Single Product Review

Bitdefender Security for Virtualized Environments

Language: English
November 2012
Last Revision: 1st December 2012

www.av-comparatives.org

Review commissioned by Bitdefender

Bitdefender Security for Virtualized Environments

Introduction

Bitdefender make an extensive range of security products for home users, small businesses and enterprises. Their products cover Windows, Mac and Linux operating systems, as well as Android mobile phones. As its name suggests, Bitdefender Security for Virtualized Environments is designed for virtualised computer systems rather than traditional hardware computers. Two different versions are available to cover the different virtualisation platforms, which include Microsoft Hyper-V, Citrix XenServer, VMware vSphere, Red Hat Enterprise Virtualization, and Oracle VM.

The architecture of the product is essentially the same for all versions, however. The VM protection software is deployed and managed using preconfigured Linux-based virtual machines (called Security Virtual Appliances) which run on the same physical host as the guest machines. The first VM is called the Security Virtual Appliance. This may be described as the functionality of the system, as it is responsible for scanning, updating and upgrading tasks. The second VM is known as the Security Console, and provides the management interface via a web-based console. The third component of the product is the Silent Agent, which is the endpoint protection software.

For this review, we installed Bitdefender Security for Virtualized Environments on Microsoft Hyper-V, running on Windows Server 2008 R2.

As an experiment, we installed the client software on a physical PC running 32-bit Windows 7 Professional, as well on virtual client computers. We found that the software functioned exactly the same on the physical computer as on a virtual machine running the same operating system.

Software version reviewed

Silent Agent by Bitdefender 1.2

Documentation

Bitdefender provide two manuals applicable to systems running on Microsoft Hyper-V, namely a Quick Start Guide and an Admin Guide. There is also a Reporter's Guide.

The Quick Start Guide is 13 pages long, and is essentially an introduction to the product, along with basic installation and deployment instructions. It describes the architecture and components of the software in simple terms, so that the administrator has an overview of how the product operates. There is also a detailed system requirements section, covering the (virtualised) hardware requirements needed to run the software, compatible virtualisation platforms, and supported guest operating systems.

A section entitled Quick Deployment Guide provides basic instructions on how to set up the virtual appliances and deploy the endpoint protection software. We note that the pdf file contains hyperlinks that lead directly to the preconfigured virtual machines, enabling the administrator to download the correct packages in quite literally a couple of clicks:

Environment	Format	Security Console	Security Virtual Appliance
Microsoft Hyper-V	VHD*	• download • checksum	• download • checksum
Citrix XenServer, XenDesktop, VDI-in-a-Box	XVA	• download • checksum	• download • checksum
VMware vSphere, View	OVA	• download • checksum	• download • checksum
Red Hat Enterprise Virtualization	OVF**	• download • checksum	• download • checksum
Oracle VM	OVF***	• download • checksum	• download • checksum

We found this to be innovative and extremely convenient.

The Admin Guide is much more comprehensive at 86 pages. Like the Quick Start Guide, it covers the architecture and system requirements of the product. There is a more detailed description of the installation and deployment procedures, along with details of the management console, and extensive instructions for managing and monitoring.

Both the Quick Start Guide and the Admin Guide have been produced to a very high standard. They are well written and have been logically organised into sections. Both have hyperlinked tables of contents, meaning the reader can click on an entry and be taken directly to the page. Likewise, both documents have been appropriately bookmarked, so that the headings of sections and subsections are displayed in Adobe Reader's bookmarks bar, and can be used to access the relevant section with a single click. Whilst there is a diagrammatic representation of the system architecture in both manuals, neither has any actual screenshots, which is our only (minor) criticism of the documentation. Although displaying pictures of a Linux terminal window would be pointless, we feel that a few appropriate screenshots of the management console and client software would be a useful addition.

Installation and deployment

To protect our Microsoft Hyper-V virtual network, we downloaded the appropriate versions of the Security Virtual Appliance and Security Console as complete, pre-configured virtual machines, using the hyperlinks in the Quick Start Guide. We followed the instructions in the Admin Guide, which were very clear and helpful. Each of the virtual appliances is then integrated into the virtualised system. They come as single zip files, which are unzipped to reveal a Virtual Machine folder and a Virtual Hard Disk (VHD) file, the standard components of a Hyper-V virtualised computer. We were able to import the virtual machines into the Hyper-V console quickly and easily. We then started both the new virtual machines, and very soon we had both virtual appliances up and running on our system. Both of these require network configuration, to assign a fixed IP address, along with appropriate subnet mask, default gateway and DNS server. This is done by typing appropriate commands in the Linux console. These are clearly described in the Admin Guide, and could be carried out easily even by an administrator with no previous experience of Linux. Similarly, there are straightforward instructions for logging on to the Security Console, changing the administrator password, and creating a Bitdefender account with an email address (used for notifications) and password.

There are two methods of deploying the endpoint software on virtual machines. The first, Local Installation, involves clicking on a link in a web page or email to start the process. The administrator

can log on to the VM and browse to the installation page of the web interface running on the security console, or send the link in an email to a user. This method has to be used for Linux systems.

The second method, Remote Installation, requires the administrator to perform a Local Installation on one Windows client first. This enables the discovery of all the other Windows machines on the network, which are displayed on the Computers page of the console (please see screenshot in the following section). The administrator then selects all the computers to be installed (there is a "select all" button) and clicks "Install Client" on the Quick Tasks menu. There is no further action required, and the deployment of the client software to the virtual PCs is extremely quick.

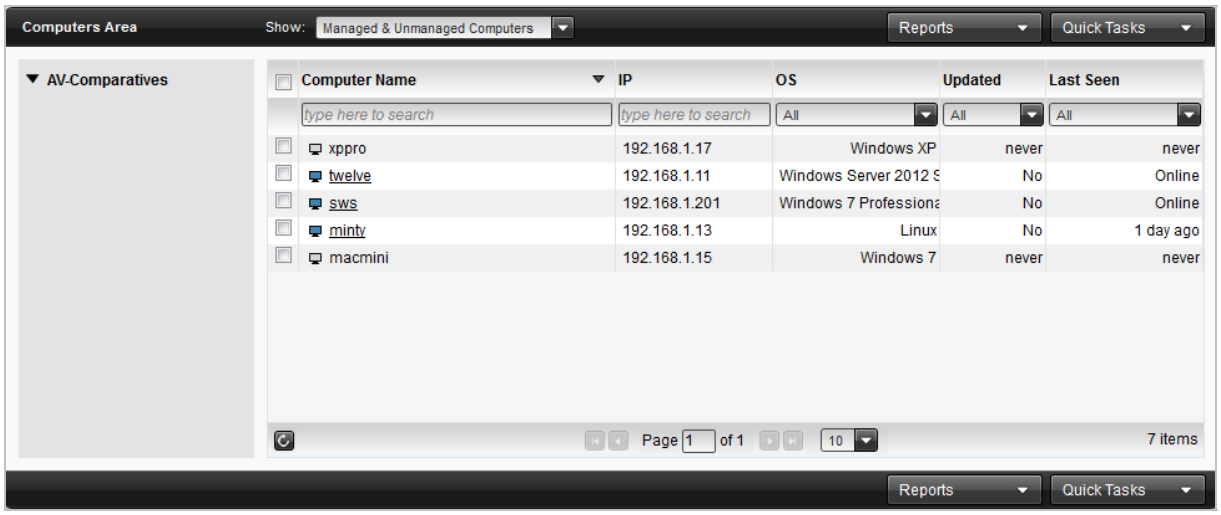
Client/server antivirus management interface

Bitdefender SVE's management console is web based, and is accessed by simply typing the IP address of the Security Console VM into a web browser. Having logged in with the email address and password configured during the setup process, the administrator will see the default Dashboard view of the management console. This provides a graphical overview of the state of the computers on the network, in the form of six tiles in the main pane of the window.

There is a pie chart entitled Network Status, which shows percentages of virtual computers that are unmanaged, protected, vulnerable and offline. Computer Malware Status also uses a pie chart, and displays the proportion of VMs that are malware-free, have resolved infections, or blocked malware. Bar charts show Top 10 Detected Malware (by name), Top 10 Most Infected Computers, and Computer Status. The latter shows the percentages of computers with antivirus installed, up to date, licenced, and online. Finally, a line graph displays Malware Activity, i.e. malware discoveries over time, and a notifications tile is minimised.

Each of the tiles has a title bar with a refresh button, an options button, and a minimise button. The administrator can minimise, say, two of the tiles, showing the remaining four tiles, which expand to fill the available space. This makes it easy to emphasise the information the administrator deems most important.

A menu bar running along the top of the console has the following items: Dashboard (default), Computers, Policies, Reports, Quarantine, Accounts, and Log. Computers show a list of computers on the network, which can be filtered to show e.g. only managed or unmanaged machines:



Policies allow different configuration options to be defined and applied to individual computers or groups. Reports allow details status reports to be configured, whereby the computers/groups, time period and reporting criteria can all be specified. Quarantine is self-explanatory, while Accounts manages user accounts for the console. Log refers to activities carried out by specific user accounts, e.g. logging in and out, creating and deleting groups, installing or uninstalling computers, etc.

There is a link to Help and Support in the top right-hand corner of the window.

Client/server antivirus monitoring

The status of real-time protection is shown in the Computer Status tile of the dashboard, as On (green) or Off (red). When we disabled the real-time protection on our client VMS, we noted that the program window of the client software showed almost immediately that this had happened. However, the Antivirus status shown in the Dashboard continued to show "All Well" (green), and it was some time before the status display updated to show that the RTP had been switched off. Bitdefender inform us that this is a known issue and that they are working on minimising the synchronisation time.

There are no other components (such as firewall or antispam) in the software that could be monitored. The update status is shown as proportions of computers updated and not updated in the Dashboard view; the status of individual computers is shown in the computers view. In the event that all computers are up to date, this will be seen immediately from the dashboard, and the administrator will not need to investigate any further.

We could not find any means of displaying the current program version of the endpoint protection software in the console, although this can be seen in the Help box of the endpoint software on each client.

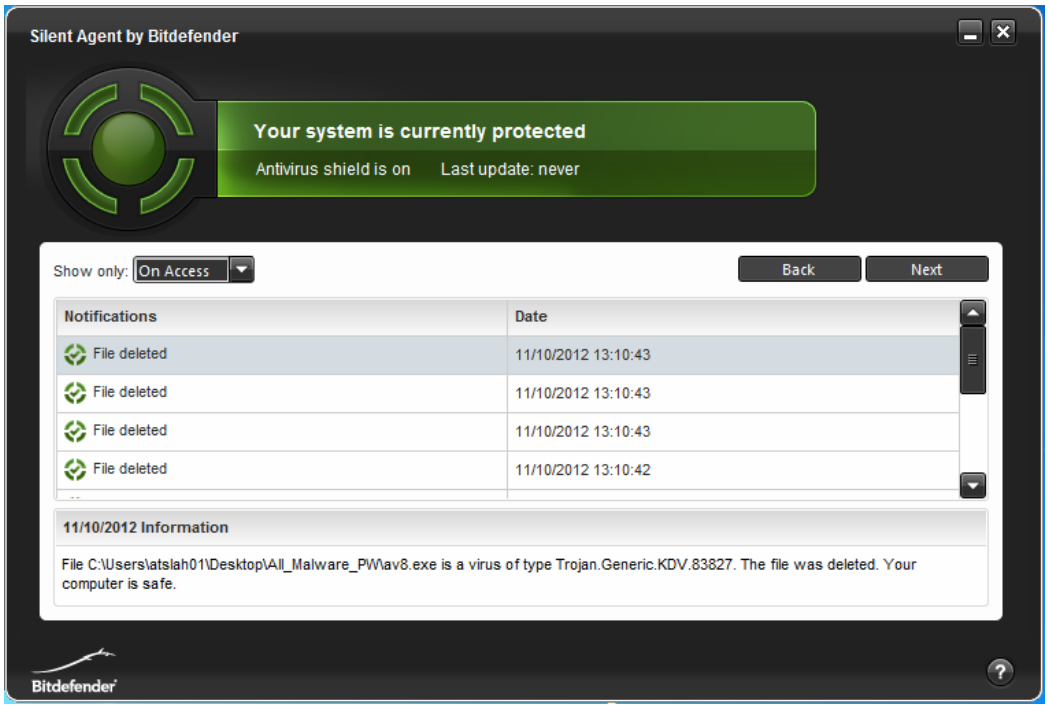
Client/server antivirus tasks

Selecting a computer or multiple computers in the Computers view of the console allows endpoint software to be installed or uninstalled, or a full scan run, from the Quick Tasks menu. Real-time protection can be disabled by editing the policy applied to the computer(s), which is a quick and easy process. There are no other components of the software that could be disabled or uninstalled. We could not find any means of running an instant signature update, although the update interval can be set in the policy, the shortest being 1 hour. A full system scan can be run from the Computers page, by selecting the computer(s) desired and selecting Scan from the Quick Tasks menu. A custom scan can be run by editing the policy applied to the machine(s), and adding a custom scan task to be run at a specific day and time. We could not find any means of running a vulnerability scan or updating the program version.

As the client software does not allow any configuration changes to be made locally, password protecting it is not necessary.

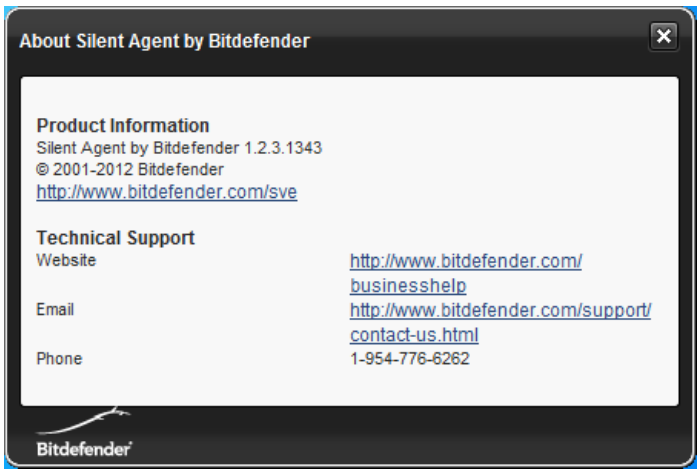
Client/server antivirus software

Bitdefender Silent Agent is, as its name suggests, effectively hidden after installation. On a Windows PC or server, there is no system tray icon or desktop shortcut from which to open the program interface, although a program folder with a program shortcut can be found in the All Programs section of the Windows Start Menu. Clicking on the Bitdefender Silent Agent link here opens the program window shown below:



The interface displays information but does not allow any kind of action to be carried out, or any configuration changes to be made. The big green information strip at the top shows the current protection status, and notes the state of real-time protection and the time of the last update. If real-time protection is disabled, the green strip and circular symbol turn red, and the information text changes to "Your system is not protected | Antivirus shield is off". A table in the centre of the window displays details of malware found, and other system events such as updates.

The help button in the bottom right-hand corner displays an information box with links to online help:



We note that when the program window is opened from the Start Menu, a system tray icon appears. However, this disappears again once the current user has logged off. This "Silent Mode" can be switched off, displaying the GUI permanently.

When we attempted to download the EICAR test file, the download was blocked silently without any sort of message, though this can be changed in the settings to show a warning. The information table in the program window gave details of the file and noted that it had been quarantined, however:

Additionally, an email notification was sent to the registered address. The reaction to the discovery of local malware is identical.

Summary

We found Bitdefender Security for Virtualized Environments to be a simple but effective suite that provides easy-to-manage protection for virtual networks. Installation is straightforward for any administrator familiar with the virtualisation platform; despite being Linux-based, the suite does not require any knowledge or experience of Linux, as the documentation provides clear instructions that an experienced Windows administrator can easily follow. Essential monitoring and everyday tasks can easily be carried out using the web-based console, which can be accessed via a browser from any computer on the network.

Copyright and Disclaimer

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

AV-Comparatives e.V. (November 2012)