Independent Tests of Anti-Virus Software

Business Security Test

TEST PERIOD:	MARCH – JUNE 2020
LANGUAGE:	ENGLISH
LAST REVISION:	10TH JULY 2020

WWW.AV-COMPARATIVES.ORG

Contents

Introduction

This is the first half-year report of our Business Main-Test Series[1] of 2020, containing the results of the Business Real-World Protection Test (March-June), Business Malware Protection Test (March), Business Performance Test (May), 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 products[2] were tested under Microsoft Windows 10 1909 64-bit:

Vendor	Product	Version March	Version April	Version May	Version June
Acronis	Cyber Protect Cloud – Advanced Edition	12.5	12.5	12.5	12.5
Avast	Business Antivirus Pro Plus	19.7	20.1	20.2	20.3
Bitdefender	GravityZone Elite Security	6.6	6.6	6.6	6.6
Cisco	AMP for Endpoints	7.1	7.1	7.2	7.2
CrowdStrike	Falcon Pro	5.26	5.29	5.30	5.32
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 & CA	7.2	7.2	7.2	7.2
FireEye	Endpoint Security	31.28	31.28	31.28	32.30
Fortinet	FortiClient with EMS, FortiSandbox & FortiEDR[3]	6.2	6.2	6.2	6.2
G DATA	AntiVirus Business	14.3	14.3	14.3	14.3
K7	Enterprise Security	14.2	14.2	14.2	14.2
Kaspersky	Endpoint Security for Business - Select	11.2	11.3	11.3	11.3
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	3.0	3.1	3.1	3.2
VIPRE	Endpoint Security Cloud	11.0	12.0	12.0	12.0
VMware	Carbon Black[4] Cloud	3.5	3.5	3.5	3.5

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] Formerly known as "enSilo" (acquired by Fortinet).

[4] **VMware** acquired **Carbon Black** in 2019.

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 PUA[5] 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 not 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.

[5] 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.

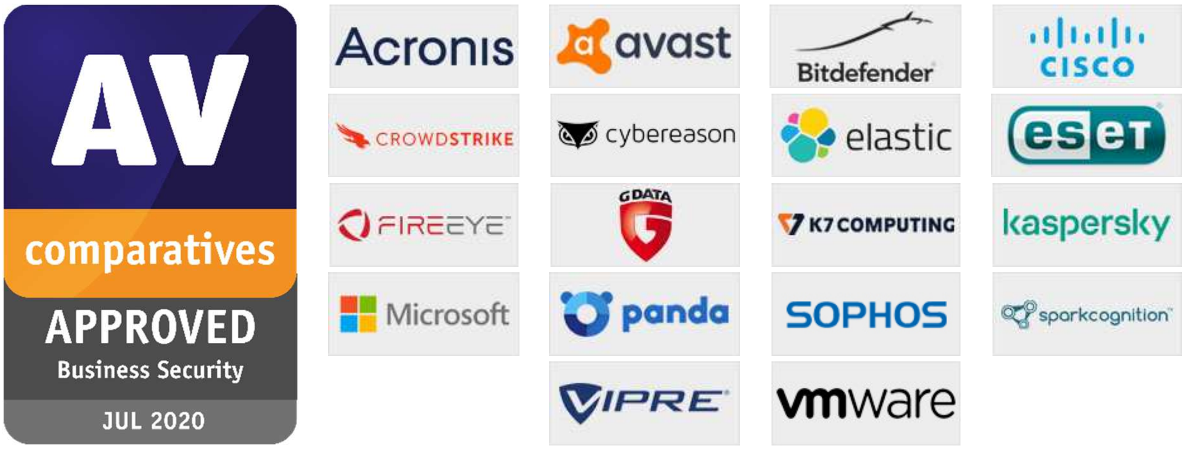
At the larger end of the market, **Cisco, CrowdStrike**, **Elastic, FireEye** and **SparkCognition** all offer exceptionally powerful tools. How well they will fit to your organization, both how it is today and how you intend to grow it over the next five years, needs to be carefully planned. There is 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 July 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 July 2020:



Although Fortinet achieved very good malware protection scores, it unfortunately did not reach all the requirements for the July 2020 Approved Award. This was due to significant performance impact on low-end hardware. We hope to see these issues resolved in the second round of testing this year (results of which are due in December 2020). The Performance Test in the second half of the year is always performed on high-end hardware.

Real-World Protection Test (March-June)

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).

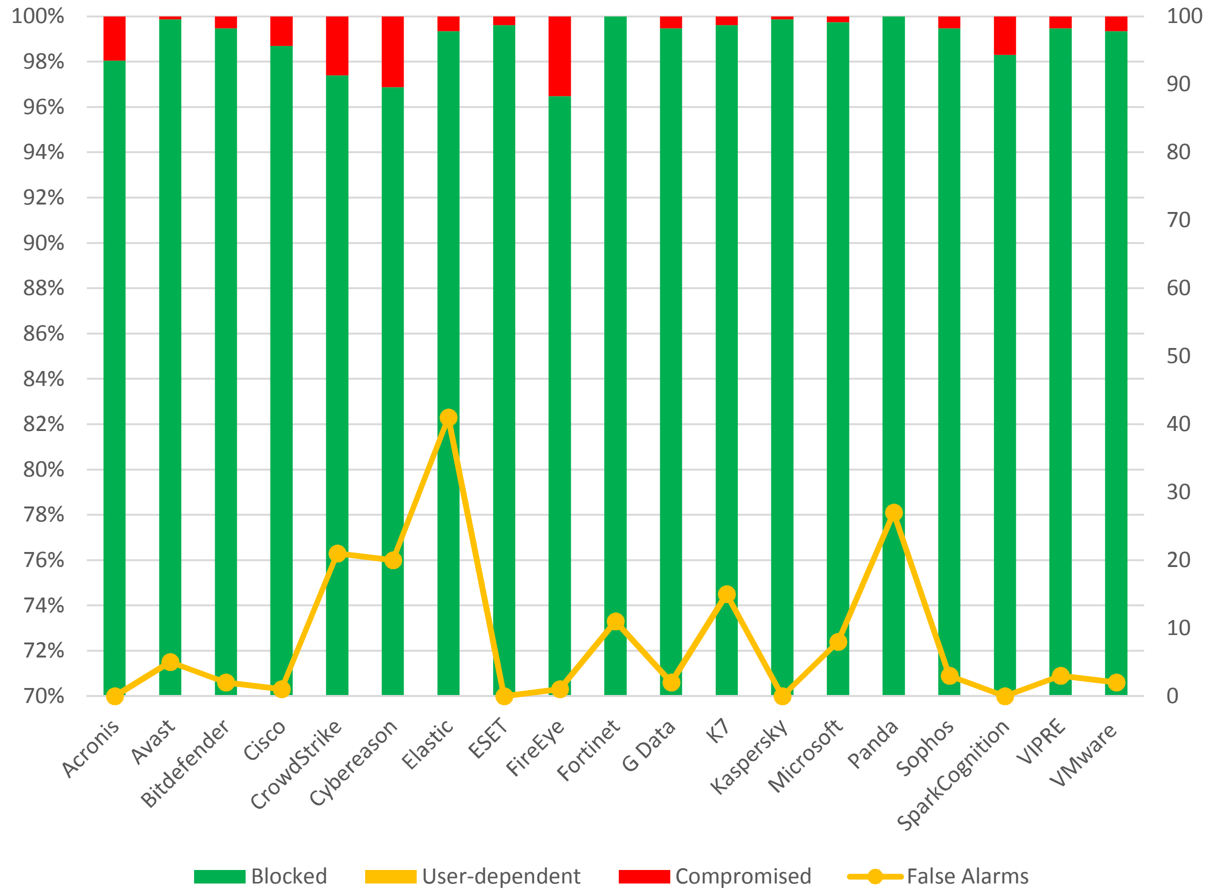
Due to the dynamic nature of the test, i.e. mimicking real-world conditions, and because of the way several different technologies (such as cloud scanners, reputation services, etc.) work, it is a matter of fact that such tests cannot be repeated or replicated in the way that e.g. static detection rate 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 **767** test cases (such as malicious URLs), tested from the beginning of March 2020 till the end of June 2020.



	Blocked	User dependent	Compromised	PROTECTION RATE [Blocked % + (User dependent %)/2][6]	False Alarms
Fortinet	767	-	-	100%	11
Panda	767	-	-	100%	27
Kaspersky	766	-	1	99.9%	0
Avast	766	-	1	99.9%	5
Microsoft	765	-	2	99.7%	8
ESET	764	-	3	99.6%	0
K7	764	-	3	99.6%	15
Bitdefender, G Data	763	-	4	99.5%	2
Sophos, VIPRE	763		4	99.5%	3
VMware	762	-	5	99.3%	2
Elastic	762	-	5	99.3%	41
Cisco	757	-	10	98.7%	1
SparkCognition	754	-	13	98.3%	0
Acronis	752	-	15	98.0%	0
CrowdStrike	747	-	20	97.4%	21
Cybereason	743	-	24	96.9%	20
FireEye	740	-	27	96.5%	1

[6] 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.

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

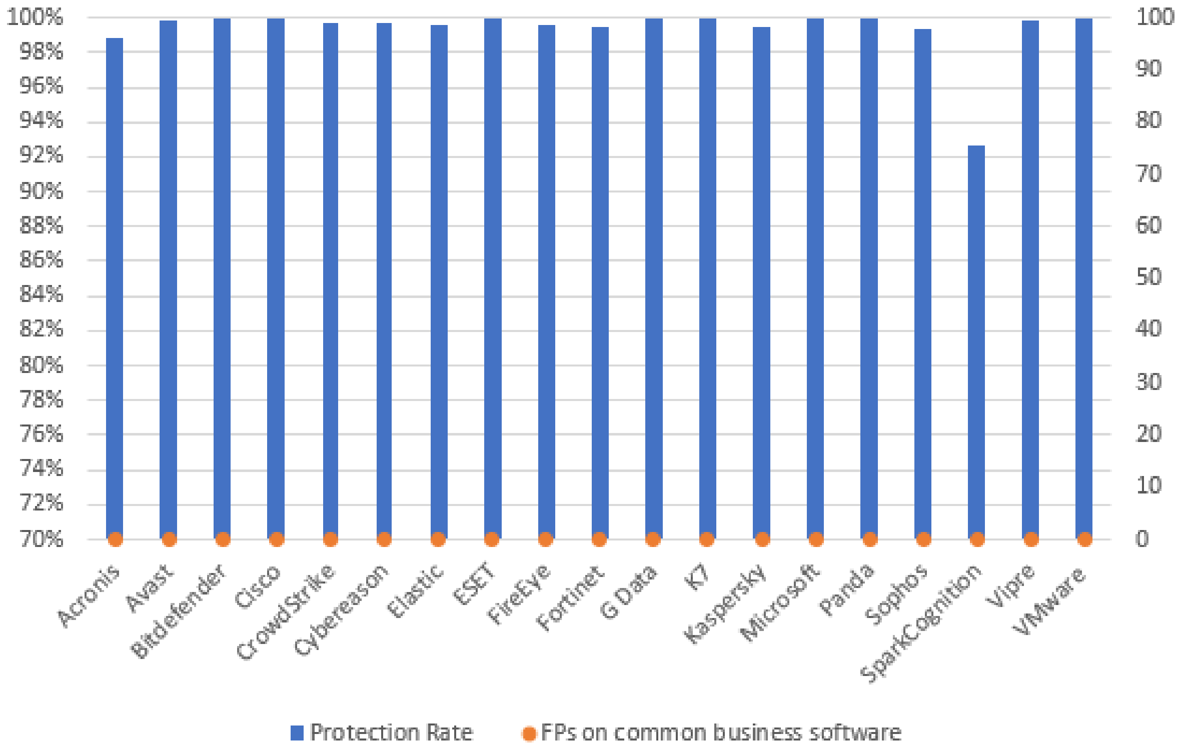
Malware Protection Test (March)

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. behavioral 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, **1,192** 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
Cisco, K7, Microsoft, VMware	100%	0
Bitdefender, ESET, G Data, Panda	99.9%	0
Avast, Vipre	99.8%	0
CrowdStrike, Cybereason	99.7%	0
Elastic, FireEye	99.6%	0
Fortinet, Kaspersky	99.5%	0
Sophos	99.4%	0
Acronis	98.9%	0
SparkCognition[7]	92.7%	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	6-25
Medium	26-50
High	51-100
Very High	101-150
Remarkably High	>150

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

[7] A SparkCognition product issue was uncovered during the Malware Protection Test which led to some missed detections. The bug has now been fixed.

Performance Test (May/June)

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 1909 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 i3 CPU system with 4GB of RAM and SSD system drives. We consider this machine configuration as "**low-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: copying[8] 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).

[8] 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, Windows operating system files, 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

Vendor	File copying		Archiving/ unarchiving	Installing/ uninstalling applications	Launching applications		Downloading files	Browsing Websites
	On first run	On subsequent runs			On first run	On subsequent runs		
Acronis	▮▮▯	▮▮▯	▮▮▮	▮▮▯	▮▮▯	▮▮▯	▮▮▮	▮▮▮
Avast	▮▮▮	▮▮▮	▮▮▮	▮▮▮	▮▮▮	▮▮▮	▮▮▯	▮▮▮
Bitdefender	▮▮▯	▮▮▮	▮▮▮	▮▮▮	▮▮▯	▮▮▮	▮▮▮	▮▮▮
Cisco	▮▮▯	▮▮▯	▮▮▮	▮▯▯	▮▮▮	▮▮▮	▮▮▮	▮▮▮
CrowdStrike	▮▮▮	▮▮▮	▮▮▮	▮▮▯	▮▮▮	▮▮▮	▮▮▮	▮▮▮
Cybereason	▮▮▯	▮▮▯	▮▮▮	▮▮▯	▮▯▯	▮▯▯	▮▮▮	▮▮▮
Elastic	▮▮▮	▮▮▮	▮▮▮	▮▮▮	▮▮▮	▮▮▮	▮▮▮	▮▮▮
ESET	▮▮▮	▮▮▮	▮▮▮	▮▮▮	▮▮▮	▮▮▮	▮▮▮	▮▮▮
FireEye	▮▯▯	▮▯▯	▮▮▯	▮▮▮	▮▮▯	▮▮▯	▮▮▮	▮▮▮
Fortinet	▯▯▯	▯▯▯	▮▮▯	▮▮▯	▮▮▯	▮▮▯	▮▯▯	▮▮▮
G Data	▮▯▯	▮▯▯	▮▮▮	▮▮▯	▮▮▯	▮▮▯	▮▮▯	▮▮▮
K7	▮▮▮	▮▮▮	▮▮▮	▮▮▮	▮▮▮	▮▮▮	▮▮▮	▮▮▮
Kaspersky	▮▮▮	▮▮▮	▮▯▯	▮▮▮	▮▮▮	▮▮▮	▮▮▮	▮▮▮
Microsoft	▮▯▯	▮▯▯	▮▮▮	▮▮▯	▮▮▮	▮▮▮	▮▮▮	▮▮▮
Panda	▮▮▮	▮▮▮	▮▮▮	▮▮▮	▮▮▮	▮▮▮	▮▮▮	▮▮▮
Sophos	▮▮▯	▮▮▯	▮▮▮	▮▯▯	▮▯▯	▮▮▮	▮▮▮	▮▮▮
SparkCognition	▮▮▮	▮▮▮	▮▮▮	▮▮▯	▮▮▯	▮▮▯	▮▮▮	▮▮▮
VIPRE	▮▮▮	▮▮▮	▮▮▮	▮▮▯	▮▮▮	▮▮▮	▮▮▮	▮▮▮
VMware	▮▮▮	▮▮▮	▮▮▮	▮▯▯	▮▮▮	▮▮▮	▮▮▮	▮▮▮

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 Edition[9] testing suite. Users using PC Mark 10 benchmark[10] 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 website[11].

"No security software" is tested on a baseline[12] system without any security software installed, which scores 100 points in the PC Mark 10 benchmark.

	PC Mark Score
Baseline	*100*
K7	98.9
ESET	98.7
Elastic	98.6
Vipre	98.4
Kaspersky	97.9
CrowdStrike	97.6
SparkCognition	96.9
Microsoft	96.8
Cybereason	96.6
Avast	96.5
Panda	96.3
Bitdefender	96.2
FireEye	95.7
G Data	95.3
Sophos	95.1
VMware	94.6
Acronis	94.3
Cisco	93.4
Fortinet	92.5

[9] For more information, see https://benchmarks.ul.com

[10] PC Mark® is a registered trademark of Futuremark Corporation / UL.

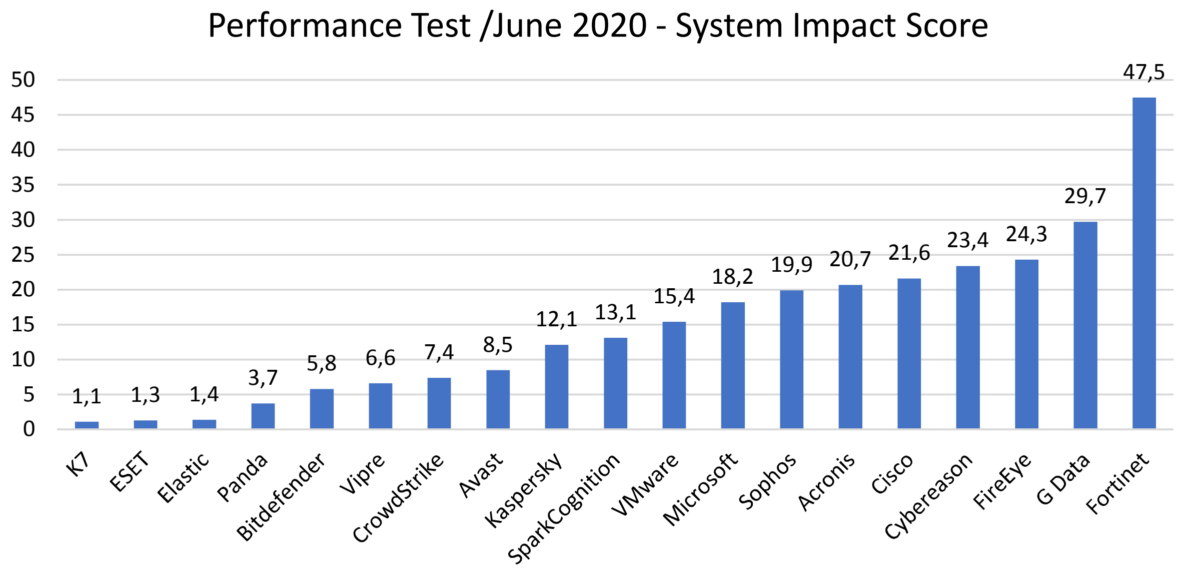
[11] http://s3.amazonaws.com/download-aws.futuremark.com/PCMark_10_Technical_Guide.pdf (PDF)

[12] Baseline system: Intel Core i3 machine with 4GB 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
K7	90	98.9	188.9	1.1
ESET	90	98.7	188.7	1.3
Elastic	90	98.6	188.6	1.4
Panda	90	96.3	186.3	3.7
Bitdefender	88	96.2	184.2	5.8
Vipre	85	98.4	183.4	6.6
CrowdStrike	85	97.6	182.6	7.4
Avast	85	96.5	181.5	8.5
Kaspersky	80	97.9	177.9	12.1
SparkCognition	80	96.9	176.9	13.1
VMware	80	94.6	174.6	15.4
Microsoft	75	96.8	171.8	18.2
Sophos	75	95.1	170.1	19.9
Acronis	75	94.3	169.3	20.7
Cisco	75	93.4	168.4	21.6
Cybereason	70	96.6	166.6	23.4
FireEye	70	95.7	165.7	24.3
G Data	65	95.3	160.3	29.7
Fortinet	50	92.5	142.5	47.5



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.

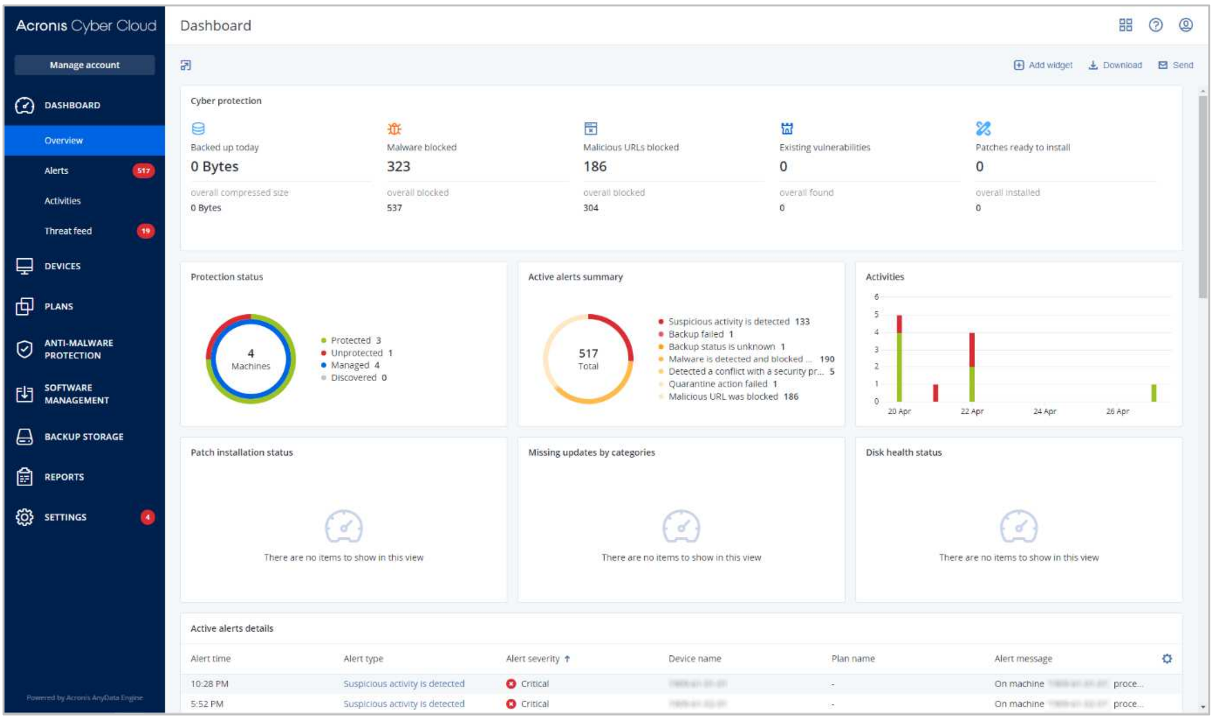
We first look at the type of product, i.e. whether the console is cloud based or server based, and what sort of devices/operating systems can be protected and managed.

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.

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.

Acronis Cyber Protect Cloud – Advanced Edition



Cyber protection

Backed up today	Malware blocked	Malicious URLs blocked	Existing vulnerabilities	Patches ready to install
0 Bytes	323	186	0	0
overall compressed size	overall blocked	overall blocked	overall found	overall installed
0 Bytes	537	304	0	0

Protection status

4 Machines

- Protected 3
- Unprotected 1
- Managed 4
- Discovered 0

Active alerts summary

517 Total

- Suspicious activity is detected 133
- Backup failed 1
- Backup status is unknown 1
- Malware is detected and blocked ... 190
- Detected a conflict with a security pr... 5
- Quarantine action failed 1
- Malicious URL was blocked 186

Activities

Patch installation status

There are no items to show in this view

Missing updates by categories

There are no items to show in this view

Disk health status

There are no items to show in this view

Active alerts details

Alert time	Alert type	Alert severity ↑	Device name	Plan name	Alert message
10:28 PM	Suspicious activity is detected	Critical	[redacted]	-	On machine [redacted] proce...
5:52 PM	Suspicious activity is detected	Critical	[redacted]	-	On machine [redacted] proce...

Verdict

Acronis' cloud-based management console stands out for its very clear and clean modern interface. All the management functionality is easily accessible via a single menu column on the left-hand side of the window. Individual pages have a simple, uncluttered view, which makes it easy to find the details. In many ways the console resembles a well-designed smartphone app, and would doubtless scale very well when used on the smaller screen of, say, a tablet. The product's simplicity and clarity mean that it would be particularly well suited to smaller businesses and less-experienced administrators.

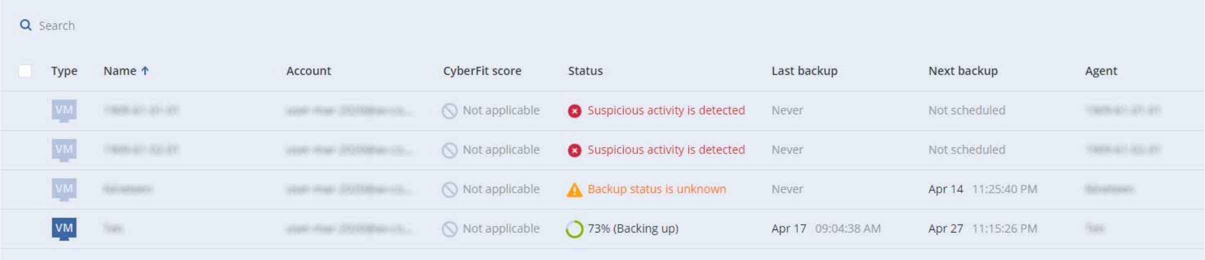
About the product

The Acronis Cyber Cloud platform provides a combined cybersecurity and data protection service. There is a variety of cloud-based services included, including backup, disaster recovery, and secure file-synchronisation, in addition to endpoint protection. This review considers only the malware protection features. There are clients for Windows and macOS workstations, Windows and Linux servers, plus Android and iOS mobile devices.

Getting up and running

Installing the client software is very simple. Just go to the *Devices* page and click the *Add* button, and select the appropriate installer from the list that then opens. This can be downloaded and run on the client device. You can also create .mst and .msi files for unattended installation. When the endpoint software has been installed, you have to assign a *Protection Plan* to the newly installed machine, in order to activate the antimalware service. We note that Windows Defender is not disabled by the setup wizard, so administrators may wish to do this manually or by policy.

Everyday management



Search

□	Type	Name ↑	Account	CyberFit score	Status	Last backup	Next backup	Agent
	VM	[redacted]	[redacted]	⃠ Not applicable	✖ Suspicious activity is detected	Never	Not scheduled	[redacted]
	VM	[redacted]	[redacted]	⃠ Not applicable	✖ Suspicious activity is detected	Never	Not scheduled	[redacted]
	VM	[redacted]	[redacted]	⃠ Not applicable	⚠ Backup status is unknown	Never	Apr 14 11:25:40 PM	[redacted]
	VM	[redacted]	[redacted]	⃠ Not applicable	○ 73% (Backing up)	Apr 17 09:04:38 AM	Apr 27 11:15:26 PM	[redacted]

The *Devices* page lists the devices 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. 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.

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, cryptomining 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.

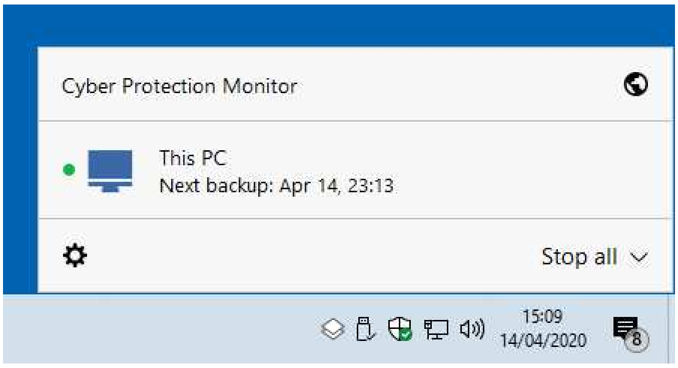
Under *Anti-Malware Protection*, the *Quarantine* page lists the names of malicious files that have been detected, along with the date quarantined and device name. You can add columns for the threat name and applicable protection plan from the page settings. A mini menu at the end of each entry lets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

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.

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* 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.

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.

Windows endpoint protection software

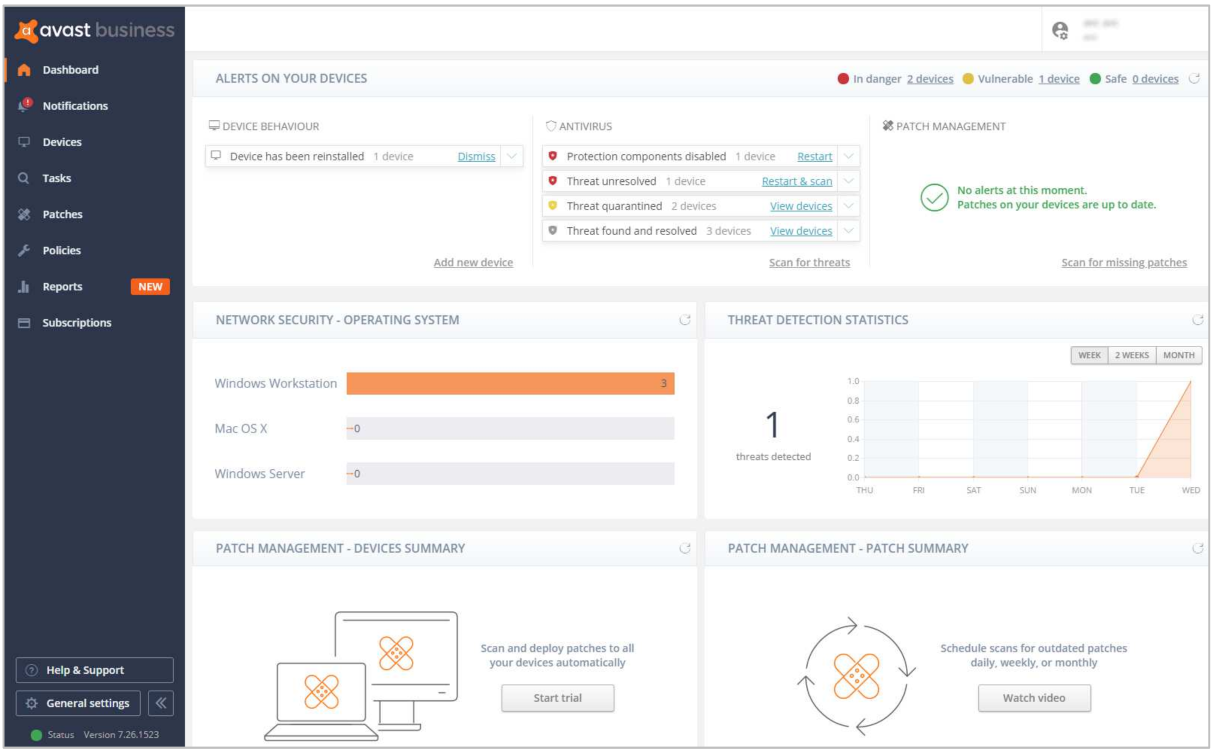


Cyber Protection Monitor

This PC
Next backup: Apr 14, 23:13

The client software has a minimalist interface, which does not allow any users to interact with the malware protection service. The *Stop all* link in the screenshot above refers to the backup service – the protection service cannot be disabled here. If the user should inadvertently copy a malicious file to the system, Acronis will detect and quarantine it on access. Malware detections are silent, i.e. no alerts are shown. Exactly the same interface is used for client and server protection software.

Avast Business Antivirus Pro Plus



Device has been reinstalled 1 device Dismiss

Protection components disabled 1 device Restart

Threat unresolved 1 device Restart & scan

Threat quarantined 2 devices View devices

Threat found and resolved 3 devices View devices

No alerts at this moment.
Patches on your devices are up to date.

Scan and deploy patches to all your devices automatically

Schedule scans for outdated patches daily, weekly, or monthly

Verdict

Avast Business Antivirus Pro Plus is a strong cloud-based product ideal for small to medium-sized businesses. The UI is intuitive and clean, and the defaults are sensible for the smaller organisation. A non-technical user should not have any problems deploying this and keeping track of events. However, it still has grouping and profile capabilities to protect the larger estates. We liked the straightforward nature of the platform.

About the product

Avast Business Antivirus Pro Plus uses a cloud-based console to deploy, manage, and monitor the endpoint protection software on all devices. The product protects Windows clients, Windows servers and macOS devices. Windows client features 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.

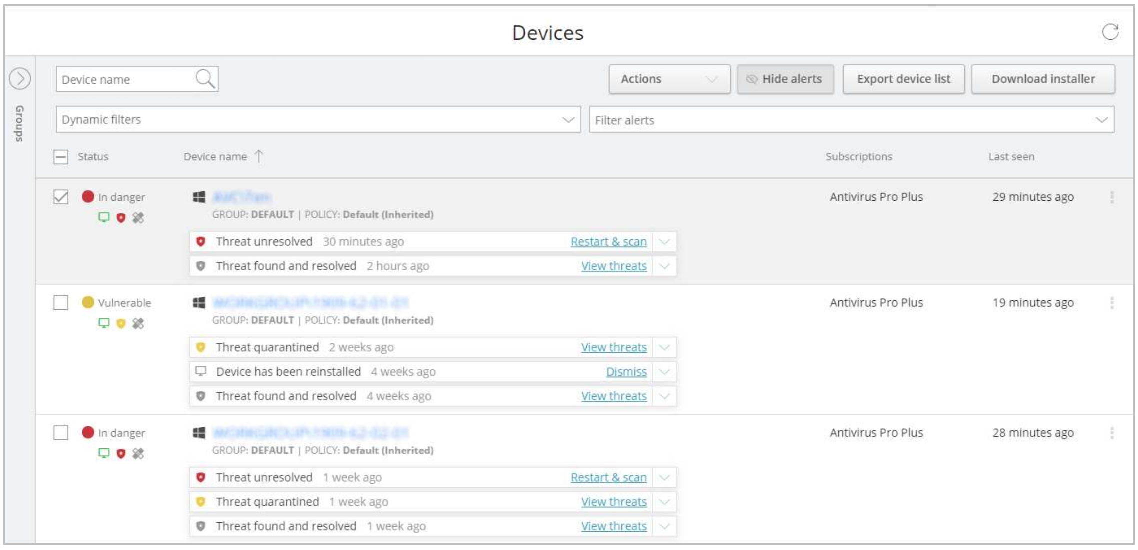
Getting up and running

There is no server component to install because it is run from a cloud-based console. You create the account, apply appropriate licensing, and then add devices. Deployment can be carried out via remote push, downloading an installer package, or by sending a download link via email. The installer is offered in two sizes, both being very simple to use. There is a Light version, around 6MB in size, which is just a downloader. The full version is around 300 MB and can be run offline. The former is ideal for smaller networks, the latter is better for larger deployments to minimise internet traffic. The wizard offers to remove existing competitive AV products.

Everyday management

On the server console, there is a clear set of main menus down the left-hand side. These are: *Dashboard*, *Notifications*, *Devices*, *Tasks*, *Patches*, *Policies*, *Reports,* and *Subscriptions*. *Help & Support* and *General Settings* are found at the bottom. The default *Dashboard* page gives an overview of the installation and how it is running. You can see alerts on your devices, OS distribution, threat detection statistics, and patch management summaries.

Notifications collates all the main event information into one place. Malware detection notifications link through to the *Virus Chest* (quarantine) on the affected computer. The *Notifications Settings* panel is comprehensive. It allows you to set up how notifications will be handled across a wide range of scenarios. We particularly liked the "if not read then send email notification" which can be set to "instantly", "batched end of week" or "never" for each setting. This offers a lot of control of how you are notified when an event occurs. You can ensure that you are not swamped with information that is not immediately relevant.



Status	Device name	Subscriptions	Last seen
☑ In danger	[redacted] GROUP: **DEFAULT** | POLICY: **Default (Inherited)** Threat unresolved 30 minutes ago Restart & scan Threat found and resolved 2 hours ago View threats	Antivirus Pro Plus	29 minutes ago
□ Vulnerable	[redacted] GROUP: **DEFAULT** | POLICY: **Default (Inherited)** Threat quarantined 2 weeks ago View threats Device has been reinstalled 4 weeks ago Dismiss Threat found and resolved 4 weeks ago View threats	Antivirus Pro Plus	19 minutes ago
□ In danger	[redacted] GROUP: **DEFAULT** | POLICY: **Default (Inherited)** Threat unresolved 1 week ago Restart & scan Threat quarantined 1 week ago View threats Threat found and resolved 1 week ago View threats	Antivirus Pro Plus	28 minutes ago

The *Devices* tab (screenshot above) 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.

Tasks is a powerful scheduler area. Here the administrator can create tasks to run particular events. For example, do a quick scan every day at 2pm. You can also use it to send a short message to your devices, to update the device and to shut it down too. It is a simple task management tool, but has useful capabilities for the small office and organisation.

The *Patches* page provides a very brief description of the feature, which is available to purchase as a separate component, along with a button marked *Start* Trial.

Policies allows you to create a settings template which is then applied to a group of devices. In here, you have access to all the control functionality for the device. So, you can determine that file scanning is on, the antispam service is running, the firewall must be applied, and so forth. From these templates, you can apply policies to devices. Separate policies can be configured for Windows workstations, Windows servers, and macOS devices.

At the time of writing (May 2020), *Reports* was marked as a “new” feature in the console menu column, though in fact it is an update of an existing feature. 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.

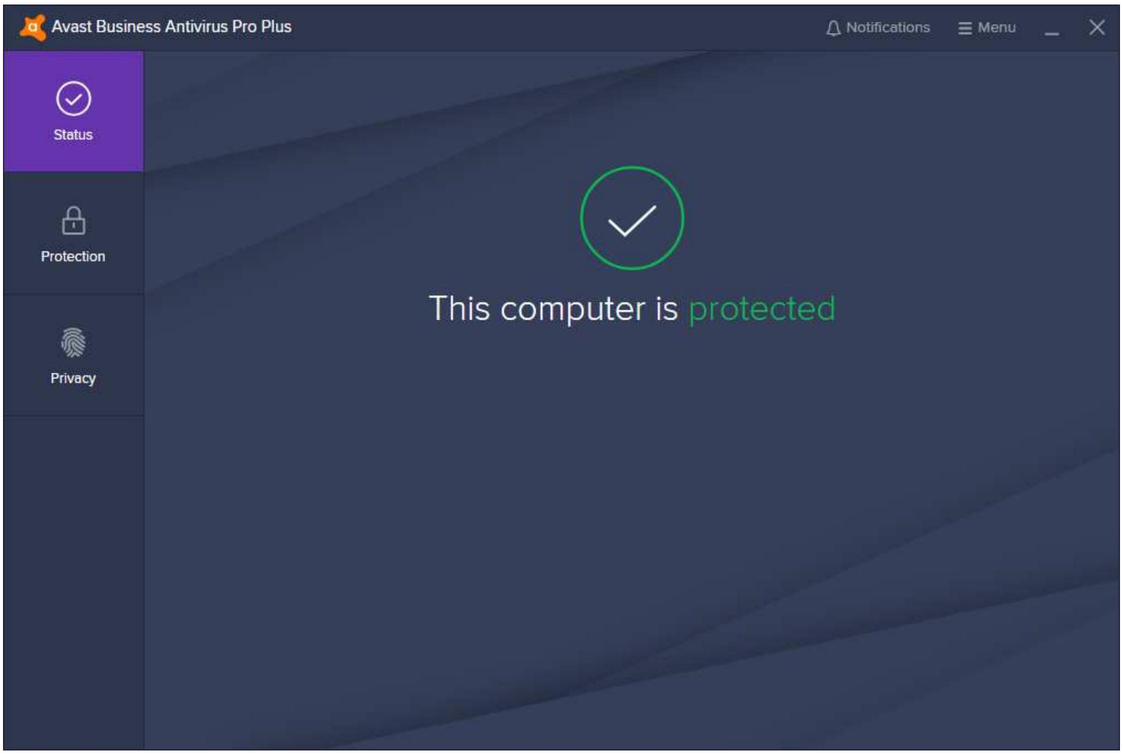
As you would expect, *Subscriptions* shows you the product licences you currently have, and how many of them you have used. There are also links that let you try or buy other versions of Avast Business Antivirus, and the Patch Management component.

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 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, and import the database of another Avast console.

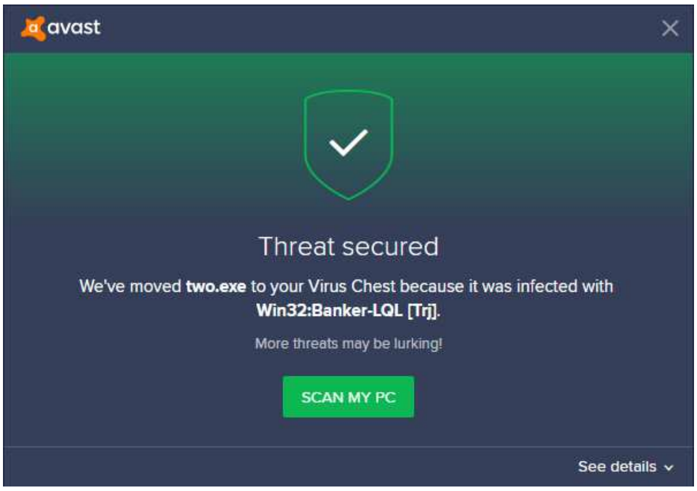
Windows endpoint protection software

The Windows desktop protection software offers a wide range of capabilities, much like a normal end-user desktop solution. Users can run scans and updates. The central policies determine what they can change or adjust. By default, Windows Standard User Accounts can disable all protection features, and supress further warnings by clicking *Ignore*. This results in a misleading message, stating “You’re protected”, even though all protection components have been switched off. Protection will be automatically re-enabled when the computer is restarted. However, admins may want to prevent Standard Users from changing the settings, which can be done by enabling the password protection feature in the console.



This computer is protected

If the user should inadvertently copy a malicious file to the system, Avast will detect and quarantine it on access. An example alert is shown below. The user can start a scan of the PC, and see details of the threat.



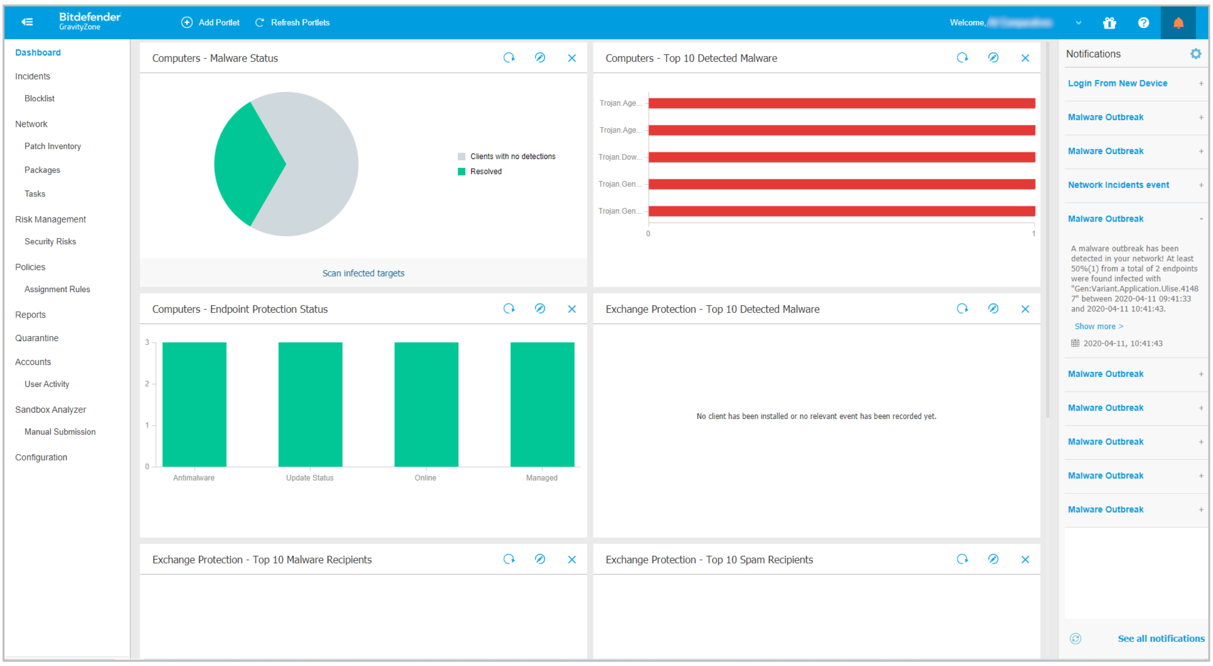
Threat secured

We've moved **two.exe** to your Virus Chest because it was infected with **Win32:Banker-LQL [Trj]**.

More threats may be lurking!

The GUI of the server protection software is identical to that of its desktop counterpart.

Bitdefender GravityZone Elite Security



No client has been installed or no relevant event has been recorded yet.

A malware outbreak has been detected in your network! At least 50%(1) from a total of 2 endpoints were found infected with "Gen:Variant.Application.Ulise.41487" between 2020-04-11 09:41:33 and 2020-04-11 10:41:43.

2020-04-11, 10:41:43

Verdict

There is much to like in Bitdefender GravityZone Elite Security. The design of the management console is very clear. Relevant tasks are grouped together, and the initial walkthrough wizard makes deployment easy. We particularly liked the *Dashboard* functionality. The *Policies* feature gives a clear understanding of the rules applied to endpoints. One minor suggestion for improvement would be to clarify the process for setting scan exclusions.

About the product

Bitdefender GravityZone Elite Security uses a cloud-based console to manage endpoint protection software. Desktops and servers running Windows, macOS and Linux are all supported.

Getting up and running

Getting the main cloud console up and running is very simple: create the cloud account, log in and you have a working environment.

The first thing you see on login is the *Essential Steps* wizard. This is a four-step process to guide you on getting up and running as quickly as possible. Each panel has copious explanations to help explain what that step is achieving.

Step 1 is *Install Protection*, which allows you to install directly onto the computer you are working on. You can also email an installation link to remote users. Alternatively, you can use the *Remote Installation* capability to remotely install the endpoint client on network computers. To enable this, you need to install a “relay” computer, to act as the bridgehead.

Step 2 is to create the *Security Policies* to be used in your organisation. This allows you to define a pre-cooked set of operational requirements onto each target device, or group of devices.

Step 3 is to create appropriate *User Accounts*. These are administrative accounts for the management of the platform. The roles here can be *Partner*, *Company Administrator*, *Network Administrator*, *Reporter* and *Custom*. A *Reporter* might be e.g. a help-desk role, and can see reports of activity without being able to change users or the company structure.

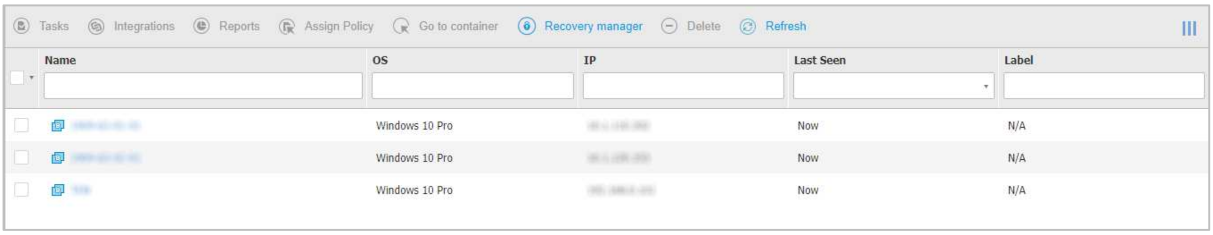
Step 4 is *Reporting*, where it shows you how to create appropriate reports of activity on your network. Having gone through these steps, you should have a deployed and managed network.

Everyday management

The console is particularly clear and clean. This helps make the product suitable for a smaller companies with limited IT support, as well as larger organisations. The main console has a menu structure down the left-hand side. The items are *Dashboard*, *Incidents*, *Network*, *Risk Management*, *Policies*, *Reports*, *Quarantine*, *Accounts*, *Sandbox Analyzer* and *Configuration*.

Dashboard gives you an instant overview of the installation and the performance of the clients. Each panel here is called a "Portlet", and can be clicked on to drill into more information. There are three pages of Portlets in total. We particularly liked the way that the Portlets can be rearranged, added to, and laid out to your preferences. The strong capabilities of *Dashboard* mean that you can quickly and easily find the information you need.

Incidents allows you to review and investigate threats detected on the network.



	Name	OS	IP	Last Seen	Label
□	[redacted]	Windows 10 Pro	[redacted]	Now	N/A
□	[redacted]	Windows 10 Pro	[redacted]	Now	N/A
□	[redacted]	Windows 10 Pro	[redacted]	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). The *Packages* sub-page lets you configure deployment packages. On the *Tasks* sub-page you can create tasks such as scans and updates, which can be run once or multiple times on specified devices or groups.

The *Risk Management* page displays a breakdown of risks according to factors such as date, severity, and number of endpoints affected.

Policies is where you define the operational groups within your organisation, and then apply policies to them. There is a wealth of capability here. You can control the firewall functionality, application operation, and device access (e.g. blocking USB drives). You can set rules for Exchange Server too. We found that the process of setting scan exclusions here took a little getting used to. It would be helpful to separate the entry boxes for new exclusions from the table of existing exclusions, and to make clearer that the former are also drop-down lists.

Reports lets you build views of what is happening, by functional group or by task area.

Quarantine gives you an overview of all the malware that has been quarantined on the network, and the ability to choose what to do with those files.

Accounts lets you add and remove console users, and monitor the activities of the user accounts that have been set up.

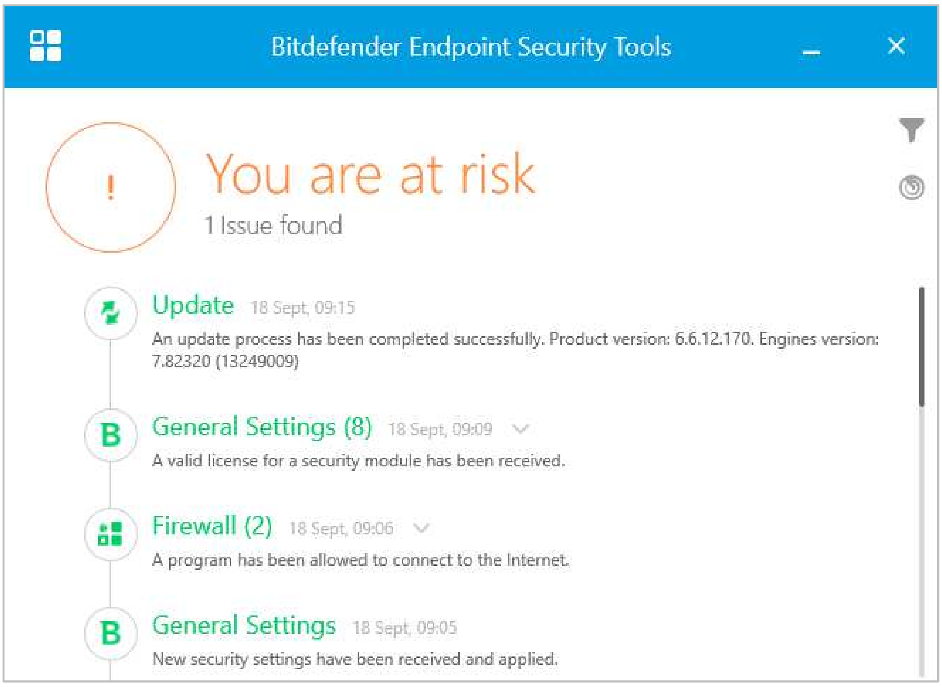
Sandbox Analyzer provides a breakdown of unknown files that have been analysed by the sandbox feature, with a severity score from 0 (completely harmless) to 30 (clearly malicious).

The *Configuration* page lets you change settings for the console itself.

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. Drilling into an item gives a clear description of what happened. We particularly liked the reporting of a malware outbreak. This informed us that "at least 28% from a total number of X endpoints were found infected with Y malware". This makes it easy to separate out isolated incidents from a network-wide pandemic.

Windows endpoint protection software

The Windows desktop protection software is a simple application with a clean interface. It clearly shows what is going on, with details of updates carried out, modules enabled, and programs allowed through the firewall. The user interface allows the user to check for updates, and initiate quick, full or custom scans. Users can also view the program's settings, but the default policy prevents any changes being made. You can easily change the user interface language from the System Tray menu.



You are at risk

1 Issue found

Update 18 Sept, 09:15

An update process has been completed successfully. Product version: 6.6.12.170. Engines version: 7.82320 (13249009)

General Settings (8) 18 Sept, 09:09

A valid license for a security module has been received.

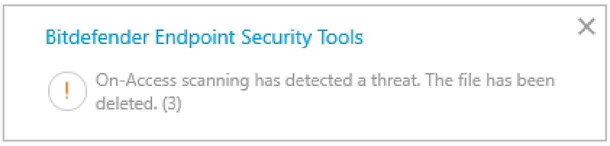
Firewall (2) 18 Sept, 09:06

A program has been allowed to connect to the Internet.

General Settings 18 Sept, 09:05

New security settings have been received and applied.

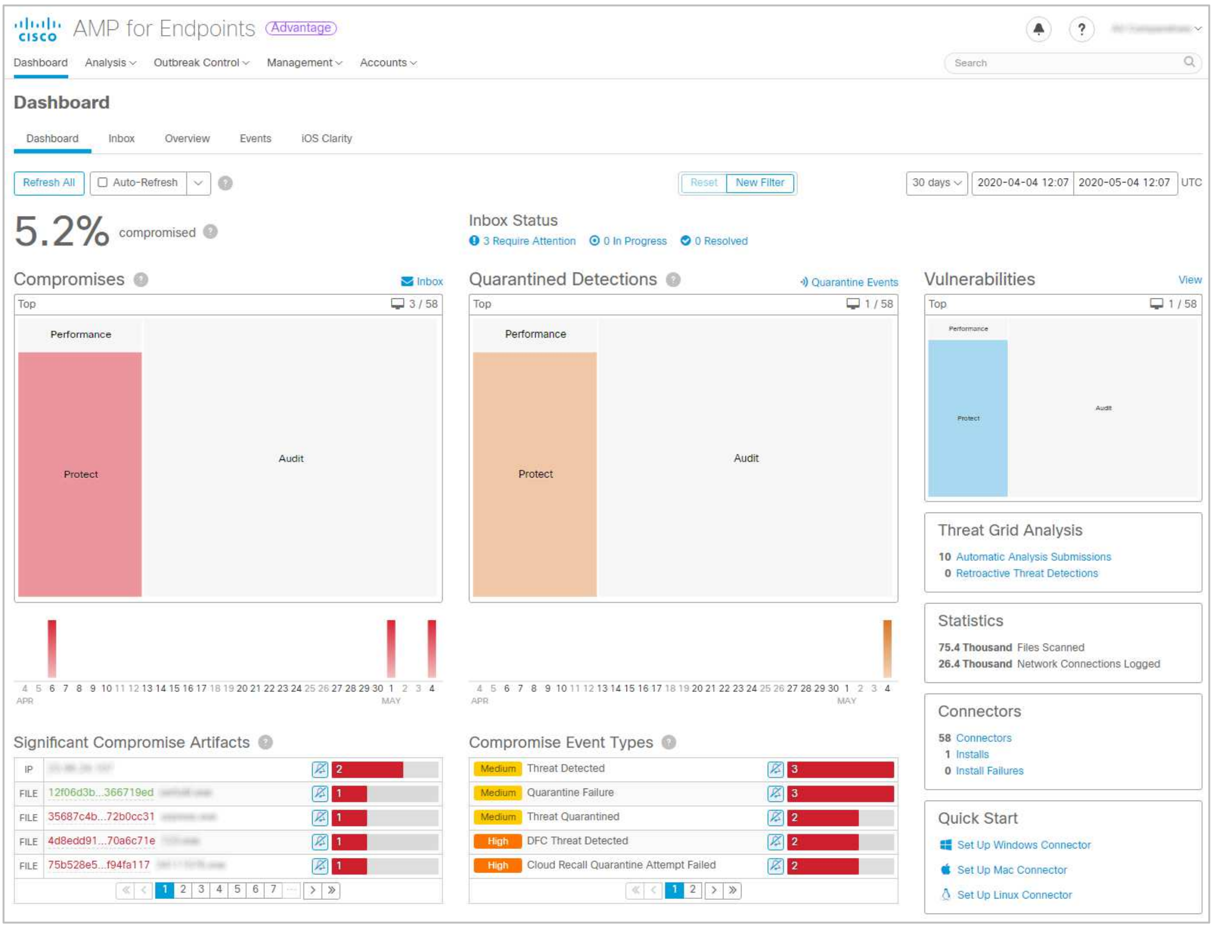
If the user should inadvertently copy a malicious file to the system, Bitdefender will detect and quarantine it on access. An example alert is shown below. The user cannot take any action, and the alert closes after a few seconds.


Bitdefender Endpoint Security Tools

On-Access scanning has detected a threat. The file has been deleted. (3)

The GUI of the server protection software is identical to that of its desktop counterpart.

Cisco Advanced Malware Protection for Endpoints



5.2% compromised

Inbox Status

3 Require Attention 0 In Progress 0 Resolved

Significant Compromise Artifacts

IP	[redacted]	2
FILE	12f06d3b...366719ed [redacted]	1
FILE	35687c4b...72b0cc31 [redacted]	1
FILE	4d8edd91...70a6c71e [redacted]	1
FILE	75b528e5...f94fa117 [redacted]	1

Compromise Event Types

Medium	Threat Detected	3
Medium	Quarantine Failure	3
Medium	Threat Quarantined	2
High	DFC Threat Detected	2
High	Cloud Recall Quarantine Attempt Failed	2

Threat Grid Analysis

10 Automatic Analysis Submissions
0 Retroactive Threat Detections

Statistics

75.4 Thousand Files Scanned
26.4 Thousand Network Connections Logged

Connectors

58 Connectors
1 Installs
0 Install Failures

Quick Start

Set Up Windows Connector
Set Up Mac Connector
Set Up Linux Connector

Verdict

Getting started with Cisco Advanced Malware Protection for Endpoints (AMP) is very straightforward. The console requires no setup, and deploying the client software is quick and easy. Clear and colourful charts summarise the most important information. Regarding more advanced monitoring and management, there is a lot of functionality available here. The console's design makes the different features easy to access. However, unlocking the product's full potential may take some time, depending on various factors like size and complexity of your environment, use cases and so on. For organisations with appropriate IT staff resources, it provides a wealth of features for monitoring, investigating and blocking security threats.

About the product

Cisco AMP provides malware protection for Windows, macOS, Linux, Android and Apple iOS devices. These are all managed from a cloud-based console.

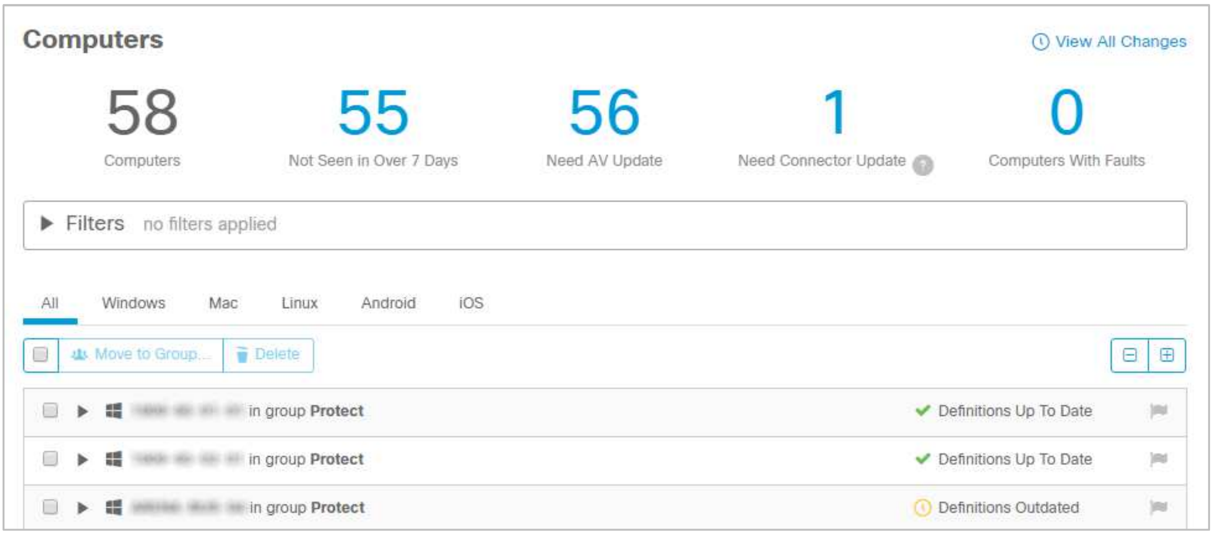
Getting up and running

As the console is cloud-based, no installation is necessary. You just browse to the URL and log in. Installers for desktop systems can be found by clicking *Management\Download Connector*. You need to select *Protect* from the Group menu. The setup process is very quick and simple, and only takes a couple of clicks. We note that Windows Defender is not disabled automatically on Windows desktop systems when the Cisco endpoint software is installed. Administrators might like to do this themselves, either manually or by policy.

Everyday management

The cloud console is navigated from a single menu bar at the top of the page. The *Dashboard* page has a number of sub-pages accessible from a row of tabs at the top. *Analysis, Outbreak Control, Management and Accounts* are drop-down menus. Each has about 10 individual items.

The *Dashboard* sub-page of the *Dashboard* 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* sub-page shows a compact, summarised version of the same thing. The *Overview* sub-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 and file analysis. These provide a very clear summary of the most important information, and we wonder whether this might not be made the default page of the console. The *Events* sub-page lists recent detections.



Computers

View All Changes

58 Computers | 55 Not Seen in Over 7 Days | 56 Need AV Update | 1 Need Connector Update | 0 Computers With Faults

▶ Filters no filters applied

All | Windows | Mac | Linux | Android | iOS

□ Move to Group... | Delete

□ ▶	[redacted] in group **Protect**	✓ Definitions Up To Date	
□ ▶	[redacted] in group **Protect**	✓ Definitions Up To Date	
□ ▶	[redacted] in group **Protect**	Definitions Outdated	

The *Computers* page, shown above, is accessed from the *Management* menu. It 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 device 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 device list can be narrowed by OS type, using the tabs at the top. You can also filter the device list using various details. These include specific OS version, group, or definitions status, by clicking on *Filters* at the top.

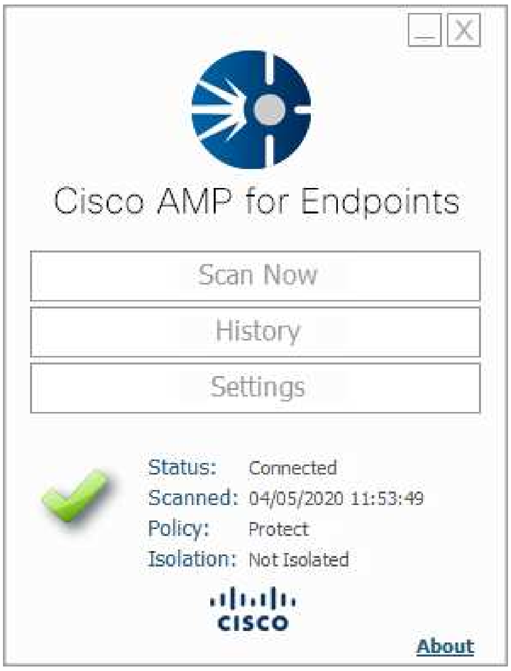
The *Management* menu contains a number of other standard features. There are *Groups, Policies, Exclusions*, and deployment options. There is also a *Quick Start* guide, in the form of a video explaining the product’s features and usage. In the *Analysis* menu you can find features for investigating attacks. *Events* shows a list of 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. If you right-click a file’s hash here, you can take action against the threat. Options include blacklisting the file, and *Investigate in Cisco Threat* Response. This opens a separate console, which provides additional analysis data. Cisco tell us that this includes information from third-party security services as well as their own.

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 weekly report. This covers numerous items such as threats, compromises and vulnerabilities. These are illustrated with coloured bar and doughnut charts. Finally, the *Indicators* page lets you search for Cloud IOCs. You can access the page from *Analysis\Indicators* on the main menu. Each indicator includes a brief description along with information about the tactics and techniques employed based on the Mitre ATT&CK knowledge base. Tactics represent the objective of an attack, such as executing malware or exfiltrating confidential information. Techniques are the methods attackers use to achieve the objectives or what they gain.

The *Outbreak Control* menu provides options for blocking or whitelisting 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.

Windows endpoint protection software

The Windows desktop protection software has a very simple GUI, which allows users to run scans and view the logs. Both of these functions open in separate, larger windows. Users can also view settings, but by default these are locked down. Users have a choice of scans they can run. Options are *Flash Scan* (running processes), *Custom Scan, Full Scan* and *Rootkit Scan*.

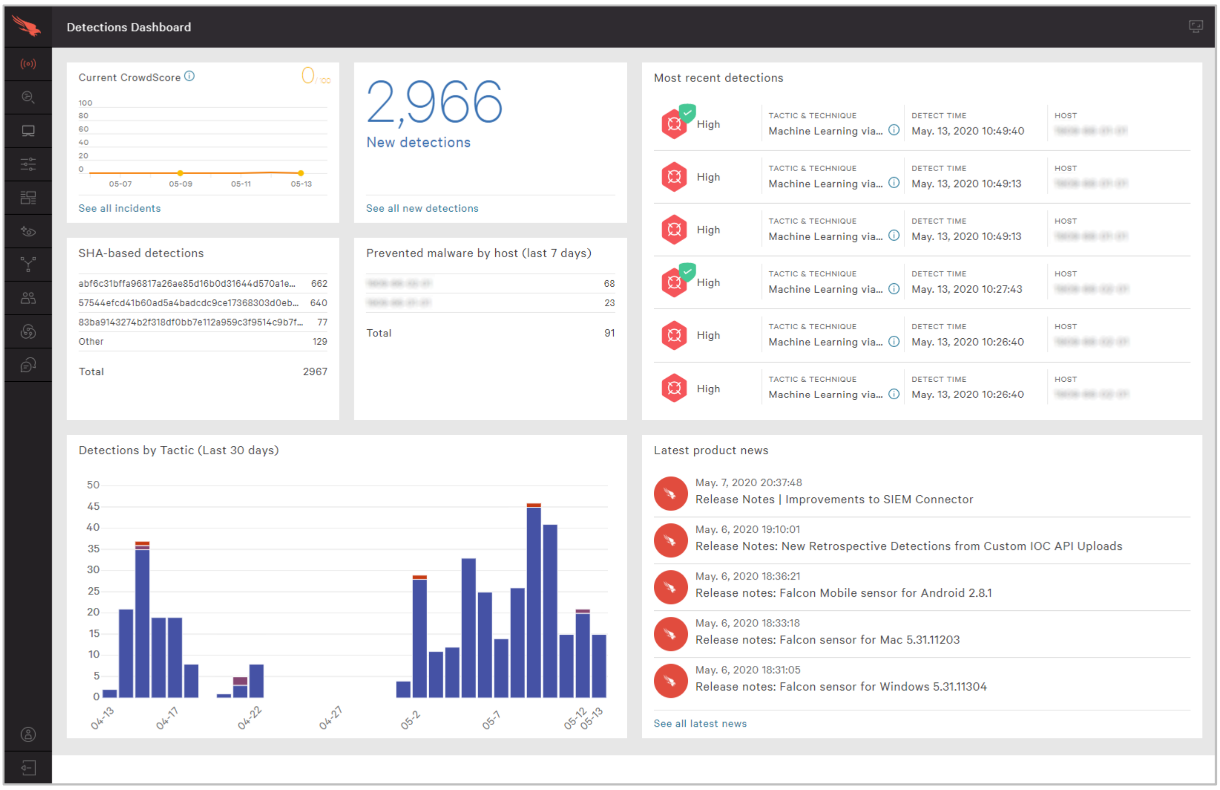


Status: Connected
Scanned: 04/05/2020 11:53:49
Policy: Protect
Isolation: Not Isolated

If the user should inadvertently copy a malicious file to the system, Cisco will detect and quarantine it on access. By default, detection is silent, i.e. no alert is shown to the user. However, the endpoint software can be configured by policy to show notifications.

The GUI of the server protection software is identical to that of its desktop counterpart.

CrowdStrike Falcon Pro



Detections Dashboard

Current CrowdScore ⓘ 0/100

See all incidents

2,966

New detections

See all new detections

SHA-based detections

abf6c31bffa96817a26ae85d16b0d31644d570a1e...	662
57544efcd41b60ad5a4badcdc9ce17368303d0eb...	640
83ba9143274b2f318df0bb7e112a959c3f9514c9b7f...	77
Other	129
Total	2967

Prevented malware by host (last 7 days)

[redacted]	68
[redacted]	23
Total	91

Most recent detections

	TACTIC & TECHNIQUE	DETECT TIME	HOST
High	Machine Learning via... ⓘ	May. 13, 2020 10:49:40	[redacted]
High	Machine Learning via... ⓘ	May. 13, 2020 10:49:13	[redacted]
High	Machine Learning via... ⓘ	May. 13, 2020 10:49:13	[redacted]
High	Machine Learning via... ⓘ	May. 13, 2020 10:27:43	[redacted]
High	Machine Learning via... ⓘ	May. 13, 2020 10:26:40	[redacted]
High	Machine Learning via... ⓘ	May. 13, 2020 10:26:40	[redacted]

Detections by Tactic (Last 30 days)

Latest product news

May. 7, 2020 20:37:48
Release Notes | Improvements to SIEM Connector

May. 6, 2020 19:10:01
Release Notes: New Retrospective Detections from Custom IOC API Uploads

May. 6, 2020 18:36:21
Release notes: Falcon Mobile sensor for Android 2.8.1

May. 6, 2020 18:33:18
Release notes: Falcon sensor for Mac 5.31.11203

May. 6, 2020 18:31:05
Release notes: Falcon sensor for Windows 5.31.11304

See all latest news

About the product

CrowdStrike Falcon Pro is a security package for business networks. Details of the management console described here are applicable to all supported operating systems (macOS, Windows and Linux). Falcon allows you to proactively look for malicious activities and adversaries (nation state, eCrime, or hacktivist actors). The cloud-based management console can be run from the cloud on any modern browser.

Verdict

CrowdStrike Falcon Pro is a very comprehensive platform. It provides not only AV services within an organisation, but also a comprehensive set of detection and analysis services. We note that CrowdStrike Falcon is available as a fully managed service for organisations that desire a more hands-off solution to endpoint protection. Otherwise, it is aimed at the larger organisation, and is not really a “fit and forget” product. Basic everyday monitoring and management tasks are simple enough, even with minimal understanding of its operations. However, the product’s capabilities are sufficiently deep that making some investment of time for learning is worthwhile to realize maximum value. CrowdStrike tell us that learning modules are available on-line or via external consultancy.

Getting up and running

The management infrastructure comes pre-packaged for you in a cloud console and requires no on-premises equipment – only a modern browser. Deployment of the client "sensor" (agent) is quite simple here. It relies on the download of the installation package appropriate to the target platform. On Windows, you can use an automatic sensor deployment like Windows System Center Configuration Manager. Once installed, the Falcon Sensor is almost invisible to the end user. Docker support allows the installation of the Falcon agent on hosts running Docker.

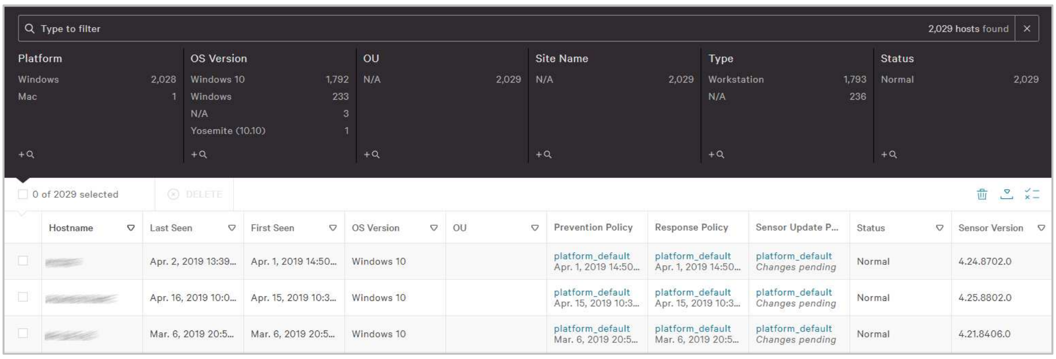
Deployment across an organisation will take planning and appropriate tools. This includes preparation for the appropriate layers of policy to be applied to users. Once this work has been done, deployment should be quite straightforward.

Everyday management

The management console is based in a web browser, as you would expect from a cloud-based solution. Two-factor authentication is required to log in, and support for single sign-on solutions is available. There is a menu of buttons down the left-hand side, and this menu can be expanded by clicking on the Falcon icon at the top left. The major items are *Activity*, *Investigate*, *Hosts*, *Configuration*, *Dashboards*, *Discover*, *Intelligence*, *Users*, and *Support*.

Activity is the first place to start work once the platform is up and running. There is a strong dashboard here, with the most important items brought into view. Good graphics show detections by scenario over the last 30 days, and you can click through here into the *Detections* submenu to view more detail. You get a strong reporting infrastructure, with a good choice of filter options presented front and centre here. You can also examine quarantined files and real-time response sessions here too.

The *Investigate* menu takes you into a comprehensive search facility. This covers hosts, hashes, users, IP addresses, domain and event searching. This is aimed at locating specific issues across the network estate in the recent history. The default is 24 hours, pre-set filters are provided up to 60 days, and customization options are available.



Type to filter 2,029 hosts found ×

Platform		OS Version		OU		Site Name		Type		Status	
Windows	2,028	Windows 10	1,792	N/A	2,029	N/A	2,029	Workstation	1,793	Normal	2,029
Mac	1	Windows	233					N/A	236		
		N/A	3								
		Yosemite (10.10)	1								

□ 0 of 2029 selected DELETE

	Hostname	Last Seen	First Seen	OS Version	OU	Prevention Policy	Response Policy	Sensor Update P...	Status	Sensor Version
□	[redacted]	Apr. 2, 2019 13:39...	Apr. 1, 2019 14:50...	Windows 10		platform_default Apr. 1, 2019 14:50...	platform_default Apr. 1, 2019 14:50...	platform_default *Changes pending*	Normal	4.24.8702.0
□	[redacted]	Apr. 16, 2019 10:0...	Apr. 15, 2019 10:3...	Windows 10		platform_default Apr. 15, 2019 10:3...	platform_default Apr. 15, 2019 10:3...	platform_default *Changes pending*	Normal	4.25.8802.0
□	[redacted]	Mar. 6, 2019 20:5...	Mar. 6, 2019 20:5...	Windows 10		platform_default Mar. 6, 2019 20:5...	platform_default Mar. 6, 2019 20:5...	platform_default *Changes pending*	Normal	4.21.8406.0

The *Hosts/Host Management* page, shown above, lists all the device installations, by version and platform. It provides immediate understanding of which devices are offline or disconnected. From here, you can go to the *Sensor Download* menu and download sensor installations for all the platforms.

The *Configuration* menu is the heart of the policy driven process within CrowdStrike Falcon. From here, you create policy definitions which cover all aspects of the AV and prevention processes of the platform. And then you apply that process to groups of installations. You can have different policies for Windows, Mac and Linux clients here too.

The *Dashboards* menu gives access to the executive summary view of the estate. There are detailed graphics for detections by scenario and severity, and identifications of the top 10 users, hosts and files with most detections. This is just the tip of a very deep iceberg, allowing for comprehensive analysis of what is happening. You can search by almost anything, and use this to discover what has happened on the network during an outbreak. This includes where something entered, how it attempted to execute, what processes it used, and how it was contained. Getting through this is not for the fainthearted, but it cannot be denied that you have very powerful set of audit and analysis tools here.

The *Discover* menu allows you to discover devices, users and applications on the network. You can search by application inventory, asset, MAC address, accounts and other app/process-based inventory. You can also review user account information including domain accounts, local accounts and their password reset status.

The *Intelligence* menu takes you into an overview of the current landscape threat as perceived by CrowdStrike. This can be categorised by different factors. Examples include geographical origin of threat, target industry, target country, and motivation (espionage/criminal/Hactivist and destruction). Each threat is detailed by these parameters. Clicking *View Profile* on the threat takes you to a comprehensive analysis and explanation of that specific threat. This is a comprehensive resource, which is unusual and most welcome.

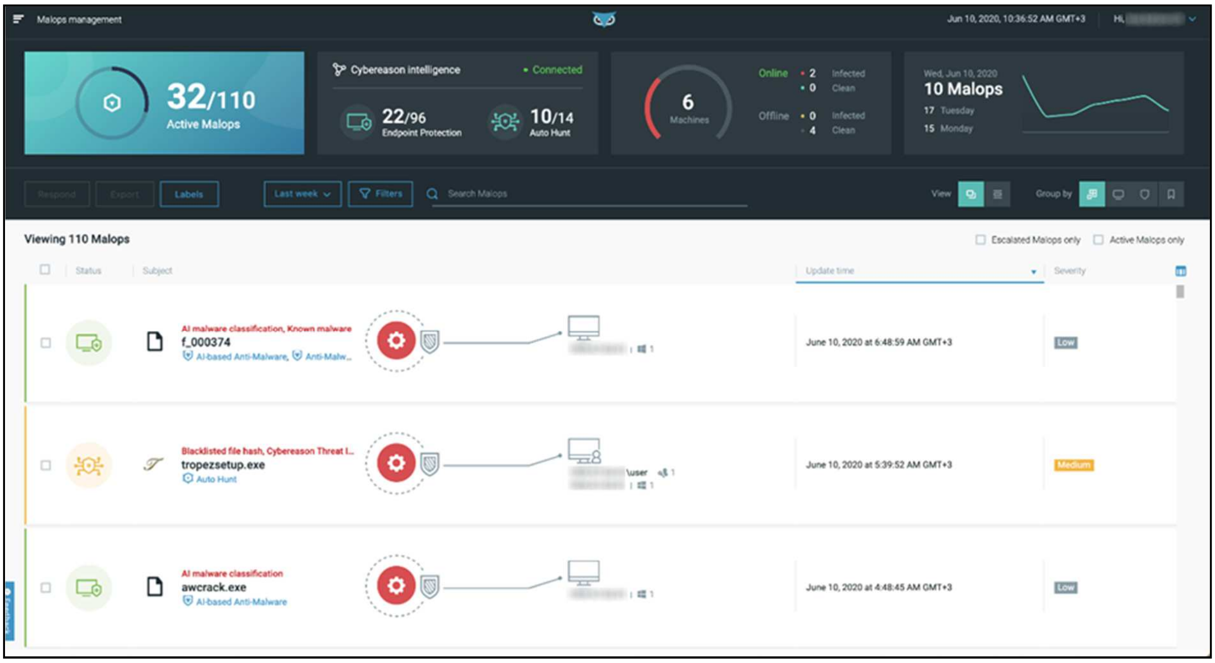
The *User* menu allows you to create the usual user profiles for administrators and other activities within the platform. There are pre-built roles already created for *Endpoint Manager*, *Event Viewer*, *Administrator*, *Analyst*, *Investigator*, *Real Time Responder*, and others. You can map these roles onto existing internal working structures, or to custom-build new roles as required.

The *CrowdStrike Store* allows you to extend the capabilities of the Falcon platform with a host of ready-to-go partner apps and add-ons.

Endpoint protection software

On the end-user client, the default setting is to have the client completely invisible to the user. No alerts or user interface are shown. In our test, we found that malware copied to the test system was immediately detected and deleted on access.

Cybereason Defense Platform Enterprise



32/110 Active Malops

Cybereason intelligence • Connected

22/96 Endpoint Protection

10/14 Auto Hunt

6 Machines

Online • 2 Infected • 0 Clean

Offline • 0 Infected • 4 Clean

Wed, Jun 10, 2020 10 Malops

17 Tuesday

15 Monday

Viewing 110 Malops

□ Escalated Malops only □ Active Malops only

□	Status	Subject		Update time	Severity
□		AI malware classification, Known malware f_000374 AI-based Anti-Malware, Anti-Malw...	[redacted] 1	June 10, 2020 at 6:48:59 AM GMT+3	Low
□		Blacklisted file hash, Cybereason Threat I... tropezsetup.exe Auto Hunt	[redacted]\user 1 [redacted] 1	June 10, 2020 at 5:39:52 AM GMT+3	Medium
□		AI malware classification awcrack.exe AI-based Anti-Malware	[redacted] 1	June 10, 2020 at 4:48:45 AM GMT+3	Low

Verdict

Cybereason's management console is easily navigated from a single menu. We were impressed with the clear, well-illustrated way in which information is laid out, particularly the Malops Inbox and Malops detail pages. Amongst other advantages, this would make the console very comfortable to use on a tablet. The ultra-simple and fast client deployment process means that even inexperienced administrators would have no difficulty getting the product up and running. We noted that the product's real-time protection is highly sensitive, and detected malware instantly in our functionality test.

About the product

Cybereason Defense Platform Enterprise uses a cloud-based console to manage endpoint protection software for Windows, macOS, Linux, Android and iOS devices.

Getting up and running

The endpoint agent can be installed by downloading the setup file from the console and running it. There is a *Download Cybereason Installers* button on the *System\Overview* page of the console. A slide-out menu lets you choose one of four OS versions: Windows, macOS, Linux or Linux Ubuntu. Once the installer file has been downloaded and executed, setup takes a single click, and completes in seconds.

Everyday management

The console is navigated from the menu in the top left-hand corner. The default *Discovery board*, shown in the screenshot above, 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 console). If you click on a dot, a pop-up box displays the name of the file/process, 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 threat, with an abundance of information about the Malop in question. This includes the device, user, 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 a remarkably effective way of communicating the important information quickly and easily. Actions that can be taken from the details page include *Investigate, Isolate* and *Respond*.

The *Malop inbox* 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. Clicking on one of the Malops opens its details page, as described in the paragraph above.

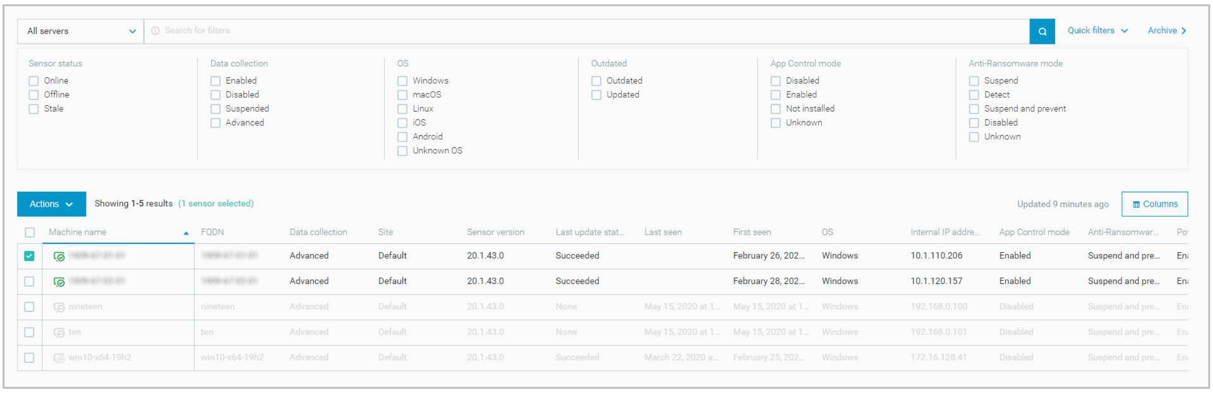
Malware alerts shows items that “need your attention”. These are given names like “vaultfile12009845677446252183.vol”, based on the system’s internal quarantine naming process. For each item, there are *Investigate* and *Exclude* buttons.

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*.

On the *Security profile* page, you can adjust reputation criteria, create custom rules for detection and behavioural whitelisting, and manage machine isolation exceptions.

The main *System* page has a number of sub-pages. These are *Overview, Sensors, Policies management* and *Detection servers*. The default *Overview* page is divided into 5 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, services and performance, with the latter displaying a graph of the processing rate over time.

The *System\Sensors* page is shown below. It 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 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.



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

Anti-Ransomware mode
- □ Suspend
- □ Detect
- □ Suspend and prevent
- □ Disabled
- □ Unknown

Showing 1-5 results (1 sensor selected)

Updated 9 minutes ago

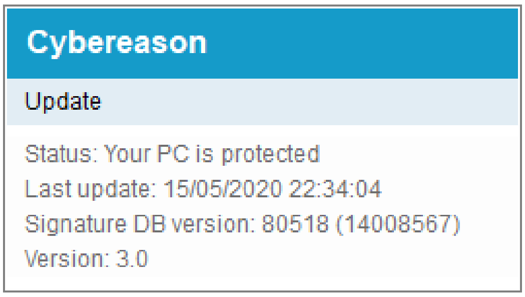
□	Machine name	FQDN	Data collection	Site	Sensor version	Last update stat...	Last seen	First seen	OS	Internal IP addre...	App Control mode	Anti-Ransomwar...	Po
☑	[redacted]	[redacted]	Advanced	Default	20.1.43.0	Succeeded		February 26, 202...	Windows	10.1.110.206	Enabled	Suspend and pre...	En
□	[redacted]	[redacted]	Advanced	Default	20.1.43.0	Succeeded		February 28, 202...	Windows	10.1.120.157	Enabled	Suspend and pre...	En
□	nineteen	nineteen	Advanced	Default	20.1.43.0	None	May 15, 2020 at 1...	May 15, 2020 at 1...	Windows	192.168.0.100	Disabled	Suspend and pre...	En
□	ten	ten	Advanced	Default	20.1.43.0	None	May 15, 2020 at 1...	May 15, 2020 at 1...	Windows	192.168.0.101	Disabled	Suspend and pre...	En
□	win10-x64-19h2	win10-x64-19h2	Advanced	Default	20.1.43.0	Succeeded	March 22, 2020 a...	February 25, 202...	Windows	172.16.128.41	Disabled	Suspend and pre...	En

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. Items 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* lets you add and edit the details of the sites and servers that manage the protection software.

The *Settings* menu item lets you configure items such as notifications, authentication, and password policy. The product's support services can be accessed by clicking *Support*, as you would expect.

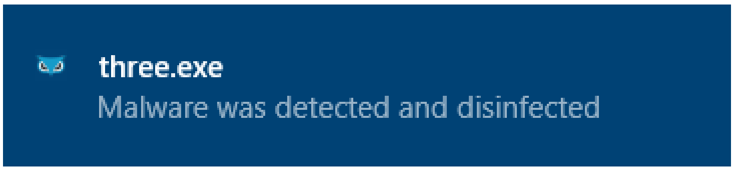
Windows endpoint protection software

There is a minimalist interface to the endpoint protection software. This consists of a System Tray icon, which shows a concise status display when right-clicked:



Status: Your PC is protected
Last update: 15/05/2020 22:34:04
Signature DB version: 80518 (14008567)
Version: 3.0

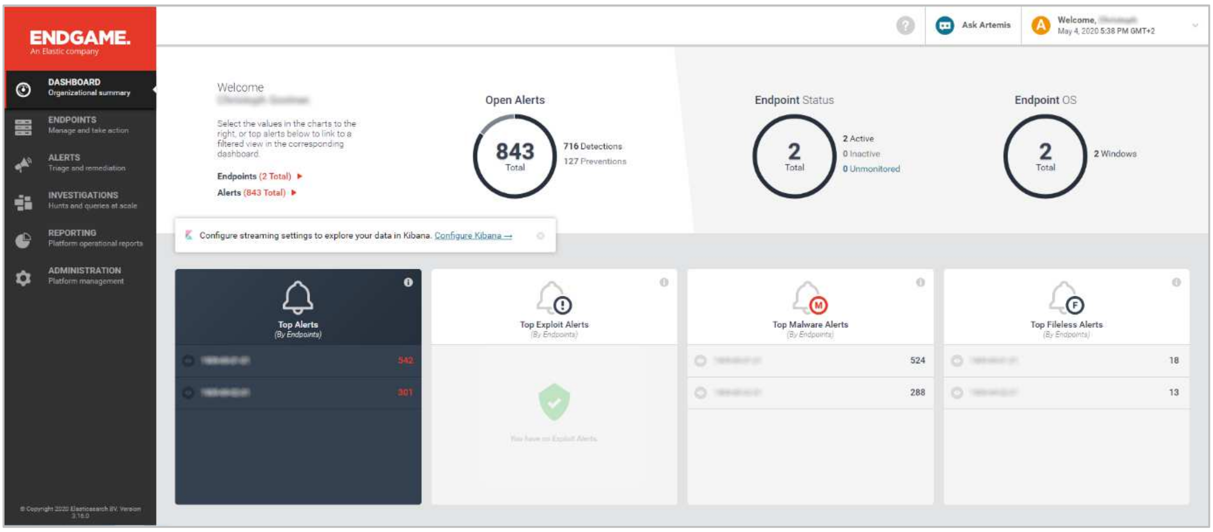
If a user should inadvertently copy a malicious program to their system, Cybereason will instantly detect and delete it. A sample alert is shown below:



three.exe
Malware was detected and disinfected

The interface of the server protection software is identical to that of its client counterpart.

Elastic Endpoint Security



Select the values in the charts to the right, or top alerts below to link to a filtered view in the corresponding dashboard.

Configure streaming settings to explore your data in Kibana.

Verdict

Elastic Endpoint Security is aimed at larger organizations that require prevention and EDR capabilities. Deploying it will require some planning and training, meaning that it is not a solution that you can just install and forget about. However, for larger organisations with suitable resources, it provides a comprehensive range of features.

About the product

Elastic Endpoint Security provides prevention, detection and response measures. It has threat-hunting capabilities aimed at stopping targeted attacks. The management console can be run from the cloud on any modern browser. On-premises deployment is also an option. Elastic Endpoint Security supports Windows, Linux, Mac, and Solaris clients and servers.

Getting up and running

We used Elastic Endpoint Security's cloud-based infrastructure. This simply requires you to browse to the URL and log in to the management console. Deployment of the client "sensor" (agent) can be done in one of two ways: "in-band" and "out-of-band".

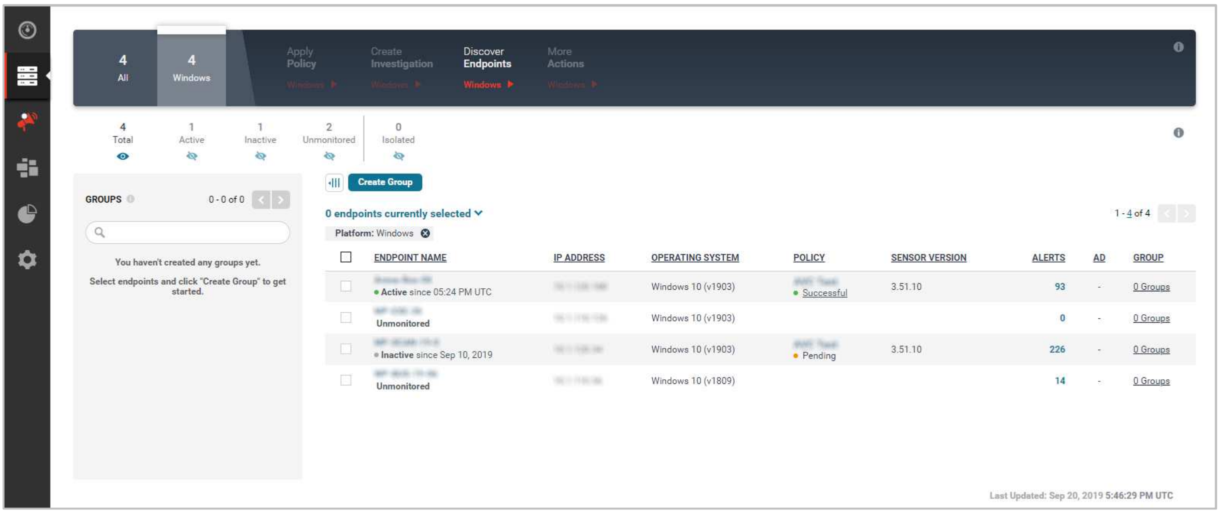
In-band is currently only for Windows. The administrator installs the sensor directly onto Windows clients or servers from the Elastic Endpoint Security management console. The administrator can scan the network for unmonitored endpoints and install the sensor after entering credentials for that endpoint.

Out-of-band is supported for all operating systems. Out-of-band installation lets you deploy the sensor using a management tool such as Microsoft System Centre Configuration Manager. You can also install manually after downloading an installation package from the *Administration/Sensor* page.

The installer is transferred by the administrator to an endpoint and run from an elevated command-prompt window. You have to use specific command-line syntax (in the documentation) to do this. Double-clicking the .exe file simply deletes it.

Everyday management

The management console has six menu choices on the left-hand side. *Dashboard* gives an overview of the status of the entire estate of client devices, and reports how many alerts are in play at any one time. It also displays top alerts, exploits, malware and file-less alerts, allowing for a comprehensive view of what is happening. Each of these can be clicked through to drill into more information.



You haven't created any groups yet.

Select endpoints and click "Create Group" to get started.

0 endpoints currently selected

Platform: Windows

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

Last Updated: Sep 20, 2019 5:46:29 PM UTC

The *Endpoints* page (shown above) gives a view of all the managed clients. You can select and sort by name, IP address, OS version, policy applied, sensor version, alerts and groups. From here, you can choose a range of endpoints and then run tasks on them. These include applying a new policy, deploying/upgrading/uninstalling/deleting endpoints, and configuring a response when threats are encountered.

Alerts takes you into the heart of the platform. Here you get a list of current event types such as malicious file execution prevention or file detection. The catalogue of events can be sorted and categorised by event type, assignee, OS, IP address, hostname and date.

If you click on an event, it takes you to the *Alert Details* page for that event. 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. Here you can choose *Take Action*, whereby the options include *Download Alert, Resolve, Dismiss, Start Investigation, Isolate Host, Download File, Delete File* and *Whitelist Items*.

Of particular interest here is the *Start Investigation* feature which lets you create a "Hunt". A Hunt can cover multiple information sources, e.g. firewall rules, drivers, network, persistence, process, registry, media, or system configuration. It allows you to search the network for information relevant to your enquiry. A key component here is the "Ask Artemis" feature, which is a natural-language query engine. You can simply type in a question, and Artemis will attempt to resolve it.

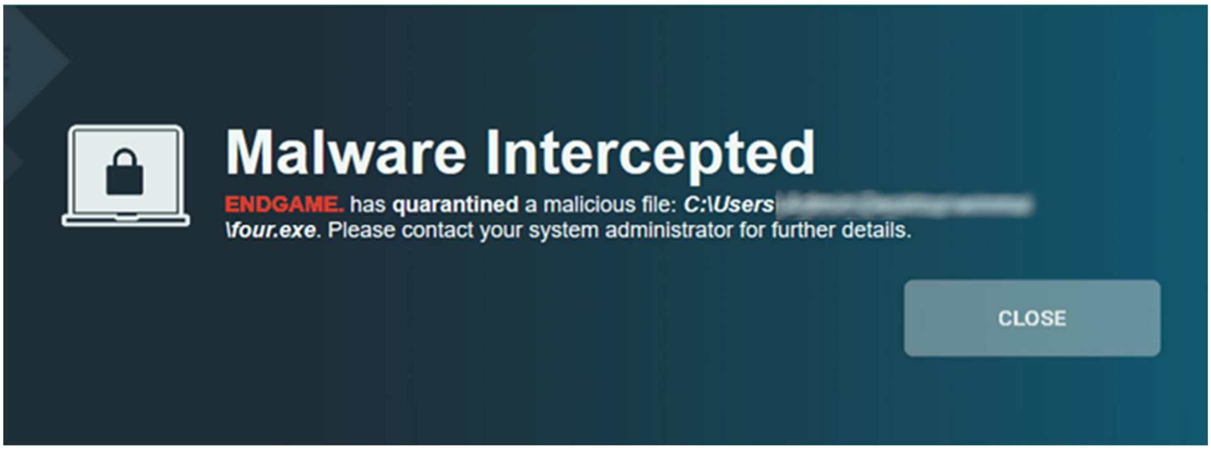
The *Investigations* menu item shows a list of ongoing investigations, who is assigned to them, which endpoints are involved, and so forth. This is very important for understanding how the current analysis is progressing.

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

Finally, the *Administration* menu item gives access to the *Policy Settings, Users, Sensors, Alerts, Whitelist* and *Platform* features. The *Policy Settings* page lets you define policy for events such as privilege escalation, process injection, and credential access. As an example, you can choose what policy to apply when malware is executed. Do you detect or prevent it? Do you allow self-injection or detect DLL injection and so forth? This is a level of power and control that goes significantly beyond normal antivirus.

Windows endpoint protection software

The Windows desktop protection software is essentially invisible to the user. If the user should inadvertently copy a malicious file to the system, Elastic will detect and quarantine it on access. An example alert is shown below. This takes the form of a banner running across the screen. The user cannot take any action, other than to close the alert.

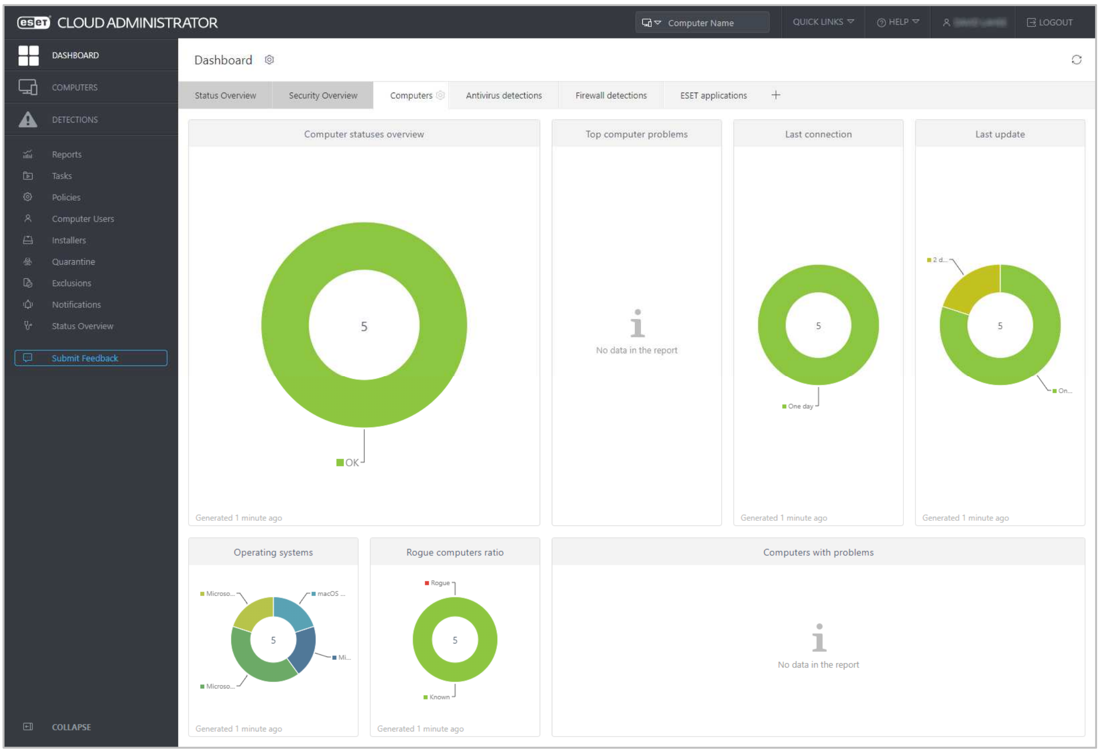


Malware Intercepted

ENDGAME. has **quarantined** a malicious file: *C:\Users*[redacted]*\four.exe*. Please contact your system administrator for further details.

The GUI of the server protection software is identical to that of its desktop counterpart.

ESET Endpoint Protection Advanced Cloud with ESET Cloud Administrator



Verdict

The ESET Endpoint Protection Advanced Cloud package is very well suited to the SME market. ESET have made it very flexible and scalable. It is simple enough for a company of 25 users, but also sophisticated enough to cope with larger networks. You can get the console operational in no time, and its simple menu structure makes it very easy to navigate. We found the interface very intuitive, and were able to deploy and manage the client software without any difficulty. The ability to customise different elements of the console is very welcome. We also noticed that the console is very responsive when it comes to showing alerts. Overall, it provides a very attractive option for small to medium-sized businesses.

About the product

As its name suggests, ESET Endpoint Protection Advanced Cloud includes a cloud-based management console. There is endpoint protection software for Windows clients, Windows file servers, and macOS clients. For the Windows and macOS clients, you get the choice of Endpoint Antivirus or Endpoint Security; the latter includes a web control feature and ESET's Network Protection module. The licence also allows you to install unmanaged protection for Linux and Android devices.

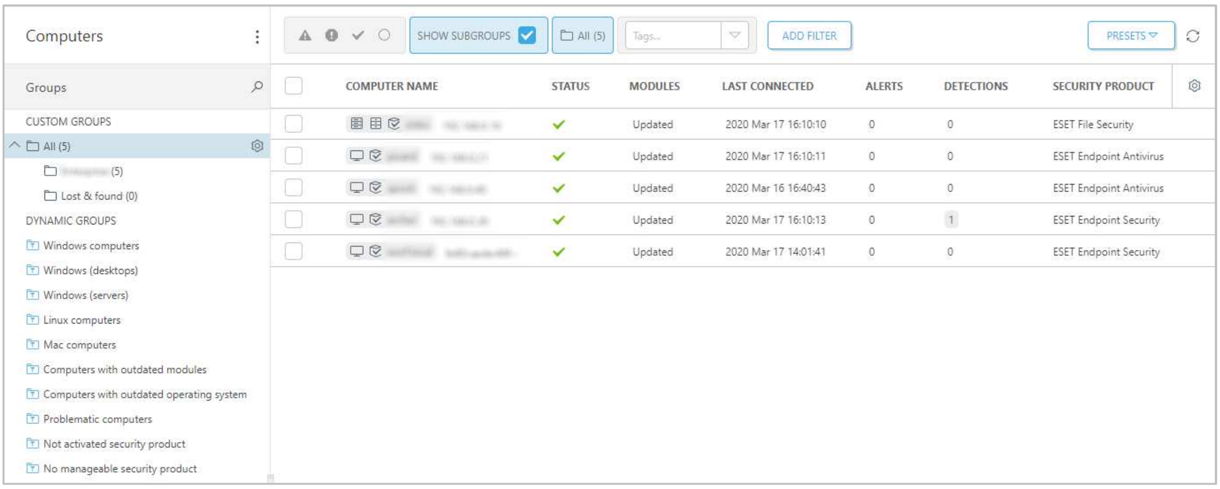
Getting up and running

As the console is cloud-based, there is no installation required. You just open the URL and enter your credentials. When you log on for the first time, you can choose the location (country) of the datacentre to be used. There is also a recommendation to set up two-factor authentication, but this is optional. Next, the startup wizard invites you to create installation packages. Naturally, you can cancel this and come back to the task later. After the wizard has been completed, a tutorial runs. This is very short and simple, and points out the main areas of the console interface.

To install the client software, you first need to create installation packages on the *Installers* page. This just requires you to select a product. You can enable or disable the PUA detection and ESET Live Grid feedback options, or get the wizard to prompt for these during installation. Language, Group and Policy can also be specified. Once you have made an installer, you can send it to users by email directly from the console. Alternatively, you can download it and distribute it via network share or removable device, or use the mass deployment tool. When you run the installer on a target computer, the setup wizard lets you choose the interface language. Otherwise there are no choices to make, and installation completes with a couple of clicks. It is also possible to install the ESET Management Agent via a Microsoft Active Directory or System Center Configuration Manager script, and then push the endpoint software from the console. This choice of deployment methods means that the product would work well for both smaller and larger networks.

Everyday management

You can find all the main functions of the console in a single menu column on the left-hand side. 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. The time of last connection and last update are also shown, as is the distribution of different operating systems. 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 zoom in on antivirus or firewall threats, ESET applications, and incidents.



□	COMPUTER NAME	STATUS	MODULES	LAST CONNECTED	ALERTS	DETECTIONS	SECURITY PRODUCT
□	[redacted]	✓	Updated	2020 Mar 17 16:10:10	0	0	ESET File Security
□	[redacted]	✓	Updated	2020 Mar 17 16:10:11	0	0	ESET Endpoint Antivirus
□	[redacted]	✓	Updated	2020 Mar 16 16:40:43	0	0	ESET Endpoint Antivirus
□	[redacted]	✓	Updated	2020 Mar 17 16:10:13	0	1	ESET Endpoint Security
□	[redacted]	✓	Updated	2020 Mar 17 14:01:41	0	0	ESET Endpoint Security

The *Computers* page is shown above. It gives you an overview of all the managed devices on the network; you can click on a computer's entry to get more detailed information about that device. This includes a detailed hardware inventory, amongst other things. You can also organise computers into groups, and carry out tasks such as scans and updates. 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.

The *Detections* page shows information about all threats encountered by all managed devices on the network. You can click on the entry for any threat to get details such as file hash, source URL and detection mechanism.

Reports provides a wide range of preconfigured scenarios such as *Active Threats* and *Last Scan*. Running a report on one of these is as simple as clicking its tile on the page. You can also create your own report scenarios if you want. Reports can be scheduled, and you can specify the language.

Tasks allows you to take a wide variety of actions on individual devices or 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 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. You can also create your own custom policies if you want.

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

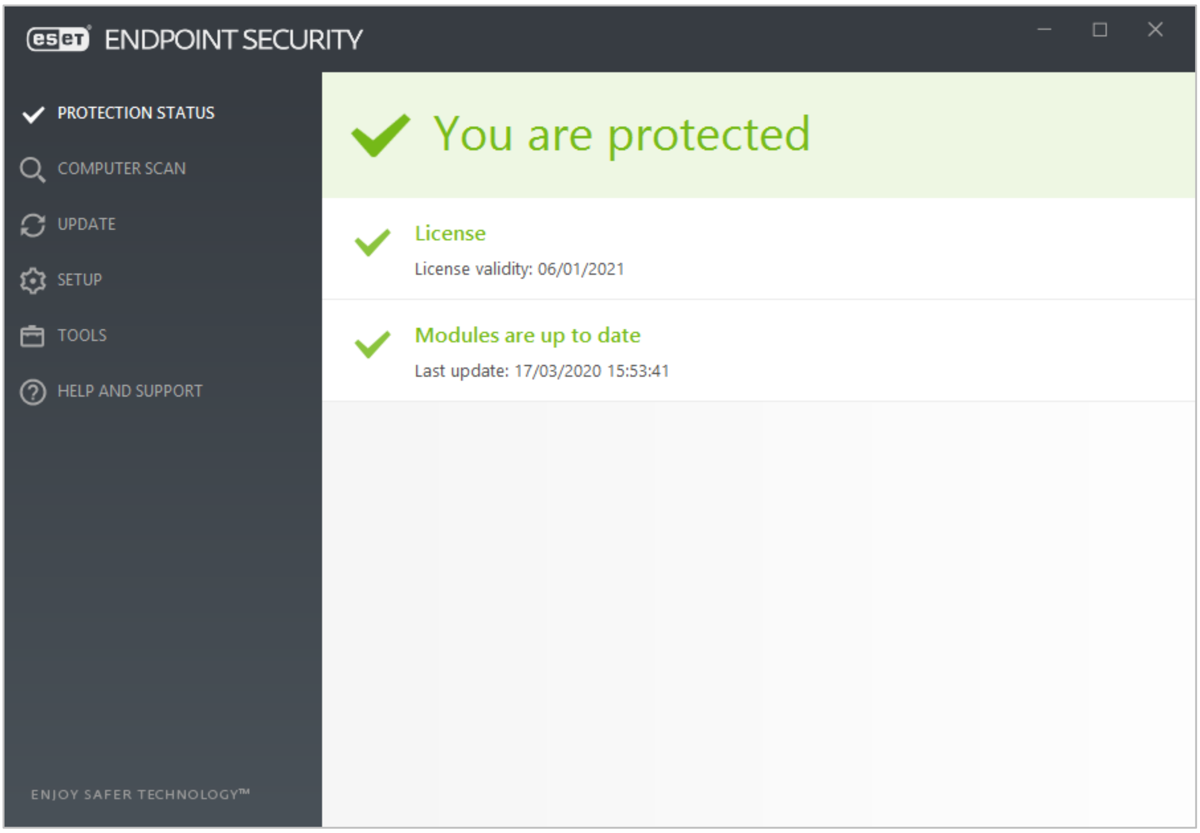
On the *Quarantine* page, you can see all quarantined files, along with useful details such as the hash, detection type (Trojan, PUA, test file), and number of computers affected.

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

Notifications lets you receive email notifications for a number of different scenarios. These include threats being detected, and endpoint software being out of date. 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.

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 any issues that cannot be resolved automatically, and require the attention of the administrator.

Windows endpoint protection client



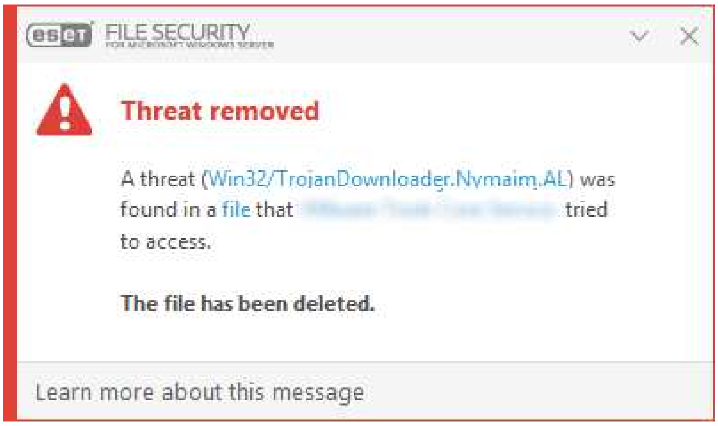
✓ You are protected

✓ License
License validity: 06/01/2021

✓ Modules are up to date
Last update: 17/03/2020 15:53:41

By default, users can access a fully-featured endpoint protection client. This has very similar functionality to a consumer antivirus program. The GUI is a model of simple and clean design. All the features are easily accessible from a single menu on the left-hand side of the window. Users can run updates and scans, and see logs and quarantined files. However, Windows Standard Users cannot disable protection or restore items from quarantine. If you want, you can set a policy from the console to disable the GUI on any device or group; in this case, no interface will be visible to the user.

If the user should inadvertently copy a malicious file to the system, ESET will detect and quarantine the malware on access. An example alert is shown below. The user cannot take any action, and the alert closes after a few seconds.



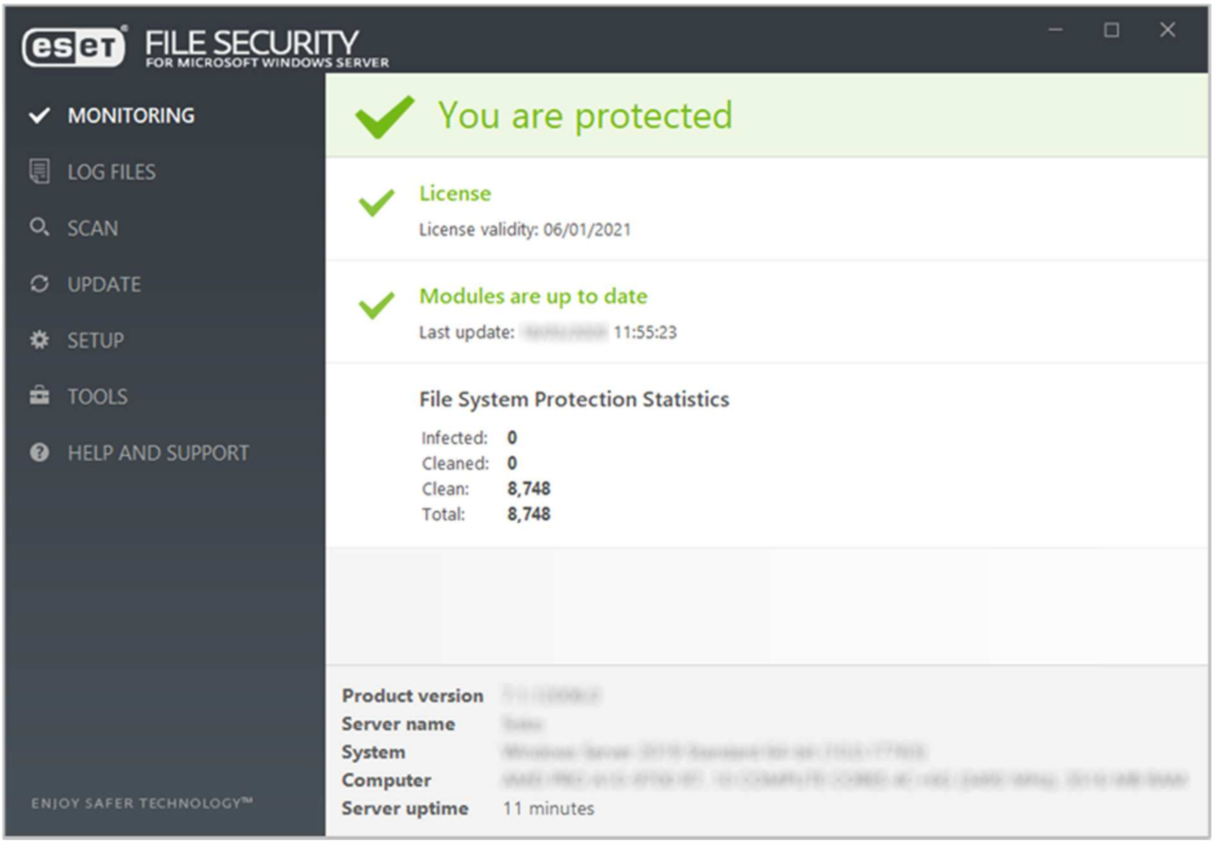
Threat removed

A threat (Win32/TrojanDownloader.Nymaim.AL) was found in a file that [redacted] tried to access.

The file has been deleted.

Learn more about this message

The GUI of the server protection software is very similar to its desktop counterpart. However, additional system information is provided on the home page. The Log Files feature also has its own entry in the menu column.



You are protected

License

License validity: 06/01/2021

Modules are up to date

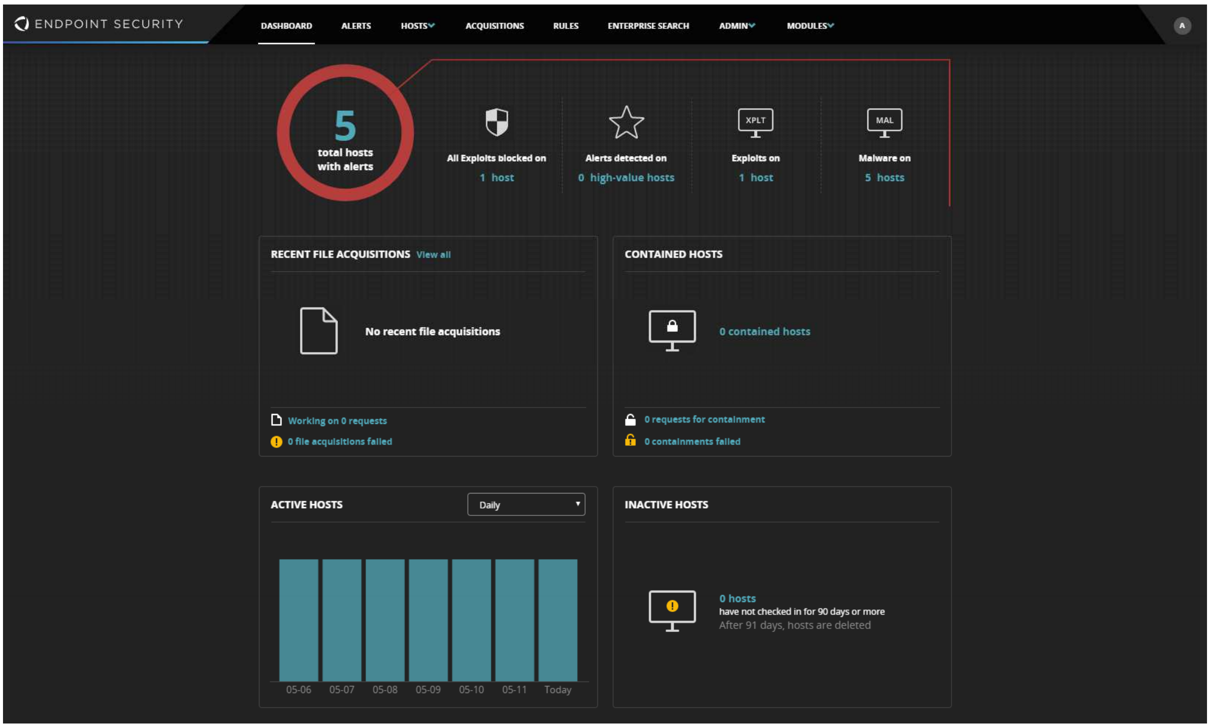
Last update: [redacted] 11:55:23

File System Protection Statistics

Infected: 0
Cleaned: 0
Clean: 8,748
Total: 8,748

Product version [redacted]
Server name [redacted]
System [redacted]
Computer [redacted]
Server uptime 11 minutes

FireEye Endpoint Security



5 total hosts with alerts

All Exploits blocked on 1 host

Alerts detected on 0 high-value hosts

Exploits on 1 host

Malware on 5 hosts

RECENT FILE ACQUISITIONS View all

No recent file acquisitions

Working on 0 requests

0 file acquisitions failed

CONTAINED HOSTS

0 contained hosts

0 requests for containment

0 containments failed

ACTIVE HOSTS Daily

INACTIVE HOSTS

0 hosts
have not checked in for 90 days or more
After 91 days, hosts are deleted

Verdict

FireEye Endpoint Security is a highly powerful platform. It includes signature-based, behavioural and machine-learning engines. A core strength is in the acquisition of data from the agent for analysis and subsequent decision-making process. This allows the admin to hunt down and investigate any threats that might bypass initial detection.

This deep insight enables analysis and response across the largest of enterprises. There is however a significant entry cost in terms of training. This is required for both the initial configuration and ongoing operations. To get the most out of FireEye Endpoint Security, security operations teams should have some knowledge of investigations. Alternatively, FireEye can assist with their Managed Defence practice. However, it should deliver a level of insight and operational management which is at the bleeding edge.

About the product

FireEye Endpoint Security provides endpoint protection with detection and response. There is a cloud-based management console. The product is designed to handle the largest of organizations, with support for up to 100,000 endpoints per appliance. There are agents available for Windows clients and servers, macOS, and various Linux distributions.

Getting up and running

The cloud console requires no significant installation. Client installers can be downloaded from the *Admin* menu/*Agent Versions* page, and deployed onto the client machines.

The management console is quite different from a conventional centralised AV product. The emphasis is on detection and response. This involves acquisition of data from clients, analysis of it, and then responding appropriately.

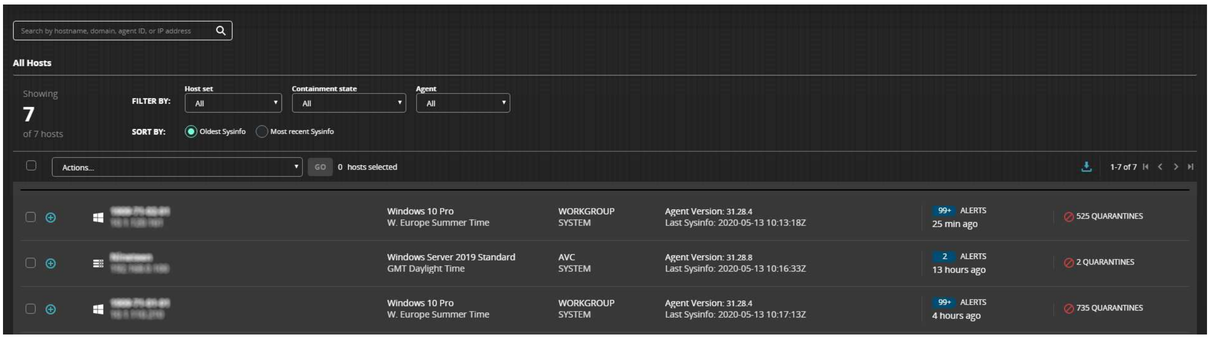
The platform has an extremely powerful and extensive set of information gathering tools. These allow you to build comprehensive queries of almost any type. These are then dispatched to the clients. Analysing this information is the core of the server product.

You could treat FireEye as a straightforward AV package, allowing the engines to process malware as it is found. However, the real strength comes in the analysis and containment capabilities.

There is little work required to configure the platform once the agents are deployed. Of course, you can build custom policies if you wish. But it is likely that global default settings will be the bedrock of the deployment.

There isn't much in the way of handholding in the initial setup process for the smaller organisation. Clearly the product is aimed at the more professional, larger organisation. It also assumes there will be training and consultancy for deployment.

Everyday management



Search by hostname, domain, agent ID, or IP address

All Hosts

Showing 7 of 7 hosts

FILTER BY: Host set: All; Containment state: All; Agent: All

SORT BY: ● Oldest Sysinfo ○ Most recent Sysinfo

□ Actions... GO 0 hosts selected

1-7 of 7

□	[redacted]	Windows 10 Pro W. Europe Summer Time	WORKGROUP SYSTEM	Agent Version: 31.28.4 Last Sysinfo: 2020-05-13 10:13:18Z	99+ ALERTS 25 min ago	525 QUARANTINES
□	[redacted]	Windows Server 2019 Standard GMT Daylight Time	AVC SYSTEM	Agent Version: 31.28.8 Last Sysinfo: 2020-05-13 10:16:33Z	2 ALERTS 13 hours ago	2 QUARANTINES
□	[redacted]	Windows 10 Pro W. Europe Summer Time	WORKGROUP SYSTEM	Agent Version: 31.28.4 Last Sysinfo: 2020-05-13 10:17:13Z	99+ ALERTS 4 hours ago	735 QUARANTINES

The management console is not a tool to be dipped into occasionally. Unlocking its huge power needs considerable understanding of what the platform offers and how to achieve it. There is little handholding here. The product is aimed squarely at the large corporate space, where training and consultancy will be provided. From that point of view, this is not a product for the SME space.

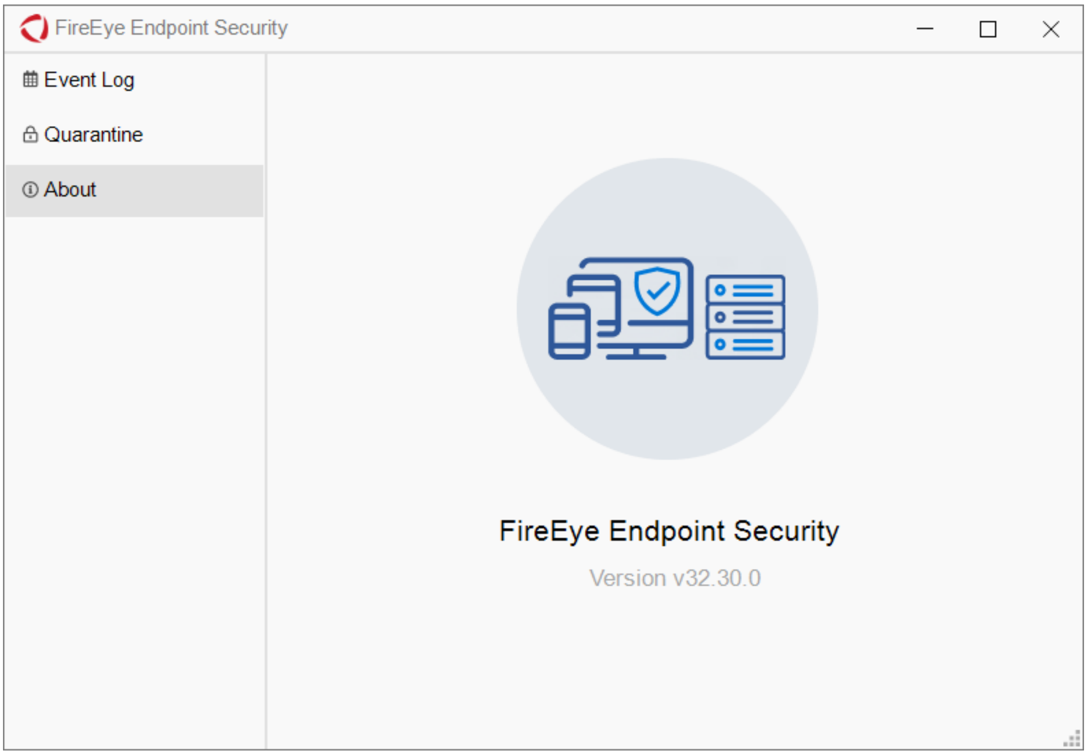
Firstly, you need to understand what FireEye is trying to achieve. It relies on threat detection, plus data gathering and analysis. The emphasis here is solidly on information acquisition, analysis and reporting. This allows the administrator to gather information from a wide array of client machines. The information can then be processed, allowing you to take actions based upon it.

There is a basic front-page overview of the status of the deployed agents. This allows you to drill down into more detail. As an ongoing view, this is probably sufficient. The power comes once you drill into the *Hosts*, *Enterprise Search*, *Acquisitions* and *Rules* sections. The essential component here is building search routines to find what you are looking for. You can request containment of the device. This locks out the user whilst informing them of the centralised management control. You can then to dig through what is happening. This ability to lock out a device is a key component of the handling of a widespread malware event.

It should not be underestimated how much technical and systems knowledge is required to get the best from this. This is not a criticism. Indeed, for a hard-core IT administrator, it is a great strength to have access to this level of query and analysis of the network.

Windows endpoint protection software

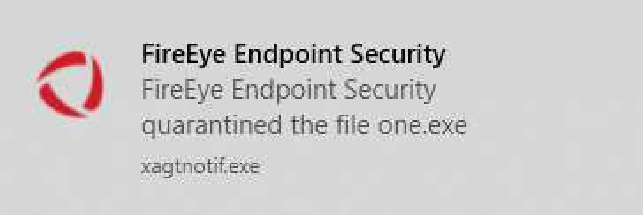
The Windows desktop protection software displays a System Tray icon, from which a program window can be opened. This lets you see the event log and quarantined items.



FireEye Endpoint Security

Version v32.30.0

If the user should inadvertently copy a malicious file to their system, FireEye will detect and quarantine it on access. An example alert is shown below. The user cannot take any action, and the alert closes after a few seconds.

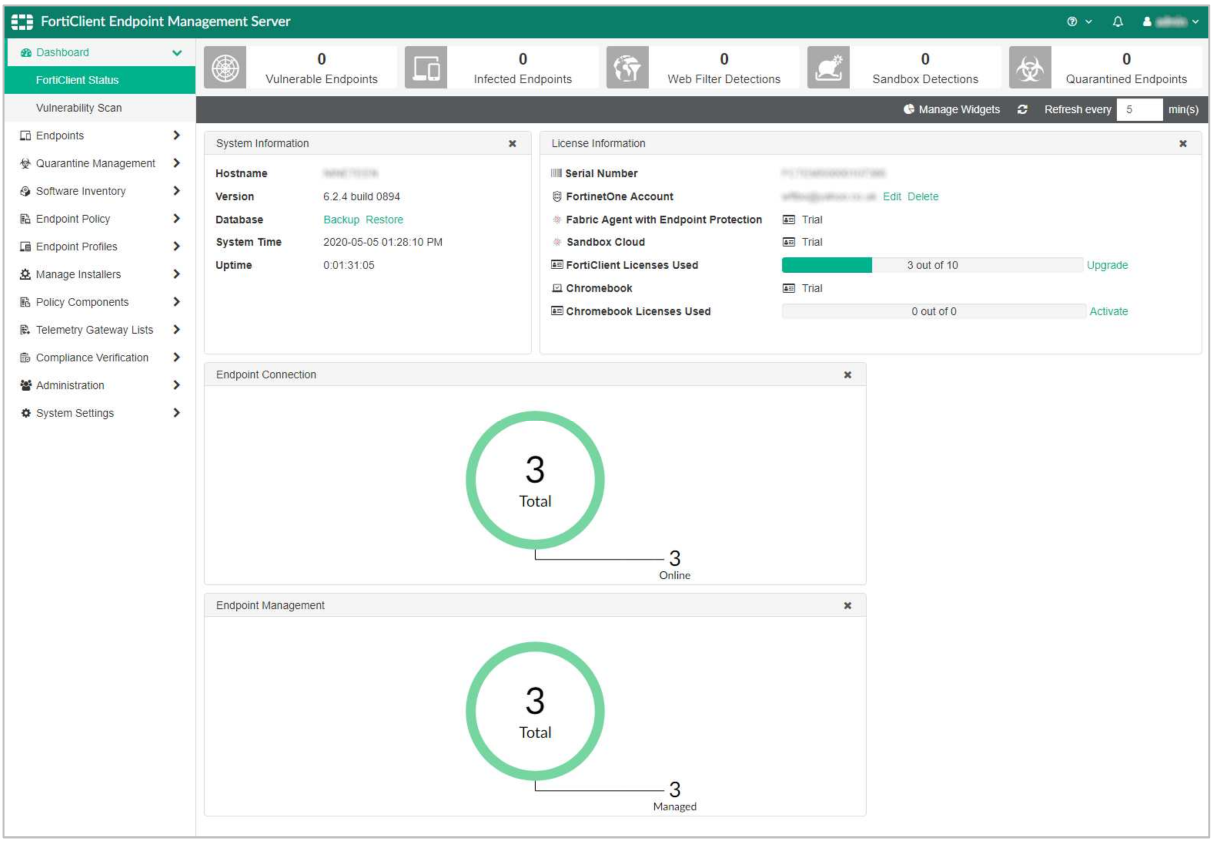


FireEye Endpoint Security

FireEye Endpoint Security quarantined the file one.exe

xagtnotif.exe

Fortinet FortiClient with EMS, FortiSandbox and FortiEDR



0	Vulnerable Endpoints
0	Infected Endpoints
0	Web Filter Detections
0	Sandbox Detections
0	Quarantined Endpoints

System Information

Hostname	[redacted]
Version	6.2.4 build 0894
Database	Backup Restore
System Time	2020-05-05 01:28:10 PM
Uptime	0:01:31:05

License Information

Serial Number	[redacted]	
FortinetOne Account	[redacted] Edit Delete	
Fabric Agent with Endpoint Protection	Trial	
Sandbox Cloud	Trial	
FortiClient Licenses Used	3 out of 10	Upgrade
Chromebook	Trial	
Chromebook Licenses Used	0 out of 0	Activate

Endpoint Connection

3 Total

3 Online

Endpoint Management

3 Total

3 Managed

Verdict

The Fortinet Enterprise Management Server package is a strong product. It is probably aimed at larger organisations. It is straightforward to deploy, but would benefit from more handholding for the smaller organisation. There is some welcome graphical reporting, but more help could be given to dig through the status of the network. The day-to-day operation would benefit from training time to get the most out of the product.

About the product

The server-based console is called FortiClient Endpoint Management Server (EMS), and the client is called FortiClient. The console requires a Windows Server OS (2008 R2) or later. There is endpoint protection software for Windows clients and servers, Mac OS X and Linux. Please note that as well as anti-malware functions, the product includes other features such as telemetry and secure remote access. These are not covered by this review, however.

Getting up and running

EMS is a local server-based product. Installing the management console is very simple and requires almost no user interaction, although you may have to restart the server during installation. The console functionality can be accessed from the desktop shortcut (dedicated window), or a web browser. Once up and running, there are some tasks you need to perform before the client can be deployed. The real-time protection feature of the endpoint protection software is disabled in the default policy. However, it is very simple to switch it on under *Endpoint Profiles/Default*.

You can then deploy the client to the desktop. Under *Manage Installers/Deployment Packages* you can create an installer 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. Setup is very quick and easy, and the client connects to the management server automatically. On the server side, there are good reports for devices discovered that are not part of the management structure, and it is easy to remediate this. There is a clear and clean view of the status of the network through the *Dashboard/FortiClient Status* view.

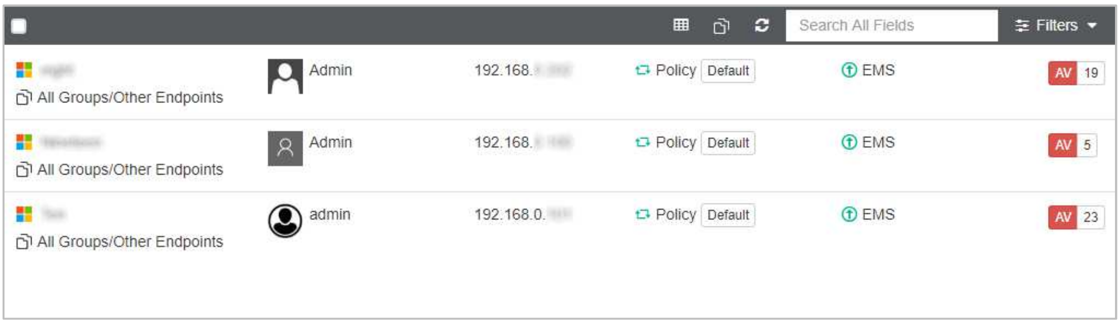
Creating users for the management console is fairly easy. A user can be assigned granular permissions. These include creation, update and deleting of various settings, and the abilities to manage endpoints. Finally, you can assign permissions for policy management here too. So, you can create a relatively fine-grained set of permissions here for various administrative levels.

There isn't much in the way of handholding in the initial setup process for the smaller company. Clearly the product is aimed at larger organisations, with training and consultancy provided.

Everyday management

The Enterprise Management Server console has a fairly clear UI. It definitely benefits from a larger screen. There is a single menu down the left-hand side. Clicking an item here populates the right-hand side of the window. The *Dashboard/FortiClient Status* page provides a graphical overview of the platform and client status. You can click through from the items to get more data, but it is not always clear what detail has been uncovered. For example, taking our "2 infected endpoints", we click through and get a view of the two devices. But again, there is little here to tell me what is actually wrong with these devices. More clarity here would help when dealing with problems and outbreaks.

The *Vulnerability Scan* page has an interesting set of "traffic light" views. These go from green (low) through yellow (medium) to orange (high) and red (critical). Underneath this is a set of buttons selecting what is being reported. For example, operating system, browser, MS Office and Services are shown. Moving the mouse over these buttons causes a graphical refresh of the traffic lights. However, it is not clear what the data means until you actually click on a button. This is a useful interface that is slightly compromised by its implementation.



[redacted] All Groups/Other Endpoints	Admin	192.168.[redacted]	Policy Default	EMS	AV 19
[redacted] All Groups/Other Endpoints	Admin	192.168.[redacted]	Policy Default	EMS	AV 5
[redacted] All Groups/Other Endpoints	admin	192.168.0.[redacted]	Policy Default	EMS	AV 23

The *Endpoints* page (shown above) allows you to look at the status of all endpoints. There is an attempt to be graphical here, but some of the icons could be clearer in their meaning.

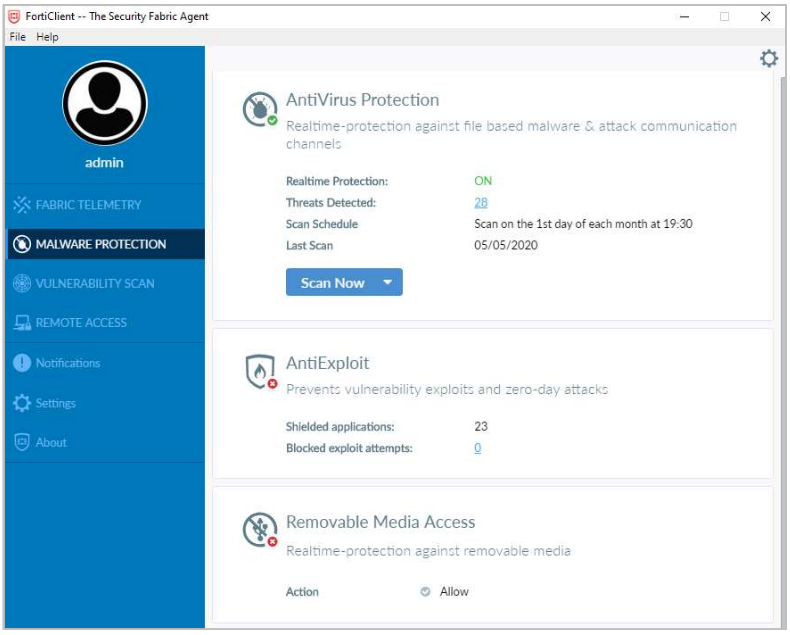
Endpoint Profiles lets you build up the policy to be pushed to a user's computer. It is quite straightforward and obvious what needs to be done here. There is a *Basic/Advanced* view button which is helpful if you want to dig into the details, or stay with a more simplified view.

Finally, *Administration* and *System Settings* allow control of the underlying settings of the platform.

It is fairly straightforward to get reports of what is happening, and initiate scans or remedial actions as required. The UI is quite well designed, but would benefit from some final polish to make it more obvious. A stronger splitting of setup from day-to-day and from system administration would help too.

Windows endpoint protection software

The Windows desktop protection software provides a program window with status information. Users can run scans, but not change any settings.



AntiVirus Protection

Realtime-protection against file based malware & attack communication channels

Realtime Protection: ON
Threats Detected: 28
Scan Schedule Scan on the 1st day of each month at 19:30
Last Scan 05/05/2020

AntiExploit

Prevents vulnerability exploits and zero-day attacks

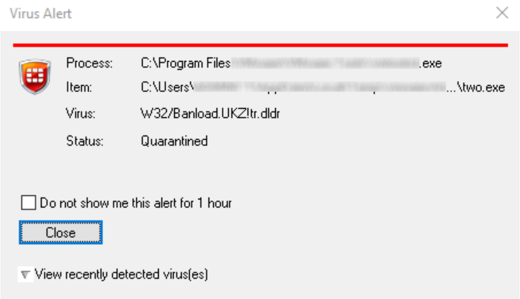
Shielded applications: 23
Blocked exploit attempts: 0

Removable Media Access

Realtime-protection against removable media

Action Allow

If a user should inadvertently copy a malicious file to the system, FortiClient will detect and quarantine it on access. An example alert is shown below. The user cannot take any action, other than to close the alert.



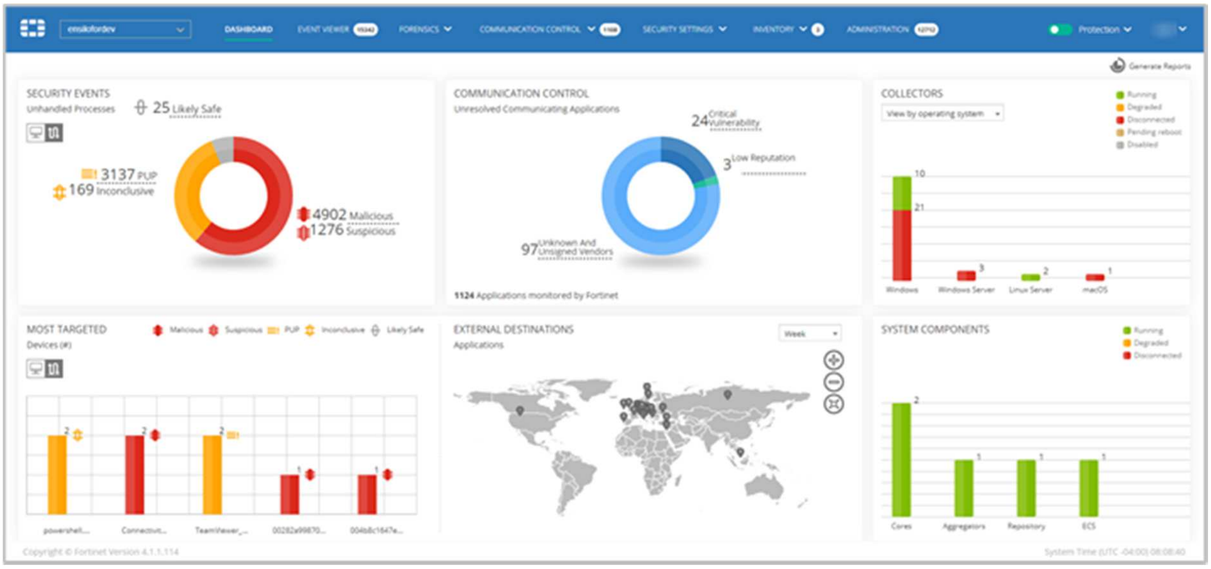
Process: C:\Program Files[redacted].exe
Item: C:\Users\[redacted]...\two.exe
Virus: W32/Banload.UKZ!tr.dldr
Status: Quarantined

□ Do not show me this alert for 1 hour

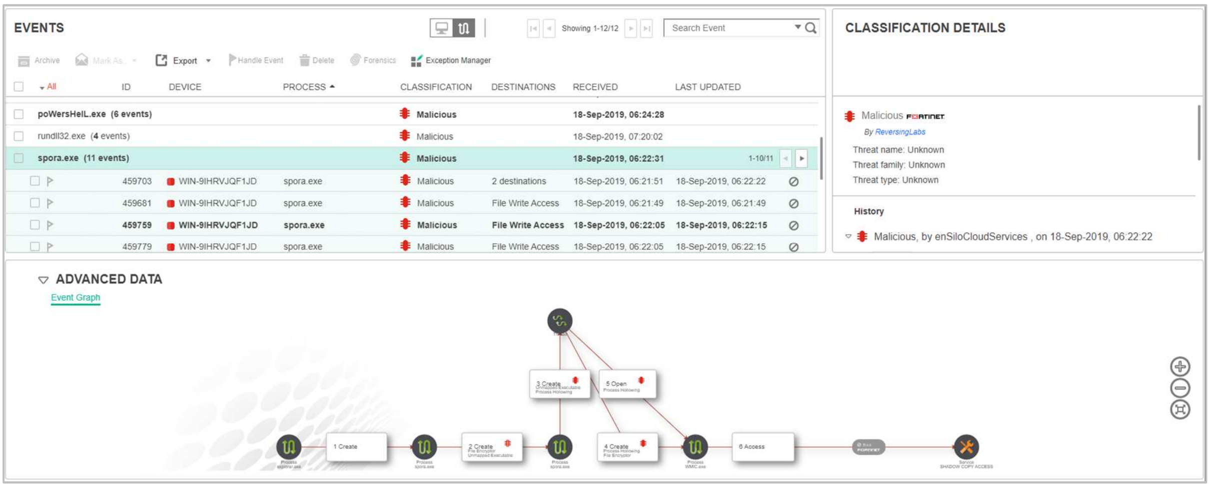
The GUI of the server protection software is identical to that of its desktop counterpart.

FortiEDR

The FortiEDR component of the package has a separate, cloud-based management console.



The *Dashboard* page, shown above, provides a graphical overview of threats and suspicious processes. *Event Viewer*, shown below, gives details of such processes, and allows you to take action by e.g. investigating or deleting them. 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.).



EVENTS

Showing 1-12/12 | Search Event

Archive | Mark As... | Export | Handle Event | Delete | Forensics | Exception Manager

□	All	ID	DEVICE	PROCESS	CLASSIFICATION	DESTINATIONS	RECEIVED	LAST UPDATED	
□	**poWersHelL.exe (6 events)**				**Malicious**		**18-Sep-2019, 06:24:28**		
□	rundll32.exe (4 events)				Malicious		18-Sep-2019, 07:20:02		
□	**spora.exe (11 events)**				**Malicious**		**18-Sep-2019, 06:22:31**	1-10/11	
□		459703	WIN-9IHRVJQF1JD	spora.exe	Malicious	2 destinations	18-Sep-2019, 06:21:51	18-Sep-2019, 06:22:22	⊘
□		459681	WIN-9IHRVJQF1JD	spora.exe	Malicious	File Write Access	18-Sep-2019, 06:21:49	18-Sep-2019, 06:21:49	⊘
□		**459759**	**WIN-9IHRVJQF1JD**	**spora.exe**	**Malicious**	**File Write Access**	**18-Sep-2019, 06:22:05**	**18-Sep-2019, 06:22:15**	⊘
□		459779	WIN-9IHRVJQF1JD	spora.exe	Malicious	File Write Access	18-Sep-2019, 06:22:05	18-Sep-2019, 06:22:15	⊘

CLASSIFICATION DETAILS

Malicious FORTINET
By ReversingLabs
Threat name: Unknown
Threat family: Unknown
Threat type: Unknown

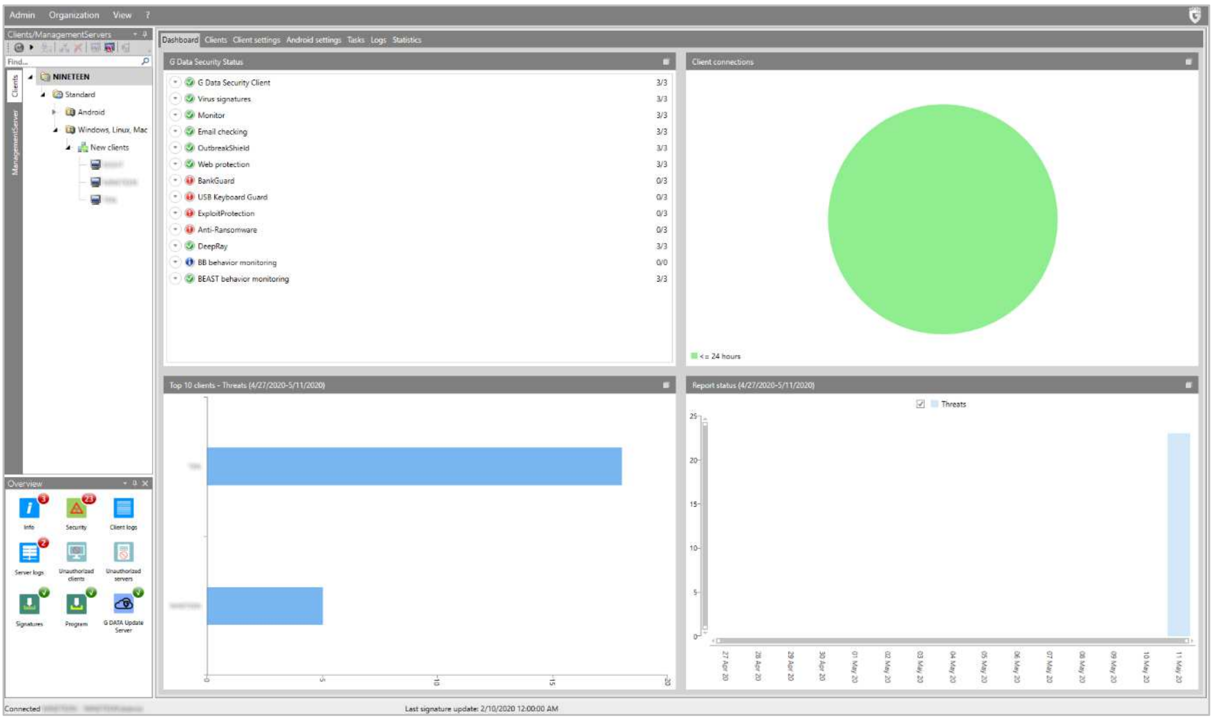
History

Malicious, by enSiloCloudServices , on 18-Sep-2019, 06:22:22

ADVANCED DATA

Event Graph

G DATA AntiVirus Business



G Data Security Status	
G Data Security Client	3/3
Virus signatures	3/3
Monitor	3/3
Email checking	3/3
OutbreakShield	3/3
Web protection	3/3
BankGuard	0/3
USB Keyboard Guard	0/3
ExploitProtection	0/3
Anti-Ransomware	0/3
DeepRay	3/3
BB behavior monitoring	0/0
BEAST behavior monitoring	3/3

Connected

Last signature update: 2/10/2020 12:00:00 AM

Verdict

G DATA AntiVirus Business provides a sophisticated, server-based management console. It could be used to manage larger networks with multiple servers. It offers a wide range of functions, in a design similar to the Microsoft Management Console in Windows. It may appear slightly dated, and a little exploration may be needed to find all the functions. Nonetheless, professional system administrators should have no difficulty finding their way around it. There is some scope for customising the types of information displayed, which we liked. The endpoint protection software has a minimalist interface. However, admins can let users carry out simple everyday tasks such as updates and scans.

About the product

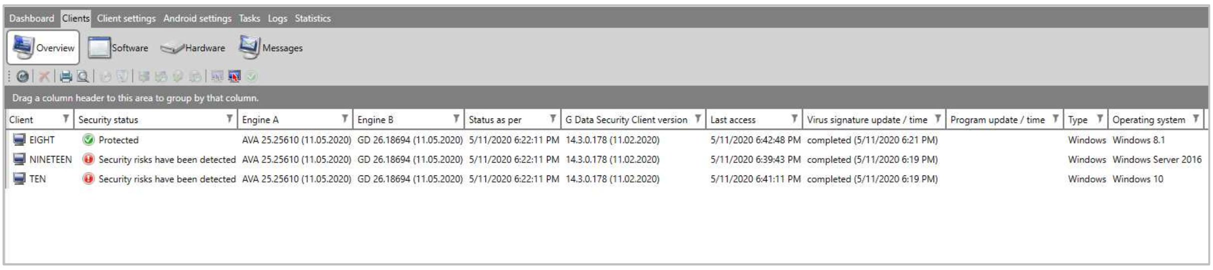
G Data uses a server-based console to manage endpoint protection software for Windows, Linux, Mac, iOS and Android devices.

Getting up and running

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. We note that you may need to adjust Windows Firewall settings on the server and clients to enable communication between them, however. When the console is first used, a deployment wizard runs, allowing you to push the endpoint software to clients over the network. Alternatively, you can run the installer on individual client devices. To connect the client to the server, just need to enter the latter’s IP address.

Everyday management

The panel in the top left-hand corner of the console displays the management server(s) in use. Here you can switch between different servers if you have more than one. For each server, 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.



Drag a column header to this area to group by that column.

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	Operating system
EIGHT	✓ Protected	AVA 25.25610 (11.05.2020)	GD 26.18694 (11.05.2020)	5/11/2020 6:22:11 PM	14.3.0.178 (11.02.2020)	5/11/2020 6:42:48 PM	completed (5/11/2020 6:21 PM)		Windows	Windows 8.1
NINETEEN	! Security risks have been detected	AVA 25.25610 (11.05.2020)	GD 26.18694 (11.05.2020)	5/11/2020 6:22:11 PM	14.3.0.178 (11.02.2020)	5/11/2020 6:39:43 PM	completed (5/11/2020 6:19 PM)		Windows	Windows Server 2016
TEN	! Security risks have been detected	AVA 25.25610 (11.05.2020)	GD 26.18694 (11.05.2020)	5/11/2020 6:22:11 PM	14.3.0.178 (11.02.2020)	5/11/2020 6:41:11 PM	completed (5/11/2020 6:19 PM)		Windows	Windows 10

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. From the row of buttons along the top, you can run various tasks. These include installing or uninstalling client software, updating the definitions and software, and deleting devices. 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.

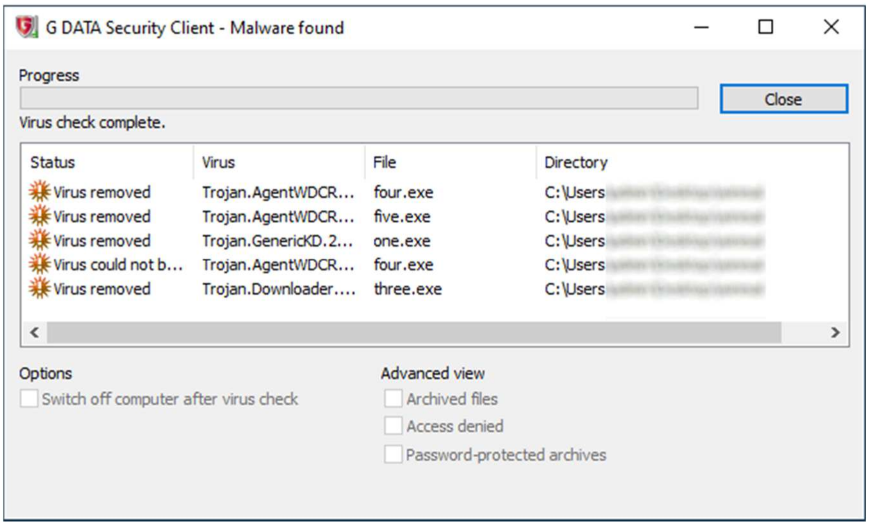
The *Client settings* pages lets you configure some options such as automatic signature and program updates. You can also allow users a degree of interaction with the endpoint software on their PCs. For example, you could let them run scans and/or display the local quarantine.

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 lists malware detections. Details provided are status, date and time, affected device, file name, threat name, and location. *Info* displays information relating to the anti-spam functionality. 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 software

By default, the endpoint protection client has a minimalist user interface. There is a System Tray icon. This lets you run an update, and display details of the program version and current signatures. As mentioned above, you can change settings from the console to allow users to run scans, if you want. This adds a variety of scan options to the System Tray menu. It also adds a *Scan for viruses (G Data Antivirus)* item to Windows Explorer's right-click context menu. If a user should inadvertently copy a malicious file to their system, G Data will detect and quarantine it on access. A sample alert is shown below:



G DATA Security Client - Malware found

Progress

Virus check complete.

Status	Virus	File	Directory
Virus removed	Trojan.AgentWDCR…	four.exe	C:\Users[redacted]
Virus removed	Trojan.AgentWDCR…	five.exe	C:\Users[redacted]
Virus removed	Trojan.GenericKD.2…	one.exe	C:\Users[redacted]
Virus could not b…	Trojan.AgentWDCR…	four.exe	C:\Users[redacted]
Virus removed	Trojan.Downloader.…	three.exe	C:\Users[redacted]

Options

□ Switch off computer after virus check

Advanced view

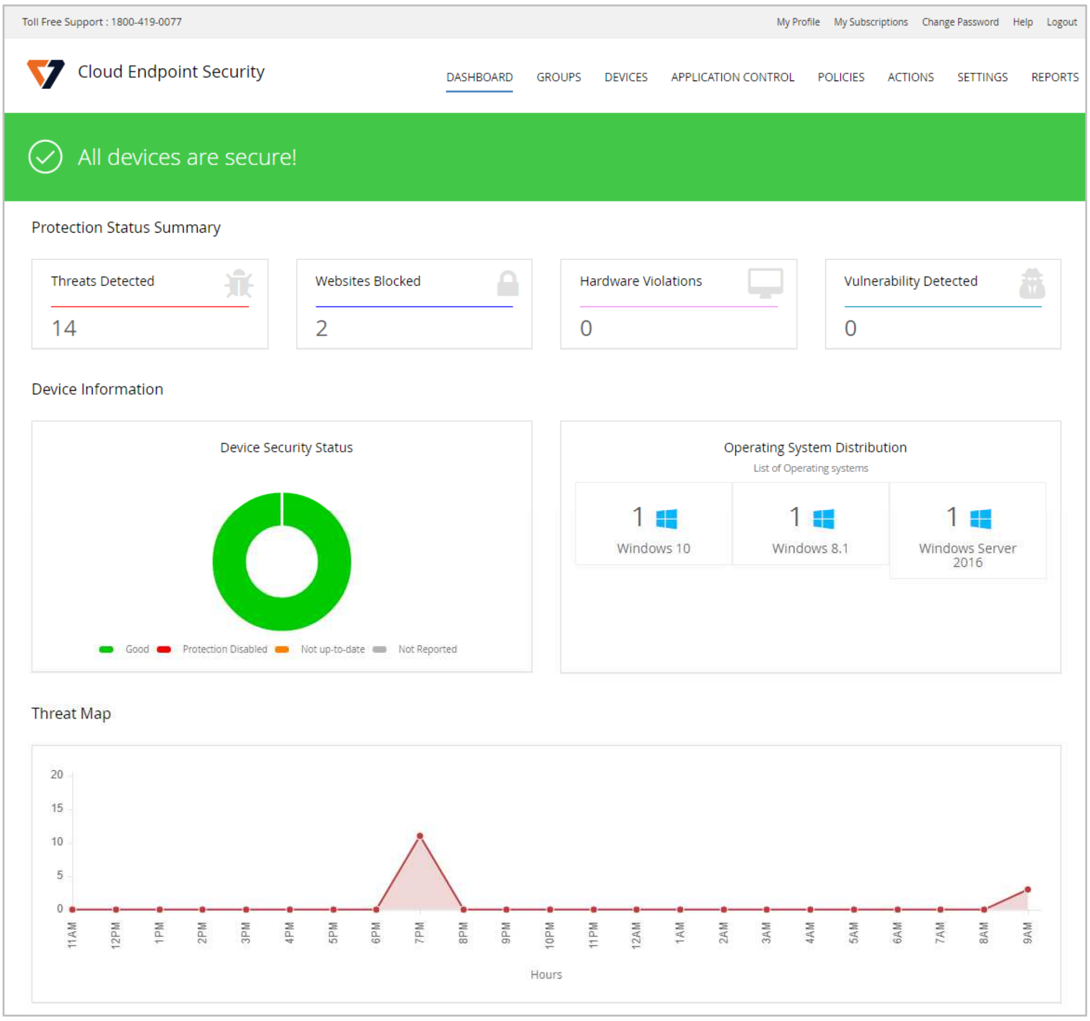
□ Archived files

□ Access denied

□ Password-protected archives

The interface and options for the server protection software are exactly the same as for the client.

K7 Cloud Endpoint Security



All devices are secure!

Protection Status Summary

Threats Detected	Websites Blocked	Hardware Violations	Vulnerability Detected
14	2	0	0

Device Information

Operating System Distribution

List of Operating systems

1	1	1
Windows 10	Windows 8.1	Windows Server 2016

Threat Map

Verdict

K7 Cloud Endpoint Security is designed for enterprises of all sizes, but its ease of use makes it particularly suitable for smaller businesses and less-experienced administrators. It is very quick and straightforward to set up, due to the cloud-based console and very simple installation process. The management console is very easy to navigate, and the endpoint client lets users carry out scans and updates very simply. One minor suggestion for improvement would be a means of selecting multiple devices at once on the *Devices* page. However, overall it is very straightforward and intuitive to use.

About the product

K7 Cloud Endpoint Security uses a cloud-based administration console to manage endpoint protection software for Windows clients and servers.

Getting up and running

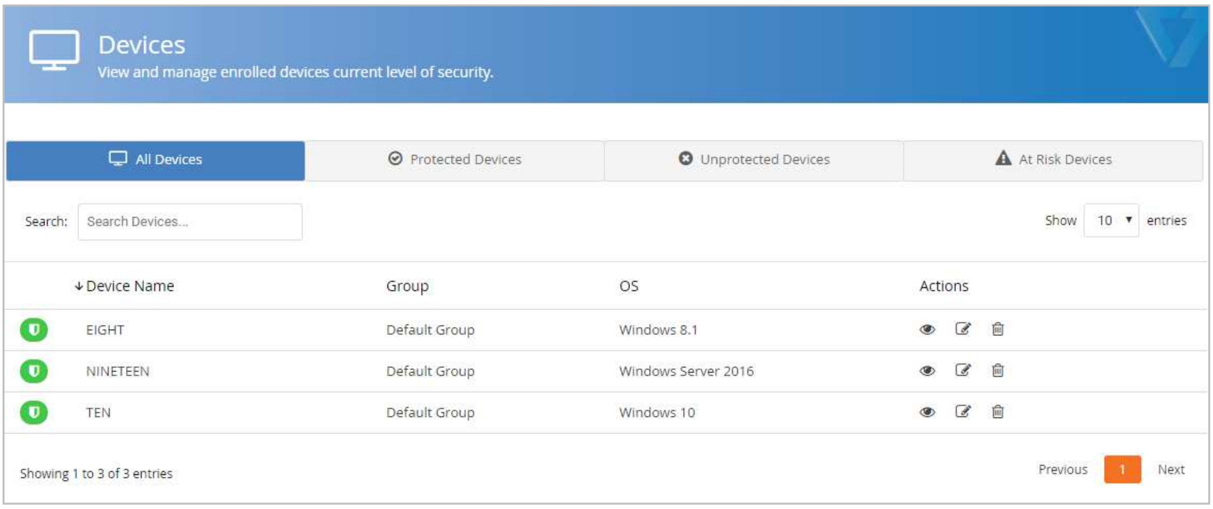
As the console is cloud-based, no installation is necessary. When you log on for the first time, a help page is displayed, with concise explanations of the features and how to use them. Deploying endpoint protection software is almost as simple. All you need to do is go to the *Settings* page and download an installation package, then run this. The setup wizard is very simple, with no choices to be made. Thus, you can install the client with just a couple of clicks.

Everyday management

All the console's functionality can be accessed from a single menu strip at the top of the window. When you log in, 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.

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 you can apply to all group members.

The *Devices* page, shown in the screenshot below, 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. For the latter two tasks, means of selecting multiple devices at once would be helpful. Currently you can only select one device at a time.



Devices
View and manage enrolled devices current level of security.

Device Name	Group	OS	Actions
EIGHT	Default Group	Windows 8.1	
NINETEEN	Default Group	Windows Server 2016	
TEN	Default Group	Windows 10	

Showing 1 to 3 of 3 entries

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 selecting *Block from Running, Block Internet Access* or *Block Network Access* from 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.

The *Policies* page lets you control settings for the endpoint software. These are conveniently ordered into groups such as *Anti-Virus, Behaviour Protection, Firewall, Web Filtering* and *Device Control*.

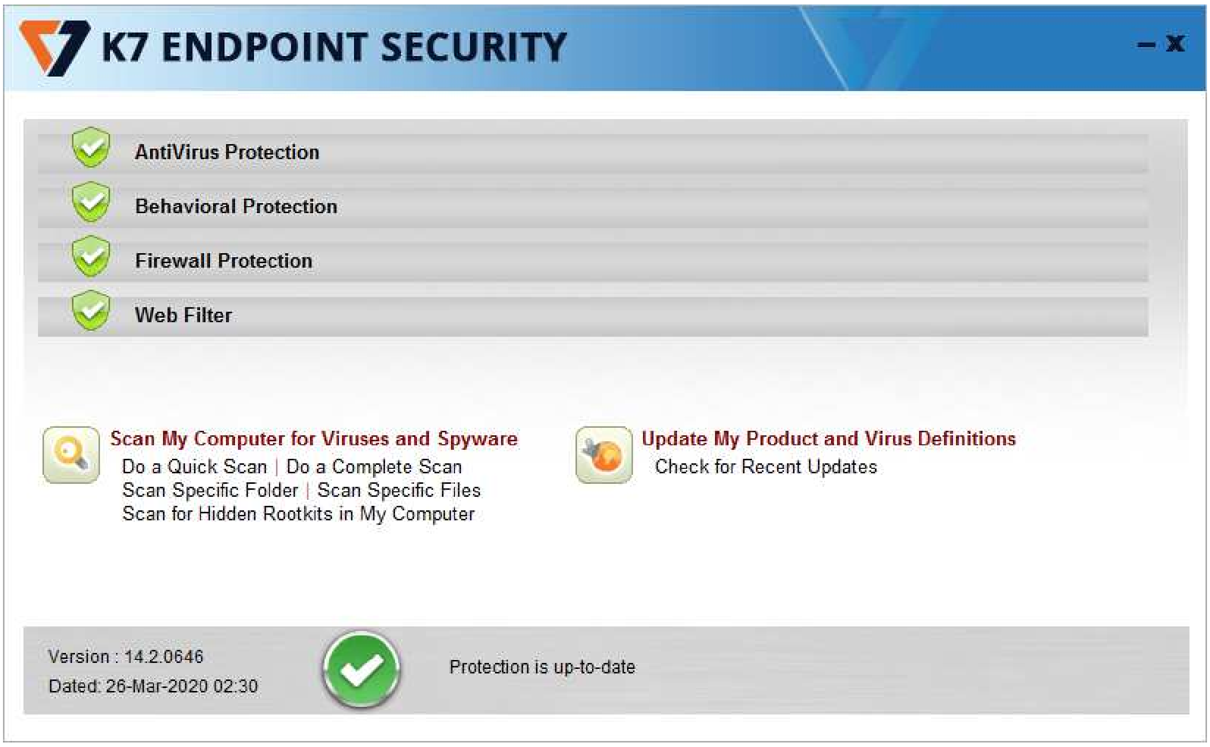
Under *Actions* you can create tasks to run on individual computers or groups. Available tasks include a variety of scans and a client update.

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

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 software

The Windows desktop protection software has a window with a component status display. This lets users run definition updates and a wide variety of scans. However, no settings are accessible to the user by default. This can be changed by the administrator in the policy, if so desired.


K7 ENDPOINT SECURITY

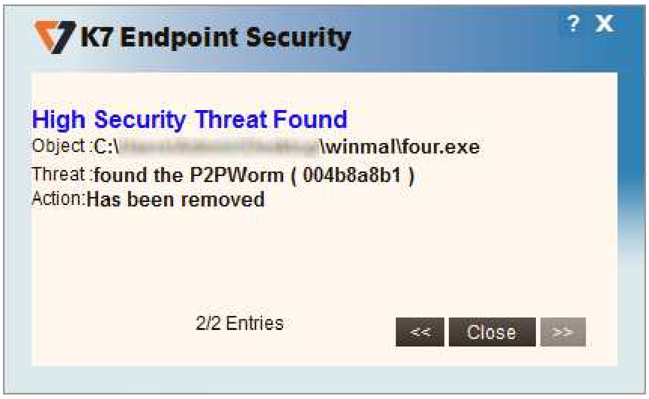
✓ AntiVirus Protection
✓ Behavioral Protection
✓ Firewall Protection
✓ Web Filter

Scan My Computer for Viruses and Spyware
Do a Quick Scan | Do a Complete Scan
Scan Specific Folder | Scan Specific Files
Scan for Hidden Rootkits in My Computer

Update My Product and Virus Definitions
Check for Recent Updates

Version : 14.2.0646
Dated: 26-Mar-2020 02:30
Protection is up-to-date

Should the user inadvertently try to copy malware to the system, K7 will detect it on access, and delete it. An example alert is shown below. The user cannot take any action, and the alert closes after a few seconds.

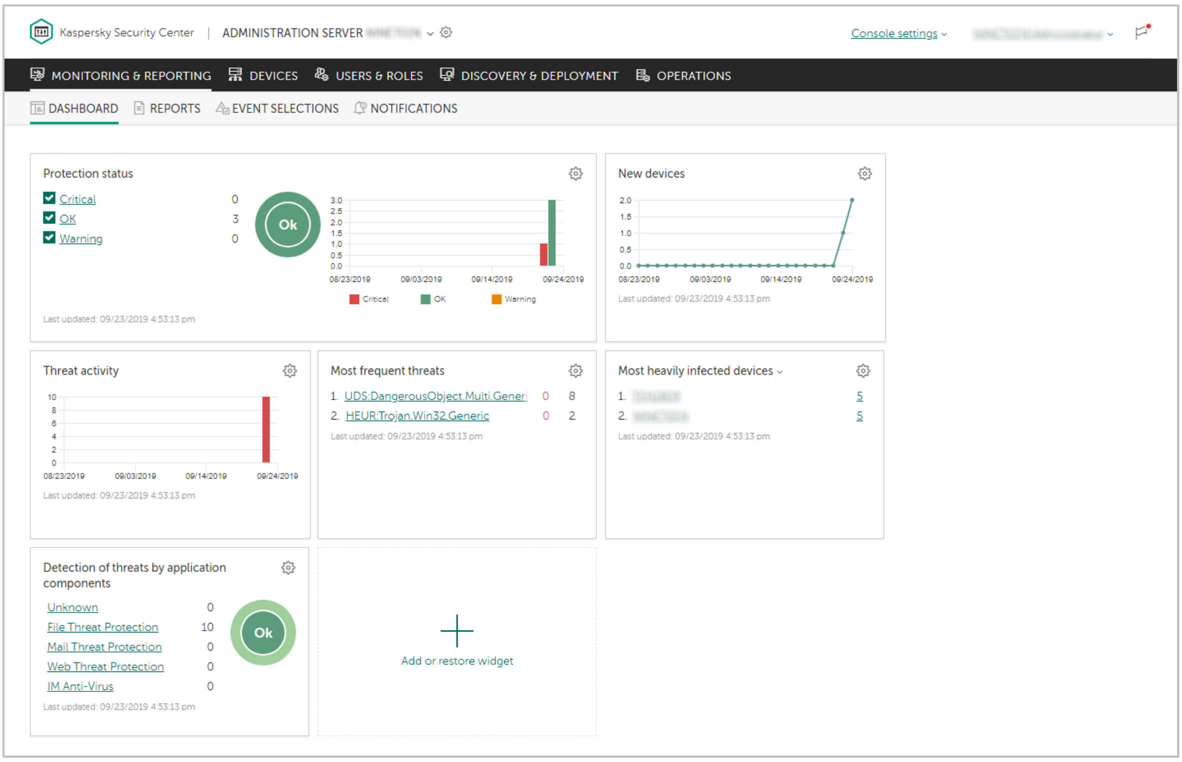

K7 Endpoint Security

High Security Threat Found
Object :C:\[redacted]\winmal\four.exe
Threat :found the P2PWorm (004b8a8b1)
Action:Has been removed

2/2 Entries

The GUI of the server protection software is identical to that of its desktop counterpart.

Kaspersky Endpoint Security for Business (KESB) - Select



Protection status

☑ Critical	0
☑ OK	3
☑ Warning	0

Last updated: 09/23/2019 4:53:13 pm

New devices

Last updated: 09/23/2019 4:53:13 pm

Threat activity

Last updated: 09/23/2019 4:53:13 pm

Most frequent threats

1. UDS:DangerousObject.Multi.Generi	0	8
2. HEUR:Trojan.Win32.Generic	0	2

Last updated: 09/23/2019 4:53:13 pm

Most heavily infected devices

1. [redacted]	5
2. [redacted]	5

Last updated: 09/23/2019 4:53:13 pm

Detection of threats by application components

Unknown	0
File Threat Protection	10
Mail Threat Protection	0
Web Threat Protection	0
IM Anti-Virus	0

Last updated: 09/23/2019 4:53:13 pm

Verdict

Kaspersky Endpoint Security for Business (KESB) Select is a tier of Kaspersky's Endpoint Security for Business product line. It is a powerful and sophisticated product, aimed at medium-sized businesses and larger enterprises. There is very good cross-platform support, and the web-based console provides a wealth of functionality. The menu structure is straightforward. However, some learning time would be required to make the most of it.

About the product

Kaspersky Endpoint Security for Business Select provides server-based management tools. It supports management of endpoint software for Windows PCs and servers, Linux tablets, PCs and servers, and macOS. There is also support for Android and iOS mobile devices. Users can choose between a modern web-based console and a legacy MMC-based console. We have looked at the web-based console (shown in the screenshot above) in this review.

Getting up and running

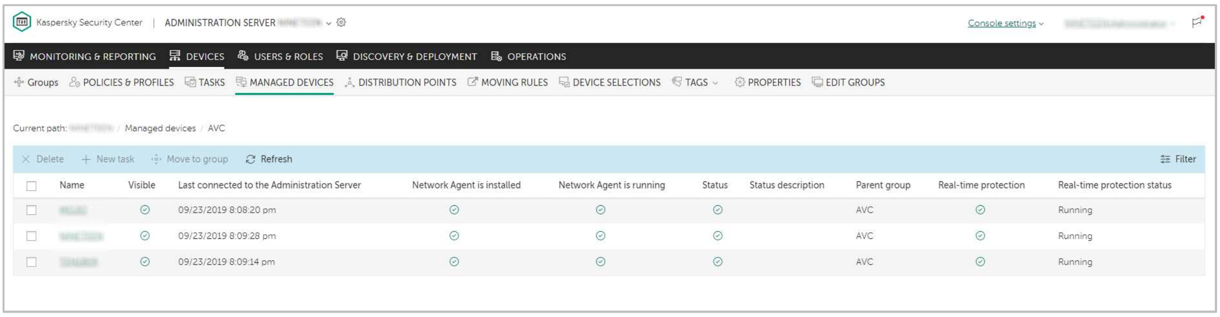
Installing the management console is a straightforward process for an experienced administrator. An SQL database is required, which could be the free Microsoft SQL Server Express. You can use Windows credentials to log in to the console if you want. When you first run the web-based console, an optional 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. Finally, the *Protection Deployment Wizard* lets you set up remote push software installation. This is a very neat and simple process. You can also install clients manually (there are three different methods of doing this).

Everyday management

The console functions are arranged in two menu bars across the top of the page. The upper menu bar shows the main functionality areas. These are *Monitoring & Reporting, Devices, Users & Roles, Discovery & Deployment,* and *Operations*. The lower menu bar provides access to the sub-pages of each major menu item. In some cases, the items on the lower menu bar open drop-down lists of further items. The *Monitoring and Reporting\Dashboard* page provides a graphical overview of important items. These include protection status, new devices, plus details of threats and infected devices. Please see the screenshot above. 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.

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

The *Devices* tab, *Managed Devices* page 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.



Current path: [redacted] / Managed devices / AVC

□	Name	Visible	Last connected to the Administration Server	Network Agent is installed	Network Agent is running	Status	Status description	Parent group	Real-time protection	Real-time protection status
□	[redacted]	✓	09/23/2019 8:08:20 pm	✓	✓	✓		AVC	✓	Running
□	[redacted]	✓	09/23/2019 8:09:28 pm	✓	✓	✓		AVC	✓	Running
□	[redacted]	✓	09/23/2019 8:09:14 pm	✓	✓	✓		AVC	✓	Running

The *Policies and Profiles* page lets you create and apply new configuration policies. *Device Selections* provides advanced filtering options for selecting clients.

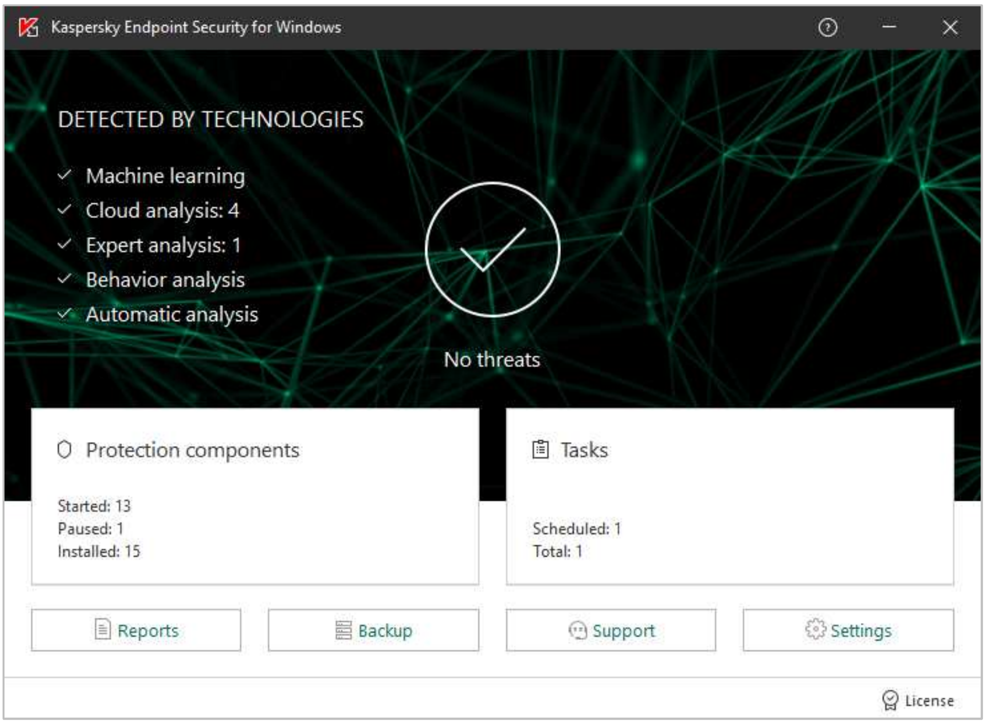
Under *Users & Roles*, you can see a list of predefined console users, along with Windows local and domain accounts for the Windows computers on the network. These can be assigned one of 16 different management roles for the console, allowing very granular access.

Discovery & Deployment includes various features for discovering unmanaged devices on the network, and deploying software to them. The *Quick Start Wizard* can be rerun from here. The *Device Selections* page lets you find devices in pre-configured groups. Examples include *Databases are outdated* and *Devices with Critical status*.

Amongst other things, the *Operations* tab provides an overview of licensing, repositories, and the quarantine functions. The *Backup* feature actually appears to be a standard quarantine function. Malware that had been detected on client PCs was found here. However, there is a separate *Quarantine* feature, which was empty after our test. The Kaspersky online knowledge base explains the functions of these two items: https://help.kaspersky.com/KSC/11/en-US/12429.htm

Windows endpoint protection software

The Windows desktop protection application is evidently designed for central management by IT staff, rather than local management by the end user. Consequently, under default settings, users can view settings, but not change them. The program window is essentially a comprehensive status display. It shows security status and detection statistics for the different technologies involved. These include machine learning, cloud analysis, and behavioural analysis. As in the console, the *Backup* feature is part of the quarantine functionality. We note that users can run manual scans of both local and remote drives, folders or files by means of the context menu in Windows Explorer.



Kaspersky Endpoint Security for Windows

DETECTED BY TECHNOLOGIES

- ✓ Machine learning
- ✓ Cloud analysis: 4
- ✓ Expert analysis: 1
- ✓ Behavior analysis
- ✓ Automatic analysis

No threats

Protection components

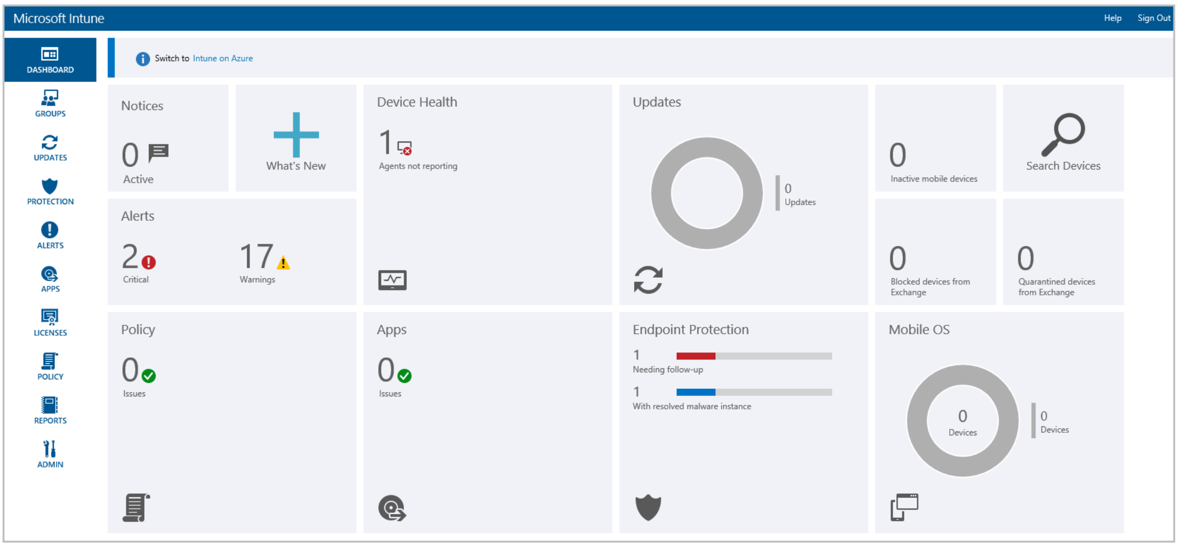
Started: 13
Paused: 1
Installed: 15

Tasks

Scheduled: 1
Total: 1

If the user should inadvertently copy a malicious file to the system, Kaspersky Endpoint Security will detect and quarantine it on access. No alert is shown on the desktop system. The GUI of the server protection software is identical to that of the client.

Microsoft Defender ATP's Antivirus for Business with Intune



Verdict

The Intune cloud console has a very clean, modern design. It is very easy to navigate using the single menu bar on the left-hand side. The Live Tiles on the Dashboard page provide a good overview of the security situation. The integrated links mean that the admin can easily find more information, and take the necessary action. The management agent can easily be deployed manually in smaller companies. You can also deploy via Group Policy, for larger enterprises. Intune can be used to manage thousands of devices. Its intuitive, easy-to-navigate interface make it an excellent choice.

About the product

Intune is a cloud-based service. It provides companies with security management for their devices, apps and data. Platforms covered are Windows Desktop, Windows Mobile, macOS, iOS and Android. This review covers the use of Microsoft Intune to manage Windows' out-of-box antivirus and security features. Please note that a dual management interface is available. In this review, we have covered the Classic interface, shown above.

Getting up and running

As the management console is cloud based, no installation is necessary. A management agent has to be deployed to the clients. After this, you can monitor and control them from the console. The agent is easily found under Admin/Client Software Download. You can install it manually on the client with just a couple of clicks. For larger networks, the admin can use Group Policy to deploy the software automatically.

In the case of Windows 10 and Windows 8.1 clients, Microsoft's antivirus client is already incorporated into the operating system. No further software installation is required. With Windows 7 PCs, however, the antivirus client is not pre-installed, but is available as an update. If the Intune management agent is installed on a Windows 7 client without AV protection, the Microsoft AV client update will be installed automatically.

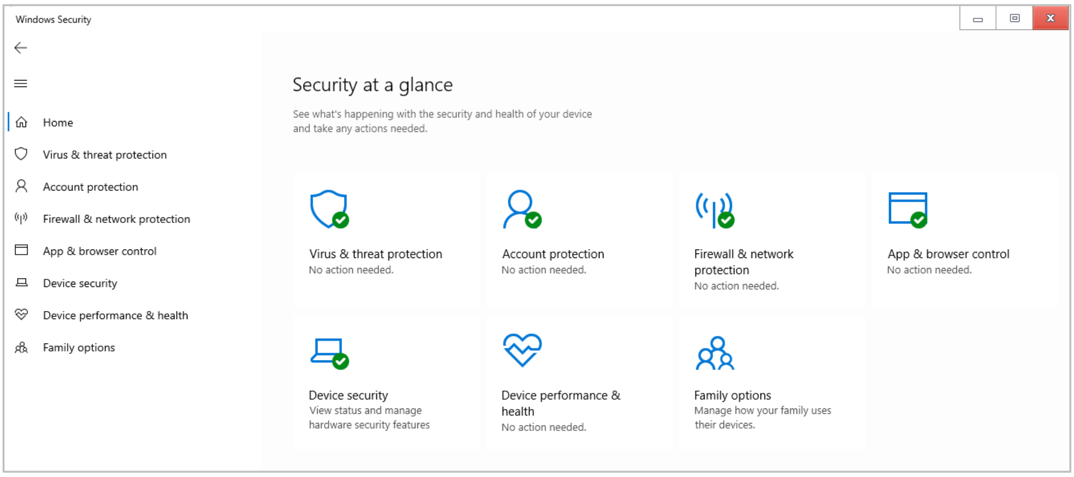
Everyday management

The Intune console is navigated using a very neat, clean menu column on the left-hand side. The *Dashboard* (home) page displays the status of different components using Live Tiles. The *Endpoint Protection* tile shows the number of devices with resolved and unresolved malware detections. These are displayed graphically as colour-coded bar charts. Other tiles provide information on *Warnings/Critical Alerts*, and *Device Health*. Clicking on an element within a tile, such as *Warnings*, opens the relevant details page for the item concerned.

Under *Groups\Devices*, you can see managed computers. There are details such as operating system and date & time of last update. The *Protection* page provides a more detailed overview of malware detections, device status and most frequently detected malware. There is also a list of all malware items that have been detected in the network. *Alerts* displays details of all security-related warnings, including reports any of failed client software deployments.

Endpoint protection software

The precise nature of the Windows desktop protection software GUI is dependent on the version of Windows installed on the PC. Recent Windows 10 clients (Builds 1809, 1903 and 1909) have the Windows Defender Security Center interface. This is shown below:



Security at a glance

See what's happening with the security and health of your device and take any actions needed.

Virus & threat protection
No action needed.

Account protection
No action needed.

Firewall & network protection
No action needed.

App & browser control
No action needed.

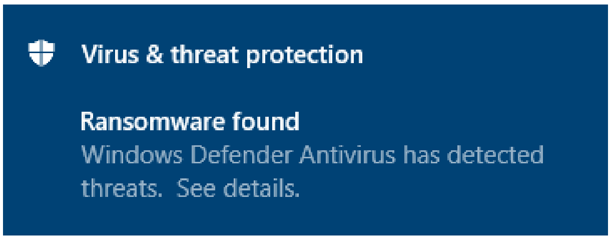
Device security
View status and manage hardware security features

Device performance & health
No action needed.

Family options
Manage how your family uses their devices.

Older versions of Windows, including Windows 7 and 8.1, use the same GUI as Microsoft Security Essentials. This is similar to that of a typical consumer antivirus program. All variants allow the user to update malware definitions, and run full, quick, custom and context-menu scans.

Malware is detected on file copy, and quarantined. An example alert is shown below. The user cannot take any action, and the alert closes after a few seconds.

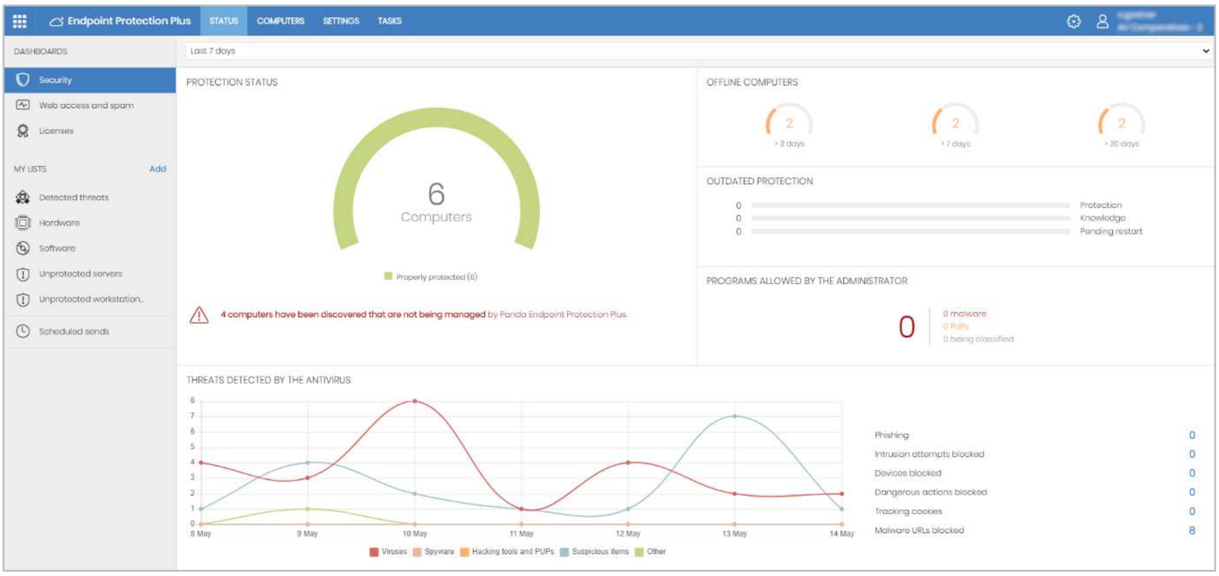


Virus & threat protection

Ransomware found
Windows Defender Antivirus has detected threats. See details.

The GUI of the server protection software is essentially the same as its desktop counterpart. However, the components *Account protection, Device performance & health* and *Family options* are not included in Windows Server.

Panda Endpoint Protection Plus on Aether



Last 7 days

4 computers have been discovered that are not being managed by Panda Endpoint Protection Plus.

0	Protection
0	Knowledge
0	Pending restart

0 | 0 malware
0 PUPs
0 being classified

Phishing	0
Intrusion attempts blocked	0
Devices blocked	0
Dangerous actions blocked	0
Tracking cookies	0
Malware URLs blocked	8

Verdict

Panda Endpoint Protection Plus on Aether is a very strong product. It is powerful enough for larger organisations, but simple enough for smaller businesses too. It is very easy to set up, as it requires no on-site server. There is an excellent, very clean and useful administrative console. This has a clear installation and deployment workflow. We were particularly impressed with the clean and obvious design of the user interface, and the speed at which it could be mastered.

About the product

This is a cloud-console managed system. There are device clients for Windows/Linux servers, Windows/Linux/macOS PCs, and Android mobile devices. The desktop client software has a simple interface, which allows users to run updates and various scans. It is suitable for organisations of all sizes.

Getting up and running

The product is managed from a cloud-based console, which requires no installation. Deployment is carried out using the *Add Computers* button on the *Computers* page. You can download the installer directly, or click on *Send by email*. This opens an email message with a link for download and installation. This works for Windows, Linux, macOSand Android. The user clicks on the provided link to install the client, and this is then automatically licensed. Either installation method lets you pre-allocate the client to a management group.

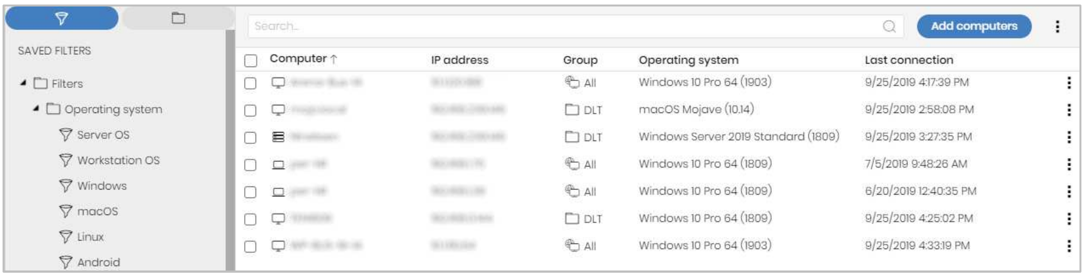
Everyday management

Protection status and threat detection history are provided on the *Status* tab/*Security* page, which opens by default. There are excellent graphics for detected threats. These include offline computers, outdated protection, and blocked URLs here. This provides a solid daily overview of issues. We particularly liked it because it provides a headline view of the status, but allows you to click through for more detailed information. For example, clicking on the main *Protection Status* graphic takes you to the *Computers* page. The console's quarantine function is accessed by clicking on *Threats detected by the antivirus*.

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 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, lists of unprotected workstations and servers, and threats detected by AV. This list is customisable, and a number of other categories can be added. These include computer protection status, and web access by computer.

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.



□	Computer ↑	IP address	Group	Operating system	Last connection
□	[redacted]	[redacted]	All	Windows 10 Pro 64 (1903)	9/25/2019 4:17:39 PM
□	[redacted]	[redacted]	DLT	macOS Mojave (10.14)	9/25/2019 2:58:08 PM
□	[redacted]	[redacted]	DLT	Windows Server 2019 Standard (1809)	9/25/2019 3:27:35 PM
□	[redacted]	[redacted]	All	Windows 10 Pro 64 (1809)	7/5/2019 9:48:26 AM
□	[redacted]	[redacted]	All	Windows 10 Pro 64 (1809)	6/20/2019 12:40:35 PM
□	[redacted]	[redacted]	DLT	Windows 10 Pro 64 (1809)	9/25/2019 4:25:02 PM
□	[redacted]	[redacted]	All	Windows 10 Pro 64 (1903)	9/25/2019 4:33:19 PM

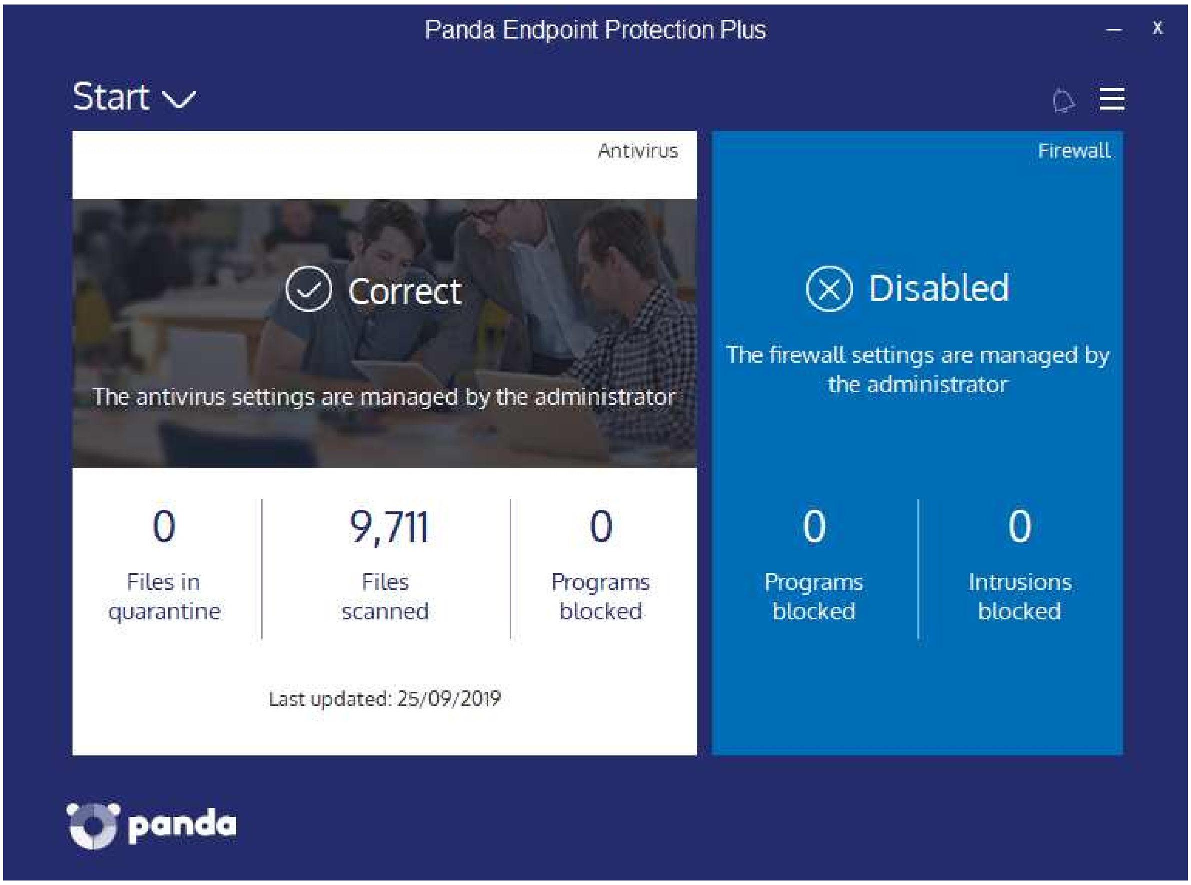
This page shows all the protected computers and mobile devices. It is very clearly laid out, and shows essential information. A Windows-like folder tree on the left lets you show devices by group.

Using the *Settings* tab/*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 *Settings/My Alerts* you can set up email notifications for various items. These include malware and phishing detections, unlicensed/unmanaged/unprotected/unlicensed computers, and installation errors. Other settings pages let you manage updates and proxy servers etc.

Finally, the *Tasks* tab can be used to set up scheduled scans.

Windows endpoint protection software

The Windows desktop protection software allows access to solid end-user capabilities like Full Scan, Critical Areas Scan and Custom Scan. The user can force a synchronisation of the updates from the System Tray menu. However, there is no access to any settings.



Correct

The antivirus settings are managed by the administrator

0 Files in quarantine

9,711 Files scanned

0 Programs blocked

Last updated: 25/09/2019

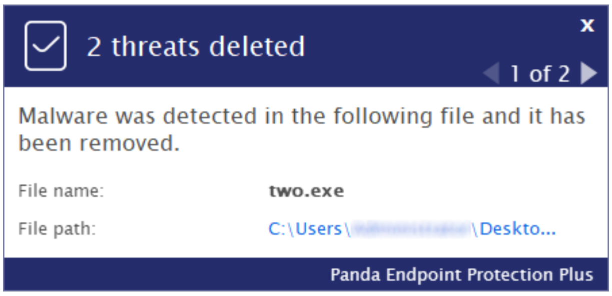
Disabled

The firewall settings are managed by the administrator

0 Programs blocked

0 Intrusions blocked

If a user should inadvertently copy a malicious file to their system, Panda will detect and quarantine it on access. An example alert is shown below. The user cannot take any action, and the alert closes after a few seconds.



2 threats deleted

Malware was detected in the following file and it has been removed.

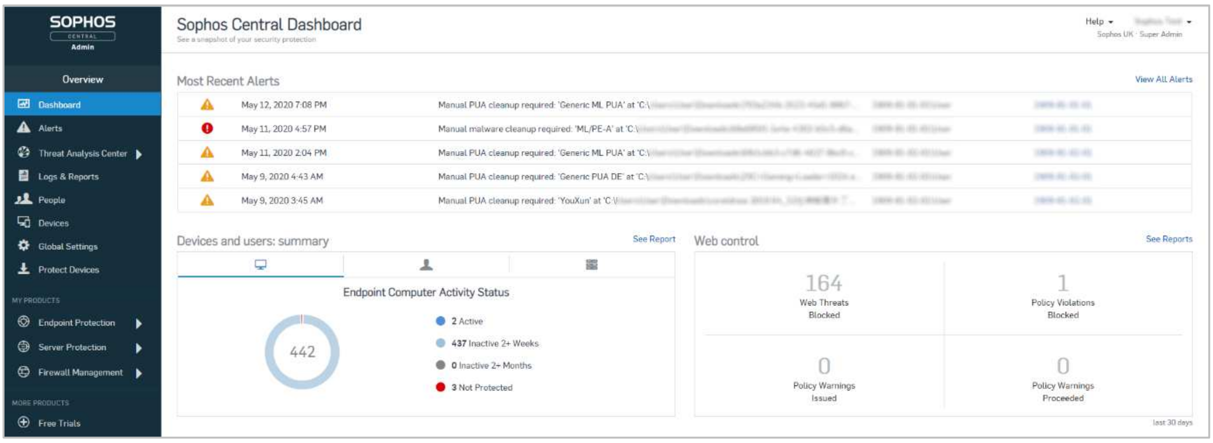
File name: two.exe

File path: C:\Users\[redacted]\Deskto...

Panda Endpoint Protection Plus

The GUI of the server protection software is identical to that of its desktop counterpart.

Sophos Intercept X Advanced



Sophos Central Dashboard

See a snapshot of your security protection

[redacted] Sophos UK · Super Admin

Most Recent Alerts

⚠	May 12, 2020 7:08 PM	Manual PUA cleanup required: 'Generic ML PUA' at 'C:\[redacted]	[redacted]	[redacted]
●	May 11, 2020 4:57 PM	Manual malware cleanup required: 'ML/PE-A' at 'C:\[redacted]	[redacted]	[redacted]
⚠	May 11, 2020 2:04 PM	Manual PUA cleanup required: 'Generic ML PUA' at 'C:\[redacted]	[redacted]	[redacted]
⚠	May 9, 2020 4:43 AM	Manual PUA cleanup required: 'Generic PUA DE' at 'C:\[redacted]	[redacted]	[redacted]
⚠	May 9, 2020 3:45 AM	Manual PUA cleanup required: 'YouXun' at 'C:\[redacted]	[redacted]	[redacted]

Devices and users: summary

Endpoint Computer Activity Status

442

- ● 2 Active
- ● 437 Inactive 2+ Weeks
- ● 0 Inactive 2+ Months
- ● 3 Not Protected

Web control

164 Web Threats Blocked	1 Policy Violations Blocked
0 Policy Warnings Issued	0 Policy Warnings Proceeded

last 30 days

Verdict

There is a lot of power and capability here, and the design of the management console is clean and well laid out. Most of the product works in a clear and consistent way. For a reasonably experienced system administrator, it is straightforward to implement, deploy and manage. For new system admins, the scope of functionality available in the console may make essential AV management tasks a little slower to find.

About the product

Sophos Intercept X Advanced uses a cloud console (Sophos Central) to manage Windows clients and servers, Linux servers, and macOS clients. Intercept X uses neural network analysis of malware. It provides protection from ransomware and exploits, along with additional browser security. There are also investigative and removal capabilities.

Getting up and running

The product is wholly managed from a cloud-based console. Licenses are applied to this, and then can be handed out to client computers. Installing the client is very straightforward. You can download the installation package and install from that, or push it out through your chosen management interface.

Devices can be assigned to groups (as you would expect), and inherit centrally defined policy. Users are automatically created in Sophos Central when they use a Sophos-protected device. They can also be imported via CSV, and synched via an Active Directory application. A user account is also used to control access to the Sophos management facilities. A user can be classified as *User*, *SuperAdmin*, *Admin*, *Help Desk* and *Read-only* here. This allows a layered configuration of management of the Sophos platform. There is a range of capabilities which can be applied to policy. These include web URL blocking, peripheral control and management of application execution.

Everyday management

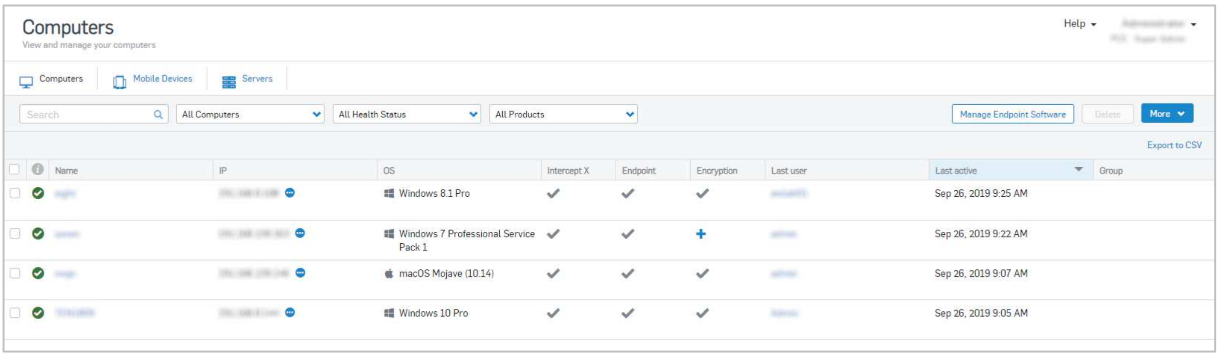
The *Sophos Central Dashboard* view is quite straightforward. It has a clean, uncluttered user interface, offering an overview of all the systems and protection capabilities. Here you can see how many endpoints are active, the most recent alerts, and statistics on the web URL access management.

The *Alerts* item gives you a list of all the alerts which have occurred. You can sort by *Description*, *Count* and *Actions*.

Logs and Reports shows a collection of default reports. A notable report here is *Policy Violators*. This shows those users who have tried to access blocked websites most often.

The *Global Settings* page does what you would expect. People provides a user-centric view of the network, letting you see all the devices assigned to a particular user, and all the activity associated with these.

Devices shows the managed devices on the network. These are separated into three different pages: *Computers, Mobile Devices, Servers*, as shown below:

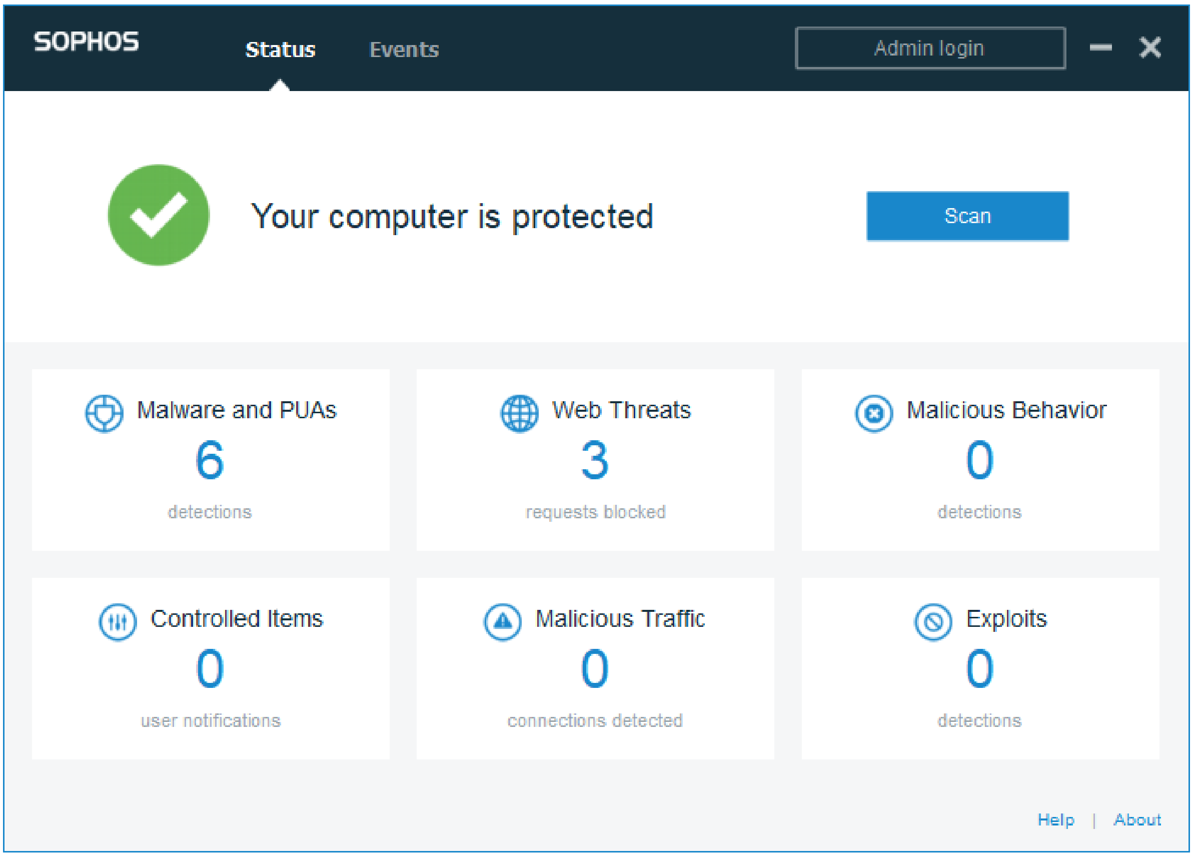


□		Name	IP	OS	Intercept X	Endpoint	Encryption	Last user	Last active	Group
□	✓	[redacted]	[redacted]	Windows 8.1 Pro	✓	✓	✓	[redacted]	Sep 26, 2019 9:25 AM	
□	✓	[redacted]	[redacted]	Windows 7 Professional Service Pack 1	✓	✓	+	[redacted]	Sep 26, 2019 9:22 AM	
□	✓	[redacted]	[redacted]	macOS Mojave (10.14)	✓	✓	✓	[redacted]	Sep 26, 2019 9:07 AM	
□	✓	[redacted]	[redacted]	Windows 10 Pro	✓	✓	✓	[redacted]	Sep 26, 2019 9:05 AM	

Endpoint Protection takes you to another set of user interface and menus. This also has pages for *Dashboard*, *Logs* and *Reports*, *People* and *Computers* menu items. Here you can also configure policies, settings and download endpoint installation packages.

Windows Endpoint Protection Software

The Windows desktop protection software has a GUI with a comprehensive status display. It also allows users to carry out scan tasks. The *Status* tab displays the overall security status, and provides summaries of recent threat types. The *Events* tab lists recent malware detections. Users can run a full system scan from the *Scan* button on the *Status* page. Alternatively, they can right-click a file, folder or drive in Windows Explorer, and click *Scan with Sophos Anti-Virus* in the context menu.



Your computer is protected

Malware and PUAs 6 detections

Web Threats 3 requests blocked

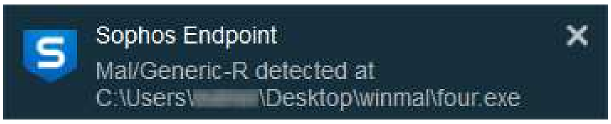
Malicious Behavior 0 detections

Controlled Items 0 user notifications

Malicious Traffic 0 connections detected

Exploits 0 detections

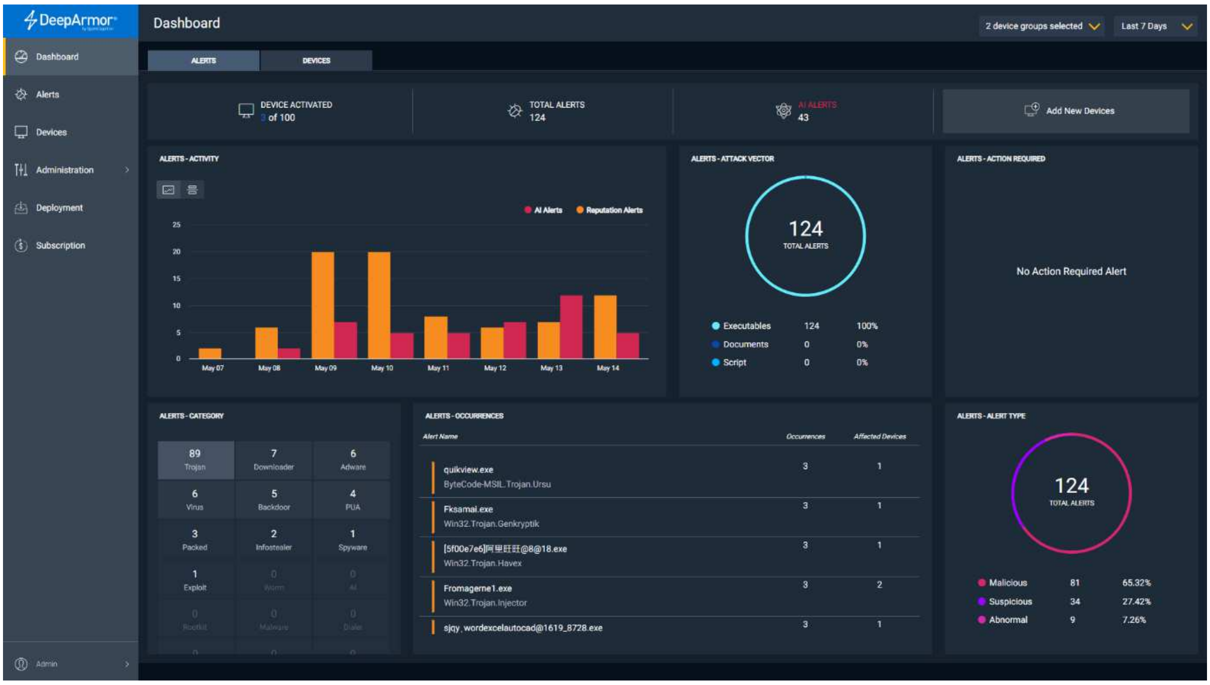
If a user should inadvertently copy a malicious file to their system, Sophos will detect and quarantine it on-access . An example alert is shown below. The user cannot take any action, and the alert closes after a few seconds.



Sophos Endpoint
Mal/Generic-R detected at
C:\Users\[redacted]\Desktop\winmal\four.exe

The GUI of the server protection software is identical to that of its desktop counterpart.

SparkCognition DeepArmor Endpoint Protection Platform



DEVICE ACTIVATED
3 of 100

TOTAL ALERTS
124

AI ALERTS
43

● Executables	124	100%
● Documents	0	0%
● Script	0	0%

No Action Required Alert

89 Trojan	7 Downloader	6 Adware
6 Virus	5 Backdoor	4 PUA
3 Packed	2 Infostealer	1 Spyware
1 Exploit	0 Worm	0 AI
0 Rootkit	0 Malware	0 Dialer
0	0	0

Alert Name	*Occurrences*	*Affected Devices*
quikview.exe ByteCode-MSIL.Trojan.Ursu	3	1
Fksamai.exe Win32.Trojan.Genkryptik	3	1
[5f00e7e6]阿里旺旺@8@18.exe Win32.Trojan.Havex	3	1
Fromagerne1.exe Win32.Trojan.Injector	3	2
sjqy, wordexcelautocad@1619_8728.exe	3	1

● Malicious	81	65.32%
● Suspicious	34	27.42%
● Abnormal	9	7.26%

Verdict

SparkCognition DeepArmor Endpoint Protection Platform (EPP) is very straightforward to set up. The console is cloud based, and the deployment process is simple. The management console has a very clean design that avoids overwhelming the admin. Getting the most out of the product would doubtless take some time, but the user interface makes this process as easy as possible.

About the product

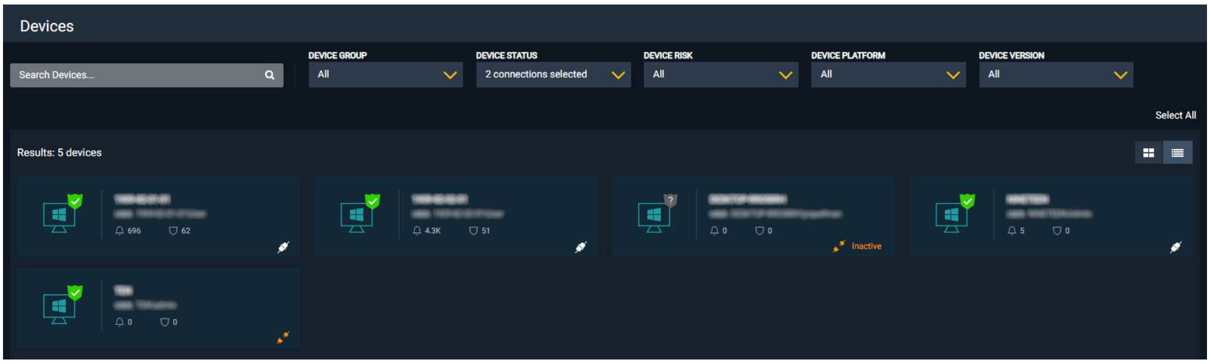
SparkCognition uses a cloud-based console to manage the endpoint protection software. There are clients for Windows, Mac and Linux systems.

Getting up and running

The console does not require any installation, as it is cloud-based. Deployment of endpoint protection software is similar for all platforms. You just download the appropriate installer from the *Deployment* page of the console, and run it on the respective client device. This is a very straightforward process. You can install Windows clients using System Centre Configuration Manager or PowerShell.

Everyday management

When you log in to the console, you will see the *Alerts Dashboard* (screenshot above). This provides a summary of recent threats. The *Devices Dashboard* displays a device-centred overview. This shows you the total number of devices on your network, group membership, devices at risk, device connection status, and distribution of different endpoint agent versions. The title text for each dashboard panel is a link to more details. For example, clicking *Medium Risk Devices* shows you a list of devices with that status.



Devices

Search Devices...

DEVICE GROUP: All

DEVICE STATUS: 2 connections selected

DEVICE RISK: All

DEVICE PLATFORM: All

DEVICE VERSION: All

Select All

Results: 5 devices

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. 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 device version.

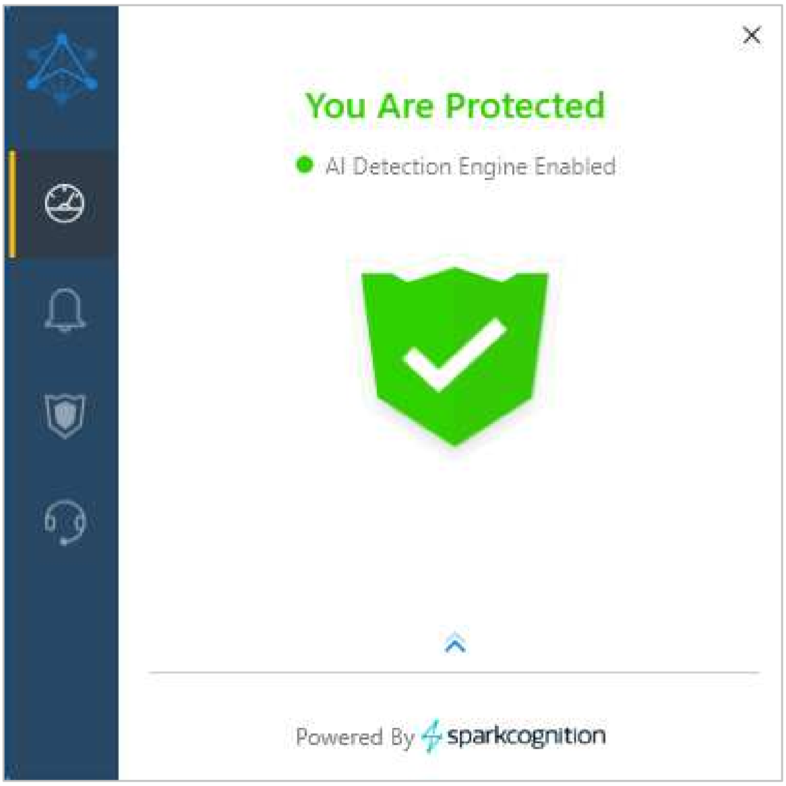
The *Alerts* page shows recent alerts, along with details. These include the file name of the malware, how it was detected, detection name, "confidence" (probability that the file really is malicious), name of affected device, time of detection, action taken or required, and file hash. Sub-tabs of each file's details page show all detections of the file across the network (*Occurrences*). Clicking on an entry provides further details in a separate page. The *Take Action* button here provides the options *Remote Remediate, Remote Restore,* and *External Remediate*. These allow the admin to take immediate action.

The *Administration* menu includes the submenus *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 individual devices or groups. You can manage the latter 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.

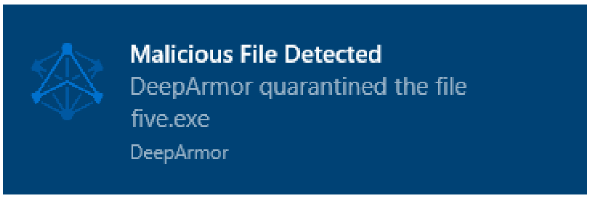
On the *Deployment* page you can find installers for Window, macOS, and various different Linux distributions. Finally, *Subscription* shows you the total number of device licences available and used, and the validity period.

Windows endpoint protection software

The endpoint protection client has a GUI, but does not allow users to take any action. The *Notification* page (bell icon) lists the most recent threats discovered. The *Protection* page shows the configuration options for protection components, but these are deactivated by default.



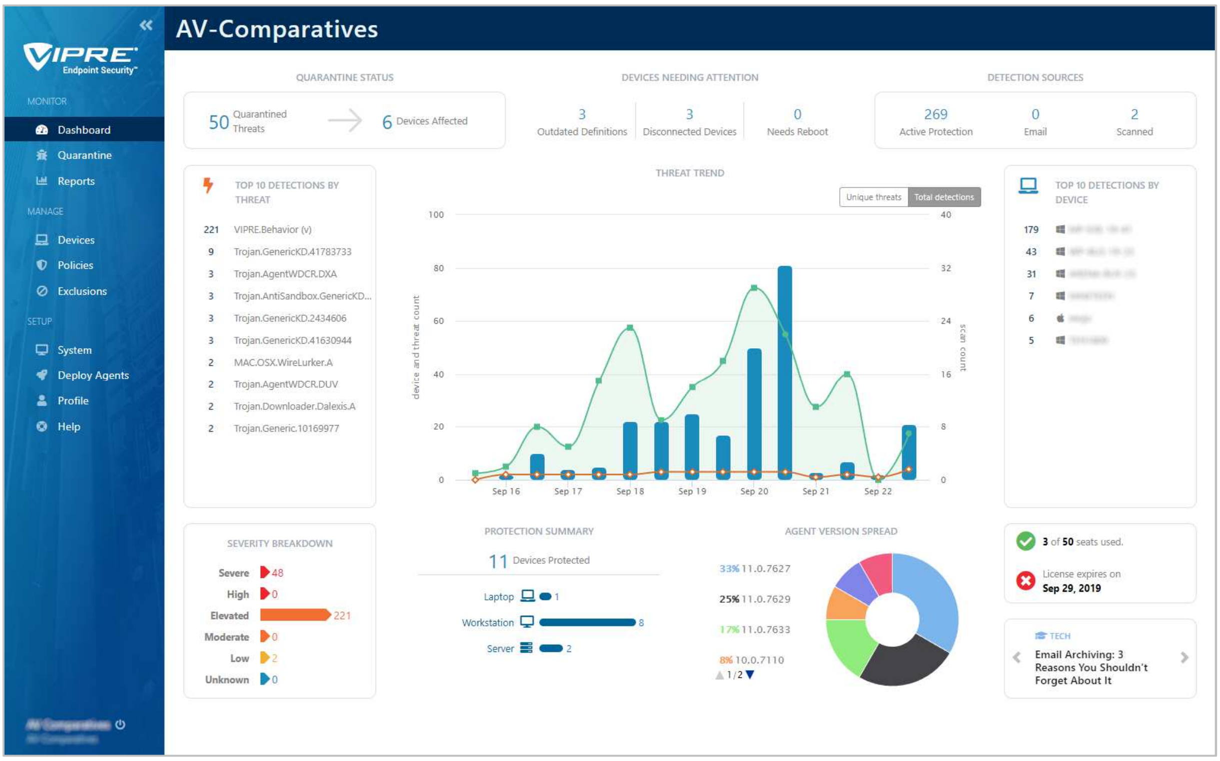
In our test, we found that malware copied to the test system was not detected on access. However, when executed, it was detected and quarantined on access. An example alert is shown below. The user cannot take any action, and the alert closes after a few seconds.



Malicious File Detected
DeepArmor quarantined the file
five.exe
DeepArmor

The GUI of the server protection software is identical to that of its desktop counterpart.

VIPRE Endpoint Security Cloud



TOP 10 DETECTIONS BY THREAT

221	VIPRE.Behavior (v)
9	Trojan.GenericKD.41783733
3	Trojan.AgentWDCR.DXA
3	Trojan.AntiSandbox.GenericKD...
3	Trojan.GenericKD.2434606
3	Trojan.GenericKD.41630944
2	MAC.OSX.WireLurker.A
2	Trojan.AgentWDCR.DUV
2	Trojan.Downloader.Dalexis.A
2	Trojan.Generic.10169977

Verdict

This product impresses with clear design, simple operational processes and strong reporting features. Even a less-experienced user could deploy the agent and manage the network. The product shows what clear thinking and good deployment flow can bring. There is strong reporting and an obvious process for day-to-day operation.

About the product

VIPRE Endpoint Security Cloud uses a cloud-based console to manage Windows and macOS clients and Windows servers. VIPRE Endpoint Security is the client that runs on the desktop. VIPRE tell us that the cloud service runs on the Amazon AWS cloud, and that this brings efficiency, scalability and growth.

Getting up and running

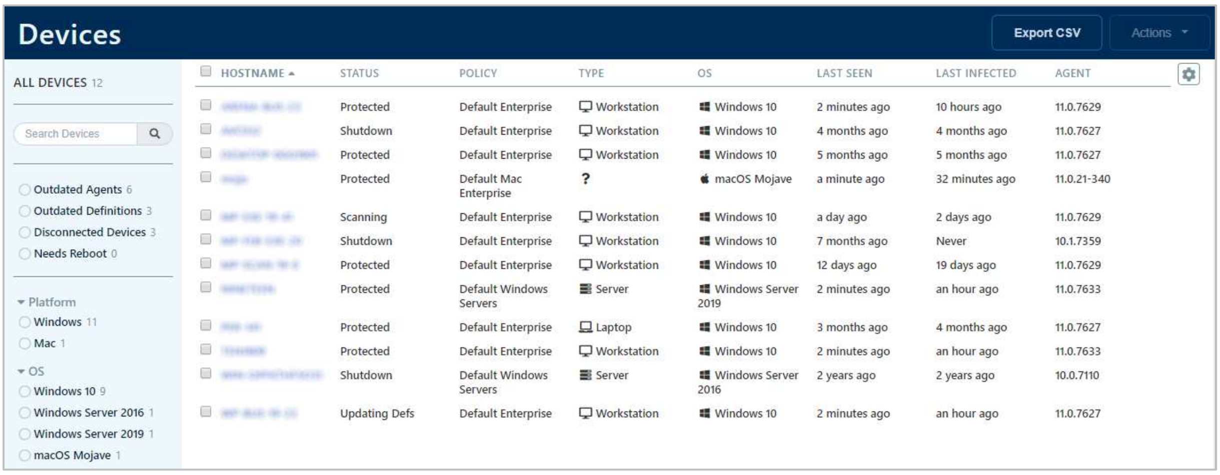
Access to the web portal is straightforward via a standard username/password login combination (two-factor authentication is also available). The user interface immediately impresses with its clean and clear design. The first page you see has a *Getting Started* area. This covers deploying of agents, creation of users and the setting of appropriate policies. The next section deals with more advanced post-setup topics. These include *Dashboard*, *Devices*, *Exclusions*, *Notifications* and *Reports*. A link on the *Getting Started* page takes you to the *Deploy Agents* page of the console. From here you can download installers for the endpoint software, or use the email function to send links to users. We note that when a new version of the agent installer is made available, the page displays a note to that effect. You can either approve the new version for all devices, or try it out on a few test machines first.

Everyday management

Once you have deployed the endpoint software to your devices, the menus on the left-hand side come into play. From the top, the *Monitor* section covers *Dashboard* which is a straightforward view of the status of all the clients. It is obvious which ones need attention, what the device and threat count is, and the version numbering of the devices deployed.

Quarantine gives a strong overview of the quarantine actions over the past week. You can easily extend the reporting-time window using obvious choices such as "Last 24 hours", "Last 3 days" and so forth. The reporting is clear and clean, showing what devices have had issues, and with which malware sources.

Reports lets you dig into the data in a more detailed fashion, for example by client, by malware, by action taken, by policy definition. All of these are clear and clean, but more designed to be used through the web console. You can set up notifications and reports to be sent through the *System* menu.



HOSTNAME	STATUS	POLICY	TYPE	OS	LAST SEEN	LAST INFECTED	AGENT
[redacted]	Protected	Default Enterprise	Workstation	Windows 10	2 minutes ago	10 hours ago	11.0.7629
[redacted]	Shutdown	Default Enterprise	Workstation	Windows 10	4 months ago	4 months ago	11.0.7627
[redacted]	Protected	Default Enterprise	Workstation	Windows 10	5 months ago	5 months ago	11.0.7627
[redacted]	Protected	Default Mac Enterprise	?	macOS Mojave	a minute ago	32 minutes ago	11.0.21-340
[redacted]	Scanning	Default Enterprise	Workstation	Windows 10	a day ago	2 days ago	11.0.7629
[redacted]	Shutdown	Default Enterprise	Workstation	Windows 10	7 months ago	Never	10.1.7359
[redacted]	Protected	Default Enterprise	Workstation	Windows 10	12 days ago	19 days ago	11.0.7629
[redacted]	Protected	Default Windows Servers	Server	Windows Server 2019	2 minutes ago	an hour ago	11.0.7633
[redacted]	Protected	Default Enterprise	Laptop	Windows 10	3 months ago	4 months ago	11.0.7627
[redacted]	Protected	Default Enterprise	Workstation	Windows 10	2 minutes ago	an hour ago	11.0.7633
[redacted]	Shutdown	Default Windows Servers	Server	Windows Server 2016	2 years ago	2 years ago	10.0.7110
[redacted]	Updating Defs	Default Enterprise	Workstation	Windows 10	2 minutes ago	an hour ago	11.0.7627

The next section is *Manage,* which covers *Devices* (shown above). This displays which devices are in play, and their operational status. For any device or group, you can assign policy, run a scan, update the definitions, reboot the device, or delete the agent.

Policies lets you control how the clients are allowed to operate, and the security policies that they will deploy. There is a wide range of customisation here, but the *Default Enterprise* settings will probably be appropriate for most users. Here you can allow users to interact with the VIPRE client. For example, you can allow them to scan items via a right click, or force USB devices to be scanned on insertion.

Exclusions allows you to create exclusion lists of files, paths, folders and so forth that are excluded from scanning. This might, for example, include some shared space that is managed in a different way from normal storage.

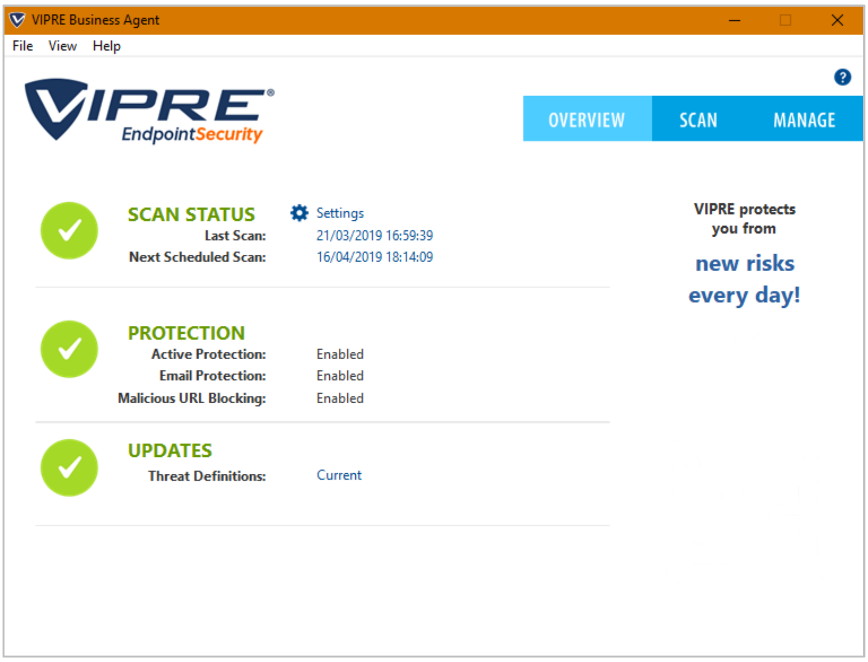
Finally, the *Setup* area covers system settings and all the main defaults of the platform. *Deploy Agents* allows you to download an agent installer package, to create a policy installer, and to invite users via email. *Profile* lets you enable two-factor authentication.

The web console impresses both from the initial setup and deployment through to the ongoing management. The defaults are sensible, the screens clear and clean, and it is obvious what it is reporting and how healthy the clients are. It is simple to get clients to do centrally managed tasks, and the configuration of policy is easy too. Creating users is simple, and they can have the role of Admin or Analyst. The latter might be appropriate for, say, a help desk operative.

It is simple to create ongoing reports, and you don't need to specify a mail server to send it through – this is provided for you. We would say the platform is appropriate for any size of company, from a small business with a few seats, through to a much larger organisation. The UI of the management console was always responsive under testing. It is built to cope with thousands of desktops and large numbers of events.

Windows endpoint protection software

The Windows desktop protection software is very similar to a consumer antivirus program. By default, users can run scans and updates, and view quarantine. However, they cannot not change settings or restore quarantined items. Admins can give users increased or reduced functionality, by means of changing the applicable policy from the console.



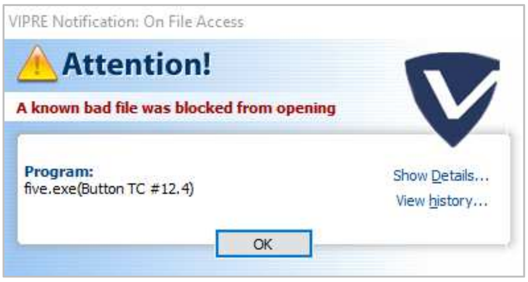
SCAN STATUS
Last Scan: 21/03/2019 16:59:39
Next Scheduled Scan: 16/04/2019 18:14:09

PROTECTION
Active Protection: Enabled
Email Protection: Enabled
Malicious URL Blocking: Enabled

UPDATES
Threat Definitions: Current

VIPRE protects you from new risks every day!

If a user should inadvertently copy a malicious file to their system, VIPRE will detect and quarantine it on access. An example alert is shown below. The user cannot take any actions, other than to close the alert.



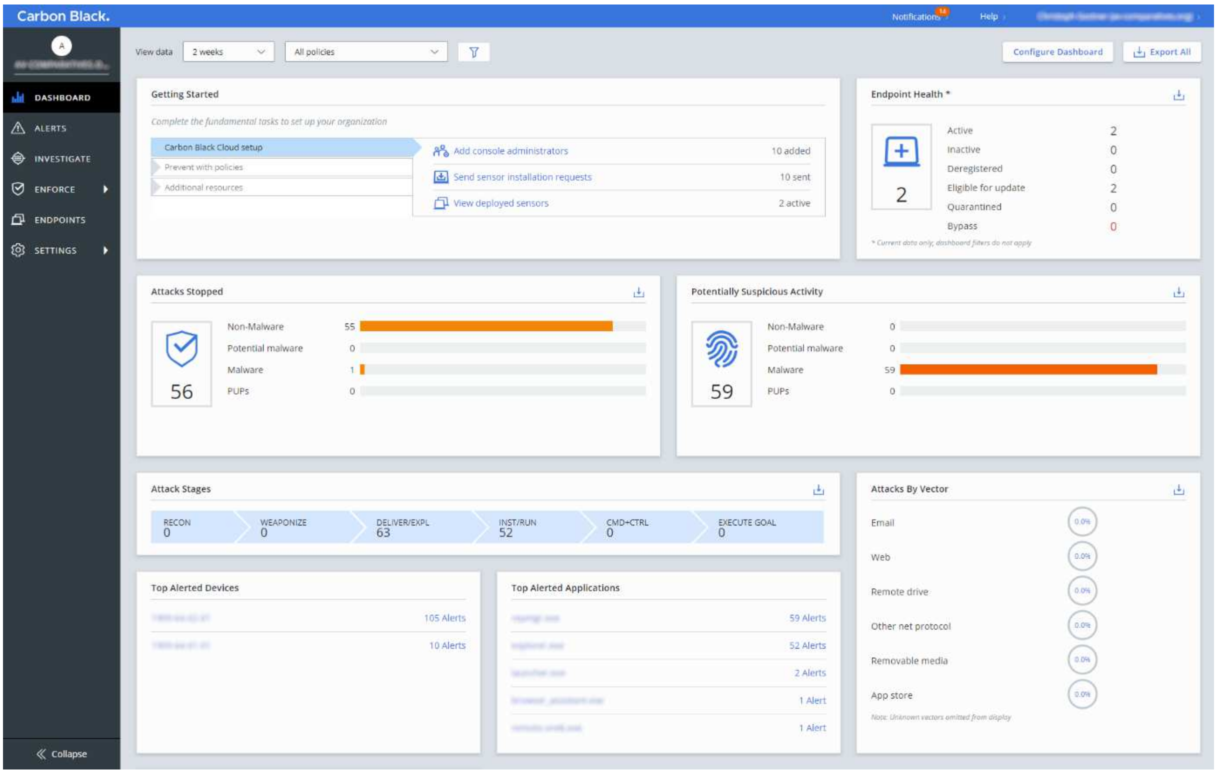
Attention!

A known bad file was blocked from opening

Program:
five.exe(Button TC #12.4)

The GUI of the server protection software is identical to that of its desktop counterpart.

VMware Carbon Black Cloud



Getting Started

Complete the fundamental tasks to set up your organization

Carbon Black Cloud setup
Prevent with policies
Additional resources

Add console administrators	10 added
Send sensor installation requests	10 sent
View deployed sensors	2 active

Endpoint Health *

2

Active	2
Inactive	0
Deregistered	0
Eligible for update	2
Quarantined	0
Bypass	0

* *Current data only; dashboard filters do not apply*

Attacks Stopped

56

Non-Malware	55
Potential malware	0
Malware	1
PUPs	0

Potentially Suspicious Activity

59

Non-Malware	0
Potential malware	0
Malware	59
PUPs	0

Attack Stages

RECON	WEAPONIZE	DELIVER/EXPL	INST/RUN	CMD+CTRL	EXECUTE GOAL
0	0	63	52	0	0

Attacks By Vector

Email	0.0%
Web	0.0%
Remote drive	0.0%
Other net protocol	0.0%
Removable media	0.0%
App store	0.0%

Note: Unknown vectors omitted from display

Top Alerted Devices

[redacted]	105 Alerts
[redacted]	10 Alerts

Top Alerted Applications

[redacted]	59 Alerts
[redacted]	52 Alerts
[redacted]	2 Alerts
[redacted]	1 Alert
[redacted]	1 Alert

Verdict

The manufacturers have clearly put a lot of thought into making Carbon Black Cloud intuitive to use. The design principle of the console is to show essential information without overwhelming the admin. You can drill down to get more details when you want. We found it very straightforward to see what actions were necessary, and to carry these out. Despite the simplicity of the design, the package provides a high degree of functionality. This makes it suitable for both larger and smaller businesses.

About the product

Carbon Black Cloud uses a cloud-based console to manage endpoint security software. There is support for Windows, macOS and Linux clients, and Windows Servers.

Getting up and running

The Carbon Black Cloud console is cloud based, so no installation is required. You just log on with your credentials and the console is ready to use.

You can install endpoints from the *Sensor Options* menu on the *Endpoints* page. There are two main options here, downloading the installer, or sending an installation link to users via email. Both are very quick and straightforward. The installation wizard is simple, only requiring you to accept the licence agreement and enter a vendor-provided code. Once setup has completed, the device will show up on the *Endpoints* page of the console.

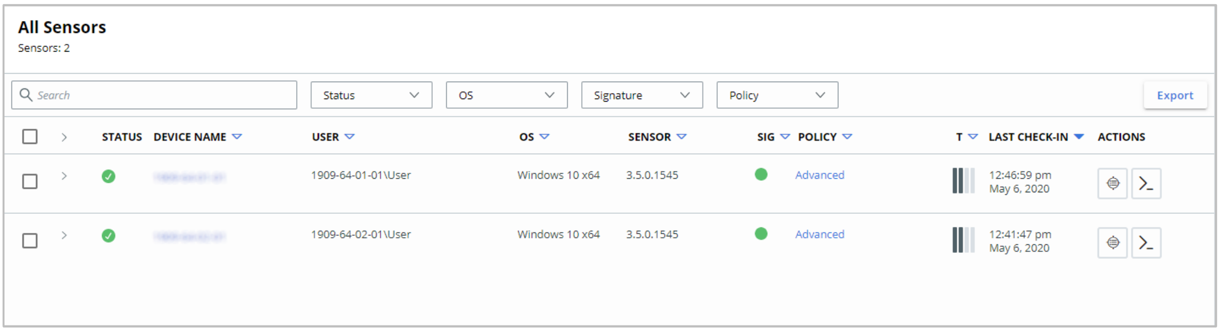
Everyday management

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. The *Dashboard* page shows you an overview of threats, displayed in panels. These are *Attacks stopped, Potentially Suspicious Activity, Attack Stages, Attacks by Vector, Top Alerted Devices,* and *Top Alerted Applications*. 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 the status of common tasks, such as adding console administrators.

The *Alerts* page shows you a list of threats encountered in chronological order. You can investigate any individual threat in more detail from here.

On the *Investigate* page, you can see a chronological list of events on any particular device. This allows you to monitor network connections and program executions, and build up a detailed picture of security-related events.

Enforce is home to the *Policies* page (amongst other things). Various configuration options for the endpoint protection software can be configured here. We found it very easy to create, edit and apply a new policy to specific endpoints. Policy changes take effect on applicable devices as soon as you log in to them. *Malware Removal* is also found under the *Enforce* sub-menu. Here you can see a list of quarantined malicious items, which you can e.g. investigate, delete or blacklist/whitelist. Malware is removed very quickly once you have given the command to delete it.



All Sensors
Sensors: 2

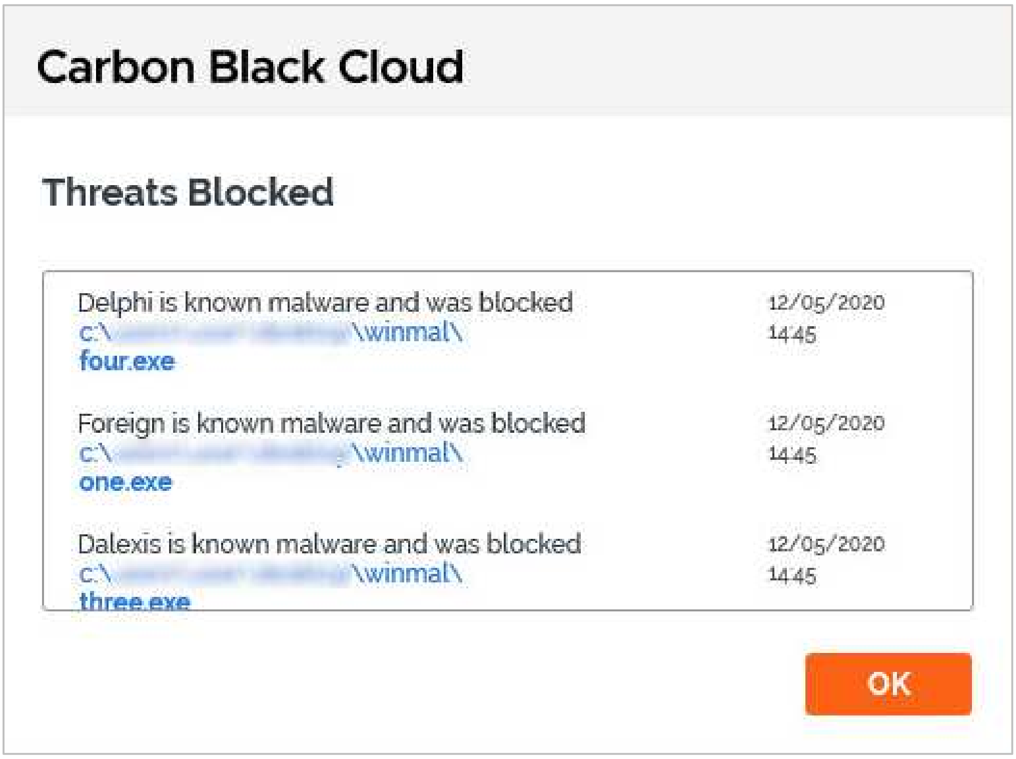
□		STATUS	DEVICE NAME	USER	OS	SENSOR	SIG	POLICY	T	LAST CHECK-IN	ACTIONS
□	>	✓	[redacted]	1909-64-01-01\User	Windows 10 x64	3.5.0.1545	●	Advanced		12:46:59 pm May 6, 2020	>_
□	>	✓	[redacted]	1909-64-02-01\User	Windows 10 x64	3.5.0.1545	●	Advanced		12:41:47 pm May 6, 2020	>_

The *Endpoints* page, shown above, provides an overview of devices on the network. Details are kept to a very manageable level (status, details of the OS and sensor version, policies and last check-in time), but you can easily get more information about an individual device just by clicking on its name. This will show take you to that device's *Investigate* page. A search box lets you search for a specific client in a larger network.

The *Settings* menu item lets you configure options for the console/system as a whole. These include *Users* and *Notifications*.

Windows endpoint protection software

The Windows desktop protection software has a minimalist interface. You can display a list of the most recent blocked threats, by right-clicking the System Tray icon. Users cannot change any settings or run any tasks.



Carbon Black Cloud

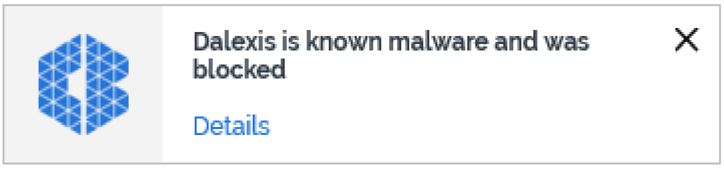
Threats Blocked

Delphi is known malware and was blocked 12/05/2020 14:45
c:\[redacted]\winmal\four.exe

Foreign is known malware and was blocked 12/05/2020 14:45
c:\[redacted]\winmal\one.exe

Dalexis is known malware and was blocked 12/05/2020 14:45
c:\[redacted]\winmal\three.exe

If the user should inadvertently copy a malicious file to their system, Carbon Black will detect it on access, and quarantine it in situ. Should the user then try to execute the file, an alert like the one below will be shown. The user cannot take any action, and the alert closes after a few seconds.



Dalexis is known malware and was blocked

The GUI of the server protection software is identical to that of its desktop counterpart.

Features (as of June 2020)	Acronis Cyber Protect Cloud Advanced Edition	Avast Business Antivirus Pro Plus	Bitdefender Endpoint Security Elite (GravityZone Elite HD)	Cisco AMP for Endpoints	CrowdStrike Falcon Pro	Cybereason Defene Platform Enterprise	Elastic Endpoint Security	ESET Endpoint Protection Advanced Cloud & ESET Cloud Administrator	FireEye Endpoint Security	FortiClient with EMS, FortiSandbox & FortiEDR	G DATA AntiVirus Business	K7 Enterprise Security	Kaspersky Endpoint Security for Business Select	Microsoft Defender ATP's Antivirus with Intune	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		•		•		•	•	•	•	•	•	•	•			•	•	•	
Client software deployment methods																			
Creation of .exe or .msi installer package	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•
Email 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	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•
Detection notifications are shown on the client	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•
Right-click on-demand scan of files/folders		•	•	•				•		•	•	•	•		•	•	•	•	
Protection settings are enabled by default (out-of-the-box-protection)		•	•	•	•	•	•	•			•	•	•	•	•	•	•	•	•
Can clean-up a previously infected system (incl. registry leftovers and inactive malware)		•	•			•		•	•	•	•	•	•	•	•	•		•	•
The online malware detection rate is the same as offline	•		•	•	•		•	•	•		•	•					•	•	•
Scans files only on execution (by default/design)					•														
Web access control / webfilter (custom blacklisting of URLs / site categories)	•	•	•	•		•		•		•	•	•	•	•	•	•		•	
Phishing protection (blocking of phishing URLs)	•	•	•					•		•	•	•	•	•	•	•		•	
Firewall		•	•	•		•		•				•	•	•	•	•		•	
Anti-Spam		•	•					•						•	•	•		•	
Data or Email encryption	•		•					•								•			
Data backup	•							•											
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, Herbrew	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	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	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	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, 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	English, Spanish				
Pricing (based on LIST PRICES as of June 2020; 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	Average	Average	Average	High	High	Very high	Average	Low	High	Very high	N/A	Low	Average	Very High	Average	Average	High	Average	High
On-premise Windows-based console	N/A		N/A	Very High	N/A						Low			N/A	N/A				N/A

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
(July 2020)