Single Product Test

Head-to-Head Comparison

VIPRE Endpoint Security - Cloud Edition

Webroot SecureAnywhere Business Endpoint Protection

Language: English
October 2017

Last revision: 3rd November 2017

www.av-comparatives.org

Table of Contents

Management Summary

As regards malware protection, the study utilized Real-World Protection Test on a test set of over 300 live malicious URLs found in the field, thus replicating the same daily infection vectors that typical SMBs would experience. VIPRE Cloud achieved a superior 100% protection rate— versus an 86.4% rate for Webroot SecureAnywhere.

With regard to the management interface, both VIPRE and Webroot products could be successfully deployed by small and medium size businesses (SMBs). However, VIPRE Cloud has a number of advantages which, although individually small, in sum make network management significantly quicker and easier. These can be summarised as follows:

1. Visibility: the graphical design of the VIPRE Cloud console and endpoint GUI makes individual items stand out very clearly, even when used on the small touchscreens of mobile devices
2. Speed: thoughtful design of the UI elements, combined with the high-visibility graphic design, make it faster to accomplish tasks
3. Easy analysis: intelligent linking of related items allows the admin to find more information quickly and easily.

Whilst the Webroot console requires the creation of a site for the company concerned, VIPRE Cloud is ready to go as soon as the admin has logged in for the first time. The deployment page shown in the VIPRE Cloud console after the first login makes it particularly easy and fast to get started. The single menu column on the left-hand side of the VIPRE Cloud console makes navigation very simple.

VIPRE Cloud's menu-naming scheme for features is very simple and rational. For example, deployment is found under *Deploy Agents*, managed computers can be seen under *Devices*, and the quarantine function is called *Quarantine*. By contrast, Webroot names the first two of these features *Resources* and *Group Management*, while the quarantine functionality is found under *Reports*.

The VIPRE Cloud console uses a very bright, clean, modern design for its console. There is clear spacing between menu items, and appropriate use of colour to help differentiate between adjacent items. Aside from any aesthetics, this has two advantages. Firstly, it is quick and easy to find the items you want on the page, because they stand out clearly. Secondly, the console is well suited to use on a touchscreen and mobile devices; it adapts when viewed on a tablet or smartphone, making text large enough to read and menu items large enough to tap. With mobile devices being used increasingly for management, this is an important point to consider. Whilst the Webroot console is by no means badly designed, its overwhelmingly grey interface and more densely-packed text make it slower to navigate. The console does not adapt when used on a mobile device, meaning that the admin has to go through the fiddly process of reorienting and resizing the page to make any item usable. Additionally, whilst this is arguably a subjective viewpoint, we found it easy to modify and apply policies with the VIPRE Cloud console, while with Webroot a certain amount of trial and error was necessary to make effective changes.

The VIPRE Cloud console makes use of intelligent linking of UI elements. For example, clicking/tapping on the name of a quarantined threat instantly provides detailed analysis of the threat, including detection method and action taken by the system.

With regard to the endpoint protection software, VIPRE Cloud again has a number of advantages relative to Webroot. Firstly, admins will find VIPRE Cloud's short and simple installation wizard very familiar, due to its similarity to e.g. iTunes setup. Webroot's setup process is certainly very quick and requires no user action beyond executing the installer file and clicking the Windows User Account Control prompt – but its totally silent nature may leave admins wondering if the product has actually been installed.

For an administrator, having a full, consumer-like GUI on the client software makes local administration very familiar and straightforward. This can be helpful in some situations, particularly at the beginning when the admin is still learning how to manage using the cloud console. Although Webroot can display a full GUI and malware alerts, both of these are deactivated by default, meaning an admin has to understand and apply the principles of policies in order to activate them. VIPRE Cloud's client software displays a very familiar interface, with major features very easy to find, by default.

As with the console, the clean, well laid-out design, single menu bar and good use of colours in the endpoint client make it easy to see items quickly, and would again be useful if using a touchscreen device. All the VIPRE Cloud endpoint client's settings can be accessed from one dialog, whereas Webroot's are distributed between *Advanced Settings* and *Scan Settings*. VIPRE Cloud malware alerts persist until closed by the user/admin, making it easier to find out what has happened.

Overall, we feel that VIPRE Endpoint Security-Cloud Edition is very well suited to the SMB market as a whole. We also regard it as particularly well suited to small businesses with limited IT support resources, as the very clear and simple design would make it easy for even inexperienced admins to get to grips with.

Introduction

This review – commissioned by VIPRE - compares VIPRE Endpoint Security Cloud Edition with Webroot SecureAnywhere Business Endpoint Protection, with emphasis on suitability for use in SMBs. To assess both products, we have described using each one in typical everyday scenarios, including the following points:

CONSOLE

- Installation and configuration
- Layout
- Deployment of endpoint protection software
- Status and alerts
- Showing the program version of installed endpoint software
- Scanning, and setting scheduled scans
- Removing devices from the console
- Quarantine
- Policies
- Reports
- Licence information
- Integrated help feature

ENDPOINT PROTECTION SOFTWARE

- Installation
- Status
- Scans (full, custom, quick, scheduled, context menu)
- Logs
- Quarantine
- Updates
- Settings
- Help
- Integration with Windows Security Center and Windows Defender
- System Tray menu
- Alerts (malware, phishing, disabled protection)

Program versions reviewed

- VIPRE Business Agent for Windows servers and workstations 10.0.7110
- VIPRE Cloud Console as at September 2017
- Webroot SecureAnywhere Endpoint Protection 9.0.18.34
- Webroot SecureAnywhere management console as at October 2017

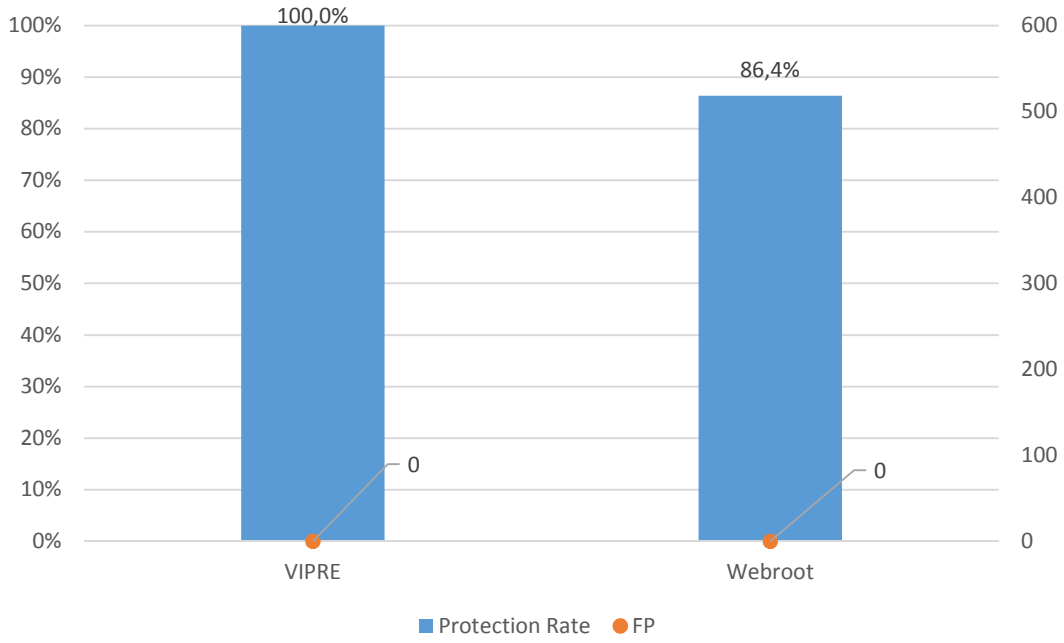
Test results

A Real-World Protection Test[1] was performed in October 2017.

Real-World Protection Test

The results[2] are based on the test set of **316** live malicious URLs found in the field. Thus exactly the same infection vectors are used as a typical user would experience in everyday life. The test-cases used cover a wide range of current malicious sites and provide insights into the protection given by the product while surfing the web.

Product	Protection Rate	False Positives
VIPRE Cloud	100%	0
Webroot SecureAnywhere	86.4%	0



[1] For more information about the Real-World protection Test, please visit:
https://www.av-comparatives.org/dynamic-tests/

[2] We would like to point out that while some products may sometimes be able to reach 100% protection rates in a test, it does not mean that these products will always protect against all threats on the web. It just means that they were able to block 100% of the widespread malicious samples used in a test.

VIPRE Endpoint Security – Cloud Edition

Overview

Windows operating systems supported

Clients: Windows Vista, 7, 8.1, 10

Servers: Windows Server 2008/R2, 2012/R2, 2016; Windows Small Business Server 2003, 2008, 2011

Product information on vendor's website

https://www.vipre.com/products/business-protection/cloud/

Online support

https://businesssupport.vipre.com/support/home

Documentation

https://success.vipre.com/

Summary

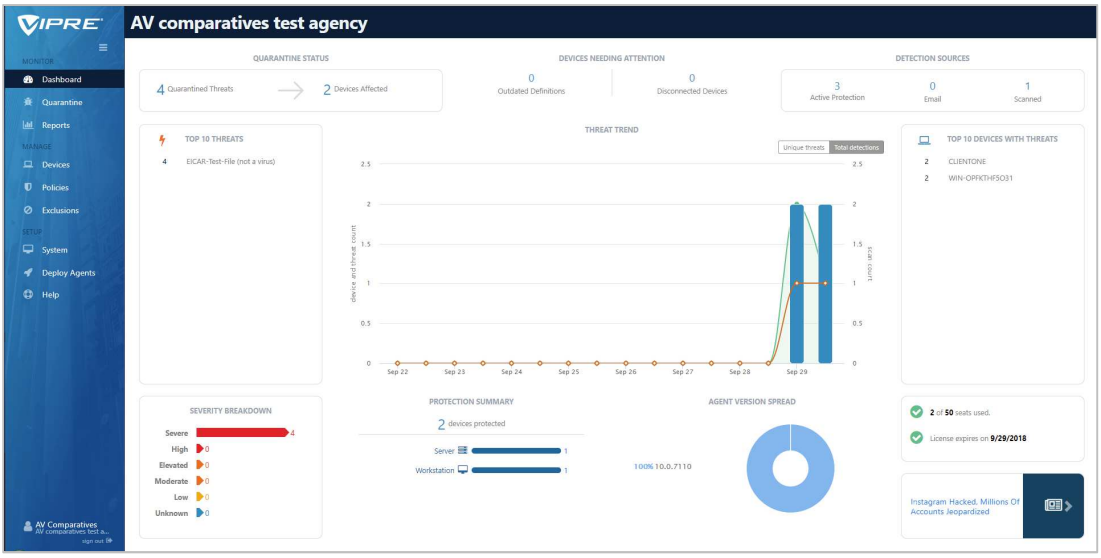
VIPRE Endpoint Security Cloud stands out because of the very clean, modern design used in both the console and the endpoint protection software. We found the product very intuitive to use, with sensibly-named menus and very effective layout making it easy to find essential features. A number of details, such as the deployment options being offered when the admin first logs on to the console, result in a very positive user experience overall. The product is ideally suited to SMBs.

Management Console

Installation and configuration

The console is cloud-based, so no installation or configuration is required.

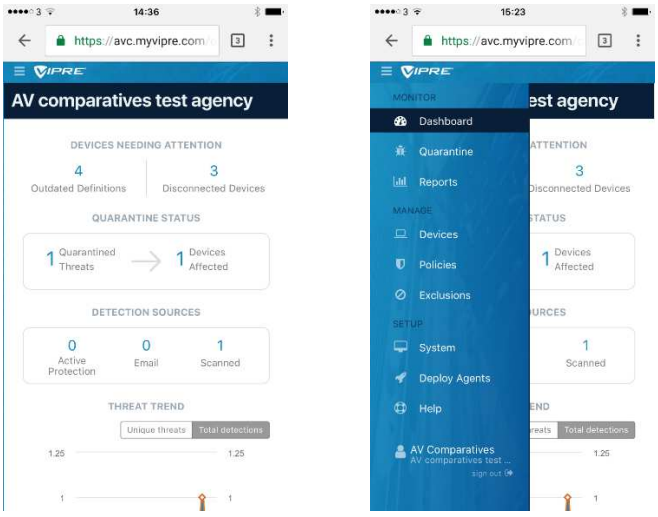
Layout



The console can be navigated from a left-hand menu column, with links to the pages *Dashboard, Quarantine, Reports, Devices, Policies, Exclusions, System, Deploy Agents,* and *Help*. The menu panel can be collapsed to show just the icons, or expanded to include text.

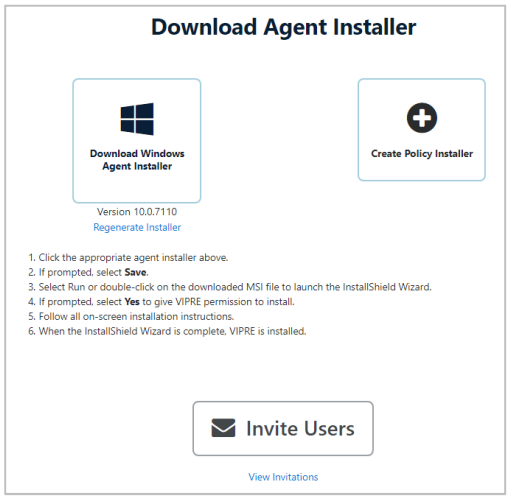
Use with tablet or smartphone

VIPRE Cloud's management console has been designed to adapt to use on small touchscreen devices. When viewed on a tablet or smartphone, the page content is rearranged so that individual items are clearly legible, and the admin only needs to swipe down to see additional items (left-hand screenshot below). The menu panel can be easily accessed by tapping the "hamburger" menu button in the top left-hand corner, which then shows the entire navigation menu as an overlay (right-hand screenshot):



Deployment of endpoint protection software

When the admin first logs on to the console, the *Deploy Agents* page (shown below) is displayed, making it easy to start deployment. The page can easily be accessed at any time by clicking *Deploy Agents* in the menu column.



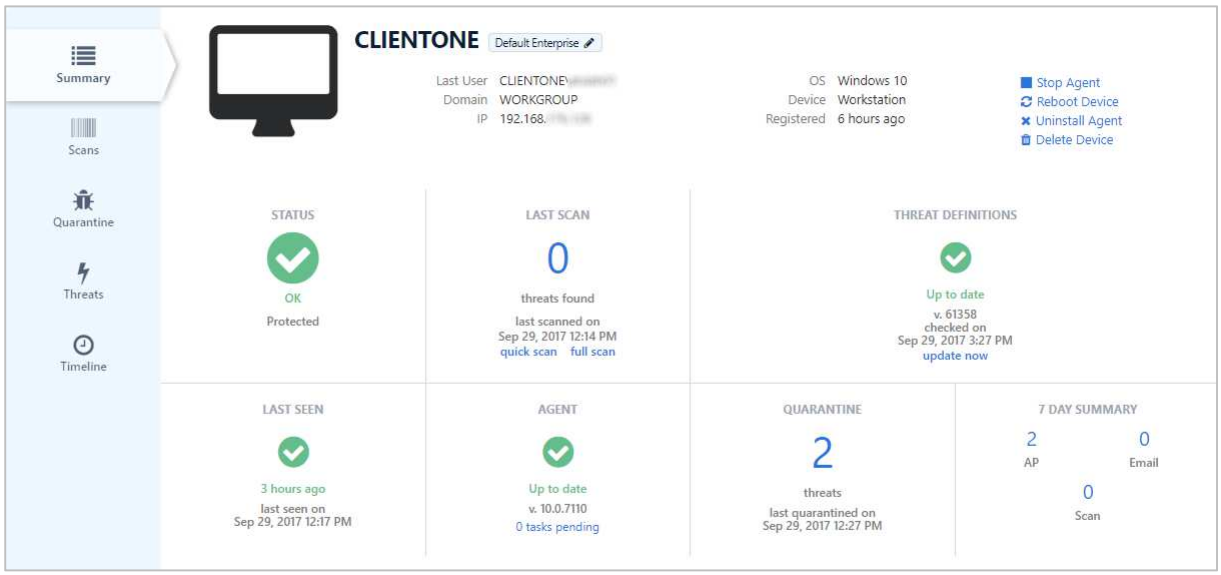
Monitoring the network

Status and alerts

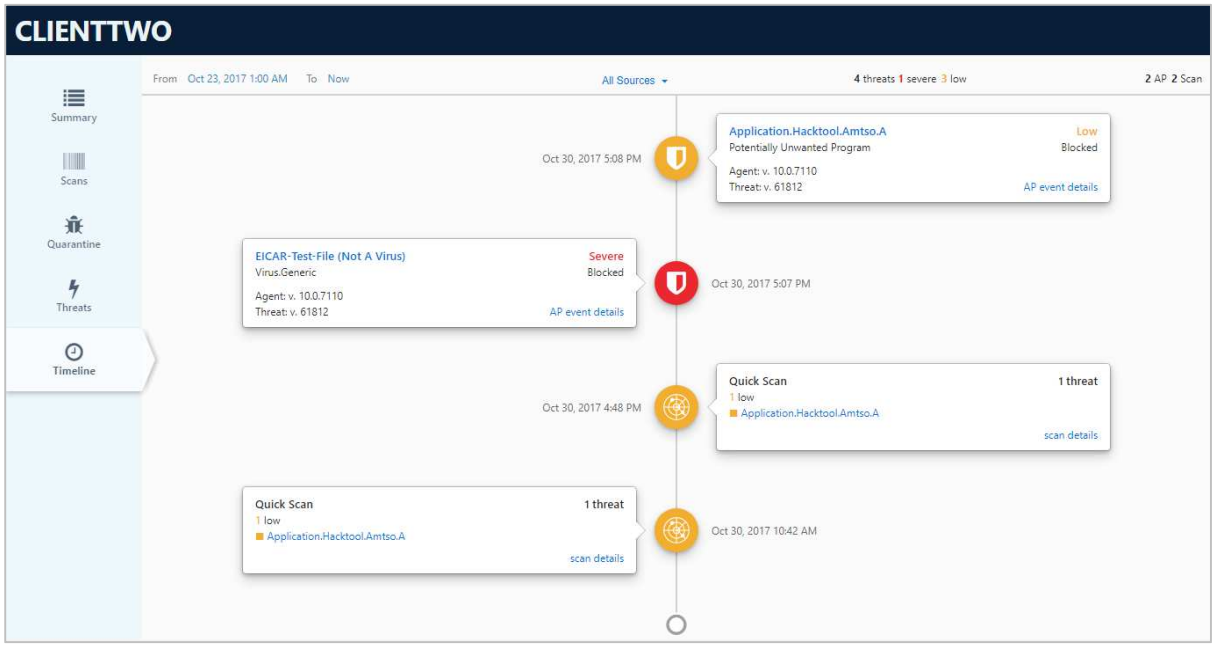
These are shown on the *Dashboard* (home) page of the console. Various panels show *Quarantine, Devices Needing Attention, Detection Sources, Top 10 Threats, Top 10 Devices with Threats, Severity Breakdown, Protection Summary,* and *Agent Version Spread*.

Program version

This can be seen by opening the *Devices* page and clicking on an individual client to see its properties:



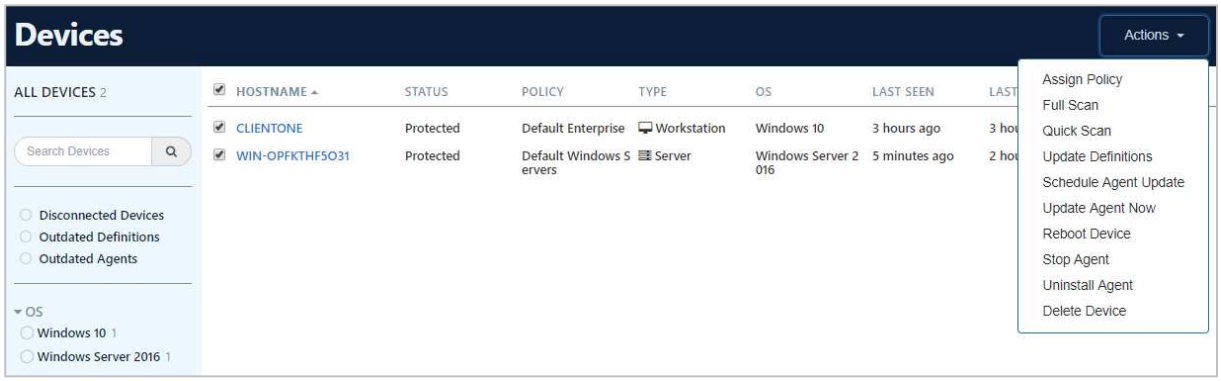
We note that the *Devices* page also includes an innovative feature called *Timeline*, which enables the admin to see a history of threat detection for a particular device, and thus assess whether there is a recurrent threat pattern. Information displayed includes threat name (hyperlinked to an information page), type and severity of threat, detection method and action taken:



Managing the network

Scanning, scheduling scans, updates and removing devices from the console

These tasks can all be carried out from the *Devices* page, by selecting clients' check boxes, then clicking the *Action* menu:

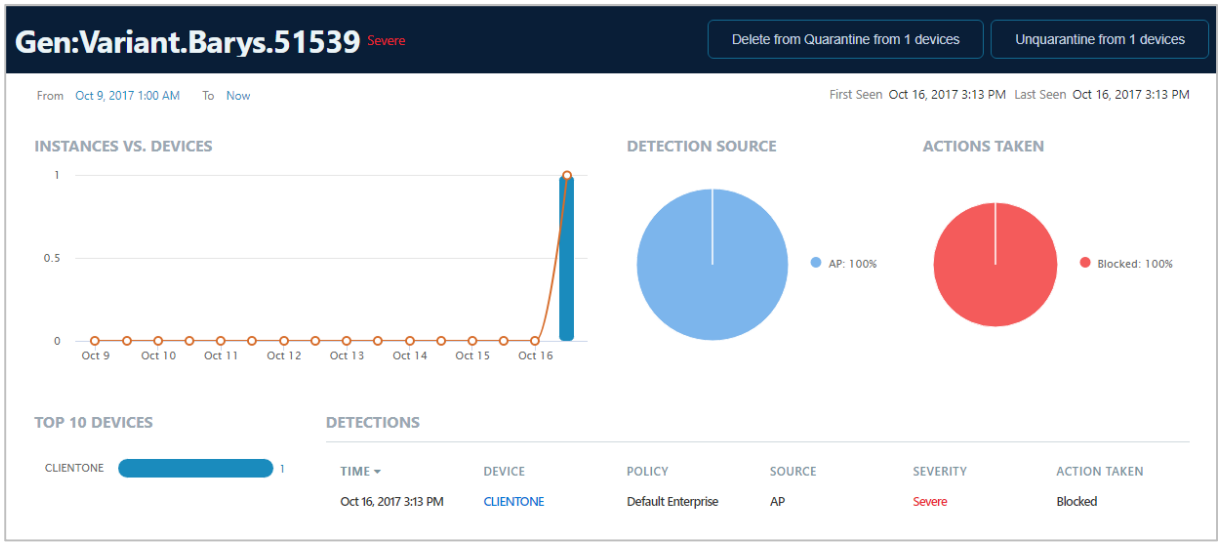


Quarantine

The *Quarantine* page displays details of malware items quarantined on client computers:

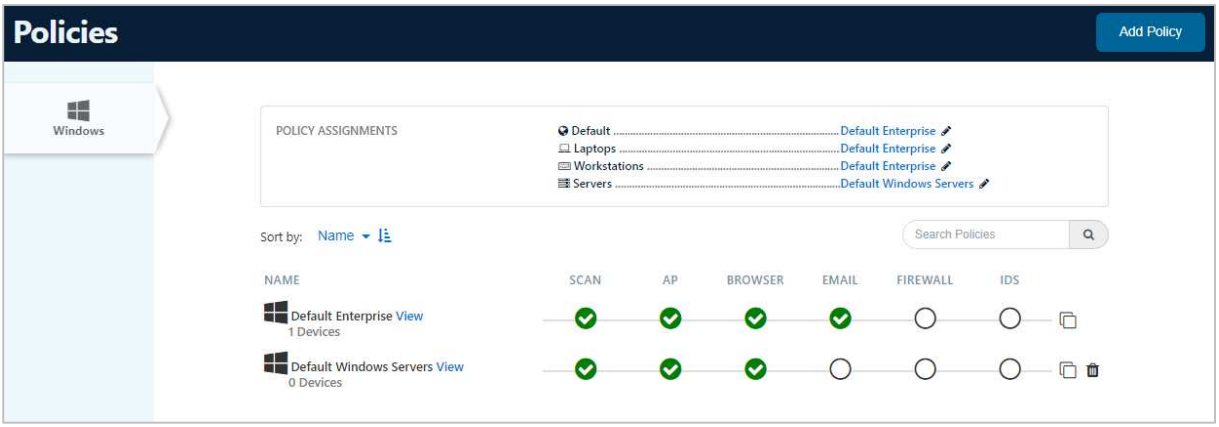
Clicking on the date of the infection shows the path to the infected file on the client computer, along with links to delete the file from quarantine, or restore it:

Clicking on the name of the malware opens a page showing details of that particular threat, including which computers have been affected by it, how it was detected, and the action taken:



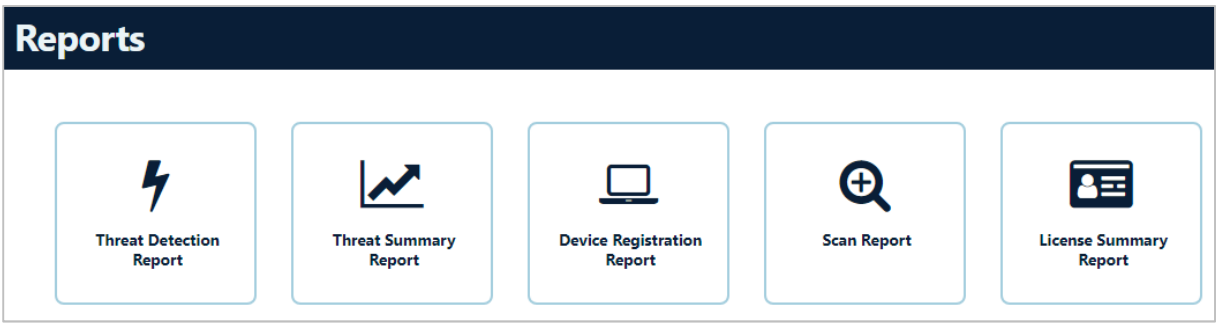
Policies

The *Policies* page provides a clear, simple graphical overview of the policies available, the protection components activated by each policy, and which policy is respectively applied to laptops, workstations and servers:



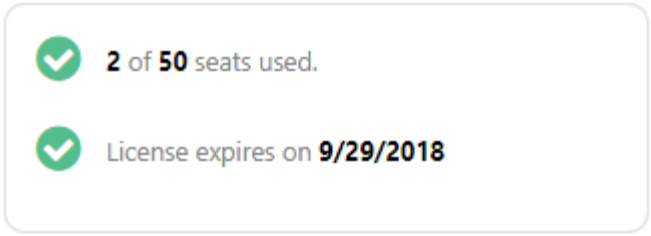
Reports

The *Reports* page shows tiles for the various different types of report available, namely *Threat Detection, Threat Summary, Device Registration, Scan* and *License Summary*:

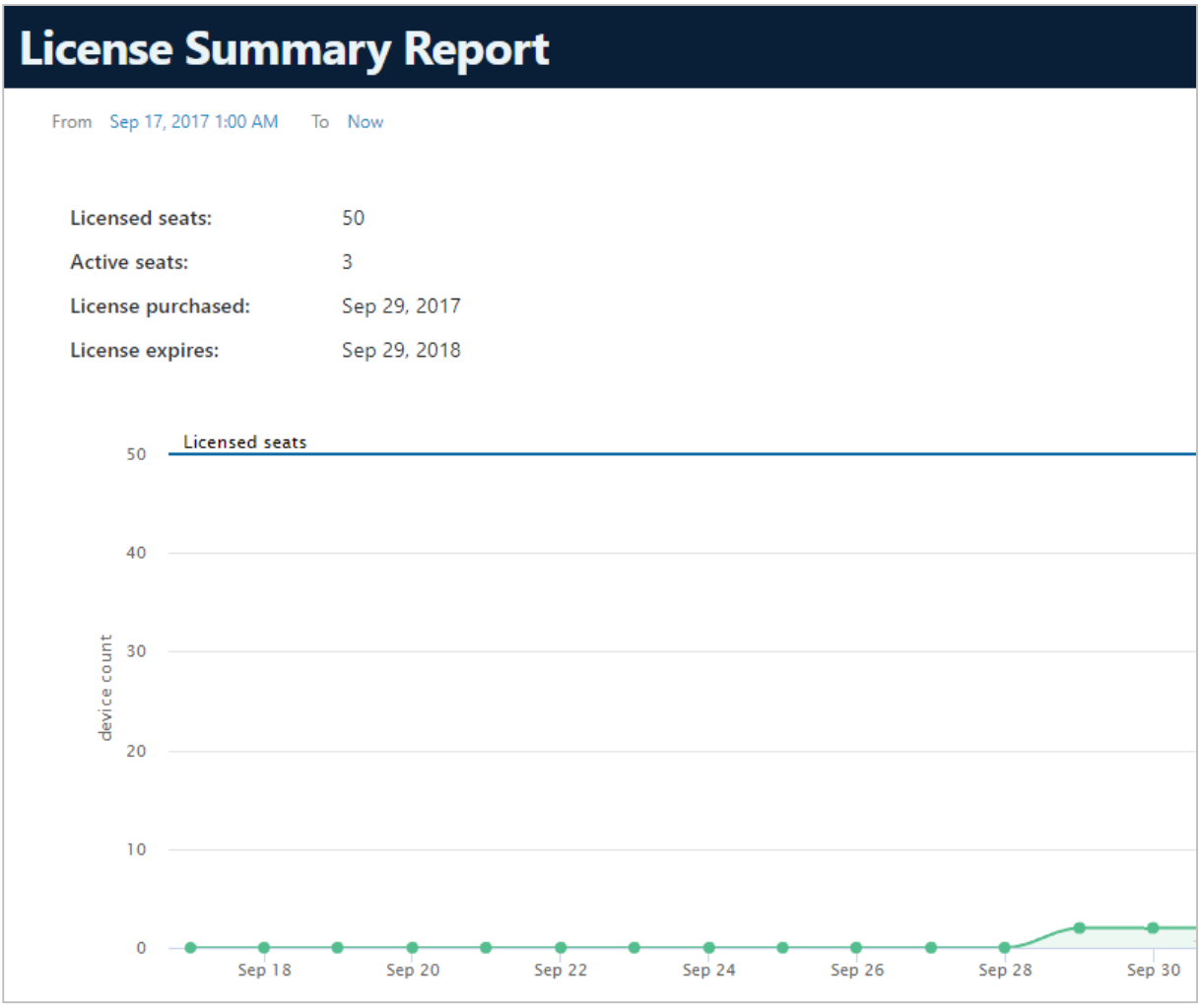


Licences

A summary of licence information is displayed in the bottom right-hand corner of the *Dashboard* page:

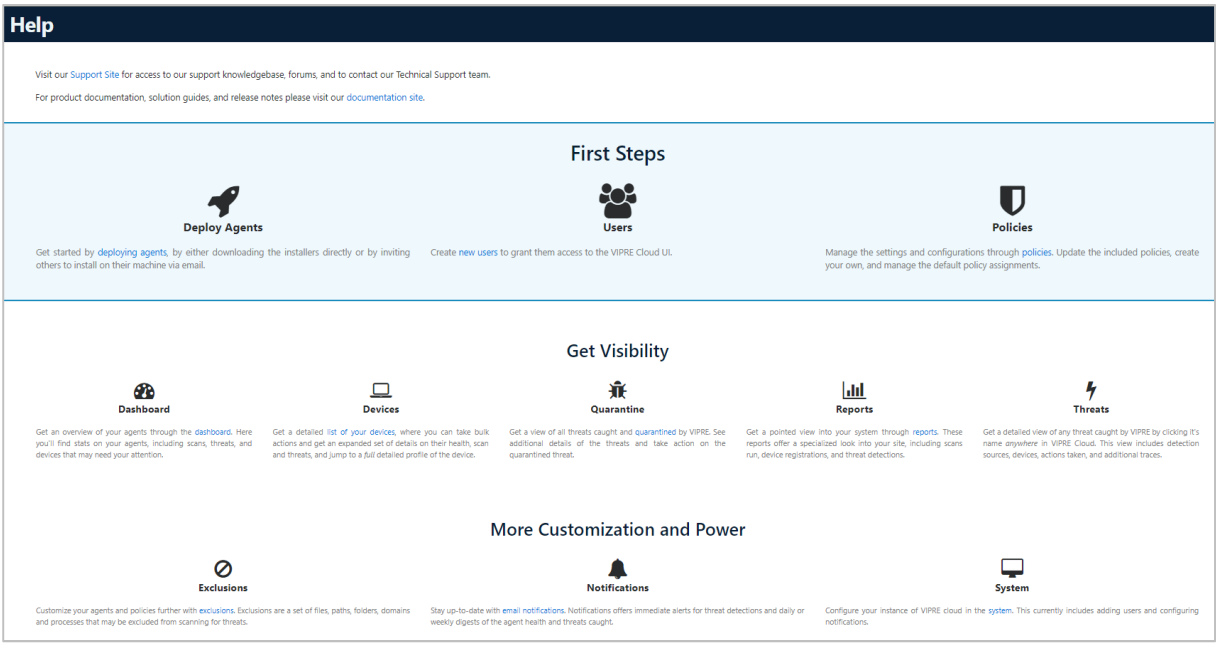


Clicking on this panel opens the *License Summary Report* page, which shows a graph of licences used over time:

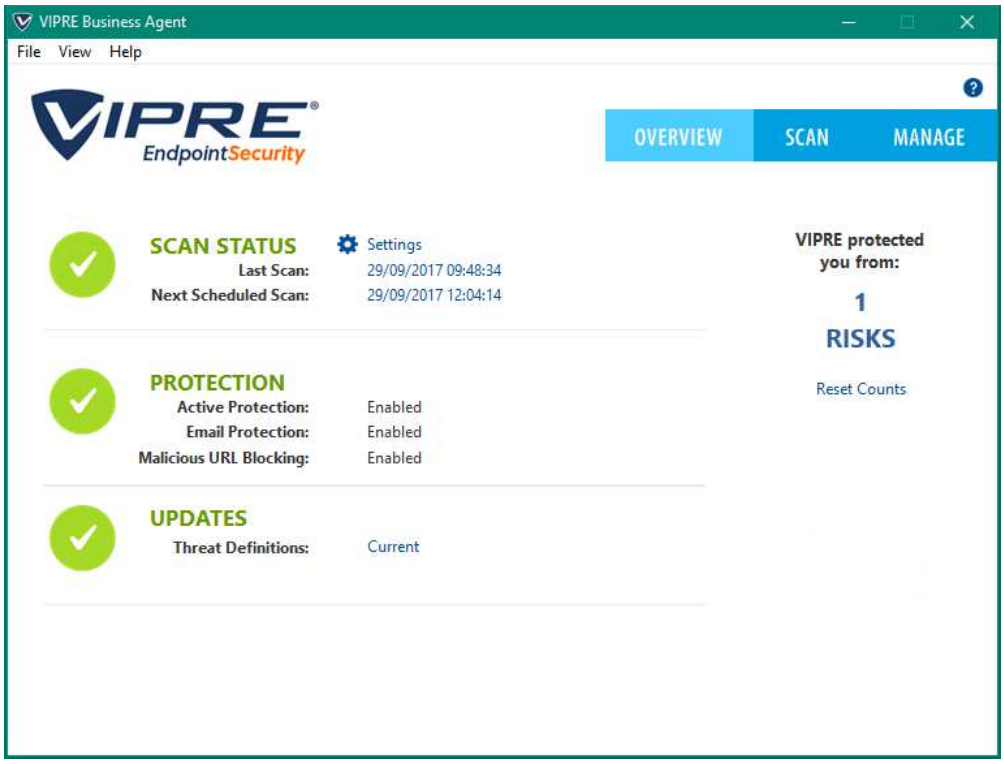


Integrated console help

Clicking the *Help* link in the console opens an overview page of the console's functions, with a succinct explanation of each, and a link to the relevant console page. There are also links to the support and documentation pages of the manufacturer's website:



Windows client endpoint protection software



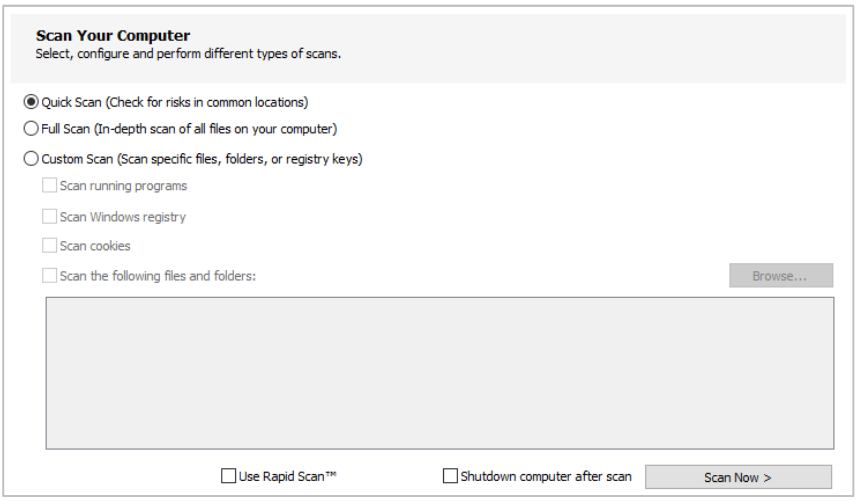
Installation

The setup wizard is very short and simple, and does not require the admin to make any decisions.

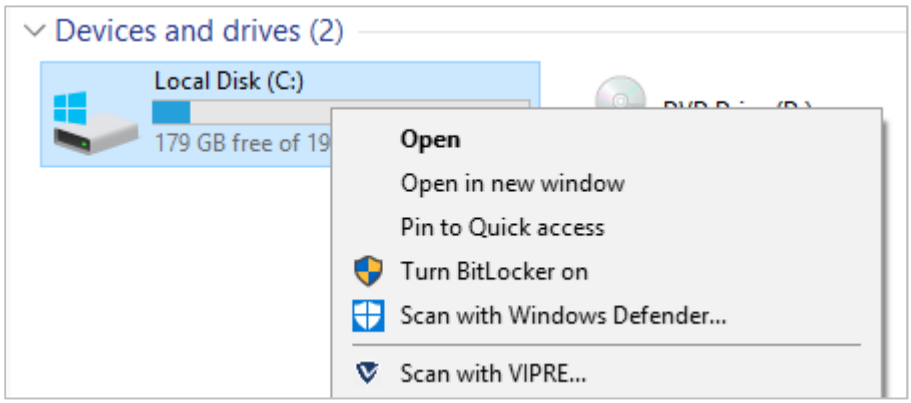
Finding essential functionality

Security status: the status display is very prominent, and provides detailed information on scan status, protection components and malware signatures, as shown in the screenshot above.

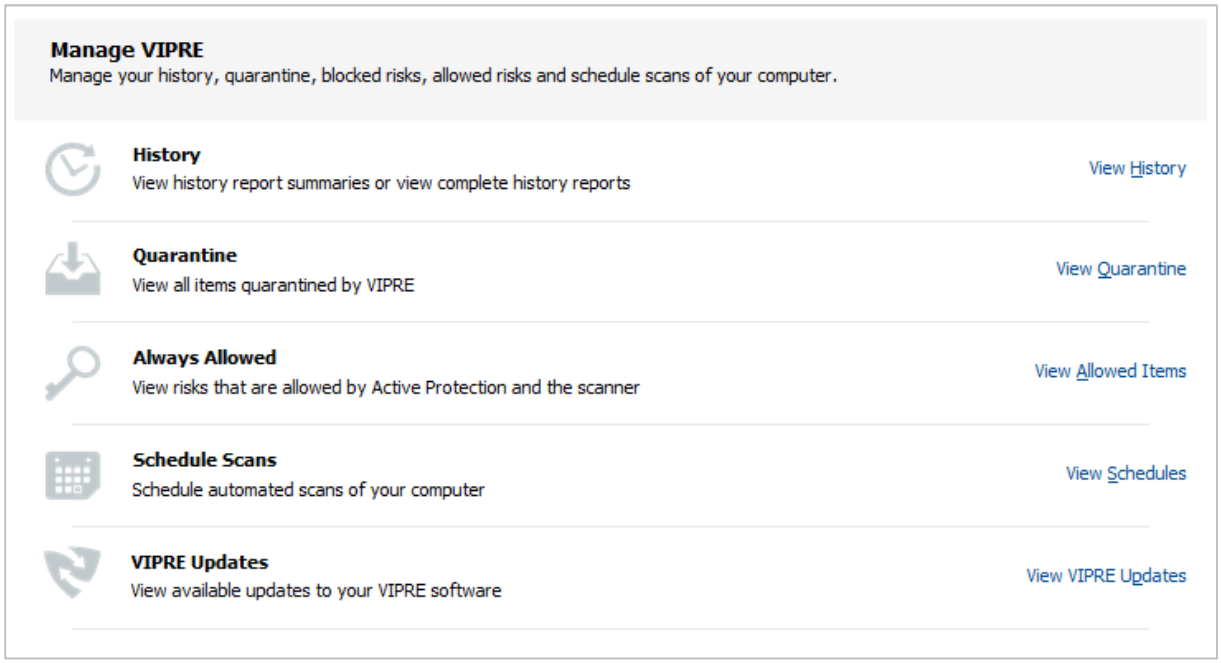
Scans: Clicking the *SCAN* tab at the top of the window opens a page of scan options, including **full**, **quick** and **custom** scans:



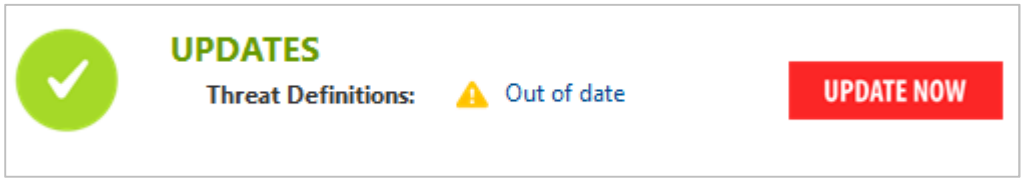
Context menu scan: Users can scan an individual file, folder or drive by right-clicking it in Windows Explorer and clicking *Scan with VIPRE*:



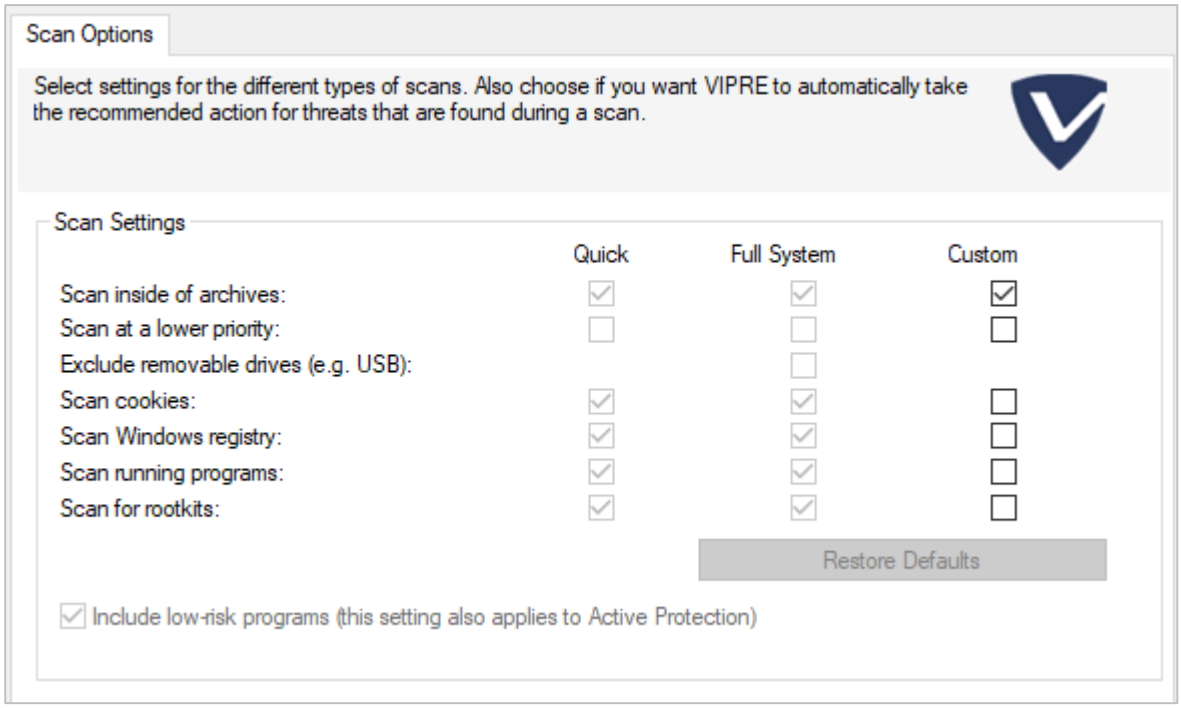
Logs, quarantine, exceptions, scheduled scans and software updates can be configured by clicking the *MANAGE* tab:



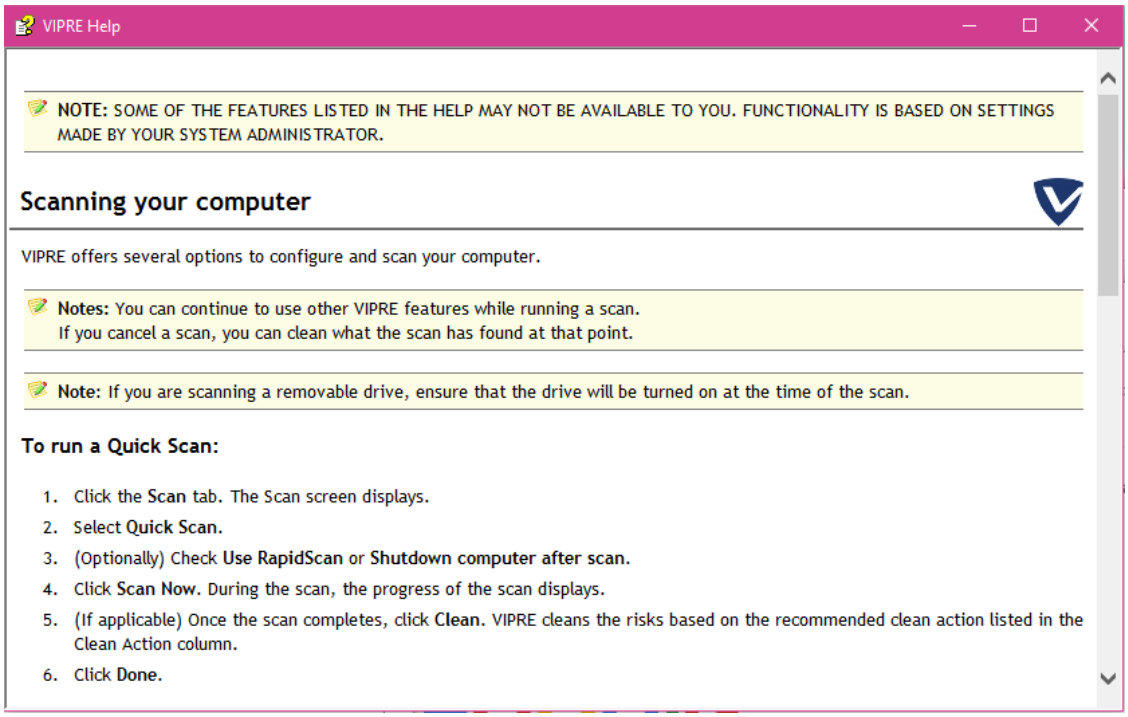
Updates: An *Update Now* button appears if the threat definitions are out of date:



Settings can be accessed from the link in the *Scan Status* section, or from the *File* menu. Users cannot disable any protection components from the GUI; this can only be done from the console. The settings dialog is shown below:



Help can be found by clicking the *?* button in the top right-hand corner of the window. The help feature is context sensitive, that is to say, it opens the appropriate help page for the feature currently being used in the main window. For example, if the user clicks the help button while looking at the *Scans* page, the help page shown below will be displayed:

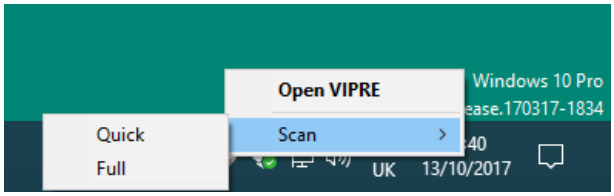


Windows Security Center/Windows Defender

VIPRE Business Agent registers in Windows Security Center as the antivirus program. Windows Defender is disabled.

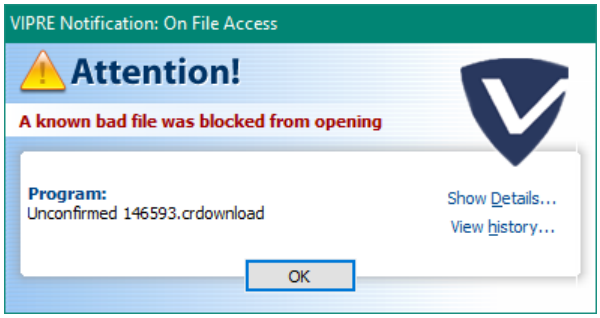
System Tray menu

Right-clicking the VIPRE icon in the System Tray lets the user run quick or full scans, or open the program window:



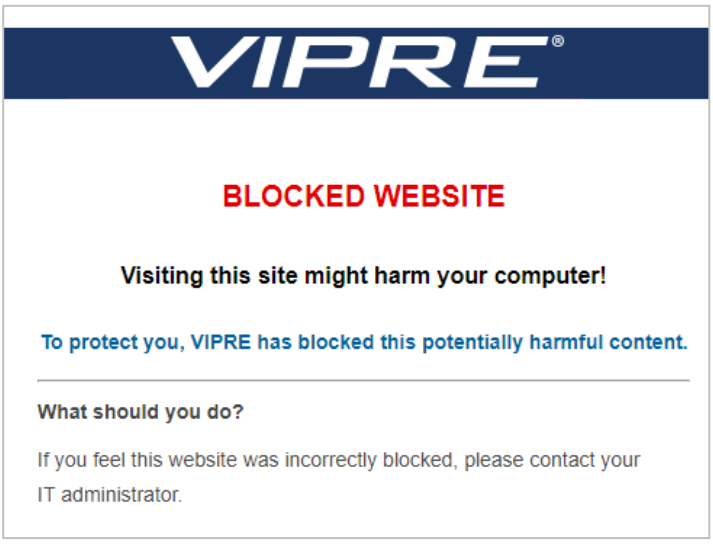
Alerts

If the EICAR test file is downloaded, the alert below is shown:



No user action is required. The alert persists until closed by the user.

If the AMTSO Phishing Test Page is accessed, VIPRE blocks the page and displays the warning below in the browser window:



If real-time protection is disabled, the status display in the main program window changes to show a warning:

Protection can only be reactivated from the console.

Windows Server endpoint protection software

This can be regarded as identical to the client software. In keeping with the nature of a server, email client protection is not installed on server systems by default.

Webroot SecureAnywhere Business Endpoint Protection

Overview

Windows operating systems supported

Clients: Windows XP, Vista, 7, 8, 8.1, 10

Servers: Windows Server 2003/R2, 2008/R2, 2012/R2, 2016; Small Business Server 2008, 2011, 2012

Product information on vendor's website

https://www.webroot.com/us/en/business/smb/endpoint-protection

Online support

https://www.webroot.com/us/en/business/support

Documentation

https://docs.webroot.com/us/en/business/wsab_endpointprotection_adminguide/wsab_endpointprotection_adminguide.htm

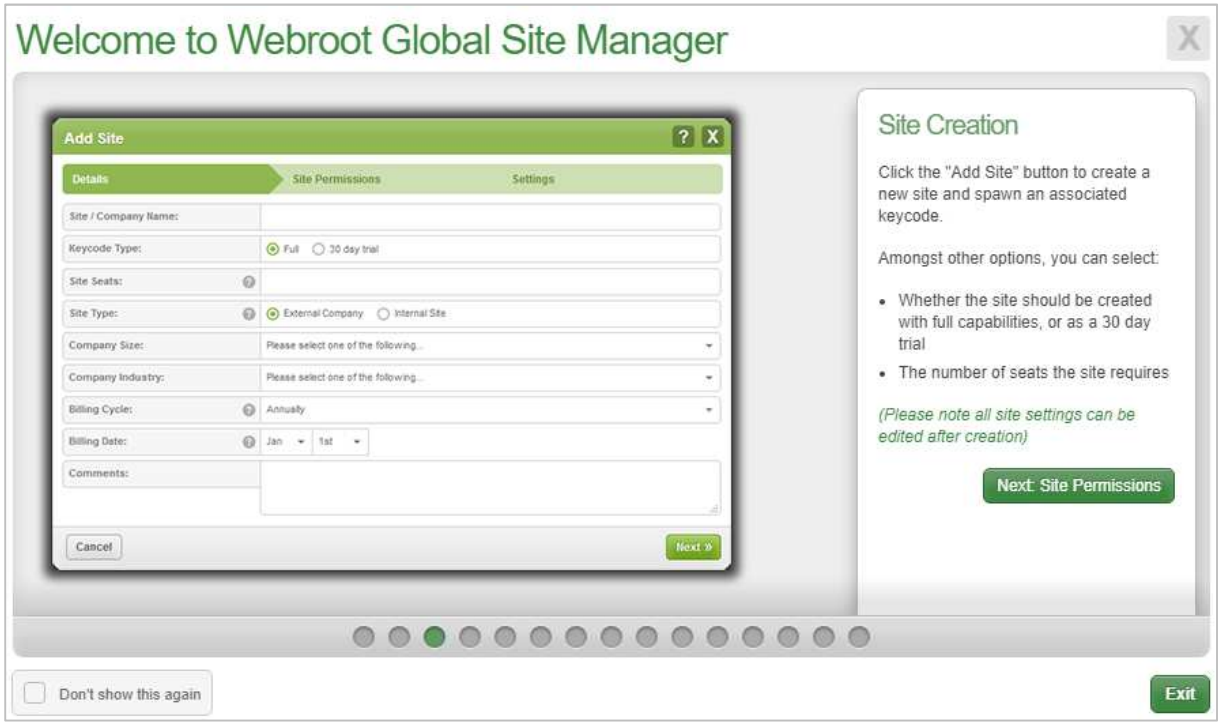
Summary

For an experienced network administrator, Webroot's endpoint protection product would be very straightforward to use. The layout of the console is essentially good, if a little old-fashioned. We were able to perform most everyday tasks without any difficulty, although we had to experiment with the policies feature just a little in order to get it to work. We note that the console does not adapt to mobile devices, meaning that a degree of patience would be required to use it on a smartphone or tablet.

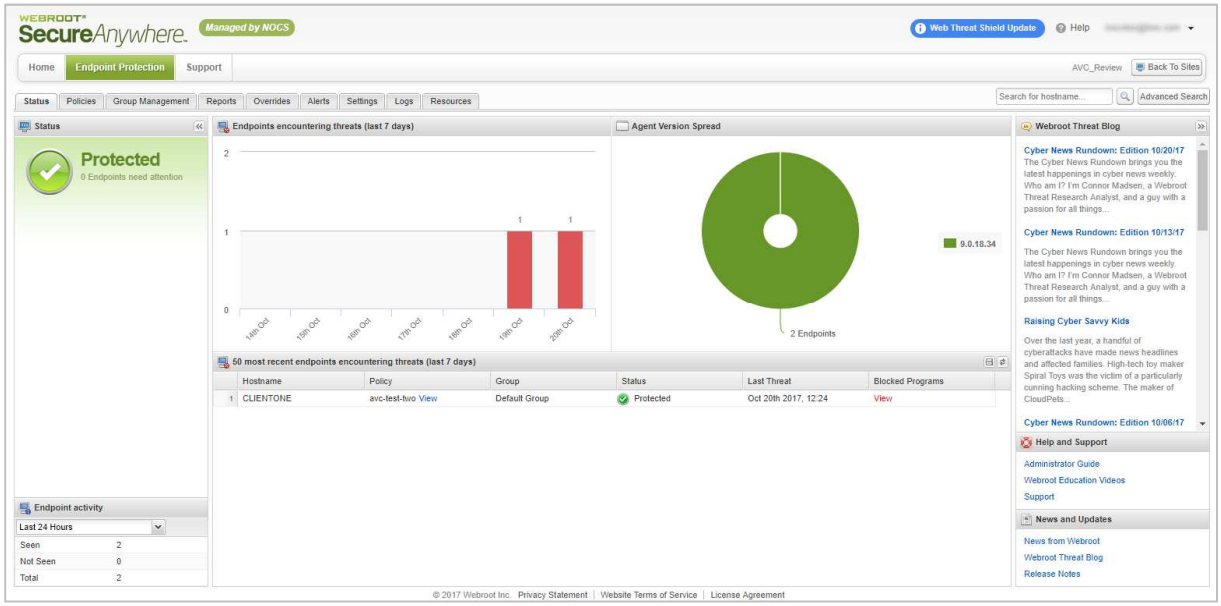
Management Console

Installation and configuration

The console is cloud-based, so no installation is required. However, as the console is capable of managing multiple networks, a new site has to be created Global Site Manager; this is quite straightforward, and just involves filling in the form shown below:



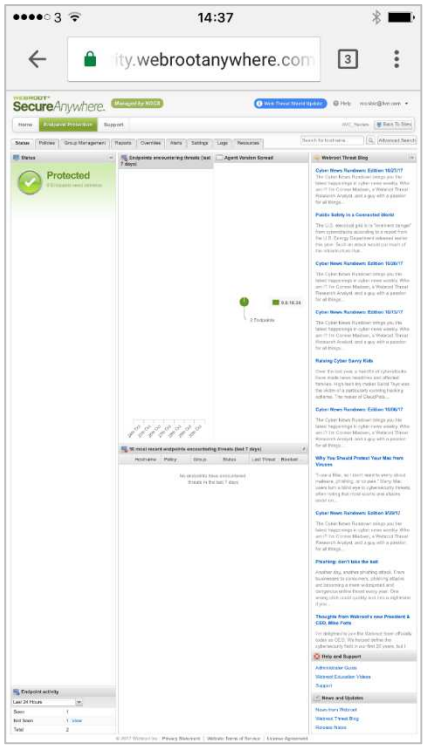
Layout



The row of tabs along the top of the console includes links to the pages *Status* (=home), *Policies*, *Group Management*, *Reports*, *Overrides*, *Alerts*, *Settings*, *Logs* and *Resources*. The left-hand column can be collapsed to provide more space to show the main panels.

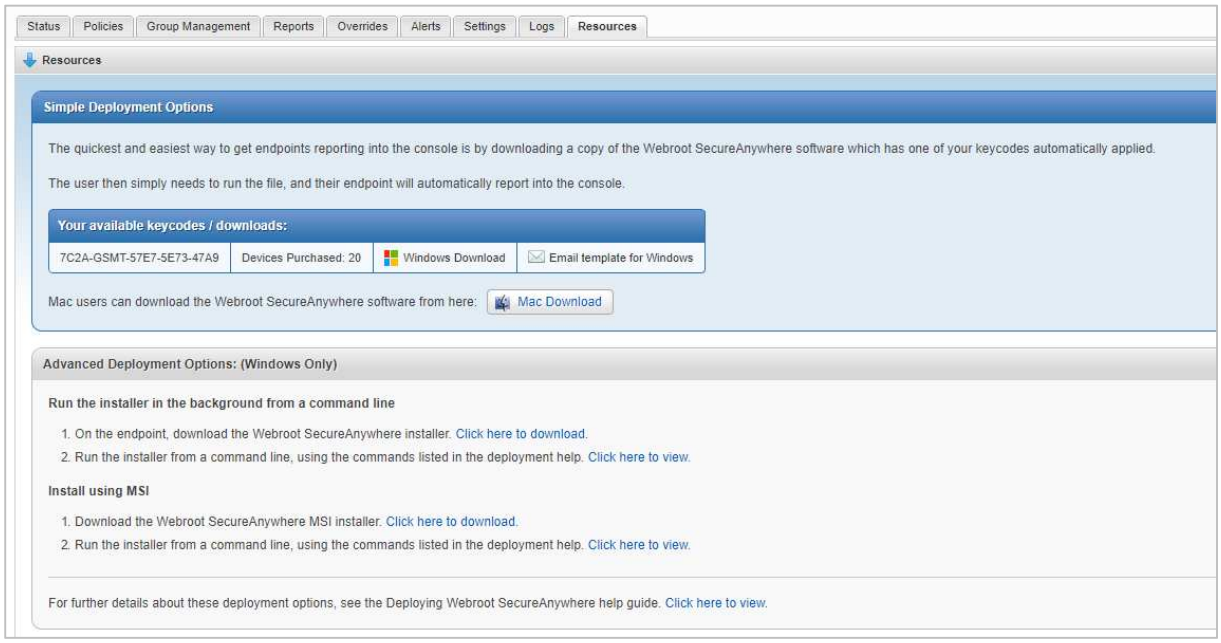
Use with tablet or smartphone

Webroot's console does not adapt when displayed on small touchscreen devices; this means that more or less the entire page is shown, making text too small to read and menu items too small to tap, unless the page is reoriented/zoomed:



Deployment of endpoint protection software

Deployment options can be found on the *Resources* tab:



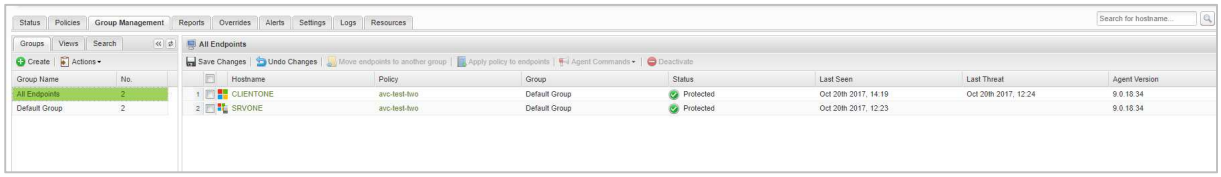
Monitoring the network

Status and alerts

The *Status* (home) page of the console shows the overall security status, endpoints encountering threats, 50 most recent endpoints encountering threats, and agent version spread. Alerts are shown on the tab of the same name.

Program version

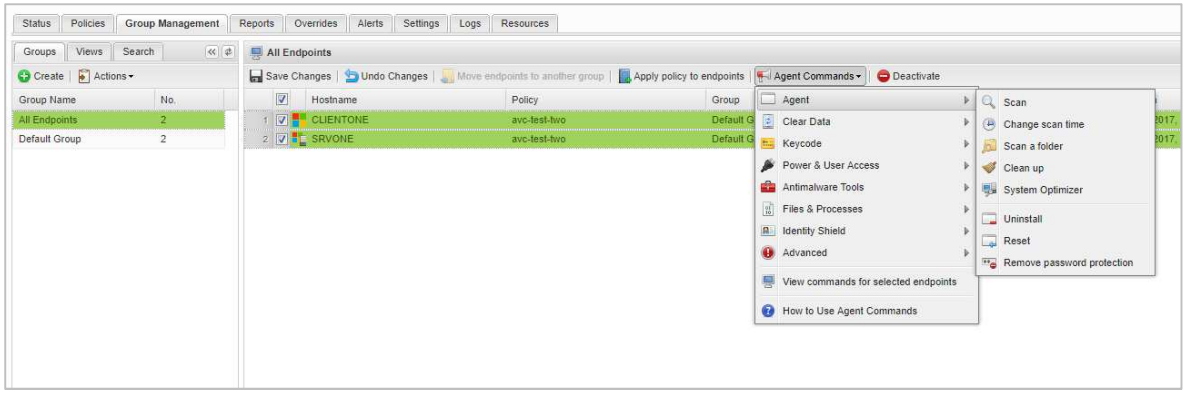
This can be seen by going to the *Group Management* page and clicking on the relevant group. Details of individual computers, including program version, are shown in the top pane:



Managing the network

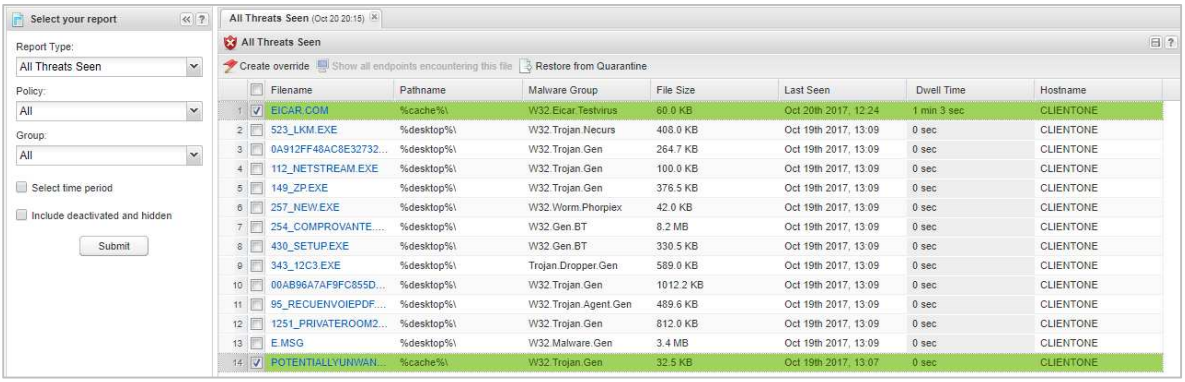
Scanning, scheduling scans, updates and removing devices from the console

By selecting a computer or computers on the *Group Management* page, and clicking the *Agent Commands* menu, the admin can schedule or run a scan, or uninstall the agent (client software):



Quarantine

The Webroot console does not actually have a feature called "quarantine". However, by going to the *Reports* page and searching for *All Threats Seen*, the admin can find details of items quarantined on endpoints, and restore them if necessary:



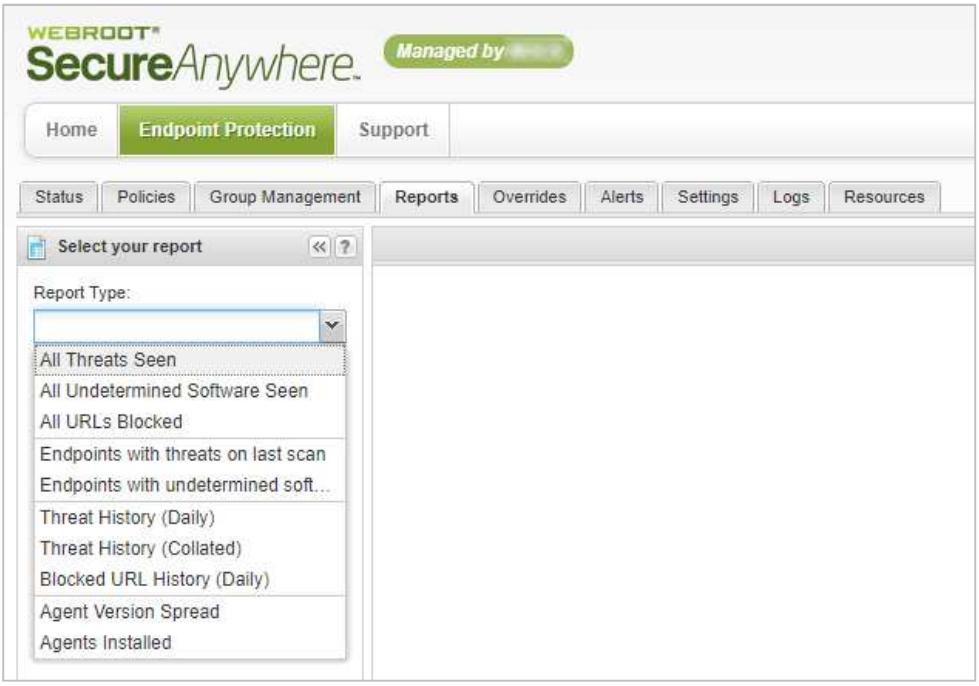
Policies

These are accessed by the tab of the same name in the row along the top of the console.

We did not initially find the policies feature very easy to use. It was simple enough to create and edit a new policy, but not immediately clear how to assign the new policy to a device or site.

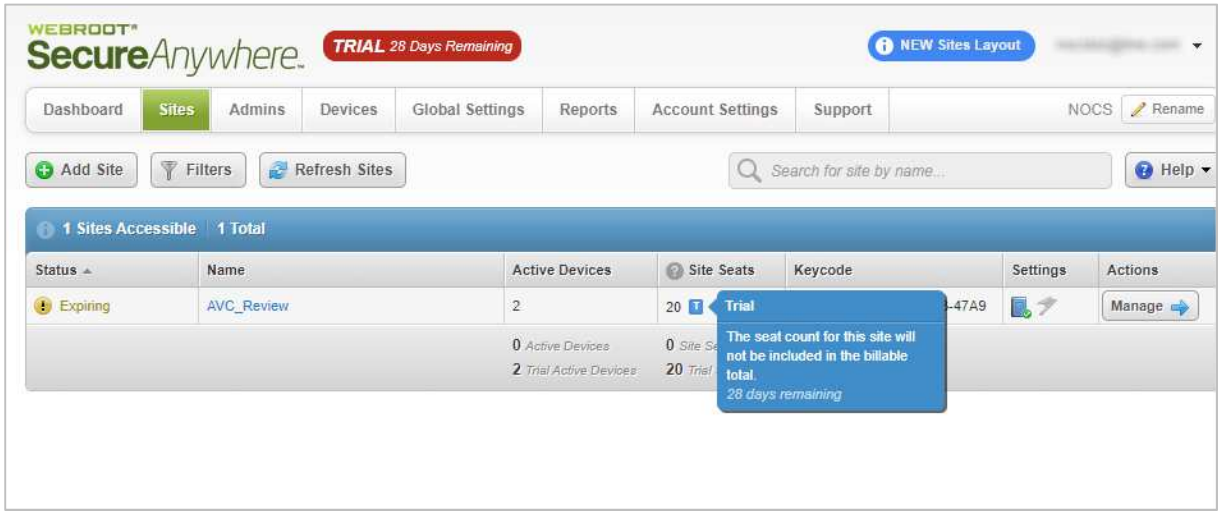
Reports

Clicking the *Reports* tab at the top of the console displays a search box with a menu of different report types that can be created:



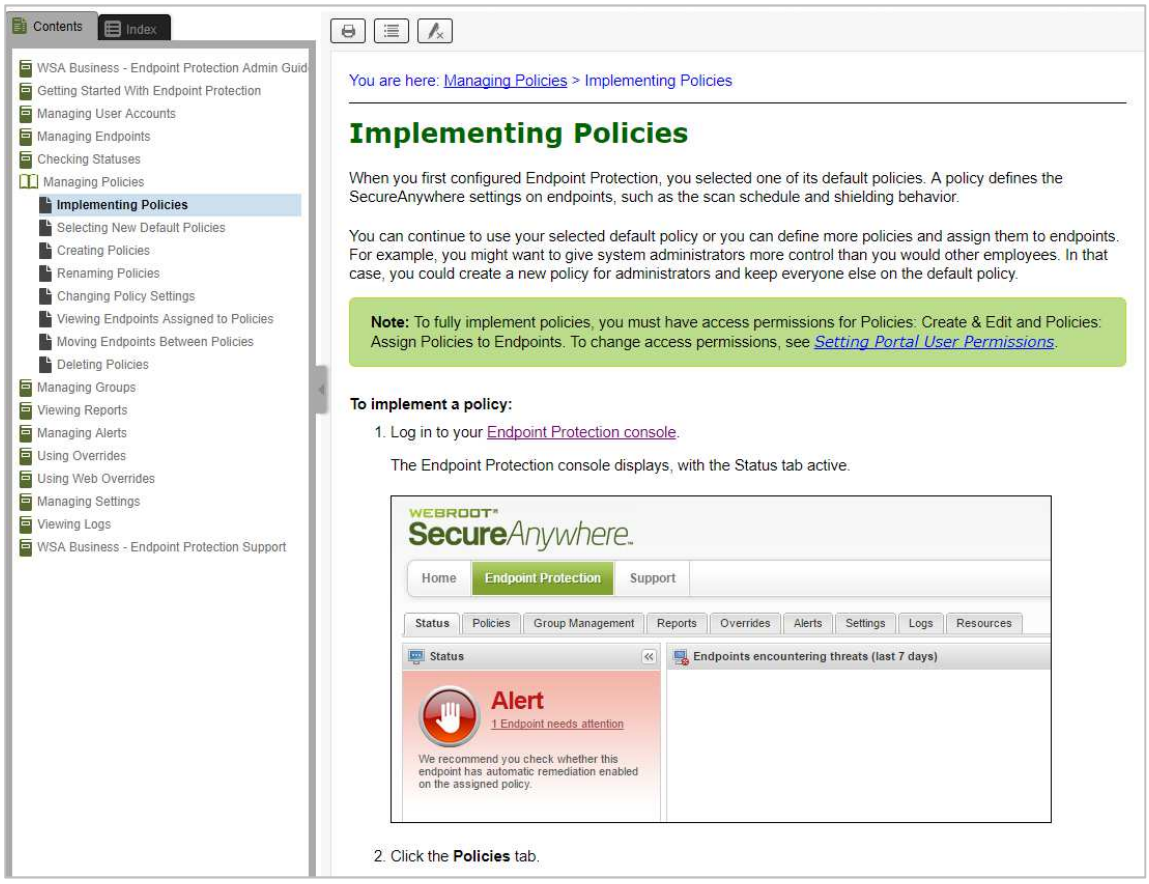
Licences

To view licence information, the admin needs to go to the Global Site Manager (opening page of the console). Available keys and their usage is shown in the site details line:



Integrated console help

Clicking the *? Help* link in the top right-hand corner of the console opens the help feature, which could be described as an online manual:



Windows client endpoint protection software

Installation

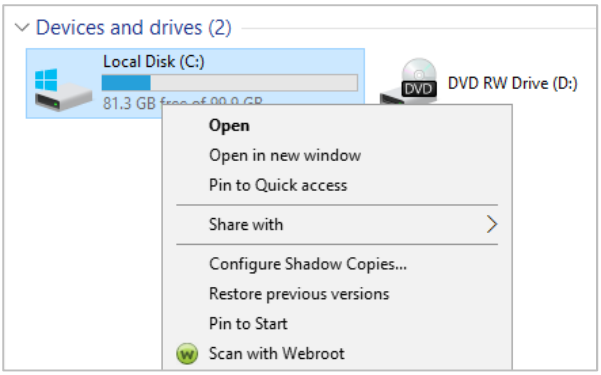
Installation of the client software is very quick and simple, but might prove a little confusing to the inexperienced. The admin runs the installer file and accepts Windows' User Account Control prompt, as normal, but there is no wizard to complete, or indeed any other obvious indication that the program is being installed. However, after a few seconds, sharp-eyed admins will note that a Webroot icon has appeared in the System Tray.

Note regarding default configuration

The default policy for Webroot SecureAnywhere hides the main program window and suppresses malware alerts. That is to say, the default interface is limited to the System Tray menu and context-menu (right-click) scan, and malware is blocked silently, without any notification. However, the administrator can enable a full GUI with the main program window shown further below, and activate malware alerts, by editing the policy applied to client PCs and servers.

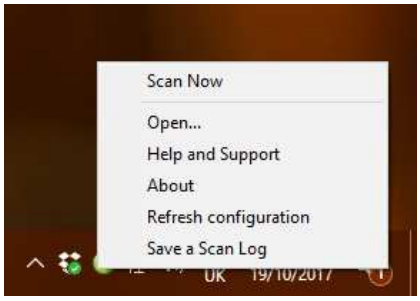
Functionality available in the default configuration

Context menu scan: A scan can be run on a file, folder or drive, by right-clicking it in Windows Explorer, and clicking *Scan with Webroot*:



System Tray menu

Right-clicking the Webroot System Tray icon displays the menu shown below:

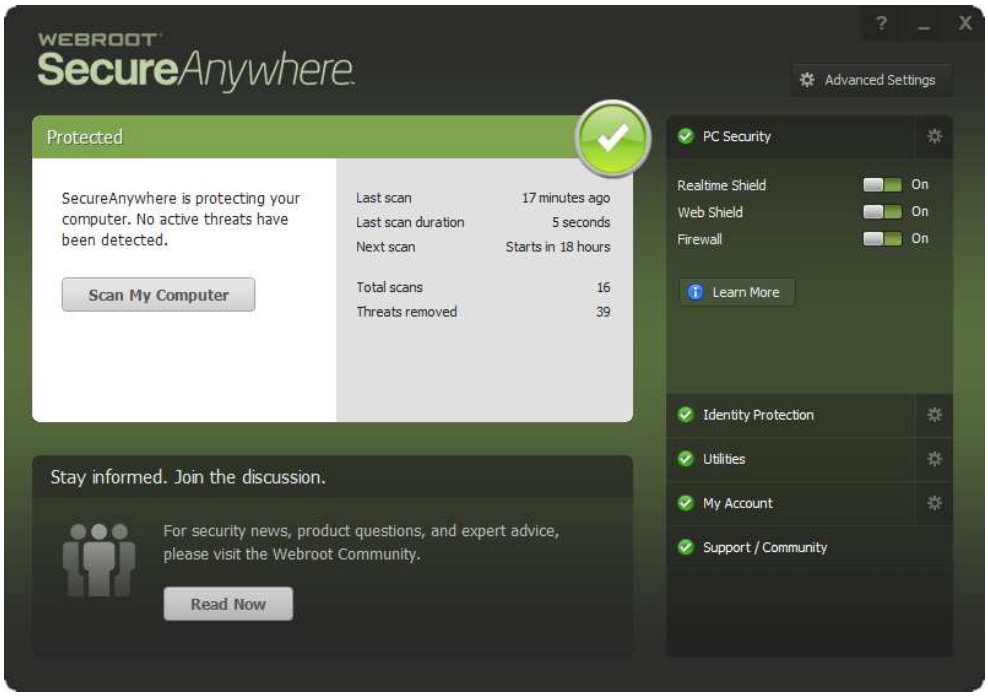


Windows Security Center/Windows Defender

Webroot SecureAnywhere registers with Windows Security Center as the antivirus program. Windows Defender is disabled.

Functionality available if GUI and malware alerts are enabled

Main program window



Security status: This is shown in the form of text and graphic in the main panel of the window. The status of individual components – *Realtime Shield, Web Shield, Firewall* – is shown in the *PC Security* panel on the right-hand side of the window.

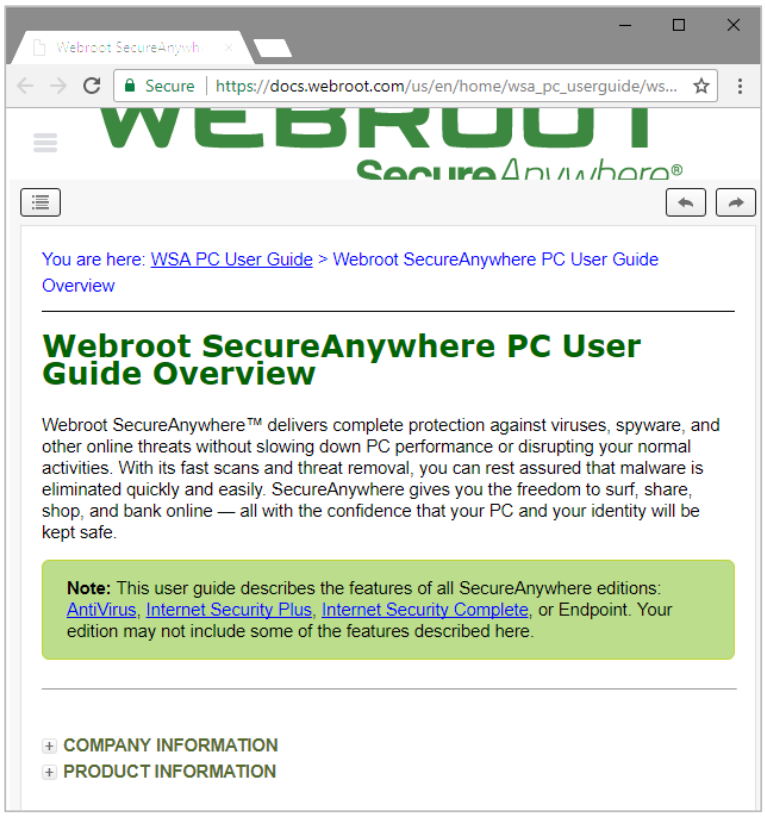
Scans: A default scan can be run from the *Scan My Computer* button in the status panel. Users can run a custom scan by clicking the cogwheel in the *PC Security* panel, then *Scan & Shields, Custom Scan*:

This page also displays a simple **scan log**. The *Block/Allow* tab of the same dialog allows exceptions to be set, while **quarantine** can be found under the tab of the same name.

Updates: as the product uses cloud-based signatures, an update function is not necessary.

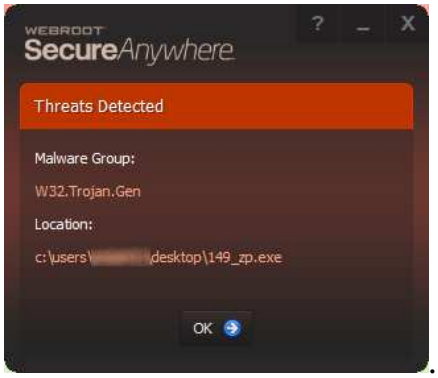
Settings can be opened by clicking *Advanced Settings* in the top right-hand corner of the window. There is also a separate scan settings dialog, which can be opened by clicking the cogwheel symbol in the top right-hand corner of the *PC Security* panel.

Help: clicking the *?* symbol in the top-right corner opens the program's online help pages:



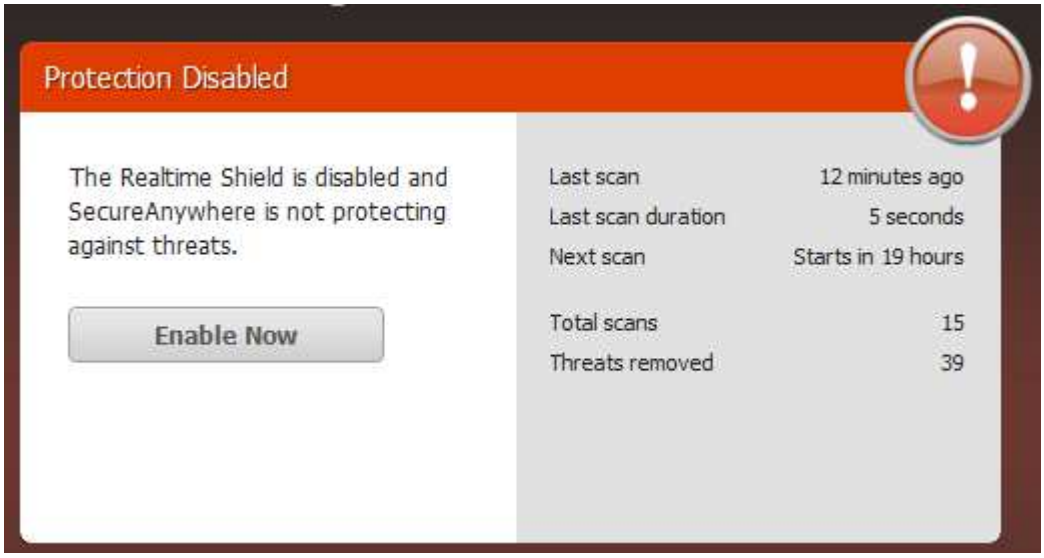
Alerts

If malware alerts are enabled via policy, and the EICAR test file is downloaded, the alert below is shown:



In our test, the AMTSO Phishing Test Page was not blocked.

If real-time protection is disabled, the status display in the main program window changes to show an alert:



Even with the GUI enabled, users cannot switch protection on or off, so the *Enable Now* button is redundant. We could not find a means of changing the policy in the console to allow users to change the configuration of the program themselves.

Windows Server endpoint protection software

This can be regarded as identical to the client software.

Copyright and Disclaimer

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

AV-Comparatives (November 2017)