Independent Tests of
Anti-Virus Software

Kaspersky Endpoint Security Cloud Plus

A feature comparison with seven other cloud-based endpoint solutions

TEST PERIOD: JULY 2021
LAST REVISION: 13TH SEPTEMBER 2021

COMMISSIONED BY: KASPERSKY

WWW.AV-COMPARATIVES.ORG

Executive Summary

This comparative report focuses on security solutions for companies in the SMB segment. There are several aspects to this: basic and advanced protection features, ease of trying out and management, and supported operating systems. Most of the products reviewed in this report provide similar capabilities for essential threat protection. However, additional protection features are important for SMB customers, as is ease of use. With regard to the latter, easy access to a trial version, installation that does not require vendor support, and uniform policies for all platforms, are very relevant.

Kaspersky Endpoint Security Cloud Plus serves as the standard to which the other products in this report are compared. It is a security product aimed at small and medium-sized businesses, that covers all major platforms. It includes a very good complement of basic Windows protection capabilities, such as file-, mail- and web-threat protection. There is also a wide range of advanced Windows protection features, including anti-ransomware with rollback, vulnerability assessment & patch management, device-, web access- and cloud services-access control, Microsoft 365 protection, encryption management, EDR functionality and integrated cybersecurity training.

Introduction

This report was commissioned by Kaspersky. Its purpose is to check whether specific features found in Kaspersky Endpoint Security Cloud Plus (KES Cloud Plus) are included in seven other cloud-managed endpoint protection products for small and medium-sized businesses.

AV-Comparatives have merely verified whether the specified features are available in the products reviewed. We have not tested the features for this review, and so cannot make any statement as to their effectiveness or reliability. The lists of features described here were correct as at the date of writing (July 2021). As vendors constantly update the features in such products, the respective feature sets may be liable to change at any time.

We advise prospective buyers of endpoint security products to decide for themselves which features are most important to their respective businesses before making a purchase. Please note that competitor products might have additional features that are not included in KES Cloud Plus. Naturally, all the vendors have other products in their respective business ranges, and these will have different feature sets from those described here.

Products Reviewed

Kaspersky selected the following products/packages for this comparison. We purchased these in July 2021, so the features described relate to the versions at that time. The selected products/packages are in a similar price range; that is to say, all were within +/- 25% of the average price. This was calculated using prices for 5 users and 1 year, as shown on each vendor's German website, at the time of writing.

- Kaspersky Endpoint Security Cloud Plus
- Bitdefender GravityZone Elite Business Security (cloud-managed)
- ESET Protect Complete
- McAfee Complete Endpoint Protection Business
- Panda Adaptive Defense 360 + ART
- Sophos Central Intercept X Advanced
- Trend Micro Worry-Free Business Security Services Advanced
- Webroot Business Endpoint Protection with DNS Protection and Security Awareness Training

Review criteria

Here we have described the security and management features that Kaspersky asked us to check for in the eight business security products. Terms in bold italics refer to the names used in the tables below.

List of features for Windows client systems specified by Kaspersky

In most companies, Windows desktops and laptops still account for the majority of devices. Features available for such systems will thus be of critical importance. The greater the number of protection layers, the greater the chance that threats can be blocked. We have thus considered Windows client protection features in detail below.

Basic protection capabilities

***File threat protection*:** this is an essential and standard feature of all business security products, needed to prevent malicious files being executed on client systems.

***Mail threat protection*:** email remains a common means of distributing malware and malicious links. It is clearly optimal if such threats can be detected before they even reach the user.

***Web threat protection*:** many attacks use malicious or compromised websites as their starting point. Blocking such threats at source is an optimal first line of defence.

***Desktop firewall*:** whilst current Windows desktop platforms include the Windows Firewall to prevent malicious connections to the PC, a third-party firewall can provide more features and management options.

HIPS (host intrusion prevention system): this helps prevent infection of a client PC, by analysing programs and their behaviour.

Advanced protection capabilities

***Anti-ransomware*:** ransomware has become a major threat to organisations, as it can render their private data unusable. An effective means of blocking it has become critically important. Whilst any antimalware program should detect ransomware executable files on access or on execution, this report refers to specific anti-ransomware measures, such as protection against malicious encryption.

***Ransomware rollback*:** in the event that a ransomware attack succeeds in encrypting company data, mitigating this is a vital last line of defence. The ability to undo the actions of the ransomware in such cases will prevent the attack turning into a disaster.

***Vulnerability assessment & Patch management*:** many malware attacks rely on exploiting vulnerabilities in outdated software on the client PC. Identifying any such programs being used on company computers allows the system administrator to proactively close the gap in the defences. When vulnerabilities have been detected, updating the programs concerned to more secure versions is vitally important. Patch management enables this to be done quickly and with minimal effort required by IT staff. Whilst the Windows operating system is included among the software that should be assessed for available patches, the reviewed products would be expected to cover third-party applications as well for the feature to count in this review.

***Device Control*:** one of the ways that malware can be introduced into a company network is via employees using their own removeable devices, such as USB flash drives. Device control allows the system administrator to block the use of such devices, hence stopping the threat.

***Web Access Control*:** this ensures that an organisation's staff do not access inappropriate websites while at work. Additionally, administrators could make use of this feature to improve protection against phishing attacks.

***Cloud services access control*:** this limits access to unauthorised public cloud services (which fall under Gartner's definition of "Shadow IT"[1]), thus increasing security and productivity.

***Microsoft 365 protection*:** Microsoft's cloud-based 365 service for business includes managed email and file storage facilities, and is becoming very widely used by businesses of all sizes. Detection of malware and malicious links sent via these services will stop these threats at source.

***Encryption management*:** encrypting the system drives of company computers means that the data on them cannot be read in the event that the device is lost or stolen. Clearly this is of particular importance for Windows laptops and tablets. Whilst the encryption technology itself is built into Windows (BitLocker), the ability to manage this encryption centrally makes it much easier to for the IT manager to ensure all devices are appropriately protected.

Integrated root cause analysis (EDR): today, advanced persistent threats (APTs) are becoming more common and more dangerous. These targeted multi-stage attacks are highly sophisticated and potentially catastrophic for the victim. The ability to detect, investigate and remediate such threats is thus essential to modern businesses. Endpoint detection and response (EDR) features allow IT staff to fully understand the nature of such attacks, thus blocking current ones and helping to protect against possible future threats.

***Integrated cybersecurity training*:** the motto "Prevention is better than cure" is highly applicable to IT security. An obvious means of preventing attacks is to educate company staff, so that they can understand how best to recognise any signs of an attack that they encounter, thus helping prevent it from causing business disruption or financial losses.

[1] https://www.gartner.com/en/information-technology/glossary/shadow

Supported Operating Systems

In most businesses, there will be a variety of different platforms in use. Windows Server, Windows desktop, macOS, Android and iOS devices are all commonplace. Clearly, the more platforms a product supports, the greater the overall protection will be.

Ease of Trying Out and Management

The ability to try out a product before purchasing it will be regarded as essential by most IT departments. Only by testing a solution in real life can the system administrator find out how well it suits the specific requirements of the business.

Trial/demo available immediately means that the administrator does not have to wait for a response from the vendor before they can start exploring the product. Even if contact details are requested, the trial or demo will be provided instantly once these details have been submitted. This allows the administrator to proceed with the evaluation immediately, and means that unnecessary and time-consuming discussions with the vendor can be avoided.

A further help when evaluating a product is being able to find the cost of the product immediately. ***Pricing displayed on website*** means that the administrator can find costs for default numbers of licences without having to make an enquiry. This speeds up the evaluation process for the product.

Having purchased a product, the administrator will need to deploy the endpoint protection software to client devices and configure settings and alerts etc. ***Easy installation without requiring vendor support*** means the product is intuitive enough that an administrator who is not already familiar with the product can complete this process without requiring assistance from the vendor.

Single security policy for all platforms means that the administrator can define protection settings that will be applied to all supported platforms. This simplifies the initial protection-setup and security-management tasks.

Features and Platform Support

Windows Client Features

	Kaspersky	Trend Micro	Bitdefender	ESET	Panda	Sophos	Webroot	McAfee
Basic protection capabilities								
File threat protection	●	●	●	●	●	●	●	●
Mail threat protection	●	●	●	●	●	○	○	●
Web threat protection	●	●	●	●	●	●	●	●
Desktop firewall	●	○	●	●	○	○	○	●
HIPS	●	●	●	●	●	●	●	●
Advanced protection capabilities								
Anti-ransomware	●	●	●	●	○	●	●	○
Ransomware rollback	●	●	●	○	○	●	○	○
Vulnerability assessment & Patch mgmt	●	○	○	○ **	○	○	○	○
Device control	●	●	●	●	●	●	○	○
Web access control	●	●	●	○	●	●	○	●
Cloud services access control	●	○	○	○	○	○	○	○
Microsoft 365 protection	●	●	○	●	○	○	○	○
Encryption management	●	●	○	●	○	○	○	●
Integrated root cause analysis (EDR)	●	●	●	○	●	●	◑ ***	●
Integrated cybersecurity training	●	○	○	○	○	○	●	○

Key

● Feature present

○ Feature not present

◑ Feature present but with limitations, please see further notes below

* Not available in cloud management option, only in on-premises option

** Vulnerability assessment / Patch management for Windows Updates, but not for 3rd-party applications

*** Limited functionality

Supported Operating Systems

	Kaspersky	Trend Micro	Bitdefender	ESET	Panda	Sophos	Webroot	McAfee
Windows Desktop	●	●	●	●	●	●	●	●
Windows Server	●	●	●	●	●	○	●	●
macOS	●	●	●	●	●	●	●	●
Android	●	●	○ *	●	●	○	○	○ *
iOS	●	●	○ *	◑ **	○	○	○	○ *

Ease of Trying Out and Management

	Kaspersky	Trend Micro	Bitdefender	ESET	Panda	Sophos	Webroot	McAfee
Trial/demo of entire product available immediately	●	●	●	●	●	●	●	○
Pricing displayed on website	●	●	●	●	○	○	●	○
Easy installation without requiring vendor support	●	●	●	●	●	●	●	○
Single security policy for all platforms	●	●	●	○	●	●	●	●

Key

● Feature present

○ Feature not present

* Not available in cloud management option, only in on-premises option

** Management only

Product summaries

Here we have provided a summary of each product, including the number of specified features it has.

Kaspersky Endpoint Security Cloud Plus is a security product aimed at small and medium-sized businesses covering all major platforms. It includes EDR, patch management, vulnerability assessment, anti-ransomware with rollback. Naturally, it represents the criteria defined by Kaspersky for this review. Thus it is the only product to include all 24 of the protection, security management and training features within the one license. We note that even so, it is only in the average price range for the products reviewed. Its cloud services access control is unique among the reviewed products.

Trend Micro Worry-Free Business Security Services Advanced has 20 out of 24 of the specified features. It offers a full range of supported platforms and trialling/management features. However, it misses some advanced features, e.g. for dealing with vulnerabilities.

Bitdefender GravityZone Elite Business Security includes 17 out of 24 of the specified features. These include basic protection capabilities and EDR functionality, as well as all the designated trialling and management features. It does not cover mobile platforms with its cloud-managed console though. It also misses vulnerability-assessment and patch-management features.

ESET Protect Complete provides good platform support and 16.5 of the specified 24 features. It is at the higher end of the price range among the products in this report. ESET supplies encryption management for its own encryption technology. However, it lacks some of the more advanced protection features, such as web access control and EDR functions.

Panda Adaptive Defense 360 + ART has 14 out of 24 specified features. It supports most platforms, and provides web-access and device controls, as well as EDR functionality. A very realistic online demo is available immediately. However, the product misses some basic and some advanced protection features.

Sophos Central Intercept X Advanced has 13 of 24 specified features. It supports Windows desktop and macOS devices, and includes device & web controls and EDR functionality. It requires an additional licence for other platforms, and lacks vulnerability-assessment and patch-management features.

Webroot Business Endpoint Protection with DNS Protection and Security Awareness Training includes 12.5 out of 24 specified features. It includes the most basic protection features, and simple EDR functionality. Aside from the latter, there are no advanced protection features, however. It has no support for mobile platforms, but does include security awareness training.

McAfee Complete Endpoint Protection Business has 12 of the specified features. It is at the lower end of the price range for products in this report. It protects Windows Server, Windows client and macOS clients with the cloud console. Whilst it includes most of the basic protection features, the cloud-managed product lacks many of the advanced features such as web access control. No trial version or demo is available other than via request to the vendor. We would say that an administrator who is not already familiar with McAfee business products will almost certainly require help from the vendor's support service in order to deploy and configure the product.

Copyright and Disclaimer

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

AV-Comparatives
(September 2021)