

AVIRA

Product Installation

Download

The layout of the manufacturer's website is simple and logical, and it is easy to find the product you're looking for. If you already have a key, you can download the setup files without further ado. Registration is necessary to get a test licence. 30 days is long enough to test the product thoroughly. The registration details are forwarded to a certified Avira partner. An improvement here is that the individual products of the suite no longer have to be downloaded separately, as there is now a Small Business Suite installer as a single item. This is very much better than the previous version. Another plus point is that the new Avira website provides a very well organized overview on the complete range of Avira business products (the SmallBusiness among them) which makes it very easy to compare the features of the different product offerings.

Installation

Avira has also worked hard on the installation process, and there is no longer any need to consult the SMB product handbook during basic setup. The installation starts by decompressing the setup files. Once the installation files have been unpacked into a temporary folder, we are greeted by the Welcome page of the installer. Next comes the obligatory licence agreement. The path to the installation folder can now be selected. We chose to install to the standard location. The first step is the local installation of the products belonging to the Suite, i.e. the Anti-Vir Workstation, the AntiVir Server and (optionally) AntiVir Exchange. The next step is to enter the credentials of a Windows user account with administrator privileges. The installer now has the information it needs to begin. After successful installation, the SmallBusiness Suite wizard starts. The future security environment database is populated with AntiVir Professional and the AntiVir Server, so that the program can be remotely installed to client PCs. The product now searches the network environment for computers that are not already managed. Computers are added to the managed network simply by marking the tick-box. There is also a feature which allows additional clients (not found automatically) to be manually added to the list of machines to be installed. The ability to name them individually is particularly useful. Next, we can choose a user account for adding the marked computers to the managed security environment. This is an ideal solution for larger networks where there is a system administrator who looks after security issues. The product then checks if the administrative account is valid for all marked computers and lists the result. If the check was negative for certain computers the account data can be corrected on the spot. Next the marked computers are added to the security environment. In an up-to-date Windows environment with Windows Server 2008 and Windows 7 clients it is not possible to carry out a remote installation without changing firewall settings. However, with centrally controlled means such as Group Policy, this shouldn't be too much of a hurdle. The installation then works very smoothly and especially quickly. Products to be installed are chosen from a list. Then choose the computer(s) that the product is to be installed on. The product is then installed on the marked computer(s). The completion status is also displayed very clearly. Once the whole installation process is finished we get a final summary listing the computers with their installed products that are now managed within the security environment. Once the configuration wizard is finished we can start the Security Management Center (SMC) and log on with the credentials used during the server installation. At first glance, not much has changed from previous versions, so experienced Avira users will feel at home. Thanks to the new installer, it is no longer necessary to register the licence at this stage, as it has already been done using the setup

wizard. Software packets have also been configured with the wizard. The integration of additional clients or additional products can now be carried out directly from the Security Management Center or by using the configuration wizard again which can be started directly from the Avira/Avira SmallBusiness Suite program group. Especially the configuration wizard makes the initial configuration of Avira SmallBusiness Suite child's play. It is very nice to see a manufacturer reacting to customer feedback, and Avira has really succeeded in making the management center much more user-friendly. The general features have not been significantly changed, and so anyone familiar with Avira will still find their way around the settings very easily. It is of course possible to create an individual structure for complex networks, so that different configurations can be applied as necessary.

For example, separate configurations could be assigned for local and remote computers. Remote Installation remains unchanged. Rightclicking a client machine, then "Installation | Avira SMC Agent" allows installation of the agent. Other software, such as the client antivirus program, can be installed in a similar way if it has not already been installed through the wizard. The authentication possibilities for a push installation were already exemplary in last year's version. During the installation, the hour glass symbol is displayed, until the SMC announces that client installation is complete. The function scope dialog box also remains unchanged.

On successful completion of the installation, the installed product can be seen under the individual client PC. The Update Manager is now completely integrated into the Security Management Center which means that it is now possible to have more than one update manager, e.g. you can assign one update manager to one specific security environment group to speed up the distribution of updates. In spite of these changes the update manager remains very user-friendly. The update settings are diverse, making the suite very suitable for complex networks. The Update Manager also provides very detailed scheduling options. The user interface is, as in the last version, exemplary, and configuration changes are largely made using convenient drop-down menus. The installation routine for the Exchange scanner remains unchanged, as do the management console for mail and spam protection.

Manufacturer's website

The website (www.avira.com) is designed in a suitably clear fashion. The home page gives an overview of current threats and warnings in the support/virus lab area. You can subscribe to various RSS feeds, in order to keep up to date with the latest events. There is also a "Virus Lab" area on the Support page where you can find out about viruses and other types of malware. Avira has consolidated the various products into appropriate suites, and the licence model is, in contrast to the current trend, very simple. The trial versions of the products run for 30 days without any reduction of functionality.

The installation process

This year, as previously, Avira's installation process stands out, due to its simplicity and intuitive nature. The manufacturer has evidently reacted to user feedback, and produced optimal solutions to the small problems that spoiled last year's product.

The installation wizard makes it unnecessary to consult the manual during installation. The user-friendly nature of the product means that it can be deployed quickly and easily, without having to learn how to use it, and the basic configuration is very simple.

Administrator Console

The Administrator Console is, due to its MMC compatibility, clearly laid out and easy to understand. It can be said that after the installation, only organisational work remains to be done. In particular, the opportunity to create one's own security structure is especially impressive. We very much liked the possibility to import inventory lists for large networks; this is very simple to do, and saves a great deal of configuration. If you use an Active Directory you can also import your AD directory directly into the security environment and synchronize it automatically. We have also noticed that the suite now offers a number of features that simplify its use in larger network environments. The remote installation of clients is particularly simple. You only need to configure the login account to be used for the installation, and choose a package to install. No other preparation is necessary.

Unfortunately, you do need to configure the Windows firewall on the client PCs in order to perform the remote installation. A note from the manufacturers to this effect, giving details of the relevant ports, would be helpful here. What is particularly helpful for your every day work with the system is that whenever you add a computer to the security environment you can define that it automatically gets an Avira security product installed. What is also worth mentioning is the active reporting on errors and other security relevant issues by so called filtering groups that show clients that in one way or another need the attention of the administrator. If you want to use your own SSL certificates you can generate, deploy and use those certificates with Avira's SmallBusiness Suite. There is a convenient solution for licence administration, which is easy to configure.

Deployment areas

The Avira suite is ideally suited to small and medium-sized business. There have also been notable improvements for complex networks and enterprise environments. It is possible to live without some other features that would be valuable in an enterprise environment, given the extreme ease of installation and configuration. In the SMB field, Avira remains a top player.

Antivirus Clients

The message pop-ups are pleasantly discreet. After installation has completed, the initial update must be started manually, unfortunately. The client software is otherwise clearly laid out and gives a good overview of the state of the system.

Summary

The Avira Small Business Suite is very easy to install and fulfils all essential requirements. The suite is ideal for small to medium networks, although improvements for larger networks have been implemented. The client software is light on system resources, and the remote installation runs very quickly and easily. Unfortunately, Avira is no exception to the general failure of security suites to provide real-time status information. The noticeable development and improvement of the product is particularly worthy of praise. Even if there are small imperfections in the product now, you can happily use it, as there is every chance that even these will be improved in the future.

BitDefender

Downloading the product

The website design is simple and logical. There is no difficulty finding the products you want, and they can all be downloaded in fully functioning versions. You have to register to get a test key for the software. This allows an adequate 30 days in which to test the product. With BitDefender trial registration you get an email message with download instructions and links, where you are pointed to videotutorials, too. Two possible installation methods are described in the documentation. The components can be installed individually with their own installers, or by the management console. The latter is significantly simpler, but the individual components method may be useful in special cases. In the business section of the website, there is an overview of the functionality provided by different versions of the suite. This is very simple and practical for the user.

Installation

We begin with the installation of the management server, which will then be used to install the other components. We then have to agree to the obligatory licence agreement. After this, we can choose the installation method. For the purposes of our test we chose the Custom Installation, in order to better evaluate the functions of the installer. The next step is to choose the scope of the installation.

The following point gives us an idea of the scalability of the security system. The Master/ Slave variant is ideally suited to large networks, or those with remote sites. The next step is decisive for the communication of the individual components. The ports used by the suite can be configured to suit your own network environment. Even the port used to provide updates can be selected.

Like many other management products, BitDefender Security Suite needs a database server running in the background. As there is no SQL server in our test network, we select the SQL Express option. We leave the database login credentials as the defaults. The additional software components for SQL Server Express are now shown. After the installation of SQL Server Express and its additional components comes the setup of the management server. After the installation, a summary report of the changes made is shown. The first task is to provide authentication credentials. The standard password has to be used here, which requires delving into the user manual, unfortunately. We confirm the password without change, and log in to the management console for the first time. We are initially greeted by a very simple, dashboard, which informs us of the next steps. After successful registration of the management console, we proceed to the next stage of initial configuration. We start the Network Builder in order to define networks. As soon as we start with the Network Builder, the simple handling of the suite is clearly demonstrated, and we can make rapid progress. In order to find the client computers more quickly, and get around any network security barriers, Network Builder enables us to use Active Directory to choose the clients. Now comes step 2 in the Network Builder wizard. After clicking on "Apply Changes", we immediately see the "Deployment Wizard", which allows us to configure various options for the installation. After selecting the desired options, we can begin with deployment. Configuration continues after successful installation of the clients. The next point on our dashboard is quickly dealt with. The standard password needs to be changed. The next job is to bring the clients we have just installed into a group, which we have called simply "Clients". This grouping function is, as in other security suites, the best way to create a security structure which can be modified to fit the individual requirements of the organisation's network. We remove our client from the "Ungrouped" PCs and add it to our new group. This example shows clearly the way the management console works. In MMC-compatible style, the console shows the available areas to be selected, and individual objects can be conveniently configured by means of a rightclick.

After using the “Paste Client(s)” command, we immediately see the client we have just installed appearing in our newly created group. Having completed this step, we have already finished the initial configuration. Now we can take a look at the rest of the management console. The “Policies” area gives us the opportunity to create various security policies, whereby a number of preconfigured plans are available. It is easy to create one policy for clients and another for the management server. This policy management structure is the best means of realising complex security environments in corporate networks. The various templates can be used to control the individual functions of the clients, so there are specific templates for the firewall, scan behaviour, and other client functions. The next point, the script manager, is well known in corporate circles, and is an essential component of every good security suite. As with policies, BitDefender provides a very good choice of pre-configured templates. This makes it very easy to configure the suite according to the requirements of your own network, without needing to consult the manual. The template-based user interface is also used in the “Report Center”. Again, it is an optimal method, and enables you to configure the system as you want in minimal time. The “Activity Log” is the logging centre of the suite, and very simple logs enable the administrator to maintain an overview of the system. The Spartan nature of the information recorded in the logs is ideal for quickly checking the main functions of the suite, but has the downside that it is only of limited use in troubleshooting procedures where detailed information is needed. All in all, the management console is a very successfully designed tool for the central administration of the suite. The Dashboard in particular gives an excellent overview of the remaining tasks, and little time is needed for the initial configuration.

Exchange 2007 Protection

In order to demonstrate the second means of installation, we also set up the Exchange Protection using the standalone installer. To begin with, the installer unpacks the installation files into a temporary folder, and then displays message on the first page of the setup wizard. As usual, we have to accept a licence agreement. As we have already installed the file server protection using the management console, we will deactivate this option in our installation. The next step is to choose the number of scanning processes. The installer informs us that up to 24 instances can be selected, but recommends 4 (the minimum number) for our own network. In the next step, you can decide whether to send reports to BitDefender. This option should be deselected for high-security environments. At the start of the process we chose to install the Exchange scanner, so now we are asked about the role of the Exchange Server. The installer now has enough information to begin the installation process. Installation of the Exchange Protection component using the standalone installer is thus complete.

The management console for the Exchange 2007 protection

The Exchange server protection is also configured using a simple, familiar console like the MMC. The monitoring section of the Exchange console is exemplary. A very clear overview of the mail system and processed emails is presented. You can display detailed information from the various different areas, and so easily track potential problems/threats. We were particularly pleased to see that BitDefender gives us the opportunity to create our own SMTP groups, a feature that we have very rarely seen elsewhere. The configuration options are diverse and comprehensive. Due to the really exemplary choice of configuration options, the Exchange protection module in the BitDefender suite is extremely flexible, and can be adapted perfectly to the needs of your own network.

Manufacturer's Website

The manufacturer's website (www.bitdefender.com) is designed in an appropriately clear and simple way, in accordance with current standards. Additionally, the site offers a security zone, where you can find out about viruses and other malicious programs. The management console has been very well designed.

The installation process

The installation procedure is very simple if the management server is used, and can easily be performed by any user without resorting to the handbook. However, we were also pleased that the standalone option is available, as this allows the product to be installed on smaller networks without any need to worry about the many detailed configuration options.

The administration console

The MMC (Microsoft Management Console) compatibility of the administration console makes it clear and easy to use. Here too it can be said that after the installation, only organisational tasks still need to be completed. The opportunities to customise a security structure for your own network are excellent. The available functions and configuration possibilities mean that the suite is intended primarily for up to 3500 endpoints. The remote installation of the clients is in itself extremely simple. Unfortunately it is necessary to configure the Windows Firewall on all client PCs, to allow the remote installation to work. The management console for the Exchange protection is extremely powerful but still very straightforward to use.

Deployment areas

The BitDefender suite is suitable for networks of all sizes, including complex environments.

Antivirus clients

The antivirus software for clients is efficient, very user friendly and easy to find your way around. Once installed, clients need virtually no configuration and do not present excessive pop-up warnings.

Summary

The entire suite impresses due to its simple installation routine and very convenient user interface. Regardless of the size and complexity of your network, the BitDefender suite offers you all the features you need. The Exchange server protection must be particularly praised, as it is possible to make very detailed configuration changes, without feeling overwhelmed by the possibilities. The user interface is so simple that a manual is more or less redundant. In conclusion, the suite can be recommended to everybody.

ESET

Installation

Downloading the product

It is easy to find the products you're looking for, as the website is clear and well designed. ESET is the only manufacturer amongst those in this review to limit the availability of the test version. It is only possible to download a trial of the corporate software after making contact with the company. Like

many other manufacturers, ESET makes a separate installer for every individual product or tool. The products can be bought online from the web store. There is all information and user guides about them on the site. ESET offers an online scanner as an additional service free of charge.

Installation of the products

We start with the installation of the Remote Administrator Server. Next we have to confirm acceptance of the licence agreement. After this, we can choose the installation method. The Advanced Installation gives the option of Cluster Mode.

The next step is to locate the licence key file. We now have the opportunity to enter passwords for the individual functions of the software. Using different passwords for different areas of access increases security, although some administrators would surely prefer to use one password for all functions. But, as mentioned before, it is more secure this way! The next point concerns the update settings. The installer now has enough information to begin the setup process.

The next step is to install the Remote Administrator Console. This can be installed on any PC on the network, and serves as the interface for the Remote Administrator Server, which we have already installed. This distinction is not

very clear to the new user without reading the manual. There is another licence agreement to accept. Again, there is a choice of "Typical" and "Advanced"

installation methods. We can then choose the installation folder. The installer has now collected enough information and can begin the setup process. On completion of the installation, we can open the console. In the case of a Typical Installation, the Microsoft Access Engine (Jet Database) is selected by default as the database. If you want to use an SQL server, this has to be configured manually with the help of the manual.

The management interface

By default, two clients can be managed using ESET Remote Administrator. If you import a test license obtained from ESET, you will be able to manage as many clients as the license permits. The console needs a good deal of getting used to, but offers the users a wide variety of options. Studying the manual is unavoidable. There is a help option within the product, quick start guide and user manual for full feature explanation. Our first task is to configure the security structure and the clients. To do this, we click on the "Group Manager" button on the taskbar and create the desired group(s). Aside from creating the security structure, dynamic groups can be created – clients become members of these groups based on meeting certain criteria defined at group creation. The Active Directory Import Wizard is very helpful here. To make the software packets ready for a push installation, we first have to create them, or download them from the manufacturer's website with the help of a wizard. If the relevant MSI files for client installation are already available on the network, these can naturally be used to form the installation packets. Now we can distribute ESET Smart Security (the client software) to the clients. The "Remote Installation" tab allows you to select the client machines to be installed. We choose the PCs we want and click on "Push Installation". We then need to enter the login details for these machines. The next stage is to choose the package to be installed. The installation can be carried out immediately, or scheduled for a later time. As with almost all other suites, there is no real-time status, but by clicking on "Task Details" in the context menu, and then "Refresh", the degree of progress can be seen. After a short wait we are informed that installation is complete. The push installation without interaction improves the user-friendliness of the software. As in our test last year, we found the filtering and organisational options very comprehensive and

good. With ERA 4, ESET has also added a centralized view of the quarantine on the clients; i.e. files that are in quarantine remain on the clients, but the administrator has a centralized view of what has been quarantined and can download the files from the clients for further inspection, delete them or restore them. The list view with tabs at the bottom of the window for the individual areas is a good solution. The variety of functions is strength of the suite. It offers very detailed configuration options, and can thus cope with complex demands. Aside from clients on Windows based systems, the console allows management and configuration of clients running product for Mac OS X, servers running ESET Mail/File/Gateway security solutions, or even mobile clients (ESET Mobile Security for Windows Mobile/ Symbian). In other words, it is possible to manage, configure and update all ESET security solutions from a single console.

Exchange 2007 protection

To start off with, the Exchange protection component has to be installed. Once again, there is a licence agreement to accept. There is also a choice of installation options. We have already entered all the information necessary for the installer to begin. Setup is now complete, and we can take a look at the configuration. The Exchange 2007 management interface Starting the management console also opens the Help window for the initial configuration. Mail Security advises a restart, which we carry out. The management interface is simply and appropriately designed. On the "Protection Status" page we see what needs to be done next.

The first step is to enter the licence key. Extended configuration options can be found by clicking on the "Setup" menu, then "Advanced Setup". If the standard options available are insufficient for you, you can use this advanced menu to find all available settings. The choice of a simple or an advanced interface is very convenient, and makes it easy for less experienced users to configure the Exchange protection. To enter the licence key, we click on "Miscellaneous" and then "License". As soon as we have entered a valid licence, we can see that the status indicators in the Mail Security window have all turned to green. Most users will be happy with the Standard view, although the Advanced view is useful for

anyone needing to set up very complex configurations. Anyone who knows their way around the ESET Smart Security Client will feel at home with the interface of Mail Security. Configuration can be carried out quickly and easily.

Manufacturer's website

The website, www.eset.com, is suitably clear and simple, and conforms to current standards. The site gives basic information about ESET products, and there is an online scanner available to download. ESET is one of very few manufacturers to limit the functionality of their test software. Additionally, it is only possible to obtain a test licence by contacting a member of their sales team. Some users may regard this as an unnecessary hurdle, although it does mean that users will be properly advised before installing the software.

The installation process

The installation is in itself very straightforward and simple. Hardly any information needs to be entered. Any necessary configuration changes can be made afterwards. We suggest that ESET should reconsider the Microsoft Jet Engine as the default database.

The administrator console

The management console is very extensive and offers sometimes an too abundant choice of configuration. Thorough consultation of the manual is indispensable or has to consult the in-product help. The icons are arranged so as to enable a good overview. The system is well designed and allows individual systems to be found and configured easily, even in extremely big network environments.

Deployment areas

“The ESET suite can scale for very large networks.”

Antivirus clients

There are no complaints about the client software, which is well designed and simple to use.

Summary

The management console takes a lot of time and effort to investigate and understand, but compensates for this with an abundance of configuration possibilities. The management console shows the status at a glance. The Exchange protection is very simple to configure and cannot be faulted. All in all, the product is a really well done software for enterprise environments.

G Data

Installation

Downloading the product

It is easy to find your way around the website, which is clear and simple. There is no difficulty finding the products you want, and all software can be downloaded as a fully functional version. Most modules come as an ISO file, weighing in at 1.3 GB. It's important to allow enough time to download this much. Fortunately, G Data's servers have high-speed connections. There is of course an overview of the functions contained in the different suites.

Product installation

We begin with the installation of the management server, which is then used to install the other products. We were very pleased to see that G Data, as one of very few manufacturers, produces one installer that will install the whole suite. The

installation of the management server also includes the AntiVirus Administrator, which will be used later to carry out the remote installation of the clients. We start at the beginning with the G Data AntiVirus Management Server. As usual, there's a licence agreement to accept. Next we choose the installation folder. Now we can decide on the type of server to be installed. Compatibility mode for earlier client

versions can also be selected here. You can see that G Data also allows you to install secondary and local servers, to enable easier distribution in large networks.

The next selection also allows for scalability of the security system. Settings can be stored in an integrated database, an existing SQL server instance, or SQL Express. The SQL Express option states that it is “required for large networks”, which gives inexperienced users a completely false impression. If you have a own SQL server, there is no need for the Express version, you can use your SQL server. As we don't have an SQL server in our test environment, we use the integrated database for our test. The next step is to confirm the hostname of the computer being installed, via which it can be accessed by client PCs. The installer now has all the information it needs to begin the

installation process. When installation has successfully completed, we have to decide whether to register. Services and servers are then installed and configured.

The management interface

When the administration console first starts, we are asked for logon credentials, and given a choice of integrated or Windows authentication. Once we have entered the correct logon details, the management console opens and the setup wizard starts. The next step is to select the computers in our network that we need to protect. It is of course possible to manually add any computers that don't appear in the list. The wizard then asks if we want to install the client protection automatically, which we confirm. The next part of setup is the opportunity to change the default settings for the client installation, which can be done very easily. It is of course possible to change these settings later. In this case we rely on G Data's default settings and don't make any changes. After this, we can change Internet update settings, to optimise virus updates for the clients. The default configuration is manual, but can easily be changed to one's own requirements. When the wizard has finished, we open the G Data Administrator, which shows a status overview. In the left-hand pane of the window we see a list of all the PCs in the network. You can easily right-click on a machine and activate the G Data client software. There is also the option of forming groups to make larger networks more manageable. Now we are ready to carry out the remote installation of the clients. To do this, we click on the "Clients" tab and select "Install G Data Client". We notice that G Data is a leader with regard to user interface design and intuitive use of the software. After the access credentials have been entered, we are asked if the G Data client firewall should also be installed. Unfortunately, there is no real-time progress display, and the messages provided by the status windows can only be described as Spartan. However, the client installation completes very quickly and easily, and in just a few moments the remote client is installed. All further work can be carried out using the G Data Administrator, be it generating reports with various criteria, or changing client settings. An obvious plus point is that there is a preconfigured button for each standard action, so there is no need to go searching through menus. It is very convenient to be able to install the AV client software on the server itself, using the Administrator. It is exactly the same as installing the software on a client.

Exchange 2007 protection

We start with the installation of Mail Security. Here again it is pleasing to see one installer for all the mail products. Installing G Data Mail Security also installs the Administrator, although the latter can also be installed separately. The setup wizard starts after the installation files have been unpacked. First we have to accept the licence agreement. The next step is to choose the installation folder. Of course, a database will be necessary for statistics and reports in the background. Once again, there is a choice of using an existing SQL Server instance, or installing SQL Express. The installer now has all the information it needs to begin. During the installation it will be automatically be recognised that the AV client is installed on the server, and the user is shown a message that its virus database will be used by MailSecurity. When the installation is complete, we can start the administration console and start configuring. The MailSecurity management interface after the installation, we start the administrator console.

Here too, a password has to be entered. As we have not yet set up a password for MailSecurity administration, we have to do this now. Once again it is clear here that G Data is at the forefront of simple user interface design. All essential information is shown on the first page of the intuitive interface. The warning indicators show the administrator immediately which areas need immediate attention. To make configuration changes, we click on "Options". The dialog box has tabs to show the different areas, starting by default with incoming security.

The Incoming tab allows groups etc. to be imported from Active Directory, which is a very useful feature. The tabs have been arranged so as to show all the important options on one page, without overwhelming the user with choices. Having configured the options, we then see from the overview page of the Administrator

window that the system is now well protected.. The "Filter" area allows us to use preconfigured filters, or create our own. We were also impressed with the various options for viewing the mail protection system, such as the queue, or processed mails. Any malware found is clearly displayed in the "Virus results" section. The last of the configuration options is found under "Spam Filter". This is structured in the same way as the Options dialog box, which we have already seen. Thus the whole configuration interface of the G Data suite is very much self-explanatory, and the user can immediately find all necessary functions. All the features one could want are present, and so MailSecurity contributes to our overall very positive impression of the suite.

Summary

Manufacturer's website

The G Data website (www.gdata.com) is well designed and easy to find your way around, being compatible with current standards. The site offers everything that you would expect from an antivirus manufacturer. There is information about current threats, and a virus encyclopaedia. The business section is appropriate to the needs of business users. G Data makes it clear on the website that the suite is aimed primarily at medium-sized businesses.

The installation process

As with the version we tested last year, the installation of the G Data suite is made very pleasant by the simple and intuitive user interface, which could be used even by inexperienced users without any need to consult the manual. The manufacturers have remained true to their philosophy of simple installation, making this one of the best products we have tested.

The administration console

The administration console is certainly one of the simplest we have ever reviewed.

After the installation, only administrative work remains to be done. The numerous functions and configuration possibilities mean that the suite is lacking nothing in terms of functionality. Remote installation of clients is very well handled and can be carried out very quickly. The MailSecurity Administrator is no exception, being very simple to use without lacking anything in the way of functions.

Deployment areas

Although the suite copes with all standard requirements, the manufacturers see it as being appropriate for medium-sized businesses. The simplicity of the administration means that some sorting functions, which would be valuable in larger networks, have to be forfeited.

Antivirus clients

The client software is very user friendly and easy to find your way around. There is effectively no configuration to be done, and warning pop-ups are infrequent. The default settings are ideal, as is the ability to prevent the local user from making configuration changes.

Summary

G Data has, like last year, succeeded in producing a suite that is very easy to use.

There is no lack of functionality, and G Data sets the standard for intuitive user interfaces.

Particularly the Exchange suite and the remote installation are exemplary. The manual is virtually redundant.

Kaspersky

Installation procedure

Downloading the product

All the products can be downloaded in fully functioning versions from the manufacturer's website. It is easy to find the products, and the website design is simple and clear. The trial versions of the software run for 30 days, which is adequate time to carry out comprehensive tests. It is necessary to register to

obtain a trial licence. Unfortunately, Kaspersky conforms to the general rule whereby there is no single installer for the whole suite. This does however give

you the opportunity to choose the individual products suitable for your own network. We note that Kaspersky also produce security software for Linux networks. There is a clear and simple diagram of the different products and their functions. By and large we had no complaints about the design of the website.

Product installation

We begin with the installation of the Administrator Kit. The first step is to choose the folder for the setup files. The installer then unpacks the setup files to this folder. The setup wizard then starts.

There is the usual licence agreement to accept. The next point allows us to choose between "Standard" and "Custom" installation. To get an idea of the options available, we select Custom. Now we have to choose the installation folder. The next step is to choose the features we want to install. We particularly liked the next step, which asks us to choose the expected size of the network. Unfortunately there is no information as to how

each of these options will be configured. In the next step we can choose the user account for administering the suite. There is a choice of using an existing account, or creating a new one. We then have to choose a database option from SQL Express or MySQL. The next point concerns the SQL parameters. We select SQL Express for our test. We now just need to choose the authentication method. Kaspersky uses a network share to distribute installation packets and updates. You can choose between using an existing share and creating a new one. An Administration Server port also needs to be defined. The method of name resolution for the server can also be set. The installer now has enough information to begin the setup process. It must be noted here that the installation must

be carried out using the main Administrator account; any other user account, even with administrator privileges, will not work. We feel that the wizard should notify the user of this at the start. Once the installation is complete, we can open the administration console.

The management interface

First use of the admin console conveniently starts a configuration wizard. The first step is to select a licence file. We choose a locally stored licence key. Next, the installer carries out a thorough scan of the network. By clicking on "View discovered computers" you can see the client PCs that have been discovered.

Next, we can configure the notifications for the mail server. We then see a summary of the completed tasks. The configuration wizard then downloads updates to the administration server. A great number of update files will be downloaded for the various systems, but there is no need to wait for the update process to finish, as it will run unattended in the background. Like last year, Kaspersky's configuration wizard is definitely one of the best we have tested, as finishing one wizard leads to the start of the next, so that no important tasks can be forgotten. Next we start the deployment wizard. Here we can select the installation packets that we want to distribute to the clients. Any installation packet not in the default list can be added manually. If the wizard has already been used before, there is a choice of installing software to new clients, or additional packets to existing clients. As this is the initial configuration, we have to select the client PCs to be installed. The next point is the selection of options for the client installation. We particularly liked the option for Active Directory integration. Now we have to select a licence for the client installations. Kaspersky provide an exemplary choice of actions to be carried out on client computers when a restart is necessary. The installer can be configured to remove any incompatible applications, such as other antivirus or firewall programs. The next step allows client computers to be assigned to administration groups. We then choose the Windows account to be used for the installation. The wizard now has enough information to begin the deployment process. The wizard then informs us that the deployment task has been created and started. It seems impossible, but Kaspersky is the first manufacturer to have created a real-time installation display that informs the user of the current state of client installations. The only thing to be criticised here is the speed with which the clients are installed. The console is designed in the accustomed clear and comprehensible manner. All the necessary functions are present and easy to find. This simplicity means that even inexperienced users can find their way around easily, without any need to consult the manual.

Exchange 2007 protection

We begin with the mail security setup. There is the usual licence agreement to accept. There is the choice of "Typical" or "Custom" installation. The installer points out that additional parameters can be configured in the next stages. Here we can choose whether to start protection immediately after setup completes.

We were pleased to note that the installer points out that some Microsoft services need to be restarted after the installation. The installer now has enough information to begin. The upcoming Kaspersky Security Suite for Microsoft Exchange has fewer steps. We will report in one of our next tests. The MMC-compatible management console for the Exchange protection is very clear. An initial screen allows us to define what servers we want to manage with that console. This can be useful for

some administrators, who by some reason do not want to use Administration Kit. If you switch to managed server you can see installed components and basic license overview. There is a limited range of options here, so it is an easy task to configure the available settings. These are notification, reaction in the event of an infection, backups and reports. Server protection menu have two tabs related to two main tasks the product is charged with – Anti-Virus and Anti-spam protection. Anti-SPAM protection tab allows us to define rules for spam processing. Updates management also allows setting up update source and frequency, again as a separate settings for Anti-spam and Anti-virus protection. Notification settings allow us to set up notification rules for main predefined event types. Reports management allows us to create and view reports on virus and spam detection. Settings tab used to set up some main system configuration like logging and backup storage capacity. And final License tab used for license management.

Summary

Manufacturer's website Kaspersky's website (www.kaspersky.com) conforms to normal Internet standards and is easy to find your way around. There is also a "security zone" where you can find out about viruses and other types of malware. There is a lot of information to be entered during the setup process. However, the cleverly designed setup wizards are a big help, and so even inexperienced users can carry out the installation quickly and easily. The configuration is also made easy by the wizards. The entire suite can be installed and configured in minimal time, without having to consult the manual.

The administration console

As with the product we tested last year, Kaspersky knows how to make life easy for the user, and so the entire configuration process is child's play. The MMC-compatible console, with its graphical presentation in the functions pane is particularly pleasing.

Deployment areas

Kaspersky is at home in networks of all sizes, and the Active Directory integration is a big help. It is only in very large networks that the product might be a little inconvenient.

Antivirus clients

The client software is, as usual for Kaspersky, very professionally produced, and hard to find fault with.

Summary

Kaspersky has, as it did last year, produced a very good corporate suite, which can be recommended to everyone without reservation. The setup wizards and administrator interface make working with the suite very easy. It is of particular note that Kaspersky is one of very few manufacturers to produce a real-time display of the status of client deployment. It is actually mystifying that other software companies don't follow Kaspersky's excellent example and allow the administrator to keep up with the installation status of the clients.

McAfee

Installation process

Downloading the products

The layout of the McAfee website is simple. It is, however, the least informative of all the manufacturer's websites in this review. You could be forgiven for thinking that it serves rather more as a storage area for developers' documents, and less as a source of information for customers. Even after searching the website for hours, it is still not clear to the corporate user which products to choose. Having eventually reached the download area for the trial versions, you are faced with a huge variety of products. There is a filter function, but the labelling of the filter options is just as mysterious as the naming of the products. Registration is necessary to obtain a trial key. This is valid for 30 days, which is sufficient time to test the selected product thoroughly. When we reviewed the beta release of McAfee's ePolicy Orchestrator management server we were pleased to see it bypasses this web site complexity. ePO provides a Software Manager screen that presents the user a list of available evaluation and licensed software for download directly into the management server.

Product installation

We begin the installation of the "Total Protection Suite for Endpoint". The first task is to confirm that additional software packets should be installed. We confirm this installation. We note that McAfee is one of very few manufacturers to demand a restart of the server after installing the C++ Redistributable Package. Now the installation proper can begin. Next we have the choice of entering a licence key, or using a test version. We accept the licence agreement. Following this, we can choose the scope of functionality to be installed. The next step is to enter the user credentials for the management console. Here we can select the installation folder. The access data for the database server is then entered. This is followed by the choice of ports for communication with the suite. The installer now has enough information to complete its task. When installation is complete, we start the "Orchestrator" to carry out the configuration.

The management interface

After starting the ePolicy Orchestrator, we are greeted by the login site of the web application. The first step is to authenticate yourself. The standard password has to be entered here, which can only be found by reading the handbook. We confirm without changing the password and log in to the management console for the first time. The management interface of the Orchestrator has a very pleasing graphic design. McAfee is entering new territory here by offering the user an interactive tour of the suite, in order to learn how to use it, and what the next steps will be. The first step is to create groups for network organisation, and assign client PCs to these. By clicking on System Tree we can begin creating our security structure. Having created two groups, for the server and clients respectively, we add the machines to these. This very extensive form allows the administrator fine control over the process of adding computers, and also enables pre-configuration of some important settings, thus saving a lot of work later. Having activated the Computer Browser service on the server and entered details of an administrator account, you can select the computers and add them into the security structure. We import our server with a click on OK. When the computer has been added into the group, there is a variety of actions which can be applied to it. The scope of the Orchestrator is very wide, and the well-designed web interface makes it very user-friendly. It is very easy to download the necessary software packets and store them in the Repository of the Orchestrator, from where they can be distributed with just a few clicks. To do this, we go to the Client Tasks area and select "New Task". The wizard that then starts has a wide variety of tasks which can be applied to our

selected computers. This type of configuration is found throughout the interface and is very easy to get used to. The individual areas are clear and easy to understand, and laid out in a well-structured manner. The Interactive Learning Tour is intended to make using the suite easier for less experienced users. However, it must be said that the suite is designed more for very large and complicated networks, which of course requires more in the way of knowledge and experience from the user. The query area is ideally prepared for analysis of the log files, and offers a huge variety of pre-configured queries, which provide a convenient means of finding out all important information about the system. It is also very practical that the Exchange protection has been installed at the same time, and everything can be controlled using the Orchestrator. McAfee has definitely created one of the best all-in-one management consoles here.

Summary

Manufacturer's website

The McAfee website (www.mcafee.com) conforms to normal Internet design standards. Unfortunately, it is very easy to get lost on the website, due to the confusing mass of different products. For a corporate user, it is practically impossible to find clear information about the available suites. You are simply overwhelmed with information and cannot get any sort of overview. This should be improved by McAfee as soon as possible, either by simplifying their product line or finding a way of presenting their products more clearly.

The installation process

When you have eventually managed to find the right suite, you can look forward to a very easy installation. The fact that the management console, Exchange protection and intrusion prevention system are installed together by one setup program saves a great deal of time and effort. Other manufacturers should see this as an example and follow suit. Too many "suites" come in the form of separate products with separate installers.

The administrator console

The ePolicy Orchestrator is currently one of the best and most powerful management consoles on the market. After just a short familiarisation period, the user can carry out the most complex tasks easily. The enormous functionality and organizational opportunities mean that the Orchestrator is very suitable for large and complex networks.

Antivirus clients

The client software is very user-friendly and easy to find your way around, with no obvious flaws.

Summary

After the initial confusion on the website, you will be very pleasantly surprised by the suite. Installation is very simple. The management console provides trend-setting solutions in several areas, and the degree of functionality is impressive.

Whether you need to protect a small network or a huge domain, the McAfee suite will be ideally suited for all requirements.

Sophos

Installation

Downloading the product

The website impresses with its pleasant design. It is simple, clear and fast. Registration is necessary to obtain a free trial key. This gives an adequate 30 days to test the software. The inexperienced user should take some time to understand NAC; he or she may otherwise waste time trying to find the additional module, which may not be necessary. By the time you come to download the product, it should be clear which component does what.

Product installation

The first task is to unpack the installation files to the local hard drive. We are then greeted by the install wizard. Next, the setup programs checks that its requirements are met. In this case we have to update to the newest Windows Installer (it is worth checking before installation that this is up to date). Having done this, we can proceed with the installation, and accept the licence agreement. Next we can choose the installation folder. Sophos gives us the option of a "Complete" or "Custom" installation. We choose the "Complete" option. As in last year's test, we can only applaud Sophos' optimal Active Directory support. The next step allows us to choose an AD group which will be given administrator access to the suite. Sophos offers a service that sends information on installation and operation of the system to them, in order to improve support. Again, we advise careful consideration as to whether to use this service in high-security environments. The installer has now gathered sufficient information to proceed. With the Complete installation, SQL Server Express is installed. When installation has finished, the installer informs us that the current user must log out of Windows to complete the installation. Immediately after the user has logged on again, the Sophos wizard appears and connects to the newly installed management server. When the management console has started, the configuration is checked.

The management interface

Sophos is one of very few manufacturers to have their own management console design. This is very well thought out and structured. We particularly like the dashboard with its overview of the state of all important security aspects. The experienced user will see the immediate tasks at a glance.

1. Create network organisation groups and add computers to these
2. Configure updates
3. Remote installation of the client software
4. Changes to the central configuration

The most important commands can be found as buttons with appropriate icons on the menu bar. The second section is the configuration area, where the organisational structures are created and configuration is assigned according to policies. This layout is simple and convenient. Our first task is to start the download wizard which will obtain the additional software needed to protect the clients. Now we have to enter the username and password for the Sophos download account. In the event that the system connects to the Internet via a proxy server, this information can be added in the same dialog box. The next page of the wizard allows client software for different operating systems, including Mac and Linux, to be selected. The necessary files are now downloaded to the hard drive. It is not necessary to wait until the download has completed; you can click on Next to go on to the next page. However, Sophos unfortunately leaves you in the dark as to how fast the download is progressing and when it will finish. The next stage allows you to use AD to import computers into organisational groups. At the end of the wizard, there is the opportunity to view a tutorial on the

next stages of the configuration process. As we unfortunately don't know how long we will have to wait before we can start deploying the software to the clients, investigate how easy it is to manually create new security groups. The wizard above appears after we click on "Find New Computers". Again we see that Sophos has the best Active Directory support of any of the products we have tested here. Even importing complex AD forests is child's play. Of course, it's also possible to add computers that are not part of AD. For our test, we select "Import from Active Directory". In the Sophos management console we create a new group called Clients, and use it to import our Client group from AD. Next we look for the AD container with our client PC in. The container structure can be imported here as well, making it the quickest and most convenient method of importing groups. A summary is displayed, and then the import process can proceed. The results of the import wizard are displayed at the end. At this point we still do not know how far the downloader has progressed with obtaining the client software; we can do little except wait. It is hard to understand why an otherwise highly professional suite gives no information at all as to the status of the download. Once we have ascertained that the client software is available, we can proceed with the installation of the client PCs. To do this, we right-click on the computer we have just imported and select "Protect Computers". The Protect Computers wizard starts. Next we can select the features to be installed on the client. Our client is immediately recognised, and the deployment can proceed. We now enter the credentials of a Windows account with the necessary privileges to carry out the installation. When installation has finished, we can immediately see that the policies are being pushed out to the client, thus assigning it the configuration settings. The entire suite follows this principle. Functions are configured using policies, which are distributed to the relevant PCs. The descriptions of the different policies are self-explanatory, and the default settings appropriate. The clear ordering, with pre-defined filters, makes administering even large networks very straightforward. The Report Manager, for example, hardly requires any changes to be made to the standard report.

Exchange 2007 protection

Again, we start by unpacking the installation files onto the local hard disk. We accept the licence agreement. Here we can select the features to be installed.

Next we define the installation folder. Here we have to supply Sophos with the registration information, in order to be able to download updates. Now we can choose a database for the storage of quarantined items and other data. If there is no SQL Express server available, this can be automatically installed too. Alternatively, a connection can be made to an existing SQL server. The next step is to enter details of the service account to be used to run PureMessage. Here we can create a configuration group for PureMessage. Then we enter the admin email address. At this point it is possible to enter routing information for the email domain, although this can of course be done later. There are a few details to be entered about the company size and location. Once again, a summary of the installation details is displayed before the installer begins. When setup is completed, the installer informs us that a restart is required. Immediately after the restart, Sophos begins post-installation tasks. For example, configuration of SQL Server Express, if this is used. As soon as these automatic tasks are completed, we can continue with our own configuration.

The management interface of Pure Message

The management console for Sophos's mail protection is also very well-designed and professional. The MMC-compatible format provides a clear functional structure, with a good summary page. Even the real-time summary display, called "Activity monitor", is a feast for the eyes. It is the clearly

ordered and professional design that makes working with the console a pleasure. The wide variety of functions can be clearly seen, and leaves nothing to be desired. With the Exchange Server protection too, Sophos comes up trumps with outstanding AD support. The configuration possibilities, with convenient drop-down menus, work very well. The Exchange Server protection thus fits very well with the positive impression created by the entire suite.

Summary

Manufacturer's website

The Sophos website (www.sophos.com) is pleasantly designed, clear, and conforms to current standards. If you want to find out more about Network Access Control, the Sophos website is an ideal starting point. There is a lot of well-presented information on the subject, with appropriate references to suitable products.

The installation procedure

The installation is quick and easy, as is to be expected from Sophos. A basic understanding of network security is desirable, but the installer leads you through the process well. The single installer for the majority of the products is to be commended. The Active Directory support is also outstanding, and makes child's play of setting up accounts etc.

The management console

As with last year's product, the current Sophos management console is a trend-setting solution. The clear and simple design with strong reporting functions can cope with the most complex requirements, and the configuration wizards are convincing throughout. This console should serve as an example for many others.

Deployment areas

The Sophos suite is suitable for all networks, without exception. Its strengths are particularly suited to large and complicated networks.

Antivirus clients

Endpoint Protection is based on the principles of Network Access Control (NAC). This is hardly noticeable to the user, and the remote installation is very simple to carry out.

Summary

This year (as last) Sophos has, along with McAfee, produced the best suite of those we have reviewed. The consistent design of the product line and its installation is convincing throughout. Almost no other suite offers the user more functionality with such ease of use and organizational features.