Anti-Virus Comparative

Comparison of cloud management consoles

Language: English
July 2016

Last Revision: 30th August 2016

www.av-comparatives.org

Table of Contents

Executive Summary

For SMB companies and service providers, it's important to have simple, effective security solutions that don't require enterprise-level skills for IT staff to manage.

Of the six solutions reviewed for this comparison, Kaspersky Endpoint Security Cloud is both simple to use and a perfect fit for the requirements of such companies. In the usability scenarios review, it demonstrated clear ease of use in management capabilities.

Criteria	Kaspersky Lab	Symantec	Sophos	Trend Micro	Bitdefender	McAfee
(1) Trial	●●●	●●●	●●○	●●●	●●○	●●○
(2) Distribution	●●●	●●●	●●●	●●●	●●●	●●●
(3) Deployment	●●●	●●○	●●●	●●○	●○○	●○○
(4) Settings	●●●	●●●	●●○	●○○	●●○	●○○
(5) Policies	●●●	●●○	●●●	●●○	●●○	●●○
(6) Simplicity	●●●	●●●	●○○	●●●	●●●	●○○
Total points (out of 18)	18	16	14	14	13	10

Description of usability criteria

1. Ability to access **trial** version of product for end-users (i.e. IT administrators) and MSP's – multi-tenancy support.

2. Single **distribution** package. This feature allows automatic detection of operating system type (32- or 64-bit Microsoft OS) and deploys the appropriate distributive on the endpoint.

3. Full installation package. For endpoints with slow internet connections, allows protection **deployment** from a removable drive.

4. Customization of connection **settings.** Needed to specify proxy server configuration before product deployment on endpoints.

5. Support for user-based and device-based **policies** – for flexible protection settings based customer requirements.

6. **Simplicity** of use for product's management console: doesn't require advanced administrator skills (doesn't use hierarchy or inheritance of security policies).

Introduction

The use of cloud-based management consoles for business security products is becoming more and more popular. These consoles have the advantage of being installation and maintenance-free, and don't require additional company resources (such as a server) to operate. They require no further on-premise security measures, such as firewall configuration, and work equally well on devices inside and outside the company LAN – a significant advantage in the era of mobile computing and an obvious benefit for companies with mobile or remote workforces.

Because they facilitate the management of multiple networks from a single console, cloud-based consoles are also ideal for managed service companies looking after the IT infrastructure of customers who don't have their own IT staff.

This review considers the capabilities of six popular cloud-based security management consoles and assesses their suitability for use by both internal, non-technical staff and managed service providers who take care of IT for multiple client companies.

This review was commissioned by Kaspersky Lab, who asked us to assess ease-of-use criteria for six business endpoint protection products with cloud-based management consoles.

Tested products

For this review, we used the latest publicly available version (as of July 2016) of the following products:

- Bitdefender GravityZone Business Security (SaaS deployment)
- Kaspersky Endpoint Security Cloud
- McAfee Endpoint Protection Advanced for SMB
- Sophos Cloud Endpoint Protection Bundle
- Symantec Endpoint Protection Small Business Edition
- Trend Micro Worry-Free Services

Usability Criteria

1. When signing up for a trial version of the product, can users specify whether they're an end user or an IT service provider that will manage the product on behalf of a client? Three points are awarded for products that allow managed service providers to specify when signing up; two points are awarded for products offering a post-registration configuration facility for managed service providers.

2. Does the product provide a single installer to deploy the endpoint protection software[1] to any supported Windows client? Three points are awarded to products that do this.

3. Is the installer available as a single, complete, self-contained package (as opposed to a downloader) that could be used to set up endpoint protection on a client PC without an Internet connection? Products that provide this option score three points. If additional actions are required to prepare distributive – two points. One point is assigned to vendors offering only a downloader.

4. If necessary, is it possible to pre-configure the installer file to include customised proxy settings for the update server? Three points are awarded to products that allow this. Two points are awarded to products that support proxy settings customization, but through the command line / during package creation. One point assigned to vendors that don't provide settings customization.

5. Can configuration policies be applied to devices, users, or both? Products that allow policies to be applied to both users and devices receive three points. Two points for products that allow *either* device-based *or* user-based policies only.

6. Is the scope of policy configuration suitable for a small business with a simple IT infrastructure and no full-time IT professional to manage it? To qualify for a point here, a product must use self-contained policies rather than a hierarchy of interdependent policies. Three points are awarded for simple-to-manage solution, one point for complicated hierarchical management.

Please note that the scope of this review is limited to the protection test and specific usability criteria listed above, and does not cover any other factors such as impact on system performance. We recommend that readers consult other relevant tests/reviews by reputable organizations.

---

[1] Please note that other systems, such as Windows servers and Mac OS X clients, are excluded from this requirement.

Detailed usability scenarios

1. **Multitenancy support: obtaining a trial version of the product for end-users (company IT administrators) and managed service providers**
   This allows IT administrators to try the product for their own internal use, and also managed service providers to set up a trial for their clients. The latter enables an MSP to manage multiple companies from one console.

   Products which do not allow for MSPs score no points. Products which allow MSPs to set up multiple companies but only after validation or on request score half a point. Products that allow multiple companies to be set up by an MSP from the start score one point.

Kaspersky Lab	Symantec	Sophos	Trend Micro	Bitdefender	McAfee
●●●	●●●	●●○	●●●	●●○	●●○

2. **Single distribution package**
   This enables the administrator to install the relevant product on all client computers without having to consider whether a 32 or 64-bit version is required, or whether the client is running e.g. Windows 7, 8 or 10. One point is given for products which provide such an installer.

Kaspersky Lab	Symantec	Sophos	Trend Micro	Bitdefender	McAfee
●●●	●●●	●●●	●●●	●●●	●●●

3. **Full installation package**
   A full installation package contains the entire software needed to install the endpoint protection on a client computer, as opposed to a downloader which has to take the code from a cloud server each time. The obvious benefit to a full installer is that it can install the product from e.g. a USB flash drive, with either a slow Internet connection or none. One point is given to products which provide this.

Kaspersky Lab	Symantec	Sophos	Trend Micro	Bitdefender	McAfee
●●●	●●○	●●●	●●○	●○○	●○○

4. **Connection settings customization**
   If a company uses a proxy server which is used by the endpoint protection product to download definition updates, it is a clear advantage if this can be specified when creating the installer, making installation faster for experienced admins and easier for standard users who install the software themselves.
   Products that allow proxy server settings to be specified when creating an installer score one point. Products which allow proxy server settings to be specified under some circumstances – e.g. only a particular type of installer – score half a point.

Kaspersky Lab	Symantec	Sophos	Trend Micro	Bitdefender	McAfee
●●●	●●●	●●○	●○○	●●○	●○○

5. **User-based and device-based policies supported for flexible protection settings depending on customer`s requirements.**

   Business security software traditionally provides policies which are applied to specific devices. In companies where employees may use multiple devices – e.g. desktop PC, laptop PC, tablet and mobile phone – it makes more sense to apply the policy (permissions etc.) to the user rather than the device. Products which allow device-based and user-based policies score one point; products which allow EITHER device-based OR user-based policies score half a point.

Kaspersky Lab	Symantec	Sophos	Trend Micro	Bitdefender	McAfee
●●●	●●○	●●●	●●○	●●○	●●○

6. **Non-hierarchical policies.**

   For a small business without full-time IT staff, non-hierarchical policies without inheritance are much easier to understand and apply. Products with simple, non-hierarchical policies score one point here.

Kaspersky Lab	Symantec	Sophos	Trend Micro	Bitdefender	McAfee
●●●	●●●	●○○	●●●	●●●	●○○

Total score

	Kaspersky Lab	Symantec	Sophos	Trend Micro	Bitdefender	McAfee
Total score (out of 18)	18	16	14	14	13	10

Conclusion

In terms of the usability criteria specified, Kaspersky Lab is the clear winner, being the only product to score maximum points in all scenarios.

Criteria	Kaspersky Lab	Symantec	Sophos	Trend Micro	Bitdefender	McAfee
(1) Trial	●●●	●●●	●●○	●●●	●●○	●●○
(2) Distribution	●●●	●●●	●●●	●●●	●●●	●●●
(3) Deployment	●●●	●●○	●●●	●●○	●○○	●○○
(4) Settings	●●●	●●●	●●○	●○○	●●○	●○○
(5) Policies	●●●	●●○	●●●	●●○	●●○	●●○
(6) Simplicity	●●●	●●●	●○○	●●●	●●●	●○○
Total points (out of 18)	18	16	14	14	13	10

Bitdefender GravityZone Business Security SaaS

1. Obtaining a trial version of the product for administrators and MSPs

The trial is available directly from the product information/purchase page. There is no obvious distinction between a trial for company internal use and for MSP use. Under *My Company*, the console does however have the option *allow your partner to assist with the security management of this company*. We would argue that this partly fulfils the criterion of setting up a trial for both in-company and managed service-provider use, and so award Bitdefender GravityZone two points.

2. Initial protection deployment, single distribution package

When the administrator logs on to the console, two introductory screens are shown. The second of these includes buttons for installing the endpoint protection software on the local computer, or emailing links to users so that they can install the software themselves. Clicking *Install on this computer now* downloads a 3 MB installer, which downloads the appropriate version of the endpoint security software for the local computer. In our view, this entirely meets the criterion of a single installation package for all platforms being available, and Bitdefender thus receives three points.

3. Initial protection deployment, full installation package

A full installer package can be created (the system automatically makes OS-specific versions of this) and then downloaded from the console, by going to the *Packages* page and clicking *Download*. We note that whilst the admin only needs to *create* a single installation package, there are multiple options for *downloading* it, and thus the criteria of a single distributable installer is not fulfilled. As a result, Bitdefender score one point.

4. Connection settings customization for deployment package

If the endpoint protection software is installed by clicking the *Install on this computer* now button in the introductory pages, there is no option to specify connection settings. A proxy server *can* be specified when creating an installation package. Bitdefender GravityZone only partly meets the criterion for specifying connection settings, and so receives two points.

5. User- and device-based security policies

Bitdefender GravityZone allows policies to be applied to computers, but not to users. Consequently, it only receives two points for this criterion.

6. Easy management of security policies

The GravityZone management console allows a policy to be edited from a single page, using a left-hand menu column with which the administrator can switch between components of the policy. There is no hierarchy of policies or inheritance from one to another. We thus regard the criterion of simple policy management as fully met, and award Bitdefender three points.

Summary
Bitdefender GravityZone receives a total of 13 points out of a possible total of 18.

Kaspersky Endpoint Security Cloud

1. Obtaining a trial version of the product for administrators and MSPs

When the admin has created the main account which provides access to the console, the *Add Company* link can be used to create one or more companies, allowing an IT service company to create a separate sub-account for each of their clients. Kaspersky Lab thus receives three points for this criterion.

2. Initial protection deployment, single distribution package

The *Download* button on the *Distribution packages* page of the console downloads an installer file that can be used for all compatible systems. The only choice the admin has to make is whether to specify proxy server settings (see point 4 below). Kaspersky Lab meets the requirements for a single installer and receives three points.

3. Initial protection deployment, full installation package

The installer file downloaded as described above is a complete package of approximately 331 MB which does not need to download further components. This meets the criterion for this point, so Kaspersky Lab receives three points here.

4. Connection settings customization for deployment package

There is a button next to the one for package download that allows the admin to specify proxy settings before creating the package.

This meets the criterion perfectly, and so Kaspersky Lab receives three points.

5. User- and device-based security policies

Kaspersky Lab Endpoint Security Cloud allows policies (*Security Profiles*) to be assigned to users as well as devices.

This meets the relevant test criterion and thus Kaspersky Lab receives three points.

6. Easy management of security policies

Security policies are independent of each other, and each policy can be edited using three sub-pages, accessed from a menu panel on the left-hand side of the page.
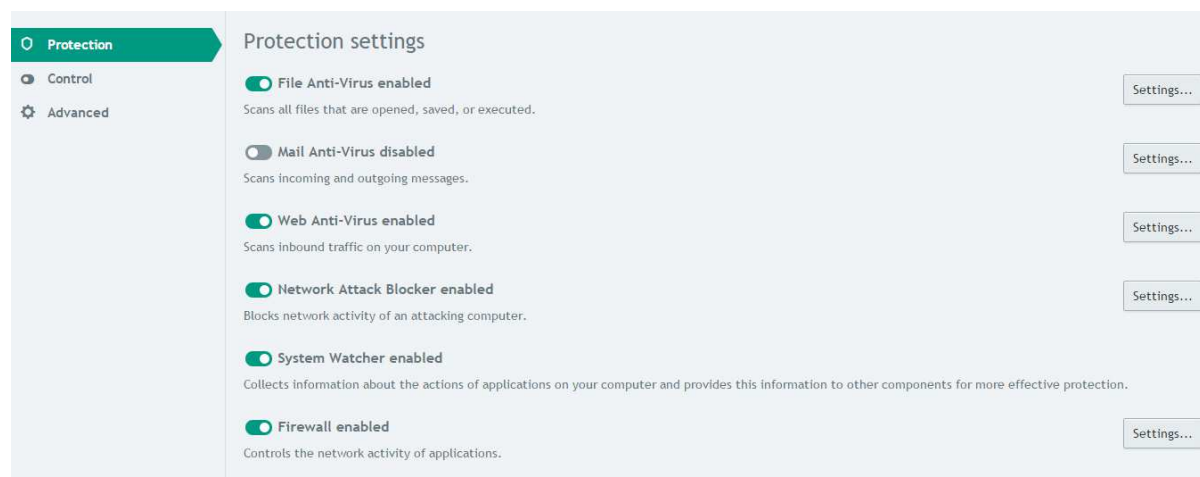
This meets the criterion of easy security-policy management and so Kaspersky Lab receives three points for this item.

Summary

Kaspersky Lab receives a total of 18 points out of a possible total of 18.

McAfee Endpoint Protection Advanced for SMB

1. Obtaining a trial version of the product for administrators and MSPs

McAfee ePolicy Orchestrator allows for management of a company by a managed service provider. However, McAfee provide access to the portal only for authorized partners. Consequently we award McAfee two points here.

2. Initial protection deployment, single distribution package

A single customisable installer is provided by ePolicy Orchestrator, and can be downloaded from the *Getting Started* page. This meets the criterion of a single installer, thus McAfee receives three points here.

3. Initial protection deployment, full installation package

The default installation file is a downloader of 769 KB. This does not meet the requirement for a full installer and so McAfee score one point here.

4. Connection settings customization for deployment package

The default installation package provided by McAfee can be customised, but this does not allow for proxy settings to be configured. Consequently, McAfee receive one point here.

5. User- and device-based security policies

ePolicy Orchestrator allows policies to be assigned to devices (via groups) but not users. Consequently it receives two points for this criterion.

6. Easy management of security policies

ePolicy Orchestrator uses a hierarchy of policies, in accordance with its enterprise focus. As this is contrary to the criterion of very simple, non-hierarchical policies specified for this test, McAfee receive one point here.

Summary

McAfee receives a total of 10 points out of a possible total of 18.

Sophos Endpoint Protection Cloud

1. Obtaining trial version of the product for administrators and MSPs

There is an option to access Sophos Central Partner management console, which supports multitenancy. However, this requires authorisation. Sophos receives two points in this scenario.

2. Initial protection deployment, single distribution package

A single full installer is available for all Windows clients. This satisfies the requirement for a single installation package and Sophos thus receives three points.

3. Initial protection deployment, full installation package

The installer mentioned in point 2 above also satisfies the requirement for a full installer, as opposed to a downloader, and so Sophos scores three points for this item.

4. Connection settings customization for deployment package

The installer package can be customized via command line, and so partially meet the requirement for pre-configuring proxy settings since it require advanced skills for administrator. Sophos does receive two points here.

5. User- and device-based security policies

Policies can be applied to both devices and users, giving Sophos three points here.

6. Easy management of security policies

Sophos uses policy inheritance, meaning that when a policy is placed in top of the list it overrides other policies. This is contrary to the criterion of very simple, non-hierarchical policies specified for this test, and so Sophos receives one point here.

Summary

Sophos receives a total of 14 points out of a possible total of 18.

Symantec Endpoint Protection Small Business Edition

1. Obtaining trial version of the product for administrators and MSPs

There is an option to register for participate in partner program. Symantec score three points in this section.

2. Initial protection deployment, single distribution package

A single installer is available by logging on to the console from the device to be protected, and clicking *Install Now*. Symantec thus scores three points here.

3. Initial protection deployment, full installation package

A 5 MB Package Creator can be downloaded, which can then be used to make a 354 MB full installer package. However, it require additional actions from IT-administrator, thus Symantec receives two points here.

4. Connection settings customization for deployment package

Proxy settings can be specified when creating the deployment package. Three points are awarded to Symantec for this item.

5. User- and device-based security policies

Policies can be applied to groups of computers, but not to individual users or user groups. Symantec thus only scores two points here.

6. Easy management of security policies

Policies are very straightforward and clearly arranged on one page. Symantec scores three points for this.

Summary

Symantec receives a total of 16 out of a possible total of 18 points.

Trend Micro Worry-Free Business Security Services

1. Obtaining trial version of the product for administrators and MSPs

There is a clear option for managed service providers to register as such when signing up for the trial. Trend Micro thus scores three points here.

2. Initial protection deployment, single distribution package

The *Add Devices* page allows the admin to download a single installer for use on the local device. Trend Micro consequently receives three points here.

3. Initial protection deployment, full installation package

There is an option to create a single full installation package, however there are scripts considering to be used for deployment, which require advanced administrator skills. Trend Micro receives two points here.

4. Connection settings customization for deployment package

The Trend Micro Security Agent setup wizard does not provide any configuration options, meaning that custom network settings cannot be specified. Consequently Trend Micro receive one point for this item.

5. User- and device-based security policies

Trend Micro policies (*Global Settings*) can only be applied to devices, not users. The product thus only receives two points here.

6. Easy management of security policies

Management options for policies are shown on 4 different sub-pages, accessed from a row of tabs along the top. There is no hierarchy of policies, and we found the layout very clear and easy to navigate. Consequently we award Trend Micro three points for this item.

Summary

Trend Micro receives a total of 14 points out of a possible total of 18.

Copyright and Disclaimer

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

AV-Comparatives (August 2016)