

Independent Tests of Anti-Virus Software



Business Security Test

TEST PERIOD: AUGUST – NOVEMBER 2020
LANGUAGE: ENGLISH
LAST REVISION: 10TH DECEMBER 2020

WWW.AV-COMPARATIVES.ORG

Content

INTRODUCTION	3
TESTED PRODUCTS	4
SETTINGS	5
MANAGEMENT SUMMARY	7
AV-COMPARATIVES' APPROVED BUSINESS PRODUCT AWARD	9
REAL-WORLD PROTECTION TEST (AUGUST-NOVEMBER)	10
MALWARE PROTECTION TEST (SEPTEMBER)	15
PERFORMANCE TEST (NOVEMBER)	17
REVIEWS	22
<i>ACRONIS CYBER PROTECT CLOUD – ADVANCED EDITION</i>	23
<i>AVAST BUSINESS ANTIVIRUS PRO PLUS</i>	27
<i>BITDEFENDER GRAVITYZONE ELITE SECURITY</i>	31
<i>CISCO ADVANCED MALWARE PROTECTION FOR ENDPOINTS - ADVANTAGE</i>	36
<i>CROWDSTRIKE FALCON PRO</i>	41
<i>CYBEREASON DEFENSE PLATFORM ENTERPRISE</i>	44
<i>ELASTIC ENDPOINT SECURITY</i>	49
<i>ESET ENDPOINT PROTECTION ADVANCED CLOUD WITH CLOUD ADMINISTRATOR</i>	53
<i>FIREEYE ENDPOINT SECURITY</i>	57
<i>FORTINET FORTICLIENT WITH EMS, FORTISANDBOX AND FORTIEDR</i>	61
<i>G DATA ANTIVIRUS BUSINESS</i>	65
<i>K7 CLOUD ENDPOINT SECURITY</i>	69
<i>KASPERSKY ENDPOINT SECURITY FOR BUSINESS (KESB) - SELECT</i>	73
<i>MICROSOFT DEFENDER WITH MICROSOFT ENDPOINT MANAGER</i>	77
<i>PANDA ENDPOINT PROTECTION PLUS ON AETHER</i>	81
<i>SOPHOS INTERCEPT X ADVANCED</i>	85
<i>SPARKCOGNITION DEEPAARMOR ENDPOINT PROTECTION PLATFORM</i>	89
<i>VIPRE ENDPOINT SECURITY CLOUD</i>	93
<i>VMWARE CARBON BLACK CLOUD</i>	97
FEATURE LIST	101
COPYRIGHT AND DISCLAIMER	102

Introduction

This is the second half-year report of our Business Main-Test Series¹ of 2020, containing the results of the Business Real-World Protection Test (August-November), Business Malware Protection Test (September), Business Performance Test (November), as well as the Product Reviews.

The test series consists of three main parts:

The **Real-World Protection Test** mimics online malware attacks that a typical business user might encounter when surfing the Internet.

The **Malware Protection Test** considers a scenario in which the malware pre-exists on the disk or enters the test system via e.g. the local area network or removable device, rather than directly from the Internet.

In addition to each of the protection tests, a **False-Positives Test** is conducted, to check whether any products falsely identify legitimate software as harmful.

The **Performance Test** looks at the impact each product has on the system's performance, i.e. how much it slows down normal use of the PC while performing certain tasks.

To complete the picture of each product's capabilities, there is a **user-interface review** included in the report as well.

Some of the products in the test are clearly aimed at larger enterprises and organisations, while others are more applicable to smaller businesses. Please see each product's review section for further details.

Kindly note that some of the included vendors provide more than one business product. In such cases, other products in the range may have a different type of management console (server-based as opposed to cloud-based, or vice-versa); they may also include additional features not included in the tested product, such as endpoint detection and response (EDR). Readers should not assume that the test results for one product in a vendor's business range will necessarily be the same for another product from the same vendor.

¹ Please note that the results of the Business Main-Test Series cannot be compared with the results of the Consumer Main-Test Series, as the tests are done at different times, with different sets, different settings, etc.

Tested Products

The following business products² were tested under Microsoft Windows 10 1909 64-bit:

Vendor	Product	Version August	Version September	Version October	Version November
Acronis	Cyber Protect Cloud – Advanced Edition	20.8	20.9	20.10	20.11
Avast	Business Antivirus Pro Plus	20.5	20.6	20.7	20.8
Bitdefender	GravityZone Elite Security	6.6	6.6	6.6	6.6
Cisco	AMP for Endpoints - Advantage	7.2	7.2	7.2	7.3
CrowdStrike	Falcon Pro	5.36	5.40	5.41	6.13
Cybereason	Defense Platform Enterprise	20.1	20.1	20.1	20.1
Elastic	Endpoint Security	3.53	3.53	3.53	3.53
ESET	Endpoint Protection Advanced Cloud ³ & CA	7.2	7.2	7.2	7.3
FireEye	Endpoint Security	32.30	32.30	32.30	32.30
Fortinet	FortiClient with EMS, FortiSandbox & FortiEDR	6.4	6.4	6.4	6.4
G Data	AntiVirus Business	14.3	14.3	14.3	15.0
K7	Enterprise Security	14.2	14.2	14.2	14.2
Kaspersky	Endpoint Security for Business - Select	11.4	11.4	11.4	11.5
Microsoft	Defender ATP's Antivirus	4.18	4.18	4.18	4.18
Panda	Endpoint Protection Plus on Aether	8.0	8.0	8.0	8.0
Sophos	Intercept X Advanced	10.8	10.8	10.8	10.8
SparkCognition	DeepArmor Endpoint Protection Platform	3.3	3.3	3.4	3.4
Vipre	Endpoint Security Cloud	12.0	12.0	12.0	12.0
VMware	Carbon Black Cloud	3.5	3.5	3.5	3.6

We congratulate the vendors who are participating in the Business Main-Test Series for having their business products publicly tested by an independent lab, showing their commitment to improving their products, being transparent to their customers and having confidence in their product quality.



² Information about additional third-party engines/signatures used by some of the products: **Acronis**, **Cisco**, **Cybereason**, **FireEye**, **G Data** and **Vipre** use the **Bitdefender** engine (in addition to their own protection features). **VMware** uses the **Avira** engine (in addition to their own protection features). **G Data's** OutbreakShield is based on **Cyren**.

³ ESET Endpoint Protection Advanced Cloud has recently been renamed in ESET PROTECT Entry.

Settings

In business environments, and with business products in general, it is usual for products to be configured by the system administrator, in accordance with vendor's guidelines, and so we invited all vendors to configure their respective products.

Only a few vendors provide their products with optimal default settings which are ready to use, and did therefore not change any settings. Cloud and PUA⁴ detection have been activated in all products.

Please keep in mind that the results reached in the Enterprise Main-Test Series were only achieved by applying the respective product configurations described here. Any setting listed here as enabled might be disabled in your environment, and vice versa. This influences the protection rates, false alarm rates and system impact. The applied settings are used across all our Enterprise Tests over the year. That is to say, we do not allow a vendor to change settings depending on the test. Otherwise, vendors could e.g. configure their respective products for maximum protection in the protection tests (which would reduce performance and increase false alarms), and maximum speed in the performance tests (thus reducing protection and false alarms). Please note that some enterprise products have all their protection features disabled by default, so the admin has to configure the product to get any protection.

Below we have listed relevant deviations from default settings (i.e. setting changes applied by the vendors):

Bitdefender: "Sandbox Analyzer" and "Scan SSL" enabled; "HyperDetect", "Device Sensor" and "EDR Sensor" disabled.

Cisco: everything enabled and set to Block.

CrowdStrike: everything enabled and set to maximum, i.e. "Extra Aggressive". "Unknown Detection-Related Executables" and "Unknown Executables" disabled.

Cybereason: "Anti-Malware" enabled; "Signatures mode" set to "Disinfect"; "Behavioral document protection" enabled; "Artificial intelligence" set to "Aggressive"; "Exploit protection", "PowerShell and .NET", "Anti-Ransomware" and "App Control" enabled and set to "Prevent"; all "Collection features" enabled; "Scan archives on access" enabled.

Elastic: "Malware" and "Process Injection" protections enabled; "Blacklist", "Credential Access", "Exploit" and "Ransomware" protections, as well as all "Adversary Behaviors" disabled.

ESET: All "Real-Time & Machine Learning Protection" settings set to "Aggressive".

FireEye: "Real-Time Indicator Detection" disabled, "Exploit Guard" and "Malware Protection" enabled.

⁴ We currently do not include any PUA in our malware tests.

Fortinet: All “AntiVirus Protection” settings enabled and set to “Block”. Additionally, “Anti-Exploit”, “Cloud Based Malware Detection”, “Advanced Heuristic”, “FortiGuard Analytics”, FortiSandbox’s “Sandbox Detection”, “Web Filter”, “Application Firewall”, “Detect and Block Exploits & Botnets” and “FortiEDR” were all enabled; “Exclude Files from Trusted Sources” for “Sandbox Detection” enabled.

G Data: “Exploit Protection”, “Anti-Ransomware” and “BankGuard” enabled; “BEAST Behavior Monitoring” set to “Pause Program and Quarantine”.

Kaspersky: “Adaptive Anomaly Control” disabled.

Microsoft: Cloud protection level set to "High", Cloud-delivered protection set to "Advanced". Google Chrome extension “Windows Defender Browser Protection” installed and enabled.

Sophos: All options in “Active Adversary Mitigations” enabled. “Web Control” and “Protect against data loss” disabled.

SparkCognition: all “Policy Settings” and all “Attack Vectors” settings enabled and set to “Aggressive”.

VMware: policy set to “Advanced”.

Acronis, Avast, K7, Panda, Vipre: default settings.

Management Summary

AV security software is available for all sizes and types of business. What fits well at the smaller end of the SME (small to medium enterprise) market is probably not going to be quite so appropriate to the larger corporates.

Before deciding on appropriate software to investigate, it is critical to understand the business environment in which it will be used, so that correct and informed choices can be made.

Let's start at the smaller end of the marketplace. These are environments that have often grown out of micro businesses, where domestic-grade AV products might well have been appropriate. But as soon as you start to scale beyond a few machines, the role of AV management comes into sharp focus. This is especially true when you consider the business and reputational damage that could result from a significant, and uncontained/uncontrolled malware outbreak.

However, in the smaller end of the SME space, there is rarely an onsite IT manager or operative. Often the role of "looking after the computers" falls to an interested amateur, whose main role in the business is that of senior partner. This model is often found in retail, accountancy and legal professions. In this space, it is critical to have a managed overview of all the computing assets, and to have instant clarity about the status of the protection delivered in way that is clear and simple. Remediation can be done by taking a machine offline, moving the user to a spare device, and waiting for an IT professional to arrive on site to perform clean-up and integrity checking tasks. Although users might be informed of status, managing the platform is a task for one, or at most, a few, senior people within the organization, often driven by overriding needs for data confidentiality within the company.

In the larger organization, it is expected to have onsite specialist IT staff, and, at the bigger end, staff whose role is explicitly that of network security. Here, the CTO role will be looking for straightforward, but real-time statistics and a management overview which allows for drilling into the data to focus on problems when they arise. There will almost be an explicit role for the software installation engineers, responsible for ensuring the AV package is correctly and appropriately loaded and deployed onto new machines. Knowing when machines "drop off grid" is almost as important here, to ensure that there are no rogue, unprotected devices on the LAN. Finally, there will almost certainly be a help desk role, as a first-line defence, who will be responsible for monitoring and tracking malware activity, and escalating it appropriately. They might, for example, initiate a wipe-and-restart on a compromised computer.

Finally, in this larger, more layered hierarchy, there is a task of remediation and tracking. Knowing that you have a malware infection is just the start. Handling it, and being able to trace its infection route back to the original point of infection, is arguably the most important function in a larger organization. If a weakness in the network security and operational procedure design cannot be clearly identified, then it is likely that such a breach will occur again at some point in the future. For this role, comprehensive analysis and forensic tools are required, with a heavy emphasis on understanding the timeline of an attack or infection from a compromised computer. Providing this information in a coherent way is not easy – it requires the handling of huge amounts of data, and the tools to filter, categorize and highlight issues as they are unfolding, often in real time.

Because of these fundamental differences, it is critically important to identify the appropriate tool for the organization, and the risk profile it is exposed to. Under-specifying this will result in breaches that will be hard to manage. Over-specifying will result in a system of such complexity that no-one truly understands how to deploy, use and maintain it, and the business is then open to attack simply because of the fog of misunderstanding and lack of compliance.

A key point for some businesses will be whether to go for a cloud-based or a server-based console. The former is almost instantaneous to set up, and usually avoids any additional configuration of client devices. The latter will require more work by the administrator before everything is up and running, including configuring clients and the company firewall. However, it means that the entire setup is on the company's own premises and under the administrator's direct control. For smaller businesses with limited IT staff, cloud-based consoles might be an easier option. Please note that in a number of cases, manufacturers provide both cloud-based and server-based options for managing their products. References to console type here only relate to the specific product used in our tests. Please consult the respective vendor to see if other console types are available.

Avast, K7 and Vipre offer easy-to-use cloud consoles that would be particularly suited to smaller businesses without full-time IT staff. These would all work well for larger companies too, and so allow the business to grow.

Fortinet, G Data and Kaspersky use server-based consoles that will prove very familiar and straightforward for experienced Windows professionals. They could be used by the SME sector upwards. Please note that Fortinet has an additional cloud-based console for its FortiEDR product. Kaspersky offer a cloud-based console as an alternative to the server-based product.

For businesses of the same size looking for cloud-based management solutions, **Bitdefender, ESET, Microsoft, Panda and Sophos** all offer strong and coherent solutions. **Acronis, Cybereason,** and **VMware Carbon Black** may require a little more learning, but would also be very appropriate for this category of business.

At the larger end of the market, **Cisco, CrowdStrike, Elastic, FireEye** and **SparkCognition** all offer exceptionally powerful tools. How well they will fit to your organization, both how it is today and how you intend to grow it over the next five years, needs to be carefully planned. There is clearly a role here for external expertise and consultancy, both in the planning and deployment stages, and all of them will require significant amounts of training and ongoing support. However, they offer a level of capability that is entirely different to the smaller packages.

AV-Comparatives' Approved Business Product Award

As in previous years, we are giving our "Approved Business Product" award to qualifying products. As we are conducting two tests for business products per year, separate awards will be given to qualifying products in July (for March-June tests), and December (for August-November tests).

To be certified in December 2020 as an "Approved Business Product" by AV-Comparatives, the tested products must score at least 90% in the Malware Protection Test with zero false alarms on common business software, and at least 90% in the overall Real-World Protection Test (i.e. over the course of four months), with less than one hundred false alarms on any clean software/websites (and with zero false alarms on common business software). Tested products must also avoid major performance issues (impact score must be below 40) and have fixed all reported bugs in order to gain certification.

We congratulate the vendors shown below, whose products met the certification criteria, and are thus given the AV-Comparatives Approved Business Security Product Award for December 2020:



Real-World Protection Test (August-November)

Malicious software poses an ever-increasing threat, due not only to the number of malware programs increasing, but also to the nature of the threats. Infection vectors are changing from simple file-based methods to distribution via the Internet. Malware is increasingly focusing on users, e.g. by deceiving them into visiting infected web pages, installing rogue/malicious software or opening emails with malicious attachments. The scope of protection offered by antivirus programs is extended by the inclusion of e.g. URL-blockers, content filtering, cloud reputation systems, ML-based static and dynamic detections and user-friendly behaviour-blockers. If these features are perfectly coordinated with the signature-based and heuristic detection, the protection provided against threats increases.

In this test, all protection features of the product can be used to prevent infection - not just signatures or heuristic file scanning. A suite can step in at any stage of the process – accessing the URL, downloading the file, formation of the file on the local hard drive, file access and file execution – to protect the PC. This means that the test achieves the most realistic way of determining how well the security product protects the PC. Because all a suite's components can be used to protect the PC, it is possible for a product to score well in the test by having e.g. very good behavioural protection, but a weak URL blocker. However, we would recommend that all parts of a product should be as effective as possible. It should be borne in mind that not all malware enters computer systems via the Internet, and that e.g. a URL blocker is ineffective against malware introduced to a PC via a USB flash drive or over the local area network.

In spite of these technologies, it remains very important that conventional and non-cloud features, such as the signature-based and heuristic detection abilities of antivirus programs, also continue to be tested. Even with all the protection features available, the growing frequency of zero-day attacks means that some computers will inevitably become infected. As signatures can be updated, they provide the opportunity to recognize and remove malware which was initially missed by the security software. Other protection technologies often offer no means of checking existing data stores for already-infected files, which can be found on the file servers of many companies. Those security layers should be understood as an addition to good detection rates, not as a replacement.

The Real-World Protection test is a joint project of AV-Comparatives and the University of Innsbruck's Faculty of Computer Science and Quality Engineering. It is partially funded by the Republic of Austria.



The methodology of our Real-World Protection Test has received the following awards and certifications, including:

- **Constantinus Award** – given by the Austrian government
- **Cluster Award** – given by the Standortagentur Tirol – Tyrolean government
- **eAward** – given by report.at (Magazine for Computer Science) and the Office of the Federal Chancellor
- **Innovationspreis IT – “Best Of”** – given by Initiative Mittelstand Germany



Test Procedure

Testing dozens of antivirus products with hundreds of URLs each per day is a great deal of work, which cannot be done manually (as it would involve visiting thousands of websites in parallel), so it is necessary to use some sort of automation.

Lab Setup

Every potential test-case to be used in the test is run and analysed on a clean machine without antivirus software, to ensure that it is a suitable candidate. If the malware meets these criteria, the source URL is added to the list to be tested with security products. Any test cases which turn out not to be appropriate are excluded from the test set. Every security program to be tested is installed on its own test computer. All computers are connected to the Internet. Each system is manually updated every day, and each product is updated before every single test case.

Software

The tests were performed under a fully patched Microsoft Windows 10 64-bit system. The use of more up-to-date third-party software and an updated Microsoft Windows 10 64-Bit makes it harder to find exploits in-the-field for the test. Users should always keep their systems and applications up-to-date, in order to minimize the risk of being infected through exploits which use unpatched software vulnerabilities.

Preparation for every testing day

Every morning, any available security software updates are downloaded and installed, and a new base image is made for that day. Before each test case is carried out, the products have some time to download and install newer updates which have just been released, as well as to load their protection modules (which in several cases takes some minutes). If a major update for a product is made available during the day, but fails to download/install before each test case starts, the product will at least have the signatures that were available at the start of the day. This replicates the situation of an ordinary user in the real world.

Testing Cycle for each malicious URL

Before browsing to each new malicious URL, we update the programs/signatures (as described above). New major product versions (i.e. the first digit of the build number is different) are installed once at the beginning of the month, which is why in each monthly report we only give the main product version number. Our test software monitors the PC, so that any changes made by the malware will be recorded. Furthermore, the recognition algorithms check whether the antivirus program detects the malware. After each test case the machine is reset to its clean state.

Protection

Security products should protect the user's PC and ideally, hinder malware from executing and performing any actions. It is not very important at which stage the protection takes place. It could be while browsing to the website (e.g. protection through URL Blocker), while an exploit tries to run, while the file is being downloaded/created or when the malware is executed (either by the exploit or by the user). After the malware is executed (if not blocked before), we wait several minutes for malicious actions and to give e.g. behaviour-blockers time to react and remedy actions performed by the malware. If the malware is not detected and the system is indeed infected/compromised (i.e. not all actions were remediated), the process goes to "System Compromised". If a user interaction is required and it is up to the user to decide if something is malicious, and in the case of the worst user decision the system gets compromised, we rate this as "user-dependent". Because of this, the yellow bars in the results graph can be interpreted either as protected or not protected (it's up to each individual user to decide what he/she would probably do in that situation).

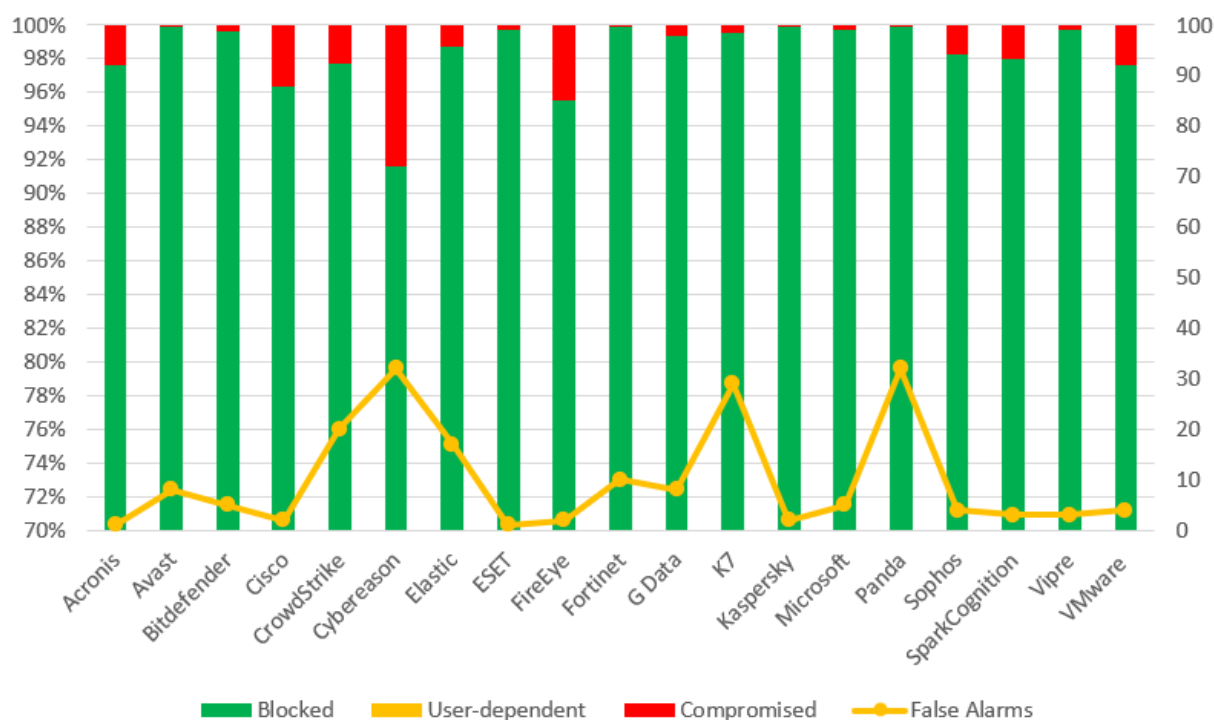
Due to the dynamic nature of the test, i.e. mimicking real-world conditions, and because of the way several different technologies (such as cloud scanners, reputation services, etc.) work, it is a matter of fact that such tests cannot be repeated or replicated in the way that e.g. static detection rate tests can. However, we log as much data as we reasonably can, in order to support our findings and results. Vendors are invited to include useful log functions in their products that can provide the additional data they want in the event of disputes. After each testing month, manufacturers are given the opportunity to dispute our conclusion about the compromised cases, so that we can recheck if there were any problems in the automation or with our analysis of the results.

In the case of cloud products, we can only consider the results that the products achieved in our lab at the time of testing; sometimes the cloud services provided by the security vendors are down due to faults or maintenance downtime by the vendors, but these cloud-downtimes are often not disclosed to the users by the vendors. This is also a reason why products relying too heavily on cloud services (and not making use of local ML/heuristics, behaviour blockers, etc.) can be risky, as in such cases the security provided by the products can decrease significantly. Cloud signatures/reputation should be implemented in the products to complement the other local/offline protection features, but not replace them completely, as e.g. offline cloud services could thus lead to PCs being exposed to higher risks.

Test Set

We aim to use visible, relevant and current malicious websites/malware, that present a risk to ordinary users. We usually try to include as many working drive-by exploits as we find – these are usually well covered by practically all major security products, which may be one reason why the scores look relatively high. The rest are URLs that point directly to malware executables; this causes the malware file to be downloaded, thus replicating a scenario in which the user is tricked by social engineering into following links in spam mails or websites, or installing some Trojan or other malicious software. We use our own crawling system to search continuously for malicious sites and extract malicious URLs (including spammed malicious links). We also search manually for malicious URLs.

The results below are based on a test set consisting of **801** test cases (such as malicious URLs), tested from the beginning of August 2020 till the end of November 2020.



	Blocked	User dependent	Compromised	PROTECTION RATE [Blocked % + (User dependent %)/2] ⁵	False Alarms
Kaspersky	800	-	1	99.9%	2
Avast	800	-	1	99.9%	8
Fortinet	800	-	1	99.9%	10
Panda	800	-	1	99.9%	32
ESET	799	-	2	99.8%	1
Vipre	799	-	2	99.8%	3
Bitdefender, Microsoft	799	-	2	99.8%	5
K7	797	-	4	99.5%	29
G Data	796	-	5	99.4%	8
Elastic	791	-	10	98.8%	17
Sophos	787	-	14	98.3%	4
SparkCognition	785	-	16	98.0%	3
CrowdStrike	783	-	18	97.8%	20
Acronis	782	-	19	97.6%	1
VMware	782	-	19	97.6%	4
Cisco	772	-	29	96.4%	2
FireEye	765	-	36	95.5%	2
Cybereason ⁶	734	-	67	91.6%	32

⁵ User-dependent cases are given half credit. For example, if a program blocks 80% by itself, and another 20% of cases are user-dependent, we give half credit for the 20%, i.e. 10%, so it gets 90% altogether.

⁶ A Cybereason product issue was uncovered during the Real-World Protection Test which led to some missed detections. The bug has now been fixed.

Whole-Product “False Alarm” Test (wrongly blocked domains/files)

The false-alarm test in the Real-World Protection Test consists of two parts: wrongly blocked domains (while browsing) and wrongly blocked files (while downloading/installing). It is necessary to test both scenarios because testing only one of the two above cases could penalize products that focus mainly on one type of protection method, either URL filtering or on-access/behaviour/reputation-based file protection.

a) Wrongly blocked domains (while browsing)

Blocked non-malicious domains/URLs were counted as false positives (FPs). The wrongly blocked domains have been reported to the respective vendors for review and should now no longer be blocked.

By blocking whole domains, the security products risk not only causing a loss of trust in their warnings, but also possibly causing financial damage (besides the damage to website reputation) to the domain owners, including loss of e.g. advertisement revenue. Due to this, we strongly recommend vendors to block whole domains only in the case where the domain's sole purpose is to carry/deliver malicious code, and otherwise block just to the malicious pages (as long as they are indeed malicious). Products which tend to block URLs based e.g. on reputation may be more prone to this and score also higher in protection tests, as they may block many unpopular/new websites.

b) Wrongly blocked files (while downloading/installing)

We used around one thousand different applications listed either as top downloads or as new/recommended downloads from various download portals. The applications were downloaded from the original software developers' websites (instead of the download portal host), saved to disk and installed to see if they are blocked at any stage of this procedure.

The duty of security products is to protect against malicious sites/files, not to censor or limit the access only to well-known popular applications and websites. If the user deliberately chooses a high security setting, which warns that it may block some legitimate sites or files, then this may be considered acceptable. However, we do not regard it to be acceptable as a default setting, where the user has not been warned. As the test is done at points in time and FPs on very popular software/websites are usually noticed and fixed within a few hours, it would be surprising to encounter FPs with very popular applications. Due to this, FP tests which are done e.g. *only* with very popular applications, or which use *only* the top 50 files from whitelisted/monitored download portals would be a waste of time and resources. Users will not care whether the malware that infects their systems affects only them, and likewise they will not care if the false positives that plague them affects only them. While it is preferable that FPs do not affect many users, it should be the goal to avoid having any FPs and to protect against any malicious files, no matter how many users are affected or targeted. Prevalence of FPs based on user-base data is of interest for internal QA testing of AV vendors, but for the ordinary user it is important to know how accurately its product distinguishes between clean and malicious files.

Fortinet, Panda, K7, Elastic, CrowdStrike and Cybereason had above-average numbers of FPs in the Real-World Protection Test.

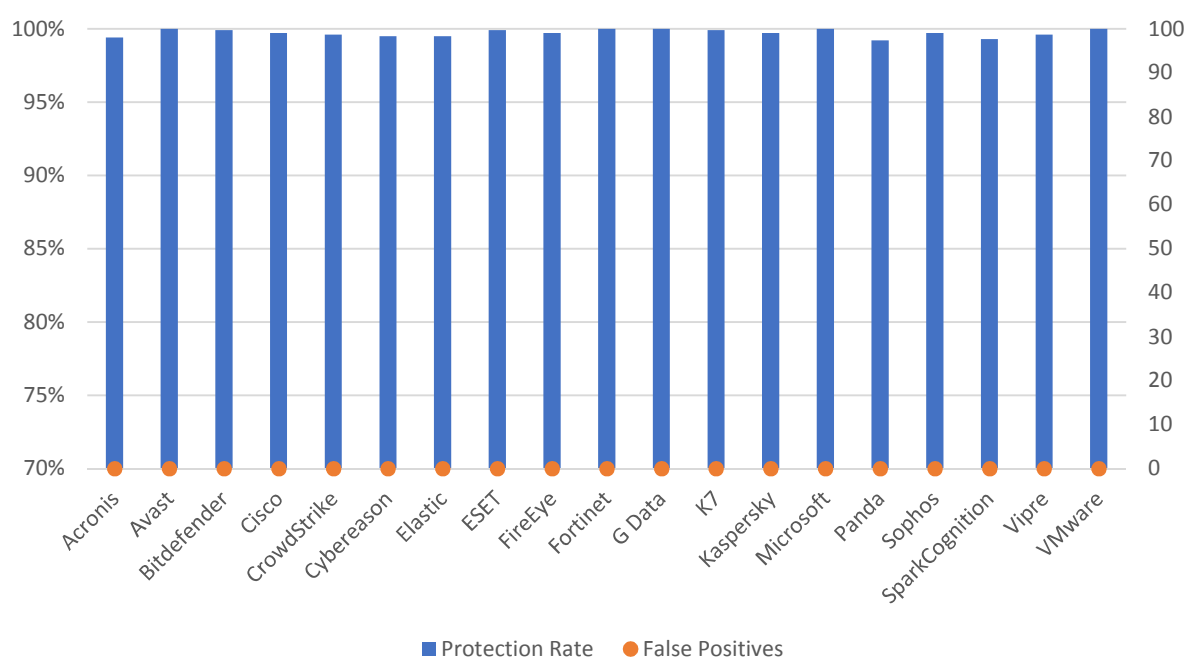
Malware Protection Test (September)

The Malware Protection Test assesses a security program's ability to protect a system against infection by malicious files before, during or after execution. The methodology used for each product tested is as follows. Prior to execution, all the test samples are subjected to on-access scans (if this feature is available) by the security program (e.g. while copying the files over the network). Any samples that have not been detected by the on-access scanner are then executed on the test system, with Internet/cloud access available, to allow e.g. behavioural detection features to come into play. If a product does not prevent or reverse all the changes made by a particular malware sample within a given time period, that test case is considered to be a miss. For this test, **1,063** recent malware samples were used.

False positive (false alarm) test with common business software

A false alarm test done with common business software was also performed. All tested products had **zero** false alarms on common business software.

The following chart shows the results of the Business Malware Protection Test:



	Malware Protection Rate	False Alarms on common business software
Avast, Fortinet, G Data, Microsoft, VMware	100%	0
Bitdefender, ESET, K7	99.9%	0
Cisco, FireEye, Kaspersky, Sophos	99.7%	0
CrowdStrike, Vipre	99.6%	0
Cybereason, Elastic	99.5%	0
Acronis	99.4%	0
SparkCognition	99.3%	0
Panda	99.2%	0

In order to better evaluate the products' detection accuracy and file detection capabilities (ability to distinguish good files from malicious files), we also performed a false alarm test on non-business software and uncommon files. This is provided mainly just as additional information, especially for organisations which often use uncommon non-business software or their own self-developed software. The results do not affect the overall test score or the Approved Business Product award. The false alarms found were promptly fixed by the respective vendors.

FP rate	Number of FPs on non-business software
Very Low	0-5
Low	6-15
Medium/Average	16-25
High	26-50
Very High	51-100
Remarkably High	>100

	FP rate on non-business software
Acronis, Bitdefender, Cisco, ESET, Kaspersky	Very low
Avast, FireEye, G Data, Sophos, Vipre	Low
Elastic, Microsoft, SparkCognition, VMware	Medium/Average
CrowdStrike, Cybereason, Fortinet	High
K7, Panda	Very high
-	Remarkably high

Performance Test (November)

We want to make clear that the results in this report are intended only to give an indication of the impact on system performance (mainly by the real-time/on-access components) of the business security products in these specific tests. Users are encouraged to try out the software on their own PC's and see how it performs on their own systems. We have tested the product that each manufacturer submits for the protection tests in the Business Main Test Series. Please note that the results in this report apply only to the specific product versions listed above (i.e. to the exact version numbers and to 64-bit systems). Also, keep in mind that different vendors offer different (and differing numbers of) features in their products.

The following activities/tests were performed under an up-to-date **Windows 10 64-Bit system**:

- File copying
- Archiving / unarchiving
- Installing / uninstalling applications
- Launching applications
- Downloading files
- Browsing Websites
- PC Mark 10 Professional Testing Suite

Test methods

The tests were performed on an Intel Core i7 CPU system with 8GB of RAM and SSD system drives. We consider this machine configuration as “**high-end**”. The performance tests were done on a clean Windows 10 1909 64-Bit system (English) and then with the installed business security client software. The tests were done with an active Internet connection to allow for the real-world impact of cloud services/features. Care was taken to minimize other factors that could influence the measurements and/or comparability of the systems. Optimizing processes/fingerprinting used by the products were also considered – this means that the results represent the impact on a system which has already been operated by the user for a while. The tests were repeated several times (with and without fingerprinting) in order to get mean values and filter out measurement errors. After each run, the workstation was reverted to the previously created system image and rebooted six times. We simulated various file operations that a computer user would execute: copying⁷ different types of clean files from one place to another, archiving and unarchiving files, downloading files from the Internet and launching applications (opening documents). We believe that increasing the number of iterations increases our statistical precision. This is especially true for performance testing, as some noise is always present on real machines. We perform each test multiple times and provide the median as result. We also used a third-party, industry-recognized performance testing suite (PC Mark 10 Professional) to measure the system impact during real-world product usage. We used the predefined *PC Mark 10 Extended* test. Readers are invited to evaluate the various products themselves, to see what impact they have on their systems (due to e.g. software conflicts and/or user preferences, as well as different system configurations that may lead to varying results).

⁷ We use around 5GB of data consisting of various file types and sizes (pictures, movies, audio files, MS Office documents, PDF documents, business applications/executables, archives, etc.).

Test cases

We strive to make our tests as meaningful as we can, and so continually improve our test methodologies. Future tests will be further improved and adapted to cover real-life scenarios even better.

File copying: We copied a set of various common file types from one physical hard disk to another physical hard disk. Some anti-virus products ignore some types of files by design/default (e.g. based on their file type), or use fingerprinting technologies, which may skip already scanned files in order to increase the speed.

Archiving and unarchiving: Archives are commonly used for file storage, and the impact of anti-virus software on the time taken to create new archives or to unarchive files from existing archives may be of interest for most users. We archived a set of different file types that are commonly found on home and office workstations.

Installing/uninstalling applications: We installed several common applications with the silent install mode, then uninstalled them and measured how long it took. We did not consider fingerprinting, because usually an application is installed only once.

Launching applications: Microsoft Office (Word, Excel, PowerPoint) and PDF documents are very common. We opened and then later closed various documents in Microsoft Office and in Adobe Acrobat Reader. The time taken for the viewer or editor application to launch was measured. Although we list the results for the first opening and the subsequent openings, we consider the subsequent openings more important, as normally this operation is done several times by users, and optimization of the anti-virus products take place, minimizing their impact on the systems.

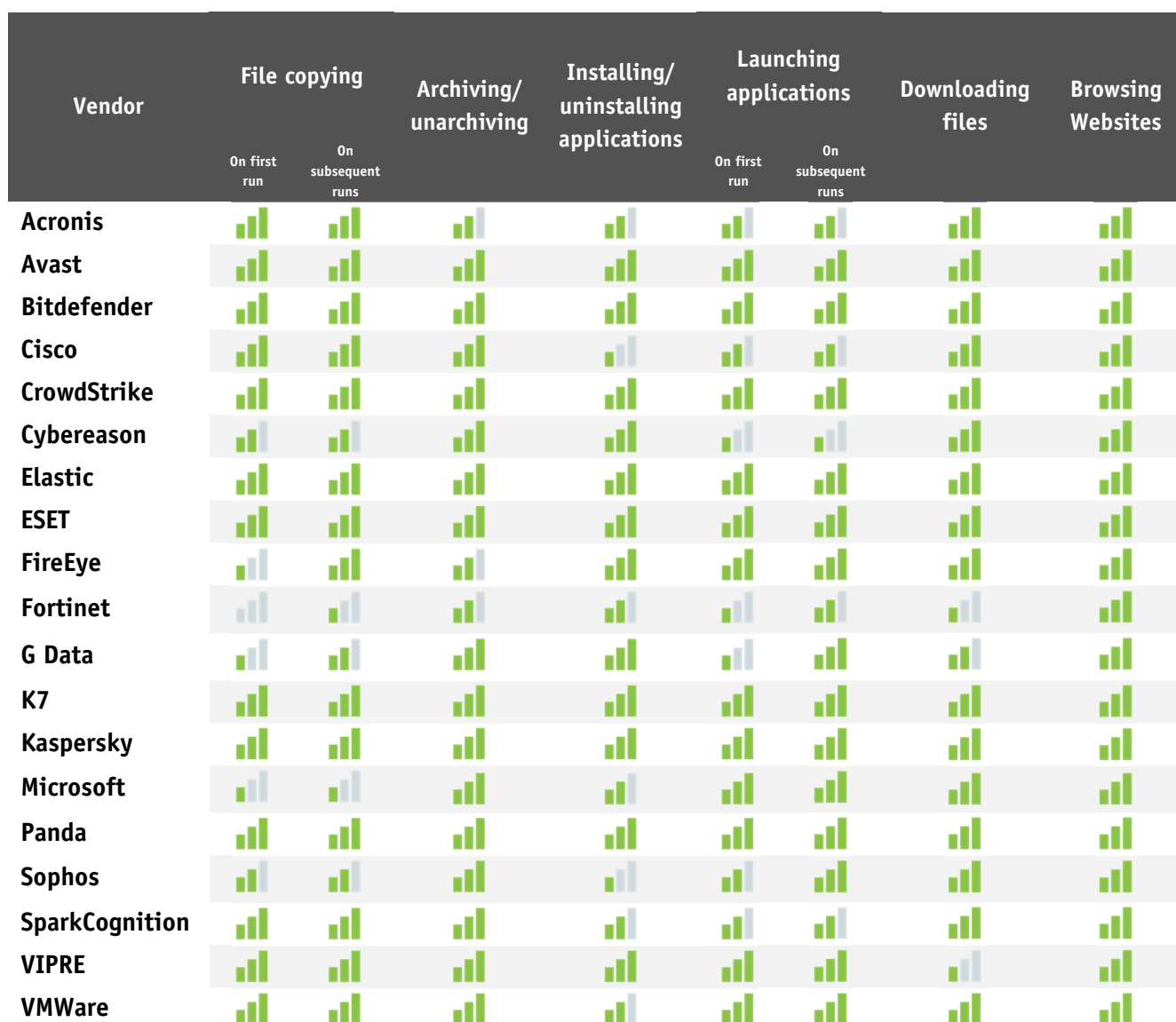
Downloading files: Common files are downloaded from a local server and public webserver.

Browsing Websites: Common websites are opened with Google Chrome. The time to completely load and display the website was measured. We only measure the time to navigate to the website when an instance of the browser is already started.

These specific test results show the impact on system performance that a security product has, compared to the other tested security products. The reported data just gives an indication and is not necessarily applicable in all circumstances, as too many factors can play an additional part. The testers defined the categories Slow, Mediocre, Fast and Very Fast by consulting statistical methods and taking into consideration what would be noticed from the user's perspective, or compared to the impact of the other security products. If some products are faster/slower than others in a single subtest, this is reflected in the results.

Slow	Mediocre	Fast	Very Fast
The mean value of the products in this cluster builds a clearly slower fourth cluster in the given subcategory	The mean value of the products in this cluster builds a third cluster in the given subcategory	The mean value of the products in this group is higher than the average of all scores in the given subcategory	The mean value of the products in this group is lower than the average of all scores in the given subcategory

Overview of single AV-C performance scores



Key:  Slow  mediocre  fast  very fast

PC Mark Tests

In order to provide an industry-recognized performance test, we used the PC Mark 10 Professional Edition⁸ testing suite. Users using PC Mark 10 benchmark⁹ should take care to minimize all external factors that could affect the testing suite, and strictly follow at least the suggestions documented inside the PC Mark manual, to get consistent and valid/useful results. Furthermore, the tests should be repeated several times to verify them. For more information about the various consumer scenarios tests included in PC Mark, please read the whitepaper on their website¹⁰.

“No security software” is tested on a baseline¹¹ system without any security software installed, which scores 100 points in the PC Mark 10 benchmark.

	PC Mark Score
Baseline	100
ESET, K7	98.8
Elastic	98.5
Acronis, Cisco	97.9
Kaspersky, Sophos	97.6
Bitdefender	97.4
SparkCognition	97.3
Fortinet	97.2
Vipre	97.1
FireEye	96.8
Avast, Microsoft	96.7
CrowdStrike, Panda	96.4
G Data, VMware	96.3
Cybereason	95.6

⁸ For more information, see <https://benchmarks.ul.com>

⁹ PC Mark® is a registered trademark of Futuremark Corporation / UL.

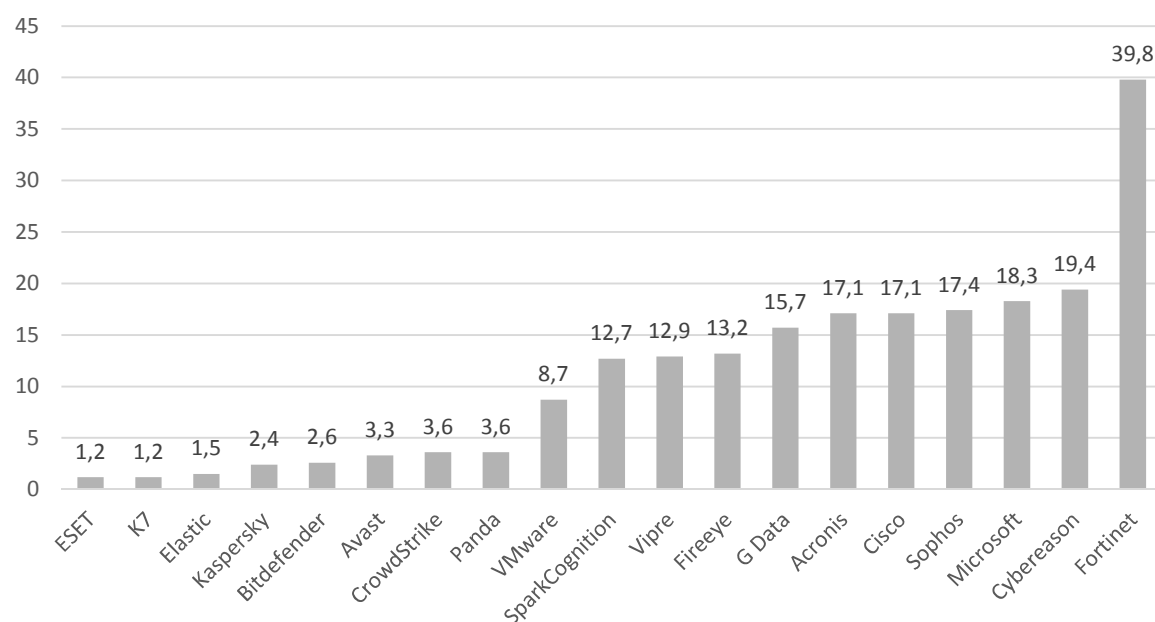
¹⁰ http://s3.amazonaws.com/download-aws.futuremark.com/PCMark_10_Technical_Guide.pdf (PDF)

¹¹ Baseline system: Intel Core i7 machine with 8GB RAM and SSD drive

Summarized results

Users should weight the various subtests according to their needs. We applied a scoring system to sum up the various results. Please note that for the File Copying and Launching Applications subtests, we noted separately the results for the first run and for subsequent runs. For the AV-C score, we took the rounded mean values of first and subsequent runs for File Copying, whilst for Launching Applications we considered only the subsequent runs. “Very fast” gets 15 points, “fast” gets 10 points, “mediocre” gets 5 points and “slow” gets 0 points. This leads to the following results:

	AV-C Score	PC Mark Score	TOTAL	Impact Score
ESET, K7	90	98.8	188.8	1.2
Elastic	90	98.5	188.5	1.5
Kaspersky	90	97.6	187.6	2.4
Bitdefender	90	97.4	187.4	2.6
Avast	90	96.7	186.7	3.3
CrowdStrike, Panda	90	96.4	186.4	3.6
VMware	85	96.3	181.3	8.7
SparkCognition	80	97.3	177.3	12.7
VIPRE	80	97.1	177.1	12.9
FireEye	80	96.8	176.8	13.2
G Data	78	96.3	174.3	15.7
Acronis, Cisco	75	97.9	172.9	17.1
Sophos	75	97.6	172.6	17.4
Microsoft	75	96.7	171.7	18.3
Cybereason	75	95.6	170.6	19.4
Fortinet	53	97.2	150.2	39.8



Reviews

On the following pages, you will find user-interface reviews of all the tested products. These consider the experience of using the products in real life. Please note that the reviews do not take test results into consideration, so we kindly ask readers to look at both the review and the test results in order to get a complete picture of any product.

We would like to point out that business security products include a wealth of features and functionality, and describing all of them would be well beyond the scope of a review such as this. We endeavour to describe the main features of each product, as presented in the user interface, and to provide similar coverage for each product. Due to different numbers and types of features in the various products reviewed, some apparent inconsistencies may occur. For example, in a simpler product with fewer features, we may be able to describe a particular function in more detail relative to a more complex product with a greater range of features.

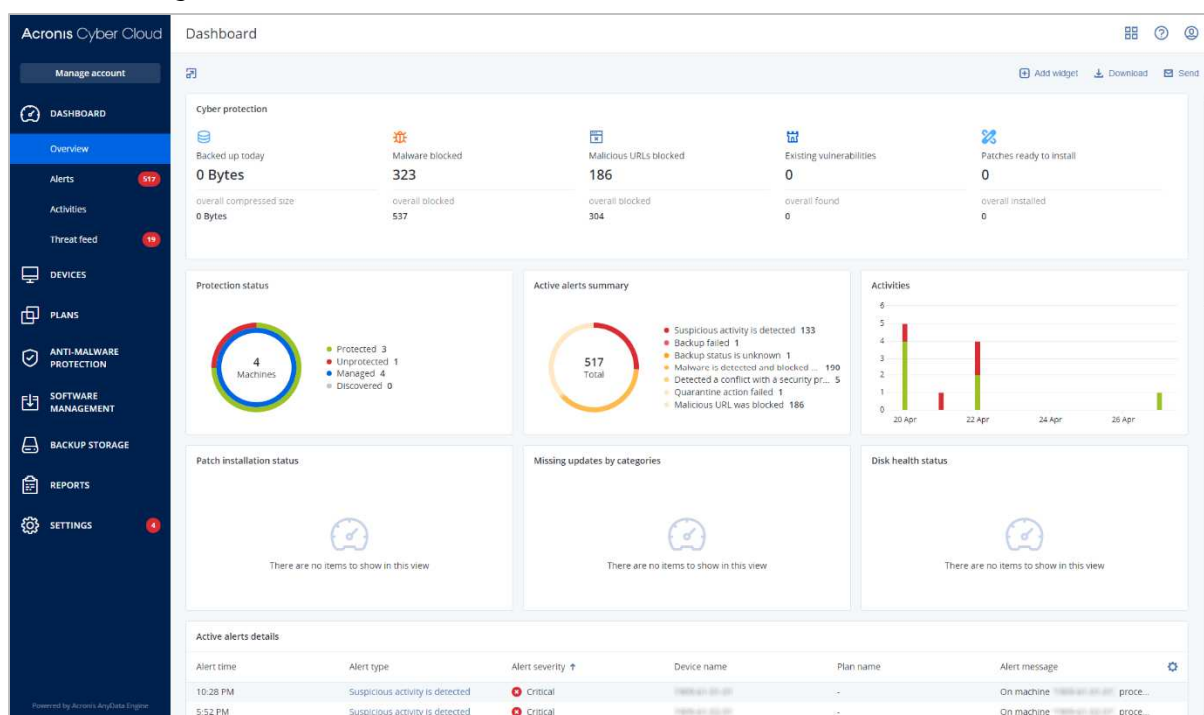
We first look at the type of product, i.e. whether the console is cloud based or server based, and what sort of devices/operating systems can be protected and managed. We have only considered Windows and macOS; Linux and mobile device support is in the feature list.

The next section looks at installation and deployment of the product. For server-based products, we describe the process of getting the console installed on the server (this is obviously not applicable to cloud-based consoles). The next step – applicable to all products – is to deploy the management agent and endpoint protection software to the client PCs.

The review then moves on to ongoing use, i.e. day-to-day management tasks such as monitoring and maintenance that need to be carried out. All the tested products include a dashboard-type page, which provides an overview of the security status, and a devices page that shows the computers on the network. We have provided a description of these for all products. With regard to the other features of each product, we have adopted a tailored approach. That is to say, we have tried to pick out some of the most important functionality of the individual product, in consultation with the respective vendor.

Finally, we take a look at the endpoint protection software installed on the client. Here we consider whether the endpoint user can perform any tasks such as scans and updates themselves, or whether such tasks are controlled exclusively by the administrator using the central management console. We also perform a brief functionality check. This involves connecting a USB flash drive containing a few malware samples to a PC with the product installed, and attempting to copy the malicious files to the Windows Desktop and then execute them. We note at which stage of the process the malware is detected, what sort of alert is shown, and whether the product prompts the user to scan the USB device when it is connected.

Acronis Cyber Protect Cloud – Advanced Edition



Advantages

- Has backup, disaster recovery, vulnerability assessment, patch management, and secure file-synch
- Well suited to smaller businesses
- Console is easy to navigate
- Pages of the console can be customised
- Geographically aware threat-feed feature

About the product

The Acronis Cyber Cloud platform provides endpoint protection software for Windows and macOS workstations, plus Windows servers. This is managed from a cloud-based console. The product contains a variety of other cloud-based services, including backup, disaster recovery, and secure file-synchronisation. This review considers only the malware protection features, however. The product can manage networks with thousands of seats. We feel it would also be suitable for small businesses without dedicated IT support staff.

Management Console

The console is navigated from a single menu panel on the left-hand side. There are entries for *Dashboard*, *Devices*, *Plans*, *Anti-Malware Protection*, *Software Management*, *Backup Storage*, *Reports*, and *Settings*.

Dashboard\Overview page

This is the page you see when you first log on to the console. It's shown in the screenshot above. It provides a graphical overview of the security and backup status of the network, using coloured doughnut and bar charts. There are panels for *Protection status*, *Active alerts summary*, *Activities*, *Patch installation status*, *Missing updates by categories*, and *Disk health status*. A panel across the top displays the items *Backed up today*, *Malware blocked*, *Malicious URLs blocked*, *Existing vulnerabilities*, and *Patches ready to install*. Details of recent alerts and other items are displayed in further panels at the bottom. You can customise the page by changing data settings for each panel, or adding/removing panels.

Dashboard\Alerts page

All alerts Loaded: 30 / Total: 1789 Clear all

Malware is detected and blocked (RTP) Oct 21, 2020, 03:04 PM

Anti-Malware Protection has detected and blocked the malware 'Trojan.Downloader.Dalexis.A' during the real-time scan.

Device	Trojan
Plan name	Default Protection Plan
File name	three.exe
File path	E:\winmal
MD5	f48d640494b4c5062b0c88834b2c845b
SHA1	b734a76e93e17541c9b917e03ff50e974653fb53
SHA256	480a3774416faa3362b59d6fa9ba0ea5c55c0e6a6e295032269d95ac45f5853a
Threat name	Trojan.Downloader.Dalexis.A
Action taken	Moved to quarantine

[Support](#) Clear

Malware is detected and blocked (RTP) Oct 21, 2020, 03:04 PM

Anti-Malware Protection has detected and blocked the malware 'Trojan.GenericKD.2434606' during the real-time scan.

Here you can see alerts relating to malware detection, blocked URLs, and also the backup functions. These can be shown as a list, or as big tiles with details (as shown above). Information for malware detections includes the device, protection policy, file name and path, file hashes, threat name and action taken (e.g. quarantined). Clicking *Clear* removes the item from the *Alerts* page, but not the system logs.

Dashboard/Threat feed page

Threat feed			
Filter Search		Loaded: 3 / Total: 3	
Name ↓	Type	Date ↑	
• RansomExx ransomware increased their activity and compromised Tyler technologies.	Malware	Sep 28, 2020	
• Active exploitation of the Zerologon vulnerability in the wild	Malware	Sep 28, 2020	
• UHS hospitals hit by reported country-wide Ryuk ransomware attack	Malware	Sep 28, 2020	

The *Threat feed* page displays warnings of current attacks and vulnerabilities to watch out for. Acronis tell us that this list is tailored to your geographic location, so that it only displays warnings that are relevant to you. The page may even warn you of natural disasters, where applicable. Clicking on the arrow symbol at the end of a threat entry opens a list of recommended actions to counteract that particular threat. These might be to run a malware scan, patch a program, or make a backup of your PCs or data.

Devices page

Type	Name ↑	Account	CyberFit score	Status	Last backup	Next backup	Agent
VM	1988-01-01-01	user-name (2020)@acronis...	Not applicable	Suspicious activity is detected	Never	Not scheduled	1988-01-01-01
VM	1988-01-01-01	user-name (2020)@acronis...	Not applicable	Suspicious activity is detected	Never	Not scheduled	1988-01-01-01
VM	1988-01-01-01	user-name (2020)@acronis...	Not applicable	Backup status is unknown	Never	Apr 14 11:25:40 PM	1988-01-01-01
VM	1988-01-01-01	user-name (2020)@acronis...	Not applicable	73% (Backing up)	Apr 17 09:04:38 AM	Apr 27 11:15:26 PM	1988-01-01-01

The *Devices* page lists the computers on the network. Sub-pages allow you to filter the view, e.g. by managed and unmanaged machines. You can see device type and name, user account, and security status, amongst other things. The columns shown can be customised, so you can remove any you don't need, and add e.g. IP address and operating system. Devices can be displayed as a list, or large tiles with additional details. Selecting a device or devices opens up a menu panel on the right, from which you can see the applied protection policy, apply patches, see machine details/logs/alerts, change group membership, or delete the device from the console.

Plans page

Under *Plans/Protection*, you can see, create and edit the policies that control the anti-malware features of the platform. Again, an uncluttered menu pane slides out from the right with the appropriate details and controls. Amongst the functions that can be configured are real-time protection, network folder protection, action to be taken on malware discovery, ransomware, crypto-mining process detection, scheduled scanning, exclusions, URL filtering, and how long to keep items in quarantine. You can configure vulnerability assessments and patch management, and there are even controls for scanning with Microsoft Windows Defender/Security Essentials too.

Anti-Malware Protection\Quarantine page

Under *Anti-Malware Protection*, the *Quarantine* page lists the names of malicious files that have been detected, along with the date quarantined and device name. You can add columns for the threat name and applicable protection plan from the page settings. A mini menu at the end of each entry lets you restore or delete the selected items.

Anti-Malware Protection\Whitelist page

The *Whitelist* page displays any applications that have been found during backup scanning and categorised as safe. A backup scanning plan has to be created in order to enable automatic whitelist generation.

Software Management pages

The *Patches* and *Vulnerabilities* pages under *Software Management* are populated if a vulnerability assessment has been created in a protection plan and run at least once.

Reports page

The *Reports* page lists a number of topics for which reports can be generated, including *Alerts*, *Detected threats*, *Discovered machines*, *Existing vulnerabilities* and *Patch management summary*. Clicking on a report name opens up a details page for that item. The *Alerts* report page, for example, contains panels showing *5 latest alerts*, *Active alerts summary*, *Historical alerts summary*, *Active alerts details*, and *Alerts history*. Coloured alert icons and doughnut charts serve to subtly highlight the most important items. As with other pages of the console, the columns in these panels can be customised.

Settings pages

Under *Settings/Protection*, you can set the schedule for protection definitions updates, and enable the *Remote Connection* function. The *Agents* page allows you to see the version of the endpoint agent installed on each client, and update this if necessary. If any devices are running outdated agents, an alert will be shown in the *Settings* entry in the menu panel of the console. This makes clear that you need to take action.

Windows Endpoint Protection Client

Deployment

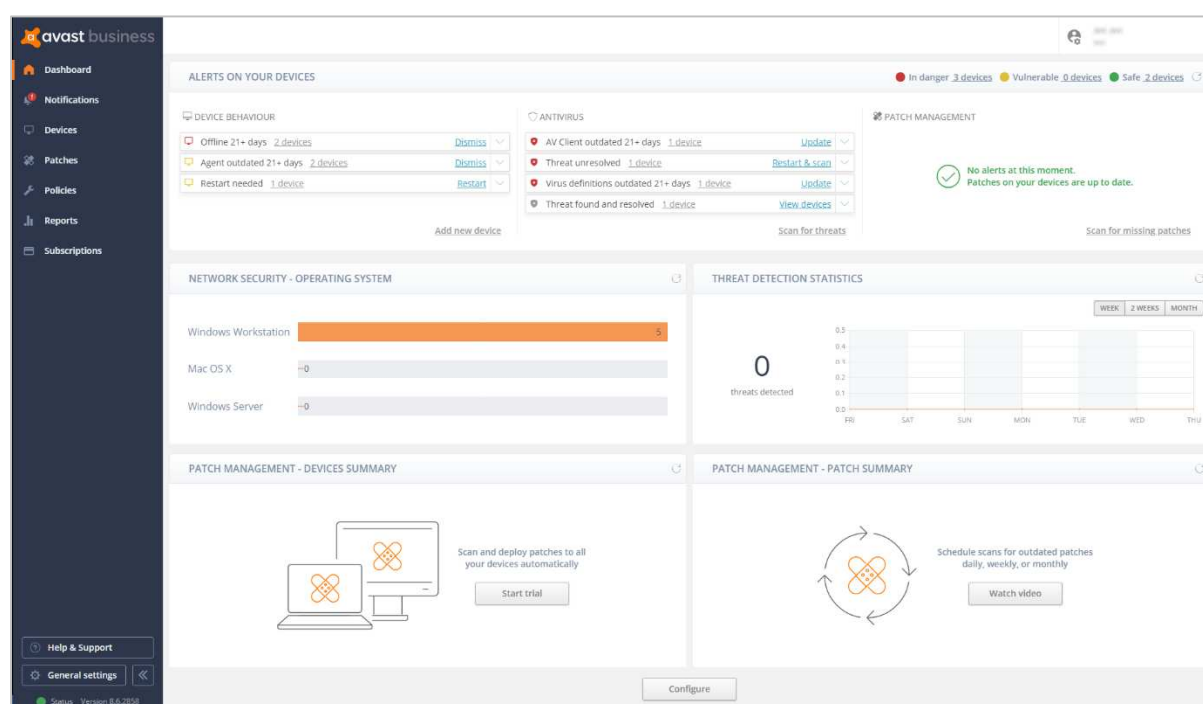
Installation files in .exe format can be downloaded by going to the *Devices* page and clicking the *Add* button. There are separate installers for Windows clients and Windows servers. The installer file can be run manually, via a systems management product, or using an AD script. Remote push installation is also possible if you set up a relay device in your LAN. By manually executing the .exe installer, you can also create .mst and .msi files for unattended installation. After performing a local installation on a client PC, you have to click *Register the machine* in the client window. You then need to log on to the management console from the client PC, find the device's entry, and click *Enable Protection*.

Functionality check

The user interface on protected endpoints consists of a System Tray icon and a small information window. Here you can see the status of the real-time malware protection, and date/time of the next scheduled backup. You can also see the program version. No other functionality is made available to users.

When we connected a flash drive containing malware samples to our test PC, and opened the drive in Windows Explorer, Acronis immediately detected and quarantined the malicious files. No alert was shown.

Avast Business Antivirus Pro Plus



About the product

Avast Business Antivirus Plus provides endpoint protection software for Windows and macOS workstations, plus Windows servers. This is managed using a cloud-based console. Additional features for Windows clients include anti-spam, data shredding, a VPN, and data & identity protection. Exchange and SharePoint security are provided for Windows Server. A patch management feature is included for all Windows computers. However, automatic installation of patches requires a separate licence for Avast Business Patch Management. This review considers only the malware protection features. The product can manage networks with tens of thousands of devices. We feel it would also be suitable for small businesses without dedicated IT support staff. Avast tell us that a new console user-interface design will be released next year.

Advantages

- Includes anti-spam, data shredding, a VPN, and data & identity protection
- Well suited to smaller businesses
- Console is easy to navigate
- Option for real-time synchronisation between clients and console
- Notifications link to details page/remediation functions

Management console

Dashboard page

This is what you will see when you first log in to the console (screenshot above). It provides an overview of the current security status. You can see alerts on your devices, OS distribution, and threat detection statistics.

Notifications page

Notifications			
Mark all as read		Notification settings	
Severity	Notification title and category	Action	Date
Warning	Threat was blocked and moved to the chest on device [device name] Security	View the Virus chest	8 Oct 2020 20:24
Warning	Devices require restart Network	See devices	7 Oct 2020 15:32
Warning	Threat was blocked and moved to the chest on device [device name] Security	Virus chest viewed	6 Oct 2020 13:57
Warning	Threat was blocked on [device name] Security		6 Oct 2020 12:21
Warning	Devices require restart Network	See devices	5 Oct 2020 15:08
Information	2 devices have been removed from your network Network		5 Oct 2020 07:57

This shows important alerts such as malware detections, and devices that are out of date or need rebooting. You can click on any alert to be taken to the relevant details page. Additional links are provided, such as the *Virus Chest* (quarantine) for malware detections, or *Update Now!* for out-of-date devices. Clicking the *Notifications Settings* button takes you to a configuration page, where you can choose which notifications to show in the console, and whether/how frequently to send email reminders if these have not been read.

Devices page

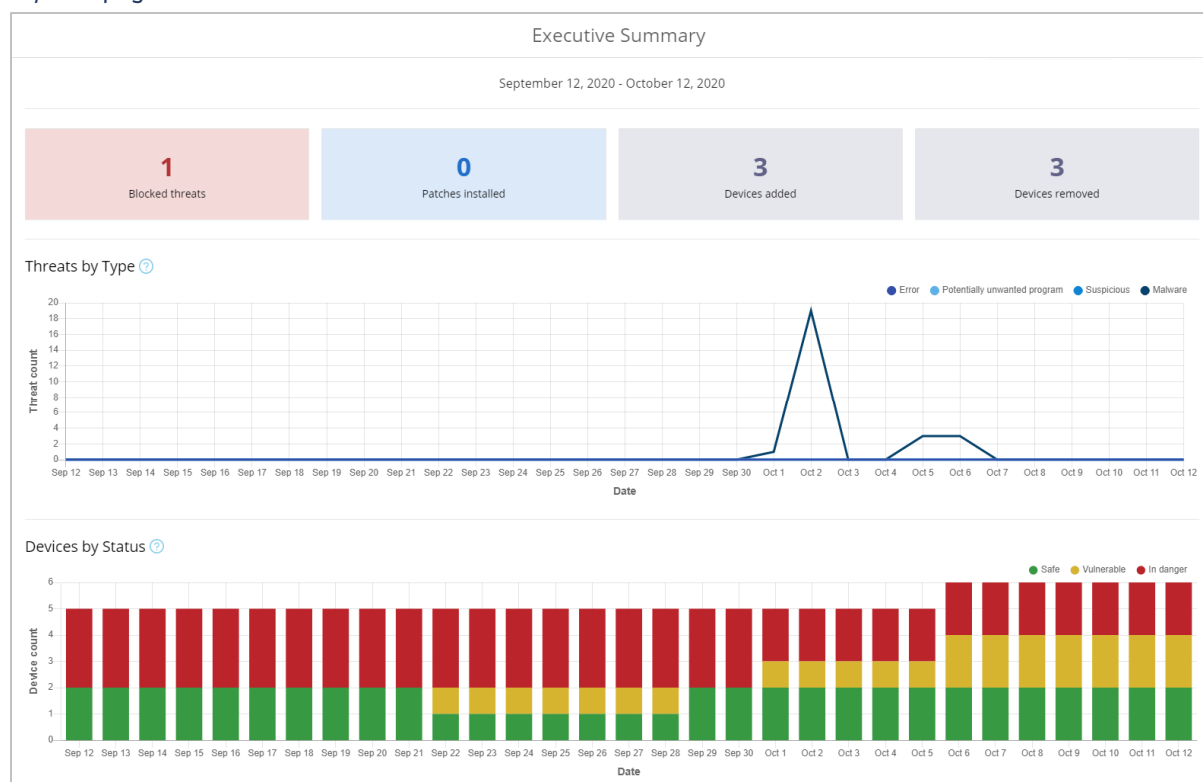
Devices			
New Devices Page			
<input type="text" value="Device name"/>		Actions	Hide alerts
Export device list		Transfer	Download installer
Dynamic filters		Filter alerts	
Status	Device name	Subscriptions	Last seen
Vulnerable	[device name] GROUP: DEFAULT POLICY: Default+Remote		5 hours ago
	Threat quarantined 1 day ago View threats		
	Threat found and resolved 2 days ago View threats		
Safe	[device name] GROUP: DEFAULT POLICY: Default	Antivirus Pro Plus	2 days ago
Vulnerable	[device name] GROUP: DEFAULT POLICY: David Test	Antivirus Pro Plus	18 hours ago
	Threat quarantined 6 days ago View threats		

The *Devices* tab shows each device's security status, group membership and policy, along with recent threats and other events. Helpful links are provided, for example *Restart & scan* for unresolved threats. You can group devices into groups, and apply settings and policy through that group.

Policies page

Here you can configure the protection settings for your devices. You can set scanning schedules for all platforms. For other settings, there are separate policies for Windows clients, Windows Servers, and macOS devices. You can configure program and definition update frequency, protection components to be used, and scan exclusions, amongst other things.

Reports page



There are five different report categories: *Executive Summary*, *Antivirus Threats Report*, *Patch Report*, *Device Report*, and *Tasks Report*. You can click on any of these headings to see a graphical representation of recent activity. For example, *Antivirus Threats Report* shows a graph of malware items detected, quarantined, blocked, deleted or repaired over the last month. You can create reports on a weekly or monthly schedule, and view scheduled reports already created.

Subscriptions page

As you would expect, this shows you the product licences you currently have, how many of them you have used, and when they expire. There are also links that let you try or buy other versions of Avast Business Antivirus, Avast's Premium Support Service, and the Patch Management component.

Help & Support provides links to various support and documentation items, including a user guide for the console. This is clear, comprehensive and well indexed, though lacking in screenshots.

General settings page

General Settings lets you change the system time zone, and enable *Labs features*. The latter is a preview of upcoming features that are "not entirely ready yet". You can also create a local server for deployments and updates (*Master Agent*), and import the database of another Avast console.

Windows Endpoint Protection Client

Deployment

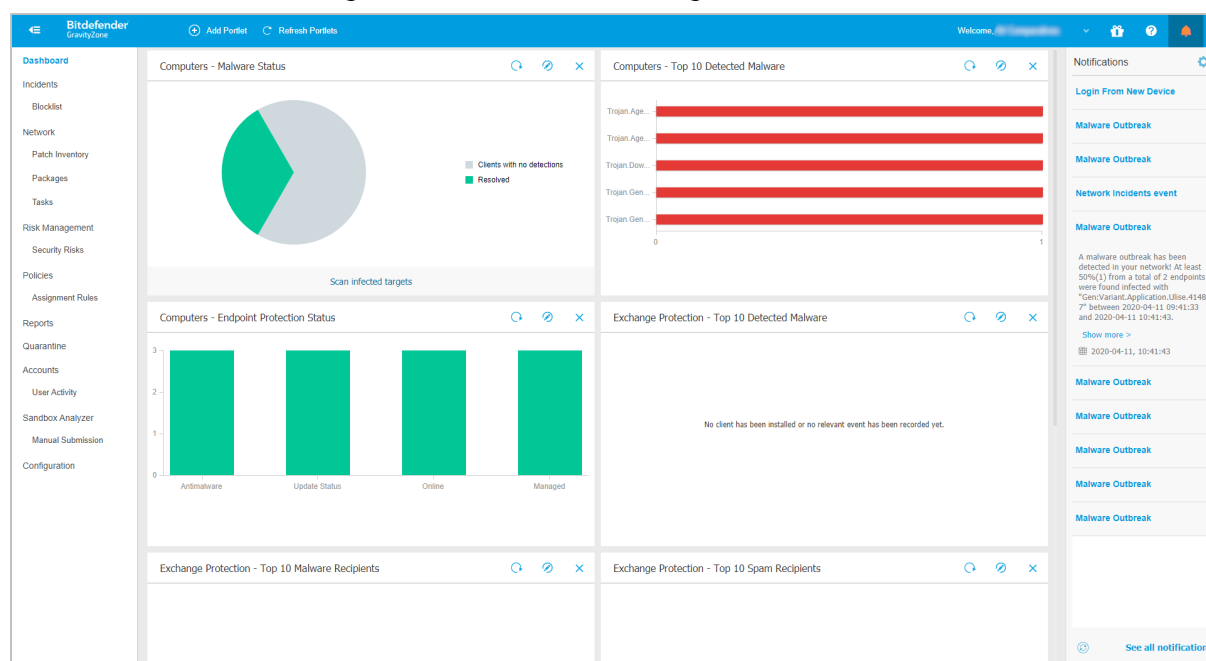
Installer files can be downloaded in either .exe or .msi format from the *Devices\Download Installer* page. You can specify the group and policy to be used, proxy server settings, and online or offline installer versions. The installer file can be run manually, via a systems management product, or using an AD script. Remote push installation is also possible in an Active Directory environment, by installing a utility on a relay computer in the LAN. On the download page, you can create a download link that you can copy and email to users. The setup wizard is very quick and easy, so even non-expert users would have no difficulty with it. You can prevent users with Windows Administrator Accounts from uninstalling the software by enabling the *Password Protection* option in the relevant policy.

Functionality check

The user interface on protected endpoints consists of a System Tray icon and a program window. You can hide the System Tray icon via policy if you choose. Users can see the protection status and detection logs, run updates, and run quick, full and custom scans. They can also scan a file, folder or drive using Windows Explorer's right-click menu. If you wish, users with Windows Administrator Accounts can be allowed to restore quarantined items, disable protection components, or uninstall the program.

When we connected a flash drive containing malware samples to our test PC, and opened the drive in Windows Explorer, Avast did not initially take any action. However, when we tried to execute the malware, or copy it to the Windows Desktop, Avast immediately detected and quarantined it. A pop-up alert was shown, which persisted until manually closed. No user action was required. Options to scan the PC, and see details of the detected threat, were shown. You can disable alerts via policy if you want.

Bitdefender GravityZone Elite Security



About the product

Bitdefender GravityZone Elite Security provides endpoint protection software for Windows and macOS workstations, plus Windows servers. This is managed using a cloud-based console. The product can manage networks with thousands of devices. We feel it would also be suitable for smaller businesses with tens of seats.

Advantages

1. Highly customisable pages
2. Clickable graphics let you easily access details pages
3. Detailed malware analysis
4. Risk-management feature
5. Easy-to-access notification details

Management Console

The console is navigated from a single menu panel down the left-hand side. The items are *Dashboard*, *Incidents*, *Network*, *Risk Management*, *Policies*, *Reports*, *Quarantine*, *Accounts*, *Sandbox Analyzer* and *Configuration*.

Dashboard page

Dashboard gives you an overview of the installation and the performance of the clients. It is divided up into information panels called *Portlets*. These provide information such as computer malware status, endpoint protection status, update status, and top 10 malware recipients. Each Portlet is clickable, so if you click on e.g. the *Clients with no detections* area of the *Malware Status* chart, you will be taken to a page listing all of the devices in that category. The *Dashboard* page is highly customisable. You can move Portlets around, hide some and add others.

Incidents page

THREATS

Root cause analysis of threats detected by Bitdefender prevention technologies

OPEN INCIDENTS

High

261

Medium

31

Low

722

TOP ALERTS

URL Malicious

179

ATC Malicious

66

Cloud Malware.Z4800101

16

Gen.Illusion Mustang 5 1020100

16

Trojan Agent.EVXQ

15

Cloud Malware.Z2260101

10

TOP AFFECTED DEVICES

192.168.1.100

890

192.168.1.100

122

10%

2

Change Status

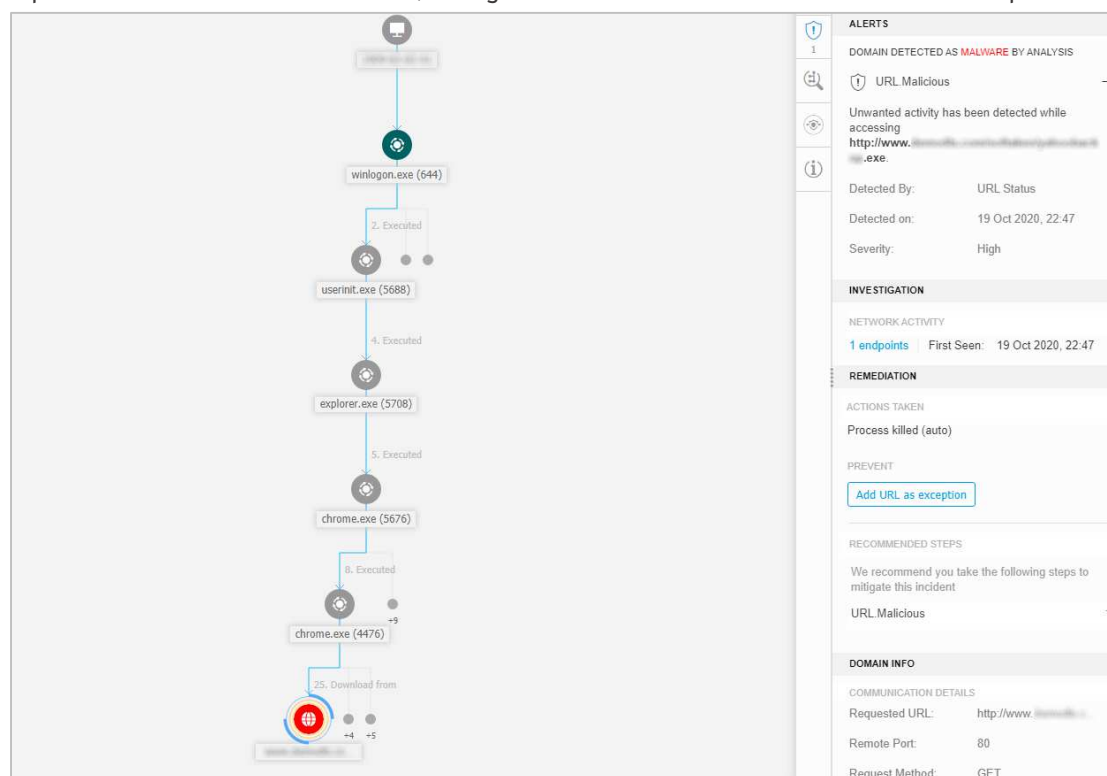
Alert name

Search for filenames, IP addresses, hostnames ...

Score	Date	Status	ID	Endpoint	Attack type	Alerts
<div><div><div><div></div></div><div>100-30</div></div><div>Select...</div></div>		<div>Open, Investigating</div>	<div>Search...</div>	<div>Search...</div>	<div>Choose...</div>	<div></div>
<div><div><div><div></div></div><div>50</div></div><div>Created 2 hours ago</div></div>		<div>Open</div>	<div>1883</div>	<div>192.168.1.100</div>	<div>Malware</div>	<div>8</div>
<div><div><div><div></div></div><div>50</div></div><div>Updated 19 hours ago</div></div>		<div>Open</div>	<div>1882</div>	<div>192.168.1.100</div>	<div>Malware</div>	<div>8</div>
<div><div><div><div></div></div><div>50</div></div><div>Created at 23:48 on 19 Oct</div></div>		<div>Open</div>	<div>1881</div>	<div>192.168.1.100</div>	<div>Malware</div>	<div>1</div>
<div><div><div><div></div></div><div>50</div></div><div>Created at 20:28 on 18 Oct</div></div>		<div>Open</div>	<div>1880</div>	<div>192.168.1.100</div>	<div>Malware</div>	<div>1</div>

Incidents allows you to review and investigate threats detected on the network. By default, it displays a chronological list of detected threats. There are columns for threat score (risk level), date and time, status of investigation, affected device, and attack type (e.g. malware). Panels at the top show the number of open alerts by severity, alerts by type, and most-affected devices. You can click on the numbers shown to go to the appropriate details page. The boxes at the top of each list column let you filter by that category, so you could specify the threat severity, time period or endpoint to narrow the list down.

By clicking on the network symbol at the right-hand end of a threat's entry, you can see a graphical representation of the threat event, along with further details and recommended steps to take:



Network page

Tasks Integrations Reports Assign Policy Go to container Recovery manager Delete Refresh					
Name	OS	IP	Last Seen	Label	
<input type="checkbox"/> [Icon] [Name]	Windows 10 Pro	192.168.1.100	Now	N/A	
<input type="checkbox"/> [Icon] [Name]	Windows 10 Pro	192.168.1.101	Now	N/A	
<input type="checkbox"/> [Icon] [Name]	Windows 10 Pro	192.168.1.102	Now	N/A	

The main *Network* page shows you all the managed devices on your network, ordered into groups which you can create yourself (screenshot above). A navigation pane on the left-hand side of the page shows your group structure, and lets you assign devices to groups by drag-and-drop. The *Tasks* menu lets you carry out various actions on selected devices, such as scans, updates, repairs and restarts.

The *Packages* sub-page lets you configure deployment packages. You can specify the components to be installed, use as a relay to enable push installation, and removal of existing AV products, amongst other things. On the *Tasks* sub-page you can see the status of tasks such as scans and updates.

Risk Management Dashboard page

Here you can see a wide range of data that you can use to proactively protect your network. Various different panels use coloured charts to display relevant items of information. The *Company Risk Score* gives you a rating from 1 to 100, based on *Misconfigurations*, *Vulnerable Apps*, and *Human Risks* (unsafe behaviour by users). For each of these items, there is a separate details panel. There is also a timeline of *Risk Score* over the past 7 days, along with panels for the most vulnerable individual servers, workstations and users. The *Security Risks* sub-page shows complete lists of the devices, users and vulnerable apps that are summarised on the main page.

Policies page

Here you can change the configuration of groups of client devices. A menu column down the left-hand side of the page lets you navigate the different areas of each policy, such as antimalware, firewall and device control.

Reports page

This lets you build information summaries on a wide variety of aspects, including blocked websites, device control activity, endpoint protection status, policy compliance and update status. The reporting interval can be set to this month, previous month, this year or previous year. You can also select device groups to be included.

Quarantine page

Quarantine gives you an overview of all the malware that has been quarantined on the network, and the ability to delete or restore selected files.

Accounts page

Accounts lets you add, remove and edit console users. There are three default permissions levels, from full control to read only. You can also create custom permission levels. On the *User Activity* sub-page you can monitor the activities of the user accounts.

Sandbox Analyzer page

Sandbox Analyzer provides a breakdown of unknown files that have been analysed by the sandbox feature, with a severity score from 0 (completely harmless) to 100 (clearly malicious).

Configuration page

The *Configuration* page lets you make configuration changes for the console itself. Amongst other things, you can set up 2-factor authentication here.

Notifications panel

Clicking the bell icon in the top right-hand corner opens the *Notifications* panel. This displays a list of events such as logins and detections. Clicking on an item displays a paragraph of information within the panel. For example, for *Login From New Device* you can see the device IP address, device operating system, browser used, and date and time. To get even more information, click on *Show more*, and you will be taken to the full details page in the main pane of the console.

Windows Endpoint Protection Client

Deployment

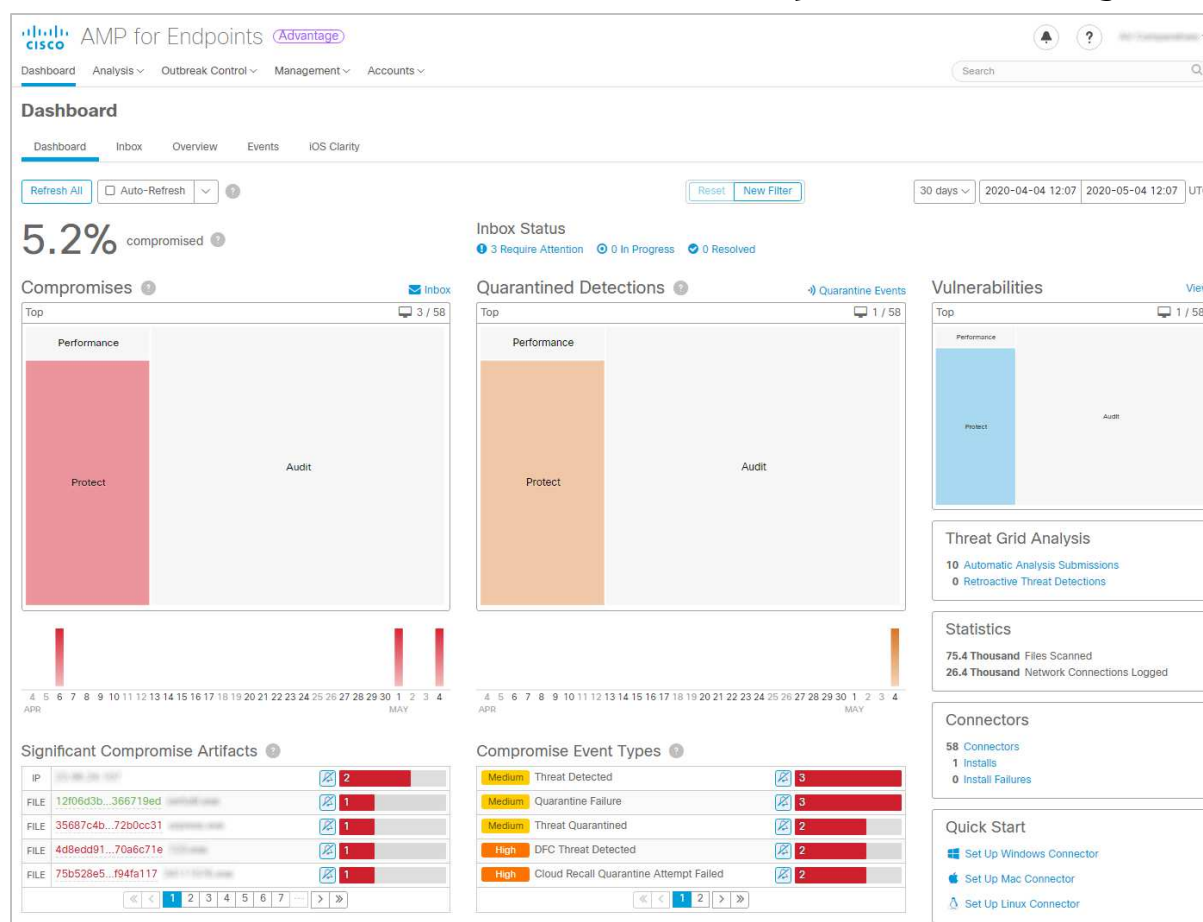
Under *Network\Packages* you can create and download installation files in .exe format. For Windows installers, there is a choice of light, full 32-bit and full 64-bit installers. The installer file can be run manually, via a systems management product, or using an AD script. Remote push installation is also possible, by installing the endpoint client on a relay computer in the LAN. Alternatively, you can email an installer to users directly from the *Packages* page. The setup wizard is very quick and easy, so even non-expert users would have no difficulty with it. You can prevent users with Windows Administrator Accounts from uninstalling the software by using the *Set uninstall password* option in the settings of the applicable policy.

Functionality check

The user interface on protected endpoints consists of a System Tray icon and a program window. Users can see the protection status and detection logs, run updates, and run quick, full and custom scans. They can also scan a file, folder or drive using Windows Explorer's right-click menu. By changing the policy, you could hide the user interface completely.

When we connected a flash drive containing malware samples to our test PC, and opened the drive in Windows Explorer, Bitdefender automatically started a scan of the external drive. We cancelled this, and opened the drive in Windows Explorer. We were unable to copy any of the malware samples to the Windows Desktop. A pop-up alert is shown when malware is detected, which closes after a few seconds. No user action is required or possible. You can disable detection alerts by policy if you want.

Cisco Advanced Malware Protection for Endpoints - Advantage



About the product

Cisco AMP provides endpoint protection software for Windows and macOS workstations, plus Windows servers. These are managed from a cloud-based console. In addition to malware protection, the product provides features for monitoring, investigating and blocking security threats. It can manage networks with hundreds of thousands of devices.

Advantages

- Investigative features
- Suitable for medium to large-sized enterprises
- Detailed timeline of attacks is shown
- Attack response can be automated
- Well-designed interface allows straightforward access to a wide range of functionality

Management Console

Dashboard tab

The *Dashboard* page of the *Dashboard* tab is shown in the screenshot above. There are a number of panels with coloured bar charts. These show *Compromises*, *Quarantined Detections*, *Vulnerabilities*, *Significant Compromise Artifacts*, and *Compromise Event Types*. The *Inbox* page shows a compact, summarised version of the same thing. The *Overview* page provides the most graphical overview of the state of the network, with coloured bar and doughnut charts showing *Compromises*, *Threats*, *Vulnerabilities*, *Computers*, *Network Threats*, *AV Definition Status* and *File Analysis*. These provide a very clear summary of the most important information. The *Events* page lists recent detections.

Analysis menu

In the *Analysis* menu you can find features for investigating attacks.

Events shows a list of events, such as endpoint client installation, deinstallation, and threats encountered by protected devices. These include access to risky websites, malicious file downloads, and attempts to quarantine suspected malware. Clicking on an item displays more details, such as the IP address and port of the threat website, and the hash of the malicious file.

You can drill down into a file's details on the *File Analysis* page. This shows you the specific behavioural indicators for detecting a file as malicious.

To see which legitimate programs have been involved in malware encounters, take a look at the *Threat Root Cause* page. A coloured pie chart shows you the distribution of malware encountered by specific applications, such as chrome.exe or explorer.exe.

On the *Prevalence* page, the number of devices affected by a particular threat is shown.

Under *Vulnerable Software*, programs with known vulnerabilities are listed. There is also CVE-ID and CVSS info to help identify and resolve the problem.

Reports provides a very detailed report by week and/or month and/or quarter. This covers numerous items such as threats, compromises and vulnerabilities. These are illustrated with coloured bar and doughnut charts.

Orbital Advanced Search is a capability that lets you query endpoints for detailed information. When enabled in AMP policy, it automatically installs an additional module (not used on our Main Test systems). Orbital can execute queries immediately, or you can schedule them using the *Orbital Jobs* feature. It includes a catalogue of queries with associated MITRE ATT&CK Tactics, Techniques or Procedure (TTP) mappings.

The *Indicators* page displays indicators of compromise (IOCs) that trigger AMP events. These act as a notification of suspicious or malicious activity on an endpoint, which can then be investigated. You can access the page from the *Analysis* menu. Each indicator includes a brief description of the nature of the attack. There is also information about the tactics and techniques employed, based on the MITRE ATT&CK knowledge base.

Outbreak Control menu

The *Outbreak Control* menu provides options for blocking or allowing specific applications and IP addresses. There are also custom detection options. These let you block the installation of any program you consider to be harmful or unwanted anywhere on the network. You can also run IOC (indicator of compromise) scans.

The *Automated Actions* feature (shown below) lets you set actions that automatically trigger when a specified event occurs on a computer. For example, if the computer is compromised, you can take a forensic snapshot, isolate it, move it to a specified group (or any combination of these). You can also submit suspicious files for analysis on detection. In each case, the minimum threat level (*Critical*, *High*, *Medium* or *Low*) required to trigger the action can be specified.

Automated Actions

Automated Actions | Action Logs

▼ **Take a Forensic Snapshot upon Compromise** (0 computers in the selected groups can take a Forensic Snapshot) Inactive ☐

High severity or higher in groups 8 selected

33 Compromise Events occurred in the last 7 days, affecting 2 distinct computers in the selected groups.

[View Changes](#) [Save](#)

▼ **Isolate a Computer upon Compromise** (0 computers in the selected groups can be isolated) Inactive ☐

High severity or higher in groups 8 selected

33 Compromise Events occurred in the last 7 days, affecting 2 distinct computers in the selected groups.

Rate Limit 10 [?](#)

Rate limit must be between 1 and 1000.

[View Changes](#) [Save](#)

▼ **Submit to Threat Grid upon Detection** (8 computers in the selected groups can submit files to Threat Grid) Inactive ☐

Medium severity or higher in groups 8 selected

33 Compromise Events occurred in the last 7 days, affecting 2 distinct computers in the selected groups.

[View Changes](#) [Save](#)

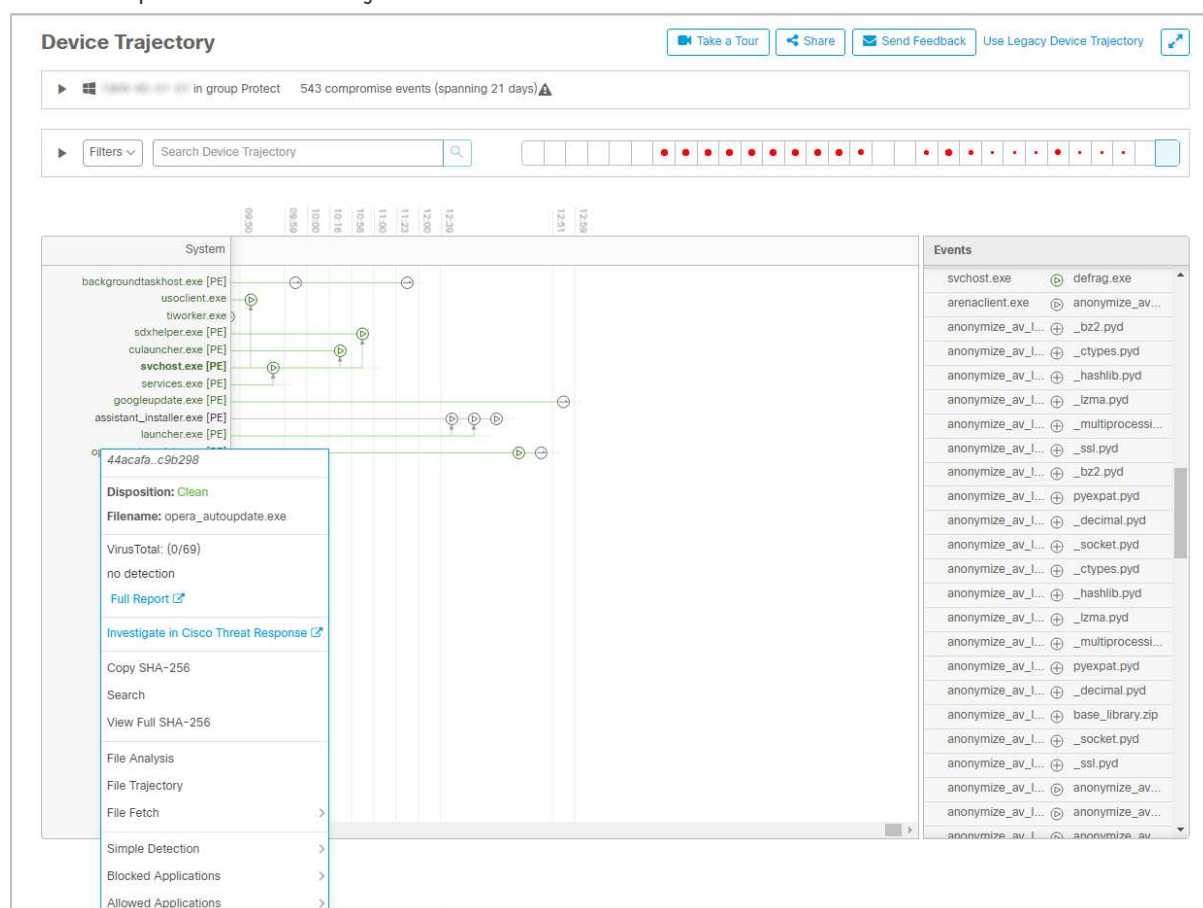
▼ **Move Computer to Group upon Compromise** (45 computers in the selected groups can be moved) Inactive ☐

Management menu

The *Management* menu contains a number of other standard features. There are *Groups*, *Policies*, *Exclusions*, and deployment options.

The *Computers* page, shown above, provides a row of statistics along the top, such as computers with faults or in need of updates. Below this is a list of individual devices, with a status summary for each one. You can mark a computer for further attention by clicking its flag icon here. Clicking on the arrowhead icon for a device displays a detailed information panel. This shows information such as OS version, connector version, definitions version, internal and external IP addresses, and date and time last seen. The computer list can be filtered by any of the above parameters.

Within the details of any individual computer is a link to *Device Trajectory* (shown in the screenshot below). This displays detection events by date (the row of red dots along the top of the page). The page provides a very detailed view of each event, using a timeline to show the order of the stages. There is a wealth of information here to assist with the investigation of an attack, including system processes involved, hashes of suspicious files, IP addresses accessed, and much more. Right-clicking on a process name in the *System* column opens a context menu with numerous options, including a summary of detections or a complete report from VirusTotal. There is also the option *Investigate in Cisco Threat Response*. This opens a separate console, which lets you explore the nature of the threat and the impact it has had on your network.



The *Endpoint Isolation* feature has to be enabled in the relevant policy before it can be used. It allows you to block all incoming and outgoing network traffic on a computer (with the exception of management-console communications). This allows you to investigate a potential threat safely.

Windows Endpoint Protection Client

Deployment

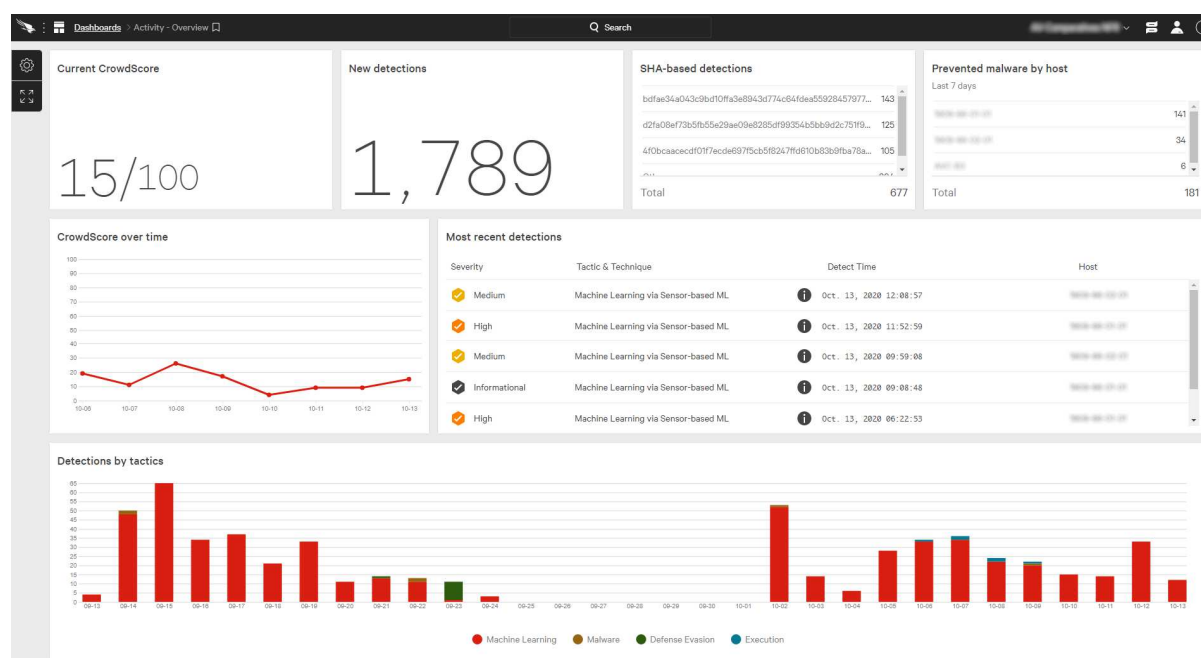
Installers in .exe format can be found by clicking *Management\Download Connector*. You need to select a device group, which defines which policy will be applied. The installer file can be run manually, via a systems management product, or using an AD script. The page also provides a download link that you can copy and email to users. The setup wizard is very quick and easy, so even non-expert users would have no difficulty with it. You can prevent users with Windows Administrator Accounts from uninstalling the software, using the *Enable Connector Protection* option in the applicable policy.

Functionality Check

The endpoint protection software allows users to run scans and updates, and view the logs. There is a choice of scans that users can run. These are *Flash Scan* (running processes), *Custom Scan*, *Full Scan* or *Rootkit Scan*. Users can also scan a file/folder/drive from Windows Explorer's right-click menu. You can hide the user interface completely if you want, by editing the policy.

When we connected a flash drive containing malware samples to our test PC, and opened the drive in Windows Explorer, Cisco AMP immediately detected and quarantined the malicious files. No alert was shown to the end user. However, the endpoint software can be configured by policy to show detection notifications.

CrowdStrike Falcon Pro



About the product

CrowdStrike Falcon Pro provides endpoint protection software for Windows and macOS workstations, plus Windows servers. This is managed using a cloud-based console. As well as malware protection, the product includes investigative functions for analysing and remediating attacks. It can manage networks with thousands of devices. We note that CrowdStrike Falcon Pro is available as a fully managed service for organisations that desire a more hands-off solution to endpoint protection. CrowdStrike tell us that they have datacentres in the USA and EU, in order to comply with the respective data protection regulations.

Advantages

- Investigative functions
- Comprehensive search facilities
- Clickable interface provides easy access to details pages
- Encyclopaedia of known cybercriminal groups
- Suitable for medium- to large-sized enterprises

Management Console

The console is navigated from the Falcon menu in the top left-hand corner of the console. This lists individual pages under headings such as *Activity*, *Investigate*, *Hosts*, *Configuration*, *Dashboards* and *Users*. You can easily bookmark any page of the console, and then go directly to that page using the *Bookmarks* section of the menu.

Activity\Dashboard page

This is the page you see when you first log on to the console. It shows various status items in large panels. There is a list of most recent detections, with a graphical severity rating. You can also see a graph of detections by tactic (e.g. *Machine learning*, *Defense Evasion*) over the past month. Terms from the MITRE ATT&CK Framework are used to show attack stages here. Some of the panels are linked to details pages. Thus, you can click on the *New detections* panel to open up the *Detections* details page.

Activity\Detections page

Here you can search a list of threat detections using a wide range of criteria. These include severity, tactics, detection technique, time, status and triggering file. For each detection, you can see full details, including a process tree view. You can contain network a host from here, and assign a console user for remediation.

Activity\Quarantined Files page

As you would expect, this page lets you see files that have been quarantined by the system. You can see the filename, device name, number of detections counted on the network, user involved, and of course date and time of detection. Quarantined files can be released or deleted. Clicking on a quarantined file opens a details panel with additional information. This includes file path for the location where it was detected, file hashes, file size, file version, detection method and severity. You can also start a sandbox analysis from here. There is a search function and a variety of filters you can use to find specific files within the quarantine repository.

Configuration\Prevention Policies page

Here you can create and edit the protection policies for endpoints. You can define behaviour for a number of different types of attack-related behaviour, such as ransomware, exploitation, and lateral movement. Some sensor components, such as *Cloud Machine Learning* and *Sensor Machine Learning* have separate configurable levels for detection and prevention. 5 different levels of sensitivity can be set, ranging from *Disabled* to *Extra Aggressive*. Custom Indicators of Attack (IOA) can also be created and assigned here.

The sensor version to be used on endpoint clients can be defined in the policy. This is done using a simple formula, whereby “n” is the latest version, “n-1” the second most recent, and so on. Policies can be assigned to devices automatically by means of a naming system. For example, any device with “Win” in its name can be automatically put into a specific group of Windows computers, to which a particular policy is assigned. Devices/groups can be assigned more than one policy, whereby a policy hierarchy determines which one takes precedence.

Hosts\Host Management page

Host Management

Q

Type to filter

1,697 hosts found

X

Platform	OS Version	OU	Site	Type	Status	Sensor Tags
Windows	1,697 Windows 10	1,697 N/A	1,697 N/A	1,697 Workstation	1,697 Normal	1,697 N/A
+Q	+Q	+Q	+Q	+Q	+Q	+Q

0 of 1697 selected

DELETE

🗑️

📄

🔍

	Hostname	Last Seen	First Seen	OS Version	OU	Prevention Policy	Response Policy	Sensor Update Pol...	Status	Sensor Version
<input type="checkbox"/>	192.168.1.101	Oct. 8, 2020 15:56:...	Oct. 8, 2020 15:19:51	Windows 10		Default (Windows) Oct. 8, 2020 15:22:...	Default (Windows) Oct. 8, 2020 15:22:...	Default (Windows) Changes pending	Normal	5.41.12309.0
<input type="checkbox"/>	192.168.1.102	Oct. 8, 2020 13:22:...	Oct. 8, 2020 10:32:...	Windows 10		Default (Windows) Oct. 8, 2020 10:34:...	Default (Windows) Oct. 8, 2020 10:34:...	Default (Windows) Changes pending	Normal	5.41.12309.0
<input type="checkbox"/>	192.168.1.103	Sep. 5, 2020 10:37:...	Sep. 5, 2020 09:07:...	Windows 10		Default (Windows) Sep. 5, 2020 09:07:...	Default (Windows) Sep. 5, 2020 09:07:...	Default (Windows) Changes pending	Normal	5.40.12202.0

The *Hosts/Host Management* page lists all the installed devices. You can immediately see which ones are online. Additional information includes operating system, policy, security status and sensor version. Clicking on a device's entry opens up a details panel for that device. Here you can find additional information, such as device manufacturer, MAC address, IP addresses and serial number.

Intelligence\Actors page

This page provides details of known cybercriminal groups. You can see the nations and industries that each one has targeted, along with technical details of the attack methods used. CrowdStrike tell us that this information is also available in *Detection* details when a detection is associated with a specific actor.

Investigate\Host Search page

The *Investigate* menu provides an extremely comprehensive search facility. It lets you search for devices, hashes, users, IP addresses, domains and events. On the *Host Search* page, you can look for specific devices. A separate menu bar allows you to look for specific aspects, such as *Activity* (including detections), *Vulnerabilities* and *Installed Applications*.

Windows Endpoint Protection Client

Deployment

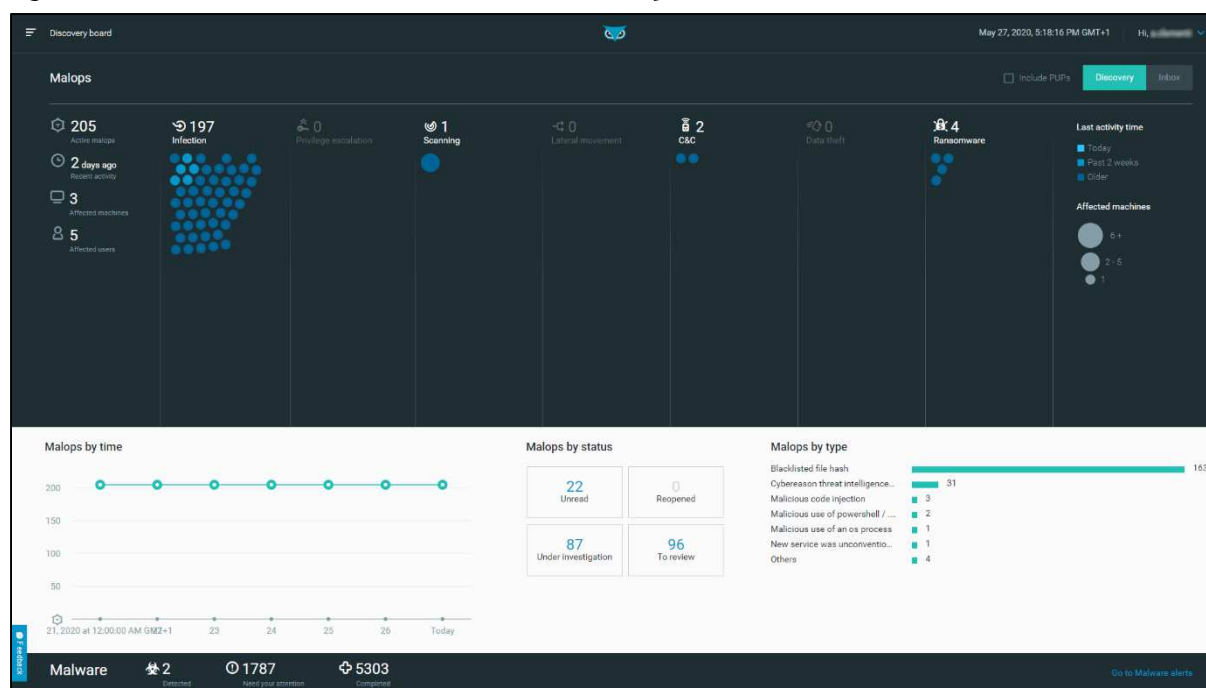
Installer files for the *sensor* (endpoint protection client) can be downloaded in .exe format from *Hosts\Sensor Downloads* page. Older versions of the sensor are available if you want. The installer file can be run manually, via a systems management product, or using an AD script.

Functionality Check

There is no interface at all to the endpoint client. It is completely invisible to the user, with the exception of malware alerts.

When we connected a flash drive containing malware samples to our test PC, and opened the drive in Windows Explorer, CrowdStrike Falcon did not take any action. We were able to copy the malicious files to the Windows Desktop. However, as soon as we tried to execute any of them, they were immediately detected and quarantined. A Windows pop-up alert was shown, which closed after a few seconds. No user action was required or possible. You can disable protection alerts by policy if you want.

Cybereason Defense Platform Enterprise



About the product

Cybereason Defense Platform Enterprise provides endpoint protection software for Windows and macOS workstations, plus Windows servers. This is managed using a cloud-based console. As well as malware protection, the product includes functions for analysing and remediating attacks. It can manage networks with hundreds of thousands of devices.

Advantages

- Investigative functions
- Ultra-simple and fast client deployment process
- Management console is easily navigated from a single menu
- Clear graphical representations of malicious activities
- Clickable interface provides easy access to details pages

Management Console

The console is navigated from the menu in the top left-hand corner.

Discovery board page

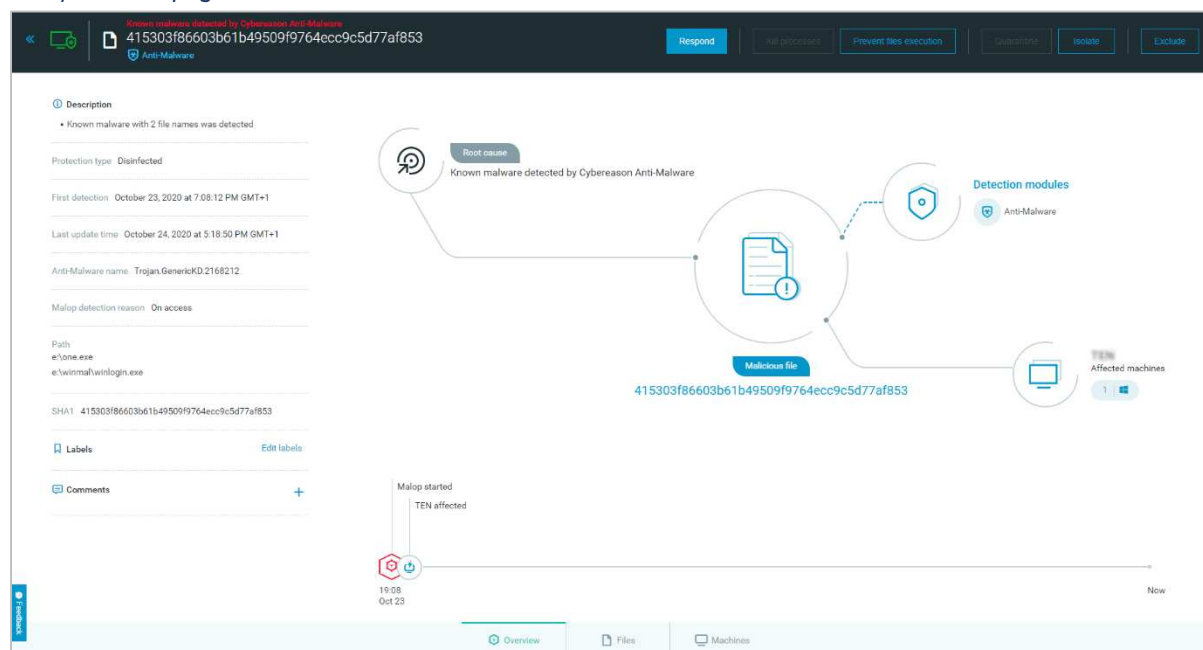
The *Discovery board* (shown in the screenshot above) is that page you will see when you first log on. It shows “Malops” (malicious operations) in columns, according to type. The blue dots represent a malicious or suspicious activity. The size of the dot represents the number of the affected machines, and the shade of colour refers to the activity time (as explained in the panel on the right-hand side of the page). If you click on a dot, a pop-up box displays the name of the file/process, and the nature of the threat (e.g. malicious code injection), along with the date and time of the action, and the affected device. Clicking on the pop-up opens the details page for that Malop. We are pleased to see that Cybereason have brought a touch of humour to the serious world of IT security. If all is well, the Discovery Board will state “No Malops found today. How about a cup of tea?”.

Malops management page



The *Malops management* page shows a list of detected malicious operations in chronological order. Information for each item includes an identifier (file/process name), detection module, and affected devices, along with date and time. This is laid out in spacious rows, making it easy to read the information. Different view options let you sort the Malops by activity type, root cause, or affected device. You can also choose a grid view, showing more items with fewer details. Clicking on one of the Malops opens its details page.

Malop details page



The *Malop details* page has an abundance of information about the Malop in question. This includes the device, SHA1 file hash, incoming and outgoing connections to and from the process, and a timeline. This information is laid out in very clear diagrams, which provide an at-a-glance summary of the threat. This strikes us as a remarkably effective way of communicating the important information quickly and easily. Big buttons at the top of the page let you carry out various actions to remediate the problem. These are Respond, Kill Process, Prevent Files Execution, Quarantine, Isolate and Exclude.

Malware alerts page

This shows items that “need your attention”. They are given names like “vaultfile12009845677446252183.vol”, based on the system’s internal quarantine naming process. Items marked as *Failed to disinfect* are shown prominently in big tiles along the top of the page. For each of these items, there are *Investigate* and *Exclude* buttons.

Investigation page

The *Investigation* page allows you to create customised hunts, using criteria such as machine, user, process, connection, network interface and registry entry. There are also pre-built queries, such as *Files downloaded from Chrome* and *Child processes of Explorer*.

Security profile page

Here you can adjust reputation criteria, create custom rules for detection and behavioural whitelisting, and manage machine isolation exceptions.

System section

The main *System* page has a number of sub-pages. These are *Overview*, *Sensors*, *Policies management* and *Detection servers*.

System\Overview page

The default *Overview* page is divided into 4 panels. The *Sensors* panel provides a doughnut chart of the status of installed devices, with a traffic-light colour-coding system for *Enabled*, *Suspended* and *Service Error* states. A simple bar graph completes the picture by showing the proportion of up-to-date clients. The other panels show details of the management server, alerts, and services.

System\Sensors page

The screenshot shows the 'System\Sensors' page. At the top, there are filter panels for 'Sensor status' (Online, Offline, Stale), 'Data collection' (Enabled, Disabled, Suspended, Advanced), 'OS' (Windows, macOS, Linux, iOS, Android, Unknown OS), 'Outdated' (Outdated, Updated), 'App Control mode' (Disabled, Enabled, Not installed, Unknown), and 'Anti-Ransomware mode' (Suspend, Detect, Suspend and prevent, Disabled, Unknown). Below these is a table with 14 columns: Machine name, FQDN, Data collection, Site, Sensor version, Last update stat..., Last seen, First seen, OS, Internal IP address, App Control mode, Anti-Ransomware mode, and Po. The table shows 1-4 results, with 1 sensor selected. The selected sensor is 'WIN-10-10-10-10' with a status of 'Advanced', 'Default' site, '20.1.329.0' version, 'Succeeded' last update, and 'February 26, 202...' first seen.

Machine name	FQDN	Data collection	Site	Sensor version	Last update stat...	Last seen	First seen	OS	Internal IP address	App Control mode	Anti-Ransomware mode	Po
WIN-10-10-10-10	WIN-10-10-10-10	Advanced	Default	20.1.329.0	Succeeded		February 26, 202...	Windows	192.168.0.10	Enabled	Suspend and pre...	En
WIN-10-10-10-10	WIN-10-10-10-10	Advanced	Default	20.1.329.0	Already up to date		February 28, 202...	Windows	192.168.0.10	Enabled	Suspend and pre...	En
WIN-10-10-10-10	WIN-10-10-10-10	Advanced	Default	20.1.329.0	Succeeded		May 15, 2020 at 1...	Windows	192.168.0.10	Enabled	Suspend and pre...	En

The *System\Sensors* page displays a list of protected devices, with details such as sensor version, OS type, IP address and component status. The details columns can be customised, letting you add a variety of items like CPU usage, memory usage and OS version. You can select a device or devices and perform tasks from the *Actions* menu, such as update, restart, set policy, set anti-ransomware mode, and start a system scan. A panel at the top of the page allows you to filter a long list of devices by sensor status, data collection, OS, update status, app control status and ransomware-protection status.

System\Policies management page

The *System\Policies management* page lets you create and edit policies for the endpoint software. For each policy, there is a configuration page with a left-hand menu column. This allows you to go to specific sections of the policy. These are *Anti-Malware*, *Exploit protection*, *PowerShell* and *.NET*, *Anti-Ransomware*, *App Control*, *Endpoint controls*, *Collection features*, and *Endpoint UI Settings*. Each item opens the relevant configuration page, with neatly laid-out controls for the individual sub-components.

System\Detection servers page

Here you can add and edit details of the sites and servers that manage the protection software.

Settings page

On this page you can configure system items such as notifications, authentication, and password policy.

Support page

The product's support services can be accessed by clicking *Support*, as you would expect.

Windows endpoint protection software

Deployment

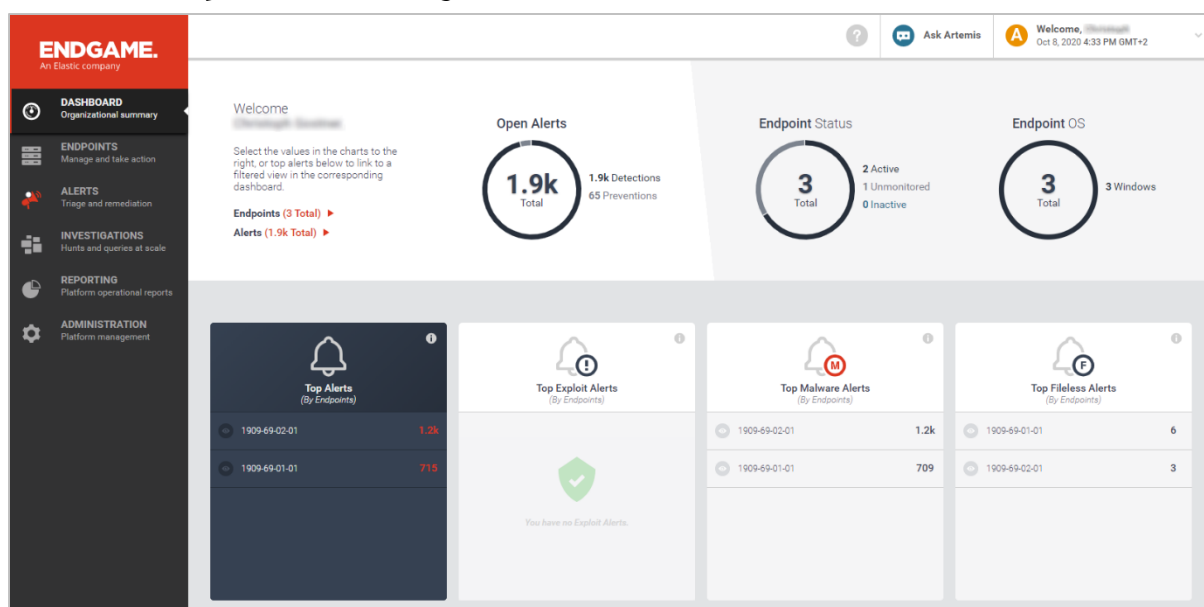
Installer files in .exe format can be downloaded from the *System\Overview* page of the console. There are 32- and 64-bit installers for Windows. The installer file can be run manually, via a systems management product, or using an AD script. Manual installation can be completed with a single click, and finishes in seconds.

Functionality test

The user interface on protected endpoints consists of a System Tray icon, which displays protection status, date and time of last update, signature version and program version. Other than this, no functionality is provided to users. You can hide the interface completely by means of policy, if you so choose.

When we connected a flash drive containing malware samples to our test PC, and opened the drive in Windows Explorer, Cybereason immediately detected and quarantined the malicious files. A pop-up alert was shown, which closed after a few seconds. No user action was required or possible.

Elastic Endpoint Security



About the product

Elastic Endpoint Security provides endpoint protection software for Windows and macOS workstations, plus Windows servers. This is managed from a cloud-based console. As well as malware protection, the product includes investigative functions for analysing and remediating attacks. appropriate IT resources. The product can manage networks with tens of thousands of devices.

Advantages

- Investigation functionality
- Clean and simple console design
- Graphical representation of attacks
- Console users can be assigned granular permissions
- Suitable for medium- to large-sized enterprises

Management Console

Dashboard page

This is the page you will see when you first open the console (screenshot above). It gives you an overview of the status of client device status, operating system distribution, and alerts. Separate panels show you 4 different alert categories, with the top three devices in each category listed. You can see total alerts, exploit alerts, malware alerts and fileless alerts. You can click on a device name in one of the panels to go directly to the details page of that device and alert type.

Endpoints page

The screenshot displays the 'Endpoints' page. At the top, there's a navigation bar with tabs: 'All', 'Windows', 'Apply Policy', 'Create Investigation', 'Discover Endpoints', and 'More Actions'. Below this, a summary bar shows: 4 Total, 1 Active, 1 Inactive, 2 Unmonitored, and 0 Isolated. A 'Create Group' button is visible. The main section is a table of endpoints. The table has columns: ENDPOINT NAME, IP ADDRESS, OPERATING SYSTEM, POLICY, SENSOR VERSION, ALERTS, AD, and GROUP. The data rows are:

ENDPOINT NAME	IP ADDRESS	OPERATING SYSTEM	POLICY	SENSOR VERSION	ALERTS	AD	GROUP
Active since 05:24 PM UTC	10.1.1.1	Windows 10 (v1903)	Successful	3.51.10	93	-	0 Groups
Unmonitored	10.1.1.1	Windows 10 (v1903)	-	-	0	-	0 Groups
Inactive since Sep 10, 2019	10.1.1.1	Windows 10 (v1903)	Pending	3.51.10	226	-	0 Groups
Unmonitored	10.1.1.1	Windows 10 (v1809)	-	-	14	-	0 Groups

A sidebar on the left shows a 'GROUPS' section with a search bar and a message: 'You haven't created any groups yet. Select endpoints and click 'Create Group' to get started.'

The *Endpoints* page gives a view of all the managed clients. You can sort and select by name, IP address, OS version, policy applied, sensor version, alerts and groups. You can choose a range of endpoints and then run tasks on them. These include applying a new policy, upgrading, uninstalling or deleting endpoints.

Alerts page

The screenshot displays the 'Alerts' page. At the top, there's a summary bar with: 2k Threats, 0 Unread, 0 Assigned To Me, and a 'View All' link. Below this, a table shows 'Most Recent Threats'. The table has columns: ALERT TYPE, HOSTNAME, ASSIGNEE, and DATE. The data rows are:

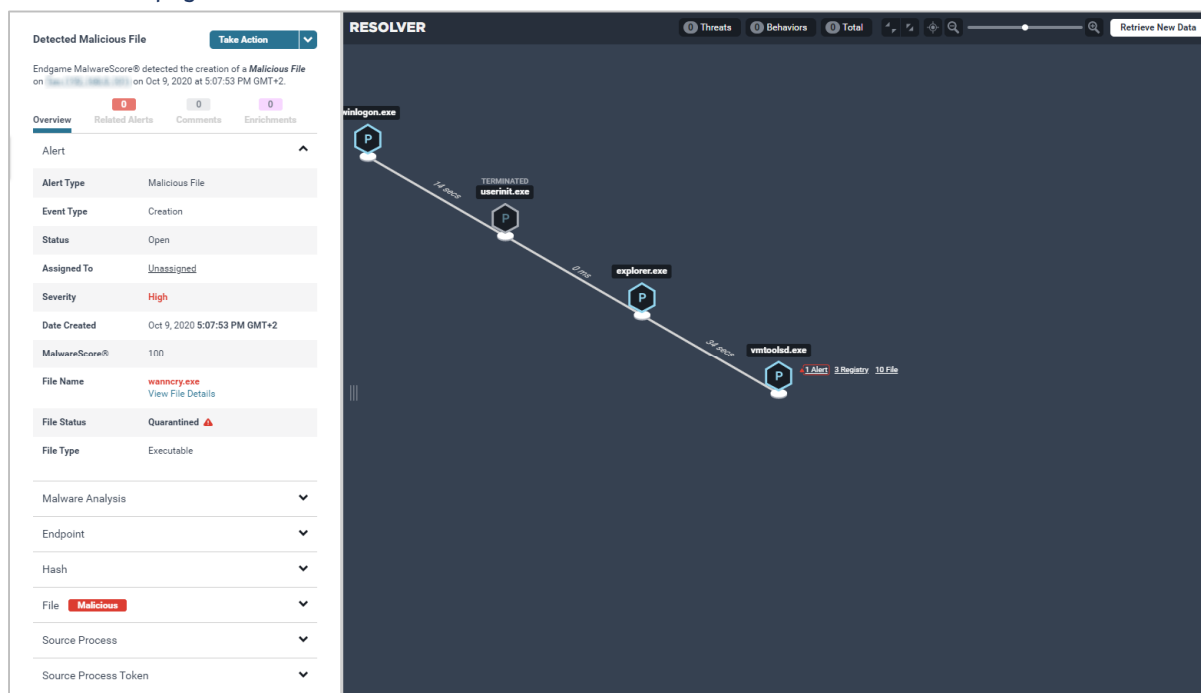
ALERT TYPE	HOSTNAME	ASSIGNEE	DATE
Malicious File	10.1.1.1	Unassigned	Oct 9, 2020 5:07:53 PM GMT+2
Malicious File	10.1.1.1	Unassigned	Oct 9, 2020 5:07:52 PM GMT+2
Malicious File	10.1.1.1	Unassigned	Oct 9, 2020 4:53:28 PM GMT+2
Malicious File	10.1.1.1	Unassigned	Oct 9, 2020 4:31:57 PM GMT+2
Malicious File	10.1.1.1	Unassigned	Oct 9, 2020 4:31:48 PM GMT+2

A sidebar on the right shows a 'Most Infected Endpoints' section with a table of alert counts and hostnames.

ALERT COUNT	HOSTNAME
1.2k	10.1.1.1
723	10.1.1.1
26	10.1.1.1

This provides you with a summary of total alerts and total *adversary behaviours*. By default, the page is kept very clean and simple, with just the five most recent alerts listed. However, you can see all alerts or adversary behaviours at the click of a link. The top five most infected endpoints are also listed here. As you would expect, you can click on links to go to the respective details page for the item in question. For example, clicking on an *Alert Type* link takes you to the *Alert Details* page for that event.

Alert details page



Here you can see much more detail about the event, where it started, what it has done and the analysis of the malware, if appropriate. You can see the alert type, severity, file hash, probability that the file is malicious, and action that has already been taken. You can also assign an analyst to deal with it. Relevant information, including processes, network connections and registry writes, is shown clearly in graphical form (screenshot above). You can choose *Take Action*, whereby the options include *Download Alert*, *Resolve*, *Dismiss*, *Start Investigation*, *Isolate Host*, *Download File*, *Delete File* and *Whitelist Items*.

Investigations page

The *Investigations* menu item shows a list of ongoing investigations, who is assigned to them, which endpoints are involved, and so forth. The *How to start an investigation* link at the top of the page displays a brief summary of the necessary steps. These are as follows. First, you have to select an OS and specific endpoints from the *Endpoints* page. You then click *Create Investigation*, enter a name and who it is assigned to, and select a *Hunt Type*. A *Hunt* can cover multiple information sources, e.g. firewall rules, drivers, network, persistence, process, registry, media, indicators of compromise, or system configuration. It allows you to search the network for information relevant to your enquiry. Having created your investigation, you can return to the *Investigations* page to see the results.

Reporting page

This page provides a simple overview of alert types and endpoints in graphical form.

Administration page

Finally, the *Administration* menu item gives access to various settings. The include *Policy*, *Users*, *Sensors*, *Alerts*, *Whitelist*, *Blacklist*, *Trusted Applications* and *Platform*. The *Policy* tab\ *Threats* sub-tab lets you define the action to be taken by the endpoint client when encountering specific threats. These include credential access, exploits, malware privilege escalation, process injection and ransomware. Each threat type has its own detailed configuration. For example, with process injection, you can choose whether to detect or prevent it, allow or block self-injection, and collect injected code. *Policy* has another sub-tab for *Adversary Behaviors*. As with *Threats*, you can decide on the course of action to be taken when encountering specific items. Here, the options are for command and control behaviour, credential access, lateral movement, privilege escalation and others. Finally, the *Policy*\ *Settings* sub-tab lets you configure events to be monitored and recorded, such as network connections, running processes and registry writes. You can also manage allowable network connections for isolated hosts here. Under *Register as Anti-Virus*, you can decide whether the Elastic endpoint client should register as the antivirus program in Windows Security and disable Microsoft Defender.

On the *Administration* page\ *User* tab, you can manage console users and assign them one of four permission levels. *Admin* level has full control, and there are levels 3, 2 and 1 below this. You can download an audit log of what each console user has done.

Windows Endpoint Protection Client

Deployment

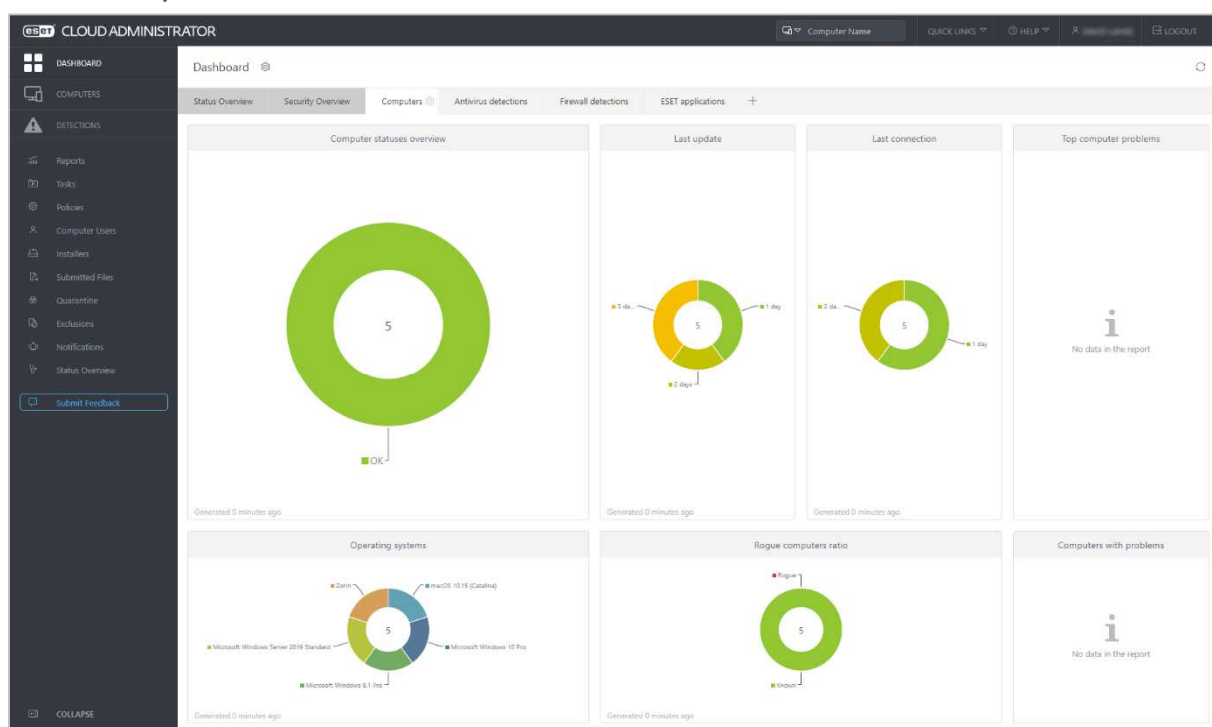
Deployment of the endpoint protection client (*sensor*) can be performed via remote push installation (*in-band*) or manual installation on the endpoint (*out-of-band*). The product can also be deployed using a systems management product or Active Directory. An installation package, comprising an installer in .exe format and a configuration file, can be downloaded from the *Settings* page\ *Sensor* tab. To perform a manual installation, you have to use specific command-line syntax (provided in the documentation) to do this.

Functionality Check

The endpoint protection software is completely invisible to the user, with the exception of malware detection alerts (see below). It does not appear in Windows' *Programs and Features* or *Apps* lists. This means that even users with Windows Administrator Accounts would find it difficult to disable.

When we connected a flash drive containing malware samples to our test PC, and opened the drive in Windows Explorer, Endgame did not initially take any action. However, as soon as we tried to copy the malicious files to the Windows Desktop, the endpoint software immediately detected and quarantined them. A banner alert was shown, which persisted until manually closed. No user action was required or possible.

ESET Endpoint Protection Advanced Cloud with Cloud Administrator



About the product

ESET Endpoint Protection Advanced Cloud provides endpoint protection software for Windows and macOS workstations, plus Windows servers. These are managed by the ESET Cloud Administrator (ECA) cloud console. We feel it would also be suitable for smaller businesses with tens of seats, but it can also cope with larger networks.

Please note that there is a choice of endpoint protection software for Windows clients. ESET Endpoint Antivirus is a full-featured antimalware program; ESET Endpoint Security (which was used in our tests) additionally includes a web control feature and ESET's Network Protection module. The package includes ESET File Security for Windows Servers.

We note that ESET have now changed the name of the package to "ESET PROTECT Entry", and that of the management console to "ESET PROTECT Cloud".

Advantages

- Modern interface design
- Functionality easily accessed from a single menu column
- Clickable, interconnected console makes it easy to go to details pages
- Interface can be customised
- Choice of endpoint protection software

Management Console

Dashboard page

The console opens on the *Dashboard/Computers* page, shown in the screenshot above. This provides an at-a-glance overview of the network, in the form of colour-coded doughnut charts. You can see the security status of the network, along with details of any problems and rogue computers. Last connection/update times and OS distribution are shown. You can easily get more details for any item just by clicking on its graphic. Similar links to details and solutions are provided throughout the console. The panels of the dashboard are very customisable. You can move them around, resize them, and change the chart type, among other things. Other tabs on the *Dashboard* page let you view antivirus or firewall threats, ESET applications, and incidents.

Computers page

Groups	COMPUTER NAME	STATUS	MODULES	LAST CONNECTED	ALERTS	DETECTIONS	SECURITY PRODUCT
CUSTOM GROUPS							
<ul style="list-style-type: none"> All (5) Windows (5) Lost & found (0) 							
DYNAMIC GROUPS							
<ul style="list-style-type: none"> Windows computers Windows (desktops) Windows (servers) Linux computers Mac computers Computers with outdated modules Computers with outdated operating system Problematic computers Not activated security product No manageable security product 							

The *Computers* page (shown above) gives you an overview of all the managed devices, and device groups, on the network. There are some pre-configured dynamic groups, for example *Computers with outdated operating system*. These make it easy to find all the devices that need your attention. You can also organise computers into your own custom groups, and carry out tasks on individual or multiple devices from the *Actions* menu. Examples include *Scan*, *Update*, *Reboot*, *Shut Down*, *Manage Policies*, *Deactivate Products*, and *Remove*. If you click on an individual computer's entry, a detailed information page for that device opens (screenshot below). Please note that *ESET Full Disk Encryption* is a separate product, not included in ESET Endpoint Protection Advanced Cloud.

- OVERVIEW
- CONFIGURATION
- LOGS
- TASK EXECUTIONS
- INSTALLED APPLICATIONS
- ALERTS
- QUESTIONS
- DETECTIONS AND QUARANTINE
- DETAILS

FQDN

Parent Group

IP

Applied Policies Count

Member of Dynamic Groups

192.168.0.10

0

/All/Windows computers
/All/Windows computers/Windows (desktops)

Products & Licenses

ESET Endpoint Antivirus 7.3.2039.0 Up-to-date version

ESET Management Agent 7.2.1266.0 Up-to-date version

ESET Endpoint Antivirus for Windows 2021 Jan 6 12:00:00

ESET Full Disk Encryption

ESET Full Disk Encryption provides powerful encryption managed natively by ESET remote management consoles, and increases your organization's data security to meet compliance regulations.

LEARN MORE

Everything is OK

Alerts

Unresolved Detections Count

Last Connected Time

Last Scan Time

Detection Engine

Updated

No alerts

0

2020 Sep 30 15:51:53

2020 Sep 30 15:41:21

22075P (20200930)

Updated

Users

Assigned Users

Logged users

n/a

Add user

Detections page

The *Detections* page shows information about all threats encountered by all managed devices on the network. Details include status, detection name, malware type, action taken, device name, user, file path, and date and time. You can click on the entry for any threat to get details such as file hash, source URL and detection mechanism. It's also possible to whitelist files this page.

Reports page

Reports allows you to collect data from a variety of categories, including *Antivirus detections*, *Automation*, *Dynamic Threat Defense*, *Firewall detections*, *Hardware inventory* and *quarantine*. For each category, a wide range of preconfigured scenarios is provided, displayed as tiles. Running a report on one of these items is as simple as clicking its tile. Example reports in the *Antivirus detection* category are *Active detections*, *Blocked files in last 30 days*, *High severity detection events in last 7 days*, and *Last Scan*. You can also create and schedule your own report scenarios if you want.

Tasks page

Tasks allows you to take a wide variety of actions on individual devices or device groups. These include running scans, product installations and updates. You can also run OS-related tasks, such as installing Windows Updates and restarting the operating system.

Policies page

This has a convenient list of preconfigured policies that you can apply. These include different security levels, device control options, and how much of the user interface to show to users. There are separate policies for Windows servers, Windows clients, and macOS/Linux clients. You can also create your own custom policies if you want. Machine-learning mechanisms can be set to either *Reporting* or *Protection*.

Computer Users page

Computer Users allows you to create users, add contact details, and link them to devices.

Installers page

Here you can create installation packages to be used to deploy the endpoint protection software. When you log on to the console for the first time, an introductory wizard lets you do this straight away. To create an installer, select the appropriate product and configure setup options.

Submitted files page

This page shows a list of possibly suspicious files on protected endpoints that have been submitted to ESET's *LiveGrid* service for analysis. Files may have been submitted automatically by the system, manually by the user, or by another ESET admin or system.

Quarantine page

Here you can see all quarantined files, along with useful details such as the hash, detection type (Trojan, PUA, test file), and number of computers affected. You can restore or delete any quarantined files.

Exclusions page

The *Exclusions* page shows files/paths that have been excluded from detection/scanning, and provides instructions for creating such exclusions.

Notifications page

Notifications lets you receive email notifications for a number of different scenarios. These include threats being detected, and out-of-date endpoint software. These are very simple to set up and edit. You just have to select the scenario(s), enter an email address, and enable the notification.

Status overview page

Finally, the *Status Overview* page provides a brief overview of important status items, divided into the categories *Licences*, *Computers*, *Products*, *Invalid Objects* and *Questions*. The *Invalid Objects* section advises of e.g. policies that refer to out-of-date installers. *Questions* points out “decisions that cannot be handled automatically and need the attention of the administrator”.

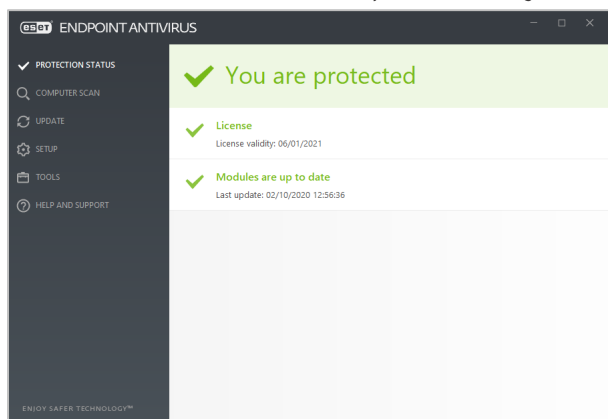
Windows Endpoint Protection Client

Deployment

Installer files in .exe or GPO/SCCM script format can be downloaded from the *Installers* page. The installer file can be run manually, via a systems management product, or using Active Directory. You can also email an installer to users directly from the *Installers* page. The installer can be configured so that no decisions have to be made, making it easy for non-expert users to install. You can prevent users with Windows Administrator Accounts from uninstalling the software or changing settings, by enabling the *Password protect settings* option in the policy.

Functionality check

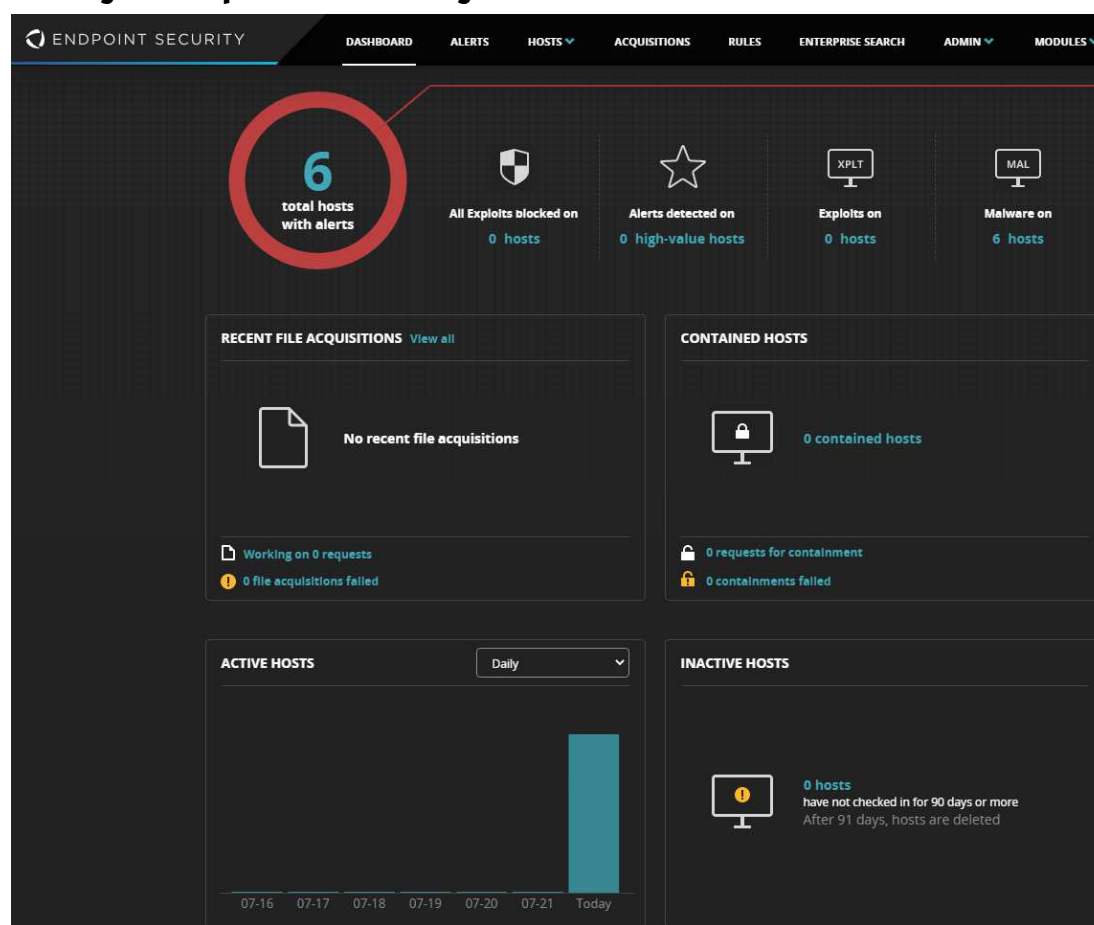
The user interface on protected endpoints consists of a System Tray icon and a program window, which is shown below. Both ESET Endpoint Antivirus and ESET File Security for Windows Servers use a virtually identical interface to ESET Endpoint Security.



The user can see the protection status and detection logs, run updates, and run full or custom scans. Users can also scan a file, folder or drive using Windows Explorer’s right-click menu. If you wish, users with Windows Administrator Accounts can be given full control of the program. Alternatively, you could hide the user interface for all users.

When we connected a flash drive containing malware samples to our test PC, ESET Endpoint Security prompted us to scan the drive. We declined, and then opened the drive in Windows Explorer. ESET immediately detected and quarantined the malicious files. A pop-up alert was shown, which closed after a few seconds. No user action was required or possible. However, a link showing further details of the threat is provided. You can disable detection alerts via policy if you want.

FireEye Endpoint Security



About the product

FireEye Endpoint Security provides endpoint protection software for Windows and macOS workstations, plus Windows servers. A variety of console types is available. These include cloud-based, hardware appliance, virtual appliance, and Amazon-hosted. We describe the cloud-based console in this review. As well as malware protection, the product includes investigative functions for analysing and remediating attacks. The product is designed to handle very large organizations, with support for up to 100,000 endpoints per appliance.

Advantages

- Attack investigation features
- Variety of console types available
- Suitable for medium- to large-sized enterprises
- Comprehensive search feature
- Containment feature lets you isolated infected devices

Management console

Dashboard

When you open the console, you will see an overview of key status items (screenshot above). These include the total number of hosts with alerts, with a breakdown by exploits and malware. Clicking on the *Total hosts with alerts* button opens the *Hosts with Alerts* page, shown below.

Hosts with alerts

Host	AVC SYSTEM	Agent Version	Last Sysinfo	Alerts	Quarantines
Windows 10 Pro GMT Summer Time	AVC SYSTEM	32.30.0	2020-07-24 11:59:06Z	18 ALERTS 7 min ago	18 QUARANTINES
Windows 10 Pro W. Europe Summer Time	WORKGROUP SYSTEM	32.30.0	2020-07-24 12:01:56Z	99+ ALERTS 46 hours ago	1085 QUARANTINES
Windows 10 Pro Pacific Daylight Time	WORKGROUP SYSTEM	32.30.0	2020-07-09 07:31:54Z	33 ALERTS 15 days ago	115 QUARANTINES

As the name suggests, this page displays details of protected devices with alerts that have not yet been dealt with. If you click on the plus sign for a device, you can see a list of alerts for that device, in chronological order. With malware alerts, a wealth of detail is provided for each one. This includes status (e.g. quarantined), detection method (e.g. signature), file path, MD5 and SHA1 hashes (but not SHA256), file size, last modified and last accessed times, process path, username of logged-on user, detection name, threat type, and times of first and last alerts for the item. Each threat can be acknowledged (marked as “read”), or marked as a false positive. You can also add comments to the threat details, for future investigation.

The *Hosts* pages also allow you to *contain* a device. This cuts all network connections to and from the device, with the exception of the management console. You can then investigate a threat without any risk of it spreading.

Alerts

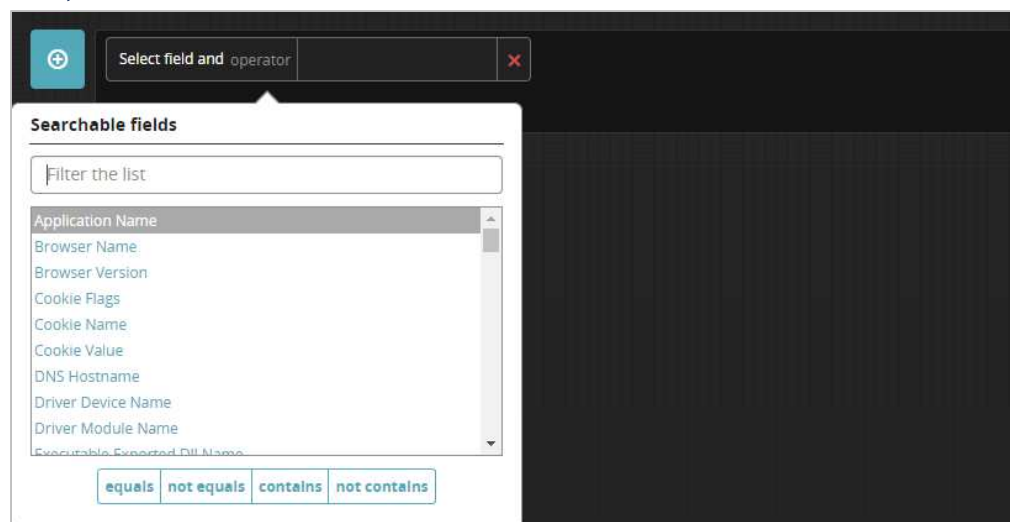
Acknowledged	Protection and Remediation	Alert Type	File Path	File Size
No	QUARANTINED	MAL	C:\Program Files\Google\Chrome\Application\chrome.exe	2020-07-22 14:15:58.86Z
No	QUARANTINED	MAL	C:\Program Files\Google\Chrome\Application\chrome.exe	2020-07-22 13:47:11.058Z
No	QUARANTINED	MAL	C:\Program Files\Google\Chrome\Application\chrome.exe	2020-07-22 13:47:11.058Z
No	QUARANTINED	MAL	C:\Program Files\Google\Chrome\Application\chrome.exe	2020-07-22 13:47:11.058Z
No	QUARANTINED	MAL	C:\Program Files\Google\Chrome\Application\chrome.exe	2020-07-22 13:47:11.058Z
No	QUARANTINED	MAL	C:\Program Files\Google\Chrome\Application\chrome.exe	2020-07-22 13:47:11.058Z
No	QUARANTINED	MAL	C:\Program Files\Google\Chrome\Application\chrome.exe	2020-07-22 13:47:11.058Z
No	QUARANTINED	MAL	C:\Program Files\Google\Chrome\Application\chrome.exe	2020-07-22 13:47:11.058Z
No	QUARANTINED	MAL	C:\Program Files\Google\Chrome\Application\chrome.exe	2020-07-22 13:47:11.058Z
No	QUARANTINED	MAL	C:\Program Files\Google\Chrome\Application\chrome.exe	2020-07-22 13:47:11.058Z

For a threat-centric rather than a device-centric view, you can go to the *Alerts* page. Here you can sort threats by name, file path, first or last detections, and hostname or IP address of the respective device. The options *Acknowledge*, *Mark False Positive* and *Add Comment* are provided here too.

Acquisitions

From the *Hosts* page, you can acquire a file or various items of diagnostic data from an individual device. The *Acquisitions* menu lets you download files that have been acquired from hosts, in order to analyse them.

Enterprise Search



This feature allows you to search the network for a very wide variety of items. These include application name, browser version, hostname, various executables, file names/hashes/paths, IP address, port, process name, registry key, service name/status/type/mode, timestamp, URL, username and Windows Event Message.

Policies

This feature is found in the *Admin* menu. Here you can configure numerous different aspects of the client protection policy. Examples are scans, whether to show the endpoint GUI on the client, logging, malware scan settings, polling frequency, tamper protection, scan exclusions, management server address and malware detection settings. Scans can be set to run on a schedule, or after a signature update or device boot.

Host Sets

These are simply groups of computers. They can be defined according to a wide variety of criteria, or simply by dragging and dropping from the list of all devices. These groups are used to apply different protection policies. The feature is found in the *Admin* menu.

Agent Versions

This is found in the *Admin* menu, and lets you download current and older versions of the endpoint agent for Windows and Mac systems. This allows the admin to e.g. avoid compatibility problems with a particular agent version on specific systems.

Appliance Settings

This page allows you to change settings for the management console itself, and is found in the *Admin* menu. There are controls for date and time, user accounts, notifications, network settings and licences, and more.

Windows Endpoint Protection Client

Deployment

Installer files in .msi format can be downloaded from the *Admin* menu, *Agent Versions*. As the name suggests, the current and earlier versions of the client (about 10 for each platform) are provided. The installer file can be run manually, via a systems management product, or using an AD script. You can use the automated update feature to keep installed devices on the latest version of the endpoint agent.

Functionality Check

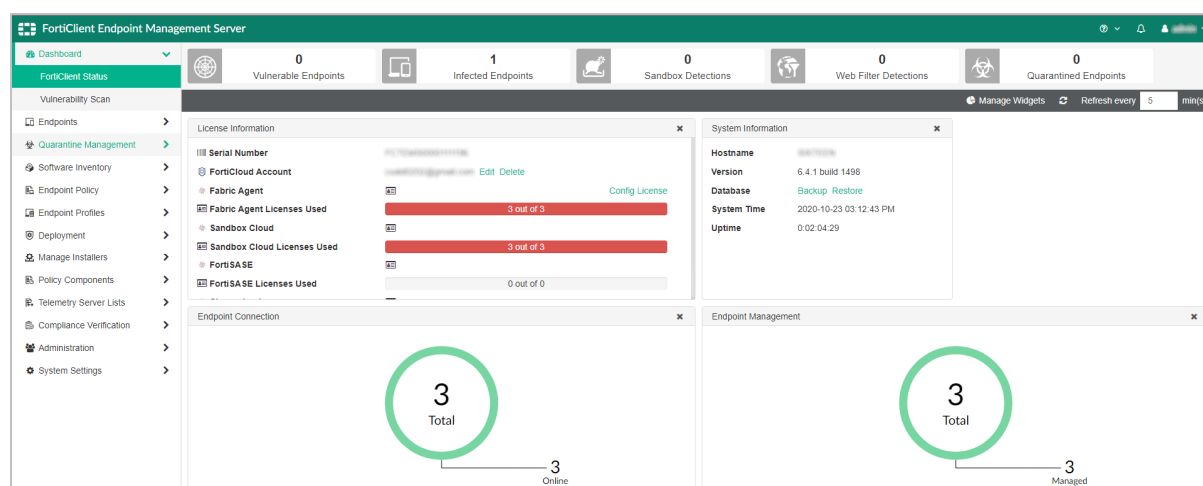
For our functionality test, we used the same settings as employed in the Main Test Series, where the option *Allow users the ability to restore files from quarantine* was enabled.

The user interface on protected endpoints consisted of a System Tray icon and program window. The window allowed users to see detection logs and quarantine, and to delete or restore quarantined items. No other controls were provided. We found that any Windows User Account (whether Standard or Administrator) could restore detected files from quarantine and run them. This effectively allowed all users to bypass the malware protection. We would thus recommend deselecting *Allow users the ability to restore files from quarantine* in the applicable policy.

If you wish, you can hide the user interface completely by deactivating the *Enable the Endpoint Agent Console on the host* policy option.

When we connected a flash drive containing malware samples to our test PC, and opened the drive in Windows Explorer, FireEye immediately detected and quarantined the malicious files. A pop-up notification was shown, but no user action was required or possible.

Fortinet FortiClient with EMS, FortiSandbox and FortiEDR



About the products

The package used in AV-Comparatives' Main Test Series consists of the server-based console FortiClient Endpoint Management Server (EMS), the cloud-based FortiEDR console, the FortiSandbox, and the FortiClient endpoint protection software. The EMS console has to be installed on a Windows Server operating system (2008 R2 or later). There is endpoint protection software for Windows clients and servers, plus macOS devices. As well as malware protection and threat investigation, the package includes other features such as telemetry and secure remote access. These are not covered by this review, however. The FortiClient endpoint protection software and EMS could be used by smaller businesses with tens of seats, but we feel the entire package as reviewed here is probably more suited to larger organisations.

Advantages

- Investigative features
- Telemetry feature
- Secure remote-access feature
- Detailed malware analysis
- Clickable graphics provide easy access to details pages

EMS Server Installation

EMS is a local server-based product. Installing the management console on a Windows Server system is very simple and requires almost no user interaction. You will need to restart the server to complete the installation, however. The console functionality can be accessed as a dedicated window, or via a web browser using the server's IP address.

EMS Management Console

The Enterprise Management Server console is navigated using a single menu column down the left-hand side. Clicking an item here populates the right-hand side of the window.



















Dashboard\FortiClient Status page

This page is what you see when you first log on to the console, and is shown in the screenshot above. It provides a graphical overview of the licensing, platform and client connection/management status. You can click on either of the two endpoint-related panels to access the devices page. A row of buttons along the top of the page show you vulnerable, infected and quarantined devices. Clicking on one of these will take you to a pre-filtered devices page, showing you just the specific devices in that category.

Dashboard\Vulnerability Scan page

The *Vulnerability Scan* page shows you software vulnerabilities that have been discovered. A “traffic light” graphic is used to show the severity. Colours go from green (low) through yellow (medium) to orange (high) and red (critical). Underneath this is a set of buttons indicate where the vulnerabilities lie. For example, operating system, browser, Microsoft Office and services are shown. Other panels list vulnerability-scan status, the top ten vulnerabilities, and the top ten endpoints with high-risk vulnerabilities.

Endpoints\All Endpoints page

	0		0		0		1		0
Not Installed		Not		Out-Of-Sync		Security Risk		Quarantined	
<div>Endpoints</div> <div> <input type="checkbox"/>  Right  [User] [IP Address] [MAC Address] ...  Policy Default  EMS No Events </div> <div> <input type="checkbox"/>  [Device Name]  [User] [IP Address] [MAC Address] ...  Policy Default  EMS No Events </div> <div> <input type="checkbox"/>  [Device Name]  [User] [IP Address] [MAC Address] ...  Policy Default  EMS  AV 5 </div>									

The *Endpoints\All Endpoints* page lists all the endpoints on your network. Other sub-pages allow you to filter the list by group, domain or workgroup. Details provided for each device are group, user account, IP address, policy used, server connection status and recent events/alerts. Graphical buttons along the top of the page show the number of endpoints that are not protected, not connected, out of sync, at risk, and quarantined. This lets you see how many devices need your attention. Clicking on an endpoint's entry opens the details page for that device. Here you can see a more detailed information, including hardware details, external IP address, MAC address, FortiClient version information and components installed.

Quarantine Management\Files page

As you would expect, this page shows you files that have been quarantined on protected endpoints. Details include device name, file name and hash, threat name, date and time quarantined, and number of endpoints affected. You can whitelist selected files by clicking *Allowlist & Restore*, after which they will be shown in the *Allowlist* page.

Endpoint Profiles\Manage Profiles page

Endpoint Profiles are standard client configuration policies that let you centrally change endpoint anti-malware settings. These include action on malware discovery, whether to show alerts, scheduled scans, and exclusions. There is a *Basic* view, which shows you the most popular settings, and an *Advanced* view, which gives you further configuration options.

Endpoint Policy\Manage Policies page

Policies in EMS might best be described as “super-policies” which include the *Profile* of client settings and allow for further configuration options on top of these.

Administration section

Under *Administration\Administrators* you can create user accounts for EMS analysts. On the *Admin Roles* page, you can manage the permissions that are assigned to different administrator levels. By default, there are five different levels, ranging from *Read-Only Administrator* to *Super Administrator*.

System Settings section

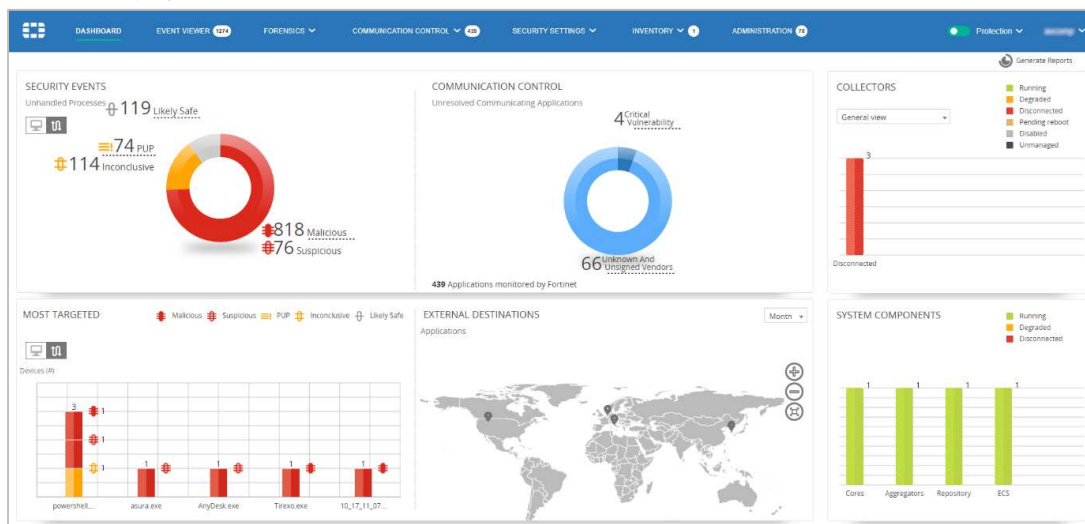
Here you can configure system-wide options. For example, on the *Server* page, you can configure security certificates and communications ports, and enable management of Chromebooks.

FortiEDR

FortiEDR is a separate endpoint detection and response platform, which has its own management console. This can be installed in the cloud, on-premise or as a hybrid solution.

FortiEDR Management Console

Dashboard page



The *Dashboard* page, shown above, uses bar and doughnut charts to provide a graphical overview of threats and suspicious processes. You can see numbers of malicious, potentially unwanted and *likely safe* processes that have been encountered on the network. There's also a chart of malicious processes that have targeted the greatest number of endpoints. A map of the world shows you the destinations of the most common network connections. If you mouse over the pin indicating a particular country, you can see the IP addresses to which the connections were made. Many of the *Dashboard* panels are clickable. For example, clicking on the *Security Events* chart takes the user to the *Events* page.

Events page

EVENTS

ID	DEVICE	PROCESS	CLASSIFICATION	DESTINATIONS	RECEIVED	LAST UPDATED
FolderGuard-20.9-setup.exe (1 event)			Likely Safe		19-Oct-2020, 02:12:45	
netsh.exe (6 events)			Suspicious		18-Oct-2020, 22:59:53	
ssm.exe (2 events)			Inconclusive		18-Oct-2020, 22:10:48	
kutuphane.ZDA64ZDA.exe (3 events)			Suspicious		18-Oct-2020, 03:03:53	
actvbslr.exe (1 event)			Inconclusive		17-Oct-2020, 10:44:01	
10_17_11_07_AY.exe (1 event)			Malicious		17-Oct-2020, 02:47:32	
91071	10_17_11_07_AY.exe	File Execution At...	Malicious		17-Oct-2020, 02:47:32	17-Oct-2020, 02:47:32
Certificate: Unsigned Process path: C:\Users\... Downloads\10_17_11_07_AY.exe Raw data items: 1						
msword-update.exe (1 event)			PUP		15-Oct-2020, 12:38:23	
HelpmeOmarIN.exe (1 event)			Inconclusive		14-Oct-2020, 04:10:52	
cassetup.exe (1 event)			Likely Safe		13-Oct-2020, 04:12:31	
758546H.exe (1 event)			Likely Safe		13-Oct-2020, 03:42:41	
Tirexo.exe (3 events)			Malicious		12-Oct-2020, 18:46:09	

CLASSIFICATION DETAILS

Malicious *ReverseEngineers*
 Threat name: Unknown
 Threat family: Unknown
 Threat type: Unknown

History

- Malicious, by FortinetCloudServices, on 17-Oct-2020, 02:47:46
- PUP, by Fortinet, on 17-Oct-2020, 02:47:32

Triggered Rules

- Execution Prevention
- Unconfirmed File Detected

ADVANCED DATA

Event Graph

Timeline: 1 Create → 2 Create → 3 Create → 4 Create → 5 Create → 6 Execute (Unconfirmed File Detected) → 7 Create

Event Viewer, shown below, gives details of security events. You can see the file name, date and time of notification, and a threat category, such as *Malicious*, *Suspicious*, *PUP* or *Inconclusive*. The *Advanced Data* panel shows you a graphical representation of the process execution and other processes involved. By selecting an event, the user can start an investigation by clicking on *Forensics*. Other pages include *Threat Hunting*; *Communication Control* (applications and policies); *Security Settings* (security policies and automated incident response); *Inventory* (collectors, IoT and system components) and *Administration* (licensing, organizations, users etc.).

Windows Endpoint Protection Client

Deployment

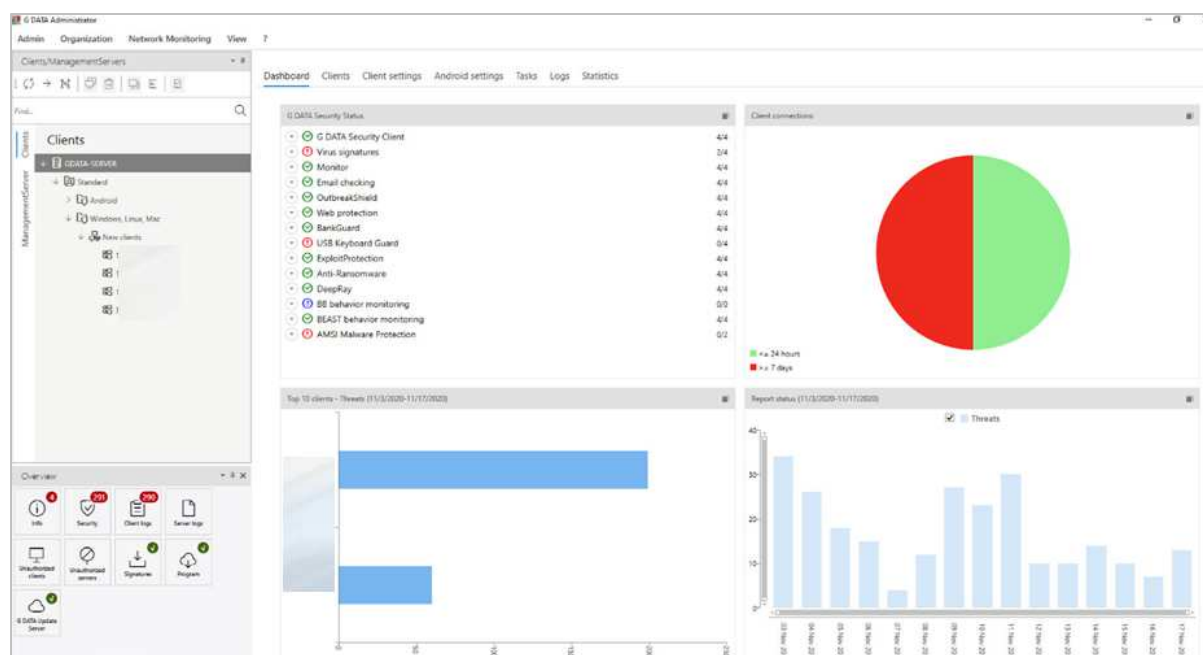
Before deploying the client software, you will need to activate *AntiVirus Protection* in the applicable profile under *Endpoint Profiles\Manage Profiles* in the management console. This enables the anti-malware features. Under *Manage Installers\Deployment Packages* you can then create an installer in .exe format with a specific program version and patch version. A URL to the server's repository is then displayed, which you can use to download the installer to client machines. The installer file can be run manually, via a systems management product, or using an AD script

Functionality check

The user interface on protected endpoints consists of a System Tray icon and a program window. Users can see the protection status and detection logs, and run quick, full custom and removeable-media scans. They can also scan a file, folder or drive using Windows Explorer's right-click menu.

When we connected a flash drive containing malware samples to our test PC, and opened the drive in Windows Explorer, Fortinet immediately detected and quarantined the malicious files. A pop-up alert was shown, which persisted until manually closed. No user action was required or possible. You can disable detection alerts via policy if you want.

G Data AntiVirus Business



About the product

G Data AntiVirus Business provides endpoint protection software for Windows and macOS workstations, plus Windows servers. This is managed using a server-based console, which can be installed on any current Windows Server or Windows client operating system. Multiple management servers can be used within an organisation, and managed from a single console. An option is available for protecting virtual machines, which uses a “light” agent and a virtual scan server. The product can manage networks with thousands of devices. We also feel it would be suitable for smaller businesses with tens of devices.

Advantages

- Familiar, MMC-like management console
- Groups can be synchronised with Active Directory
- Easy management of computer groups
- High degree of control over GUI of endpoint software
- Single installer file for management server and Windows endpoint protection client

Server Installation

G Data provide a single installer package which you can use to set up both the management console and the endpoint protection software. The console installation wizard lets you use an existing SQL Server installation if you have one. Alternatively, it can install SQL Server 2014 Express along with the management software. Installation is very quick and simple, and you can log on to the console with your Windows credentials. G Data’s own integrated authentication is available as an option.

Management Console

The *Management Server* and *Clients* buttons in the top left-hand corner allow you to switch between the respective computer types. Under *Management Server*, you can configure items for your administration server(s). These include console users, synchronisation with clients/subnet servers/Active Directory, distribution of software updates, and licence management. The remainder of the console description refers to the client management pages.

Clients pane

Here you can see and navigate the device group structure for each management server. By default, there are separate groups for computers (Windows, macOS and Linux) and Android mobile devices. You can easily make your own sub-groups within these, and they can be synchronised with Organisational Units if you use Active Directory. You could automatically install the G Data endpoint security client on computers just by adding them to a specific synchronised group. The group structure in the *Clients* pane also allows you to monitor, manage and configure devices based on group membership. If you click on the top-level group in the *Clients* pane, the configuration changes applied in the main pane (e.g. *Client Settings*) will apply to all computers. If you click on a sub-group, then the changes made will affect only the devices in that group. You can change the configuration of a device simply by moving it to a group with a different policy.

Dashboard page

For the selected server or group, the default *Dashboard* page of the console, shown above, provides a graphical display of 4 important status items. The first is the status of individual components, indicating what proportion of devices are correctly configured. Then there is the share of devices that have connected to the console recently. You can also see which clients have had the most detected threats. Finally, there is a timeline of important events.

Clients page

Client	Security status	Engine A	Engine B	Status as per	G DATA Security Client version	Last access	Virus signature update / time	Program update / time	Type
1909-73-01-01	Security risks have been detected	AVA 25.27703 (17.11.2020)	GD 27.20914 (17.11.2020)	11/17/2020 1:24:39 PM	15.0.0.53 (23.10.2020)	11/17/2020 1:26:02 PM	completed (11/17/2020 12:35 PM)	completed (8/12/2020 6:42 PM)	Windows
	Security risks have been detected	AVA 25.27702 (17.11.2020)	GD 27.20913 (17.11.2020)	11/17/2020 10:25:03 AM	15.0.0.53 (23.10.2020)	11/17/2020 10:27:46 AM	completed (11/17/2020 10:25 AM)	completed (8/12/2020 6:40 PM)	Windows
	No connection to server	AVA 25.25609 (11.05.2020)	GD 26.18695 (11.05.2020)	5/11/2020 5:16:35 PM	14.3.0.178 (11.02.2020)	5/11/2020 5:17:08 PM			Windows
	No connection to server	AVA 25.25609 (11.05.2020)	GD 26.18693 (11.05.2020)	5/11/2020 5:13:43 PM	14.3.0.178 (11.02.2020)	5/11/2020 5:15:20 PM	completed (5/11/2020 5:01 PM)		Windows

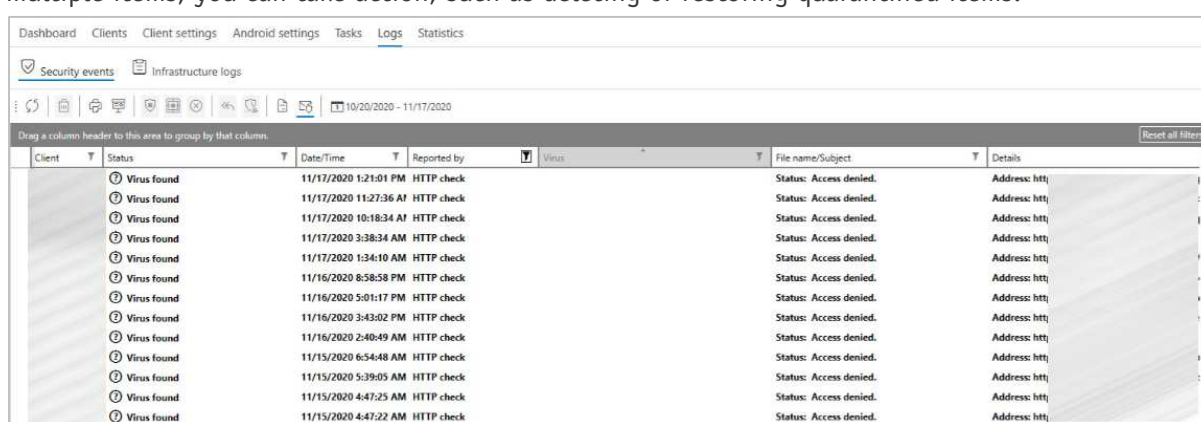
The *Overview* tab of the *Clients* page, shown above, displays a list of managed devices. You can see information such as status, definitions used, client version and operating system. The columns are customisable. Thus, you could also display the last active user, and various network items such as IP address and DNS server. You can group computers by the data in any of the columns, just by dragging the column header to the grey bar immediately above it. From the row of buttons along the top, you can run various tasks on computers. These include installing or uninstalling client software, updating the definitions and software, and deleting devices. So, you could e.g. group computers by *Virus signature update/time*, and then run an update task on any that are out of date. The *Software* button on the top toolbar provides a detailed inventory of programs installed on the client device(s). *Hardware* shows basic system details such as CPU, RAM, and free storage space.

Client settings page

The *Client settings* pages lets you configure some options such as automatic signature and program updates. You can also allow users a degree of interaction with the endpoint software on their PCs. For example, you could let them run scans and/or display the local quarantine.

As you would expect, the *Tasks* page lets you see the status of any tasks, such as installation, that you have set up. *Logs* provides a detailed list of relevant events. These include malware detections, updates, and settings changes. *Statistics* lists the status of individual protection components, such as *Email Protection* and *Anti-Ransomware*.

In the bottom left-hand corner of the console are a number of shortcuts to specific pages. The *Security* page, shown below, lists malware detections. Details provided are client name, status (action taken), date and time, detection component, threat name, file name, location and user. By selecting one or multiple items, you can take action, such as deleting or restoring quarantined items.



Client	Status	Date/Time	Reported by	Virus	File name/Subject	Details
	Virus found	11/17/2020 1:21:01 PM	HTTP check		Status: Access denied.	Address: http
	Virus found	11/17/2020 11:27:36 AM	HTTP check		Status: Access denied.	Address: http
	Virus found	11/17/2020 10:18:34 AM	HTTP check		Status: Access denied.	Address: http
	Virus found	11/17/2020 3:38:34 AM	HTTP check		Status: Access denied.	Address: http
	Virus found	11/17/2020 1:34:10 AM	HTTP check		Status: Access denied.	Address: http
	Virus found	11/16/2020 8:58:58 PM	HTTP check		Status: Access denied.	Address: http
	Virus found	11/16/2020 5:01:17 PM	HTTP check		Status: Access denied.	Address: http
	Virus found	11/16/2020 3:43:02 PM	HTTP check		Status: Access denied.	Address: http
	Virus found	11/16/2020 2:40:49 AM	HTTP check		Status: Access denied.	Address: http
	Virus found	11/15/2020 6:54:48 AM	HTTP check		Status: Access denied.	Address: http
	Virus found	11/15/2020 5:39:05 AM	HTTP check		Status: Access denied.	Address: http
	Virus found	11/15/2020 4:47:25 AM	HTTP check		Status: Access denied.	Address: http
	Virus found	11/15/2020 4:47:22 AM	HTTP check		Status: Access denied.	Address: http

Info displays event information such as software installation and client reboots. The *Signatures* page shows configuration options for definition updates. You can also run an update with a single click here. *Program* checks whether the management console itself is the latest available version.

Windows Endpoint Protection Client

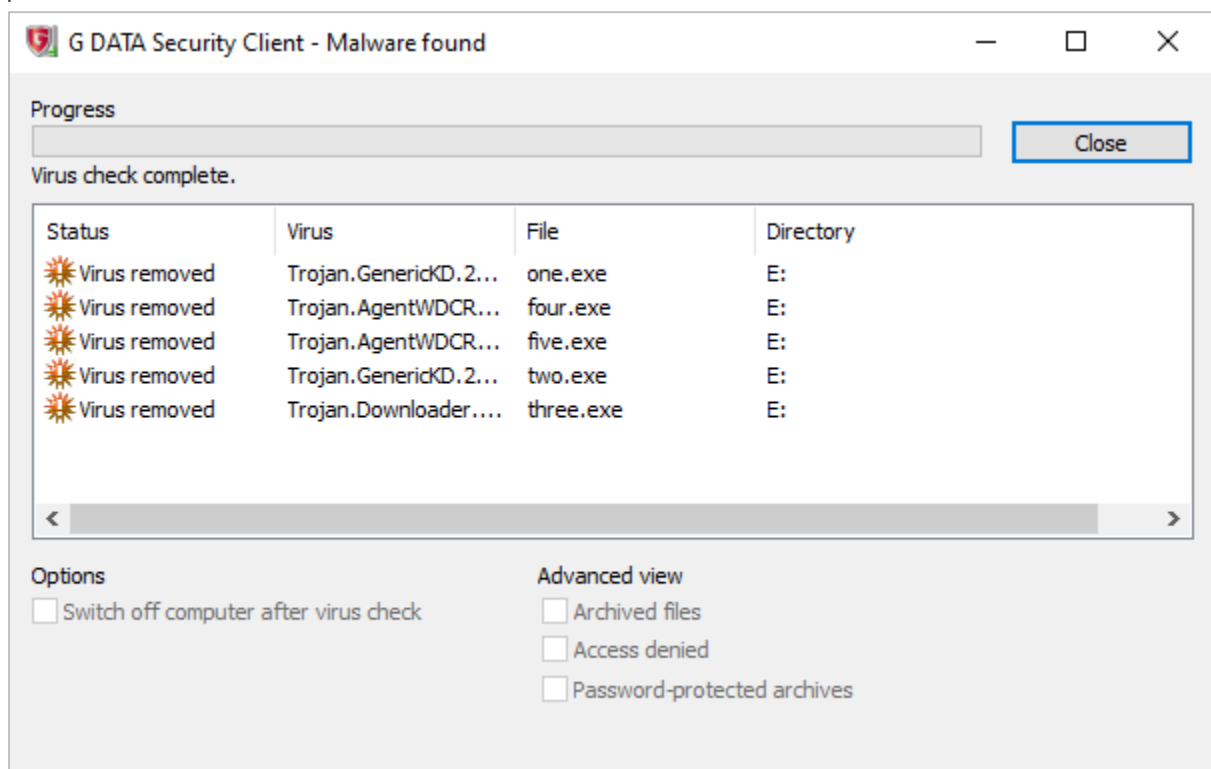
Deployment

Before deploying endpoint protection software to clients, you may need to adjust Windows Firewall settings on both server and clients to enable communication between them. When the console is first used, a deployment wizard runs, allowing you to push the endpoint software to clients over the network. This allows you to set up email notifications for e.g. malware detection or out-of-date clients. There is also the option to activate “DeepRay”, which is intended to detect disguised malware, and “BEAST”, G Data’s newest behaviour-blocking technology. This wizard can be re-run at any time from the Admin menu. Alternatively, you can run the installer manually on individual client devices, or use a systems management product or Active Directory integration. To connect the client to a management server, you just need to enter the hostname or IP address of the server in the setup wizard.

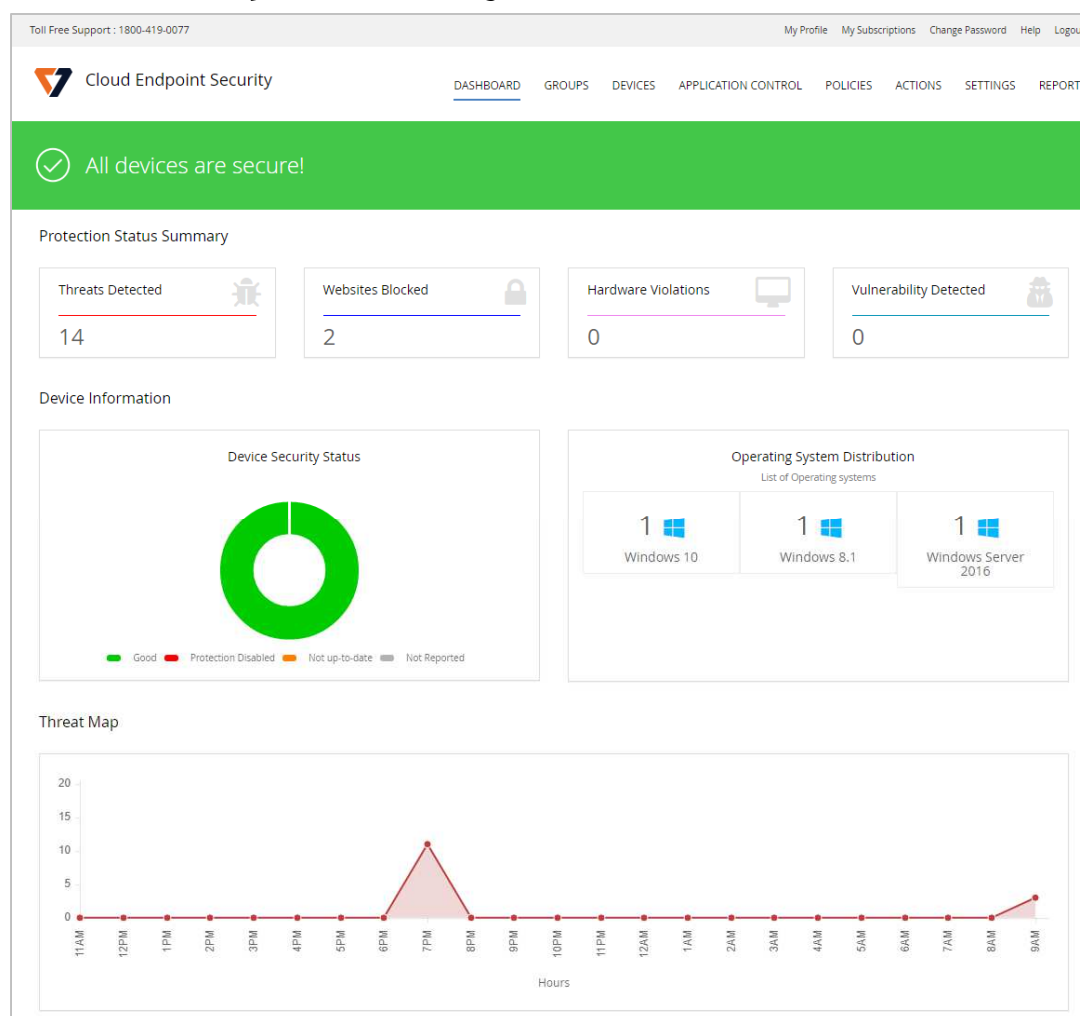
Functionality check

The user interface on protected endpoints consists simply of a System Tray icon. This can be used to run definition updates and display program information. By default, no other functionality is provided. However, by changing the policy, you could allow users to run scans (quick, full, custom and right-click); see quarantine; configure protection components. These can be selected individually. You can password protect the entire program, so that only authorised users have access to the functionality. It is also possible to hide the System Tray icon, thus leaving the product invisible.

When we connected a flash drive containing malware samples to our test PC, and opened the drive in Windows Explorer, G Data immediately detected and quarantined the malicious files. A pop-up alert (screenshot below) was shown, which persisted until manually closed. No user action was required or possible.



K7 Cloud Endpoint Security



About the product

K7 Cloud Endpoint Security provides endpoint protection software for Windows clients and servers. This is managed from a cloud-based console. The product is designed for enterprises of all sizes. We feel it is particularly suitable for smaller businesses and less-experienced administrators.

Advantages

- Suitable for micro-businesses upwards
- Easy-to-navigate console
- Help page shown at first logon provides a guide to the console
- Easy-to-use application control feature
- Granular control of functionality shown in endpoint protection client

Management console

When you log on for the first time, a help page is displayed, with concise explanations of the features and how to use them. All the console's functionality can be accessed from a single menu strip at the top of the window.

Dashboard page

After login, the console opens on the *Dashboard* page, which shows an overview of the system status. There are various detail panels, showing detected threats, blocked websites, violations of hardware policy, vulnerabilities detected, device security status, numbers of devices running specific Windows versions, and a timeline of threats discovered. There is a link from the *Device Security Status* panel to the *Protected Devices* page, so you can get more details just by clicking on it.

Groups page

The *Groups* page of the console lists device groups you have created. There are links to the policy applied to each group, and a list of tasks (such as scans and updates) that you can apply to all group members.

Devices page

Devices View and manage enrolled devices current level of security.			
<div> <div>All Devices</div> <div>Protected Devices</div> <div>Unprotected Devices</div> <div>At Risk Devices</div> </div>			
<div> <div>Search: Search Devices...</div> <div>Show 10 entries</div> </div>			
Device Name	Group	OS	Actions
Device Name	Default Group	Windows 10	
Device Name	Default Group	Windows 10	
Device Name	Default Group	Windows 10	
<div> <div>Showing 1 to 1 of 1 entries</div> <div> <div>Previous</div> <div>1</div> <div>Next</div> </div> </div>			

The *Devices* page\All Devices tab, shown in the screenshot above, lists individual computers on the network. The links in the *Actions* column let you view a computer's details, uninstall Endpoint Security, or change its group. Other tabs of the *Devices* page sort computers into the categories *Protected*, *Unprotected* and *At Risk*. This lets you see at a glance which devices need your attention.

Application Control page

Create New Rule

Save

Rule Name

Enter Rule Name

Rule Description

Enter Rule Description

Access

Block from Running

Search:

Search Application...

Show 10 entries

<input type="checkbox"/>	Application Name	Publisher	File Name	Digital Sign
<input type="checkbox"/>	MICROSOFT.PHOTOS.EXE	MICROSOFT.PHOTOS.EXE	MICROSOFT.PHOTOS.EXE	
<input type="checkbox"/>	Microsoft Office Click-to-Run Client	Microsoft Corporation	OFFICEC2RCLIENT.EXE	
<input type="checkbox"/>	Microsoft Malware Protection Command Line Utility	Microsoft Corporation	MPCMDRUN.EXE	
<input type="checkbox"/>	uhssvc	Microsoft Corporation	UHSSVC.EXE	

Showing 1 to 4 of 4 entries

Previous

1

Next

From the *Application Control* page, you can regulate which applications are allowed to run or access the LAN/Internet. This can be done very simply by selecting an application from the list, and clicking *Block from Running*, *Block Internet Access* or *Block Network Access* in the drop-down list. You can add an application not already on the list using its MD5 hash value. We note that a file's MD5 hash could potentially be spoofed, and suggest that SHA256 would be more secure.

Policies page

Policy Name

Default Policy

Description

Default Policy

ANTIVIRUS

BEHAVIOUR PROTECTION

FIREWALL

INTRUSION

WEB FILTERING

DEVICE CONTROL

CLIENT PRIVILEGES

On Access

Schedule Scan

Exclusion

Mail protection

☒ Enable On Access

What to scan

☒ All files
 ☐ Automatic Identification
 ☐ Scan only executable and vulnerable files
 ☒ Detect spyware and Adware
 ☐ Scan files on network
 ☐ Concede resources to operating system when the computer starts
 ☒ Perform background scan on running programs

Action for executable

☒ Clean automatically
 ☐ Quarantine if clean fails
 ☐ Report only, Don't take any action

The *Policies* page lets you control settings for the endpoint software. These are conveniently ordered into groups such as *Antivirus*, *Behaviour Protection*, *Firewall*, *Web Filtering* and *Device Control*. The *Antivirus* configuration tab is shown above.

Actions page

Under *Actions* you can create tasks to run on individual computers or groups. Available tasks include a variety of scans and a client update.

Settings page

The *Settings* page lets you download installation packages for the endpoint protection software, and configure email notifications.

Reports page

Reports page provides a very simple means of running reports on items such as detected threats, and vulnerabilities, websites blocked, and scan results.

Windows Endpoint Protection Client

Deployment

On the *Settings* page you can download an installation package (full or light) in .exe format. You can specify the group that the computer should be added to. The installer file can be run manually, via a systems management product, or using an AD script. You can also email it to users directly from the download page. The setup wizard is very quick and easy, so even non-expert users would have no difficulty with it. Users with Windows Administrator Accounts can be prevented from uninstalling the software, by ensuring the *Uninstall Endpoint Security* setting in the applicable policy is disabled.

Functionality check

The user interface on protected endpoints consists of a System Tray icon and a program window. Users can see the protection status, run updates, and run quick, full, custom and rootkit scans. They can also scan a file, folder or drive using Windows Explorer's right-click menu. By changing policy, you can give users full control of the program, or lock it down completely.

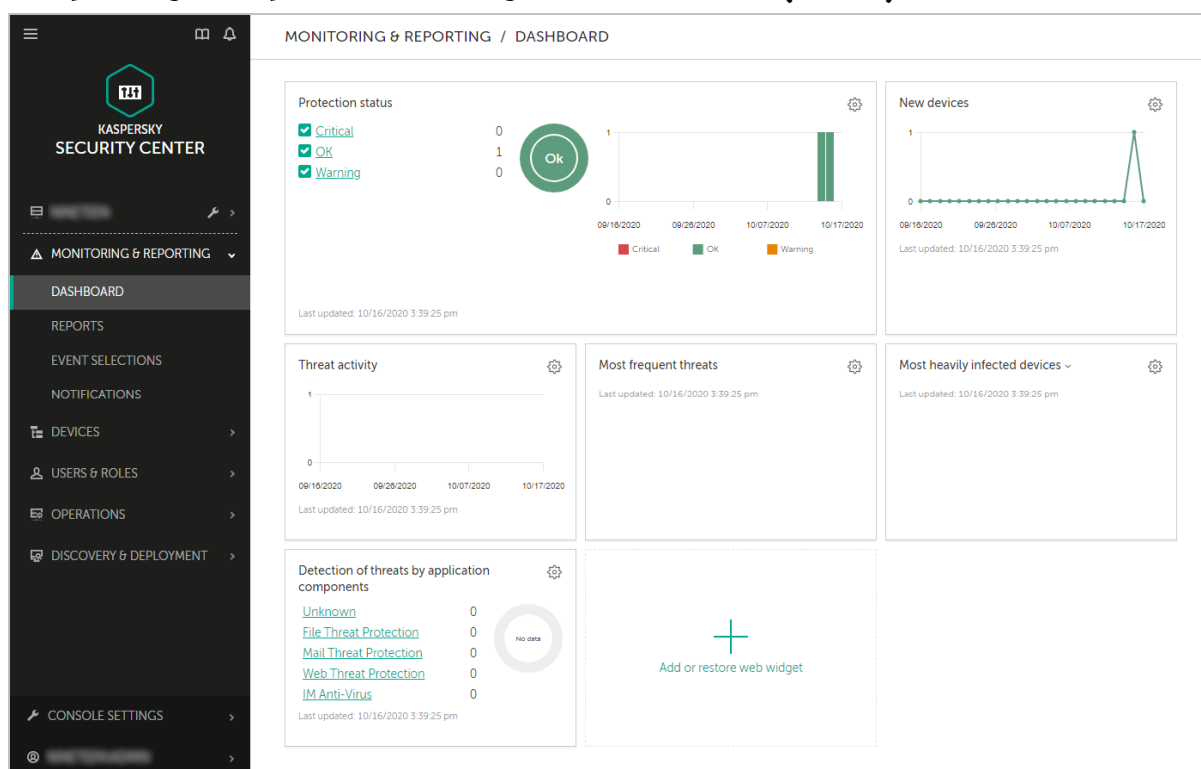
When we connected a flash drive containing malware samples to our test PC, and opened the drive in Windows Explorer, K7 immediately detected and quarantined the malicious files. A pop-up alert was shown, which closed after a few seconds. No user action was required or possible. You can disable alerts by policy if you wish.

Note

While testing K7 Endpoint Security, we found a serious security issue¹² with it, which also applied to its consumer product. We immediately reported this to K7, who have now fixed the problem in all its products. We recommend users of K7 to ensure that their products are up to date.

¹² <https://support.k7computing.com/index.php?/solutions/view-article/Advisory-issued-on-23rd-October-2020>

Kaspersky Endpoint Security for Business (KESB) - Select



About the product

Kaspersky Endpoint Security for Business (KESB) Select is a tier of Kaspersky's Endpoint Security for Business product line. It is aimed at medium-sized businesses and larger enterprises. The product provides endpoint protection software for Windows and macOS workstations, plus Windows servers. The product is managed by a server-based console. Administrators can choose between a modern web-based interface and a legacy MMC-based GUI. We have looked at the web-based console (shown in the screenshot above) in this review.

Advantages

- Choice of web-based or MMC console
- Straightforward console installation with quick-start guide
- Deployment wizard for simplified client installation
- Web console pages can be customised
- Granular role-based control permissions for console administrators

Server installation

Installing the management console is a straightforward process for an experienced administrator. A preinstalled SQL database is required, which could be the free Microsoft SQL Server Express. You can use Windows credentials to log in to the console if you want. When you first run the web-based console, an optional brief tutorial is shown. This highlights the most important functions, and provides a brief description of each. Next, the *Quick Start Wizard* takes you through initial configuration. This includes defining the type of computers to be protected (server/workstation) and operating systems. It also allows you to set up notifications.

Management console

The console functions are arranged in a single menu column on the left-hand side. The main menu items are *Monitoring & Reporting*, *Devices*, *Users & Roles*, *Operations*, and *Discovery & Deployment*. Each of these items expands to show sub-pages.

Monitoring and Reporting section

The *Dashboard* page (shown above) provides a graphical overview of key information. This includes protection status, new devices, plus details of threats and infected devices. The page is customisable, and you can add/remove various panels (*Web Widgets*) as you please.

The *Reports* page lets you run a wide variety of reports, on topics such as protection status, deployment, updates and threats. These can be easily accessed from a preconfigured list.

Under *Event Selections*, you can run reports on categories like user requests, critical events, functional failures and warnings.

On the *Notifications* page, there is a list of recent alerts. You can filter these by topic, such as deployment, devices or protection.

Devices section

The *Policies and Profiles* page lets you create and apply new configuration policies. On the *Tasks* page you can carry out everyday maintenance and backup tasks, such as updates.

DEVICES / MANAGED DEVICES									
Current path: NINETEEN									
+ Add devices × Delete + New task ⇅ Move to group Connect to Remote Desktop ↻ Refresh ⇅ Export rows to CSV file ⇅ Export rows to TXT file Grant access to the device in offline mode									
Force synchronization ⚙ Filter									
<input type="checkbox"/>	Name	Last connected to Administration Server	Network Agent is running	Status	Parent group	Real-time protection	Real-time protection status	Operating system	Created
<input type="checkbox"/>	192.168.1.1	10/16/2020 4:48:53 pm	🟢	🟢	Managed devices	🟢	Running	Microsoft Windows 8.1 6.3	10/16/2020 2:30:17
<input type="checkbox"/>	192.168.1.2	10/16/2020 4:48:36 pm	🟢	🟢	Managed devices	🟢	Running	Microsoft Windows Server 2016 10.0	10/16/2020 1:11:37
<input type="checkbox"/>	192.168.1.3	10/16/2020 4:48:55 pm	🟢	🟢	Managed devices	🟢	Running	Microsoft Windows 10 10.0	10/16/2020 2:33:06

The *Managed Devices* page, shown above, lists managed computers, along with the status of major components. You can filter the list using criteria such as status, real-time protection or last connection time. The list is customisable, and so you can add additional criteria like operating system or network details. By selecting individual devices, you can run tasks on them. These include installation, deinstallation, or changing group membership.

You can click on an individual computer's name to see its details page. Here you can see various details of the device, shown in different tabs. These include operating system, network information, protection status, installed Kaspersky applications, active policies, plus running protection components and tasks. On the *Events* page, you can see detailed information on malware detection and remediation.

The screenshot below illustrates three separate stages of one malware, namely detection, backup copy being made, and deletion:

Export to file Copy Delete							Filter
	Time	Event	Description	Application	Version number	Importance level	Task
<input type="checkbox"/>	10/18/2020 7:03:15 pm	Object deleted	Result: Deleted: UDS DangerousObject.Multi.Generic User: Administrator Object C: C:\Users\Administrator\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\B6000000\image001.png Hash: SHA256: 00	Kaspersky Endpoint Security for Windows (11.4.0)	11.4.0.233	Warning	File Threat Protection
<input type="checkbox"/>	10/18/2020 7:03:15 pm	A backup copy of the object was created	Event type: A backup copy of the object was created Application: Windows Explorer ApplicationName: explorer.exe ApplicationPath: C:\Windows\ ApplicationProcess ID: 5860 User: Administrator Component: File Threat Protection ResultDescription: Backup copy created ResultName: UDS DangerousObject.Multi.Generic ResultThreat level: High ResultPrecision: Exactly Object C: C:\Users\Administrator\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\B6000000\image001.png Object Type: File ObjectPath: C:\Users\Administrator\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\B6000000\image001.png ObjectName: five.exe Hash: SHA256: 00	Kaspersky Endpoint Security for Windows (11.4.0)	11.4.0.233	Info	File Threat Protection
<input type="checkbox"/>	10/18/2020 7:03:15 pm	Malicious object detected	Result: Detected: UDS DangerousObject.Multi.Generic User: Administrator (Active user) Object: C:\Users\Administrator\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\B6000000\image001.png Reason: Cloud analysis Hash: SHA256: 00	Kaspersky Endpoint Security for Windows (11.4.0)	11.4.0.233	Critical	File Threat Protection

The *Device Selections* page lets you find devices in pre-configured groups. Examples include *Databases are outdated* and *Devices with Critical Status*.

Users & Roles section

Under *Users*, you can see a list of predefined console users, along with Windows local and domain accounts for the Windows computers on the network. On the *Roles* page, users can be assigned one of 16 different management roles for the console, allowing very granular access.

Discovery & Deployment section

This includes various features for discovering unmanaged devices on the network, and deploying software to them. *Discovery* lets you look for devices on the network by e.g. IP address ranges or workgroup/domain membership. *Unassigned Devices* shows computers that have been found on the network but are as yet unmanaged.

Operations section

Amongst other things, the *Operations* tab contains *Licensing* and *Repositories*. The latter includes the quarantine functions, and details of the hardware on managed devices. Under *Patch Management**Software Vulnerabilities* you can see missing Windows Updates (amongst other things):

OPERATIONS / PATCH MANAGEMENT / SOFTWARE VULNERABILITIES

To configure and manage the fixing of vulnerabilities in third-party software with maximum efficiency, we recommend that you follow the [main usage scenario](#).

Preset filters

Show all

Statistics of vulnerability on devices

Run Vulnerability Fix Wizard

Fix vulnerability

Export rows to CSV file

Export rows to TXT file

✓	Name	Application	Severity level	Recommended major patch for fix
✓	KLA11772	Windows Server 2019	Critical	2020-05 Cumulative Update for .NET Framework 3.5, 4.7.2 and 4.8 for Windows Server 2019 for x64 (KB4556441)
✓	KLA11810	Windows Server 2019	Medium	2020-06 Security Update for Adobe Flash Player for Windows Server 2019 for x64-based Systems (KB4561600)
✓	KLA11859	Windows Server 2019	Critical	2020-07 Cumulative Update for .NET Framework 3.5, 4.7.2 and 4.8 for Windows Server 2019 for x64 (KB4566516)
✓	KLA11934	Windows Server 2019	Critical	2020-08 Cumulative Update for .NET Framework 3.5, 4.7.2 and 4.8 for Windows Server 2019 for x64 (KB4570505)

Windows endpoint protection software

Deployment

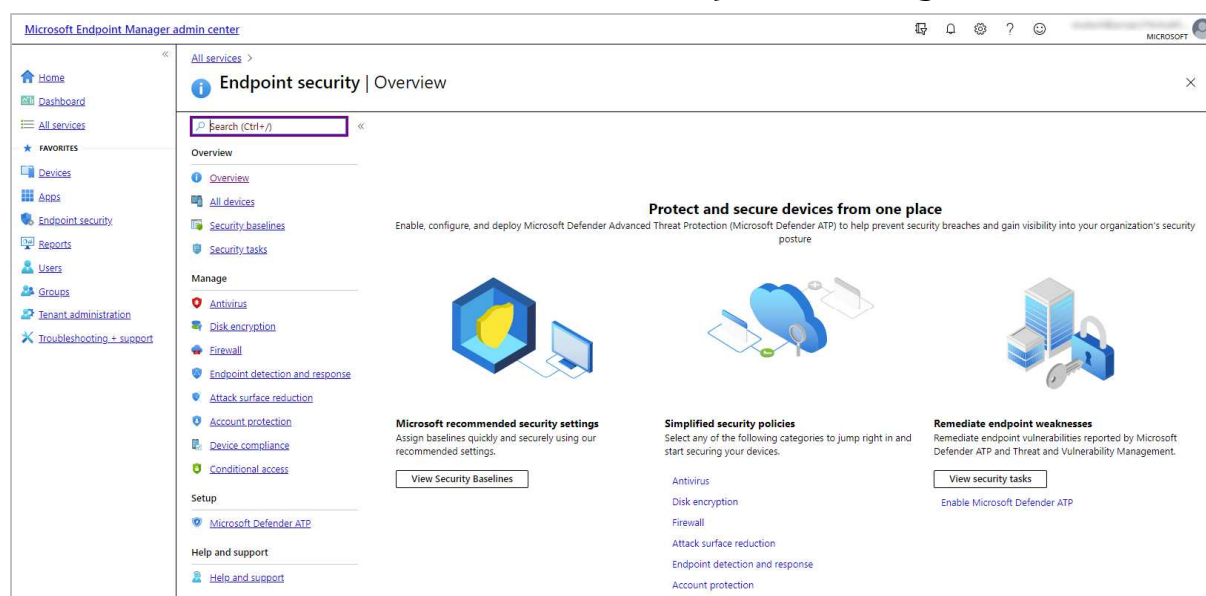
Before deploying Kaspersky Endpoint Security to clients, you may need to adjust Windows Firewall settings on both server and clients to enable communication between them. When the console is first used, a deployment wizard runs, allowing you to push the endpoint software to clients over the network. This can be (re)run later from *Discover & Deployment\Deployment & Assignment\Quick Start Wizard*. It is a very neat and simple process. The endpoint protection software could also be deployed using a systems management product or Active Directory. Alternatively, you can create a standalone, single-file installation package from *Discovery & Deployment\Deployment & Assignment\Installation Packages*. This will be automatically placed in a shared folder on the server. You can also email an installation link to users directly from the same page of the console. The setup wizard has some options, but a default installation would be simple enough for non-technical users. You can prevent users with Windows User Accounts from uninstalling the software using the *Password protection* setting in the applicable policy.

Functionality check

The Windows desktop protection application consists of a System Tray icon and program window. Users can run manual scans of both local and remote drives, folders or files by means of Windows Explorer's right-click menu. They can also check files for reputation in the Kaspersky Security Network, again using the Explorer context menu. You can hide the interface completely using the applicable policy, if you so choose.

When we connected a flash drive containing malware samples to our test PC, and opened the drive in Windows Explorer, Kaspersky immediately detected and quarantined the malicious files. No alert was shown. However, you can enable alerts by means of policy if you want.

Microsoft Defender with Microsoft Endpoint Manager



About the product

Microsoft Endpoint Manager allows administrators to centrally manage and monitor features and settings on all types of devices. In this report, we have only covered the management-console functions relating to endpoint security for Microsoft Defender Antivirus, Microsoft's own antivirus program, which is built into the Windows 10 operating system.

Microsoft Endpoint Manager is available to customers of Microsoft's cloud services for business; licensing varies based on the type of subscription. It can be used to administer a wide range of Microsoft functionality and services including Microsoft Intune, Configuration Manager, Endpoint Analytics, endpoint security, tenant-attach, co-management, and Windows Autopilot.

Advantages

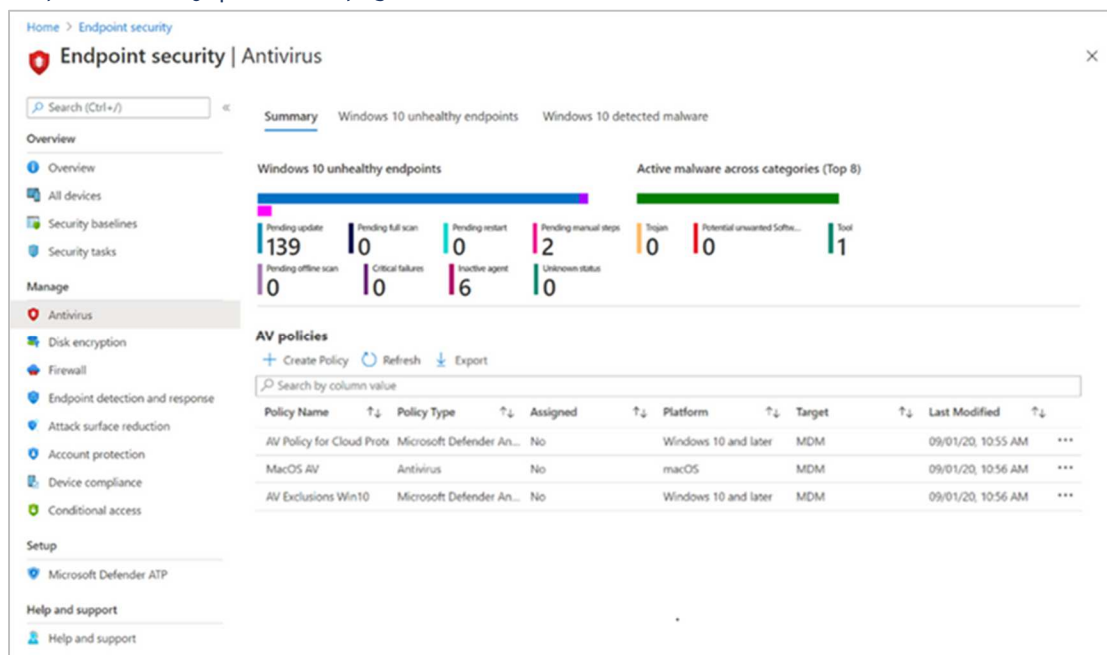
- Controls all Windows security settings
- Console is customisable
- Exceptionally simple client deployment
- Suitable for businesses of all sizes using Microsoft cloud services for business
- Granular control of security options

Management Console

Endpoint Security | Overview page

This is shown in the screenshot above. It is the main dashboard for the endpoint security features of the platform. Here you can see an overview of the individual protection components that can be configured. Examples are *Antivirus*, *Disk Encryption*, and *Firewall*. You can also view *Security Baselines*. These are policies with recommended settings for all security-related features in Windows. As well as Microsoft Defender Antivirus, the baselines also cover Microsoft browsers, Windows Firewall, BitLocker, SmartScreen, Wi-Fi settings, Remote Desktop and Windows Hello for Business, amongst other things.

Endpoint Security | Antivirus page



The *Summary* tab provides an overview of the security status of your network, by showing the number of *unhealthy endpoints*, i.e. devices with some kind of security-related problem.

Below this, under *AV policies*, you can create and edit your own antivirus policies. *AV Configuration* policies let you define settings for malware protection features. These are divided into categories: *Cloud Protection*, *Microsoft Defender Antivirus Exclusions*, *Real-Time Protection*, *Remediation*, *Scan*, *Updates* and *User Experience*.

Configuration options for each category are neatly laid out in a list, with each item having its own drop-down menu for its settings. A little information button next to each item displays a succinct explanation of the component and its settings. Examples of options found in the *Real-Time Protection* section are *Enable on-access protection*, *Turn on behaviour monitoring*, *Turn on network protection*, and *Scan scripts that are used in Microsoft browsers*.

The *User Experience* category has just one setting: *Allow user access to Microsoft Defender app*. Deselecting this hides the Microsoft Defender Antivirus (Windows Security) interface and suppresses malware alerts on client devices. However, a much more granular approach is also possible. *Security Experience* policies allow you to hide specific interface areas of the Windows Security app, such as *Firewall and Network Protection* or *App & Browser Control*.

The *Windows 10 unhealthy endpoints* tab of the *Endpoint Security\Antivirus* page displays a report of devices that require attention. Details include the status of malware protection, real-time protection, and network protection. As with other pages, you can modify the layout using the column picker to modify fields, change to a grid view for better searching, sort by any column, and export the list of records to a .csv file to save locally.

On the *Windows 10 detected malware* tab you can see devices and users with active malware. This view includes details such as malware state, active malware, category and severity. You can take remote actions here including restart, quick scan, full scan, or update signatures, to help resolve the problem.

Devices | All devices page

Dashboard > Devices

Devices | All devices

Search (Ctrl+/) Refresh Filter Columns Export Bulk Device Actions

Search by IMEI, serial number, email, user principal name, device name, management name, phone number, model, or manufacturer

Showing 1 to 1 of 1 records

Device name	Managed by	Ownership	Compliance	OS	OS version	Last check-in	Enrolled
DESKTOP-123456	Intune	Personal	Compliant	Windows	10.0.18363.1082	10/14/2020, 12:50:59 ...	10/14/2020, 12:50:59 ...
DESKTOP-123456	Intune	Personal	Compliant	Windows	10.0.18363.1082	10/14/2020, 12:50:59 ...	10/14/2020, 12:50:59 ...
DESKTOP-123456	Intune	Personal	Compliant	Windows	10.0.18363.1082	10/14/2020, 12:50:59 ...	10/14/2020, 12:50:59 ...

By platform

- Windows
- iOS/iPadOS
- macOS
- Android

Device enrollment

- Enroll devices

Here you can see a complete list of the devices on your network. Default columns show device name, ownership, platform, operating system version and date/time of last contact. You can customise the page by removing columns you don't need and adding other ones. Possibilities include device state, enrolment date, security patch level, manufacturer, model, serial number and Wi-Fi MAC address. The *Filter* button at the top of the page lets you filter the list using various criteria. Examples are ownership, compliance and OS. *Bulk Device Actions* lets you carry out tasks, such as rename, restart or delete, on the selected devices. Clicking on an individual device opens the *Device details* page, shown below.

Device details page

Retire Wipe Delete Remote lock Sync Reset passcode Restart Fresh Start Autopilot Reset Quick scan Full scan

Restart: Completed

Essentials

Device name : DESKTOP-123456

Management name : DESKTOP-123456, 10/14/2020_9:24 AM

Ownership : Personal

Serial number : DESKTOP-123456-123456-123456-123456-123456-123456-123456-123456-123456-123456

Phone number : ---

Device manufacturer : Microsoft, Inc.

Primary user (preview) : User1

Enrolled by : User1

Compliance : Compliant

Operating system : Windows

Device model : DESKTOP-123456

Last check-in time : 10/14/2020, 4:01:30 PM

Remote assistance : TeamViewer connector not configured

See less

Device actions status

Action	Status	Date/Time	Error
Restart	Complete	10/14/2020, 11:04:03 AM	

Here you can see the status of recent tasks, along with device-specific information such as manufacturer, model, serial number and primary user. The menu bar along the top of the page provides a number of management options. You can run updates and quick or full scans, and lock or restart the device. It's also possible to wipe or delete the device, or give it a *Fresh Start*. The latter is the equivalent of the *Reset this PC* function found in the settings of Windows 10. It essentially resets the software to factory settings, with options to keep or delete user data.

Windows Endpoint Protection Client

Deployment

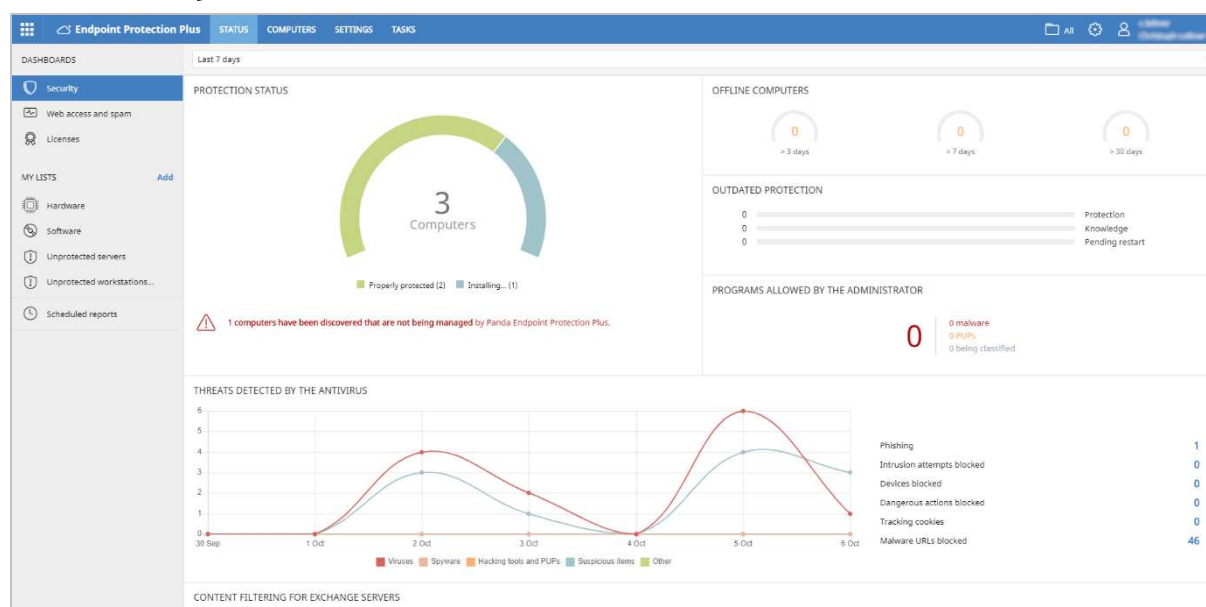
This is extremely simple, as Microsoft Defender Antivirus is already integrated into the Windows 10 operating system. For a domain-joined machine, connecting a client device to Microsoft Endpoint Manager is as simple as signing in with an appropriate business account in the *Accounts\Access work or school* section of Windows Settings. Users that don't have a domain, or who purchase a machine that is not yet configured on a domain, users can manually add their work account under Windows 10 device | Accounts | Add Work or school Account. When they log in with that work or school account, the security or device settings configured in Microsoft Endpoint Manager will automatically be applied.

Functionality check

The Windows Security app on the client PC allows access to the Microsoft Defender Antivirus functionality. By default, users can see security status and detection logs, and run scans. There is choice of *Quick*, *Full*, *Custom* and *Offline Scans*. Users can also start a scan on a drive, folder or file using Windows Explorer's right-click menu. If you prefer, you can hide the Windows Defender interface by policy. In this case, no interface or alerts will be shown on the client PC (the administrator will still see the alerts in the console).

When we connected a flash drive containing malware samples to our test PC, and opened the drive in Windows Explorer, Microsoft Defender immediately detected and quarantined the malicious files. A pop-up alert was shown, which closed after a few seconds. No user action was required or possible. However, clicking on the alert opened the Microsoft Defender window with further information about the threat. This is also displayed in Microsoft Endpoint Manager.

Panda Endpoint Protection Plus on Aether



About the product

Panda Endpoint Protection Plus on Aether provides endpoint protection software for Windows and macOS workstations, plus Windows servers. This is managed using a cloud-based console. The product can manage networks with tens of thousands of devices. We feel it would also be suitable for smaller businesses with tens of seats.

Advantages

- Easy-to-navigate console
- Clickable access gives easy access to details pages
- Network discovery process ensures all devices are protected
- Detailed information for individual devices
- Customisable menu panel

Management Console

Status tab

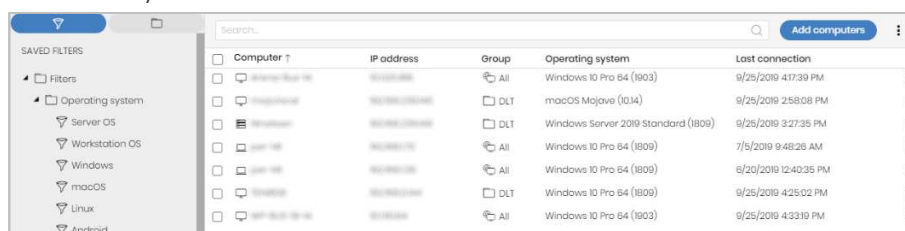
A status overview is provided on the *Status* tab/*Security* page (screenshot above), which opens by default. There are pie and bar charts for the items shown, which include *Protection Status*, *Offline Computers*, *Outdated Protection*, and *Programs Allowed by the Administrator*. You can click through for more detailed information. For example, clicking on the main *Protection Status* graphic takes you to the *Computers* page. The console's detection log/quarantine function is accessed by clicking on *Threats detected by the antivirus*. Here you can see affected computers and their IP addresses and groups, threat type and path, action taken (e.g. blocked/quarantined/deleted), and date and time.

The *Status* tab includes a left-hand menu column, from which you can open additional status pages. *Web access and spam* shows categories of website, such as webmail, games and business, which users have accessed. *Licenses* is self-explanatory. A section called *My Lists* provides simple but useful overviews of different aspects of the network. There are links for *Hardware* and *Software* of managed computers, plus *Unprotected Workstations* and *Unprotected Servers*. *Scheduled reports* lets you customise details to be sent out and when to send them.

The *My Lists* section is customisable, and a number of other categories can be added. These include *Computers with protection issues*, *Unprotected endpoints*, *Intrusion attempts blocked*, and *Threats detected by the antivirus*. These all help you to see quickly if there are any security issues that need to be addressed. The envelope icon in the top right-hand corner of the page lets you email scheduled alerts relating to the currently viewed list.

Computers tab

The *Computers* tab, shown below, lists computers on the network. You can filter by various criteria, including OS, hardware and installed software. You can also display computers by management group. This page shows all the protected computers and mobile devices. It is very clearly laid out, and shows essential information. A Windows-like folder tree on the left lets you filter devices by OS, device type, or hardware/software criteria.



Computer	IP address	Group	Operating system	Last connection
Windows Server 2019	10.0.0.100	All	Windows 10 Pro 64 (1803)	9/25/2019 4:17:39 PM
MacBook	10.0.0.101	DLT	macOS Mojave (10.14)	9/25/2019 2:58:08 PM
Windows Server 2019 Standard	10.0.0.102	DLT	Windows Server 2019 Standard (1809)	9/25/2019 3:27:35 PM
Windows 10 Pro 64	10.0.0.103	All	Windows 10 Pro 64 (1809)	7/5/2019 9:48:26 AM
Windows 10 Pro 64	10.0.0.104	All	Windows 10 Pro 64 (1809)	9/20/2019 12:40:35 PM
Windows 10 Pro 64	10.0.0.105	DLT	Windows 10 Pro 64 (1809)	9/25/2019 4:25:02 PM
Windows 10 Pro 64	10.0.0.106	All	Windows 10 Pro 64 (1803)	9/25/2019 4:33:19 PM

From the computers page, you can also create and manage computer groups, which can be synchronised with Active Directory. We would say that this functionality is not very easy to find, as we had to explore the interface for a while before locating it.

Clicking on the name of a computer opens the details page for that device, shown below. Here you can find network and domain information, OS details, Panda agent and endpoint client versions, and more. The status of individual protection components is also shown. The *Hardware* tab provides details of the CPU, RAM, system disk and BIOS, along with their usage statistics. Clicking on *Software* allows you to see information on installed programs, while *Settings* shows the policy and network configurations. A menu bar at the top of the page lets you move or delete the device, run one-off or scheduled scans, reinstall software, and reboot the computer.

Details	Hardware
Computer	
Name:	Test
Description:	Change
IP addresses:	192.168.1.101, 192.168.1.102, 192.168.1.103, 192.168.1.104, 192.168.1.105, 192.168.1.106, 192.168.1.107, 192.168.1.108, 192.168.1.109, 192.168.1.110, 192.168.1.111, 192.168.1.112, 192.168.1.113, 192.168.1.114, 192.168.1.115, 192.168.1.116, 192.168.1.117, 192.168.1.118, 192.168.1.119, 192.168.1.120, 192.168.1.121, 192.168.1.122, 192.168.1.123, 192.168.1.124, 192.168.1.125, 192.168.1.126, 192.168.1.127, 192.168.1.128, 192.168.1.129, 192.168.1.130, 192.168.1.131, 192.168.1.132, 192.168.1.133, 192.168.1.134, 192.168.1.135, 192.168.1.136, 192.168.1.137, 192.168.1.138, 192.168.1.139, 192.168.1.140, 192.168.1.141, 192.168.1.142, 192.168.1.143, 192.168.1.144, 192.168.1.145, 192.168.1.146, 192.168.1.147, 192.168.1.148, 192.168.1.149, 192.168.1.150, 192.168.1.151, 192.168.1.152, 192.168.1.153, 192.168.1.154, 192.168.1.155, 192.168.1.156, 192.168.1.157, 192.168.1.158, 192.168.1.159, 192.168.1.160, 192.168.1.161, 192.168.1.162, 192.168.1.163, 192.168.1.164, 192.168.1.165, 192.168.1.166, 192.168.1.167, 192.168.1.168, 192.168.1.169, 192.168.1.170, 192.168.1.171, 192.168.1.172, 192.168.1.173, 192.168.1.174, 192.168.1.175, 192.168.1.176, 192.168.1.177, 192.168.1.178, 192.168.1.179, 192.168.1.180, 192.168.1.181, 192.168.1.182, 192.168.1.183, 192.168.1.184, 192.168.1.185, 192.168.1.186, 192.168.1.187, 192.168.1.188, 192.168.1.189, 192.168.1.190, 192.168.1.191, 192.168.1.192, 192.168.1.193, 192.168.1.194, 192.168.1.195, 192.168.1.196, 192.168.1.197, 192.168.1.198, 192.168.1.199, 192.168.1.200, 192.168.1.201, 192.168.1.202, 192.168.1.203, 192.168.1.204, 192.168.1.205, 192.168.1.206, 192.168.1.207, 192.168.1.208, 192.168.1.209, 192.168.1.210, 192.168.1.211, 192.168.1.212, 192.168.1.213, 192.168.1.214, 192.168.1.215, 192.168.1.216, 192.168.1.217, 192.168.1.218, 192.168.1.219, 192.168.1.220, 192.168.1.221, 192.168.1.222, 192.168.1.223, 192.168.1.224, 192.168.1.225, 192.168.1.226, 192.168.1.227, 192.168.1.228, 192.168.1.229, 192.168.1.230, 192.168.1.231, 192.168.1.232, 192.168.1.233, 192.168.1.234, 192.168.1.235, 192.168.1.236, 192.168.1.237, 192.168.1.238, 192.168.1.239, 192.168.1.240, 192.168.1.241, 192.168.1.242, 192.168.1.243, 192.168.1.244, 192.168.1.245, 192.168.1.246, 192.168.1.247, 192.168.1.248, 192.168.1.249, 192.168.1.250, 192.168.1.251, 192.168.1.252, 192.168.1.253, 192.168.1.254, 192.168.1.255
Physical addresses (MAC):	08:00:27:00:00:00, 08:00:27:00:00:01, 08:00:27:00:00:02, 08:00:27:00:00:03, 08:00:27:00:00:04, 08:00:27:00:00:05, 08:00:27:00:00:06, 08:00:27:00:00:07, 08:00:27:00:00:08, 08:00:27:00:00:09, 08:00:27:00:00:0A, 08:00:27:00:00:0B, 08:00:27:00:00:0C, 08:00:27:00:00:0D, 08:00:27:00:00:0E, 08:00:27:00:00:0F, 08:00:27:00:00:10, 08:00:27:00:00:11, 08:00:27:00:00:12, 08:00:27:00:00:13, 08:00:27:00:00:14, 08:00:27:00:00:15, 08:00:27:00:00:16, 08:00:27:00:00:17, 08:00:27:00:00:18, 08:00:27:00:00:19, 08:00:27:00:00:1A, 08:00:27:00:00:1B, 08:00:27:00:00:1C, 08:00:27:00:00:1D, 08:00:27:00:00:1E, 08:00:27:00:00:1F, 08:00:27:00:00:20, 08:00:27:00:00:21, 08:00:27:00:00:22, 08:00:27:00:00:23, 08:00:27:00:00:24, 08:00:27:00:00:25, 08:00:27:00:00:26, 08:00:27:00:00:27, 08:00:27:00:00:28, 08:00:27:00:00:29, 08:00:27:00:00:2A, 08:00:27:00:00:2B, 08:00:27:00:00:2C, 08:00:27:00:00:2D, 08:00:27:00:00:2E, 08:00:27:00:00:2F, 08:00:27:00:00:30, 08:00:27:00:00:31, 08:00:27:00:00:32, 08:00:27:00:00:33, 08:00:27:00:00:34, 08:00:27:00:00:35, 08:00:27:00:00:36, 08:00:27:00:00:37, 08:00:27:00:00:38, 08:00:27:00:00:39, 08:00:27:00:00:3A, 08:00:27:00:00:3B, 08:00:27:00:00:3C, 08:00:27:00:00:3D, 08:00:27:00:00:3E, 08:00:27:00:00:3F, 08:00:27:00:00:40, 08:00:27:00:00:41, 08:00:27:00:00:42, 08:00:27:00:00:43, 08:00:27:00:00:44, 08:00:27:00:00:45, 08:00:27:00:00:46, 08:00:27:00:00:47, 08:00:27:00:00:48, 08:00:27:00:00:49, 08:00:27:00:00:4A, 08:00:27:00:00:4B, 08:00:27:00:00:4C, 08:00:27:00:00:4D, 08:00:27:00:00:4E, 08:00:27:00:00:4F, 08:00:27:00:00:50, 08:00:27:00:00:51, 08:00:27:00:00:52, 08:00:27:00:00:53, 08:00:27:00:00:54, 08:00:27:00:00:55, 08:00:27:00:00:56, 08:00:27:00:00:57, 08:00:27:00:00:58, 08:00:27:00:00:59, 08:00:27:00:00:5A, 08:00:27:00:00:5B, 08:00:27:00:00:5C, 08:00:27:00:00:5D, 08:00:27:00:00:5E, 08:00:27:00:00:5F, 08:00:27:00:00:60, 08:00:27:00:00:61, 08:00:27:00:00:62, 08:00:27:00:00:63, 08:00:27:00:00:64, 08:00:27:00:00:65, 08:00:27:00:00:66, 08:00:27:00:00:67, 08:00:27:00:00:68, 08:00:27:00:00:69, 08:00:27:00:00:6A, 08:00:27:00:00:6B, 08:00:27:00:00:6C, 08:00:27:00:00:6D, 08:00:27:00:00:6E, 08:00:27:00:00:6F, 08:00:27:00:00:70, 08:00:27:00:00:71, 08:00:27:00:00:72, 08:00:27:00:00:73, 08:00:27:00:00:74, 08:00:27:00:00:75, 08:00:27:00:00:76, 08:00:27:00:00:77, 08:00:27:00:00:78, 08:00:27:00:00:79, 08:00:27:00:00:7A, 08:00:27:00:00:7B, 08:00:27:00:00:7C, 08:00:27:00:00:7D, 08:00:27:00:00:7E, 08:00:27:00:00:7F, 08:00:27:00:00:80, 08:00:27:00:00:81, 08:00:27:00:00:82, 08:00:27:00:00:83, 08:00:27:00:00:84, 08:00:27:00:00:85, 08:00:27:00:00:86, 08:00:27:00:00:87, 08:00:27:00:00:88, 08:00:27:00:00:89, 08:00:27:00:00:8A, 08:00:27:00:00:8B, 08:00:27:00:00:8C, 08:00:27:00:00:8D, 08:00:27:00:00:8E, 08:00:27:00:00:8F, 08:00:27:00:00:90, 08:00:27:00:00:91, 08:00:27:00:00:92, 08:00:27:00:00:93, 08:00:27:00:00:94, 08:00:27:00:00:95, 08:00:27:00:00:96, 08:00:27:00:00:97, 08:00:27:00:00:98, 08:00:27:00:00:99, 08:00:27:00:00:9A, 08:00:27:00:00:9B, 08:00:27:00:00:9C, 08:00:27:00:00:9D, 08:00:27:00:00:9E, 08:00:27:00:00:9F, 08:00:27:00:00:A0, 08:00:27:00:00:A1, 08:00:27:00:00:A2, 08:00:27:00:00:A3, 08:00:27:00:00:A4, 08:00:27:00:00:A5, 08:00:27:00:00:A6, 08:00:27:00:00:A7, 08:00:27:00:00:A8, 08:00:27:00:00:A9, 08:00:27:00:00:AA, 08:00:27:00:00:AB, 08:00:27:00:00:AC, 08:00:27:00:00:AD, 08:00:27:00:00:AE, 08:00:27:00:00:AF, 08:00:27:00:00:B0, 08:00:27:00:00:B1, 08:00:27:00:00:B2, 08:00:27:00:00:B3, 08:00:27:00:00:B4, 08:00:27:00:00:B5, 08:00:27:00:00:B6, 08:00:27:00:00:B7, 08:00:27:00:00:B8, 08:00:27:00:00:B9, 08:00:27:00:00:BA, 08:00:27:00:00:BB, 08:00:27:00:00:BC, 08:00:27:00:00:BD, 08:00:27:00:00:BE, 08:00:27:00:00:BF, 08:00:27:00:00:C0, 08:00:27:00:00:C1, 08:00:27:00:00:C2, 08:00:27:00:00:C3, 08:00:27:00:00:C4, 08:00:27:00:00:C5, 08:00:27:00:00:C6, 08:00:27:00:00:C7, 08:00:27:00:00:C8, 08:00:27:00:00:C9, 08:00:27:00:00:CA, 08:00:27:00:00:CB, 08:00:27:00:00:CC, 08:00:27:00:00:CD, 08:00:27:00:00:CE, 08:00:27:00:00:CF, 08:00:27:00:00:D0, 08:00:27:00:00:D1, 08:00:27:00:00:D2, 08:00:27:00:00:D3, 08:00:27:00:00:D4, 08:00:27:00:00:D5, 08:00:27:00:00:D6, 08:00:27:00:00:D7, 08:00:27:00:00:D8, 08:00:27:00:00:D9, 08:00:27:00:00:DA, 08:00:27:00:00:DB, 08:00:27:00:00:DC, 08:00:27:00:00:DD, 08:00:27:00:00:DE, 08:00:27:00:00:DF, 08:00:27:00:00:E0, 08:00:27:00:00:E1, 08:00:27:00:00:E2, 08:00:27:00:00:E3, 08:00:27:00:00:E4, 08:00:27:00:00:E5, 08:00:27:00:00:E6, 08:00:27:00:00:E7, 08:00:27:00:00:E8, 08:00:27:00:00:E9, 08:00:27:00:00:EA, 08:00:27:00:00:EB, 08:00:27:00:00:EC, 08:00:27:00:00:ED, 08:00:27:00:00:EE, 08:00:27:00:00:EF, 08:00:27:00:00:F0, 08:00:27:00:00:F1, 08:00:27:00:00:F2, 08:00:27:00:00:F3, 08:00:27:00:00:F4, 08:00:27:00:00:F5, 08:00:27:00:00:F6, 08:00:27:00:00:F7, 08:00:27:00:00:F8, 08:00:27:00:00:F9, 08:00:27:00:00:FA, 08:00:27:00:00:FB, 08:00:27:00:00:FC, 08:00:27:00:00:FD, 08:00:27:00:00:FE, 08:00:27:00:00:FF
Domain:	
Active Directory path:	
Group:	All Change
Operating system:	Windows 10 Pro 64 (Version: 1909) (Build: 18363.1082)
Exchange Server:	Not installed
Virtual machine:	No
Is a non-persistent computer:	No
Licenses:	ENDPOINT PROTECTION PLUS ×
Agent version:	1.16.10.0000
Last bootup date:	10/6/2020 2:58:57 PM
Installation date:	10/6/2020 3:41:13 PM
Last proxy used:	No proxy
Last connection:	10/6/2020 6:12:58 PM
Last settings check:	10/6/2020 6:12:58 PM
Last logged-in user:	Test

Settings tab

On the *Users* page, you can create console users and assign them full control or read-only access. The *Settings/Security* page lets you define separate security policies for computers and Android mobile devices. Under *My Alerts* you can set up email notifications for various items. These include malware and phishing detections, unlicensed/unmanaged/unprotected computers, and installation errors. The *Network settings* page lets you manage Panda proxy and cache servers, both of which provide updates to other computers on the LAN. The former is for use in isolated LANs, and the latter for e.g. branch offices with low-bandwidth Internet connections. In the *Proxy* section, you will also find *Enable real-time communication*. This allows for almost instantaneous communications between clients and management console. The description in the console notes that it can generate high volumes of network traffic.

Tasks tab

The *Tasks* tab can be used to set up scheduled scans.

Settings menu

The settings menu is accessed from the cogwheel icon in the top right-hand corner of the console. It includes help and support links, licence and product information, and also lets you change the console language in real time.

Windows endpoint protection software

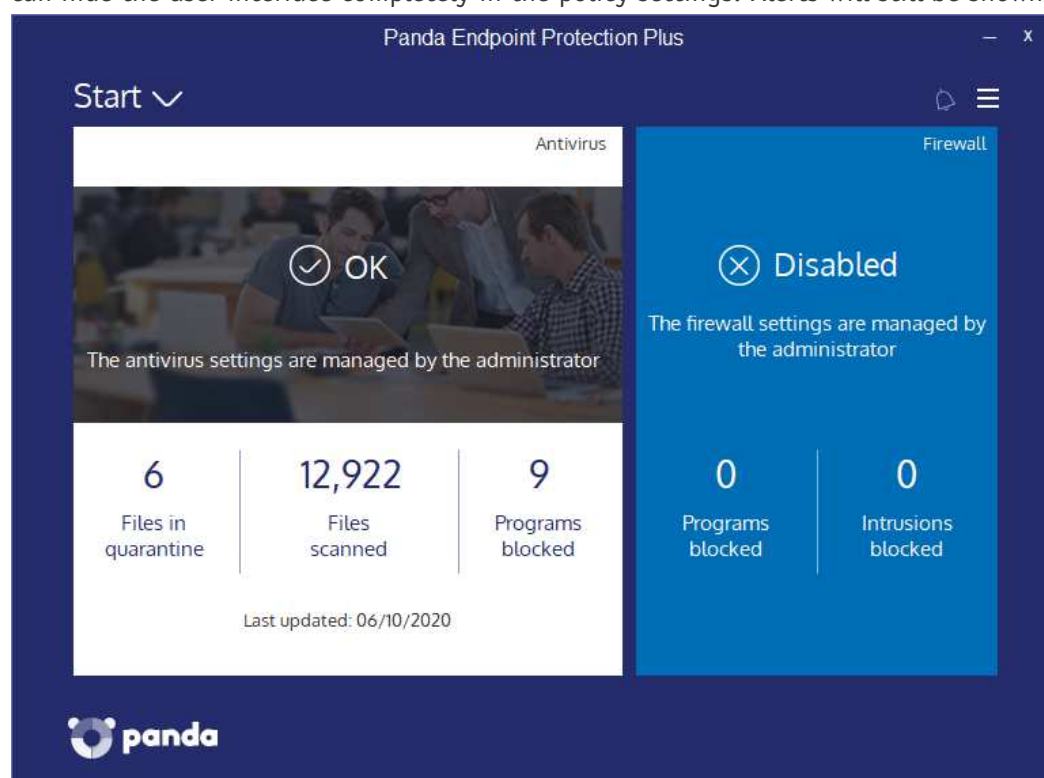
Deployment

Deployment options can be found by clicking *Add Computers* on the *Computers* page. You can create an installer in .msi format, which can be preconfigured. You can specify a Panda or Active Directory computer group, and select settings. The installer can then be downloaded or sent to users by email directly from the console. Manual installation is extremely quick and simple, and would pose no problems for non-expert users. You can password-protect the software, meaning that even users with Windows Administrator Accounts cannot uninstall it.

You could also deploy the software via a systems management product, or Active Directory script. The *Discovery and Remote Installation* option additionally allows you to install the software using remote push. The discovery process locates all the computers on the network, so you can be sure that none have been left unprotected.

Functionality check

The user interface on protected endpoints consists of a System Tray icon and a program window. Users can see the protection status and detection logs, run updates, and run quick, full and custom scans. They can also scan a file, folder or drive using Windows Explorer's right-click menu. If you prefer, you can hide the user interface completely in the policy settings. Alerts will still be shown, however.



When we connected a flash drive containing malware samples to our test PC, and opened the drive in Windows Explorer, Panda did not initially take any action. However, as soon as we tried to copy the malicious files to the Windows Desktop, they were detected and deleted. A pop-up alert was shown, which closed after a few seconds. No user action was required or possible.

SOPHOS

Central

Admin

Sophos Central Dashboard

See a snapshot of your security protection

Help

Sign Up

Log Out

Sophos UK

Super Admin

Overview

Dashboard

Alerts

Threat Analysis Center

Logs & Reports

People

Devices

Global Settings

Protect Devices

MY PRODUCTS

Endpoint Protection

Server Protection

Firewall Management

MORE PRODUCTS

Free Trials

Alerts Summary

164

Total Alerts

97

High Alerts

67

Medium Alerts

0

Low Alerts

Most Recent Alerts

View All Alerts

1	Oct 13, 2020 3:01 AM	Manual malware cleanup required: 'Ma/Generic-S' at 'C:\Users\user\AppData\Local\Temp\...	2020-10-13 03:01:00	2020-10-13 03:01:00	Show full details
1	Oct 13, 2020 3:01 AM	Manual malware cleanup required: 'Ma/Generic-S' at 'C:\Users\user\AppData\Local\Temp\...	2020-10-13 03:01:00	2020-10-13 03:01:00	Show full details
1	Oct 9, 2020 12:18 PM	Manual PUA cleanup required: 'Generic.ML.PUA' at 'C:\Users\user\AppData\Local\Temp\...	2020-10-09 12:18:00	2020-10-09 12:18:00	Show full details
1	Oct 9, 2020 12:18 PM	Manual PUA cleanup required: 'Generic.ML.PUA' at 'C:\Users\user\AppData\Local\Temp\...	2020-10-09 12:18:00	2020-10-09 12:18:00	Show full details
1	Sep 22, 2020 9:41 AM	Manual PUA cleanup required: 'Generic.ML.PUA' at 'C:\Users\user\AppData\Local\Temp\...	2020-09-22 09:41:00	2020-09-22 09:41:00	Show full details

Devices and users: summary

See Report

Endpoint Computer Activity Status

457

2 Active

1 Inactive 2+ Weeks

450 Inactive 2+ Months

4 Not Protected

Web control

See Reports

235

Web Threats Blocked

0

Policy Warnings Issued

26

Policy Violations Blocked

0

Policy Warnings Proceeded

Sophos Intercept X Advanced provides endpoint protection software for Windows and macOS workstations, plus Windows servers. This is managed using a cloud-based console. As well as malware protection, the product includes investigative functions for analysing and remediating attacks. It can cope with networks that have hundreds of thousands of seats. We feel it would also be suitable for smaller businesses with tens of seats.

- Investigative functions
- Modern, easy-to-navigate console design
- Comprehensive search feature
- Detailed alert information
- Early-access program lets you try out new features in advance

Management Console

The console is navigated using a single menu column on the left-hand side. Some of the items, such as *Threat Analysis Center* and *Endpoint Protection* open in a sort of sub-console with their own menu panel. The console layout and graphic design remain the same, and you can easily get back to the main console by clicking *Back to Overview* at the top of the applicable menu column. Some pages, such as *People*, can be accessed from either the main or the sub-console. The UI language can be changed in real time from the user menu in the top right-hand corner. The same menu also lets you join Sophos' early-access program, so you can try upcoming features before general release.

Dashboard page

The *Sophos Central Dashboard* (shown in the screenshot above) is the default landing page when you log on to the console. It shows an overview of threats and device/user status, with colour-coded graphics to make things stand out. You can see the number of total alerts, and this is also broken down into high, medium and low-level alerts. The most recent individual alerts are listed, and threat name and path, plus device and user, are shown. The *Dashboard* panels are linked to details pages, so clicking on the *High Alerts* panel displays a list of these on the *Alerts* page. The *Global Security News* panel at the bottom is linked to Sophos' *Naked Security* blog, and shows security-related news items.

Alerts page

164 Total Alerts

97 High Alerts

67 Medium Alerts

0 Low Alerts

Mark As Acknowledged

< Back Manual PUA cleanup required: 'Generic ML PUA' (59)

	Description	Occurred	User	Device	
<input type="checkbox"/>	Manual PUA cleanup required: 'Generic ML PUA' at...	Oct 9, 2020 12:18 PM	[Link]	[Link]	^
<div> <div> <p>Description</p> <p>Manual PUA cleanup required: 'Generic ML PUA' at 'C:\Users\user\AppData\Local\Temp\145414d6500.tmp'</p> <p>More information</p> <p>We tried to clean up a potentially unwanted application (PUA) but failed.</p> <p>What you need to do</p> <p>Please see knowledge base article 134586 for the steps needed to investigate the threat and clean it up.</p> </div> <div> <p>Endpoint Type: Computer</p> <p>OS: Windows</p> <p>User: [Link]</p> <p>Device: [Link]</p> </div> <div> <p>Actions</p> <p>Mark As Resolved</p> <p>Email Alert</p> <p>Change frequency for "Manual PUA cleanup required" email alerts. This will be added to your "Exceptions" list.</p> <p>None</p> </div> </div>					
<input type="checkbox"/>	Manual PUA cleanup required: 'Generic ML PUA' at...	Oct 9, 2020 12:18 PM	[Link]	[Link]	▼
<input type="checkbox"/>	Manual PUA cleanup required: 'Generic ML PUA' at...	Sep 21, 2020 9:41 AM	[Link]	[Link]	▼

The *Alerts* page shows you numbers of threat detections, both as a total and by severity category. You can sort by *Description*, *Count* and *Actions*. Clicking on an entry opens up a details panel, with additional information and links to take action. Possible actions (depending on context) include *Mark As Resolved*, *Clean Up PUA*, and *Authorize PUA*.

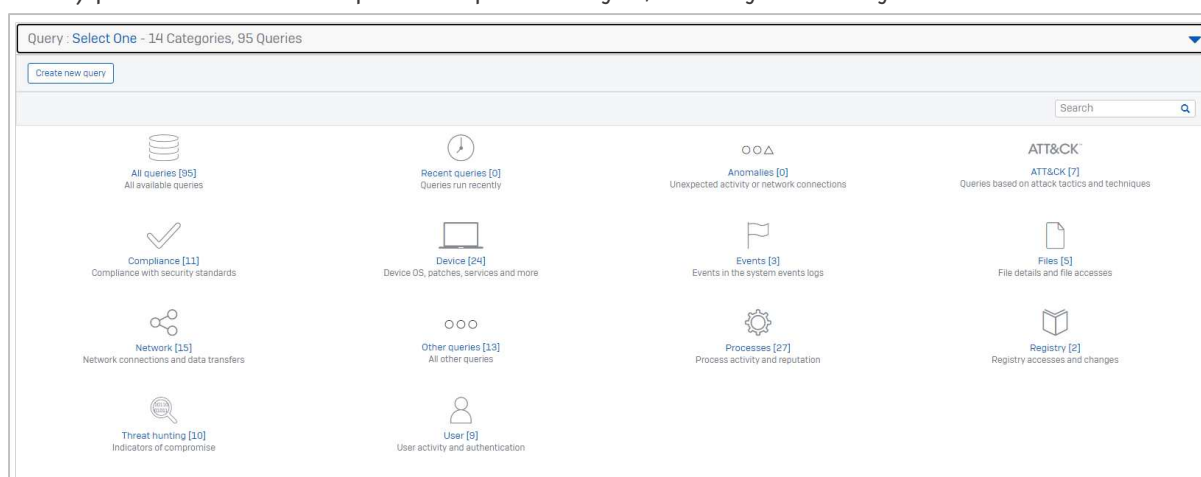
Logs and Reports page

This shows a wide variety of default reports that can be run. A notable item here is *Policy Violators*. This shows those users who have tried to access blocked websites most often.

Threat Analysis Center section

This is a sub-console, with the pages *Dashboard*, *Threat Cases*, *Live Discover*, *Threat Searches* and *Threat Indicators*. The *Dashboard* provides a summary of content from the other pages.

The *Live Discover* page lets you run queries on selected devices. In the *Device Selector* panel, you can choose from *Available devices* or *Selected devices*. With the latter, various different filtering categories are provided, so you can refine your device list precisely. These are online status, name, type (server/workstation), OS, last user, group, IP address, and *health status*. The *Query* panel (screenshot below) provides a number of pre-built queries for you, or lets you create your own.



Threat Searches enables you to look for file names, file hashes, IP addresses, domains and command-prompt commands that may have been used in attacks. The feature is intended to find applications and network destinations with bad reputations, and malicious use of administrative tools.

Endpoint Protection section

The *Endpoint Protection* sub-console has menu entries for *Dashboard*, *Logs & Reports*, *People*, *Computers*, *Policies*, *Settings*, and *Protect Devices*. The *Dashboard* page is similar in design to that of its counterpart in the main console. It shows many of the same panels, including *Most recent threat cases*, *Devices and users: summary*, *Web control* and *Global Security News*.

The *People* page lets you manage users and groups. These include Windows device users (which are added automatically) and also console users. In the details page for each user, you can see devices that the user has signed into, and run scans and updates on these.

On the *Policies* page, you can edit the configuration to be applied to endpoints. There are separate policies for *Threat Protection*, *Peripheral Control*, *Application Control*, *Data Loss Prevention*, *Web Control*, *Update Management* and *Windows Firewall*. You can apply policies to computers, users, or groups of either.

The *Settings* page lets you configure options to be applied to the whole network. Examples include *AD Sync*, *Role Management* (standard and custom permissions for console users), *Tamper Protection*, *Admin Isolated Devices*, *Live Response* (remote management feature) and *Data Loss Prevention Rules*. You can download installers for the endpoint protection client from the *Protect Devices* page.

Under *Computers* (screenshot below), you can see a list of your devices with name, IP address, OS version, installed Sophos products, last user, and date/time of last use. Mousing over the little button to the right of the IPv4 address will display IPv6 addresses. Clicking *Manage Endpoint Software* shows you which computers are eligible for which Sophos software, and which of these actually have it installed. You can remove devices from the console with the *Delete* button.

	Name	IP	OS	Endpoint	Intercept X	Last user
<input type="checkbox"/>	Test	192.168.1.100	Windows 10 Pro	✓	✓	admin
<input type="checkbox"/>	192.168.1.101	192.168.1.101	Windows 10 Pro	✓	✓	User
<input type="checkbox"/>	192.168.1.102	192.168.1.102	Windows 10 Pro	✓	✓	User
<input type="checkbox"/>	192.168.1.103	192.168.1.103	Windows 10 Pro	✓	✓	User
<input type="checkbox"/>	192.168.1.104	192.168.1.104	Windows 10 Pro	✓	✓	User
<input type="checkbox"/>	192.168.1.105	192.168.1.105	Windows 10 Pro	✓	✓	User

Windows Endpoint Protection Client

Deployment

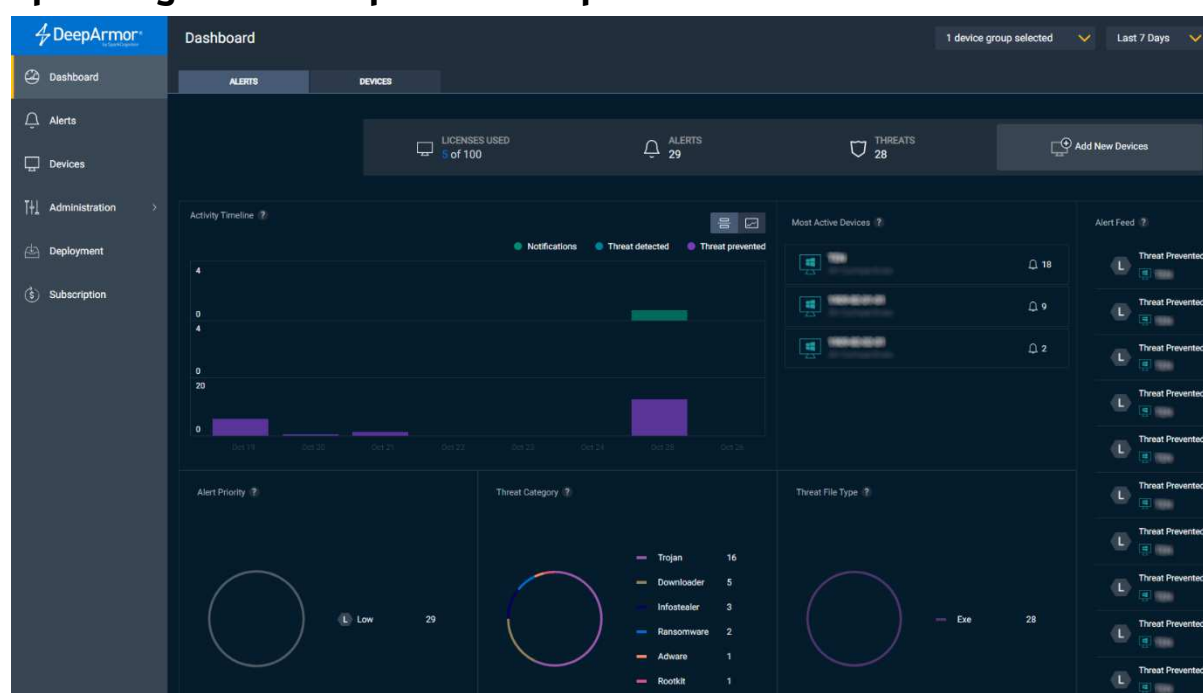
You can download installer files in .exe format from the *Protect Devices* page. These can be run manually, via a systems management product, or using an AD script. You can also email an installer to users directly from the download page. The setup wizard is very quick and easy, so even non-expert users would have no difficulty with it. You can prevent users with Windows Administrator Accounts from uninstalling the software or changing settings, using the *Enable Tamper Protection* setting under *Global Settings*.

Functionality check

The user interface on protected endpoints consists of a System Tray icon and a program window. Users can see the protection status and detection logs, and run default scans. They can also scan a file, folder or drive using Windows Explorer's right-click menu.

When we connected a flash drive containing malware samples to our test PC, and opened the drive in Windows Explorer, Sophos immediately detected and quarantined the malicious files. A pop-up alert was shown, which closed after a few seconds. No user action was required or possible. You can disable detection alerts via policy if you want.

SparkCognition DeepArmor Endpoint Protection Platform



About the product

SparkCognition DeepArmor provides endpoint protection software for Windows and macOS workstations, plus Windows servers. This is managed from either a cloud-based or premises-based console. As well as malware protection, the product includes investigative functions for analysing and remediating attacks, and can scale to manage networks with tens of thousands of endpoints.

Advantages

- Easy-to-use investigative features
- Interactive, clickable charts
- Easily navigated console
- Alert details can be easily browsed
- VirusTotal integration

Management Console

The console is navigated from a single menu panel on the left-hand side. The main entries are *Dashboard*, *Alerts*, *Devices*, *Administration*, *Deployment* and *Subscription*.

[Dashboard\Alerts page](#)

This is the page you will see when you first log in to the console (shown in the screenshot above). It provides a graphical summary of recent threats. These are displayed as several different panels, illustrated with coloured bar and doughnut charts. They show additional details when you mouse over them. The bar charts are clickable, so you if you click on the *Threats Prevented* column for a particular day in *Activity Timeline*, you will be taken to a page listing the threats blocked that day. You can see *Activity Timeline* (past 7 days), *Most Active Devices* (devices with most threats), *Alert Priority*, *Threat Category* (e.g. Trojan, Ransomware) and *Threat File Type* (e.g. .exe). The page is completed by a strip of clickable buttons along the top, showing licences used, total alerts, and total threats.

[Dashboard\Devices page](#)

Here you can get an overview of the status of your devices, also illustrated with dynamic coloured charts. You can see numbers of *Active*, *Inactive* and *Recycled* devices, devices by platform (OS), at-risk devices, and devices by endpoint protection agent version.

[Alerts page](#)

The *Alerts* page shows important notifications, along with details. These include *Alert Priority*, *Alert Type* (e.g. *Threat Prevented*, *New Device Registered*), *Device Name | Group Name*, *Username*, plus date and time. Clicking on an entry slides out a details panel on the right-hand side. This is shown below (content rearranged to fit on page). The up/down arrows in the details panel let you browse to the next or previous alert details pane with a single click.

The screenshot displays the Management Console interface. On the left, a 'Threat Prevented - Alert Summary' panel shows an alert description: 'Malicious Threat Prevented via Real-Time File Monitoring using DeepArmor's File Reputation.' Below this is a 'View Alert Details' button. The 'Current Alert Action' is 'Quarantined on October 24, 2020, GMT 09:21:41 PM', with a 'Restore' button. The 'Threat File Type' is 'WIN32 EXE' and the 'File Name' is 'winlogin.exe'. On the right, a detailed 'Alert Details' panel is shown, containing the following information:

Device Name Group Name	Username
TEN AV Comparatives	TEN\admin
Priority	
Low L	
Threat Activity Type	Analysis Type
Real-Time File Monitoring	File Reputation
SHA1	
415303F86603B61B49509F9764ECC9C5D77AF853	Copy
Confidence Score	Priority
100%	Low L
Threat Category	Original Alert Action
Trojan	QUARANTINED
Original Alert Timestamp	Current Alert Action
October 24, 2020, GMT 09:19:18 PM	QUARANTINED

For a malware detection, information provided in the details pane includes the file name, detection mechanism, SHA1 hash, threat category (e.g. Trojan), "confidence score" (probability that the file is malicious), and action taken. You can restore any erroneously quarantined files by clicking *Restore*. The button to the left of *Copy* (file hash line) lets you see the file's analysis page on VirusTotal.

If you click on *View Alert Details*, a complete page opens, with more details and options:

The screenshot shows the 'View Alert Details' page for a malware alert. At the top, there are tabs for 'Behavioral Analysis', 'Download', and 'Take Action'. Below these, a summary bar displays the SHA1 hash, file name, threat file type, confidence score, and alert timestamp. The main content area is divided into two sections: 'EVENTS DETAILS' and 'OCCURRENCES'. The 'EVENTS DETAILS' section shows the device name (TEN), device group, file path, file location, file created/modified dates, and the running user application(s) (ApplicationFrameHost, AppVShNotify, chrome). The 'OCCURRENCES' section shows the DeepArmor Cloud Service Connection status (CONNECTED), network connection status (CONNECTED), and the logged-in user name.

Here you can see the applications that were running at the time of the alert, plus the status of the network connection and DeepArmor console connection. The *Behavioural Analysis* button runs the suspected malware in a sandbox and investigates its actions. You can download the file to the local PC to analyse it yourself, or take action. The *Take Action* button provides the options *Remote Remediate*, *Remote Restore*, *External Remediate*, and *Remote Activity*.

Devices page

The screenshot shows the 'Devices' page. At the top, there is a search bar and several filter dropdowns: 'Device group' (All (5)), 'Device status' (Active, Inactive), 'Device risk' (All), 'Device platform' (All), and 'Agent Version' (All). Below the filters, there is a 'Select All' button. The main content area displays a list of devices as tiles. Each tile shows the device icon, name, user, number of alerts, and connection status. The first three tiles are active, and the fourth is inactive.

On the *Devices* page, you can see individual computers on your network. You can display these as tiles, as shown above, or as a simple list. For each device, you can see the OS type, current user, number of alerts, and connection status. By selecting a device or devices, you can run scans, change group membership, or remove from the console. It is possible to filter the devices displayed by using drop-down lists at the top of the page. You can filter by device group, device status, device risk, device platform or agent version.

Administration menu

This includes the pages *Users*, *Security Policies*, *Device Groups*, *Global Lists*, *Audit Logs* and *Reporting*. *Users* lets you add, edit and remove console administrators, who can be assigned varying levels of access (*Admin*, *Manager* or *Auditor*). Under *Security Policies* you can assign preconfigured settings to device groups. There are 4 default policies: *Detection Only*; *Detection and Protection*; *Essential Protection*; *Maximum Protection*. For each policy, there are separate settings for detection and protection. Thus, you could have e.g. a high level of protection, but a low level of detection, keeping systems safe without numerous alerts. For each category there are the standard levels *Disabled*, *Cautious*, *Moderate* and *Aggressive*. Each policy also has a detailed configuration section, where you can set items like *real-time file monitoring*, *application control* and *USB control*.

You can manage the groups to which policies are applied from the *Device Groups* page. You can create whitelists of files and certificates, and file blacklists, under *Global Lists*. A list of admin logins and logouts can be found under *Audit Logs*. The *Reporting* page lets you create reports for specific groups or all devices. You can choose the time period covered by the report, and who will receive it.

Deployment page

Here you can find installers for Window, macOS, and various different Linux distributions.

Subscription page

This shows you the total number of device licences available and used, and the validity period.

Windows endpoint protection software

Deployment

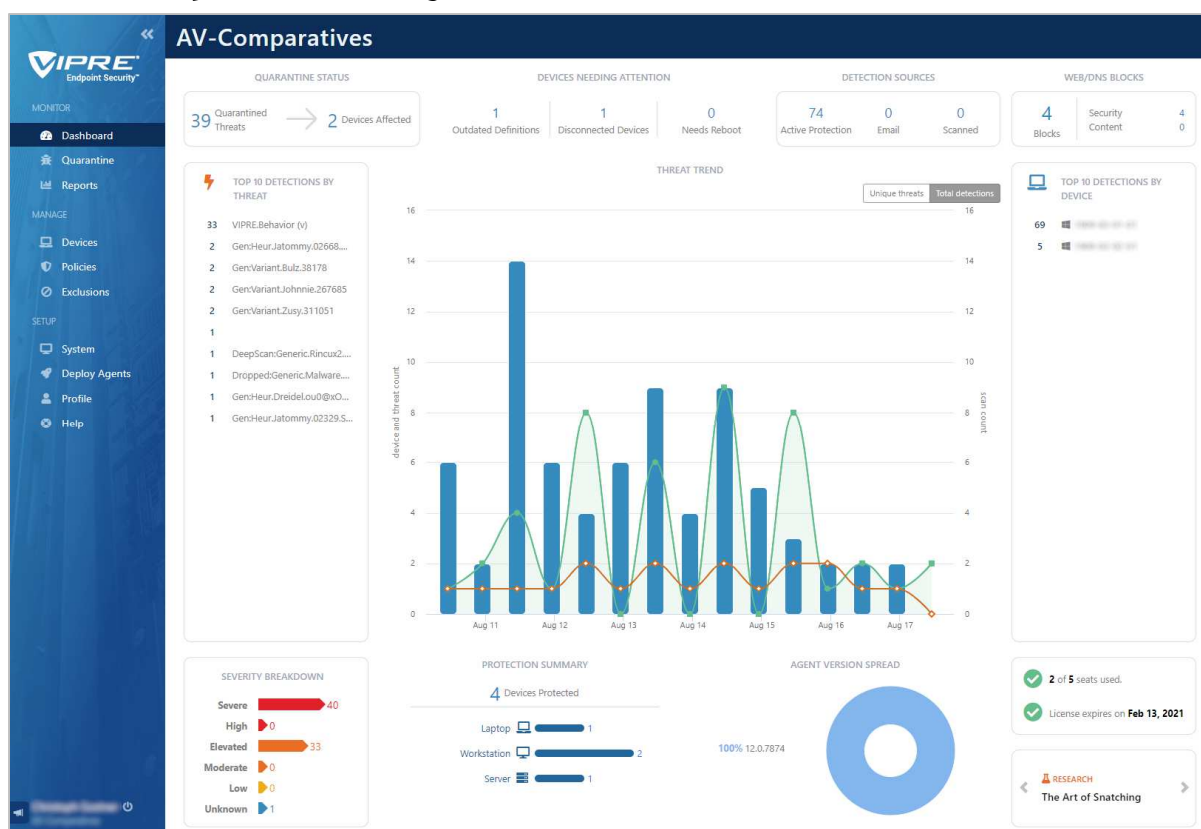
Installer files in .exe and .msi format can be downloaded from the *Deployment* page of the console. You have to specify a group to add the device to when downloading. The installer file can be run manually, via a systems management product, or using an AD script. You can also email users with installation links so that they can install the endpoint agent themselves. The setup wizard is very quick and easy, so even non-expert users would have no difficulty with it. You can prevent users with Windows Administrator Accounts from uninstalling the software, using the Agent Administrator Password setting in the applicable policy. For manual installations, you have to copy a web-service URL and registration key from the console, to prevent unauthorised use. Once the endpoint agent has been installed and the GUI is opened, a brief introductory wizard optionally explains the key points of the program window.

Functionality check

The user interface on protected endpoints consists of a System Tray icon and a program window. Users can see the protection status and detection logs, and run updates. No other functionality is provided. You can hide the interface completely via policy if you so choose.

When we connected a flash drive containing malware samples to our test PC, and opened the drive in Windows Explorer, DeepArmor did not initially take any action. However, when we tried to copy the malicious files to the Windows Desktop, they were detected and quarantined. A pop-up alert was shown, which closed after a few seconds. No user action was required or possible. Alerts can be deactivated in the policy if you prefer.

VIPRE Endpoint Security Cloud



About the product

VIPRE Endpoint Security provides endpoint protection software for Windows and macOS workstations, plus Windows servers. This is managed using a cloud-based console. The product can manage networks with thousands of devices. We feel it would also be very suitable for very small businesses with just a few seats.

Advantages

- Well-suited to micro-businesses and upwards
- Minimal technical knowledge required
- Console is very easily navigated from a single menu panel
- Very clickable, interconnected interface
- *Timeline* feature provides detailed threat-history information

Management Console

Dashboard page

This is what you will see when you first log in to the console (screenshot above). It provides an overview of the current security status, using various different panels. It is designed to be very clickable. For example, if you click on the number of *Outdated Definitions*, you will be taken to a page that shows you the specific devices in question. The main *Threat Trend* panel displays a graph of threats encountered over the past week. This can be shown as either total detections (including multiple occurrences of any individual threat), or unique threats. Separate panels illustrate the top ten detections by threat and by device, respectively.

Other *Dashboard* panels are: *Quarantine Status*, *Devices Needing Attention*, *Detection Sources*, *Web/DNS Blocks*, *Severity Breakdown*, *Protection Summary*, *Agent Version Spread*, *Research* (blog), and licensing information. Every item is clickable, and links to the respective details page.

Quarantine page

Here you can see a list of all threats that have been quarantined on any device. It displays the date and time of detection, threat name, platform, threat category, severity, source (detection module), and number of devices affected. The list can be filtered by severity, malware category, or source. Clicking on the threat name opens the details page for that threat, where you can delete or restore the quarantined file.

Reports page

This shows tiles for a variety of different preconfigured reports: *Threat Detection*, *Threat Summary*, *Device Registration*, *Scan*, *Web Activity Summary*, and *License Summary*. *Threat Summary* uses a timeline, bar and pie charts to visualise threats found in the last week.

Devices page

ALL DEVICES 4

Search Devices

Q

Outdated Agents 0

Outdated Definitions 1

Disconnected Devices 1

Needs Reboot 0

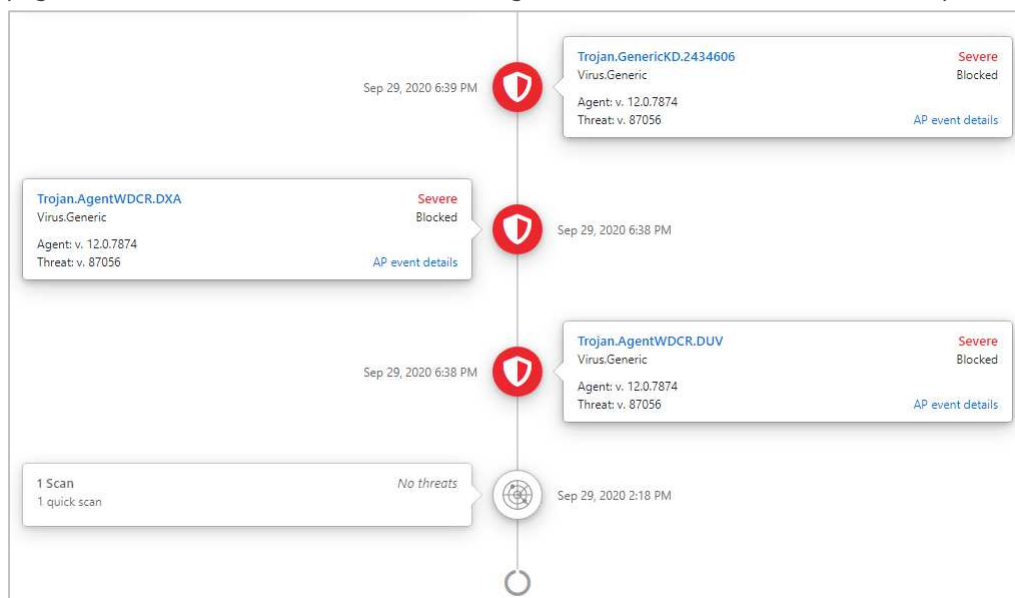
<div><input type="checkbox"/> HOSTNAME^</div>	STATUS	POLICY	TYPE	OS	LAST SEEN	LAST INFECTED	AGENT
<div><input type="checkbox"/> 1909-00-03-02</div>	Protected	Perf	<div> Laptop</div>	<div> Windows 10</div>	2 months ago	2 months ago	12.0.7874
<div><input type="checkbox"/> 1909-83-01-01</div>	Protected	Default Enterprise	<div> Workstation</div>	<div> Windows 10</div>	17 minutes ago	2 days ago	12.0.7874
<div><input type="checkbox"/> 1909-83-02-01</div>	Protected	Default Enterprise	<div> Workstation</div>	<div> Windows 10</div>	21 hours ago	4 days ago	12.0.7874
<div><input type="checkbox"/> TEN</div>	Shutdown	Default Enterprise	<div> Workstation</div>	<div> Windows 10</div>	a day ago	2 days ago	12.0.7874

The *Devices* page, shown above, lists network computers, and displays useful information. Items include status, policy, OS, and agent version. The information columns can be customised. You can add additional items such as the user, last scan, IP address or last update, as well as/instead of the standard ones. You can also filter the list of devices shown by platform, OS version, status, policy, type (workstation/laptop/server), or endpoint agent version number. Alternatively, a search box lets you find devices by name. This makes it easy to find specific devices or device categories.

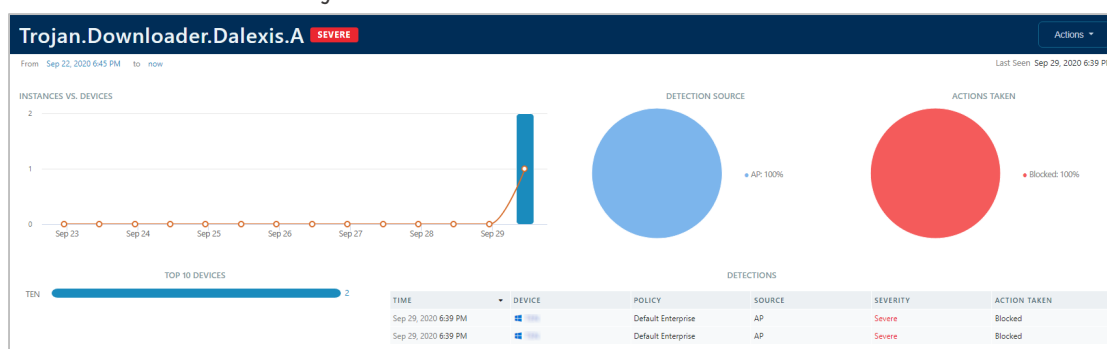
Having found the computers you were looking for, you can then carry out tasks on them from the *Actions* menu. Available actions are: *Assign Windows Policy*, *Full Scan*, *Quick Scan*, *Update Definitions*, *Schedule Agent Update*, *Reboot Devices*, *Stop Agent*, *Uninstall Agent*, and *Delete Device*. *Uninstall Agent* removes the endpoint software, but keeps associated data. This might be useful if you want to reinstall or change the agent version. *Delete Device* removes associated data and deactivates the licence.

Each individual device has its own details page, with various different tabs. These are: *Summary* (status etc.); *Scans* (what was scanned, what was found, what was done); *Quarantine*; *Threats* (source, severity, and action taken); *Web Activity* (pages visited by user); *Timeline* (scans and detections).

The *Timeline* feature is shown below. It lists important system events such as scans, blocked web pages and malware detections in chronological order. There is an information panel for each one.



Clicking on the name of a threat opens up the respective *Threat Information* page, shown below. This displays incidences of the threat in the last week, the protection component involved, action taken, and the devices affected by the threat.



Policies page

Here you can configure the protection settings for your devices. There are separate pages/policies for Windows and macOS devices, and separate default policies for Windows clients and Windows servers. For each policy you can configure: *Agent* (user interface and system integration); *Scanning* (what to scan, schedule, USB devices); *Active Protection* (sensitivity of real-time protection); *Web/DNS Protection*; *Email Protection*; *Threat Handling*, *Firewall*, *IDS* (Intrusion Detection System). On the *Agent* page is the option to remove any incompatible software, i.e. existing endpoint protection software from another vendor, when the agent is installed. A very wide range of different products and versions is included. This is listed, so you can see if a particular product/version can be removed automatically.

Exclusions page

Here you can configure scanning exclusions. These are linked to specific policies.

System page

On this page you can configure notifications, console users, system-wide settings, and the site name (sub-domain of "myvipre.com"). We note that VIPRE has a separate EU datacentre, to comply with EU data protection regulations. *Notifications* lets you set up alerts for detected threats (amongst other things). You can specify the source (real-time protection, scan or email), and the minimum threat severity needed to trigger the notification. You then add email addresses to be notified, and you can even customise the format of the email subject. The resultant email will contain links going directly to the relevant pages of the management console.

Deploy Agents page

This page lets you manage, download and email installers for the endpoint protection agent. The console lets you decide whether to auto-update all clients with the latest build of the software, or try it out on specific devices first. You can create a custom installer linked to a specific policy if you want.

Profile page

Here you can enter the contact details of the current console user, and activate 2-factor authentication.

Windows Endpoint Protection Client

Deployment

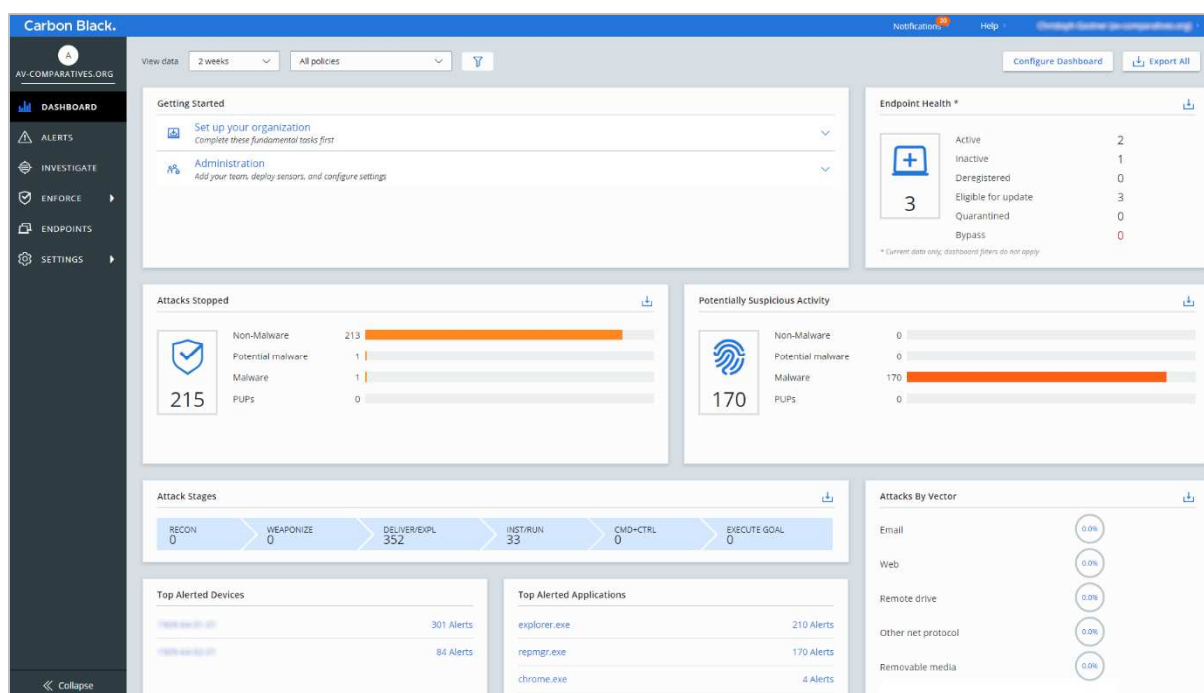
Installer files in .msi format for Windows can be downloaded from the *Deploy Agents* page. The installer file can be run manually, via a systems management product, or using an AD script. Remote push installation is also possible, by installing a utility on a relay computer in the LAN. You can also email an installer to users directly from the *Deploy Agents* page. The setup wizard is very quick and easy, so even non-expert users would have no difficulty with it. You can prevent users with Windows Administrator Accounts from uninstalling the software, using the Enable Uninstall Protection setting in the applicable policy. You will be able to see in the console who has installed the software on a particular device.

Functionality check

The user interface on protected endpoints consists of a System Tray icon and a program window. Users can see the protection status and detection logs, run updates, and run quick, full and custom scans. They can also scan a file, folder or drive using Windows Explorer's right-click menu. By changing the policy, you could hide the user interface completely, or give specified users more control, such as managing scan schedules or quarantine.

When we connected a flash drive containing malware samples to our test PC, and opened the drive in Windows Explorer, VIPRE immediately detected and quarantined the malicious files. A pop-up alert was shown, which persisted until manually closed. No user action was required or possible. However, clicking *Show Details* opened a window with further information about the threat. You can disable detection alerts via policy if you want.

VMware Carbon Black Cloud



About the product

Carbon Black Cloud provides endpoint protection software for Windows and macOS workstations, plus Windows servers. As the name implies, this is managed from a cloud-based console. As well as malware protection, the product includes investigative functions for analysing and remediating attacks. The product can manage networks with hundreds of thousands of devices. We feel it would also be suitable for smaller businesses with tens of seats.

Advantages

- Attack investigation features
- Remote-remediation feature
- Integration with VMware vSphere
- Simple, uncluttered user interface
- Console pages can be customised to your requirements

Management console

All the main functionality of the console is found in a single menu column on the left-hand side of the page. This makes it very easy to navigate.

Dashboard page

The *Dashboard* page shows you an overview of threat-related items, displayed in panels. These are *Attacks stopped*, *Potentially Suspicious Activity*, *Attack Stages*, *Attacks by Vector*, *Top Alerted Devices*, *Top Alerted Applications* and *Threat Reports*. There is also an *Endpoint Health* panel, which lets you see if you need to take action on any devices. The *Getting Started* panel shows links for common tasks, such as adding console administrators. You can customise the dashboard by moving panels around and removing any you don't need.

Alerts page

STATUS	FIRST SEEN	REASON	S	T	DEVICE	ACTIONS
<input type="checkbox"/>	2:55:33 pm Oct 15, 2020	A known virus (Trojan: Emotet) was detected.	3			[Icons]
<input type="checkbox"/>	2:06:14 pm Oct 15, 2020	A known virus (Trojan: Bulz) was detected.	3			[Icons]
<input type="checkbox"/>	12:55:53 pm Oct 15, 2020	A known virus (Trojan: Nymaim) was detected.	3			[Icons]
<input type="checkbox"/>	12:55:53 pm Oct 15, 2020	A known virus (Dropper: Delphi) was detected.	3			[Icons]
<input type="checkbox"/>	12:55:53 pm Oct 15, 2020	A known virus (Trojan: Dalexix) was detected.	3			[Icons]
<input type="checkbox"/>	12:55:53 pm Oct 15, 2020	A known virus (Trojan: ATRAPS) was detected.	3			[Icons]
<input type="checkbox"/>	12:55:53 pm Oct 15, 2020	A known virus (Trojan: Behavior) was detected.	3			[Icons]

The *Alerts* page shows you a list of threats encountered on all devices, in chronological order. You can filter the list using a wide variety of criteria, using the menu panel on the left-hand side of the page. You can filter by device, process, file reputation, sensor action and more. The main panel shows the date and time of the alert, reason (e.g. malware detection), severity, plus device and user. Buttons on the right-hand end of each entry let you open the respective *Alert Triage* or *Investigate* pages, or take action. Available actions include dismissing the alert, deleting or whitelisting (*Enable bypass*) the file that caused the alert, or opening the applicable VirusTotal page for the file.

Alert Triage page

Here you can see the system processes that were involved in the encounter with the malware. This is to assist you in understanding the nature of the threat and how to deal with it.

Investigate page

Event Timeline Device			
Last active user: [redacted]	Last IP: [redacted]	OS version: Windows 10 x64	Take Action
Policy: Standard	Last location: [redacted]	Sensor version: 3.6.0.1791	Target value: [redacted]
Last contact: 5:20:34 pm Oct 15, 2020	Device status: Registered on 12:31:52 pm Oct 15, 2020		
TIME	APPLICATION	EVENT	DEVICE
5:17:08 pm Oct 15, 2020	svchost.exe (Run as NT AUTHORITY\NETWORK SERVICE)	The application C:\Windows\system32\svchost.exe -k NetworkService -p -s CryptSvc established a TCP/80 connection to [redacted]:80 (ctdl.windowsupdate.com, located in United States) from [redacted]. The device was off the corporate network using the public address [redacted] ([redacted], home, located in [redacted], [redacted]). The operation was successful.	[redacted] (Standard)
5:03:13 pm Oct 15, 2020	chrome.exe (Run as [redacted])	The application C:\program files (x86)\google\chrome\application\chrome.exe invoked the application C:\program files (x86)\google\chrome\application\chrome.exe.	[redacted] (Standard)

On the *Investigate* page, you can see a chronological list of events for any individual device. You can filter the events by the country the device connected to, application involved, or malware alert. This allows you to monitor network connections and program executions, and build up a detailed picture of security-related events.

Enforce\Policies page

Here you can configure the settings to be applied to your devices. There are settings for malware detection, on-access detection, frequency of updates and the servers to use, scans, and the interface of the endpoint protection client. A single policy can be used for all platforms, i.e. Windows, macOS and Linux. The Windows, Apple and penguin symbols are used to show which platforms a configuration item can be applied to. Administrators can create policies to be applied to portable devices when they are outside the company LAN.

Enforce\Malware Removal page

Here you can see a list of quarantined malicious items, which you can e.g. investigate, search for in VirusTotal, delete, or whitelist. Malware can be deleted from a single device or multiple devices.

Enforce\Cloud Analysis page

This page shows you the results of analysis of suspicious files.

Endpoints page

All Sensors									
Sensors: 2									
<input type="text" value="Search"/> <input type="button" value="Status"/> <input type="button" value="OS"/> <input type="button" value="Signature"/> <input type="button" value="Policy"/> <input type="button" value="Export"/>									
		STATUS	DEVICE NAME	USER	OS	SENSOR	SIG	POLICY	T LAST CHECK-IN ACTIONS
<input type="checkbox"/>	>	✓	[redacted]	1909-64-01-01\User	Windows 10 x64	3.5.0.1545	●	Advanced	12:46:59 pm May 6, 2020 [redacted] [redacted]
<input type="checkbox"/>	>	✓	[redacted]	1909-64-02-01\User	Windows 10 x64	3.5.0.1545	●	Advanced	12:41:47 pm May 6, 2020 [redacted] [redacted]

The *Endpoints* page, shown above, provides an overview of devices on the network. A search box lets you search for a specific client in a larger network. For each device, details are kept to a very manageable level (status, user, details of the OS and sensor version, policies and last check-in time).

However, you can easily get more information about an individual device just by clicking on the arrow symbol to the left of its name. This will show items such as the scan engine version, external IP address, and last active user. Clicking on a device's name will open the *Investigate* page for that individual device. The *Go Live* button at the end of each device's entry establishes a remote administration session with the device. You can customise the columns shown on the *Endpoints* page if you like, and use the filter drop-downs to narrow the search for specific devices. By selecting a device or devices, you can carry out actions, such as scans, updates, policy changes and sensor updates. You can also quarantine a device. This cuts all network connections to and from it, with the exception of those to and from the management console.

Settings menu

The *Settings* menu item lets you configure options for the console/system as a whole. Under *Users* you can manage console users. There are 5 levels of permissions that can be assigned to a user, from *Level 1 Analyst* up to *System Admin*. Related to this is the *Roles* page, where you can edit what each permission level can actually do. Under *Notifications* you can set a threat severity at which an alert should be sent, and an email address to send it to. *Audit Log* records console-user logins and policy modifications/assignments.

Windows Endpoint Protection Client

Deployment

You can download installer files in .msi format from the *Sensor Options* menu on the *Endpoints* page. There is a choice of 32 and 64-bit packages. You need to enter an installation code, which can be found in the same menu. The installer file can be run manually, via a systems management product, or using an AD script. Using the *Send installation request* menu item, you can email users an installation link and code. The installation wizard is simple, and would present no problems even to non-technical users. You can prevent users with Windows Administrator Accounts from uninstalling the software, using the *Require code to uninstall sensor* setting in the applicable policy. Carbon Black Cloud integrates with VMware vSphere for deployment and upgrade purposes.

Functionality check

The user interface on protected endpoints consists of a System Tray icon and a small information window. Users can see product version information and a list of the most recent blocked threats. The latter includes the detection name and file path, along with date and time of detection. No other functionality is provided. The interface can be completely hidden by policy if you prefer. Integration with Windows Security Center can be enabled or disabled from the console.

When we connected a flash drive containing malware samples to our test PC, and opened the drive in Windows Explorer, Carbon Black immediately detected the malicious files and quarantined them in situ. A pop-up alert was shown, which closed after a few seconds. No user action was required or possible, though clicking on *Details* opened the program's detection-list window.

Features (as of December 2020)	Acronis Cyber Protect Cloud Advanced Edition	Avast Business Antivirus Pro Plus	Bitdefender Endpoint Security Elite (GravityZone Elite HD)	Cisco AMP for Endpoints Advantage	CrowdStrike Falcon Pro	Cybereason Defense Platform Enterprise	Elastic Endpoint Security	ESET PROTECT Entry & ESET PROTECT Cloud	FireEye Endpoint Security	FortiClient with FortiSandbox & FortiEDR	G DATA AntiVirus Business	K7 Enterprise Security	Kaspersky Endpoint Security for Business Select	Microsoft Defender ATP's Antivirus with MEM	Panda Endpoint Protection Plus on Aether	Sophos Intercept X Advanced	SparkCognition DeepArmor Endpoint Protection Platform	VIPRE Endpoint Security Cloud	VMware CarbonBlack Cloud			
Available Console Types																						
Cloud-based console	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*			
On-premise server-based console	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*			
Multi-tenancy features for managed service providers (included/paid extra/not included)	Included	Included	Included	Paid Extra	Included	Included	Included	Included	N/A	Included	Included	N/A	Included	N/A	N/A	Included	Included	Included	Included			
Client software deployment methods																						
Creation of .exe or .msi installer package	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*			
Share a link to remote users to install the software themselves	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*			
Push installation from the console	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*			
Supported Operating Systems																						
Microsoft Windows	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*			
Virtual environments (such as VMware, HyperV)	*		*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*			
Apple macOS		*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*			
Linux	*		*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*			
Google Android			*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*			
Apple iOS			*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*			
Windows Features																						
Anti-Malware	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*			
Protection settings are enabled by default (out-of-the-box-protection)		*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*			
Can clean-up a previously infected system (incl. registry leftovers and inactive malware)		*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*			
Right-click on-demand scan of files/folders		*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*			
The online malware detection rate is the same as offline	*		*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*			
Scans files only on execution (by default/design)					*										*		*	*	*			
Phishing protection (blocking of phishing URLs)	*	*	*	*				*		*	*	*	*	*	*	*	*	*	*			
Web access control / webfilter (custom blacklisting of URLs / site categories)	*	*	*	*		*		*		*	*	*	*	*	*	*	*	*	*			
Firewall		*	*	*		*		*		*		*	*	*	*	*	*	*	*			
Anti-Spam		*	*	*				*					*	*	*	*	*	*	*			
Data or Email encryption	*		*					*						*	*	*	*	*	*			
Splunk support			*	*	*	*	*	*	*	*			*		*	*	*	*	*			
Settings & Uninstall protection		*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*			
Cross-platform central management	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*			
Registers as AV product in Windows Security Center	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*			
Languages																						
Which languages can be used to contact support?	English, Japanese, German, Italian, French, Spanish, Korean	English, Czech, Japanese, French, German, Portuguese, Norwegian	English, Spanish, German, Romanian, French	All	English	English, Japanese	English	All	English, Japanese, French, Italian, Spanish, Portuguese, Arabic, Turkish, Hebrew	English, French, German, Japanese, Chinese	German, English, French, Italian, Spanish, Portuguese, Polish	English, Hindi	English, German, Dutch, French, Czech, Hebrew, Danish, Finnish, Italian, Norwegian, Portuguese, Romanian, Spanish, Swedish, Polish, Russian, Turkish, Arabic, Chinese, Japanese, Korean, Hindi, Malay	All	All	English, Italian, German, Spanish, French Japanese	English, Spanish	English, Swedish, Danish	All			
Which interface languages is the product available in?	English, German, Japanese, Russian, French, Italian, Spanish, Korean, Chinese, Polish, Czech, Hungarian, Danish, Dutch, Turkish, Indonesian, Portuguese, Bulgarian, Norwegian, Swedish, Finnish, Serbian, Malay	English, Spanish, French, German, Italian, Portuguese, Russian, Norwegian, Dutch, Bulgarian, Chinese, Czech, Estonian, Finnish, Greek, Hungarian, Japanese, Korean, Polish, Slovak, Slovenian, Swedish, Turkish, Ukrainian, Vietnamese	English, Spanish, German, Romanian, French, Italian, Portuguese, Polish, Russian, Czech, Chinese, Korean	English, Japanese, Korean, Chinese				English, German, Spanish, Greek, Turkish, French, Russian, Polish, Italian, Japanese, Chinese, Arabic, Slovak, Czech, Croatian, Korean	English	English, Chinese, French, German, Japanese, Korean, Portuguese, Spanish	English, Arabic, Polish, Korean, Italian, German, French,Chinese, Turkish, Spanish, Russian, Romanian, Portuguese, Dutch, Polish, Hungarian, Vietnamese, Czech, Japan, Kazakh	English, Chinese, French, German, Japanese, Korean, Portuguese, Spanish	German, English, French, Italian, Spanish, Portuguese, Polish, Turkish, Russian	English	English, Arabic, Polish, Korean, Italian, German, French,Chinese, Turkish, Spanish, Russian, Romanian, Portuguese, Dutch, Polish, Hungarian, Vietnamese, Czech, Japan, Kazakh	English, French, Dutch, Portuguese, Czech, Danish, German, Spanish, Italian, Norwegian, Polish, Russian, Finnish, Swedish, Turkish, Chinese, Japanese, Korean, Arabic, Hebrew		English, Spanish, French, Italian, Portuguese, Swedish, German, Hungarian, Russian, Polish, Chinese, Japanese, Finnish	English, German, French, Japanese, Italian, Chinese, Spanish, Portuguese, Korean	English, Spanish	English	English, Japanese
Which languages are the manuals available in?	English, German, French, Italian, Chinese, Korean, Japanese, Polish, Portuguese, Russian, Spanish, Taiwanese	English, Czech										English	English	English	English	English		English	English, Arabic, Bulgarian, Chinese, Croatian, Czech, Danish, Dutch, Estonian, Finnish, French, German, Greek, Hebrew, Hungarian, Italian, Japanese, Korean, Latvian, Lithuanian, Norwegian, Polish, Portuguese, Romanian, Russian, Serbian, Slovak, Slovenian, Spanish, Swedish, Thai, Turkish, Ukrainian			
Pricing (based on LIST PRICES; depending on the number of agents purchased, deal size or term, country/region, volume and competitive upgrade, discounts will apply/vary)																						
999 clients & 3 years, Relative Prices (from Very Low to Very High)																						
Cloud-based console																						
On-premise Windows-based console	Average	Average	Average	High	High	Very high	Average	Low	High	Very high	N/A	Low	Low	Average	Very High	Average	Average	High	Average			
			N/A	Very High	N/A						Low			N/A	N/A				High			



Copyright and Disclaimer

This publication is Copyright © 2020 by AV-Comparatives®. Any use of the results, etc. in whole or in part, is ONLY permitted after the explicit written agreement of the management board of AV-Comparatives prior to any publication. AV-Comparatives and its testers cannot be held liable for any damage or loss, which might occur as result of, or in connection with, the use of the information provided in this paper. We take every possible care to ensure the correctness of the basic data, but a liability for the correctness of the test results cannot be taken by any representative of AV-Comparatives. We do not give any guarantee of the correctness, completeness, or suitability for a specific purpose of any of the information/content provided at any given time. No one else involved in creating, producing or delivering test results shall be liable for any indirect, special or consequential damage, or loss of profits, arising out of, or related to, the use or inability to use, the services provided by the website, test documents or any related data.

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

AV-Comparatives
(December 2020)