\$	¢	•	•	•
Can different policies be applied for different	•	•	•	•	٠	•	÷	e	•	•
Depending on the location of the device (i.e. Office,	•		•		•		•	•	•	
Depending on group membership of the computer	•	•	•		0	•	•		•	
Depending on group membership of the user (i.e.				•	•	•	ė	•	•	
administrator vs. normal user) Actions										
Which actions can be initiated in administration console?										
Update signatures	•	•	•	÷	\$		•		•	
Reboot computer		¢	0				¢		¢	•
Scan computer	•	•	0	¢	•	4	•	<b>\$</b>	•	\$
Enable/Disable On-Access Scan		•	0	0	0	4	•	0	•	0
Enable/Disable Firewall	•	•	0	•	0		•	0	•	•
Other		Change all available product options	Change all aspects of configuration, including handing off a client to another server	Enable/disable all product features, reset statistics, configuration changes, quarantine management, software installation and upgrades	Central administration, configuration, monitoring, etc. of all available product features	Notifications on the enduser can be enabled/disabled	Vulnerability Scan, Application, Device and Web Controls			Over 32 remote commands are possible via the cloud-based management console
On which systems can the actions be initiated?										
A single computer / a group of computers	•	•	0	0	\$	•	•	•	•	•
All computers matching certain criteria (i.e. identified by logs or reports)			•		0		•	•	•	•
Other		On organization/network level		Scan for AV updates	According to the nature of the specific action and according to the administrator needs		Any set of computers or according to the administration groups hierarchy		Selected groups of clients	Selected groups of users/computers
Can the status of the actions be tracked?	•	•	0	•	÷	•	÷	•	ė	•

Is there a web based console?		é	•				ė		é	0
Administrator Management		<u> </u>					<u> </u>		<u> </u>	
Pights / Access Control										
Does the product support multiple administrators and										1
different essess levels?	•	•	•	•	•		٠	•	•	•
Authentication mechanism										
Can administrators be authenticated using an										
integrated authentication mechanism (i.e. username /				•	•		•	•	•	
integrated authentication mechanism (i.e. username /	-	-	-	-	-	-	-	-	-	-
password)?										
boes the product enforce minimum password lengths		٠	•	•	•		٠	•	٠	•
and maximum password age?										
Can administrators be authenticated using Active			•		•		•	•	•	
Directory?										
Account Security			1							
Does the product log an administrator out after being	•	•	•		•		•	•	•	•
idle for some time?										
Administrator Auditing			-						-	-
Does the product keep an audit log?		<del>\$</del>	8	ę		÷	<b>\$</b>		0	<del>.</del>
Device Control										
Does the product allow administrators to limit the use										
of external devices (USB sticks, printers, etc)?			*		•		•	•	•	•
Failover										
What if the AV Server (local) hangs up										
tinat in the fit beiter (lotal) hango ap										
automatic switching to a second local server		•	•		\$		•	•	•	
undates from vendor-server instead of local server										
upuates from venuor server instead of local server	-	-	-	<b></b>	*	-	-	+	-	
						service is automatically	any other network shared		Undates from another	All servers are cloud based
other			Log and notifications	Proxy pool and chaining		scivice is duconductedly	folder		oputies from another	and fully redundant /
						restarted	Tolder		client (peer)	worldwide
Quarantine										
Quarantine Folder										
Is there a centralized quarantine-folder			\$	\$	*		\$		\$	
Is there a guarantine-folder on the client	•		•		<b>\$</b>		<b>\$</b>		<b>\$</b>	•
can administrators specify the location of the	-								-	
guarantine folder anywhere									•	
rechecking quarantine										
after an signature update, is the guarantine folder		_			_	_	_	_	_	
checked?		*					•		•	
automatically		ė				e	ė	•	ė	•
manual	e	ė					•		•	
undo av-action if false positive is detected						ė	ė		0	
Messaging		<u> </u>								
Fychange										
Feature overview Messaging										
			Draduct for Evolution of Full	Transport and storage AV					Integrated option with MC	
			Product for Exchange. Full	Transport and storage AV					Integrated option with MS	
			integration with MS	scanning, Spam Control,					Exchange and Domino.	
		Monitoring, SMTP Groups,	Exchange, scans the whole	attachment filtering,					Secure email gateway	
		Antivirus, Antispam,	Exchange store and	intelligent file type	Transport and storage AV				option (virtual or physical	
Modules and functional areas		Content filtering,	Antispam Protection.	recognition, keyword-	Scanning and extendable by a		Anti-malware, anti-spam		appliance) for Enterprise	
		Attachment filtering.	Managable from the	based content filtering.	MailSecurity Gateway				Edition. Antispam,	
		Undate	central management	zero-day protection					antivirus antiphishing	
		opuate	convor Supports 64 bit	controlized quaranting					content filtering and date	
			server. supports 64-bit	centralized quarantine					content intering, and data	
			Exchange.	management					loss prevention	
Malware detection										
Recursive scan of all e-mails and file attachments in										
			•	•	•		٠		٠	
real time, event-and time-controlled	•	-								
real time, event-and time-controlled										
real time, event-and time-controlled	•		0	*	\$		•	0	\$	
real time, event-and time-controlled Information Store scan on every server Support of automatic virus pattern updates	0 0	0	0 0	0	0		0 0	0 0	0	
real time, event-and time-controlled Information Store scan on every server Support of automatic virus pattern updates Scanning of e-mail message text and attachments	0 0 0	0 0	0 0	•	0 0		0 0	0	0 0	
real time, event-and time-controlled Information Store scan on every server Support of automatic virus pattern updates Scanning of e-mail message text and attachments	0 0 0	0 0 0	•	0 0 0	0 0 0		0 0 0	0 0 0	0 0 0	
real time, event-and time-controlled Information Store scan on every server Support of automatic virus pattern updates Scanning of e-mail message text and attachments Definition of file limitations by a combination of file	0 0 0	0 0 0	• • •	0 0 0	0 0 0		0 0 0	0 0 0	0 0 0	
real time, event-and time-controlled Information Store scan on every server Support of automatic virus pattern updates Scanning of e-mail message text and attachments Definition of file limitations by a combination of file name, file extension and file size	0 0 0	0 0 0 0	0 0 0	¢ ¢	0 0 0		0 0 0	0 0 0	0 0 0	
real time, event-and time-controlled Information Store scan on every server Support of automatic virus pattern updates Scanning of e-mail message text and attachments Definition of file limitations by a combination of file name, file extension and file size Application of the restrictions on file archives	© © © © ©	0 0 0 0	© © © ©	* * *	• • • •		0 0 0 0	0 0 0	© © © ©	

Scanning of existing mailboxes	•	0	•	0	\$	8	0	•	ē.	
Anti-Spam										
scan according to the company's policies on										
prohibited, not desirable or confidential content	•	•	•	•				•	•	
Blocking unwanted e-mail senders (spam senders,										
mailing lists, etc.) as well as to unwanted recipients	•	•	•	•			•	•	•	
Analysis of images on undesirable content (e.g.		•	•	•			•			
pornography)										
Using current spam pattern for the fast detection of new snammer tricks	•	•	•	•			•	•	•	
User-Specific Management of White- and blacklists on										
the server solely for effective blocking unwanted e-	•	٠	•				•	÷	e	
mails Definition of transmitter / receiver channels on a										
dedicated e-mail communications			*							
Freely editable exclusion list for addresses and content	•		•				•		۵	
in subject and message text Elexible notifications of blocked e-mails (directly or	-		-							
schedule) to administration or transmitter/receiver	•	•	•	•			•	•	•	
email	-	-	-	-			-	-	-	
User-specific access to e-mails in the quarantine	•		•					¢	•	
Centralized quarantine management	0	0	0	0	•		0		0	
Formation of company-specific e-mail categories	e		e						•	
Automatic classification of e-mails to one or more	•	•	•						•	
Categories Response Management through defined										
classifications for example the customer support										
automatic forwarding of e-mails to gualified	•	٠	•						٠	
employees										
Document protection: Following categories may, for										
example, all outgoing e-mails on company-related								•	٠	
content should be examined										
A content audit of e-mail attachments is also possible			•					•	•	
if the same mail is delivered several times, would it be		•	•							
blocked as spam										
Feature overview inessaging									Integrated option with MC	
									Euchange and Domine	
									Exchange and Domino.	
			Integration with most		Colores and the Early and				Secure email gateway	
			Windows mail servers is		Gateway solution, Exchange				option (virtual or physical	
Modules and functional areas			possible through the		Plugin for Exchange 2007/2010				appliance) for Enterprise	
			command line scanner		or combination of both				Edition. Antispam,	
									antivirus, antiphishing,	
									content filtering, and data	
									loss prevention	
Malware detection										
Recursive scan of all e-mails and file attachments in	•		•	•	•	•	•		•	
real time, event-and time-controlled	•		•	•		•	•		-	
Information Store scan on every server	0		0	0	*			•	•	
Support of automatic virus pattern updates	•		•	•	•	•	0	0	0	
Scanning of e-mail message text and attachments	e		e	•	•	•	•	•	•	
Definition of file limitations by a combination of file	•		•	0			•		•	
name, file extension and file size										
Application of the restrictions on file archives such as zip. rar	•		•	•	•	•	٠		•	
Automatic detection of new mailboxes	0		0	0	•	0		0	0	
Examination of encrypted e-mails for viruses in										
combination with Crypt					4					
Scanning of existing mailboxes	0		0	0	•	0		0	¢	
Feature overview Messaging										

									Integrated option with MS	
			Special product for Linux				Constal and double of the		Fuch as a stand Denvise	
			Mail Servers and				Special product for Linux		Exchange and Domino.	
			Gateways Includes				MTA (postfix, sendmail,		Secure email gateway	
			Gateways. Includes				exim, gmail, CGP). Includes		option (virtual or physical	
Modules and functional areas			Antispam, web		Windows-based Gateway		Antivirus Antisnam and		appliance) for Enterprise	
			administration interface.		Solution		attachment filtering		Edition Antioners	
			Managable from the				attachment mitering		Euluon. Anuspain,	
			central management				modules. Managable		antivirus, antiphishing,	
			concolo				interfaces - Web and CLI.		content filtering, and data	
			console.						loss prevention	
Malware detection for messaging										
Anti-Spam										
Language:										
In which languages are your corporate products available?	German, English	English, French, Spanish, German	Management Server and Console: German, English, Spanish, French, Italian, Polish, Portuguese, Chinese, Japanese, Russian, Korean. Client: English, Slovak, Czech, Polish, Russian, Hungarian, Spanish, German, Portuguese, Dutch, French, Romanian, Turkish, Bulgarian, Swedish, Danish, Finnish, Norwegian, Chinese, Slovenian, Ukrainian, Croatian, Italian, Estonian, Korean, Thai, Kazakh, Serbian, Japanese, Lithungian	Chinese, Czech, Danish, Dutch, English, Estonian, Finnish, French, German, Greek, Hungarian, Italian, Japanese, Norwegian, Polish, Portuguese, Romanian, Russian, Slovenian, Spanish, Swedish, Turkish	German, English, Italian, Spanish, French, Russian, Polish, Turkish, Portuguese, Chinese, Japanese	German, English, French, Spanish, Italian, Chinese	English, Chinese, French, Italian, German, Japanese, Russian, Portuguese, Spanish, Turkish, Polish, Arabic, Korean, Vietnamese	English, French, German, Italian, Japanese, Spanish, Chinese	English, Chinese, Korean, French, Italian, German, Spanish, Portuguese, Russian, Czech, Polish, Japanese	Chinese, Dutch, English, French, German, Italian, Japanese, Korean, Portuguese, Russian, Spanish, Turkish
			Littiudilidii.							
In which languages are your (help) manuals available?			All		German, English, Italian, Spanish, French, Polish	German, English, Italian				English
In which languages are your (help) manuals available? Support			All		German, English, Italian, Spanish, French, Polish	German, English, Italian				English
In which languages are your (help) manuals available? Support 24/7/365 phone support		•	All	•	German, English, Italian, Spanish, French, Polish	German, English, Italian	•	•	•	English
In which languages are your (help) manuals available? Support 24/7/365 phone support Supported Support Languages	German, English	English, French, Spanish, German	All	English, Danish, Finnish, French, German, Cantonese, English, Japanese, Norwegian, Swedish	German, English, Italian, Spanish, French, Polish German, English, Italian, Spanish, French	German, English, Italian	All	English, French, German, Spanish, Italian, Japanese, Chinese	English, French, German, Italian, Spanish, Portuguese, Czech, Polish, Russian, Chinese, Korean, Japanese, Taiwanese	English All
In which languages are your (help) manuals available? Support 24/7/365 phone support Supported Support Languages Remote Desktop Control for support	German, English	English, French, Spanish, German	All	English, Danish, Finnish, French, German, Cantonese, English, Japanese, Norwegian, Swedish	German, English, Italian, Spanish, French, Polish Total German, English, Italian, Spanish, French	German, English, Italian German, English	All	English, French, German, Spanish, Italian, Japanese, Chinese	English, French, German, Italian, Spanish, Portuguese, Czech, Polish, Russian, Chinese, Korean, Japanese, Taiwanese	English All
In which languages are your (help) manuals available? Support 24/7/365 phone support Supported Support Languages Remote Desktop Control for support Support per Forum	German, English	English, French, Spanish, German	All	English, Danish, Finnish, French, German, Cantonese, English, Japanese, Norwegian, Swedish	German, English, Italian, Spanish, French, Polish German, English, Italian, Spanish, French	German, English, Italian German, English	All	<ul> <li>English, French, German,</li> <li>Spanish, Italian, Japanese,</li> <li>Chinese</li> </ul>	<ul> <li>English, French, German, Italian, Spanish,</li> <li>Portuguese, Czech, Polish,</li> <li>Russian, Chinese, Korean,</li> <li>Japanese, Taiwanese</li> </ul>	English All
In which languages are your (help) manuals available? Support 24/7/365 phone support Supported Support Languages Remote Desktop Control for support Support per Forum Support over Email	German, English	English, French, Spanish, German	All	<ul> <li>English, Danish, Finnish, French, German, Cantonese, English, Japanese, Norwegian, Swedish</li> </ul>	German, English, Italian, Spanish, French, Polish German, English, Italian, Spanish, French	German, English, Italian German, English	All	English, French, German, Spanish, Italian, Japanese, Chinese	<ul> <li>English, French, German, Italian, Spanish,</li> <li>Portuguese, Czech, Polish,</li> <li>Russian, Chinese, Korean,</li> <li>Japanese, Taiwanese</li> <li>Taiwanese</li> </ul>	English All  Control of the second s
In which languages are your (help) manuals available? Support 24/7/365 phone support Supported Support Languages Remote Desktop Control for support Support per Forum Support over Email On-Site service?	German, English	English, French, Spanish, German	All	<ul> <li>English, Danish, Finnish,</li> <li>French, German,</li> <li>Cantonese, English,</li> <li>Japanese, Norwegian,</li> <li>Swedish</li> </ul>	German, English, Italian, Spanish, French, Polish German, English, Italian, Spanish, French	German, English, Italian German, English	All	English, French, German, Spanish, Italian, Japanese, Chinese	<ul> <li>English, French, German, Italian, Spanish,</li> <li>Portuguese, Czech, Polish,</li> <li>Russian, Chinese, Korean,</li> <li>Japanese, Taiwanese</li> <li>Image: Comparison of the second second</li></ul>	English All Control of the second sec
In which languages are your (help) manuals available? Support 24/7/365 phone support Supported Support Languages Remote Desktop Control for support Support per Forum Support over Email On-Site service? Service	German, English	English, French, Spanish, German	All	<ul> <li>English, Danish, Finnish, French, German, Cantonese, English, Japanese, Norwegian, Swedish</li> <li>Swedish</li> </ul>	German, English, Italian, Spanish, French, Polish © German, English, Italian, Spanish, French © ©	German, English, Italian German, English	All	English, French, German, Spanish, Italian, Japanese, Chinese	English, French, German, Italian, Spanish, Portuguese, Czech, Polish, Russian, Chinese, Korean, Japanese, Taiwanese	English All Control of the second sec
In which languages are your (help) manuals available? Support 24/7/365 phone support Supported Support Languages Remote Desktop Control for support Support per Forum Support over Email On-Site service? Service Managed by Vendor, this means, can the whole	German, English	English, French, Spanish, German	All	<ul> <li>English, Danish, Finnish, French, German, Cantonese, English, Japanese, Norwegian, Swedish</li> <li>Cantonese, Norwegian, Swedish</li> </ul>	German, English, Italian, Spanish, French, Polish German, English, Italian, Spanish, French C	German, English, Italian German, English	All C	<ul> <li>English, French, German,</li> <li>Spanish, Italian, Japanese,</li> <li>Chinese</li> </ul>	<ul> <li>English, French, German, Italian, Spanish,</li> <li>Portuguese, Czech, Polish,</li> <li>Russian, Chinese, Korean,</li> <li>Japanese, Taiwanese</li> <li>Taiwanese</li> </ul>	English All  Control of the second s
In which languages are your (help) manuals available? Support 24/7/365 phone support Supported Support Languages Remote Desktop Control for support Support per Forum Support over Email On-Site service? Service Managed by Vendor, this means, can the whole management process be done as a service by the	German, English	English, French, Spanish, German	All	English, Danish, Finnish, French, German, Cantonese, English, Japanese, Norwegian, Swedish	German, English, Italian, Spanish, French, Polish German, English, Italian, Spanish, French	German, English, Italian German, English	All ¢	English, French, German, Spanish, Italian, Japanese, Chinese	<ul> <li>English, French, German, Italian, Spanish,</li> <li>Portuguese, Czech, Polish,</li> <li>Russian, Chinese, Korean,</li> <li>Japanese, Taiwanese</li> <li>Image: Spanish of the set of</li></ul>	English All Control of the second sec
In which languages are your (help) manuals available? Support 24/7/365 phone support Supported Support Languages Remote Desktop Control for support Support per Forum Support over Email On-Site service? Service Managed by Vendor, this means, can the whole management process be done as a service by the wanader?	German, English	English, French, Spanish, German	All	English, Danish, Finnish, French, German, Cantonese, English, Japanese, Norwegian, Swedish	German, English, Italian, Spanish, French, Polish German, English, Italian, Spanish, French	German, English, Italian German, English	All C	English, French, German, Spanish, Italian, Japanese, Chinese	English, French, German, Italian, Spanish, Portuguese, Czech, Polish, Russian, Chinese, Korean, Japanese, Taiwanese	English All  Control of the second s
In which languages are your (help) manuals available? Support 24/7/365 phone support Supported Support Languages Remote Desktop Control for support Support per Forum Support over Email On-Site service? Service Managed by Vendor, this means, can the whole management process be done as a service by the vendor? Differed (assumered)	German, English	English, French, Spanish, German	All All	<ul> <li>English, Danish, Finnish, French, German, Cantonese, English, Japanese, Norwegian, Swedish</li> <li>•</li> <li>•</li> <li>•</li> </ul>	German, English, Italian, Spanish, French, Polish German, English, Italian, Spanish, French Comparish, French	German, English, Italian German, English e e	All C	English, French, German, Spanish, Italian, Japanese, Chinese	Carlos Construction Constructio	English All  Control of the second s
In which languages are your (help) manuals available? Support 24/7/365 phone support Supported Support Languages Remote Desktop Control for support Support per Forum Support over Email On-Site service? Service Managed by Vendor; this means, can the whole management process be done as a service by the vendor? Pricing (may vary)	German, English	English, French, Spanish, German Comparison Comparis	All	<ul> <li>Finnish, Finnish, French, German, Cantonese, English, Japanese, Norwegian, Swedish</li> <li>Swedish</li> </ul>	German, English, Italian, Spanish, French, Polish German, English, Italian, Spanish, French C	German, English, Italian German, English • •	All & *	English, French, German, Spanish, Italian, Japanese, Chinese	English, French, German, Italian, Spanish, Portuguese, Czech, Polish, Russian, Chinese, Korean, Japanese, Taiwanese     Contemportation of the second s	English All  Constraints Cons
In which languages are your (help) manuals available? Support 24/7/365 phone support Supported Support Languages Remote Desktop Control for support Support per Forum Support over Email On-Site service? Service Managed by Vendor, this means, can the whole management process be done as a service by the vendor? Pricing (may vary) Scenario A: 5 clients, server, outlook as mail client	German, English	English, French, Spanish, German	All All	<ul> <li>English, Danish, Finnish, French, German, Cantonese, English, Japanese, Norwegian, Swedish</li> <li>•</li> <li>•</li> <li>•</li> </ul>	German, English, Italian, Spanish, French, Polish German, English, Italian, Spanish, French C	German, English, Italian German, English German, English	All C	English, French, German, Spanish, Italian, Japanese, Chinese	<ul> <li>English, French, German, Italian, Spanish,</li> <li>Portuguese, Czech, Polish,</li> <li>Russian, Chinese, Korean,</li> <li>Japanese, Taiwanese</li> <li>Control</li> <li>Control</li></ul>	English All Construction Constr
In which languages are your (help) manuals available? Support 24/7/365 phone support Supported Support Languages Remote Desktop Control for support Support over Email On-Site service? Service Managed by Vendor, this means, can the whole management process be done as a service by the vendor? Pricing (may vary) Scenario A: 5 clients, server, outlook as mail client recommended product	German, English	English, French, Spanish, German Cloud Security for Endpoints by Bitdefender	All All All ESET Endpoint Antivirus		German, English, Italian, Spanish, French, Polish German, English, Italian, Spanish, French	German, English, Italian German, English German, English German, English IKARUS anti.virus	All All Kaspersky Small Office Security	English, French, German, Spanish, Italian, Japanese, Chinese Chinese Chinese Sophos Endpoint Protection - Business		English  English  All  All  Business - Enterprise Protection
In which languages are your (help) manuals available? Support 24/7/365 phone support Supported Support Languages Remote Desktop Control for support Support per Forum Support over Email On-Site service? Service Managed by Vendor, this means, can the whole management process be done as a service by the vendor? Pricing (may vary) Scenario A: 5 clients, server, outlook as mail client recommended product 1 year Euro	German, English	English, French, Spanish, German Cloud Security for Endpoints by Bitdefender 143	All All All ESET Endpoint Antivirus 150	English, Danish, Finnish, French, German, Cantonese, English, Japanese, Norwegian, Swedish	German, English, Italian, Spanish, French, Polish German, English, Italian, Spanish, French Comparish German, English, Italian, Spanish, French Comparish Co	German, English, Italian German, English German, English IKARUS anti.virus 34	All All Kaspersky Small Office Security 167	English, French, German, Spanish, Italian, Japanese, Chinese		English  English  All  All  Comparison  Business - Enterprise Protection 132
In which languages are your (help) manuals available? Support 24/7/365 phone support Supported Support Languages Remote Desktop Control for support Support per Forum Support over Email On-Site service? Service Managed by Vendor, this means, can the whole management process be done as a service by the vendor? Pricing (may vary) Scenario A: 5 clients, server, outlook as mail client recommended product 1 year Euro 3 years Euro	German, English	English, French, Spanish, German Cloud Security for Endpoints by Bitdefender 143 286	All All All ESET Endpoint Antivirus 150 316	English, Danish, Finnish, French, German, Cantonese, English, Japanese, Norwegian, Swedish	German, English, Italian, Spanish, French, Polish German, English, Italian, Spanish, French C C C C C C Data SmallBusiness Security 167 467	German, English, Italian German, English e e e IKARUS anti.virus 34 55	All All Kaspersky Small Office Security 167 435	English, French, German, Spanish, Italian, Japanese, Chinese Sophos Endpoint Protection - Business 214 428		English  English  All  All  Business - Enterprise Protection 132 318
In which languages are your (help) manuals available? Support 24/7/365 phone support Supported Support Languages Remote Desktop Control for support Support over Email On-Site service? Service Managed by Vendor, this means, can the whole management process be done as a service by the vendor? Pricing (may vary) Scenario A: 5 clients, server, outlook as mail client recommended product 1 year Euro 3 years Euro 1 year USD	German, English  German, English  Avira Small Business Security Suite  267 534 343	English, French, Spanish, German Cloud Security for Endpoints by Bitdefender 143 286 177	All All All All ESET Endpoint Antivirus		German, English, Italian, Spanish, French, Polish German, English, Italian, Spanish, French C C C C C C C C C C C C C C C C C C C	German, English, Italian German, English German, English IKARUS anti.virus IKARUS anti.virus 34 55 44	All All Kaspersky Small Office Security 167 435 223	English, French, German, Spanish, Italian, Japanese, Chinese		English  English  All  All  Business - Enterprise Protection  132  318  175
In which languages are your (help) manuals available? Support 24/7/365 phone support Supported Support Languages Remote Desktop Control for support Support over Email On-Site service? Service Service Managed by Vendor, this means, can the whole management process be done as a service by the vendor? Pricing (may vary) Scenario A: 5 clients, server, outlook as mail client recommended product 1 year Euro 3 years Euro 1 year USD 3 years USD	German, English	English, French, Spanish, German Cloud Security for Endpoints by Bitdefender 143 286 177 354	All All All ESET Endpoint Antivirus 150 316 201 422		German, English, Italian, Spanish, French, Polish German, English, Italian, Spanish, French C C C C C C C C C C C C C C C C C C C	German, English, Italian German, English German, English	All All Kaspersky Small Office Security 167 435 223 581			English  English  All  All  Business - Enterprise Protection  132  318  175  420

Scenario B SMB: 1 SBS 2003 Server, 25 Clients										
recommended product	Avira Small Business Security Suite	Cloud Security for Endpoints by Bitdefender	ESET Endpoint Antivirus + ESET File Security	F-Secure Business Suite	G Data EndpointProtection Business	IKARUS security.manager	Kaspersky Endpoint Security for Business SELECT	Sophos Endpoint Protection - Business	Symantec Endpoint Protection Small Business Edition	Webroot SecureAnywhere Business - Enterprise Protection
1 year plan EURO	1260	556	473	941	570	910	810	656	684	452
3 year plan EURO	2520	1113	993	2263	1499	1456	1822	1312	1245	1086
1 year plan USD	1619	702	631	941	570	1170	1081	731	738	598
3 year plan USD	3238	1404	1326	2263	1499	1871	2433	1487	1343	1435
Scenario C: 1 Fileserver, 1 Exchange server, 200 Clients									_	
recommended product	Avira Small Business Security Suite	Cloud Security for Endpoints by Bitdefender + Bitdefender Security for Exchange	ESET Endpoint Antivirus + ESET File Security + ESET Mail Security	F-Secure Business Suite	G Data EndpointProtection Enterprise plus PatchManagement	IKARUS security.manager	Kaspersky Total Security for Business	Sophos Endpoint Protection - Business	Symantec Protection Suite Enterprise Edition	Webroot SecureAnywhere Business - Enterprise Protection
1 year plan EURO	9067	7476	4815	4818	8632	5454	10225	3950	5292	3210
3 year plan EURO	18135	14951	10113	12044	24536	8726	23004	7900	10079	7704
1 year plan USD	13390	9514	6430	4818	8632	7009	13658	4500	4944	4242
3 year plan USD	26780	19027	13503	12044	24536	11214	30728	9000	9310	10181
Scenario D, 2 Fileserver, 1 Exchange server, 1000										
Clients										
recommended product	Avira Small Business Security Suite	Cloud Security for Endpoints by Bitdefender + Bitdefender Security for Exchange	ESET Endpoint Antivirus + ESET File Security + ESET Mail Security	F-Secure Business Suite	G Data EndpointProtection Enterprise plus PatchManagement	IKARUS security.manager	Kaspersky Total Security for Business	Sophos Endpoint Protection - Business	Symantec Protection Suite Enterprise Edition	Webroot SecureAnywhere Business - Enterprise Protection
1 year plan EURO	32011	29049	15821	15842	28960	19057	36914	18000	27075	12899
3 year plan EURO	64022	58097	33244	39600	81650	30491	83056	27000	61563	30958
1 year plan USD	47280	36387	21124	15842	28960	24492	49307	20250	20060	17051
3 year plan USD	94560	72774	44388	39600	81650	39187	110940	40500	44579	40923
Scenario E: 10 Fileserver, 10 Exchange server, 10000 Clients										
recommended product	Avira Small Business Security Suite	Cloud Security for Endpoints by Bitdefender + Bitdefender Security for Exchange	ESET Endpoint Antivirus + ESET File Security + ESET Mail Security	F-Secure Business Suite	G Data EndpointProtection Enterprise plus PatchManagement	IKARUS security.manager	Kaspersky Total Security for Business	Sophos Endpoint Protection - Business	Symantec Protection Suite Enterprise Edition	Webroot SecureAnywhere Business - Enterprise Protection
1 year plan EURO	320110	216214	116084	81682	289600	120240	267067	180000	220820	105210
3 year plan EURO	742440	432428	243176	204204	816500	192384	600800	270000	530030	252504
1 year plan USD	470750	269272	154995	81682	289600	154530	356729	202500	159960	150300
3 year plan USD	1000000	538544	324688	204204	816500	247251	802507	405000	388788	360720

# **Copyright and Disclaimer**

This publication is Copyright © 2013 by AV-Comparatives e.V. ®. Any use of the results, etc. in whole or in part, is ONLY permitted after the explicit written agreement of the management board of AV-Comparatives e.V., prior to any publication. AV-Comparatives e.V. and its testers cannot be held liable for any damage or loss, which might occur as result of, or in connection with, the use of the information provided in this paper. We take every possible care to ensure the correctness of the basic data, but a liability for the correctness of the test results cannot be taken by any representative of AV-Comparatives e.V. We do not give any guarantee of the correctness, completeness, or suitability for a specific purpose of any of the information/content provided at any given time. No one else involved in creating, producing or delivering test results shall be liable for any indirect, special or consequential damage, or loss of profits, arising out of, or related to, the use or inability to use, the services provided by the website, test documents or any related data. AV-Comparatives e.V. is a registered Austrian Non-Profit-Organization.

For more information about AV-Comparatives and the testing methodologies, please visit our website.

AV-Comparatives e.V. (October 2013)

