Independent Tests of
Anti-Virus Software

Business Security Test

TEST PERIOD: AUGUST – NOVEMBER 2021
LAST REVISION: 10TH DECEMBER 2021

WWW.AV-COMPARATIVES.ORG

Content

Introduction

This is the second half-year report of our Business Main-Test Series[1] of 2021, containing the results of the Business Real-World Protection Test (August-November), Business Malware Protection Test (September), Business Performance Test (November), as well as the Product Reviews.

The test series consists of three main parts:

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

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

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

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

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

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

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

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

Tested Products

The following business products[2] were tested under Microsoft Windows 10 64-bit:

Vendor	Product	Version August	Version September	Version October	Version November
Acronis	Cyber Protect Cloud with Advanced Security pack	15.0	15.0	15.0	15.0
Avast	Business Antivirus Pro Plus	21.4	21.6	21.8	21.9
Bitdefender	GravityZone Elite	7.2	7.2	7.3	7.3
Cisco	Secure Endpoint Essentials	7.4	7.4	7.4	7.5
CrowdStrike	Falcon Pro	6.26	6.28	6.29	6.31
Cybereason	Enterprise	20.2	20.2	20.2	20.2
Elastic	Security	7.13	7.13	7.15	7.15
ESET	PROTECT Entry with ESET PROTECT Cloud	8.0	8.0	8.0	8.1
FireEye	Endpoint Security	33.46	33.46	33.46	34.28
Fortinet	FortiClient with EMS, FortiSandbox & FortiEDR	6.4	6.4	6.4	6.4
G Data	Endpoint Protection Business	15.1	15.1	15.1	15.1
K7	Cloud Endpoint Security Advanced	14.2	14.2	14.2	14.2
Kaspersky	Endpoint Security for Business – Select, with KSC	11.6	11.6	11.6	11.6
Malwarebytes	EDR	1.2	1.2	1.2	1.2
Microsoft	Defender Antivirus with MEM	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
VIPRE	Endpoint Cloud	12.0	12.0	12.0	12.2
VMware	Carbon Black Cloud Endpoint Standard	3.7	3.7	3.7	3.7

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). **Cisco** uses also the **ClamAV** engine. **VMware** uses the **Avira** engine (in addition to their own protection features). **G Data**'s OutbreakShield is based on **Cyren**.

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.

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):

Acronis: "Backup", "Vulnerability assessment", "Patch management" and "Data protection map" disabled.

Bitdefender: "Fileless Attack Protection", "Sandbox Analyzer" (for Applications and Documents) and "Scan SSL" enabled. "Encryption" and "Patch Management" add-ons registered and enabled. "HyperDetect" and "Device Sensor" disabled. "Update ring" changed to "Fast ring". "Web Traffic Scan" enabled for HTTP Web traffic and Incoming POP3 emails.

Cisco: "On Execute File and Process Scan" set to Active; "Exploit Prevention: Script Control" and "TETRA Deep Scan File" enabled; "Event Tracing for Windows" enabled.

CrowdStrike: everything enabled and set to maximum, i.e. "Extra Aggressive". "Sensor Visibility" for "Firmware" disabled. Uploading of "Unknown Detection-Related Executables" and "Unknown Executables" disabled.

Cybereason: "Anti-Malware" enabled; "Signatures mode" set to "Disinfect"; "Behavioral document protection" enabled; "Artificial intelligence" and "Anti-Exploit" 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: MalwareScore ("windows.advanced.malware.threshold") set to "aggressive".

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

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

Fortinet: "Sandbox analysis" (FortiSandbox) and FortiEDR enabled. “Submit files from USB Sources” disabled; “Exclude Files from Trusted Sources” for “Sandbox Detection” enabled; in “Execution Prevention”, “Suspicious Script Execution” was disabled and “Unconfirmed File Detected” was enabled; eXtended Detection (XDR) was disabled.

G Data: “BEAST Behavior Monitoring” set to “Halt program and move to quarantine”. “G DATA WebProtection” add-on for Google Chrome installed and activated.

Malwarebytes: “Expert System Algorithms”, “Block penetration testing attacks”, "Disable IE VB Scripting", "Java Malicious Inbound/outbound Shell Protection", "Earlier RTP blocking", "Enhanced sandbox protection" and "Thorough scan" enabled; “RET ROP Gadget detection” and "Malicious LoadLibrary Protection" enabled for all applications; "Protection for MessageBox Payload" enabled for MS Office; “Malwarebytes Browser Guard” Chrome extension enabled.

Microsoft: Google Chrome extension “Windows Defender Browser Protection” installed and enabled.

Sophos: “Threat Case creation” and “Web Control” disabled.

VIPRE: “DNS Traffic Filtering” and “Malicious URL Blocking for HTTPS Traffic” enabled. “Firewall” and “IDS” enabled and set to “Block With Notify”.

VMware: policy set to “Advanced”.

Avast, K7, Kaspersky, Panda: 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.

G Data uses a server-based console that will prove very familiar and straightforward for experienced Windows professionals. This could be used by the SME sector upwards.

For businesses of the same size looking for cloud-based management solutions, **Bitdefender**, **ESET, Kaspersky**, **Microsoft**, **Panda** and **Sophos** all offer strong and coherent solutions. **Acronis, Cybereason, Malwarebytes**, and **VMware** 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**, **Fortinet** and **FireEye** all offer exceptionally powerful tools. How well they will fit to your organization, both how it is today and how you intend to grow it over the next five years, needs to be carefully planned. There is clearly a role here for external expertise and consultancy, both in the planning and deployment stages, and all of them will require significant amounts of training and ongoing support. However, they offer a level of capability that is entirely different to the smaller packages.

AV-Comparatives' Approved Business Product Award

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

To be certified in December 2021 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[3] on common business software, and at least 90% in the overall Real-World Protection Test (i.e. over the course of four months), with less than one hundred false alarms on any clean software/websites (and with zero false alarms on common business software). Tested products must also avoid major performance issues (impact score must be below 40) and have fixed all reported bugs in order to gain certification.

We congratulate the vendors shown below, whose products met the certification criteria, and are thus given the AV-Comparatives Approved Business Security Product Award for December 2021:

[3] Starting from 2022, products will be required to have an FP rate on non-business files below the *Remarkably High* threshold.

Real-World Protection Test (August-November)

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

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

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

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

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

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

Test Procedure

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

Lab Setup

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

Software

The tests were performed under a fully patched Microsoft Windows 10 64-bit system. The use of up-to-date third-party software and an updated Microsoft Windows 10 64-Bit makes it harder to find in-the-field exploits 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).

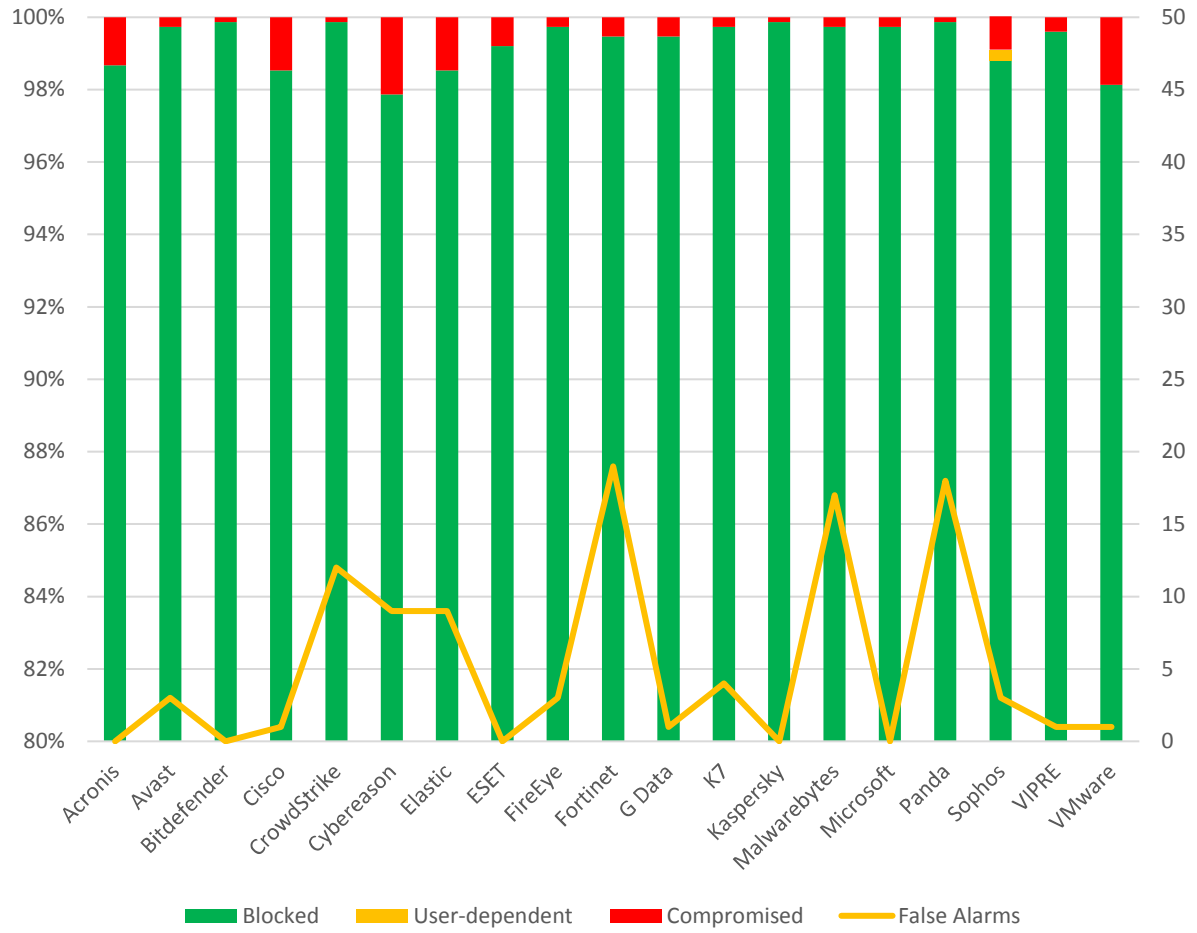
Due to the dynamic nature of the test, i.e. mimicking real-world conditions, and because of the way several different technologies (such as cloud scanners, reputation services, etc.) work, it is a matter of fact that such tests cannot be repeated or replicated in the way that e.g. static detection rate 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 **751** test cases (such as malicious URLs), tested from the beginning of August 2021 till the end of November 2021.



	Blocked	User dependent	Compromised	PROTECTION RATE [Blocked % + (User dependent %)/2][4]	False Alarms
Bitdefender, Kaspersky	750	-	1	99.9%	0
CrowdStrike	750	-	1	99.9%	12
Panda	750	-	1	99.9%	18
Microsoft	749	-	2	99.7%	0
Avast, FireEye	749	-	2	99.7%	3
K7	749	-	2	99.7%	4
Malwarebytes	749	-	2	99.7%	17
VIPRE	748	-	3	99.6%	1
G Data	747	-	4	99.5%	1
Fortinet	747	-	4	99.5%	19
ESET	745	-	6	99.2%	0
Sophos	740	4	7	98.8%	3
Acronis	741	-	10	98.7%	0
Cisco	740	-	11	98.5%	1
Elastic	740	-	11	98.5%	9
VMware	737	-	14	98.1%	1
Cybereason	735	-	16	97.9%	8

[4] 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 less-popular/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 affect 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.

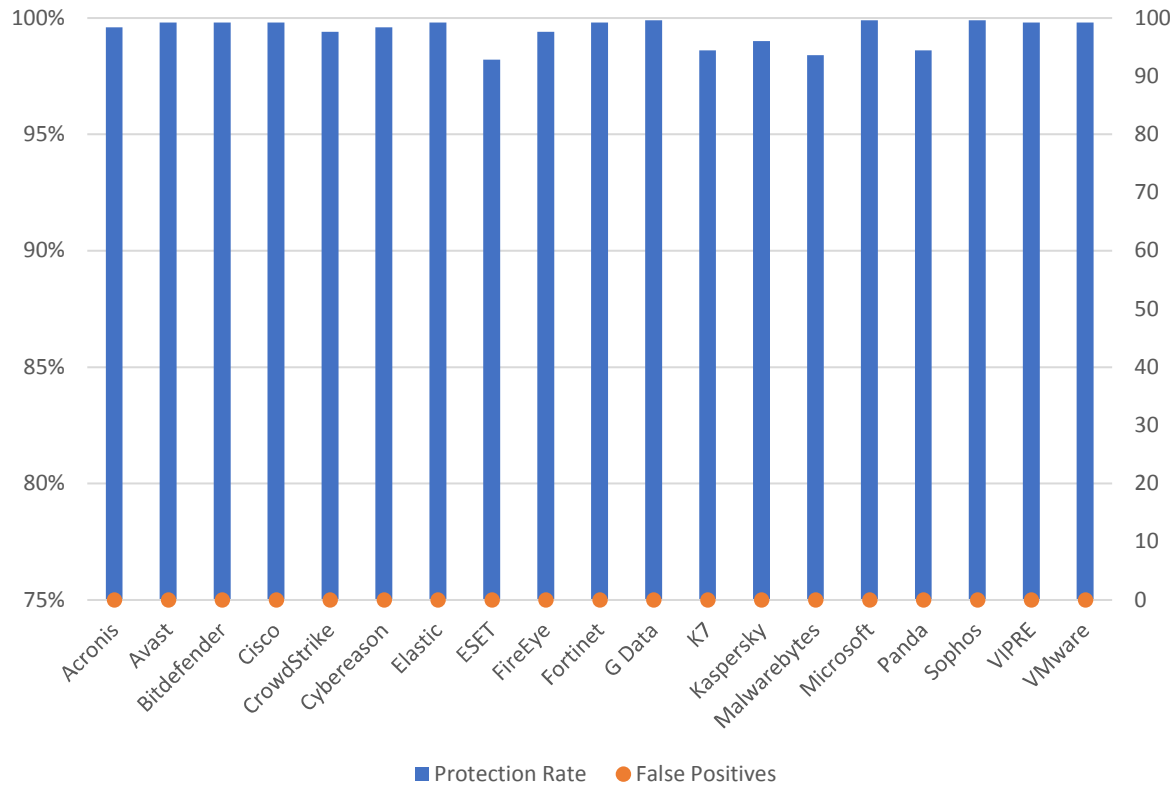
Cybereason, Elastic, CrowdStrike, Malwarebytes, Panda and **Fortinet** had above-average numbers of FPs (on non-business software) in the Real-World Protection Test.

Malware Protection Test (September)

The Malware Protection Test assesses a security program's ability to protect a system against infection by malicious files before, during or after execution. The methodology used for each product tested is as follows. Prior to execution, all the test samples are subjected to on-access scans (if this feature is available) by the security program (e.g. while copying the files over the network). Any samples that have not been detected by the on-access scanner are then executed on the test system, with Internet/cloud access available, to allow e.g. 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, **1,016** recent malware samples were used.

False positive (false alarm) test with common business software

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



	Malware Protection Rate	False Alarms on common business software
G Data, Microsoft, Sophos	99.9%	0
Avast, Bitdefender, Cisco, Elastic, Fortinet, VIPRE, VMware	99.8%	0
Acronis, Cybereason	99.6%	0
CrowdStrike, FireEye	99.4%	0
Kaspersky	99.0%	0
K7, Panda	98.6%	0
Malwarebytes	98.4%	0
ESET	98.2%	0

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

FP rate	Number of FPs on non-business software
Very Low	0-5
Low	6-15
Medium/Average	16-35
High	36-80
Very High	81-125
Remarkably High	>125

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

It should be noted that Cybereason and Fortinet had *Remarkably High* levels of false positives on non-business software. Administrators should consider whether this might create problems in their organisation's specific environments. Starting from 2022, products will be required to have an FP rate on non-business files below the *Remarkably High* threshold in order to be approved. This is to ensure that tested products do not achieve higher protection scores by using excessively restrictive settings that can cause very high levels of false positives.

Performance Test (November)

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

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

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

Test methods

The tests were performed on an Intel Core i7 CPU system with 8GB of RAM and SSD system drives. We consider this machine configuration as "**high-end**". The performance tests were done on a clean Windows 10 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[5] 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).

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

Test cases

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

File copying: We copied a set of various common file types from one physical hard disk to another physical hard disk. Some anti-virus products might 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 applications: We installed several common applications with the silent install mode 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 webserver on the Internet.

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 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								
Malwarebytes								
Microsoft								
Panda								
Sophos								
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[6] testing suite. Users using PC Mark 10 benchmark[7] 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[8].

"No security software" is tested on a baseline[9] system without any security software installed, which scores 100 points in the PC Mark 10 benchmark.

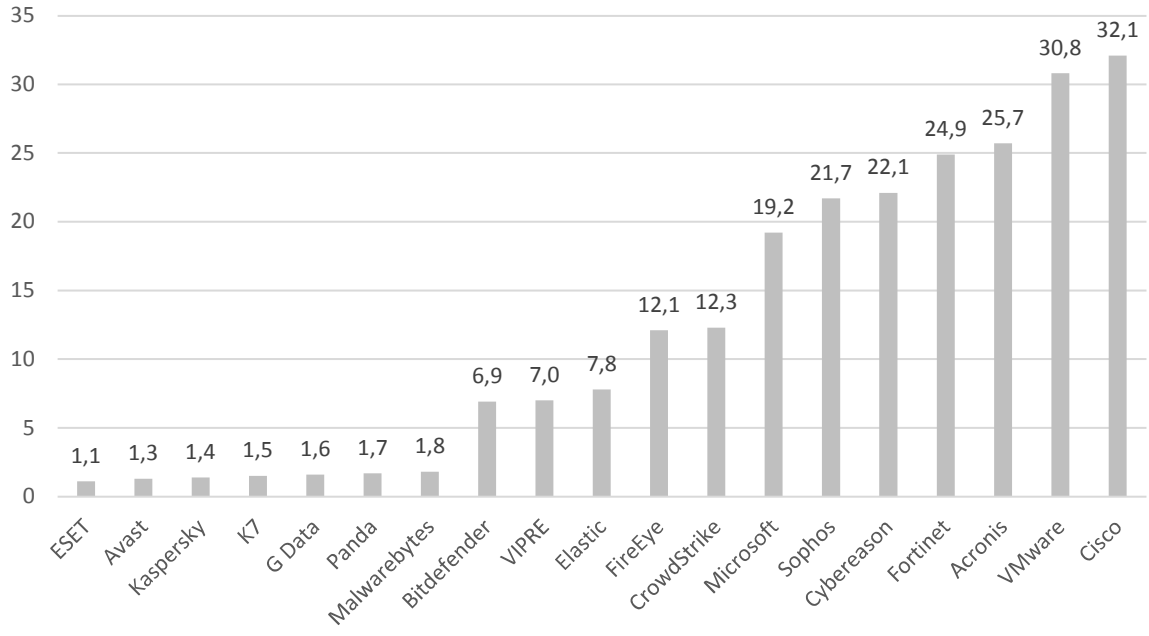
	PC Mark Score
Baseline	*100*
ESET	98.9
Avast	98.7
Kaspersky	98.6
K7	98.5
G Data	98.4
Panda	98.3
Malwarebytes	98.2
Bitdefender	98.1
VIPRE	98.0
Cybereason, FireEye	97.9
Microsoft	97.8
CrowdStrike	97.7
Elastic	97.2
VMware	96.2
Fortinet	95.1
Acronis	94.3
Sophos	93.3
Cisco	92.9

[6] For more information, see https://benchmarks.ul.com
[7] PC Mark® is a registered trademark of Futuremark Corporation / UL.
[8] http://s3.amazonaws.com/download-aws.futuremark.com/PCMark_10_Technical_Guide.pdf (PDF)
[9] Baseline system: Intel Core i7 machine with 8GB RAM and SSD drive

Summarized results

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

	AV-C Score	PC Mark Score	TOTAL	Impact Score
ESET	90	98.9	188.9	1.1
Avast	90	98.7	188.7	1.3
Kaspersky	90	98.6	188.6	1.4
K7	90	98.5	188.5	1.5
G Data	90	98.4	188.4	1.6
Panda	90	98.3	188.3	1.7
Malwarebytes	90	98.2	188.2	1.8
Bitdefender	85	98.1	183.1	6.9
VIPRE	85	98.0	183.0	7.0
Elastic	85	97.2	182.2	7.8
FireEye	80	97.9	177.9	12.1
CrowdStrike	80	97.7	177.7	12.3
Microsoft	73	97.8	170.8	19.2
Sophos	75	93.3	168.3	21.7
Cybereason	70	97.9	167.9	22.1
Fortinet	70	95.1	165.1	24.9
Acronis	70	94.3	164.3	25.7
VMware	63	96.2	159.2	30.8
Cisco	65	92.9	157.9	32.1



Reviews

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

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

We first look at the type of product, i.e. whether the console is cloud based or server based, and what sort of devices/operating systems can be protected and managed. We note that some products provide a choice of cloud-based and server-based consoles, although only one of these will be described in the review. We have only considered Windows systems in the review; macOS, Linux and mobile device support is in the feature list.

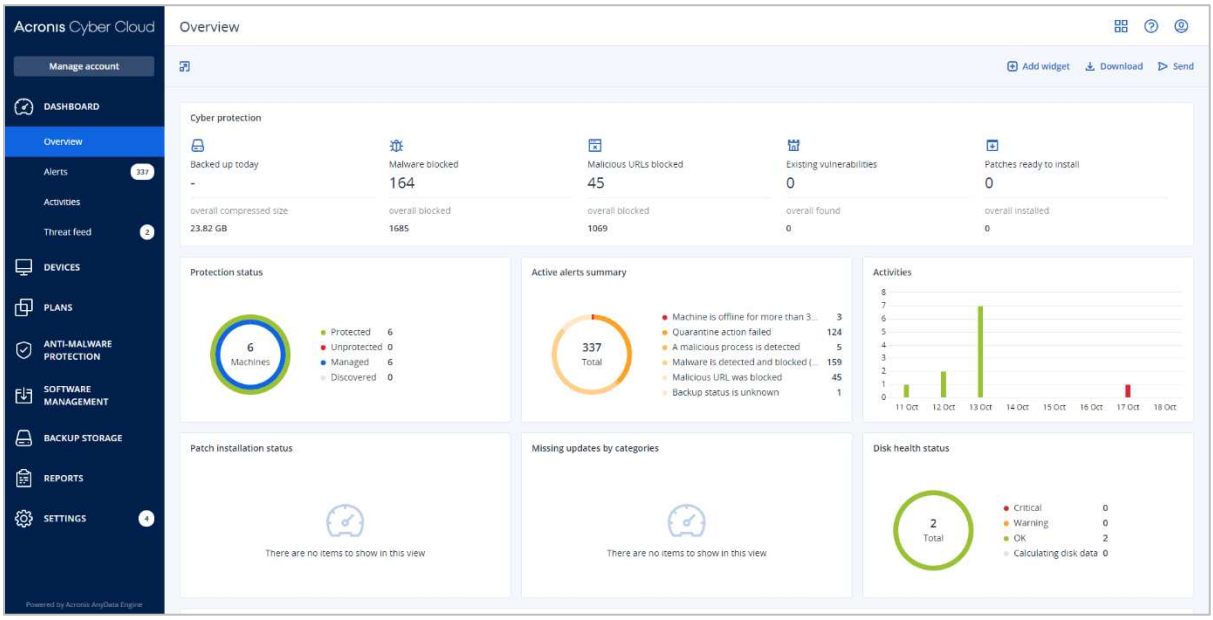
For server-based products, we describe the process of getting the console installed on the server (this is obviously not applicable to cloud-based consoles).

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

The next section looks at the endpoint protection software for client PCs. First we consider how this can be deployed. Next, we consider whether the endpoint user can perform any tasks such as scans and updates themselves, or whether such tasks are controlled exclusively by the administrator using the central management console.

We also perform a brief functionality check. This involves connecting a USB flash drive containing a few malware samples to a PC with the product installed, and attempting to copy the malicious files to the Windows Desktop and then execute them. We note whether the product prompts the user to scan the USB device when it is connected, at which stage of the copy process the malware is detected, and what sort of alert is shown.

Acronis Cyber Protect Cloud with Advanced Security pack



Advantages

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

About the product

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

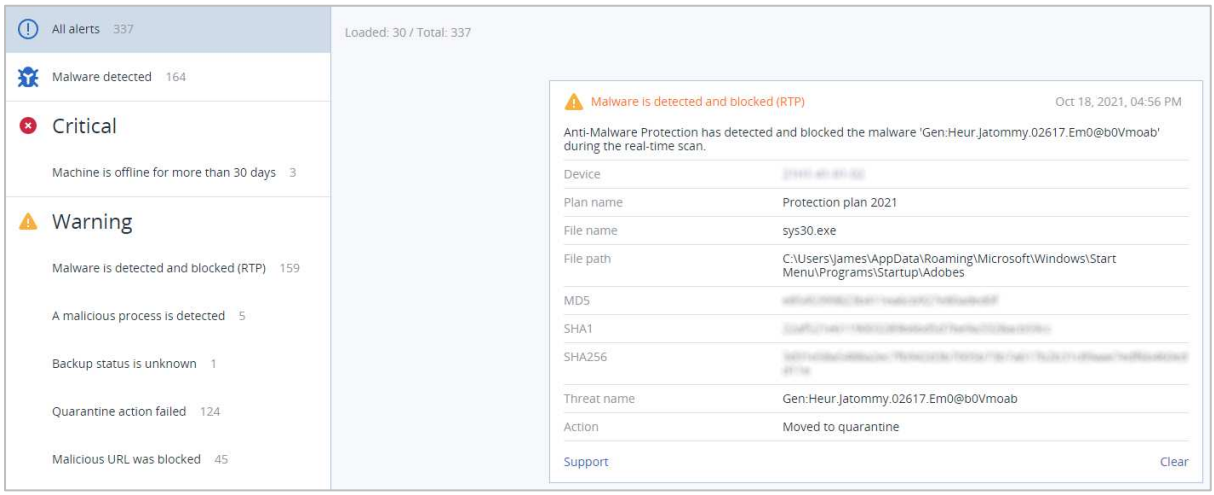
Management Console

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

Dashboard\Overview page

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

Dashboard\Alerts page

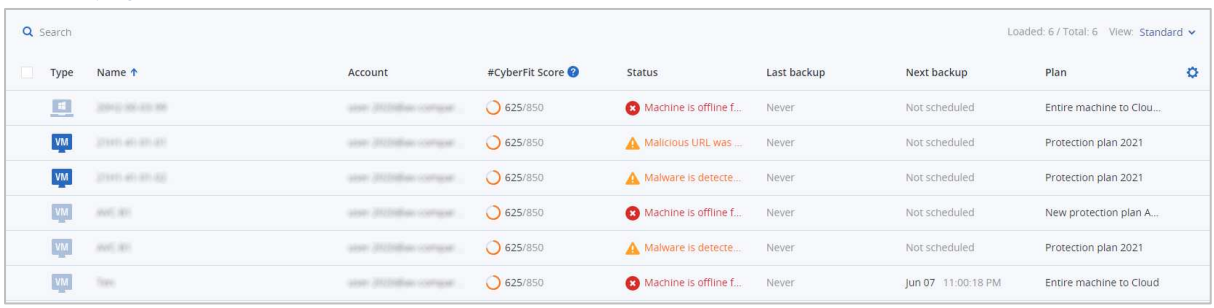


Here you can see alerts relating to malware detection, blocked URLs, and also the backup functions. These can be shown as a list, or as big tiles with details (as shown above). Information for malware detections includes the device, protection policy, file name and path, file hashes, threat name and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

Dashboard/Threat feed page

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

Devices page



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

Plans page

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

Anti-Malware Protection\Quarantine page

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

Anti-Malware Protection\Whitelist page

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

Software Management pages

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

Reports page

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

Settings pages

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

Windows Endpoint Protection Client

Deployment

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

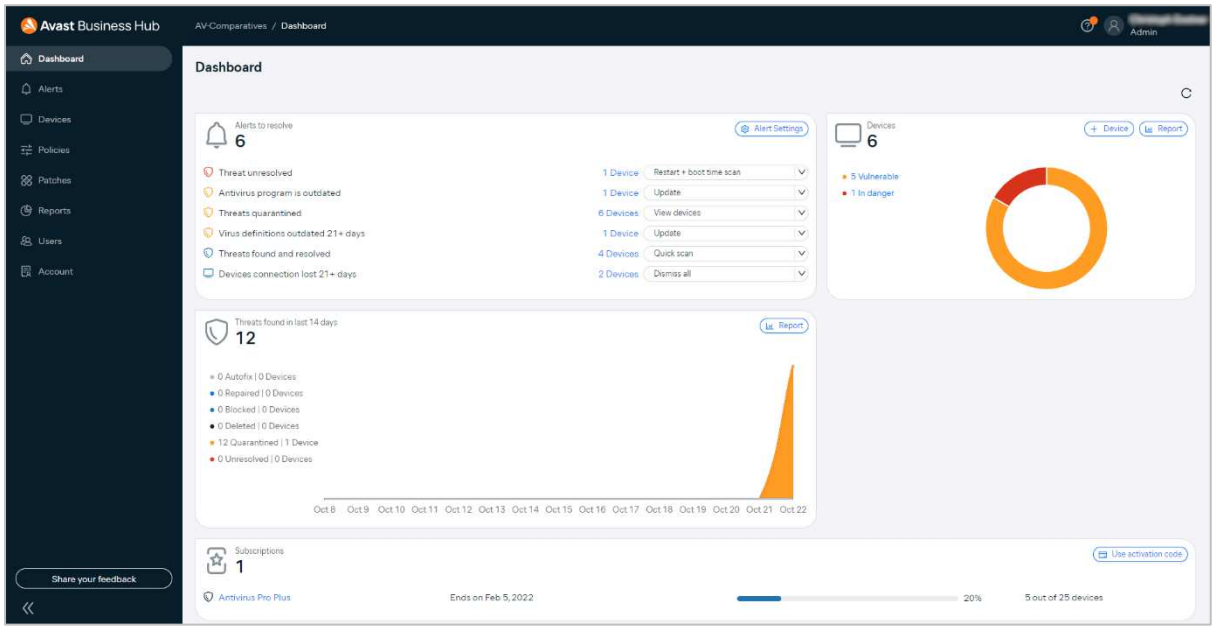
User interface

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

Malware detection scenario

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

Avast Business Antivirus Pro Plus



About the product

Avast Business Antivirus Pro Plus provides a cloud-based console for managing the endpoint protection software. Additional features for Windows clients include data shredding, a VPN, and data & identity protection. Exchange and SharePoint security are provided for Windows Server. Patch management is included for all Windows computers, although automatic installation of patches requires a separate licence for Avast Business Patch Management. This review considers only the malware protection features. The product can manage networks with thousands of devices. However, due to its ease of use, we feel it would also be suitable for small businesses without dedicated IT support staff.

Advantages

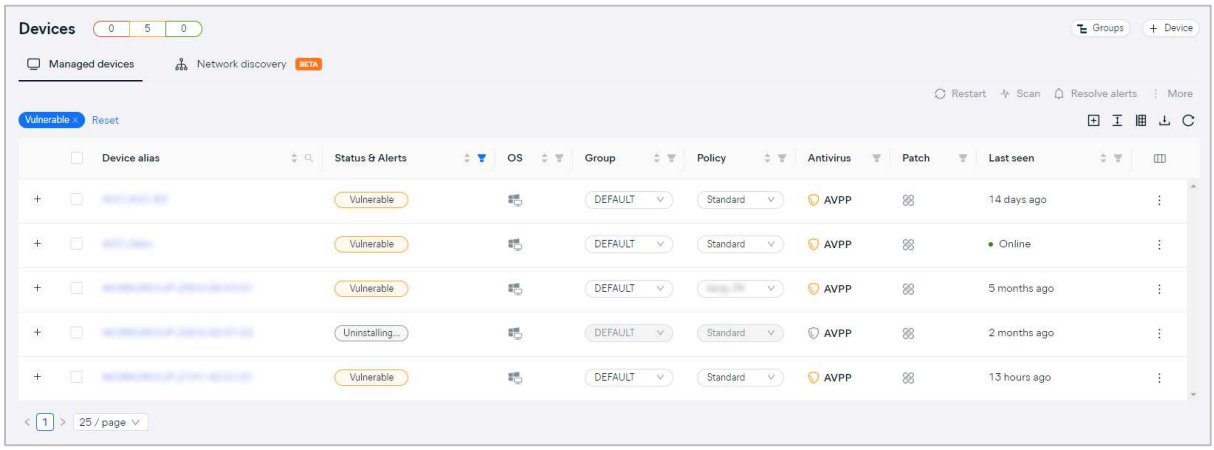
- Well suited to small and medium businesses
- Console is easy to navigate and meets accessibility standards
- One-click remediation options provided on dashboard
- Network scan feature lets you easily discover unmanaged devices
- Includes anti-spam, data shredding, a VPN, and data & identity protection

Management console

Dashboard page

The default Dashboard page provides an overview of the current security status. You can see alerts to resolve, threat detection statistics, number of devices in safe/vulnerable/dangerous states, and subscription information. Mousing over any of the graphics displays a coloured summary information box for that item. The *Alerts to resolve* panel makes it particularly convenient to see and resolve any outstanding risks. There is a list of alert types, such as *Threats unresolved* and *Antivirus program is outdated*. For each alert type, there is a corresponding suggested action, e.g. *Restart + boot time scan* or *Update* – the default can be changed from a drop-down list. Having selected the desired action, you just need to click on its text to execute it. Thus it is extremely easy to see and resolve any security issues on your network.

Devices\Managed devices page

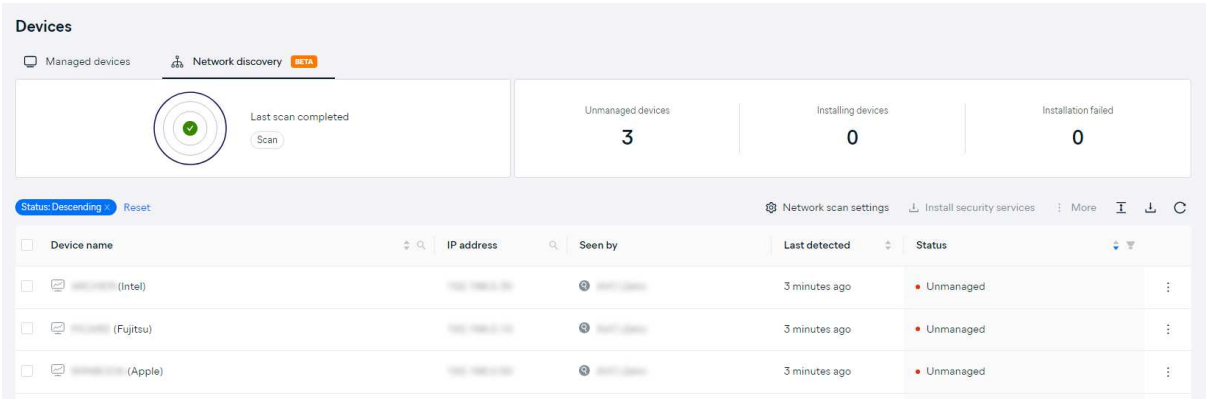


The *Managed devices* tab shows each device's status and alerts, OS, group membership and policy, along with security product installed, patch status, and last-seen date. Using the buttons and menus in the top right-hand corner, you can run various tasks on selected computers, such as restarting, scanning, resolving alerts and changing group membership or policy. The *Groups* button lets you create new groups, to which policies can be assigned. The three boxes in the top left-hand corner of the page show the number of devices with red, amber and green status, thus providing an overview of how many need attention.

Device details pane

Clicking on a device's name in the *Devices* page opens up the details pane for that device. Here you can see a wide variety of information, including precise OS version, AV program version, AV definitions version, management agent version, internal and external IP addresses, MAC address and domain membership. Additional tabs let you check on product subscription status, threats encountered, and management tasks (both pending and completed).

Devices\Network discovery page



From this page, you can scan your local area network or Active Directory Domain for computers that are not yet managed or protected by Avast. This involves designating a currently managed device to act as a scanning agent, which is very quick and easy to set up. You then just need to click *Scan*, and in a few moments, you will see a list of unmanaged devices. When we tried this out on our test LAN, all the Windows computers and even other network devices, such as routers and printers, were detected. You can deploy the endpoint protection software to manageable devices directly from the *Network Discovery* page.

Policies page

Here you can configure the protection settings for your devices. Small graphics next to each control indicate which operating systems (Windows clients, Windows servers, macOS) that item applies to. You can configure a wide range of settings in each policy. There are sections for *General Settings* (including updates, troubleshooting and restart options); *Service Settings* (antivirus, patch management and firewall); *Exclusions* (for antivirus and patch management); and *Assignments* (devices to which the policy is applied).

Reports page

There are six different report categories for Business Antivirus Pro Plus: *Executive Summary, Device Report, Tasks Report, Antivirus Threats Report, Patch Report,* and *Remote Control 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 repaired, blocked, deleted, quarantined, or unresolved over the last month. You can create reports on a weekly or monthly schedule, and view scheduled reports already created.

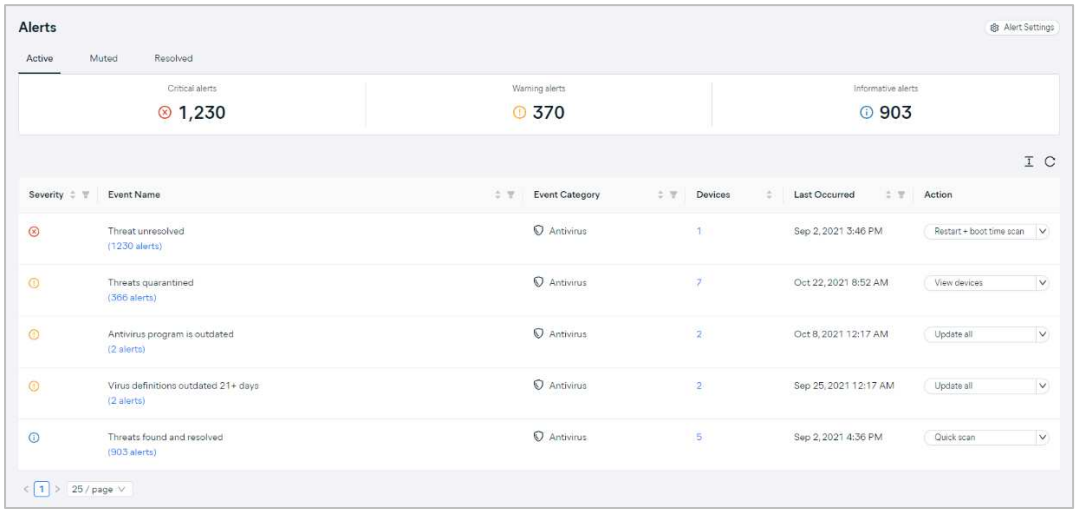
Users page

Here you can manage console users. There are two levels of permissions, which are essentially full control and read only.

Account\Subscriptions page

As you would expect, this shows you the product licences you currently have, how many of them you have used, and when they expire.

Alerts page



This shows important alerts (from various different sources) such as malware detections, and devices that are out of date or need rebooting. You can click on any alert to be taken to the relevant details page. At the end of each entry, you will find the same options for resolving the alerts that are used on the dashboard page. This drop-down list also lets you mute the alert (for all machines or specific groups) for 7, 30 or 90 days. Muted alerts are shown on a separate tab of the alerts page. A further tab lets you see resolved alerts, i.e. ones you have already dealt with. A panel along the top of the page shows the number of alerts with *Critical, Warning* and *Informative* status. Clicking the *Alert Settings* button in the top right-hand corner takes you to a configuration page, where you can choose which notifications to show in the console, and whether/how frequently to send email reminders if these have not been read.

Windows Endpoint Protection Client

Deployment

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

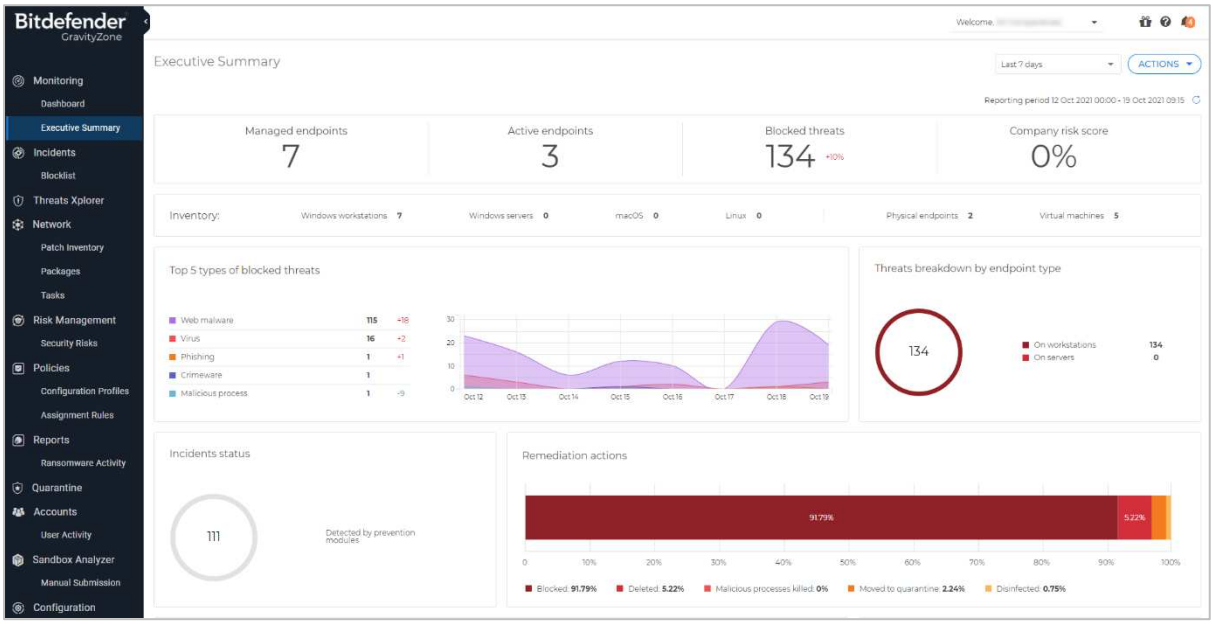
User interface

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

Malware detection scenario

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

Bitdefender GravityZone Elite



About the product

Bitdefender GravityZone Elite provides a cloud-based console for managing the endpoint protection software. The product can administer networks with thousands of devices. We feel it would also be suitable for smaller businesses with tens of seats.

Advantages

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

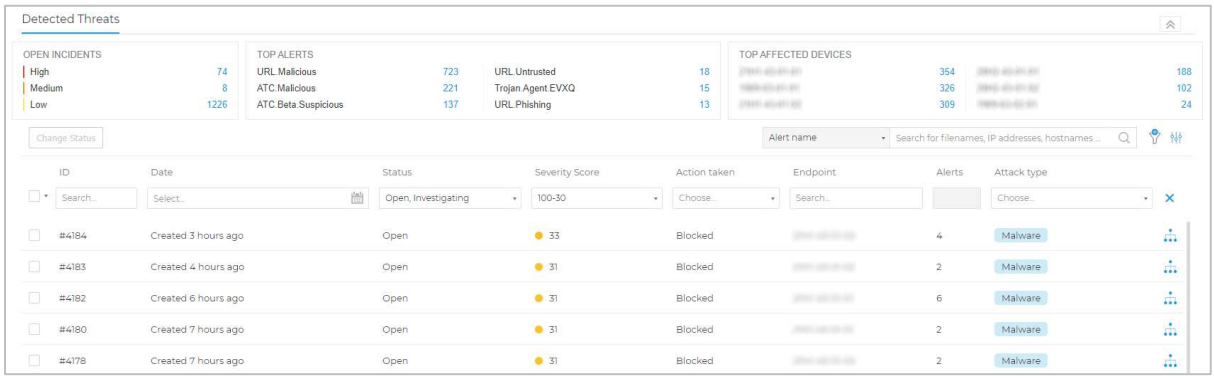
Management Console

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

Monitoring/Executive Summary page

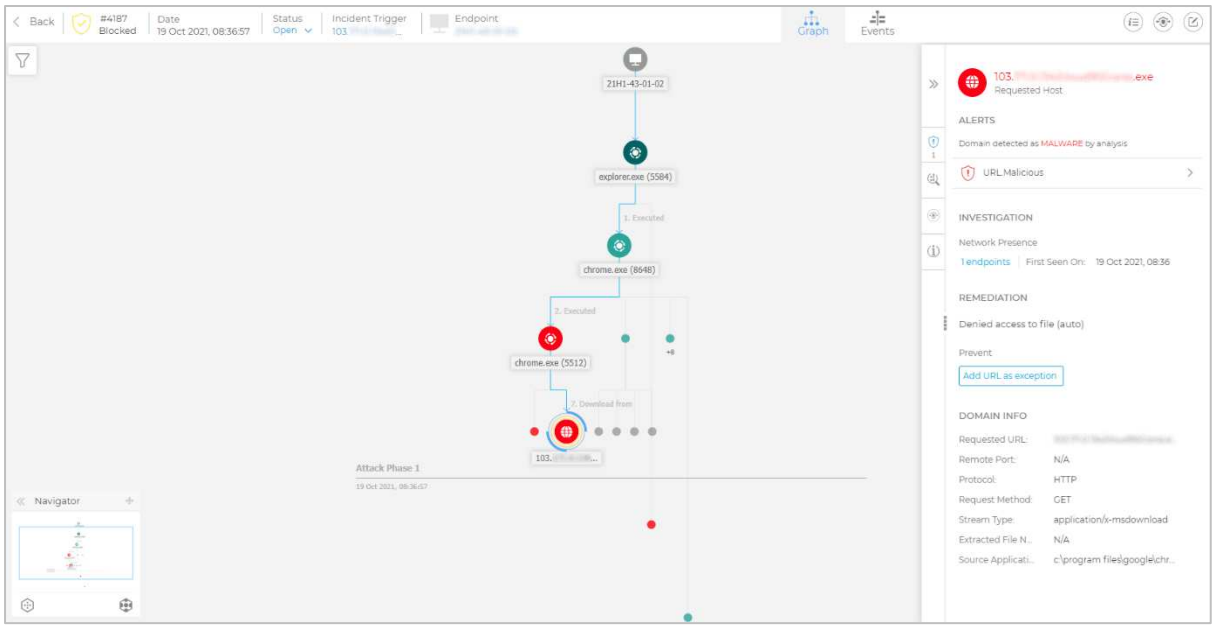
The *Executive Summary* page (screenshot above) is shown when you first open the console. It is divided up into information panels that provide an overview of managed endpoints, blocked threats, threat types, and remediation actions taken. Each information panel is clickable, so if you click on e.g. *Managed endpoints*, you will be taken to the *Network* (devices) page.

Incidents page



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

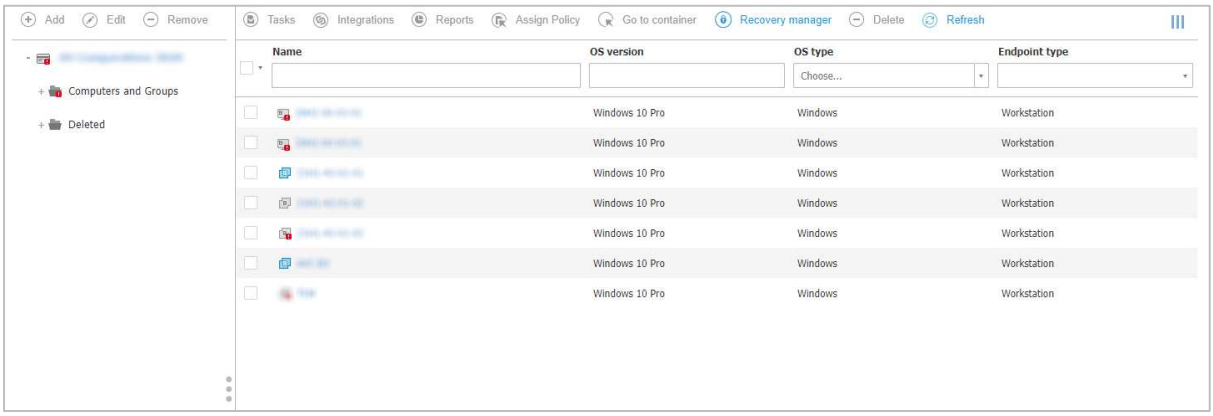
By clicking on the process-tree symbol at the right-hand end of a threat's entry, you can see a graphical representation of the threat event, along with further details such as remediation steps taken:



Threats Xplorer page

This shows a simple list of detected malware, including file name and path, action taken, device name, and day/time of detection.

Network page



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

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

Risk Management Dashboard page

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

Policies page

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

Reports page

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

Quarantine page

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

Accounts page

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

Sandbox Analyzer page

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

Configuration page

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

Notifications panel

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

Windows Endpoint Protection Client

Deployment

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

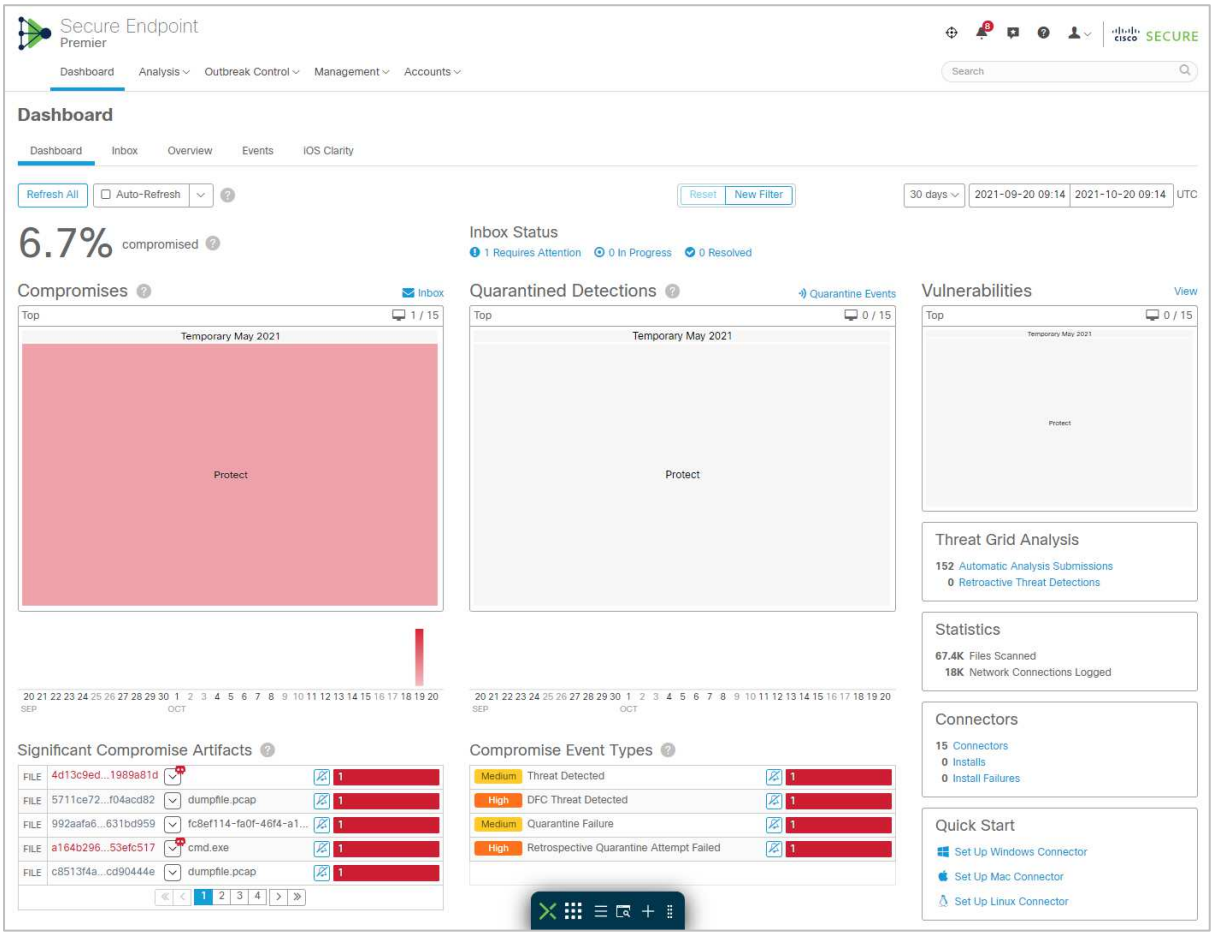
User interface

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

Malware detection scenario

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

Cisco Secure Endpoint Essentials



About the product

Cisco Secure Endpoint Essentials provides a cloud-based console for managing the endpoint protection software. In addition to malware protection, the product provides features for monitoring, investigating and blocking security threats. It can manage networks with hundreds of thousands of devices.

Advantages

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

Management Console

Dashboard tab

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

Analysis menu

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

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

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

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

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

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

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

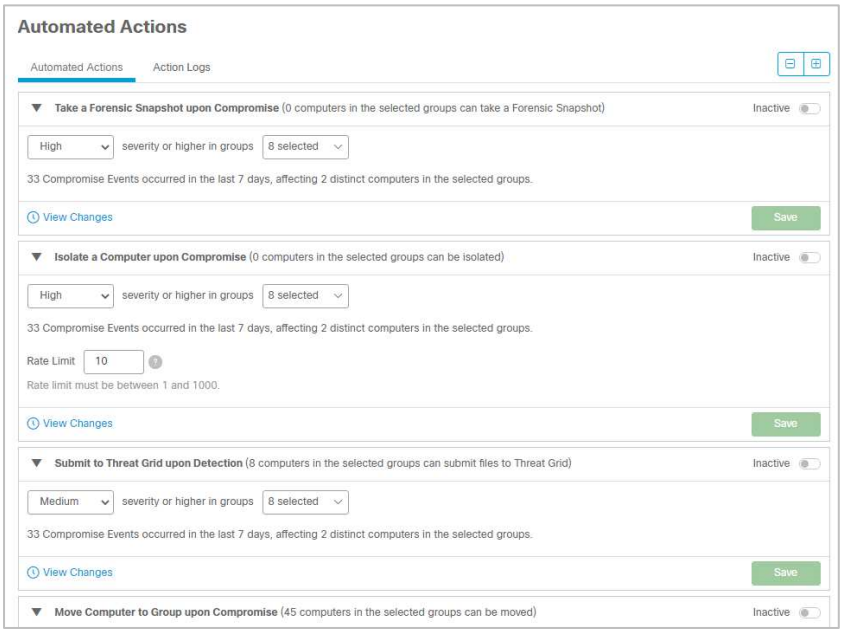
Orbital Advanced Search is a capability that lets you query endpoints for detailed information. When enabled in a policy, it automatically installs an additional module (not used on our Main Test systems). Orbital can execute queries immediately, or you can schedule them using the *Orbital Jobs* feature.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

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

Outbreak Control menu

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

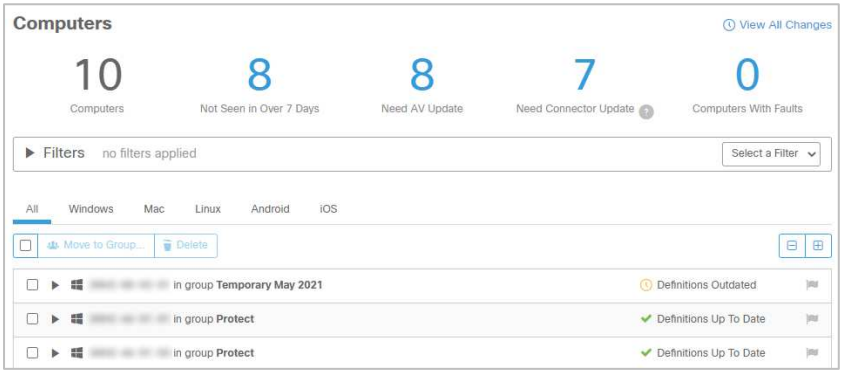
The *Automated Actions* feature (shown below) lets you set actions that automatically trigger when a specified event occurs on a computer. For example, if the computer is compromised, you can take a forensic snapshot, isolate it, move it to a specified group (or any combination of these). You can also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



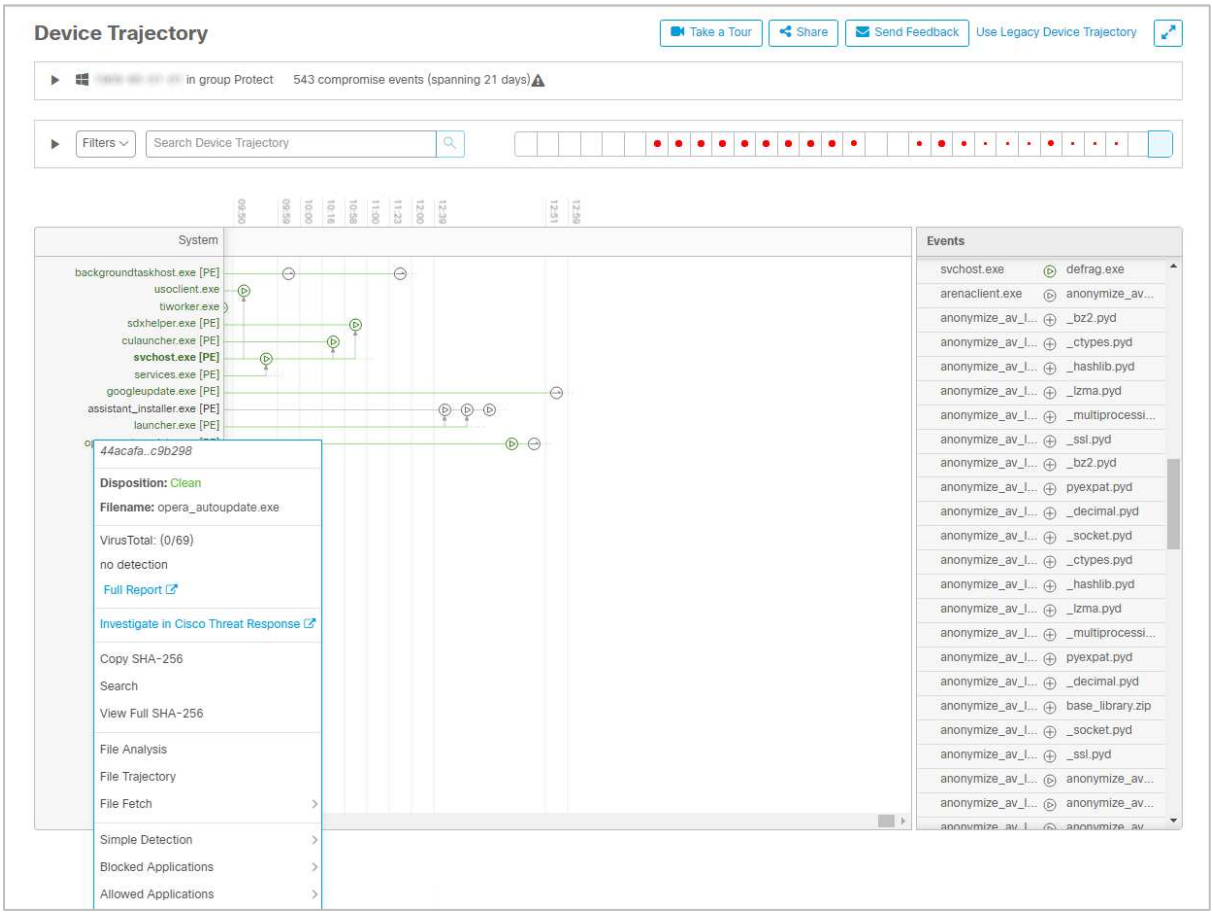
Management menu

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

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



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



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

Windows Endpoint Protection Client

Deployment

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

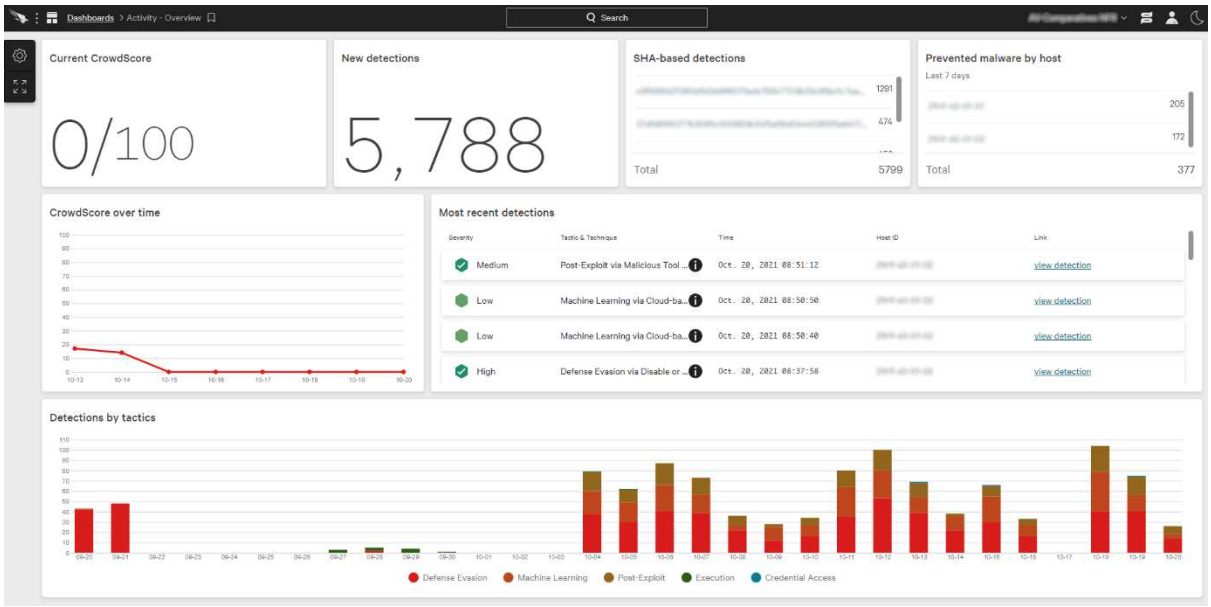
User interface

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

Malware detection scenario

When we connected a flash drive containing malware samples to our test PC, and opened the drive in Windows Explorer, Cisco initially did not take action. However, when we tried to copy the malicious files to the Windows Desktop, they were immediately detected and quarantined. No alert was shown to the end user. However, the endpoint software can be configured by policy to show detection notifications.

CrowdStrike Falcon Pro



About the product

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

Advantages

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

Management Console

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

Activity\Dashboard page

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

Activity\Detections page

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

Activity\Quarantined Files page

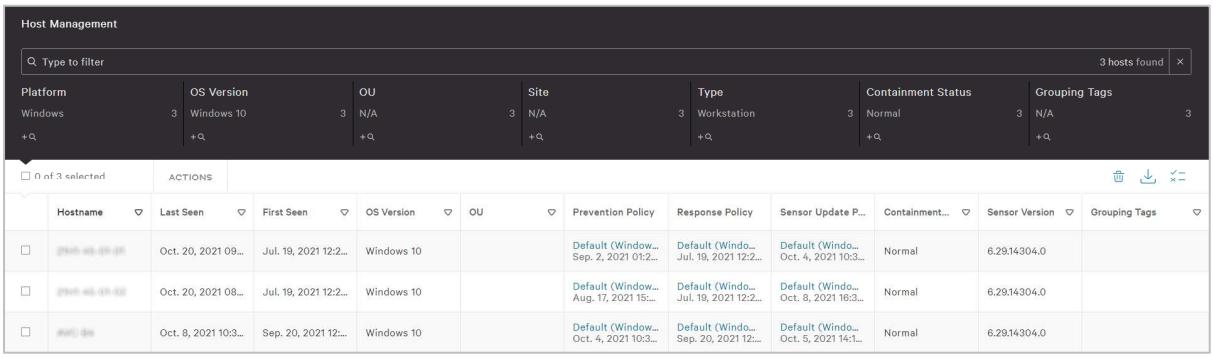
As you would expect, this page lets you see files that have been quarantined by the system. You can see the filename, device name, number of detections counted on the network, user involved, and of course date and time of detection. Quarantined files can be released or deleted. Clicking on a quarantined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

Configuration\Prevention Policies page

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

Policies can be assigned to devices automatically by means of a naming system. For example, any device with "Win" in its name can be automatically put into a specific group of Windows computers, to which a particular policy is assigned. Devices/groups can be assigned more than one policy, whereby a policy hierarchy determines which one takes precedence.

Hosts\Host Management page



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

Intelligence\Actors page

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

Investigate\Host Search page

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

Windows Endpoint Protection Client

Deployment

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

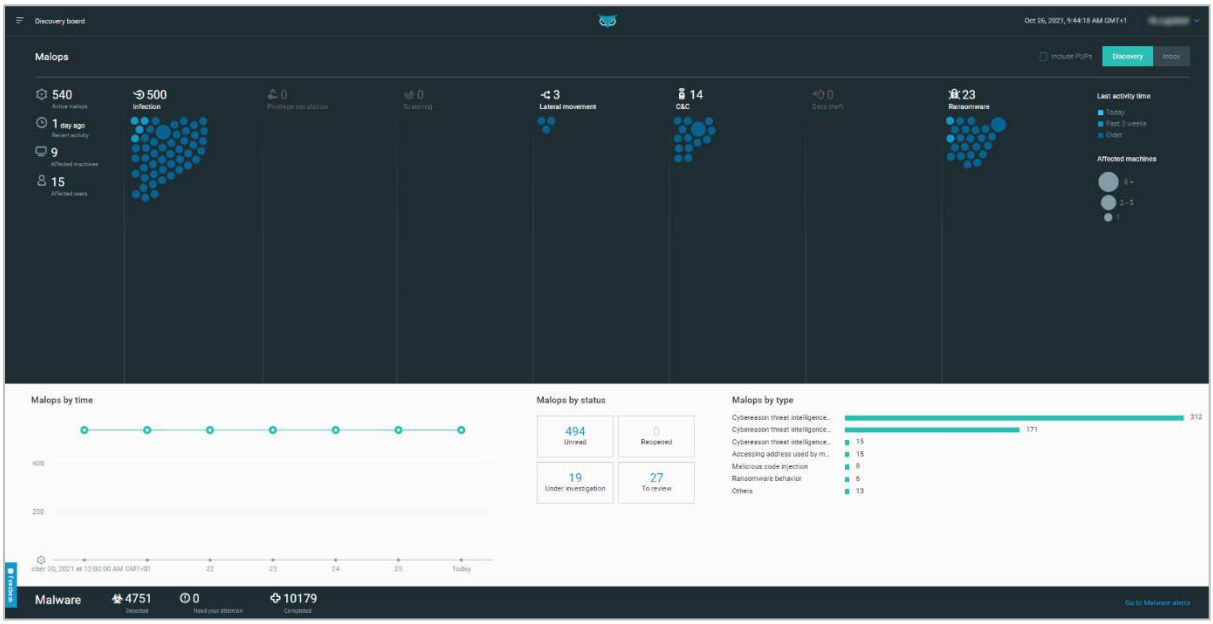
User interface

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

Malware detection scenario

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

Cybereason Enterprise



About the product

Cybereason Enterprise provides a cloud-based console for managing the endpoint protection software. In addition to malware protection, the product includes functions for analysing and remediating attacks. It can manage networks with hundreds of thousands of devices.

Advantages

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

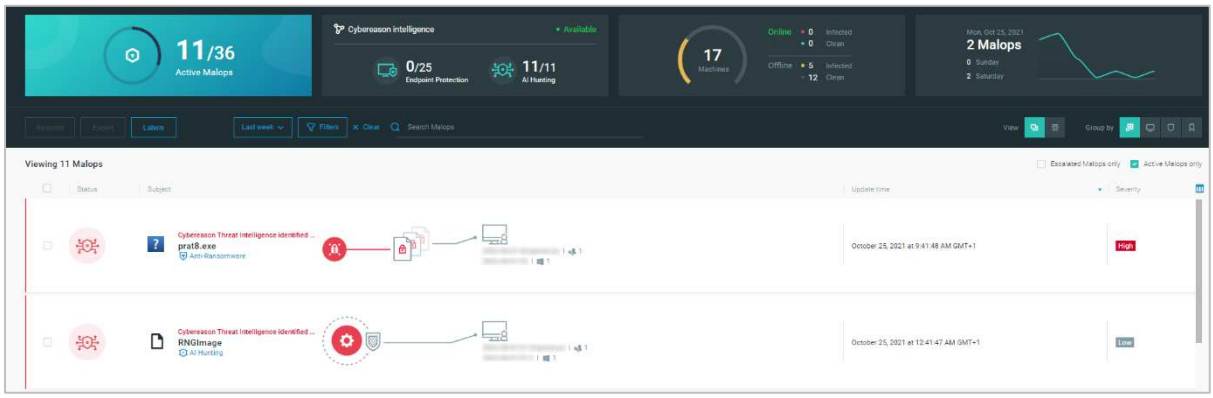
Management Console

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

Discovery board page

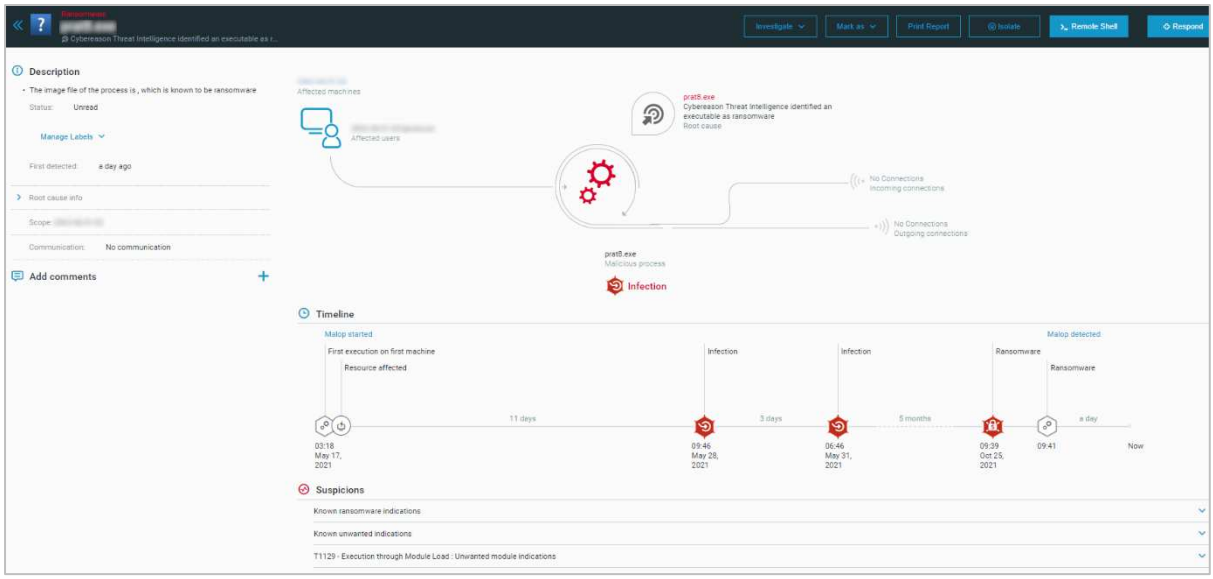
The *Discovery board* (shown in the screenshot above) is the page you will see when you first log on. It shows "Malops" (malicious operations) in columns, according to type. The blue dots represent a malicious activity. The size of the dot represents the number of the affected machines, and the shade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

Malops management page



The *Malops management* page has a number of panels that graphically illustrate the security status of the network. It also displays a list of detected malicious operations in chronological order (every alert from the Malware Alerts page is shown here). 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. There are graphics representing the root cause, and affected machines. You can filter the Malops by status, detection module, priority, OS type, machine status, user privileges and labels. You can also choose a grid view, showing more items without the graphical representation. Clicking on one of the Malops opens its details page. You can also take action on a particular Malop from this page, by selecting it and clicking the *Respond* button.

Malop details page



The *Malop details* page has an abundance of information about the Malop in question. This includes the infected device, incoming and outgoing connections to and from the process, and a timeline. Individual elements of the overview graphic and timeline are clickable, allowing you to see more details. For example, where the malicious process has used network communications, you can click on the applicable graphic in order to see the IP address of the remote computer.

The 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. Tabs at the bottom of the page let you view the Malop from the perspective of processes, network communications, machines and users. The *Processes* tab includes a reference to the applicable stage of the MITRE ATT&CK® framework. Big buttons at the top of the page let you carry out various actions to remediate the problem. These include *Investigate, Isolate* and *Respond*. The latter lets you remediate any damage done, and prevent execution of associated malicious files on other devices.

Malware alerts page

This shows warnings relating to known and unknown malware, fileless attacks, and application control. You can filter alerts using these categories. Information provided for each alert includes file name, action taken, device affected, and date/time. For each of these items, there are *Investigate* and *Exclude* buttons so you can deal with them.

Investigation page

The *Investigation* page allows you to create customised hunts for malicious activity, using criteria such as machine, user, process, file, connection, network interface and registry entry. There are also pre-built queries, allowing you to find things such as *Unsigned Services employing autostart* and *Privilege Escalation to System*.

Security profile page

Here you can configure *Reputation, Behavioral allowlisting, Custom detection rules*, and *machine isolation exceptions*.

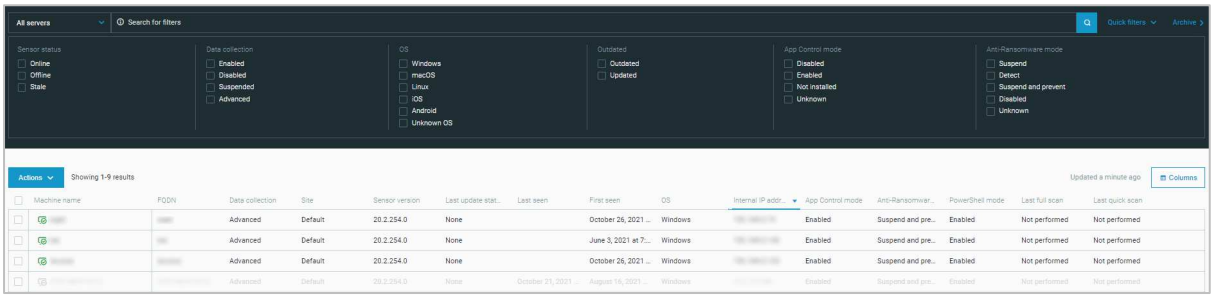
System section

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

System\Overview page

The default *Overview* page is divided into 4 panels. The *Sensors status* panel provides a doughnut chart of the status of installed devices, with a colour-coding system for *Active, Stale* and *Archived* states. The *Sensors versions* panel completes the picture by showing the proportion of up-to-date clients. The other two panels show details of the OS-type distribution and sensor activity over time.

System\Sensors page



The *System\Sensors* page displays a list of protected devices, with details such as sensor version, OS type, and IP address. We note that offline computers are shown in a very pale grey colour. 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, setting policy, setting anti-ransomware mode, and starting a system scan. A panel at the top of the page allows you to filter a long list of devices by sensor status, data collection, OS, update status, app control status and ransomware-protection status.

System\Policies management page

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

System\Detection servers page

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

System\Groups page

On this page, you can create management groups for your devices. The *Create new group* dialog lets you assign a specific policy, and add new devices to the group automatically, based on Active Directory Organizational Unit, machine name, organisation, or internal/external IP address.

Settings page

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

Support page

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

Windows Endpoint Protection Client

Deployment

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

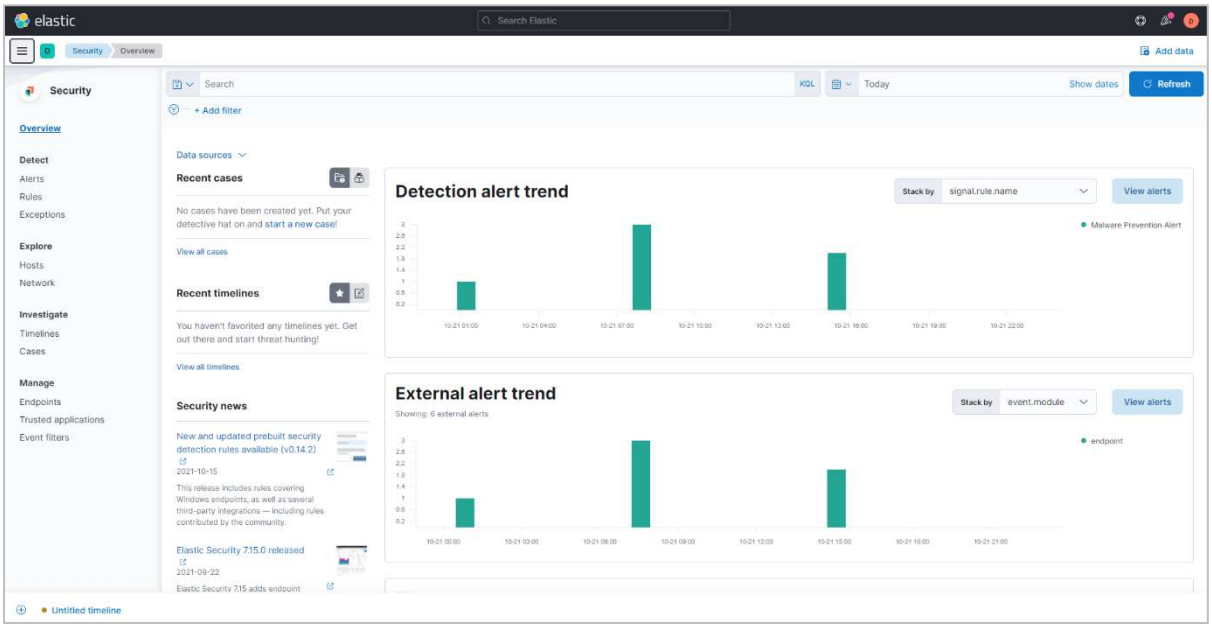
User interface

The user interface on protected endpoints consists of a System Tray icon, whose menu displays protection status, date and time of last update, date and time of last scans, signature version and program version. Users can run updates, quick scans and full scans. You can hide the interface and alerts completely by means of policy, if you so choose.

Malware detection scenario

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

Elastic Security



About the product

Elastic Security provides either a server-based or a cloud-based console for managing the endpoint protection software. We have described the latter in this review. As well as malware protection, the product includes investigative functions for analysing and remediating attacks. The product can manage networks with tens of thousands of devices.

Advantages

- Investigation functionality
- Clean and simple console design
- Detailed information on network connections is provided
- Pop-up panels quickly show details of data in graphs
- Suitable for medium- to large-sized enterprises

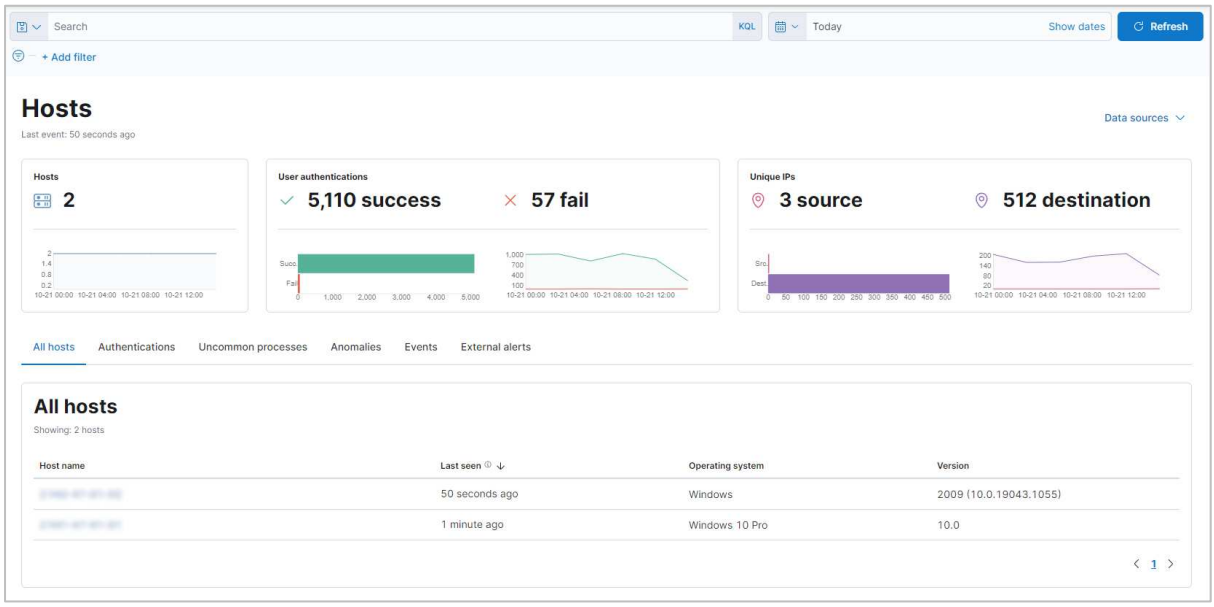
Management Console

The Elastic console as a whole provides a range of other functionality in addition to security. The security functionality is accessed (as you would expect) from the *Security* section of the main Elastic menu. In this review, we have only looked at the security-related section of the console. There is a single menu column on the left-hand side of the console, with the main categories *Overview, Detect, Explore, Investigate,* and *Manage*.

Overview page

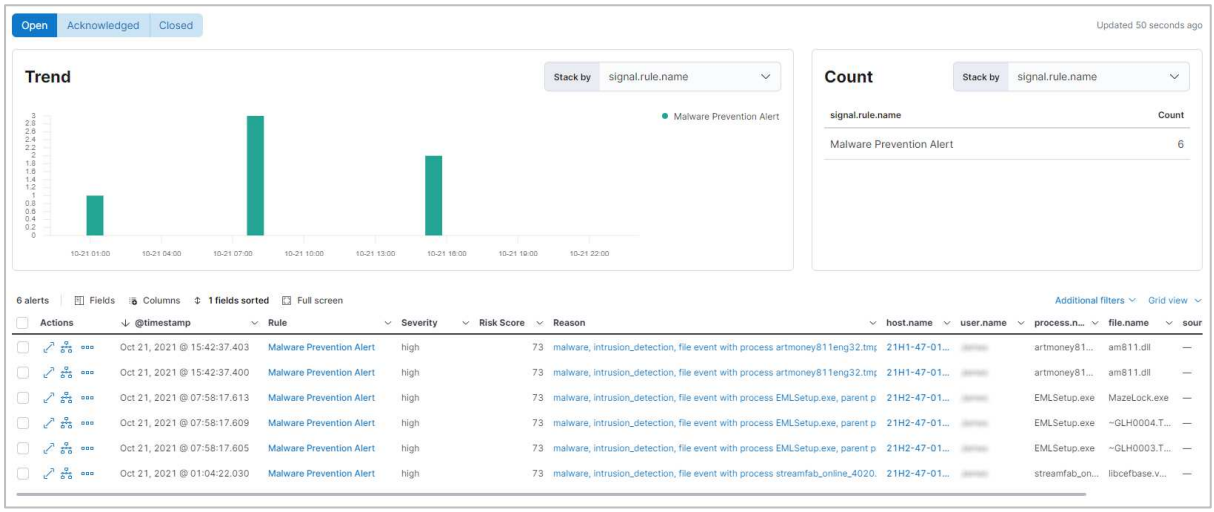
This is the page you will see when you first open the security section of the console (screenshot above). It gives you an overview of security-related events, shown in panels illustrated with bar graphs. You can see *Detection alert trend, External alert trend, Events, Host events,* and *Network events*. Mousing over one of the graphs displays a panel with detailed breakdown information for that item. A button in the top right-hand corner of each panel links to the applicable details page of the console.

Hosts page



The *Hosts* page (shown above) provides a view of active clients. You can see the device name, operating system and version. Clicking on a device's name opens up its details page. Here you can see detailed information, such as IP addresses and MAC addresses, sensor version, and authentication events.

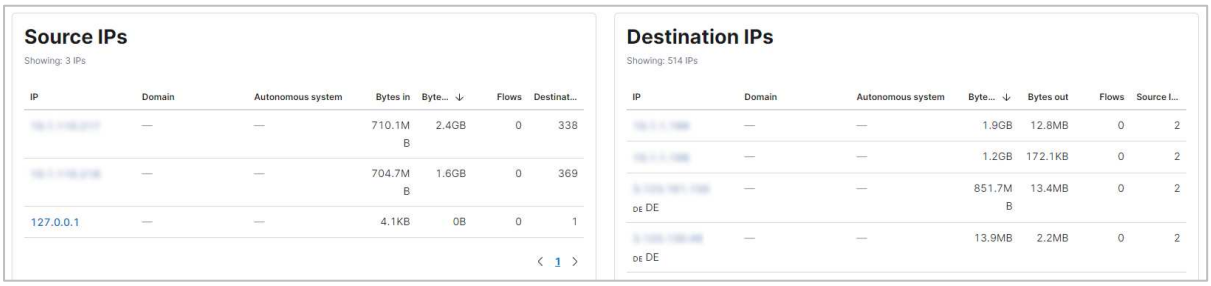
Detect/Alerts page



This provides you with a timeline of recent detection alerts, shown in 3-hour intervals. There is also a detailed panel of individual events. For each alert, the options *Mark as acknowledged* and *Mark as closed* are provided.

The *Investigate/Timelines* and *Cases* pages are only populated when an investigation has been started.

Explore/Network page



This includes a map of the world, showing the locations of servers that client PCs have connected to. Below this, there is a table showing precise details of these connections (shown above).

Manage/Trusted applications page

This lets you to add and manage whitelisted apps.

Manage/Endpoints page

This displays a complete list of all devices on the network, even those in an inactive state. Amongst other things, this page allows you to access the policies that define security settings in networked devices. These let you define key events to record for analysis, enable user notifications, and integrate with Windows Security Center, amongst other things.

Windows Endpoint Protection Client

Deployment

Deployment of the endpoint protection agent can be performed via manual installation on the endpoint, or using a systems management product or Active Directory. A zipped installation package, which includes an installer in .exe format plus some configuration files, can be downloaded using the *Add Agent* button on the *Fleet\Agents* page. The information panel that opens here also provides the PowerShell syntax needed to run the installer manually. We note that it is necessary to use the specific installer version that corresponds to the version number of the management console.

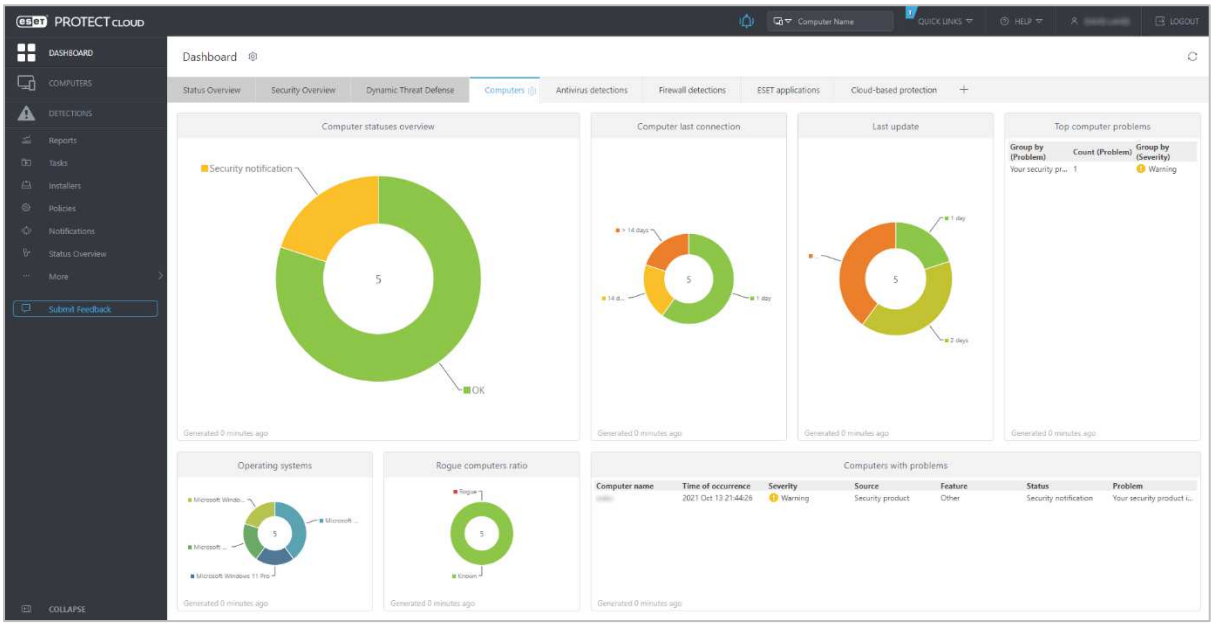
User interface

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

Malware detection scenario

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

ESET PROTECT Entry & ESET PROTECT Cloud



About the product

ESET PROTECT Entry with ESET PROTECT Cloud provides a cloud-based console for managing the endpoint protection software. We feel it would be suitable for smaller businesses with tens of seats, but it can also cope with larger networks. Please note that there is a choice of endpoint protection software for Windows clients. ESET Endpoint Antivirus is a full-featured antimalware program; ESET Endpoint Security (which was used in our tests) additionally includes additional features, such as a web control feature and ESET's Network Protection module. The package also includes ESET File Security for Windows Servers.

Advantages

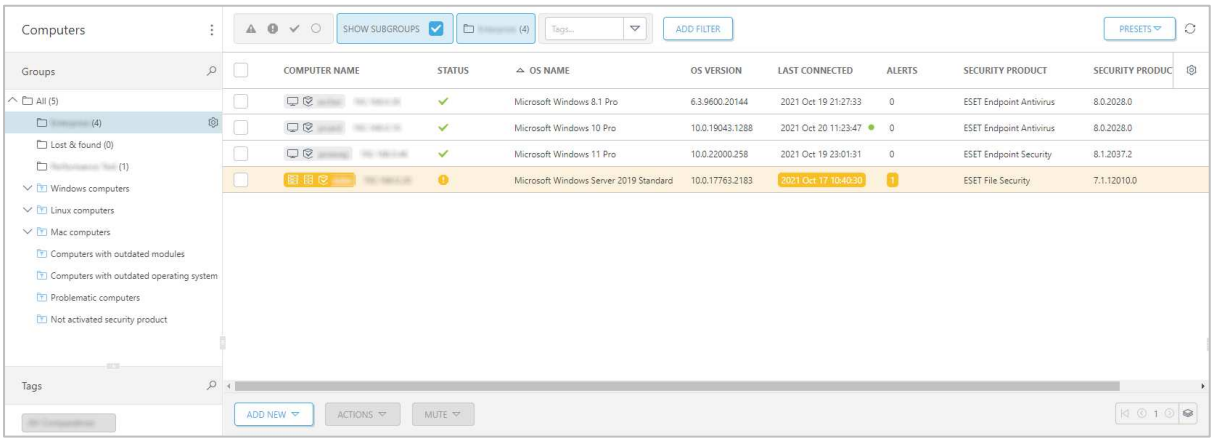
- Modern, customisable interface design
- Functionality easily accessed from a single menu column
- Clickable, interconnected console makes it easy to go to details pages
- Task automation via dynamic groups
- Choice of endpoint protection software

Management Console

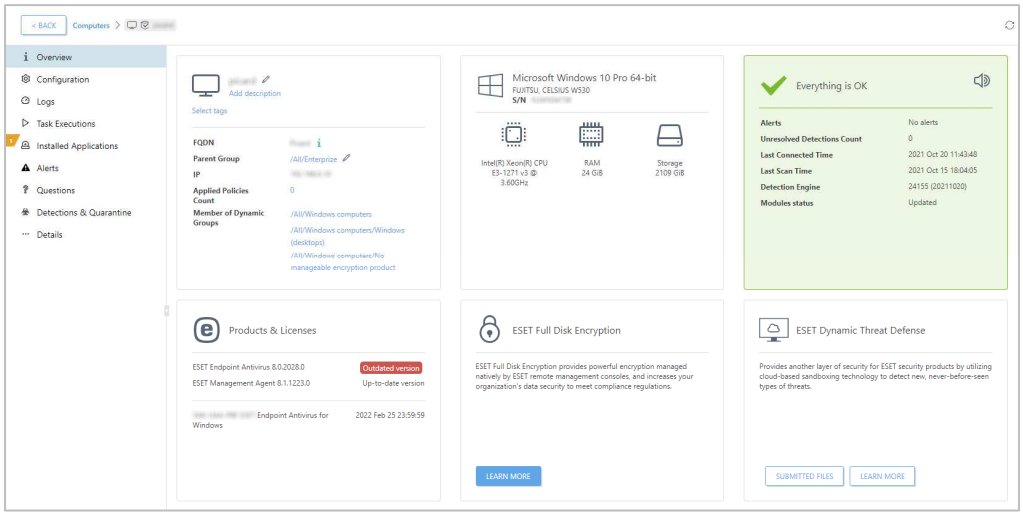
Dashboard page

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

Computers page



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



Detections page

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

Reports page

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

Tasks page

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

Policies page

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

Computer Users page

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

Installers page

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

Submitted files page

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

Quarantine page

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

Exclusions page

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

Notifications page

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

Status overview page

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

More\Audit Log page

This shows a record of actions taken by console users. You can see logins, logouts, and renaming/moving of computers, amongst other things.

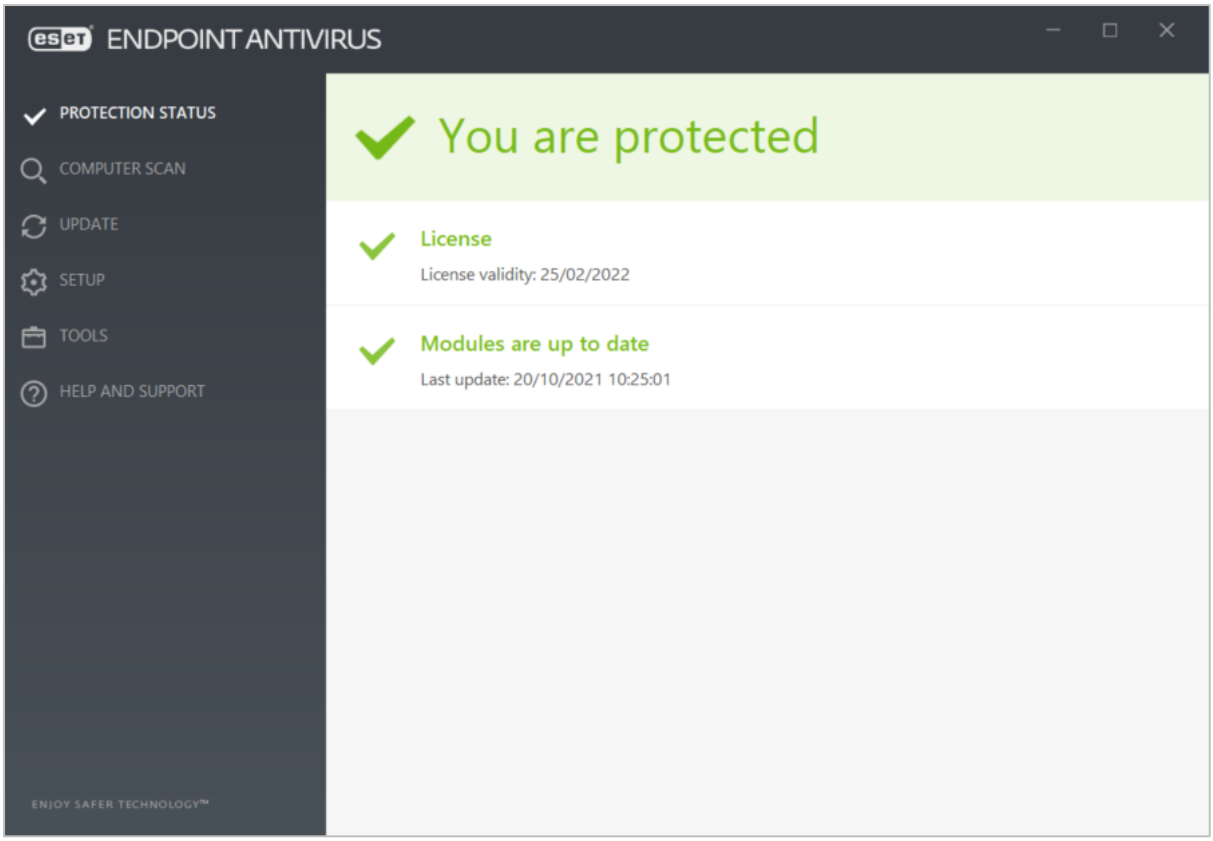
Windows Endpoint Protection Client

Deployment

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

User interface

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

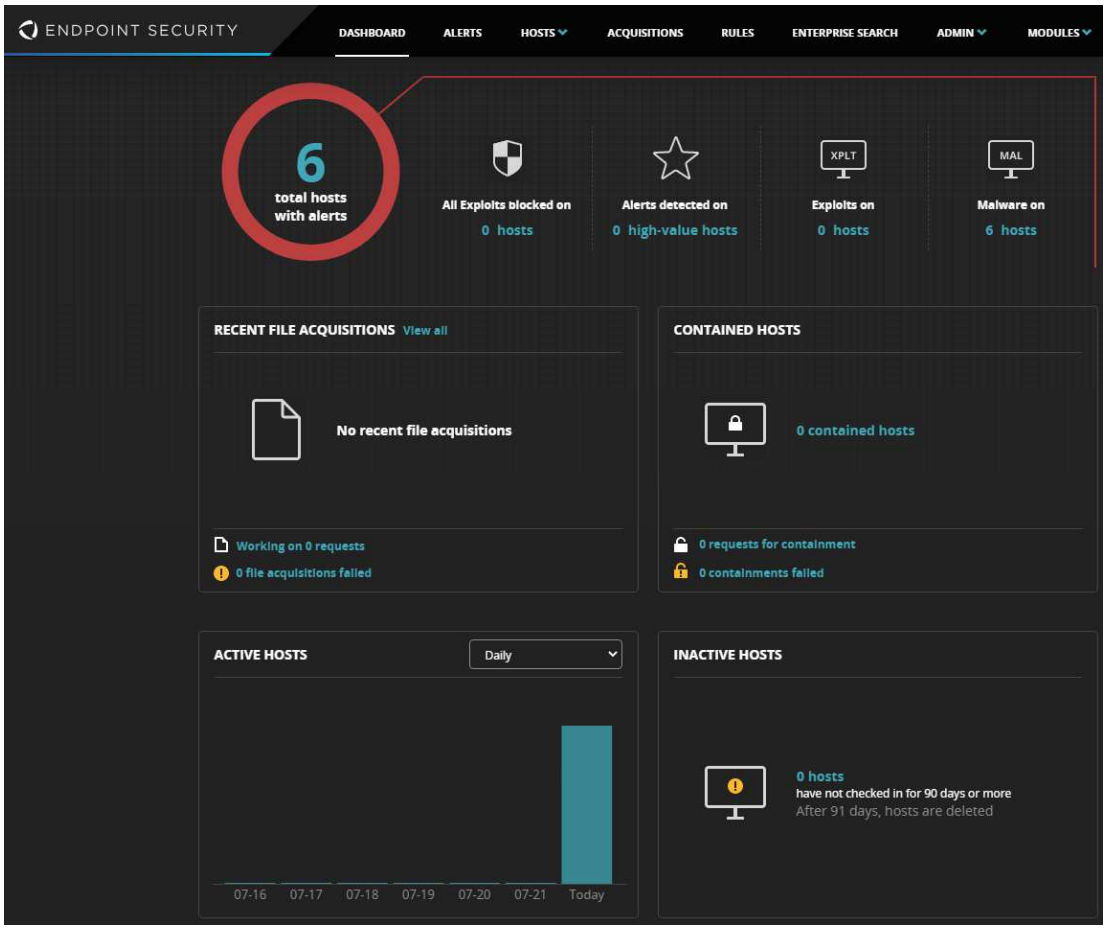


The user can see the protection status and detection logs, run updates, and run full or custom scans. Users can also scan a file, folder or drive using Windows Explorer's right-click menu. If you wish, users with Windows Administrator Accounts can be given full control of the program. Alternatively,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

Malware detection scenario

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

FireEye Endpoint Security



About the product

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

Advantages

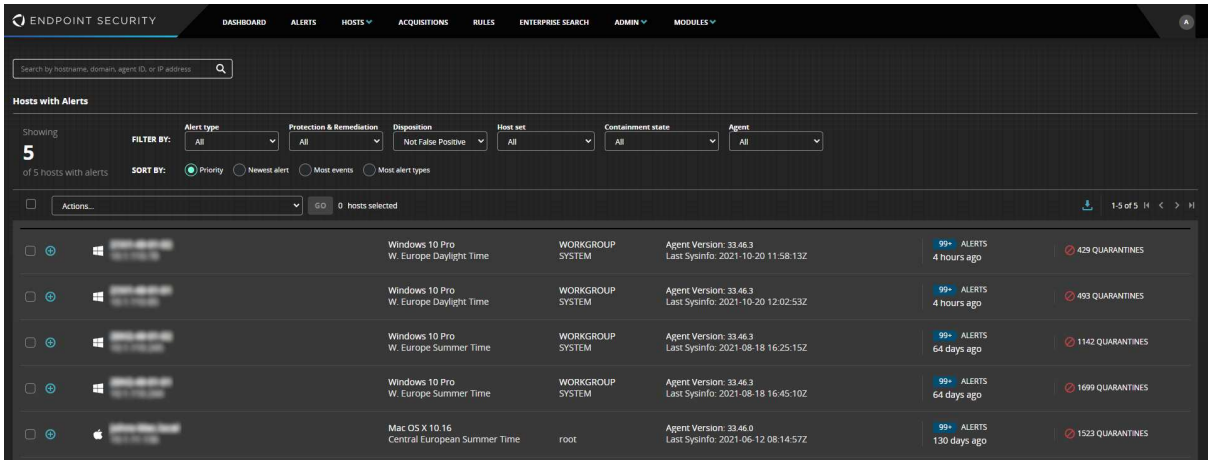
- Attack investigation features
- Variety of console types available
- Suitable for medium- to large-sized enterprises
- Comprehensive search feature
- Containment feature lets you isolated infected devices

Management console

Dashboard

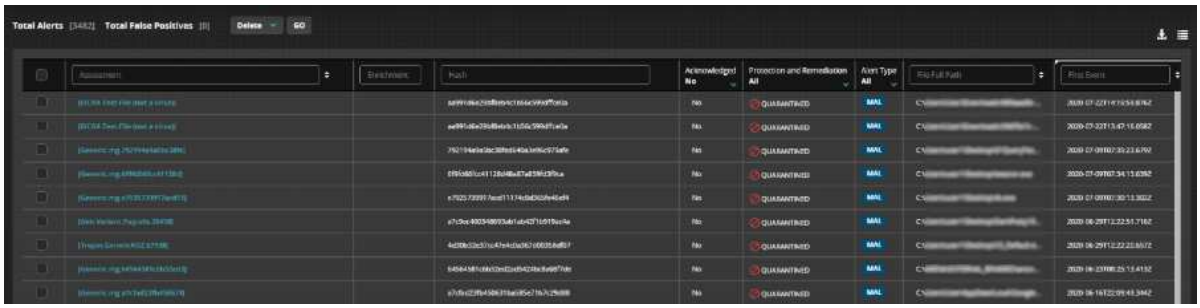
When you open the console, you will see an overview of key status items (screenshot above). These include the total number of hosts with alerts, with a breakdown by exploits and malware. Clicking on the *Total hosts with alerts* button opens the *Hosts with Alerts* page, shown below.

Hosts with alerts



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

Alerts

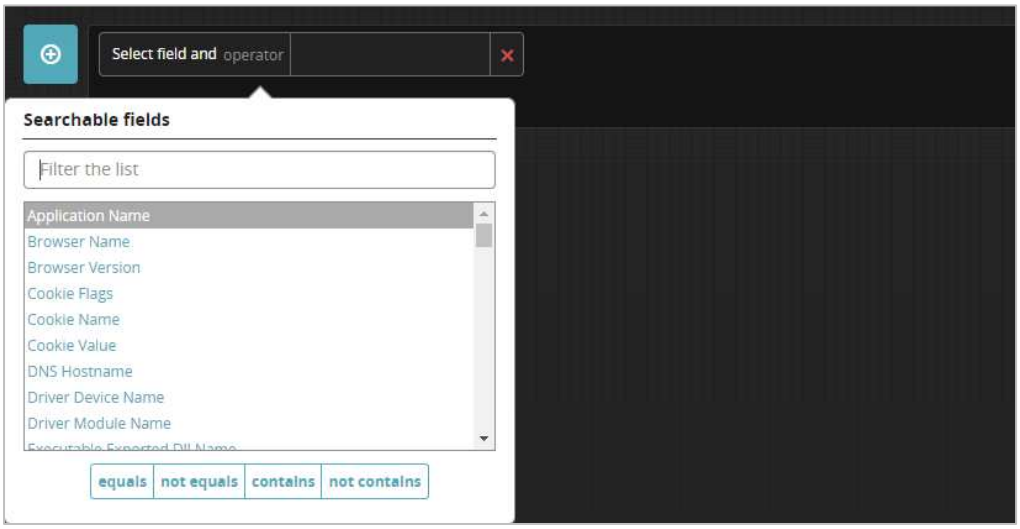


For a threat-centric rather than a device-centric view, you can go to the *Alerts* page. Here you can sort threats by name, file path, first or last detections, and hostname or IP address of the respective device. The options *Acknowledge*, *Mark False Positive* and *Add Comment* are provided here too.

Acquisitions

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

Enterprise Search



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

Policies

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

Host Sets

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

Agent Versions

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

Appliance Settings

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

Windows Endpoint Protection Client

Deployment

Installer files in .msi format can be downloaded from the *Admin* menu, *Agent Versions*. As the name suggests, the current and one or two earlier versions of the client are provided. The installer file can be run manually, via a systems management product, or using an AD script.

User interface

Aside from detection alerts, no user interface is shown on the endpoint.

Malware detection scenario

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

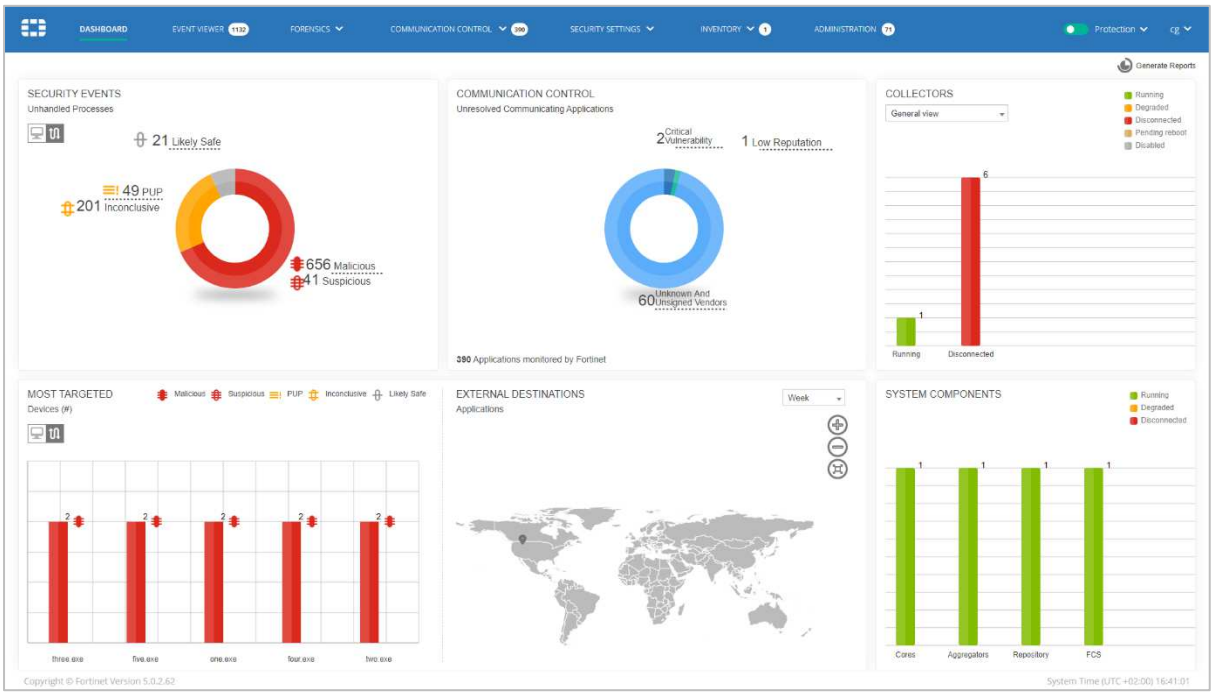
Fortinet FortiClient with EMS, FortiSandbox & FortiEDR

The Fortinet package used for AV-Comparatives' 2021 Enterprise Main Test Series consists of the FortiClient endpoint software and corresponding EMS management console, FortiSandbox, and FortiEDR agent/management console. For the purposes of this review, we have focussed on the cloud-based FortiEDR management console and the corresponding endpoint agent. This console can be used from the cloud, installed on-premises, or run as a hybrid solution.

FortiEDR Management Console

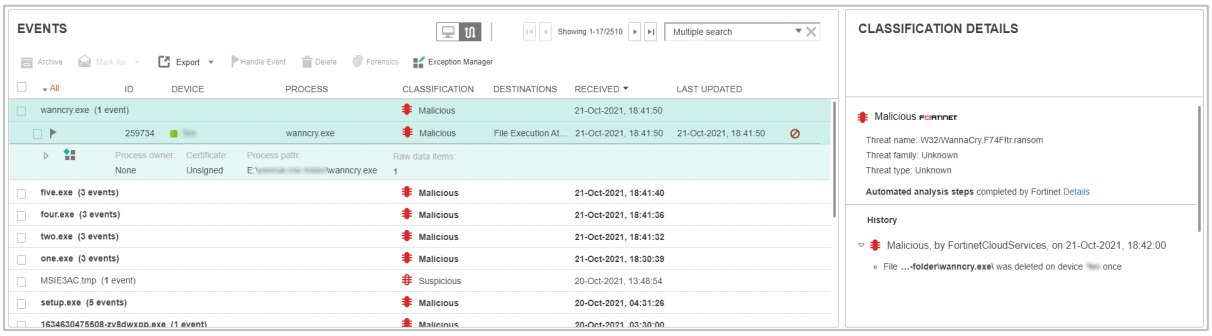
The console is navigated using a single menu bar running along the top. Items are *Dashboard, Event Viewer, Forensics, Communication Control, Security Settings, Inventory,* and *Administration*.

Dashboard page

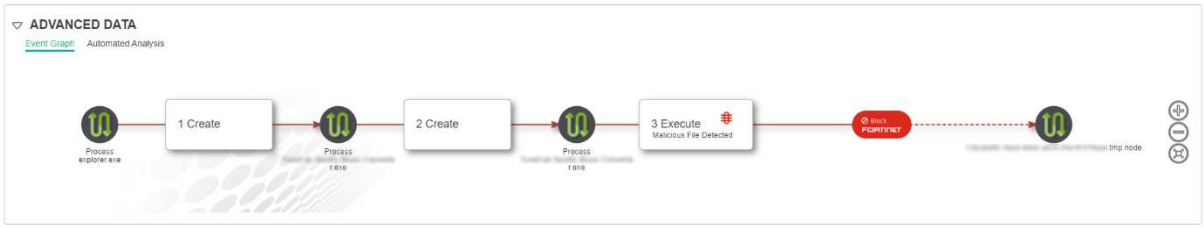


The *Dashboard* page, shown above, uses panels with bar and doughnut charts to provide a graphical overview of threats and suspicious processes. You can see the numbers of processes that have been encountered on the network, categorised as *Malicious, Suspicious, PUA, Inconclusive* and *Likely Safe*. The *Collectors* (agents installed on client PCs) panel shows the current status of devices on the network. These can be shown as *Running, Degarded, Disconnected, Pending Reboot* or *Disabled*. There's also a chart of malicious processes that have targeted the greatest number of endpoints. A map of the world shows you the destinations of the most common network connections. If you mouse over the pin indicating a particular country, you can see the IP addresses to which the connections were made. Many of the *Dashboard* panels are clickable. For example, clicking on the *Security Events* chart takes the user to the *Events* page.

Events page



The *Events* page is accessed by clicking *Event Viewer* in the menu bar at the top. It displays all the security incidents detected and blocked by the system. These can be sorted by process, classification, destination or date/time, amongst other things. For each event, details are provided, including classification as *Malicious, Suspicious, Inconclusive, PUP* or *Likely Safe*. The *Advanced Data* panel (screenshot below) shows a graphical representation of the process execution, other processes involved, and analysis details. By selecting an event, the user can start an investigation by clicking on *Forensics*, which opens the event on the *Forensics\Events* page.



Forensics\Threat Hunting page

This allows the administrator to search for and remediate threats in stealth mode.

Communication Control\Applications page

This enables virtual patching of vulnerable communication applications.

Security Settings\Security Policies page

Here you can configure the security settings for networked PCs. There are 5 separate policies: *Execution Prevention, Exfiltration Prevention, Ransomware Prevention, Device Control,* and *eXtended Detection*. For each policy, a number of individual items can be enabled or disabled, giving the admin fine-grained control. For example, *Execution Prevention* includes the items *Malicious File Detected, Suspicious File Detected, Unconfirmed File Detected, Privilege Escalation Exploit Detected, Sandbox Analysis,* and *Suspicious Driver Load*.

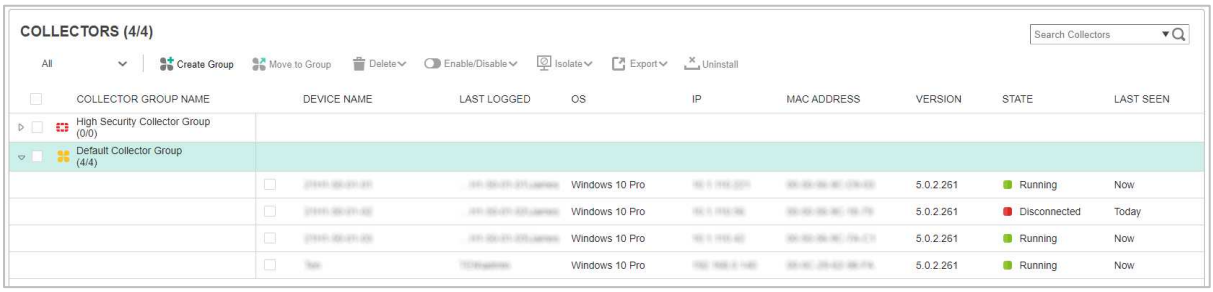
Security Settings\Playbooks page

Here you can configure automated incident response. Each *Playbook* (response policy) lets you notify the admin of an incident, remediate the problem (by e.g. terminating processes, deleting files, and cleaning persistent data), and investigate (e.g. by isolating the affected device and/or moving it to the *High Security Group*).

Security Settings\Exception Manager and *Exclusion Manager* pages

These pages allow you to exclude specific events and event flows from the threat-hunting data collection process.

Inventory\Collectors page



This provides an overview of protected devices. For each device, you can see the hostname, last user, operating system, IP address, MAC address, agent version, status and last-seen date. By selecting devices, you can run tasks on them using the buttons along the top of the page. These include *Move to Group*, *Delete*, *Isolate* and *Uninstall*.

Administration page

Here you can manage licences, users, and distribution lists, amongst other things.

Windows Endpoint Protection Client

Deployment

Installer files (*Collector Installers*) in .MSI format are provided on the *Administration* page. There are separate editions for 32- and 64-bit systems. The installers can be run manually, via a systems management product, or using Active Directory.

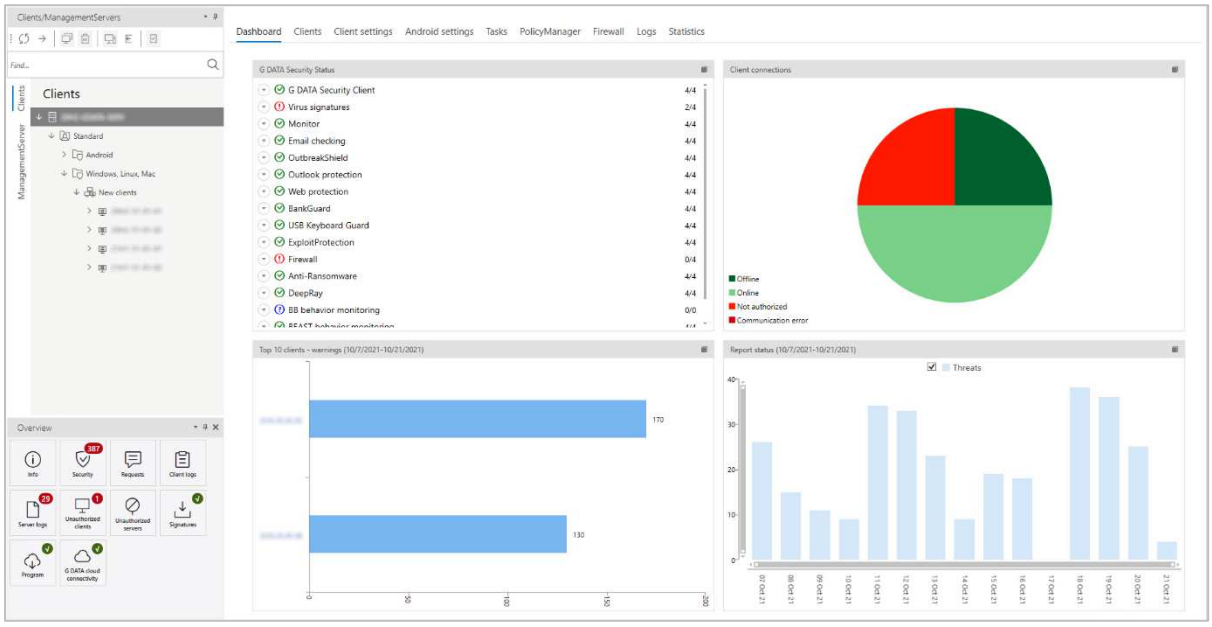
User interface

There is a minimalist user interface to the endpoint agent. A System Tray icon allows you to see the log of recent activity, and hide EDR notifications for the next 24 hours.

Malware detection scenario

When we connected a flash drive containing malware to our PC, and opened it in Windows Explorer, Fortinet did not initially take any action. We were able to copy the malware samples to the Windows Desktop. However, when we tried to execute them, the malicious files were immediately detected and quarantined in situ. A pop-up alert was shown, which closed after a few seconds. No user action was required or possible.

G Data Endpoint Protection Business



About the product

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

Advantages

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

Server Installation

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

Management Console

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

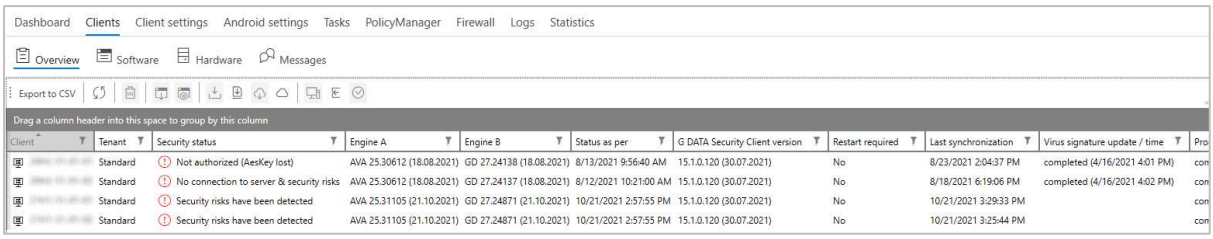
Clients pane

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

Dashboard page

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

Clients page



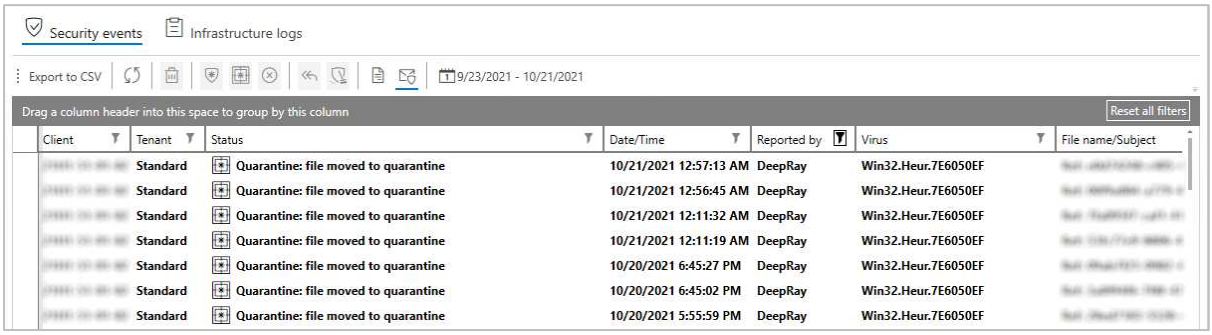
The *Overview* tab of the *Clients* page, shown above, displays a list of managed devices. You can see information such as status, definitions used, client version and operating system. The columns are customisable. Thus, you could also display the last active user, and various network items such as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

Client settings page

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

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

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



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

Windows Endpoint Protection Client

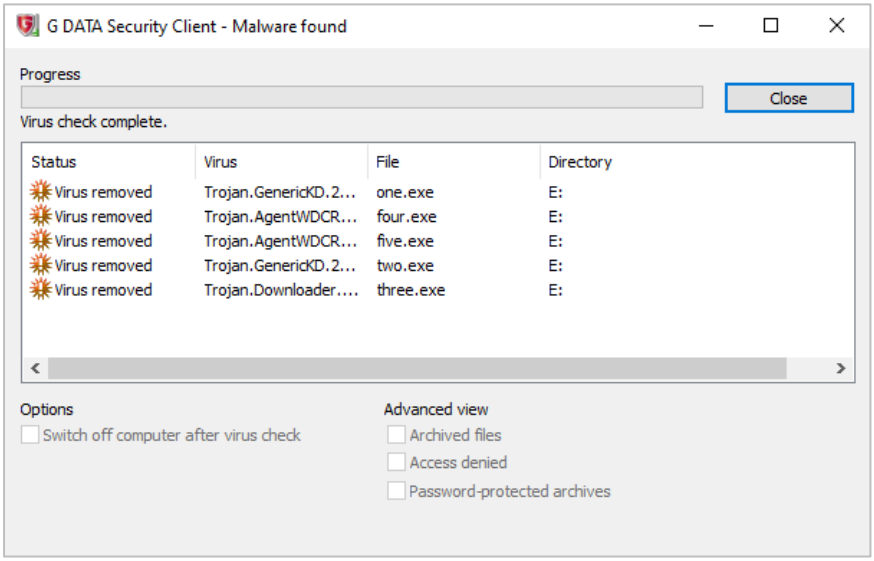
Deployment

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

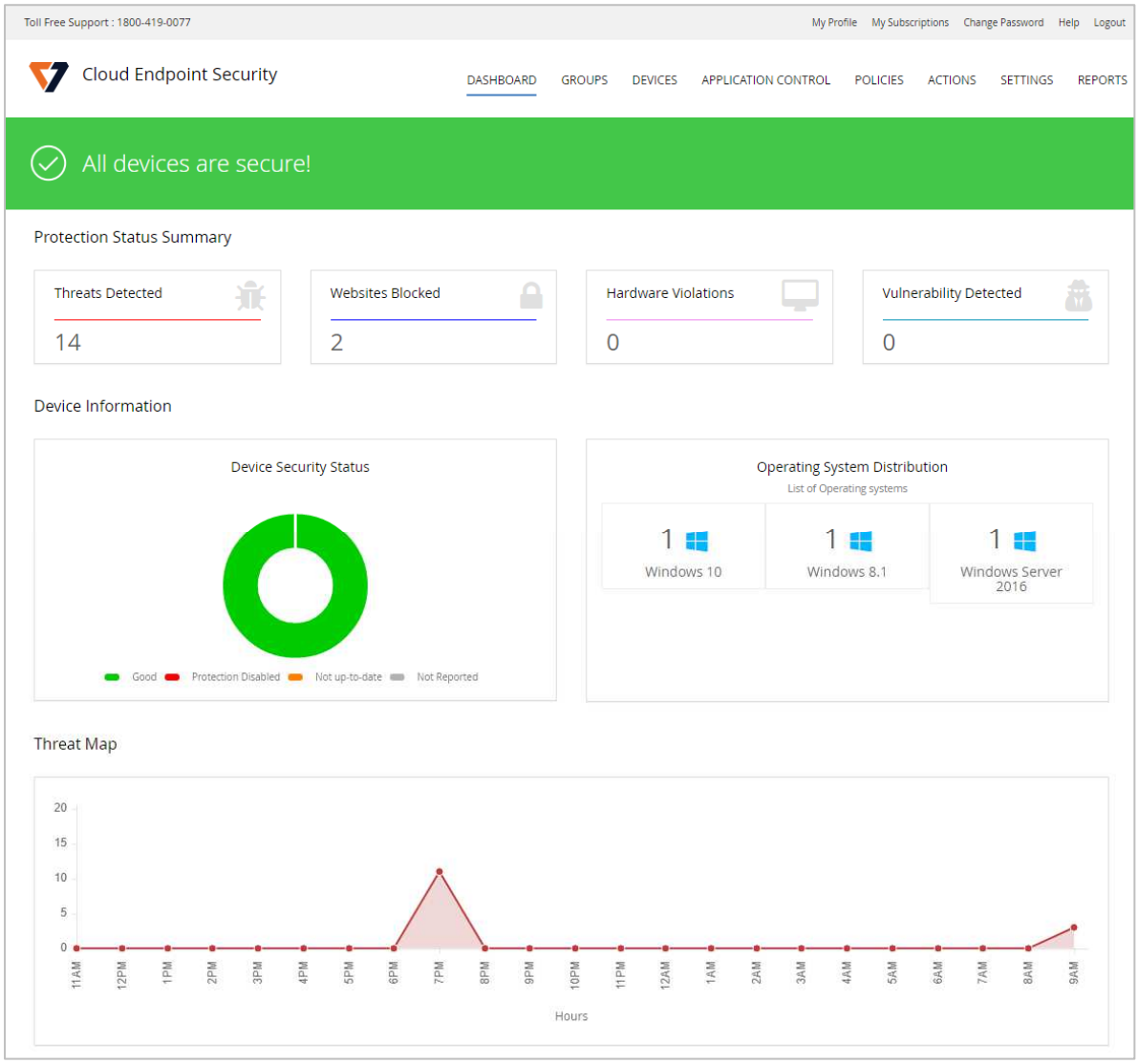
User interface

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

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



K7 Cloud Endpoint Security Advanced



About the product

K7 Cloud Endpoint Security Advanced provides a cloud-based console for managing the endpoint protection software. The product is designed for enterprises of all sizes. We feel it is particularly suitable for smaller businesses and less-experienced administrators.

Advantages

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

Management console

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

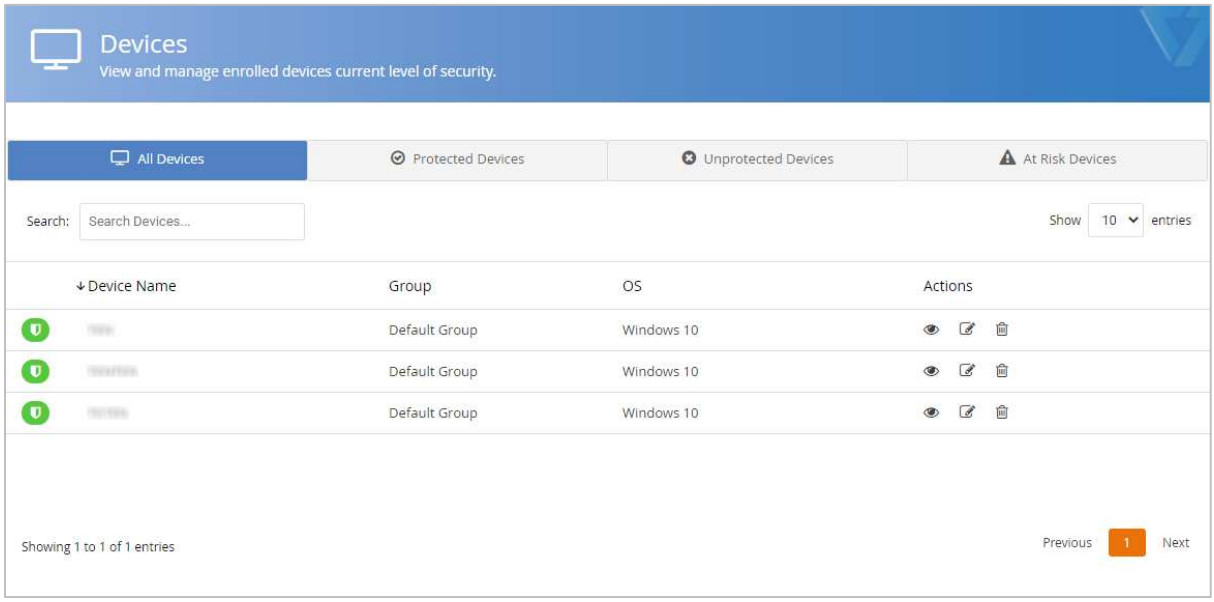
Dashboard page

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

Groups page

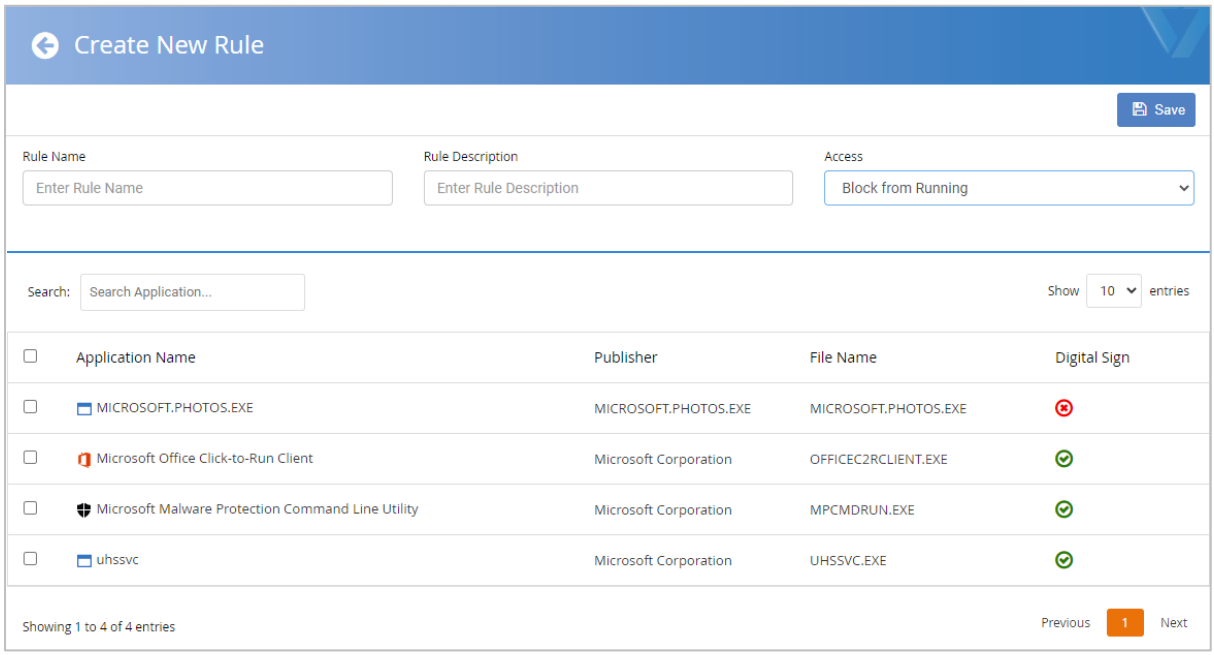
The *Groups* page of the console lists device groups you have created. There are links to the policy applied to each group, and a list of tasks (such as scans and updates) that you can apply to all group members.

Devices page



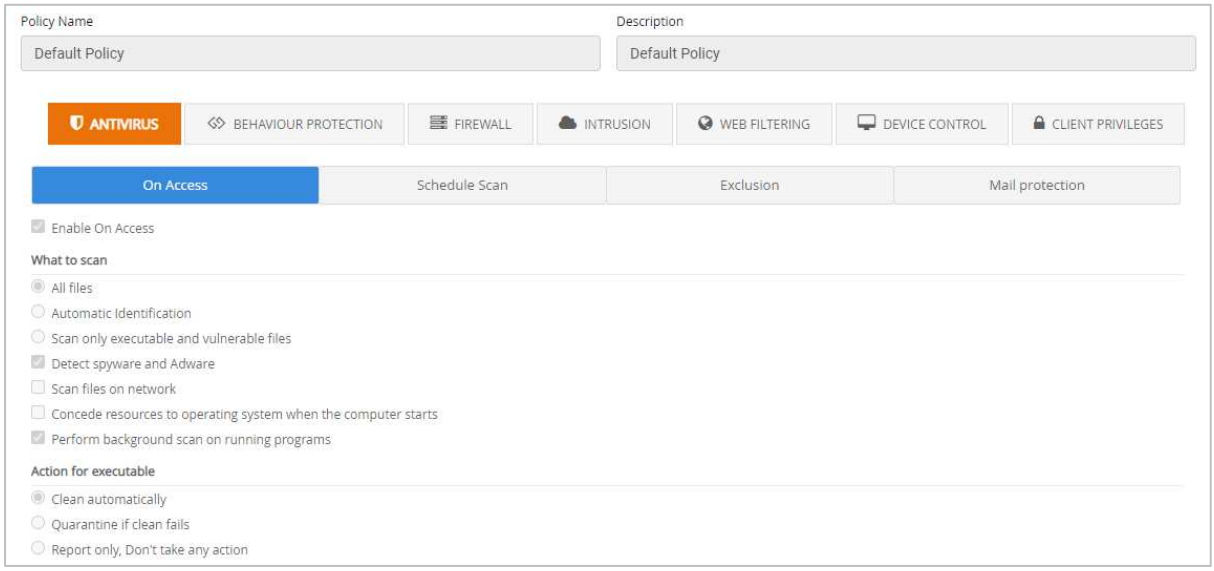
The *Devices* page*All Devices* tab, shown in the screenshot above, lists individual computers on the network. The links in the *Actions* column let you view a computer's details, uninstall Endpoint Security, or change its group. Other tabs of the *Devices* page sort computers into the categories *Protected*,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

Application Control page



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

Policies page



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

Actions page

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

Settings page

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

Reports page

Reports page provides a very simple means of running reports on items such as detected threats, and vulnerabilities, websites blocked, and scan results. You can specify day, week, month or year as the time interval for the report, or use a custom time period.

Windows Endpoint Protection Client

Deployment

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

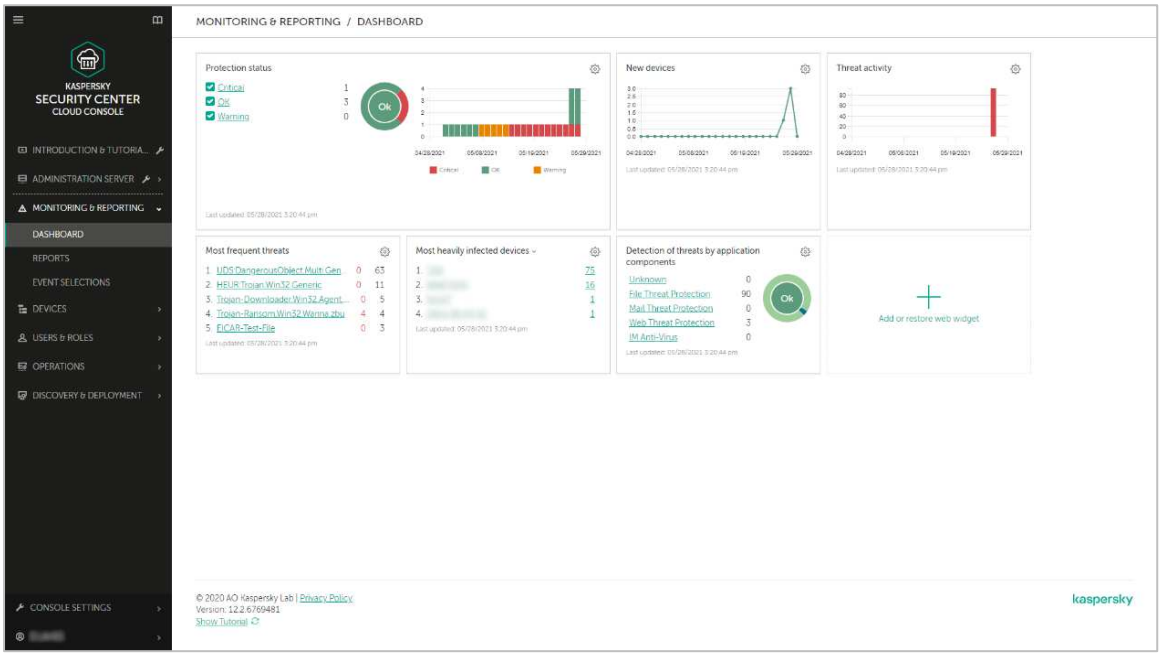
User interface

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

Malware detection scenario

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

Kaspersky Endpoint Security for Business - Select, with KSC



About the product

Kaspersky Endpoint Security for Business (KESB) Select is a tier of Kaspersky's Endpoint Security for Business product line. It is aimed at medium-sized businesses and larger enterprises. The product provides a choice of either a server-based or a cloud-based console to manage the endpoint protection software. We have looked at the cloud console in this review.

Advantages

- Choice of server-based or cloud management console
- Console easily navigated from a single menu
- Deployment wizard for simplified client installation
- Web interface can be customised
- Granular role-based control permissions for console administrators

Management console

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

Monitoring and Reporting section

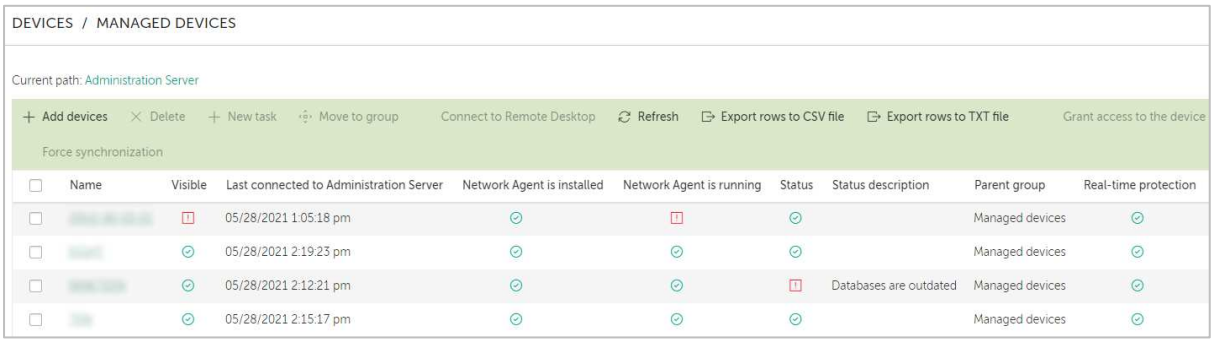
The *Dashboard* page (shown above) provides a graphical overview of key information. This includes protection status, new devices, plus details of threats and infected devices. The page is customisable, and you can add/remove various panels (*Web Widgets*) as you please.

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

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

Devices section

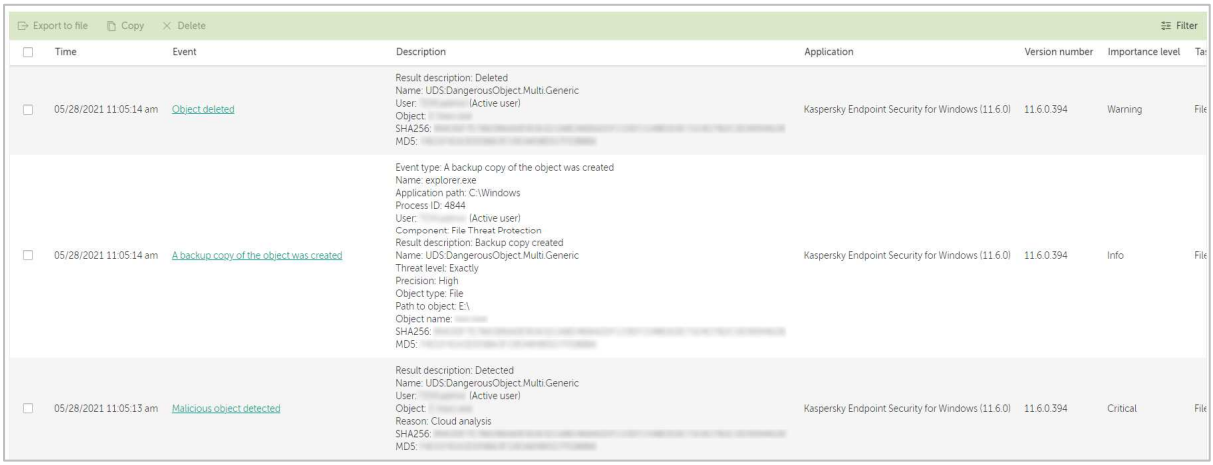
The *Policies and Profiles* page lets you create and apply new configuration policies. On the *Tasks* page you can carry out everyday maintenance and backup tasks, such as updates.



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

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

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



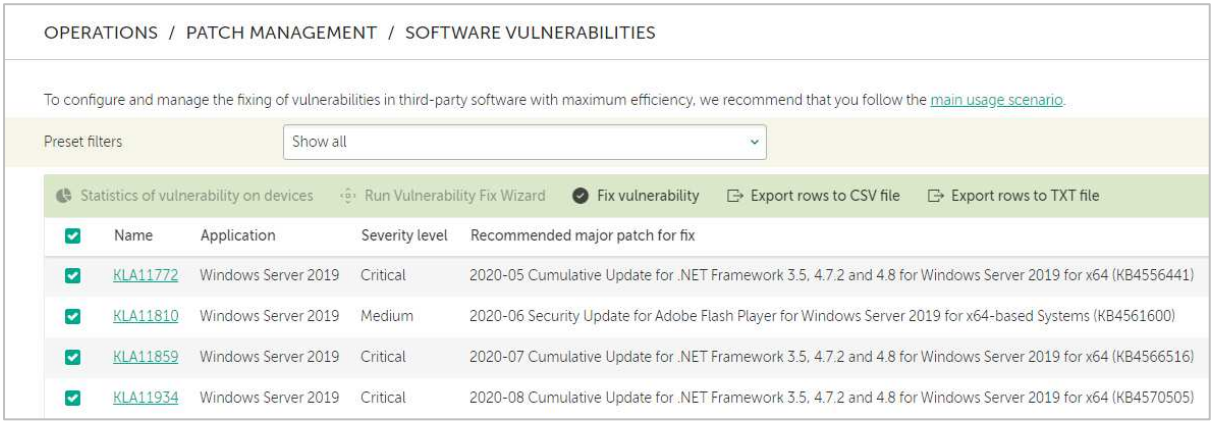
The *Device Selections* page lets you find devices in pre-configured groups. Examples include *Databases are outdated* and *Devices with Critical Status*.

Users & Roles section

Under *Users*, you can see a list of predefined console users, along with Windows local and domain accounts for the Windows computers on the network. On the *Roles* page, users can be assigned one of 14 different management roles for the console, allowing very granular access.

Operations section

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



Discovery & Deployment section

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

Windows Endpoint Protection Client

Deployment

When the console is first used, a deployment wizard runs, allowing you to push the endpoint software to clients over the network. This can be (re)run later from *Discovery & Deployment\Deployment & Assignment\Quick Start Wizard*. It is a very neat and simple process. The endpoint protection software could also be deployed using a systems management product or Active Directory. Alternatively, you can create a standalone installation package from *Discovery & Deployment\Deployment & Assignment\Installation Packages*.

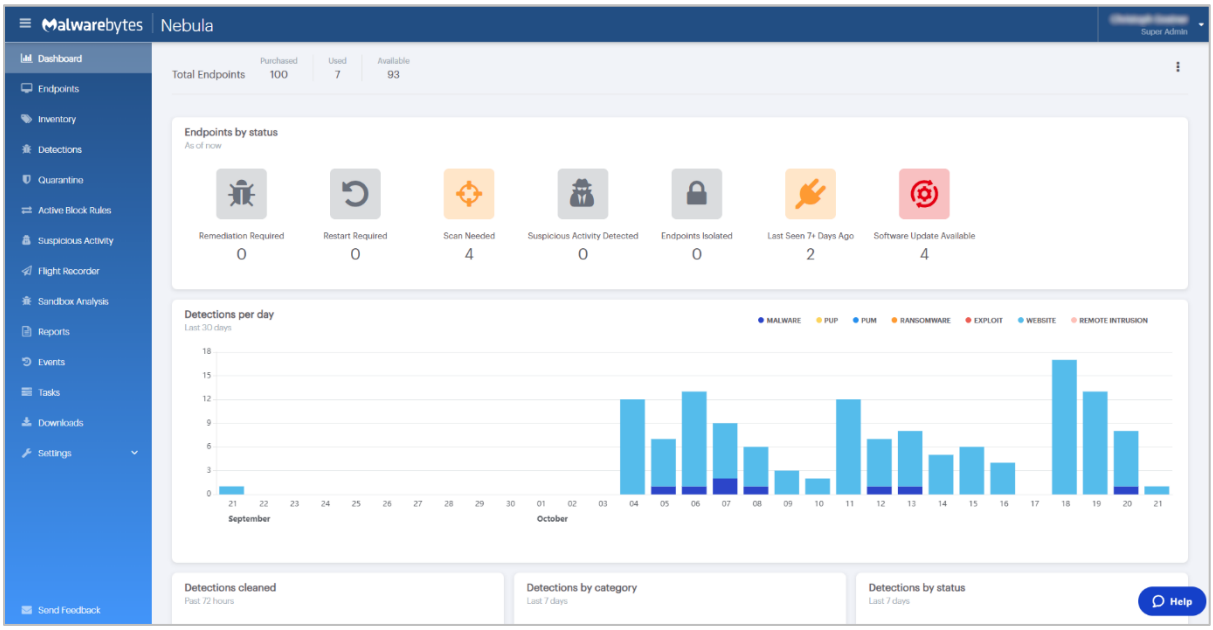
User interface

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

Malware detection scenario

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

Malwarebytes EDR



About the product

Malwarebytes EDR provides a cloud-based console for managing the endpoint protection software. The product's ease of use makes it suitable for smaller businesses, but it can also cope with tens of thousands of devices.

Advantages

- Easy-to-navigate cloud console
- Pages can be easily customised
- Clickable interface makes it easy to find more details
- Protection against brute-force attacks
- Client software inventory

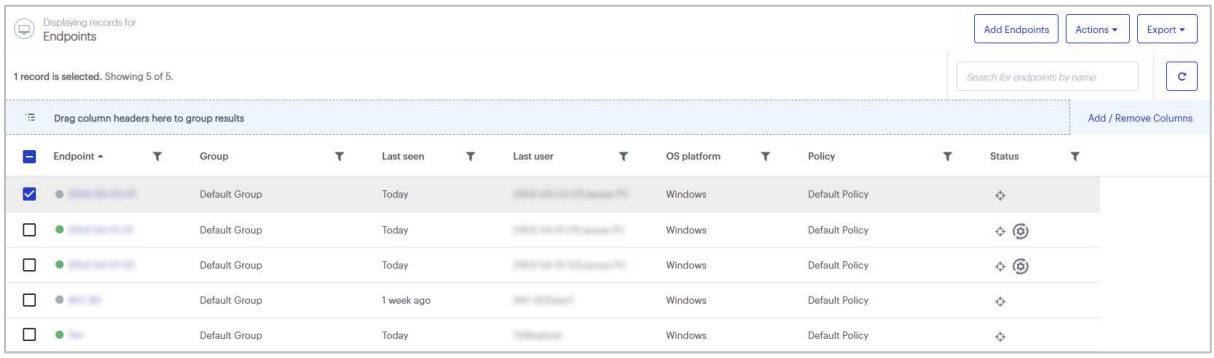
Management console

The cloud console is navigated using a single, clear menu column on the left-hand side. Items are *Dashboard, Endpoints, Inventory, Detections, Quarantine, Active Block Rules, Suspicious Activity, Flight Recorder, Sandbox Analysis, Reports, Events, Tasks, Downloads*, and *Settings*. The latter expands to show the additional items *Policies, Schedules, Exclusions, Notifications, Groups, Users, Syslog Logging, Single Sign-on, and APIs & Integrations*.

Dashboard page

This is shown in the screenshot above. It provides an overview of security-related information in various different panels, many with graphical illustration. The topmost of these are *Endpoints by status, Detections per day, Detections cleaned, Detections by category*, and *Detections by status*. By default, 15 panels are shown. However, the dashboard can easily be customised, allowing you to add, remove or move panels as you wish. The individual items in the *Endpoints by status* panel are linked to filtered pages showing the devices in question. Hence clicking on, say, *Scan Needed* will display a list of precisely those devices. The same principle is used with some of the other panels, whilst mousing over the bar graphs displays a pop-up panel with more details.

Endpoints page



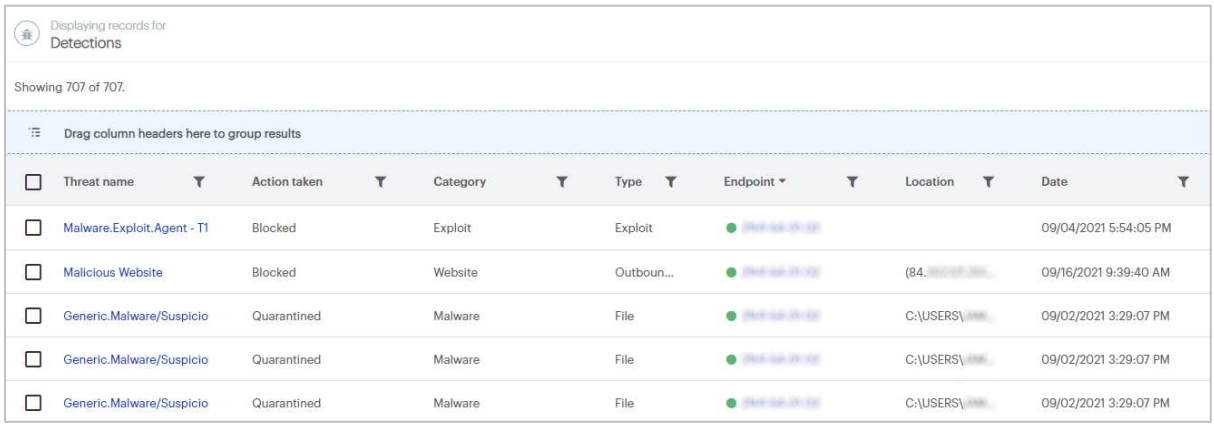
This shows you the protected computers on your network. You can see each device's assigned group, last-seen date, last user, OS type, policy applied, and status. By selecting one or more endpoints, you can run tasks from the *Actions* menu. Examples are scan, update, restart and isolate.

Inventory page

Here you can see all the software installed on computers in your network. For each application, you can see the version number, date installed, name of the endpoint, and operating system.

Detections page

As you would expect, this displays instances of malware found on network computers. You can see the threat name, action taken, threat type, affected endpoint, local path, and date/time of detection. Clicking on the name of a threat opens a panel with a summary of info for that detection.



Quarantine page

This shows quarantined malware that has been detected on protected devices. You can see the threat name and path, threat type, device name, and date/time of detection. Clicking on a threat name displays a panel with details of that particular detection. Quarantined items can be selected individually or all together, and deleted or restored from the *Actions* menu.

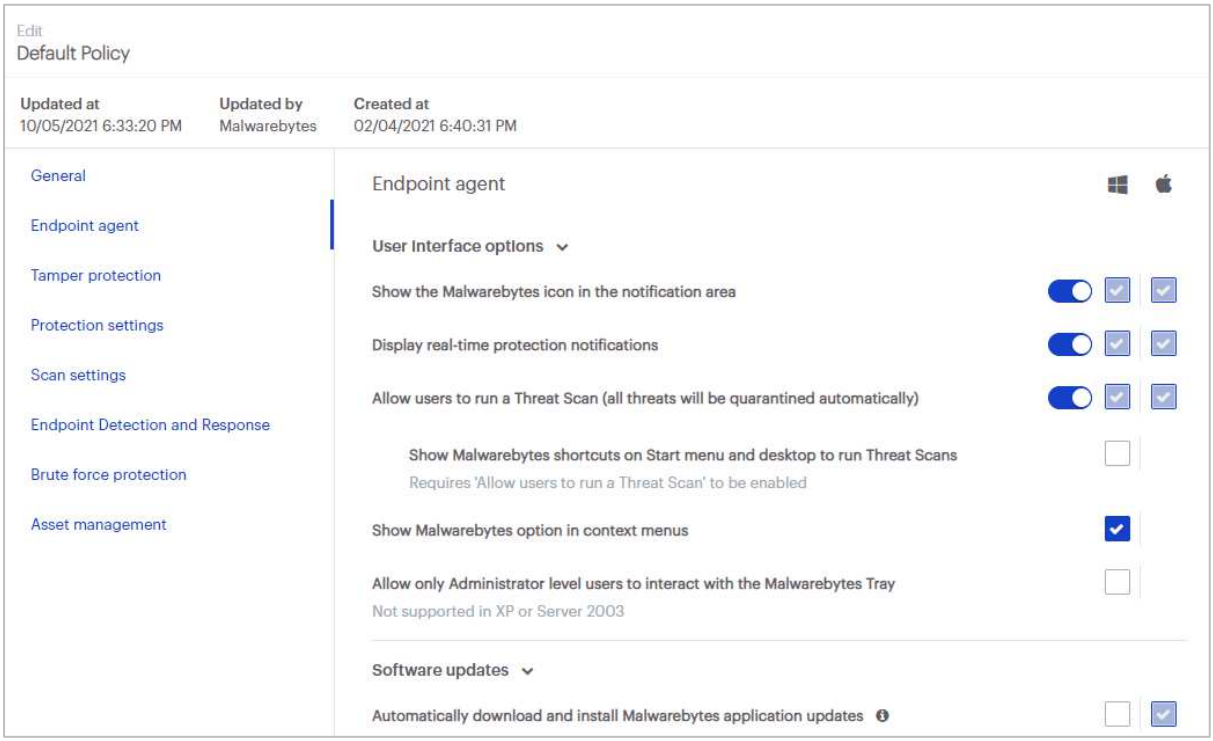
Reports page

This lets you generate reports on a variety of topics: *Assets Summary, Detections Summary, Endpoints Summary, Events Summary, Quarantine Summary, Tasks Summary,* and *Weekly Security Report*. These can be scheduled on a daily, weekly or monthly basis, and sent by email to the administrator (plus other recipients if desired). The *Weekly Security Report* provides a simple overview of the security situation, displaying tiles that show statistics for *Endpoint activity status, Endpoint protection summary, Endpoints needing attention, Top 5 operating systems,* and *Threats*. A traffic-light colour-coding system is used to highlight the statistics, with e.g. critical items shown in red.

Downloads page

On this page you can find installer files for all the supported operating systems.

Settings\Policies page



Here you can configure the policies that dictate the settings applied to protected devices. On the left-hand side of the page are links to the different policy areas, which *Endpoint Agent, Tamper Protection, Protection Settings, Scan Settings, Endpoint Detection And Response, Brute Force Protection,* and *Asset Management*. For Windows devices, you can integration with Windows Action Center, amongst other things. The brute-force protection feature allows you to defend against e.g. malicious Remote Desktop connections.

Windows Endpoint Protection Client

Deployment

On the *Downloads* page of the console, you can download installers, or email installation links to these. There is a choice of .exe and .msi installer files; the latter have specific versions for 32- and 64-bit systems. The setup wizard is very quick and easy, and should not pose any problems for non-expert users. You can prevent users with Windows Administrator Accounts from uninstalling the software using the *Tamper Protection* section in the applicable policy.

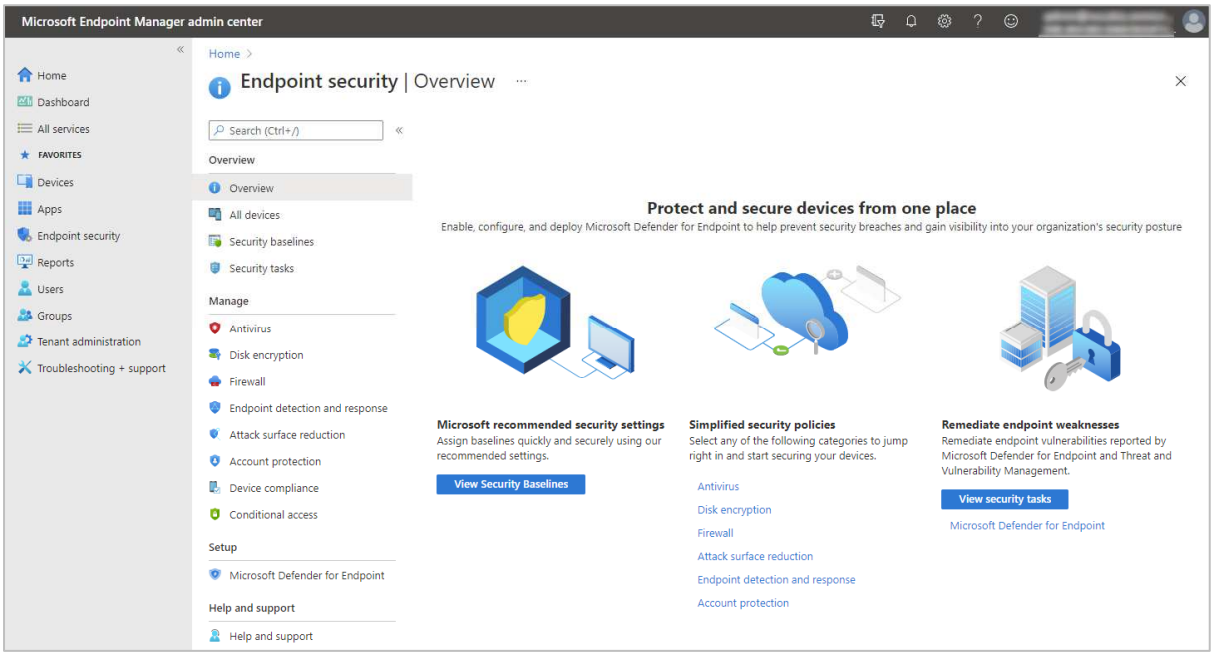
User interface

The Malwarebytes endpoint client has a minimalist user interface. There is a System Tray icon, from which users can start a scan. A small window then displays the scan status. Users can also scan a drive, folder or file using Windows Explorer's right-click menu. The System Tray icon can be hidden by policy, if you prefer.

Malware detection scenario

When we connected a flash drive containing malware to our PC, and opened it in Windows Explorer, Malwarebytes did not initially take any action. We were able to copy the malware samples to the Windows Desktop. However, when we tried to execute them, the malicious files were immediately detected and quarantined. A pop-up alert was shown, which provided the file name and path, and detection name of the malware. No user action was required or possible, and the alert closed after a few seconds.

Microsoft Defender Antivirus with Microsoft Endpoint Manager



About the product

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

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

Advantages

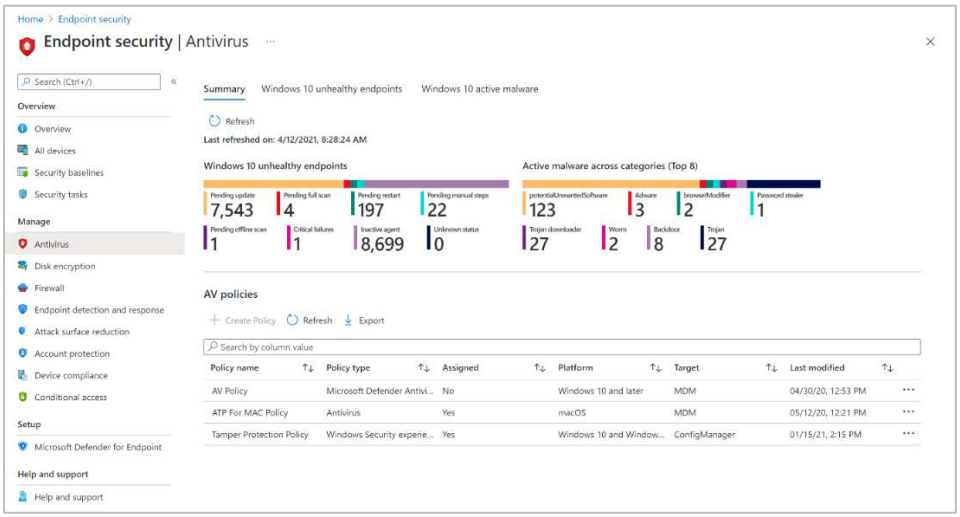
- Controls all Windows security settings
- Console is customisable
- Exceptionally simple client deployment
- Suitable for businesses of all sizes using Microsoft cloud services for business
- Granular control of security options

Management Console

Endpoint Security | *Overview* page

This is shown in the screenshot above. It is the main dashboard for the endpoint security features of the platform. Here you can see an overview of the individual protection components that can be configured. Examples are *Antivirus, Disk Encryption,* and *Firewall*. You can also view *Security Baselines*. These are policy templates with recommended settings for all security-related features in Windows. There are Baselines for *Windows 10 Security, Microsoft Defender for Endpoint,* and *Microsoft Edge*. Microsoft tell us that these are frequently updated.

Endpoint Security | Antivirus page



The *Summary* tab (shown above) provides an overview of the security status of your network. It displays the number of *Windows 10 unhealthy endpoints* (devices with some kind of security-related problem) and *Active malware across categories* (a breakdown of malware types encountered).

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

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

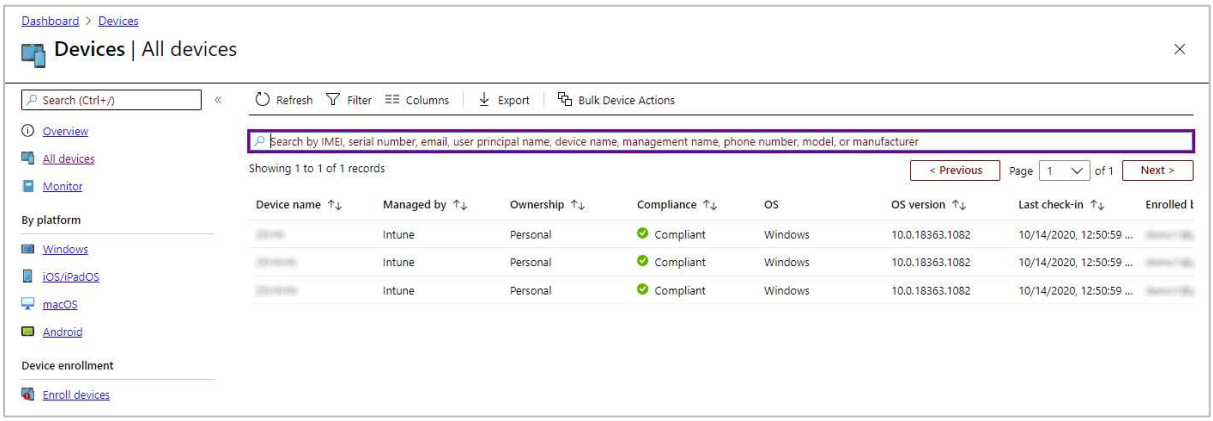
The *User Experience* category has just one setting: *Allow user access to Microsoft Defender app*. Deselecting this hides the Microsoft Defender Antivirus (Windows Security) interface and suppresses malware alerts on client devices. However, *Security Experience* policies provide a much more granular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

There is a third category of policy, *Microsoft Defender Antivirus exclusions*, which allows you to configure scan exclusions.

The *Windows 10 unhealthy endpoints* tab of the *Endpoint Security\Antivirus* page displays a report of devices that require attention. Details include the status of malware protection, real-time protection, and network protection. As with other pages, you can modify the layout using the column picker to modify fields, change to a grid view for better searching, sort by any column, and export the list of records to a .csv file to save locally. A row of buttons along the top of the page lets you easily restart selected computers, or run quick/full scans and updates on them.

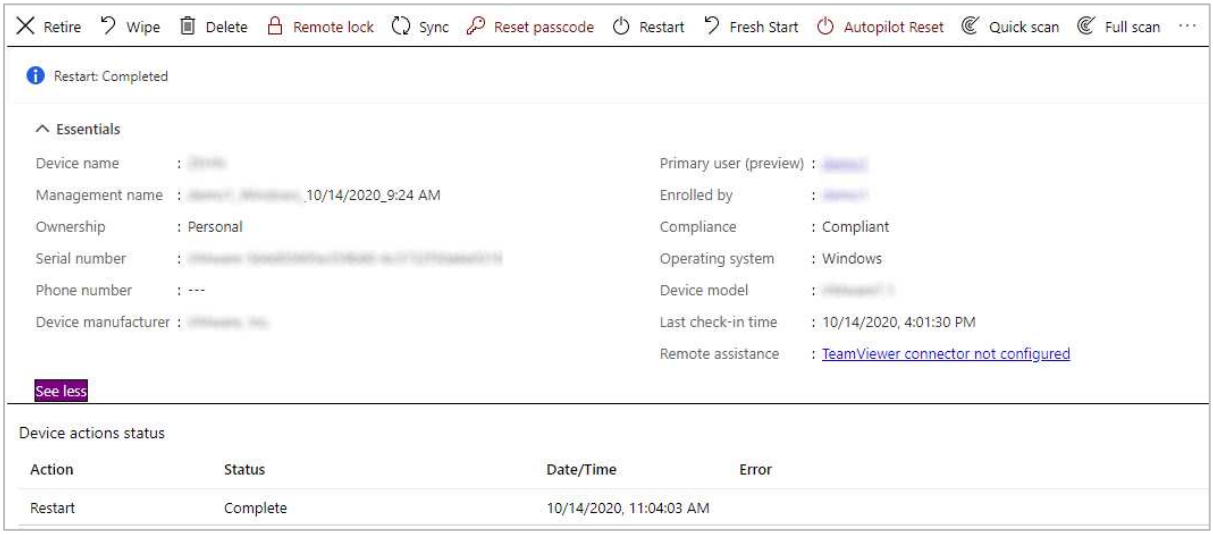
On the *Windows 10 detected malware* tab you can see devices and users with active malware. This view includes details such as malware state, active malware, category and severity. You can take remote actions here including restart, quick scan, full scan, or update signatures, to help resolve the problem.

Devices | All devices page



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

Device details page



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

Windows Endpoint Protection Client

Deployment

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

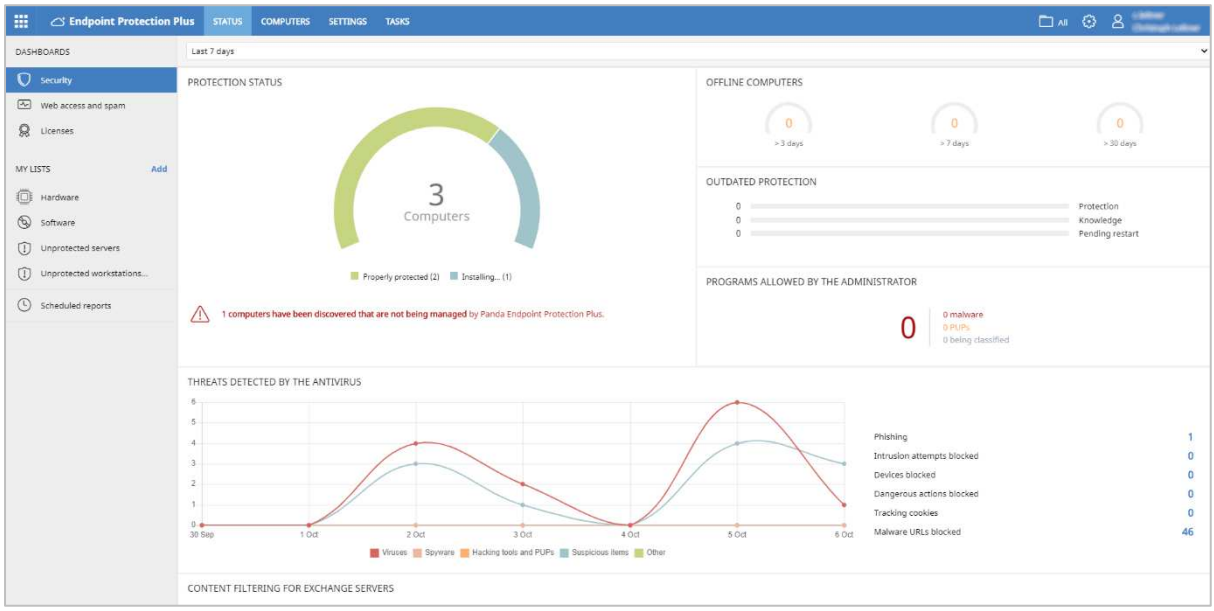
User interface

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

Malware detection scenario

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

Panda Endpoint Protection Plus on Aether



About the product

Panda Endpoint Protection Plus on Aether provides a cloud-based console for managing the endpoint protection software. The product can manage networks with tens of thousands of devices. We feel it would also be suitable for smaller businesses with tens of seats.

Advantages

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

Management Console

Status tab

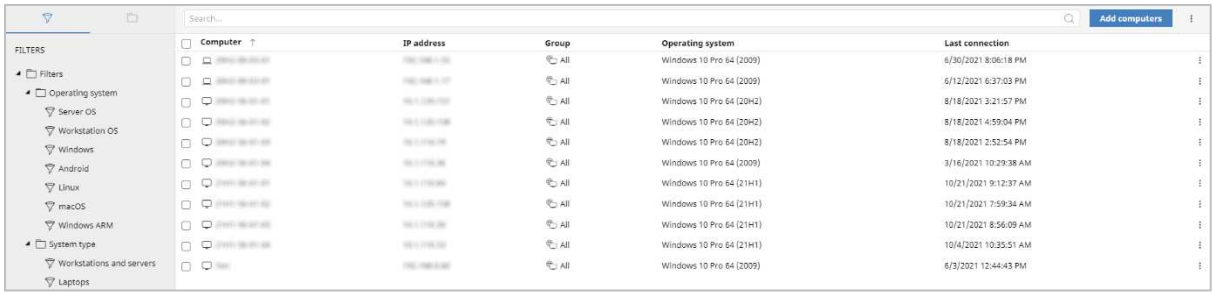
A status overview is provided on the *Status* tab/*Security* page (screenshot above), which opens by default. There are pie and bar charts for the items shown, which include *Protection Status, Offline Computers, Outdated Protection,* and *Programs Allowed by the Administrator*. You can click through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

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

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

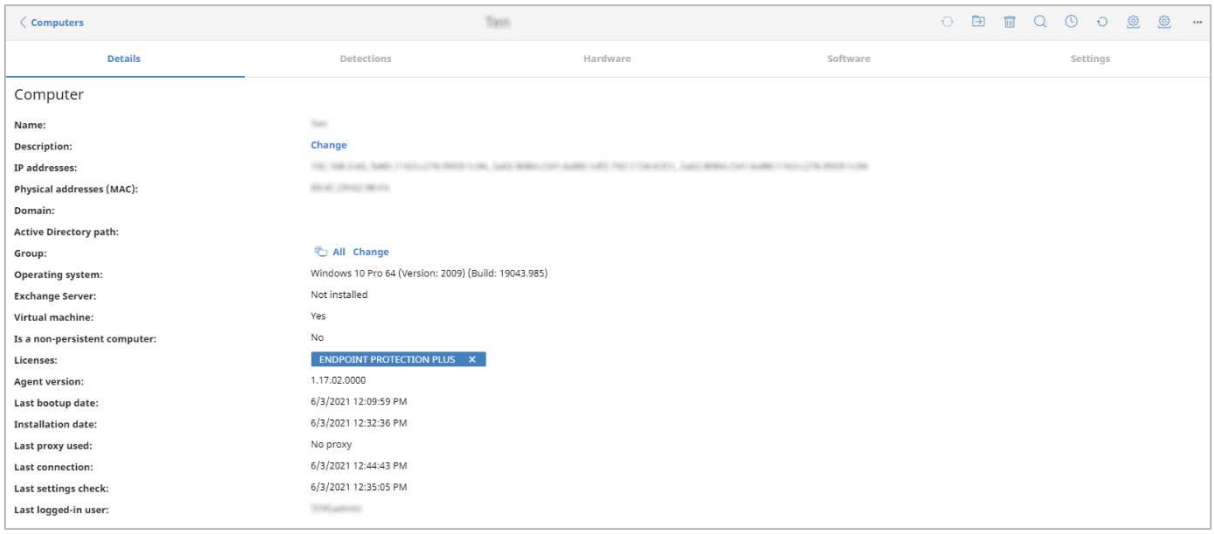
Computers tab

The *Computers* tab, shown below, lists computers on the network. You can filter by various criteria, including OS, hardware and installed software. You can also display computers by management group. This page shows all the protected computers and mobile devices. It is very clearly laid out, and shows essential information. A Windows-Explorer-like folder tree on the left lets you filter devices by OS, device type, or hardware/software criteria. The three-dots button at the end of each entry lets you carry out tasks on the specified device, such as running scans, reinstalling software, moving the computer to another group, or deleting it.



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

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



Settings tab

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

Tasks tab

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

Settings menu

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

Windows Endpoint Protection Client

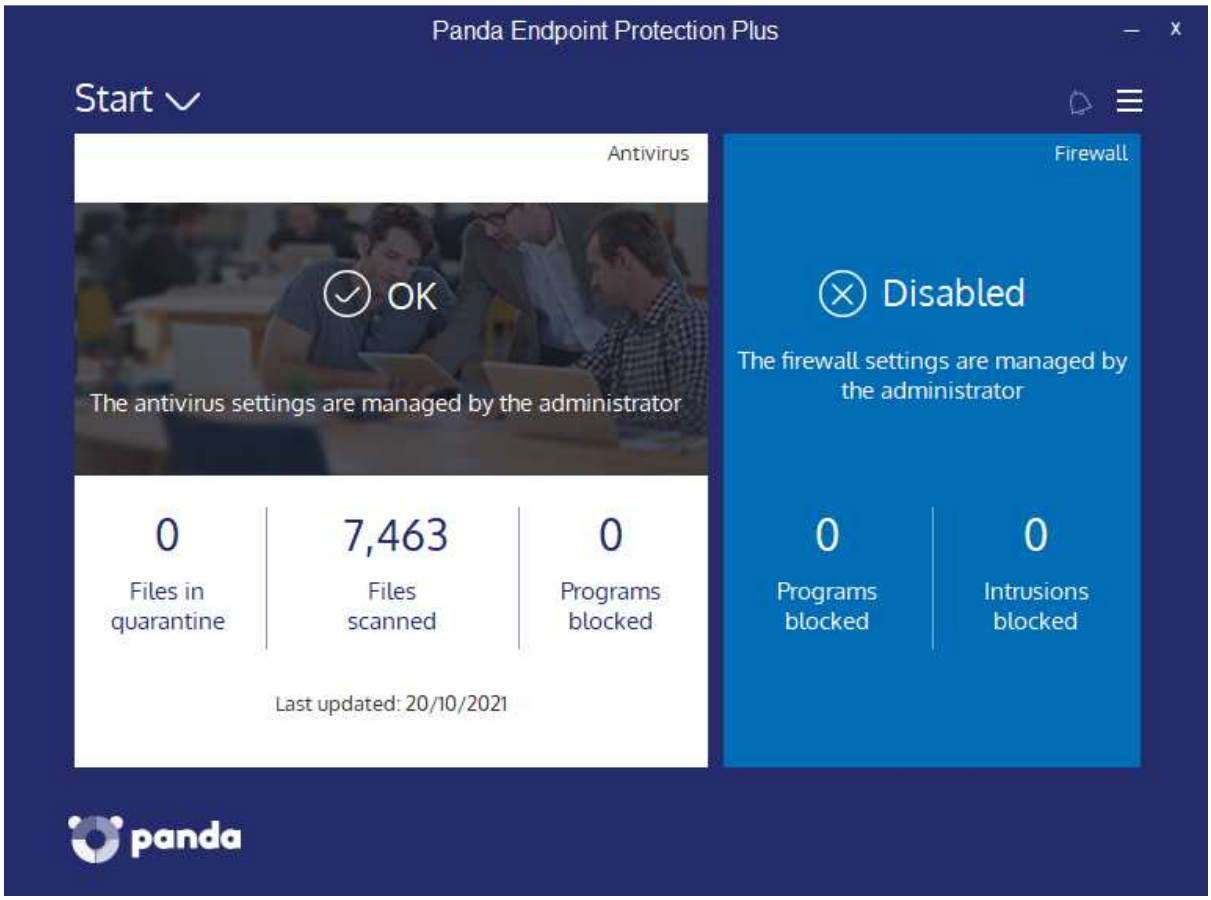
Deployment

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

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

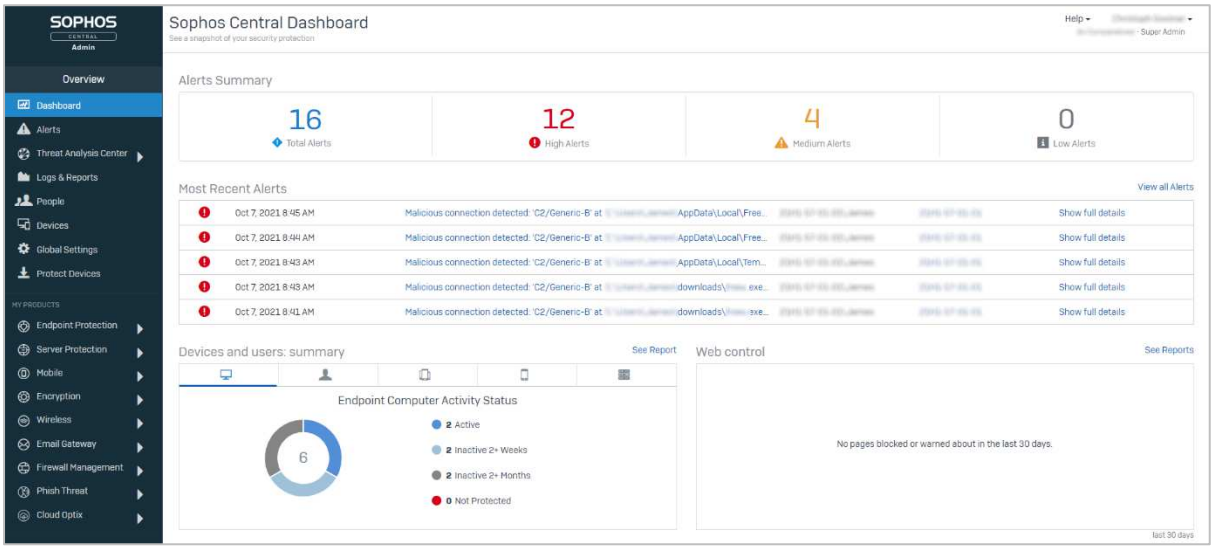
User interface

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



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

Sophos Intercept X Advanced



About the product

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

Advantages

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

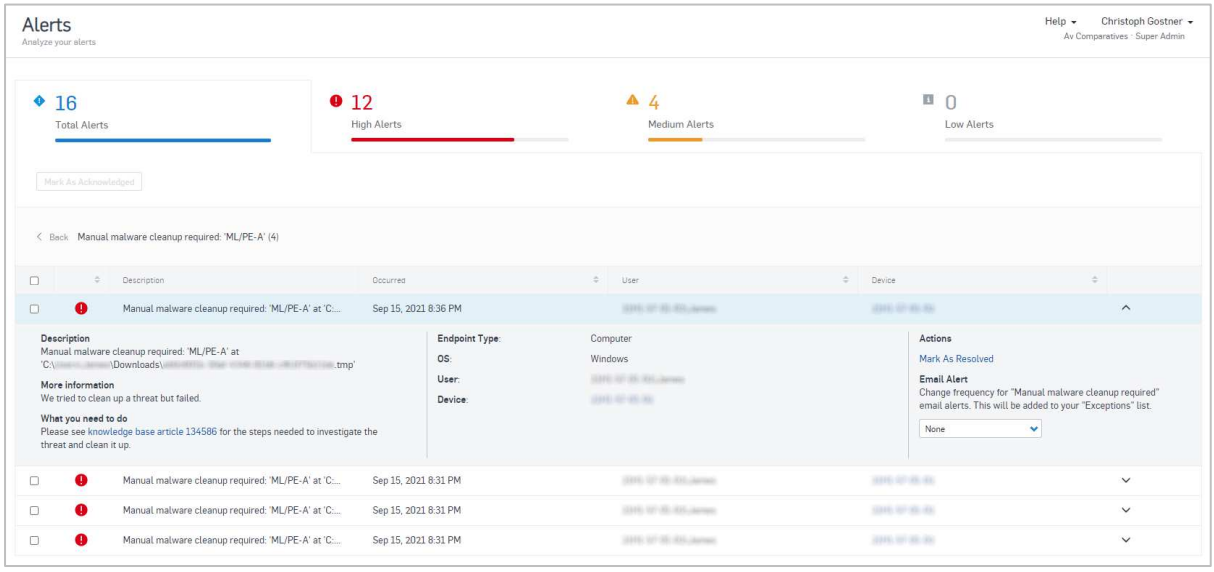
Management Console

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

Dashboard page

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

Alerts page



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

Logs and Reports page

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

Endpoint Protection section

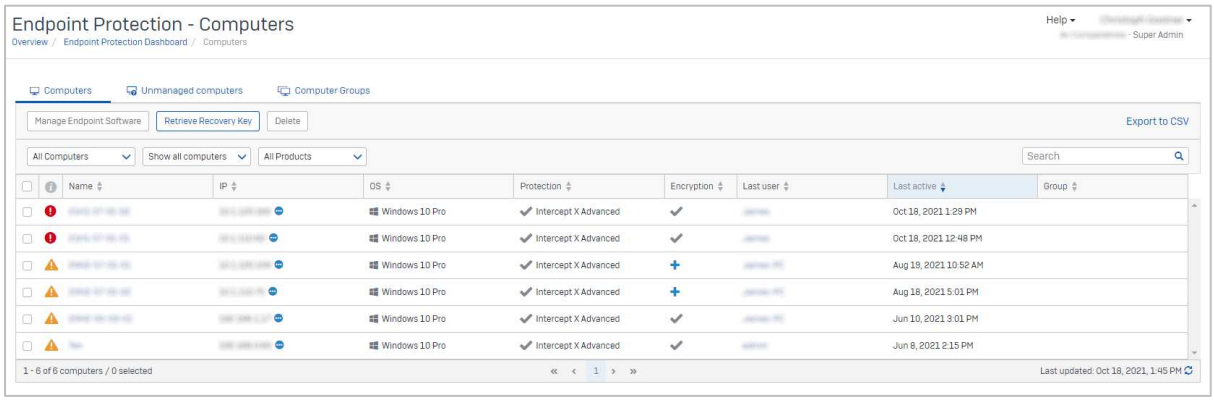
The *Endpoint Protection* sub-console has menu entries for *Dashboard, Logs & Reports, People, Computers, Policies, Settings, and Protect Devices*. The *Dashboard* page is similar in design to that of its counterpart in the main console. It shows many of the same panels, including *Most recent threat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

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

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

The *Settings* page lets you configure options to be applied to the whole network. Examples include *Directory Service, Role Management* (standard and custom permissions for console users*), Tamper Protection, Website Management, Proxy Configuration,* and *Data Loss Prevention Rules*. You can download installers for the endpoint protection client from the *Protect Devices* page.

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

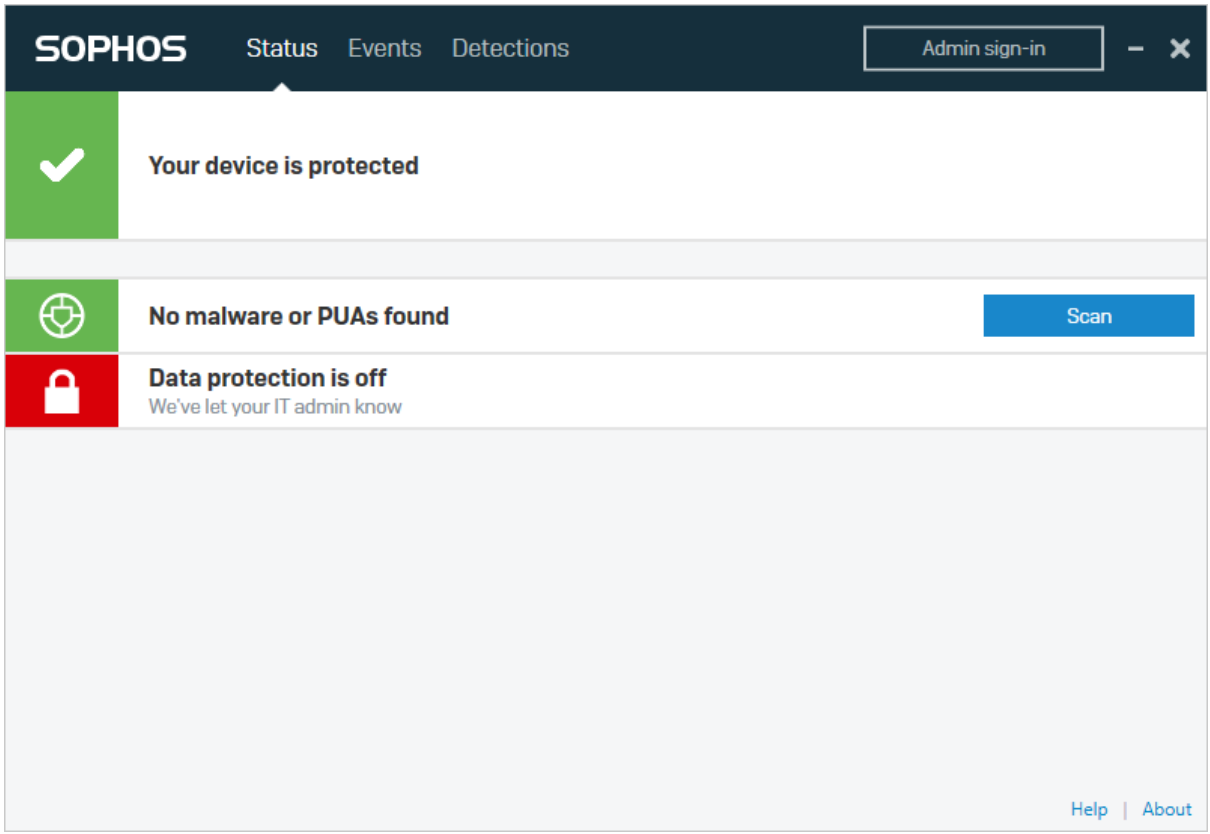


Windows Endpoint Protection Client

Deployment

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

User interface

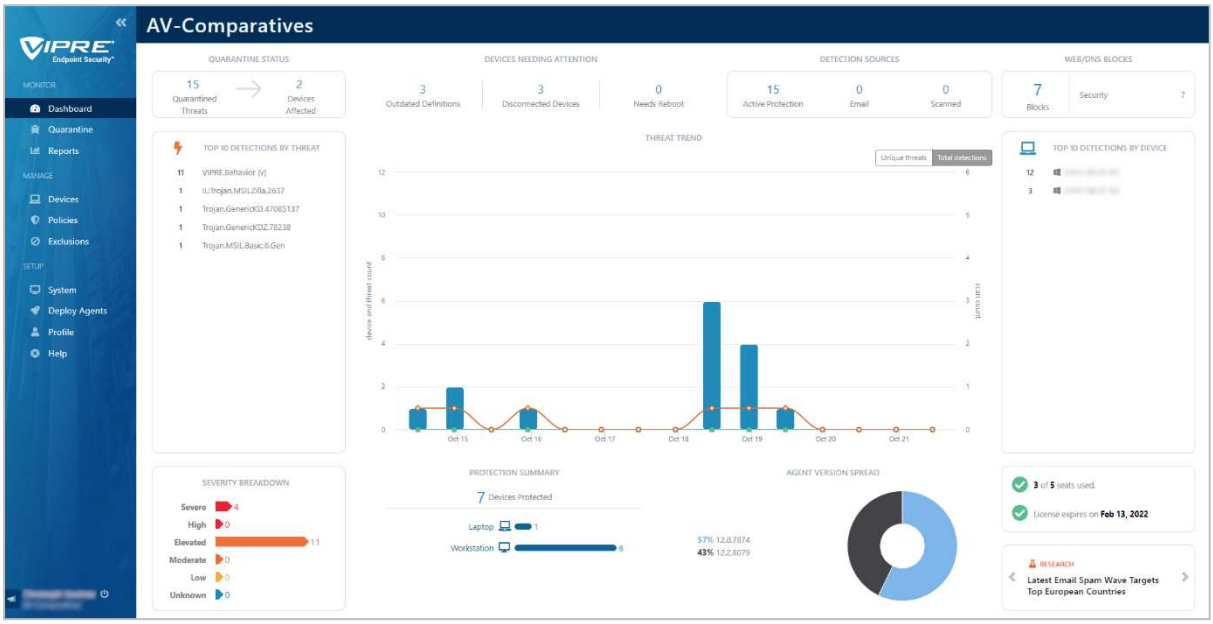


The user interface on protected endpoints consists of a System Tray icon and a program window. Users can see the protection status and detection logs, and run default scans. They can also scan a file, folder or drive using Windows Explorer's right-click menu.

Malware detection scenario

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

VIPRE Endpoint Cloud



About the product

VIPRE Endpoint Cloud provides a cloud-based console for managing the endpoint protection software, as you would expect. The product can manage networks with thousands of devices. We feel it would also be very suitable for very small businesses with just a few seats.

Advantages

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

Management Console

Dashboard page

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

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

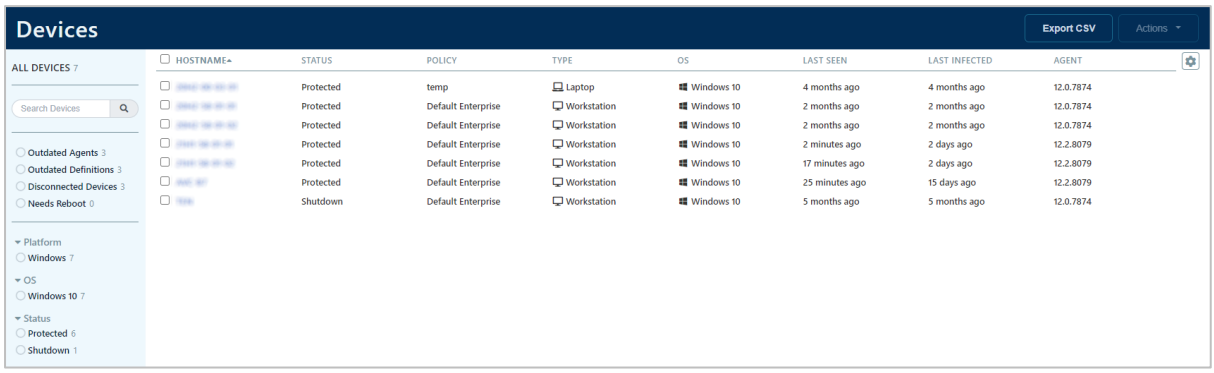
Quarantine page

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

Reports page

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

Devices page



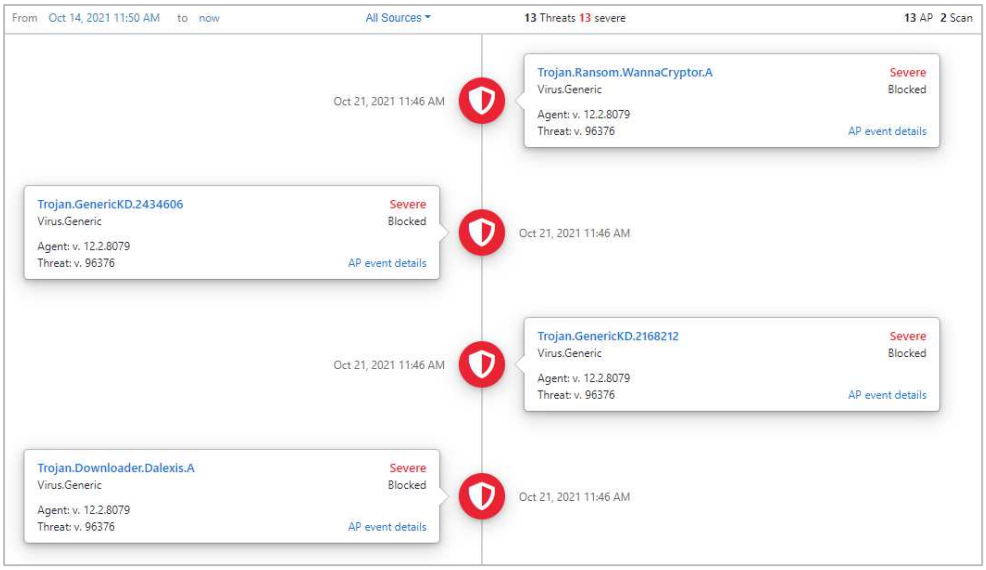
The *Devices* page, shown above, lists network computers, and displays useful information. Items include status, policy, OS, and agent version. The information columns can be customised. You can add additional items such as the user, last scan, IP address or last update, as well as/instead of the standard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

Having found the computers you were looking for, you can then carry out tasks on them from the *Actions* menu. Available actions are: *Assign Windows Policy, Full Scan, Quick Scan, Update Definitions, Schedule Agent Update, Update Agent Now, Reboot Devices, Stop Agent, Uninstall Agent,* and *Delete*

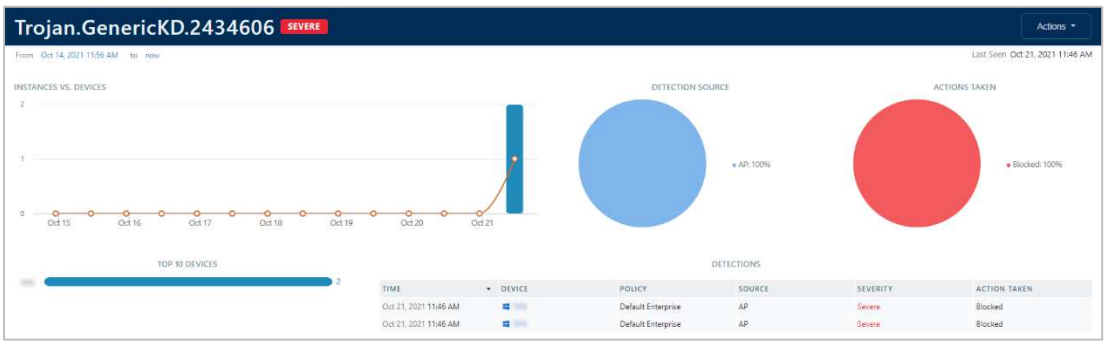
Device. *Uninstall Agent* removes the endpoint software, but keeps associated data. This might be useful if you want to reinstall or change the agent version. *Delete Device* removes associated data and deactivates the licence.

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

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



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



Policies page

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

Exclusions page

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

System page

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

Deploy Agents page

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

Profile page

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

Windows Endpoint Protection Client

Deployment

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

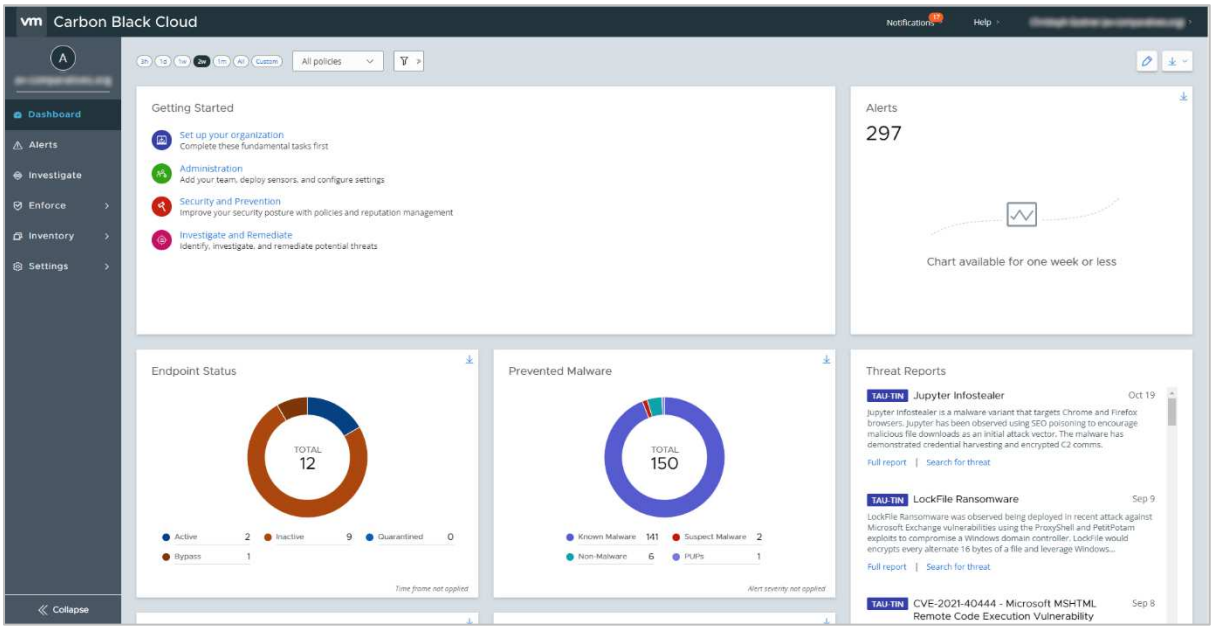
User interface

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

Malware detection scenario

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

VMware Carbon Black Cloud Endpoint Standard



About the product

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

Advantages

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

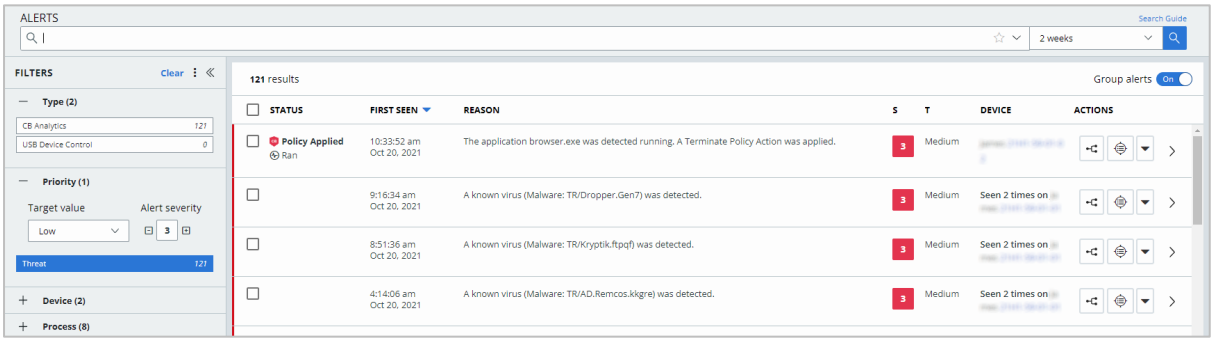
Management console

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

Dashboard page

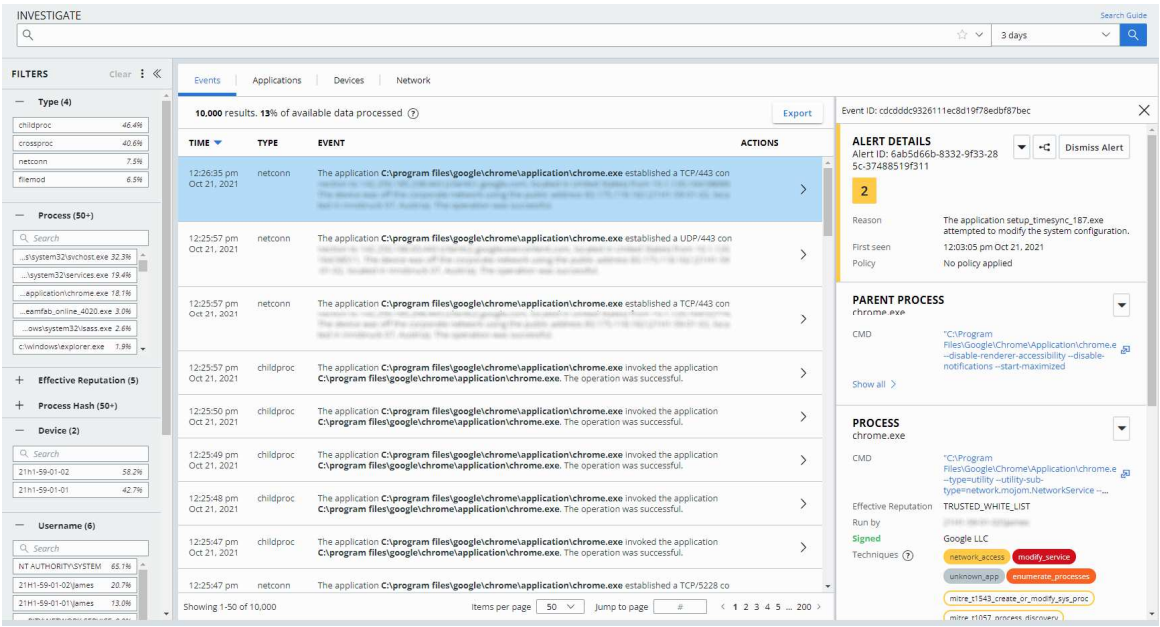
The *Dashboard* page (screenshot above) shows you an overview of security-related items, displayed in panels. These are *Alerts, Endpoint Status, Prevented Malware, Top Alerted Assets, Top Alerted Applications* and *Threat Reports* (security blog). The *Getting Started* panel shows links for common tasks, such as adding console administrators. You can customise the dashboard by moving panels around and removing any you don't need.

Alerts page



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

Investigate page



On the *Investigate* page, you can see a chronological list of events for any individual device. As with the *Alerts* page, there is a wide variety of filtering criteria shown in a panel on the left-hand side. By clicking on the *Actions* (arrowhead) button, you can see further information about the process, parent process, child process and device. This allows you to monitor network connections and program executions, and build up a detailed picture of security-related events. Drop-down menus in the details panel let you take actions such as adding the file to approved or banned lists, checking with VirusTotal, deleting or quarantining.

Enforce\Policies page

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

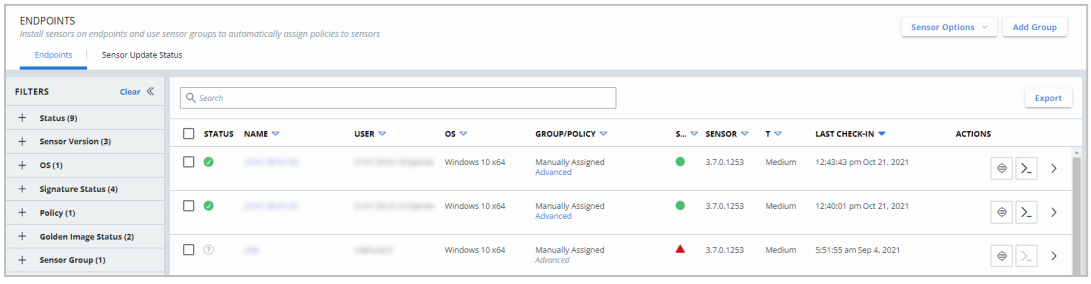
Enforce\Malware Removal page

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

Enforce\Cloud Analysis page

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

Inventory/Endpoints page



The *Endpoints* page, shown above, provides an overview of devices on the network. A search box lets you search for a specific client in a larger network. For each device, details are kept to a very manageable level (status, user, details of the OS and sensor version, policies and last check-in time). However, you can easily get more information about an individual device just by clicking on the arrowhead symbol at the right-hand end of its entry. This will show items such as the scan engine version, internal and external IP addresses, and who installed the endpoint protection software. Clicking on a device's name will open the *Investigate* page for that individual device. The *Go Live* button at the end of each device's entry establishes a remote administration session with the device. You can use the filter drop-downs to narrow the search for specific devices. By selecting a device or devices, you can carry out actions, such as scans, updates, policy changes and sensor updates. You can also quarantine a device. This cuts all network connections to and from it, with the exception of those to and from the management console.

Settings menu

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

Windows Endpoint Protection Client

Deployment

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

User interface

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

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

Features (as of December 2021)	Acronis Cyber Protect Cloud with Advanced Security pack	Avast Business Antivirus Pro Plus	Bitdefender GravityZone Elite	Cisco Secure Endpoint Essentials	CrowdStrike Falcon Pro	Cybereason Enterprise	Elastic Security	ESET PROTECT Entry & ESET PROTECT Cloud	FireEye Endpoint Security	Fortinet FortiClient with EMS, FortiSandbox & FortiEDR	G Data Endpoint Protection Business	K7 Cloud Endpoint Security Advanced	Kaspersky Endpoint Security for Business Select, with KSC	Malwarebytes EDR	Microsoft Defender Antivirus with MEM	Panda Endpoint Protection Plus on Aether	Sophos Intercept X Advanced	VIPRE Endpoint Cloud	VMware Carbon Black Cloud Endpoint Standard
Available Console Types																			
Cloud-based console	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•
On-premise server-based console	•	•	•	•		•	•	•	•			•	•					•	
Multi-tenancy features for managed service providers (included/paid extra/not included)	Included	Included	Included	Paid Extra	Included	Included	Included	Included	N/A	Included	Included	N/A	Included	Included	N/A	N/A	Included	Included	Included
Client software deployment methods																			
Creation of .exe or .msi installer package	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•
Share a link to remote users to install the software themselves		•	•	•	•		•	•		•	•	•	•	•	•	•	•	•	•
Push installation from the console	•	•	•	•			•	•		•	•	•	•	•	•	•		•	
Supported Operating Systems																			
Microsoft Windows	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•
Virtual environments (such as VMware, HyperV)	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•
Apple macOS	•	•	•	•	•	•	•	•	•	•	•		•	•	•	•	•	•	•
Linux	•		•	•	•	•	•	•	•	•	•		•		•	•	•	•	•
Google Android			•	•	•	•		•		•	•		•		•	•	•	•	
Apple iOS			•	•	•	•		•		•	•		•				•	•	
Windows Features																			
Anti-Malware	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•
Protection settings are enabled by default (out-of-the-box-protection)		•	•	•	•	•	•	•			•	•	•	•	•	•	•	•	•
Can clean-up a previously infected system (incl. registry leftovers and inactive malware)	•	•	•			•		•	•	•	•	•	•	•	•	•	•	•	•
Right-click on-demand scan of files/folders		•	•	•				•		•	•	•	•	•		•	•	•	
The online malware detection rate is the same as offline	•		•	•	•		•	•	•		•	•						•	•
Scans files only on execution (by default/design)					•										•				
Phishing protection (blocking of phishing URLs)	•	•	•	•				•			•	•	•	•	•	•	•	•	
Web access control / webfilter (custom blacklisting of URLs / site categories)	•		•	•		•		•			•	•	•		•	•	•		
Firewall		•	•	•		•		•				•	•		•	•	•	•	
Anti-Spam			•					•			•				•	•	•	•	
Data or Email encryption	•		•													•	•		
Splunk support			•	•	•	•	•		•	•	•		•	•			•		•
Settings & Uninstall protection		•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•
Cross-platform central management	•	•	•	•	•	•	•	•	•	•	•		•	•	•	•	•	•	•
Registers as AV product in Windows Security Center	•	•	•	•	•	•		•	•	•	•	•	•	•	•	•	•	•	•
Languages																			
Which languages can be used to contact support?	English, Japanese, German, Italian, French, Spanish, Korean	English, Czech, Japanese, French, German, Portuguese, Norwegian	English, Spanish, German, Romanian, French	All	English	English, Japanese	English	All	English, Japanese, French, Italian, Spanish, Portuguese, Arabic, Turkish, 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, Mandarin	English, German, Italian, Spanish, French	All	All	English, Italian, German, Spanish, French Japanese	English, Swedish, Danish	All
Which interface languages is the product available in?	English, German, Japanese, Russian, French, Italian, Spanish, Korean, Chinese, Polish, Czech, Hungarian, Danish, Dutch, Turkish, Indonesian, Portuguese, Bulgarian, Norwegian, Swedish, Finnish, Serbian, Malay	English, Spanish, French, German, Italian, Portuguese, Russian, Norwegian, Dutch, Bulgarian, Chinese, Czech, Estonian, Finnish, Greek, Hungarian, Japanese, Korean, Polish, Slovak, Slovenian, Swedish, Turkish, Ukrainian, Vietnamese	English, Spanish, German, Romanian, French, Italian, Portuguese, Polish, Russian, Czech, Chinese, Korean, Turkish	English, Japanese, Korean, Chinese	English, Japanese			English, Arabic, Chinese, Croatian, Czech, French, German, Greek, Hungarian, Indonesian, Italian, Japanese, Korean, Polish, Portuguese, Russian, Spanish, Slovak, Turkish, Ukrainian	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	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; 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	High	High	High	Very high	Average	Low	High	Very high	N/A	Low	Average	Very high	Very High	Average	Average	Average	High
On-premise Windows-based console			N/A	Very High	N/A						Low				N/A	N/A			N/A

Copyright and Disclaimer

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

AV-Comparatives
(December 2021)