

Independent Tests of Anti-Virus Software



Business Security Test

TEST PERIOD: AUGUST – NOVEMBER 2022

LAST REVISION: 10TH DECEMBER 2022

WWW.AV-COMPARATIVES.ORG

Content

INTRODUCTION	3
TESTED PRODUCTS	4
SETTINGS	5
MANAGEMENT SUMMARY	7
AV-COMPARATIVES' APPROVED BUSINESS PRODUCT AWARD	9
REAL-WORLD PROTECTION TEST (AUGUST-NOVEMBER)	10
MALWARE PROTECTION TEST (SEPTEMBER)	15
PERFORMANCE TEST (OCTOBER)	17
REVIEWS	22
ACRONIS CYBER PROTECT CLOUD WITH ADVANCED SECURITY PACK	23
AVAST ULTIMATE BUSINESS SECURITY	27
BITDEFENDER GRAVITYZONE BUSINESS SECURITY PREMIUM	31
CISCO SECURE ENDPOINT ESSENTIALS	36
CROWDSTRIKE FALCON PRO	41
CYBEREASON ENTERPRISE	45
ELASTIC SECURITY	50
ESET PROTECT ENTRY & ESET PROTECT CLOUD	54
G DATA ENDPOINT PROTECTION BUSINESS	58
K7 ON-PREMISES ENTERPRISE SECURITY	62
KASPERSKY ENDPOINT SECURITY FOR BUSINESS SELECT	66
MALWAREBYTES EDR	70
MICROSOFT DEFENDER ANTIVIRUS WITH MICROSOFT ENDPOINT MANAGER	74
SOPHOS INTERCEPT X ADVANCED	78
TRELLIX ENDPOINT SECURITY (HX)	82
VIPRE ENDPOINT PROTECTION CLOUD	86
VMWARE CARBON BLACK CLOUD ENDPOINT STANDARD	91
WATCHGUARD ENDPOINT PROTECTION PLATFORM	95
FEATURE LIST	99
COPYRIGHT AND DISCLAIMER	100

Introduction

This is the second half-year report of our Business Main-Test Series¹ of 2022, containing the results of the Business Real-World Protection Test (August-November), Business Malware Protection Test (September), Business Performance Test (October), as well as the Product Reviews.

The test series consists of three main parts:

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

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

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

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

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

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

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

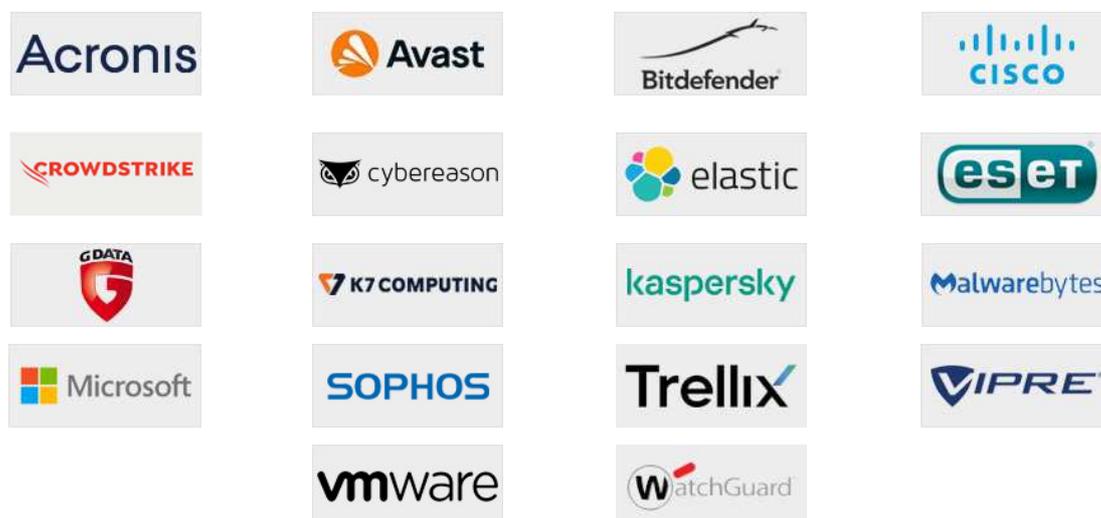
¹ Please note that the results of the Business Main-Test Series cannot be compared with the results of the Consumer Main-Test Series, as the tests are done at different times, with different sets, different settings, etc.

Tested Products

The following business products² were tested under Microsoft Windows 10 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	Ultimate Business Security	22.6	22.7	22.7	22.9
Bitdefender	GravityZone Business Security Premium	7.6	7.6	7.7	7.7
Cisco	Secure Endpoint Essentials	8.0	8.0	8.0	8.1
CrowdStrike	Falcon Pro	6.42	6.44	6.45	6.47
Cybereason	Enterprise	21.2	21.2	21.2	22.1
Elastic	Security	8.3	8.4	8.4	8.5
ESET	PROTECT Entry with ESET PROTECT Cloud	9.0	9.0	9.0	9.1
G Data	Endpoint Protection Business	15.2	15.2	15.3	15.3
K7	On-premises Enterprise Security Advanced	14.2	14.2	14.2	14.2
Kaspersky	Endpoint Security for Business – Select, with KSC	11.9	11.9	11.10	11.10
Malwarebytes	EDR	1.2	1.2	1.2	1.2
Microsoft	Defender Antivirus with MEM	4.18	4.18	4.18	4.18
Sophos	Intercept X Advanced	10.8	10.8	10.8	10.8
Trellix	Endpoint Security (HX)	34.28	34.28	34.28	35.31
VIPRE	Endpoint Protection Cloud	12.3	12.3	12.3	12.3
VMware	Carbon Black Cloud Endpoint Standard	3.8	3.8	3.8	3.8
WatchGuard	Endpoint Protection Platform	8.0	8.0	8.0	8.0

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**, **G Data**, **Trellix** 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 note that some enterprise products have all their protection features disabled by default, so the admin has to configure the product to get any protection.

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

Acronis: "Backup", "Vulnerability assessment", "Patch management", "Device control", "Data Loss Prevention" and "Data protection map" disabled. "Third-party scan engine" enabled.

Avast: "Scan for potentially unwanted programs (PUPs)" was enabled in "File Shield", "Web Shield" and "Mail Shield".

Bitdefender: "Sandbox Analyzer" (for Applications and Documents) enabled. "Analysis mode" set to "Monitoring". "Scan SSL" enabled for HTTP and RDP. "HyperDetect" and "Device Control" disabled. "Update ring" changed to "Fast ring". "Web Traffic Scan" and "Email Traffic Scan" enabled for Incoming emails (POP3). "Ransomware Mitigation" enabled. "Process memory Scan" for "On-Access scanning" enabled. All "AMSI Command-Line Scanner" settings enabled for "Fileless Attack Protection".

Cisco: "On Execute File and Process Scan" set to Active; "Exploit Prevention: Script Control" set to "Block"; "TETRA Deep Scan File" disabled; "Exclusions" set to "Microsoft Windows Default"; Engines "ETHIS", "ETHOS", "SPERO" and "Step-Up" disabled.

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" disabled; "Artificial intelligence" and "Anti-Exploit" set to "Moderate"; "Exploit protection", "PowerShell and .NET", "Anti-Ransomware" and "App Control" enabled and set to "Prevent"; "Exploit protection set to "Cautious"; all "Collection features" enabled; "Scan archives on access" enabled; Update interval set to 1 minute.

Elastic: MalwareScore (“windows.advanced.malware.threshold”) set to “aggressive”, and Rollback-SelfHealing (“windows.advanced.alerts.rollback.self_healing.enabled”) enabled.

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

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

Kaspersky: “Adaptive Anomaly Control” disabled; “Detect other software that can be used by criminals to damage your computer or personal data” enabled.

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”, “Malicious LoadLibrary Protection” and “Protected applications” 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; “CloudExtendedTimeOut” set to 55; “PuaMode” enabled.

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

Trellix: “Real-Time Indicator Detection” disabled, “Exploit Guard” and “Malware Protection” enabled.

VIPRE: “Firewall” and “IDS” enabled and set to “Block With Notify”.

VMware: policy set to “Advanced”.

K7, WatchGuard: 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 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 and **K7** use server-based consoles that will prove very straightforward for experienced Windows professionals. These could be used by the SME sector upwards.

For businesses of the same size looking for cloud-based management solutions, **Bitdefender**, **ESET**, **Kaspersky**, **Microsoft**, **Sophos** and **WatchGuard** 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** and **Trellix** 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 2022 as an "Approved Business Product" by AV-Comparatives, the tested products must score at least 90% in the Malware Protection Test, with zero false alarms on common business software, and an FP rate on non-business files below the *Remarkably High* threshold. Additionally, products must score 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 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 2022:



Although Cisco achieved good malware protection scores, it unfortunately did not reach all the requirements for the December 2022 Approved Award. This was due to the level of false positives on non-business files. We hope to see these issues resolved in the 2023 tests.

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 they would probably do in that situation).

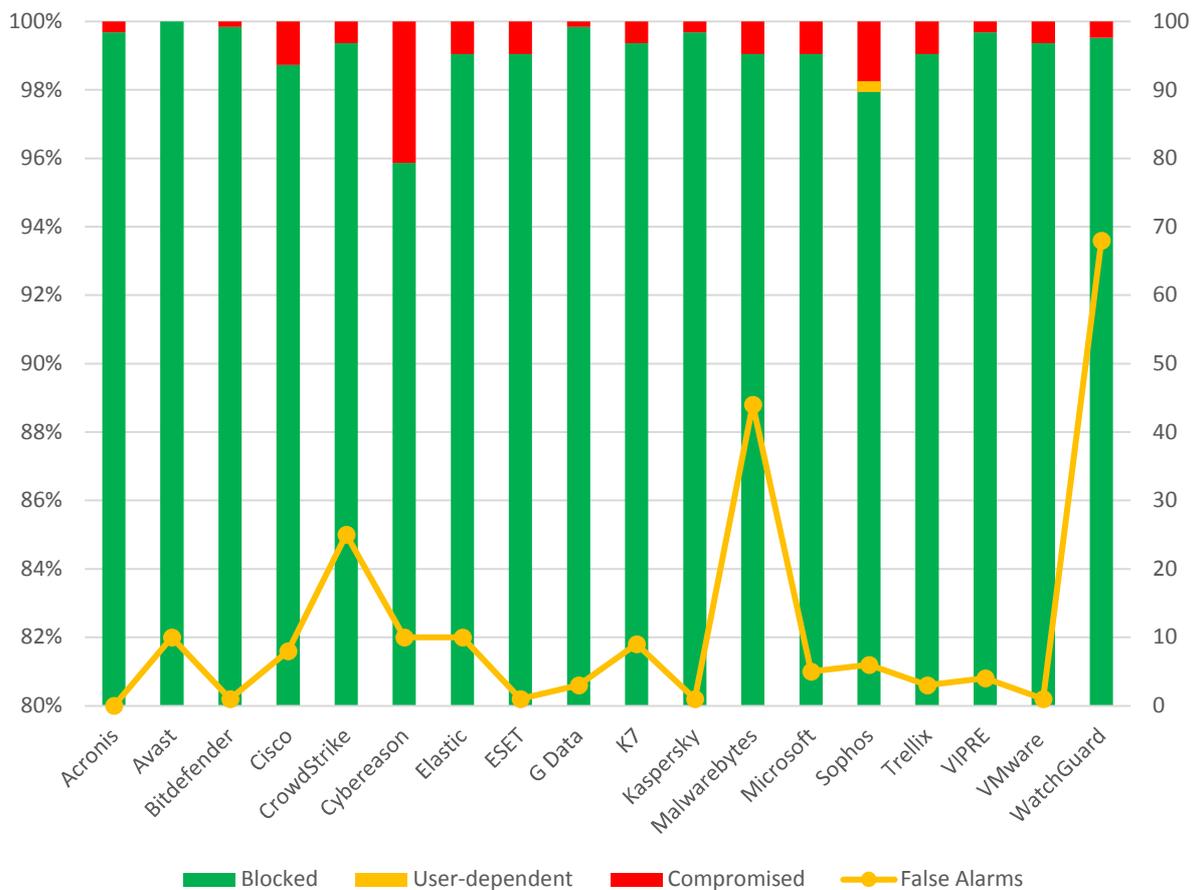
Due to the dynamic nature of the test, i.e. mimicking real-world conditions, and because of the way several different technologies (such as cloud scanners, reputation services, etc.) work, it is a matter of fact that such tests cannot be repeated or replicated in the way that e.g. static detection rate 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 **629** test cases (such as malicious URLs), tested from the beginning of August 2022 till the end of November 2022.



	Blocked	User dependent	Compromised	PROTECTION RATE [Blocked % + (User dependent %)/2] ³	False Alarms
Avast	629	-	-	100%	10
Bitdefender	628	-	1	99.8%	1
G Data	628	-	1	99.8%	3
Acronis	627	-	2	99.7%	0
Kaspersky	627	-	2	99.7%	1
VIPRE	627	-	2	99.7%	4
WatchGuard	626	-	3	99.5%	68
VMware	625	-	4	99.4%	1
K7	625	-	4	99.4%	9
CrowdStrike	625	-	4	99.4%	25
ESET	623	-	6	99.0%	1
Trellix	623	-	6	99.0%	3
Microsoft	623	-	6	99.0%	5
Elastic	623	-	6	99.0%	10
Malwarebytes	623	-	6	99.0%	44
Cisco	621	-	8	98.7%	8
Sophos	616	2	11	98.1%	6
Cybereason	603	-	26	95.9%	10

³ 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.

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

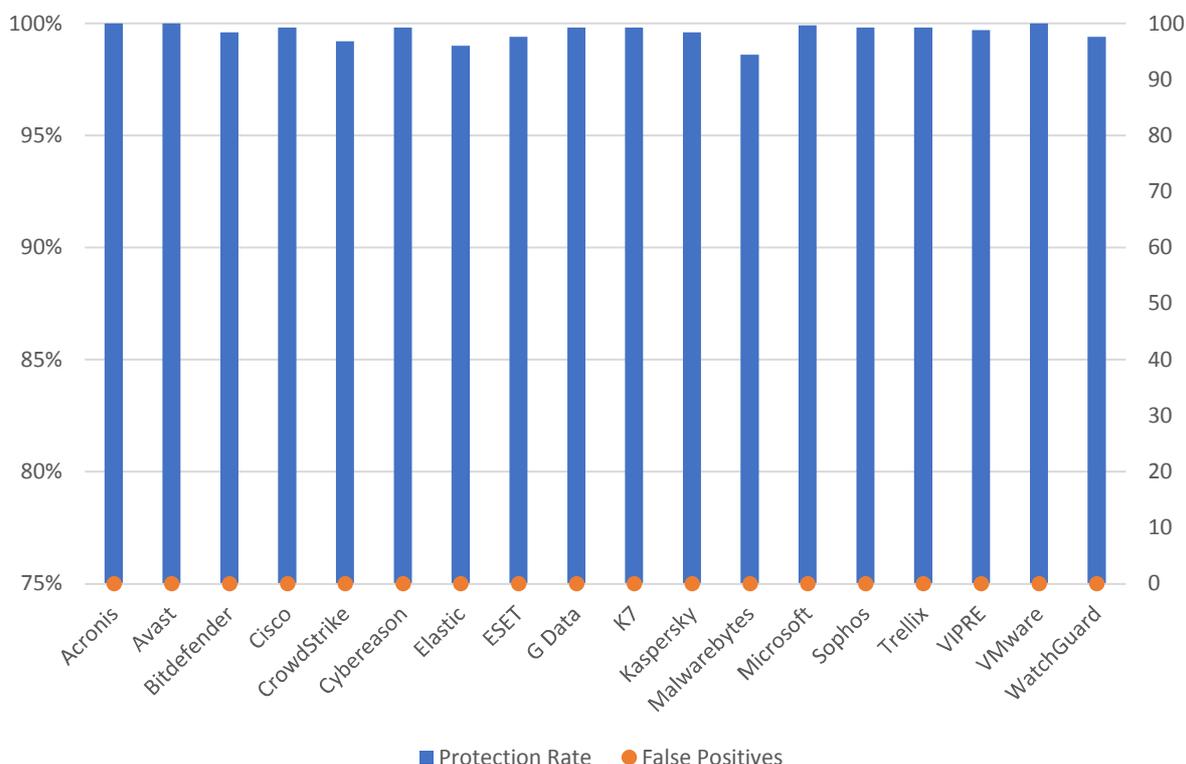
Malware Protection Test (September)

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. behavioural detection features to come into play. If a product does not prevent or reverse all the changes made by a particular malware sample within a given time period, that test case is considered to be a miss. For this test, **1,005** recent malware samples were used.

False positive (false alarm) test with common business software

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

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



	Malware Protection Rate	False Alarms on common business software
Acronis, Avast, VMware	100%	0
Microsoft	99.9%	0
Cisco, Cybereason, G Data, K7, Sophos, Trellix	99.8%	0
VIPRE	99.7%	0
Bitdefender, Kaspersky	99.6%	0
ESET, WatchGuard	99.4%	0
CrowdStrike	99.2%	0
Elastic	99.0%	0
Malwarebytes	98.6%	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. Results are shown in the tables below; the false alarms found were promptly fixed by the respective vendors. However, organisations which often use uncommon or non-business software, or their own self-developed software, might like to consider these results. Products are 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 settings that cause excessive levels of false positives.

FP rate	Number of FPs on non-business files
Very Low	0-5
Low	6-15
Medium/Average	16-35
High	36-75
Very High	76-125
Remarkably High	>125

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

It should be noted that Cisco had *Remarkably High* levels of false positives on non-business files. Administrators should consider whether this might create problems in their respective organisations' specific environments.

Performance Test (October)

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 8 GB 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: copying⁴ 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).

⁴ 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



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 Edition⁵ testing suite. Users using PC Mark 10 benchmark⁶ 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 website⁷.

“No security software” is tested on a baseline⁸ system without any security software installed, which scores 100 points in the PC Mark 10 benchmark.

	PC Mark Score
<i>Baseline</i>	100
ESET	99.2
Bitdefender	99.0
WatchGuard	98.9
Malwarebytes, VIPRE	98.4
Avast, G Data	98.2
Kaspersky	97.9
Trellix	97.7
Elastic	97.6
VMware	97.5
CrowdStrike	97.4
K7	97.3
Cybereason	97.0
Microsoft	96.4
Acronis	95.3
Sophos	93.4
Cisco	92.5

⁵ For more information, see <https://benchmarks.ul.com>

⁶ PC Mark® is a registered trademark of Futuremark Corporation / UL.

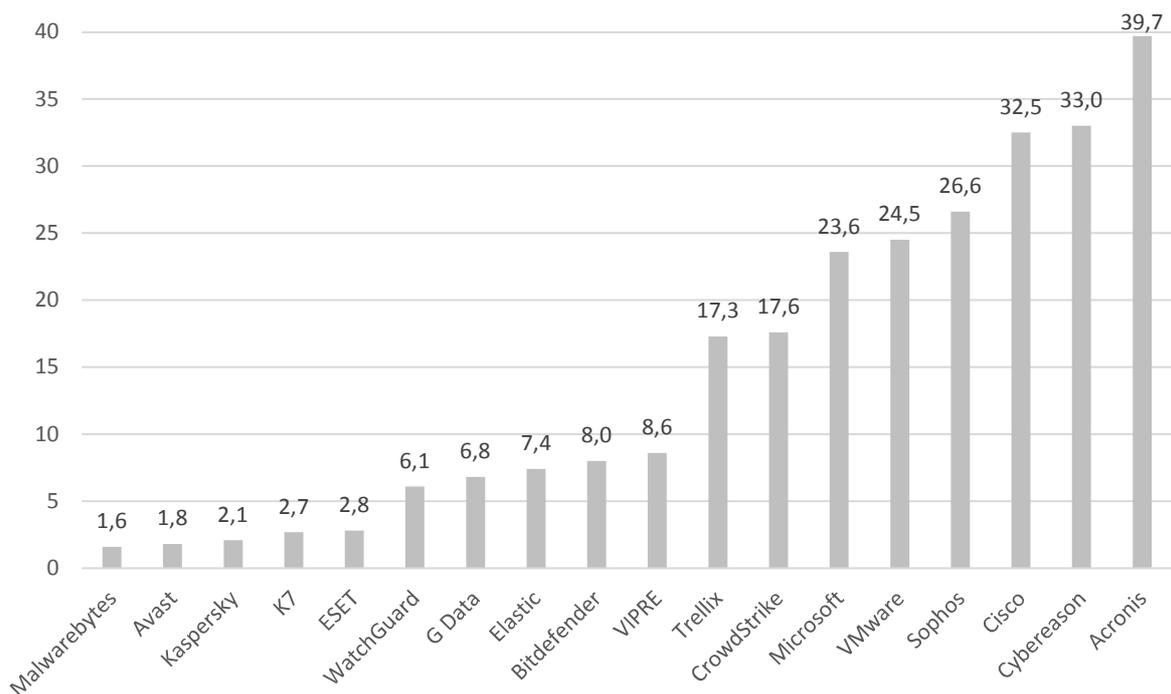
⁷ http://s3.amazonaws.com/download-aws.futuremark.com/PCMark_10_Technical_Guide.pdf (PDF)

⁸ 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
Malwarebytes	90	98.4	188.4	1.6
Avast	90	98.2	188.2	1.8
Kaspersky	90	97.9	187.9	2.1
K7	90	97.3	187.3	2.7
ESET	88	99.2	187.2	2.8
WatchGuard	85	98.9	183.9	6.1
G Data	85	98.2	183.2	6.8
Elastic	85	97.6	182.6	7.4
Bitdefender	83	99.0	182.0	8.0
VIPRE	83	98.4	181.4	8.6
Trellix	75	97.7	172.7	17.3
CrowdStrike	75	97.4	172.4	17.6
Microsoft	70	96.4	166.4	23.6
VMware	68	97.5	165.5	24.5
Sophos	70	93.4	163.4	26.6
Cisco	65	92.5	157.5	32.5
Cybereason	60	97.0	157.0	33.0
Acronis	55	95.3	150.3	39.7



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. 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.

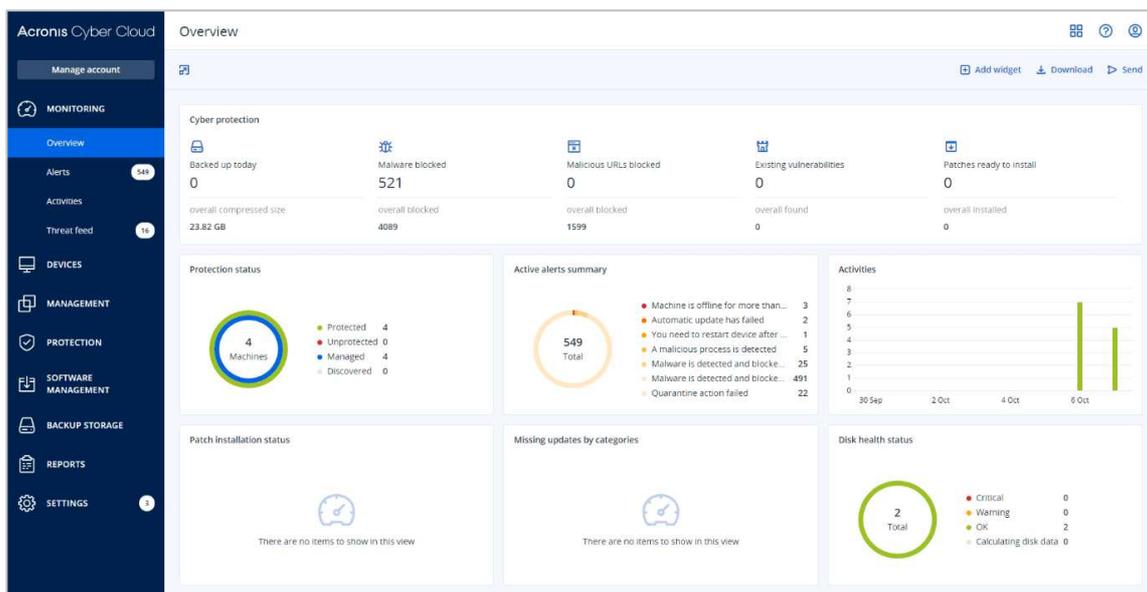
For server-based products, we describe the process of getting the console installed on the server (this is obviously not applicable to cloud-based consoles).

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. Other add-on packs are also available from the vendor. 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 *Monitoring*, *Devices*, *Management*, *Protection*, *Software Management*, *Backup Storage*, *Reports*, and *Settings*. The numbers shown to the right of each menu item represent items such as threats and alerts that the administrator should look at.

Monitoring\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*. The *Cyber protection* 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.

Monitoring\Alerts page

The screenshot shows the 'All alerts' page. On the left, there is a sidebar with categories: All alerts (549), Malware detected (521), Critical (Machine is offline for more than 30 days - 3), Error (Automatic update has failed - 2), Warning (You need to restart device after installing a new agent - 1, Quarantine action failed - 22, A malicious process is detected - 5, Malware is detected and blocked (RTP) - 25, Malware is detected and blocked (ODS) - 491). The main area shows a detailed view of a malware alert: 'Malware is detected and blocked (RTP)' on Oct 07, 2022, 15:12. The alert description states: 'Anti-Malware Protection has detected and blocked the malware 'Trojan.AgentWDCR.DXA' during the real-time scan.' The details include: Device, Plan name (ProtectionPlan 2022), File name (4.exe), File path (E:\), MD5, SHA1, SHA256, Threat name (Trojan.AgentWDCR.DXA), and Action (Moved to quarantine). A 'Support' link and a 'Clear' button are also visible.

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 (*Plan*), 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.

Monitoring/Threat feed page

The screenshot shows the 'Threat feed' page with a table of threats. The table has columns for Name, Type, and Date. There are also checkboxes for each row and a gear icon for settings. The threats listed are:

Name	Type	Date
Novel Chaos malware infect Windows and Linux for DDOS attacks	Malware	Oct 3, 2022
New Lazarus Crypto stealer targeting MacOS	Malware	Oct 2, 2022
Zero-Day unpatched Microsoft Exchange being actively exploit	Vulnerability	Oct 1, 2022
New Royal Ransomware demands a high amount of ransom payment	Malware	Sep 29, 2022

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\All devices page

The screenshot shows the 'All devices' page with a table of devices. The table has columns for Type, Name, Account, #CyberFit Score, Status, Last backup, Next backup, and Plan. There are also checkboxes for each row and a gear icon for settings. The devices listed are:

Type	Name	Account	#CyberFit Score	Status	Last backup	Next backup	Plan
VM	192.168.1.10	www.202208.comparatives.org	625/850	Suspicious activity is detected	Never	Not scheduled	ProtectionPlan 2022
VM	192.168.1.10	www.202208.comparatives.org	625/850	Suspicious activity is detected	Never	Not scheduled	ProtectionPlan 2022
VM	192.168.1.10	www.202208.comparatives.org	625/850	Malware is detected and blocked (RTP)	Never	Not scheduled	ProtectionPlan 2022

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 (virtual machine or hardware) 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 (as in the screenshot above), or large tiles with additional details. Selecting a device in the list 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.

Management/Protection plans page

Under *Management/Protection plans*, 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, exploit prevention, crypto-mining process detection, scheduled scanning, and exclusions. On other tabs of the menu pane, you can also configure other items such as URL filtering, vulnerability assessments and patch management.

Protection\Quarantine page

Under *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, using the page settings. A mini menu at the end of each entry lets you whitelist, restore or delete the selected items.

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 *Reports* page 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 apply a protection plan.

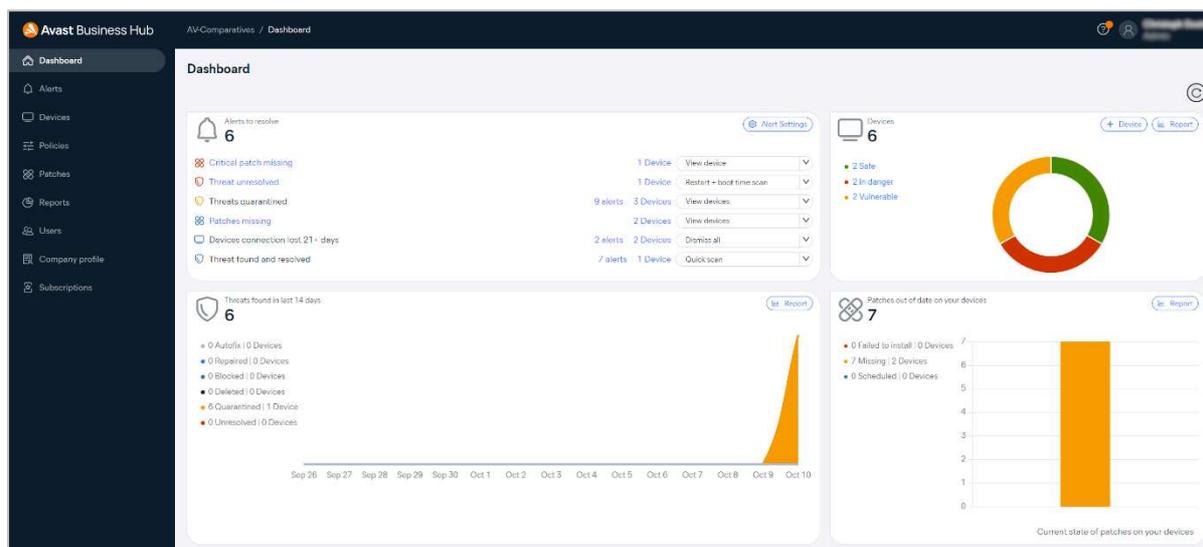
User interface

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. Settings for backup encryption and proxy server can also be changed here. Users can scan a folder or file for malware by right-clicking it in Windows File Explorer.

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 Ultimate Business Security



About the product

Avast Ultimate Business Security provides a cloud-based console for managing the endpoint protection software. Additional features for Windows clients include USB device control, a replacement firewall, data shredding, a VPN, and data & identity protection. Exchange and SharePoint security are provided for Windows Servers, and a full patch management feature is included for all Windows computers. This review considers only the malware protection features, however. 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 and install security software
- Includes patch management, a VPN, data shredding, data/identity protection, and device control

Management console

Dashboard page

The default *Dashboard* page provides an overview of the current security status. You can see alerts to resolve, threats detected, number of devices in safe/vulnerable/dangerous states, patch status, 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.

Alerts page

This shows important alerts (from various sources) such as malware detections, and devices that are out of date or need rebooting. You can click on any alert to open a panel showing relevant details. 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 opens a configuration panel, where you can choose which notifications to show in the console, and whether to send email reminders.

Devices \ Managed devices page

The Managed devices tab shows each device's status and alerts, OS, group membership and policy, along with AV status, patch status, and last-seen date. Additional items (e.g. IP address, Backup, VPN) can be added by clicking on the *Manage columns* button on the right-hand end of the table header. Using the buttons and menus in the top right-hand corner, you can run various tasks on selected computers, such as restarting, scanning, updating, 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.

Devices | Network discovery page

The screenshot displays the Avast Network Discovery interface. At the top, there are tabs for 'Managed devices' and 'Network discovery' (marked as BETA). Below the tabs, there is a 'Scan' button and a 'Last scan completed' indicator. Summary statistics show 3 unmanaged devices, 0 installing devices, and 0 installation failures. A table lists detected devices with columns for Device name, IP address, Seen by, Last detected, and Status. Three devices are listed: one Intel, one Fujitsu, and one Apple, all with a status of 'Unmanaged'.

Device name	IP address	Seen by	Last detected	Status
(Intel)			3 minutes ago	Unmanaged
(Fujitsu)			3 minutes ago	Unmanaged
(Apple)			3 minutes ago	Unmanaged

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. To do this, you first need to designate a currently managed device 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

You can use the Avast default policy or configure your own protection settings for managed devices. A wide range of settings can be configured in each policy. There are sections for *General Settings* (including updates, troubleshooting and restart options); *Service Settings* (antivirus, patch management, VPN, firewall and USB device control); *Exclusions* (for antivirus, patch management, and USB protection); and *Assignments* (devices to which the policy is applied).

Reports page

There are ten different report categories for Avast Ultimate Business Security: *Executive Summary*, *Device Report*, *Task Report*, *Audit Log*, *Antivirus Threat Report*, *Patch Report*, *Remote Control Report*, *Cloud Backup Overview*, *Cloud Backup History* and *USB Protection Report*. You can click on any of these headings to see a graphical representation of recent activity. For example, *Antivirus Threat Report* shows a graph of threats 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.

Subscriptions page

As you would expect, this shows you the product licences you currently have, the number used, and when they expire.

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. From the *Add Device* panel, 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.

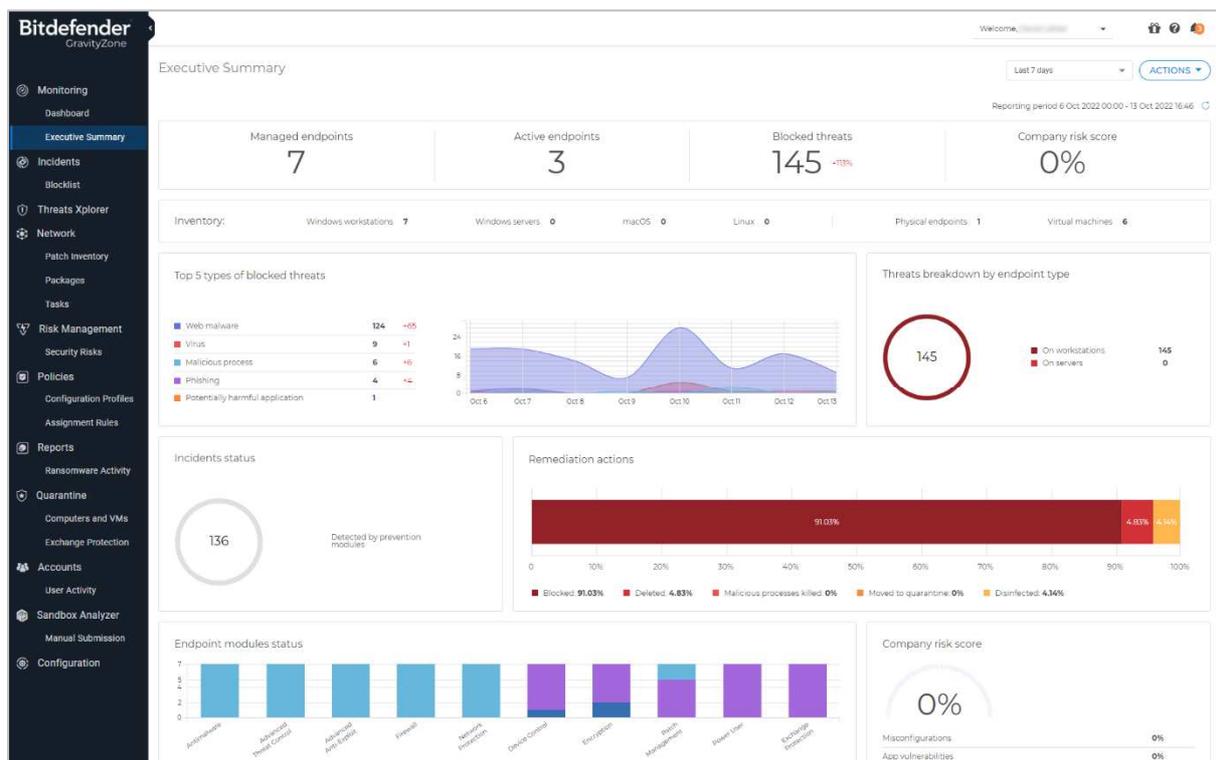
User interface

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, targeted, boot-time and custom scans. They can also scan a file, folder or drive, or perform sandbox analysis on a file, 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, 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. Pop-up alerts were 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 Business Security Premium



About the product

Bitdefender GravityZone Business Security Premium 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

Detected Threats									
OPEN INCIDENTS High 1 Medium 113 Low 811		TOP ALERTS URL.Malicious 666 Alert.HTTPFileDownloaded 649 ATC.Malicious 166				TOP AFFECTED DEVICES [Device Name] 480 [Device Name] 440 [Device Name] 4			
ID	Date	Status	Severity Score	Priority	Action taken	Endpoint	Alerts	Assigned to	
#6805	Updated 10 minutes ago	Open	45	Unassigned	Reported	[Endpoint]	6	Unassigned	[Process Tree Icon]
#6804	Updated 30 minutes ago	Open	45	Unassigned	Reported	[Endpoint]	7	Unassigned	[Process Tree Icon]
#6803	Created 58 minutes ago	Open	59	Unassigned	Reported	[Endpoint]	6	Unassigned	[Process Tree Icon]
#6802	Updated 1 hour ago	Open	45	Unassigned	Reported	[Endpoint]	4	Unassigned	[Process Tree Icon]
#6801	Updated 3 hours ago	Open	60	Unassigned	Reported	[Endpoint]	6	Unassigned	[Process Tree Icon]

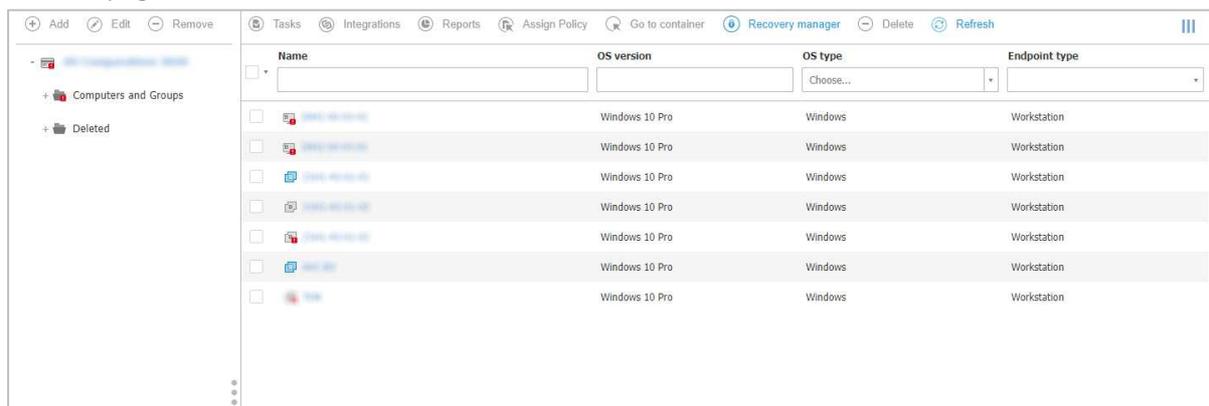
Incidents allows you to review and investigate threats detected on the network. By default, it displays a chronological list of detected threats. There are columns for threat ID, date and time, status of investigation, severity score, priority, action taken, endpoint, number of alerts, and console user assigned to investigate it. Panels at the top show the number of open incidents by severity, greatest number of 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 Explorer page

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

Network page



The main *Network* page (screenshot above) shows you all the managed devices on your network, ordered into groups which you can create yourself. 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. A menu bar along the top of the main pane lets you e.g. run reports, assign policy, or delete devices. The *Tasks* menu here includes various actions that can be taken on selected devices, such as scans, updates, repairs and restarts.

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

Risk Management Dashboard page

Here you can see a wide range of data that you can use to proactively protect your network. Various different panels use coloured charts to display relevant items of information. The *Company Risk Score* gives you a rating from 1 to 100, based on *Misconfiguration*, *App Vulnerabilities*, and *User Behavior Risks* (unsafe behaviour by users). For each of these items, there is a separate details panel. There is also *Score Over Time*, a timeline of risks 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 misconfigurations, vulnerable apps, user behaviour risks, devices and users and that are summarised on the main page.

Policies page

Here you can change the configuration applied to 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

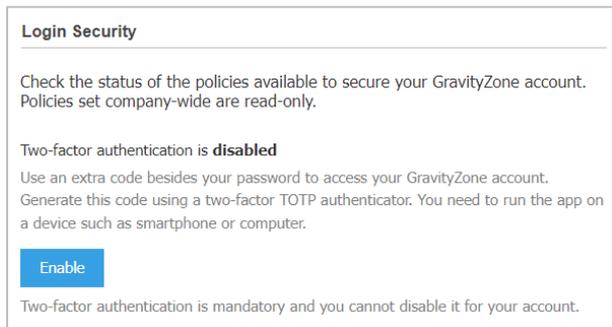
This lets you build information summaries on a wide variety of aspects, including blocked websites, device control activity, endpoint protection status, policy compliance and update status. The reporting interval can be set to this month, previous month, this year or previous year. You can also select 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 five 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. We note that 2-factor authentication for console login is not strictly enforced, even though the product states that it is mandatory. New users will see a prompt to set up 2FA when they log in, but this can be skipped. This situation is illustrated by the screenshot below:



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.

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, and a pop-up alert was shown to indicate that the malware had been detected. This closed 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

The screenshot displays the Cisco Secure Endpoint Essentials dashboard. At the top, the navigation menu includes Dashboard, Analysis, Outbreak Control, Management, and Accounts. A search bar is located in the top right corner. The main dashboard area features a large '40% compromised' indicator. Below this, there are several key sections:

- Inbox Status:** Shows 2 items requiring attention, 0 in progress, and 0 resolved.
- Compromises:** A red bar chart showing a significant increase in compromises, with a 'Protect' button.
- Quarantined Detections:** An orange bar chart showing a significant increase in detections, with a 'Protect' button.
- Vulnerabilities:** A blue bar chart showing a significant increase in vulnerabilities, with a 'Protect' button.
- Secure Malware Analytics:** Shows 582 automatic analysis submissions and 0 retroactive threat detections.
- Statistics:** Shows 5 computers, 63.2K files scanned, and 0 network connections logged.
- Quick Start:** Provides links to set up Windows, Mac, and Linux connectors.
- Significant Compromise Observables:** Lists file hashes and names such as netsh.exe, seeder.exe, and runonce.exe.
- Compromise Event Types:** Lists event types such as Command-line Obfuscation, Executed Malware, Firewall Rule Added, Item Added to Startup Folder, and Registry Run Key Removal.

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 Observables*, 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. From the details section of a suspected malicious file, you can click *Analyze*, allowing you to find more 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 bars and doughnut charts.

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.

Automated Actions

Automated Actions Action Logs
⊞ ⊕

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

High severity or higher in groups 5 selected

0 Compromise Events occurred in the last 7 days, affecting 0 distinct computers in the selected groups.

[View Changes](#) Save

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

High severity or higher in groups 5 selected

0 Compromise Events occurred in the last 7 days, affecting 0 distinct computers in the selected groups.

Rate Limit Rate limit must be between 1 and 1000.

[View Changes](#) Save

▼ **Submit to Secure Malware Analytics upon Detection** (5 computers in the selected groups can submit files to Secure Malware An...) Inactive

Medium severity or higher in groups 5 selected

12 Compromise Events occurred in the last 7 days, affecting 1 distinct computer in the selected groups.

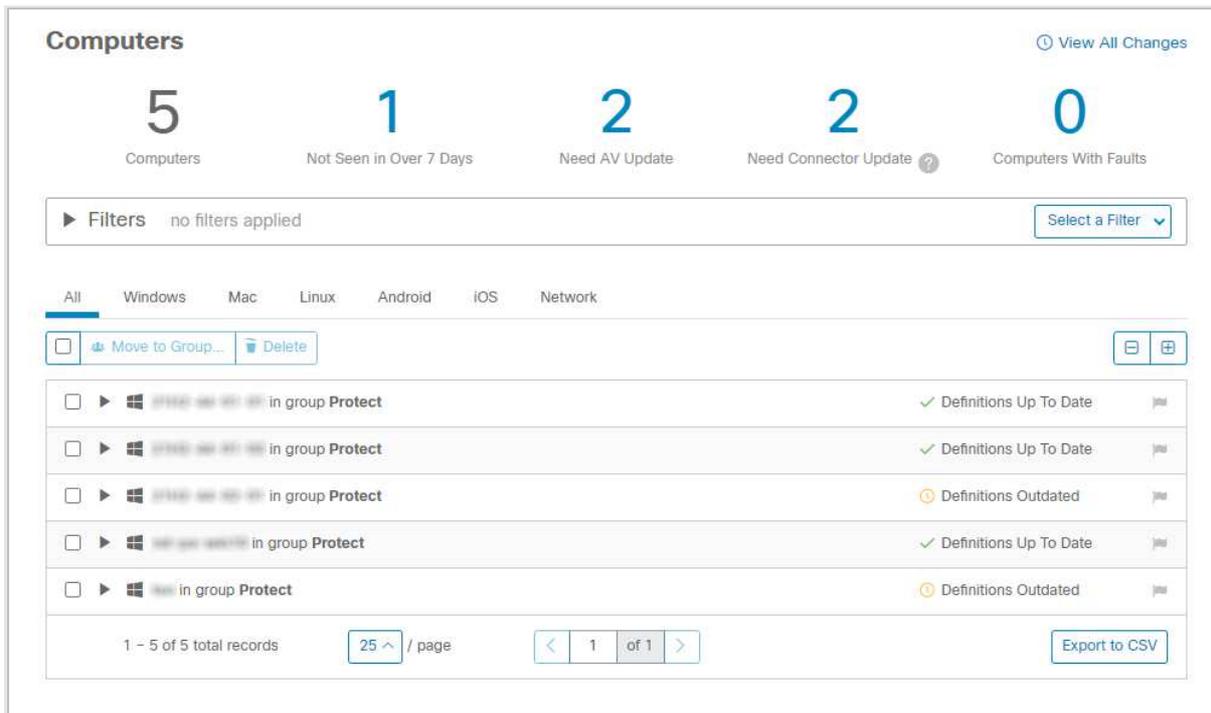
[View Changes](#) Save

▼ **Move Computer to Group upon Compromise** (5 computers in the selected groups can be moved) Inactive

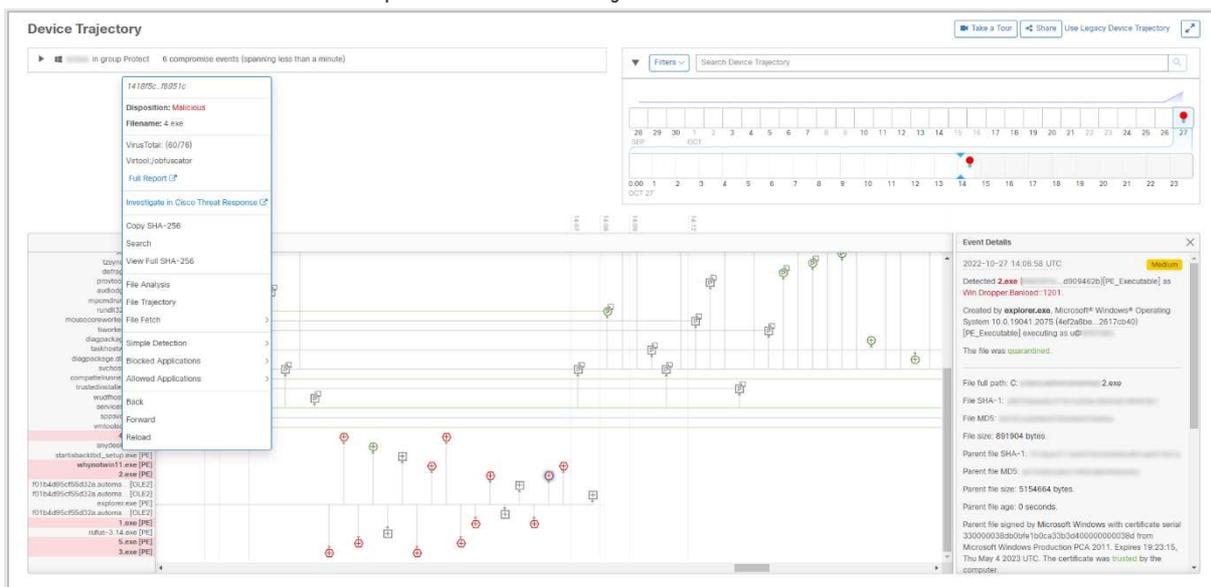
Management menu

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 (shown as red dots in the calendar section at 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, by using the *Enable Connector Protection* option in the applicable policy.

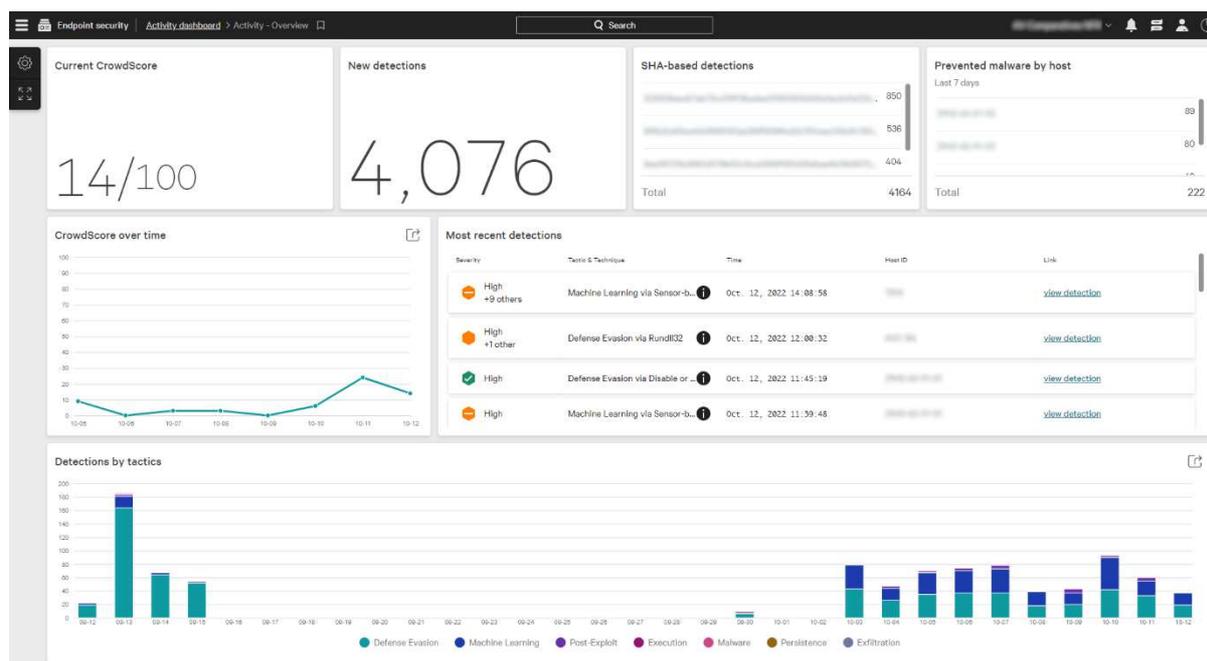
User interface

The GUI of the endpoint protection software includes a System Tray icon and program window. It allows users to run updates and scans, and view the logs. There is a choice of scans that users can run. These are *Flash Scan* (running processes), *Custom Scan*, or *Full 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 initially take any 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 and integrated threat intelligence 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. CrowdStrike Falcon Pro offers additional capabilities that were not included in this review: device control and firewall management.

Advantages

- Investigative functions
- Comprehensive search facilities
- Clickable interface provides easy access to details pages
- Integrated threat intelligence
- 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 top-level entries such as *Endpoint Security*, *Threat Intelligence*, *Investigate*, *Dashboards and Reports*, *Host Setup and Management*, *Audit Logs*, and *Support and Resources*. Each of these has its own sub-pages. 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\Activity Overview page

This is the page you see when you first log on to the console (screenshot above). 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 *Endpoint Detections* details page.

Endpoint Security\Endpoint Detections page

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

The screenshot displays a process tree on the left and a detailed execution panel on the right for the process `explorer.exe`.

Process Tree: A sequence of processes is shown: `SMSS.EXE` → `WINLOGON.EXE` → `USERINIT.EXE` → `EXPLORER.EXE`. The `EXPLORER.EXE` process is highlighted with a red hexagonal icon, indicating a detection.

Execution Details Panel:

- Status:** Unassigned
- Actions:** New, Comment
- Tags:** TEN, Network contain, Create ML exclus...
- Execution Details:**
 - DETECT TIME:** [Blank]
 - FIRST BEHAVIOR:** Oct. 12, 2022 14:08:58
 - MOST RECENT BEHAVIOR:** Oct. 12, 2022 14:08:58
 - HOSTNAME:** [Redacted]
 - HOST TYPE:** Workstation
 - USER NAME:** [Redacted]
 - ACTION TAKEN:** Files quarantined
 - SEVERITY:** High
 - OBJECTIVE:** Falcon Detection Method
 - TACTIC & TECHNIQUE:** Machine Learning via Sensor-based ML
 - TECHNIQUE ID:** CST0007
 - SPECIFIC TO THIS DETECTION:** A file written to the file-system meets the machine learning-based on-sensor AV protection's high confidence threshold for malicious files.
 - TRIGGERING INDICATOR:** Associated IOC (SHA256 on file write)

Endpoint Security\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, status, and of course date and time of detection. Quarantined files can be released, deleted or downloaded for analysis. Clicking the entry of 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 number, 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. CrowdStrike told us that protected endpoints automatically forward all quarantined files to Falcon Intelligence for investigation.

Endpoint Security\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.

Host Setup and Management\Host Management page

Host Management										
Type to filter										7 hosts found
Platform	OS Version	OU	Site	Type	Containment Status	Grouping Tags				
Windows	7 Windows 10	7 N/A	7 N/A	7 Workstation	7 Normal	7 N/A				
<input type="checkbox"/> 0 of 7 selected ACTIONS										
Hostname	Last Seen	First Seen	OS Version	OU	Prevention Policy	Response Policy	Sensor Update P...	Containment ...	Sensor Version	Grouping Tags
<input type="checkbox"/>	Oct. 12, 2022 16:...	Jan. 31, 2022 16:...	Windows 10		Default (Windo... Feb. 17, 2022 11:1...	Default (Windo... Jan. 31, 2022 16:...	Default (Windo... Changes pending	Normal	6.45.15907.0	
<input type="checkbox"/>	Oct. 12, 2022 10:...	Feb. 17, 2022 11:...	Windows 10		Default (Windo... Feb. 17, 2022 11:...	Default (Windo... Feb. 17, 2022 11:...	Default (Windo... Changes pending	Normal	6.45.15907.0	
<input type="checkbox"/>	Oct. 12, 2022 10:...	Sep. 13, 2022 14:...	Windows 10		Default (Windo... Sep. 13, 2022 14:...	Default (Windo... Sep. 13, 2022 14:...	Default (Windo... Changes pending	Normal	6.45.15907.0	
<input type="checkbox"/>	Sep. 30, 2022 10:...	Sep. 13, 2022 14:...	Windows 10		Default (Windo... Sep. 13, 2022 14:...	Default (Windo... Sep. 13, 2022 14:...	Default (Windo... Changes pending	Normal	6.44.15803.0	

The *Hosts/Host Management* page lists all the installed devices. You can immediately see which ones are online. Additional information includes operating system, policies, 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.

Threat 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\Hosts 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 *Hosts* page, you can look for specific devices.

Windows Endpoint Protection Client

Deployment

Installer files for the *sensor* (endpoint protection client) can be downloaded in .exe format from *Host Setup and Management\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.

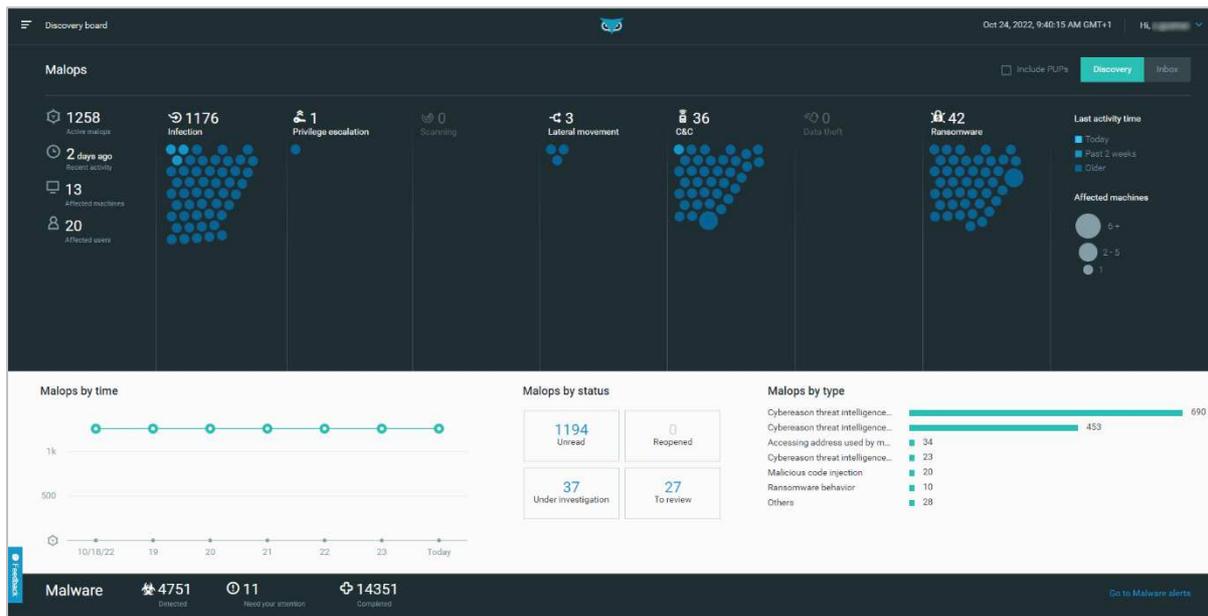
User interface

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. However, when we tried to copy the malicious files to the Windows Desktop, they were instantly deleted. Detections were immediately shown in the management console. 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

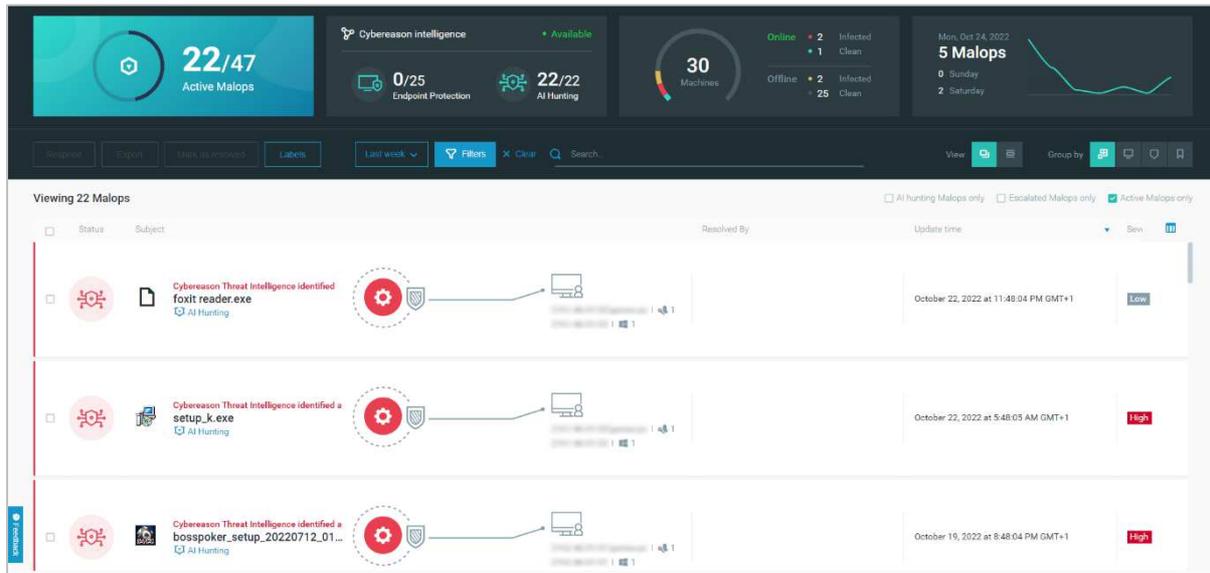
Management Console

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

Discovery board page

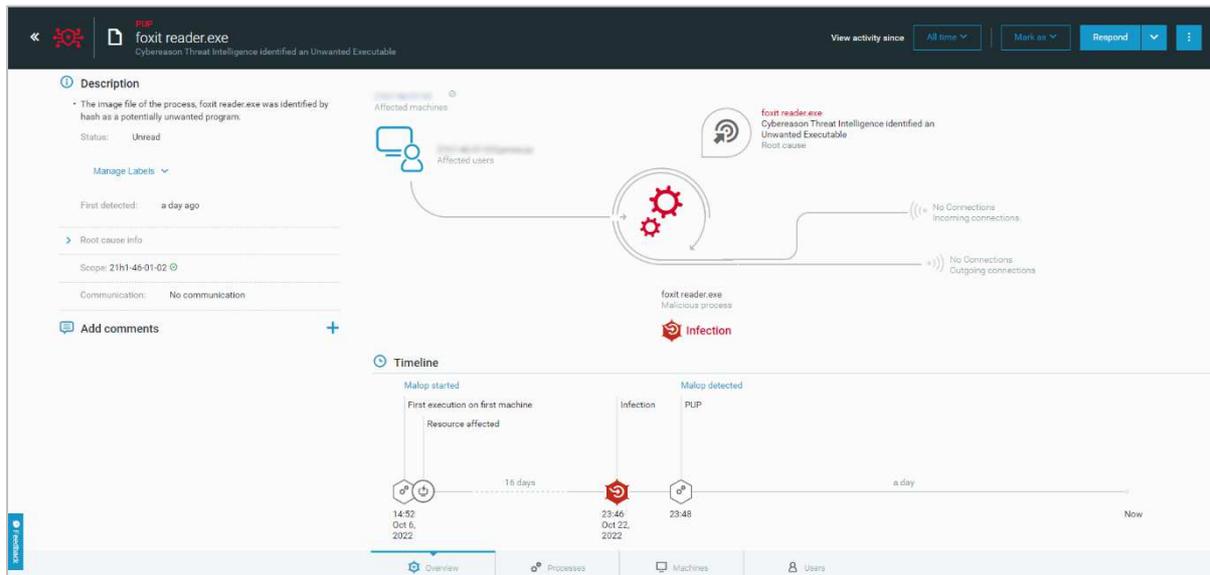
The *Discovery board* (shown in the screenshot above) is the page you will see when you first log on. It shows “MalOps” (malicious operations) in columns, according to type. The blue dots represent a malicious activity. The size of the dot represents the number of the affected machines, and the shade of colour refers to the time of the activity (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 and users, 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 with fewer graphics. Clicking on one of the MalOps opens its details page, shown below.

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 as 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 additional perspectives of processes, machines and users. The *Processes* tab includes a reference to the applicable stage of the MITRE ATT&CK® framework. The *Respond* button at the top of the page lets you carry out various actions to remediate the problem, including *Isolate*, *Quarantine*, *Prevent files execution*, and *Kill process*.

Malware alerts page

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

Investigation page

The *Investigation* page allows you to create customised hunts for malicious activity, using criteria such as machine, user, process, file, connection, domain name, registry entry, and detection event. 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 allow listing*, *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 provides a doughnut chart of the status of installed devices, with a colour-coding system for states such as *Enabled*, *Disabled* and *Offline*. Below this, a bar chart shows the proportion of up-to-date clients.

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 & Description*, *Anti-Malware*, *Exploit protection*, *Fileless protection*, *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.

System\Sensors page

The screenshot shows the 'System\Sensors' page in a security management console. At the top, there are several filter panels for 'Sensor status', 'Data collection', 'OS', 'Outdated', 'App Control mode', and 'Anti-Ransomware mode'. Below these filters, there is a table displaying a list of protected devices. The table has columns for Machine name, Data collection, Site, Sensor version, Last update stat., Last seen, First seen, OS, Internal IP address, App Control mode, and Anti-Ransomware mode. The table shows 1-8 results, and the first row is highlighted in a very pale grey color, indicating it is an offline computer.

Machine name	Data collection	Site	Sensor version	Last update stat.	Last seen	First seen	OS	Internal IP address	App Control mode	Anti-Ransomware mode
...	Advanced	Default	20.2.254.0	None	March 4, 2022 at 11:...	August 16, 2021	Windows	...	Enabled	Suspected and pre...
...	Advanced	Default	21.2.158.0	Already up to date	...	September 29, 20...	Windows	...	Enabled	Disabled
...	Advanced	Default	21.2.158.0	Already up to date	June 14, 2022 at 11:...	May 25, 2022 at 8:...	Windows	...	Enabled	Suspected and pre...
...	Advanced	Default	21.2.158.0	Already up to date	...	September 29, 20...	Windows	...	Enabled	Disabled

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.

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. The manual installation's setup wizard can be completed with a single click, and finishes in seconds.

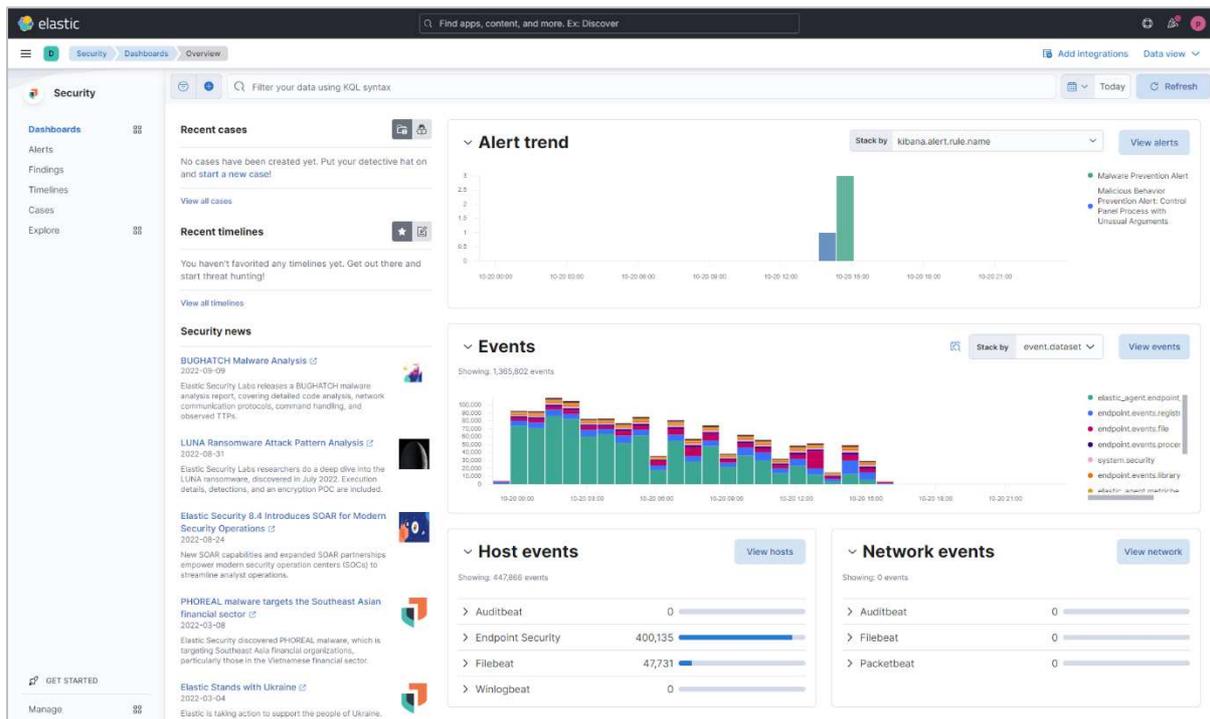
User interface

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. In this review, we have only looked at the security-related features of the console. These functions are accessed (as you would expect) from the *Security* tile on the home page of the main Elastic console. There is a single menu column on the left-hand side of the console, with the main categories *Dashboards*, *Alerts*, *Findings*, *Timelines*, *Cases*, *Explore* and *Manage*.

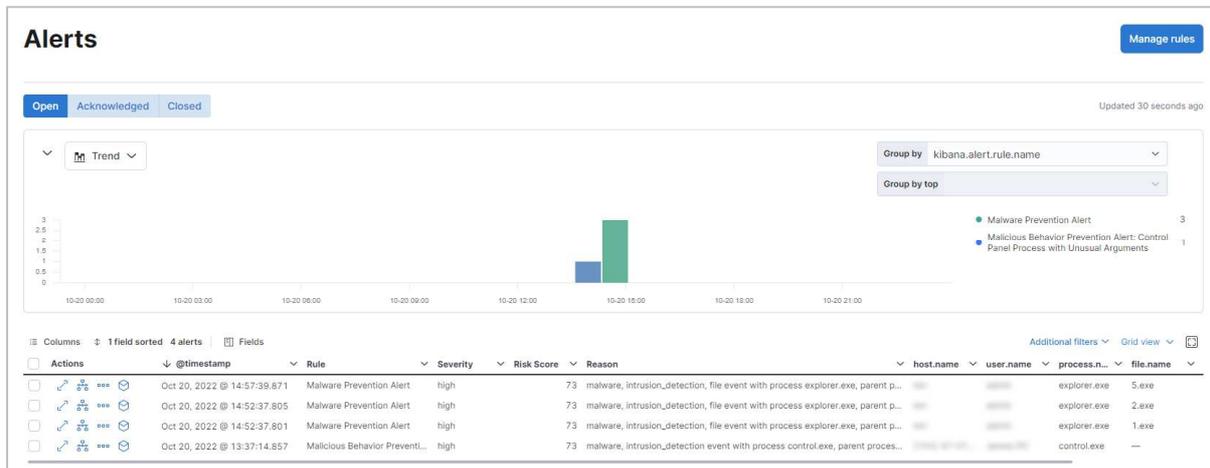
Dashboards \ *Overview* page

This page, shown in the screenshot above, gives you an overview of security-related events, shown in panels illustrated with bar graphs. You can see *Alert Trend*, *Events*, *Host Events*, *Network Events* and *Threat Intelligence*. Mousing over one of the graphs displays a panel with detailed breakdown information for that item. The *View...* button in the top right-hand corner of each panel links to the applicable details page of the console.

Dashboards \ Detection and Response page

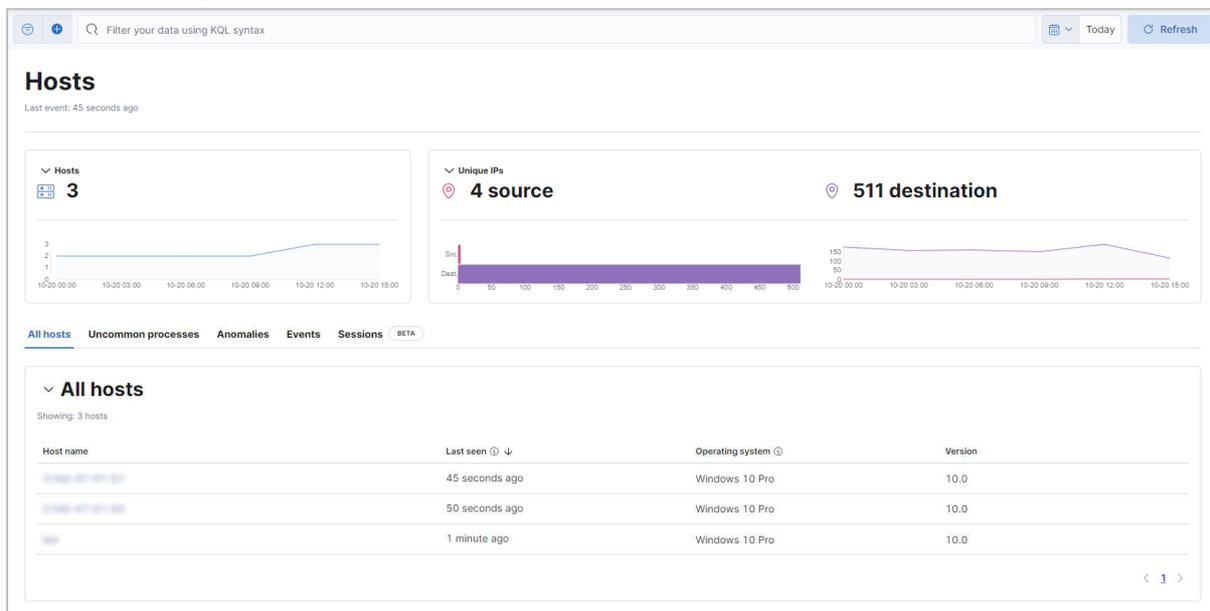
Here you can see *Alerts, Hosts by alert severity, Users by alert severity, and Cases* (investigations). The *Alerts* panel uses coloured doughnut charts to show open, acknowledged and closed alerts by severity. The time period for which alerts are displayed can be easily set to anything between the last hour and the last year.

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, Mark as closed, Add to new case* and *Add to existing case* are provided.

Explore \ Hosts page



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

Explore\Network page

Source IPs							Destination IPs						
Showing: 3 IPs							Showing: 514 IPs						
IP	Domain	Autonomous system	Bytes in	Byte... ↓	Flows	Destinat...	IP	Domain	Autonomous system	Byte... ↓	Bytes out	Flows	Source I...
192.168.1.1	—	—	710.1M B	2.4GB	0	338	192.168.1.1	—	—	1.9GB	12.8MB	0	2
192.168.1.2	—	—	704.7M B	1.6GB	0	369	192.168.1.2	—	—	1.2GB	172.1KB	0	2
127.0.0.1	—	—	4.1KB	0B	0	1	192.168.1.3	—	—	851.7M B	13.4MB	0	2
							oe DE			13.9MB	2.2MB	0	2
							oe DE						

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). Further panels show items such as network events and DNS queries.

Explore\Users page

Here you can see a list of all network computer-user accounts, including system accounts. For each account, security-related events such as logins are listed.

Manage section

From this page, you can access a variety of sub-menus, including *Endpoints*, *Policies*, *Rules*, *Exception Lists*, *Blocklists*, *Trusted Applications*, *Event Filters* and *Host Isolation Exceptions*.

Manage\Endpoints page

This displays a complete list of all endpoints on the network, even those in an inactive state. Here you can see agent status, applied policy, OS type, internal IP address, agent version, and last-seen date and time. The *Actions* menu lets you view further details, and isolate the endpoint.

Manage\Policies page

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.

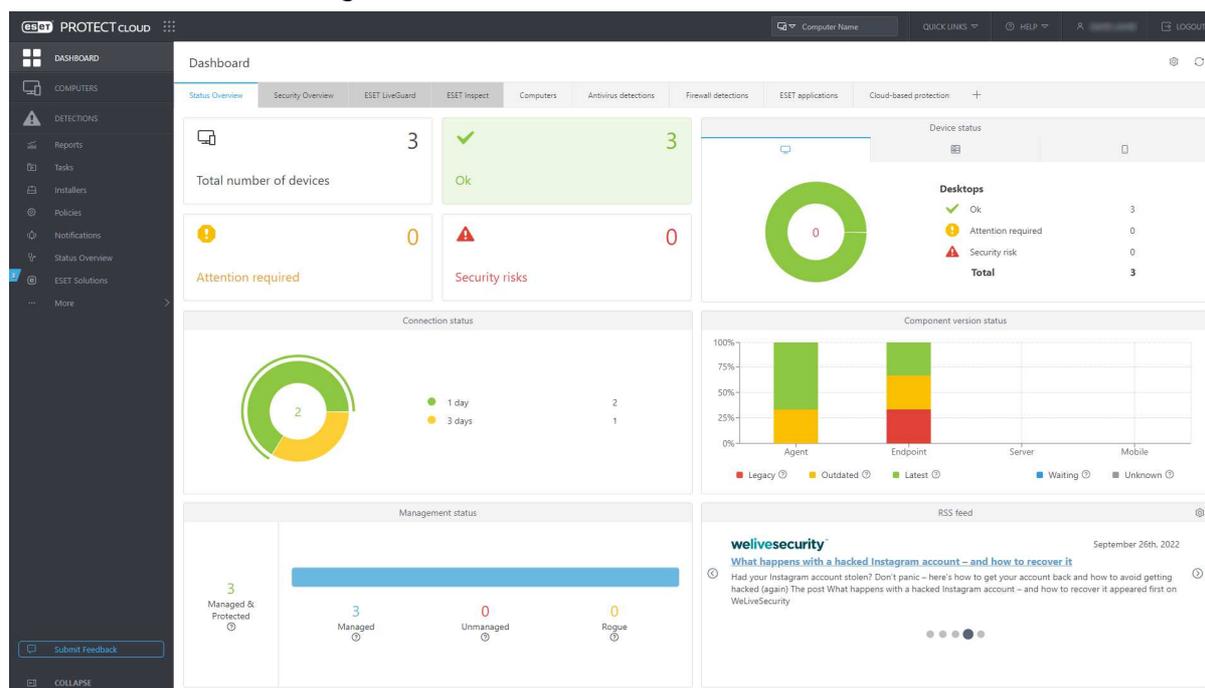
User interface

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 fully-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/Computers page

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

Groups	COMPUTER NAME	IP ADDRESS	STATUS	LAST CONNECTED	ALERTS	DETECTI...	OS NAME	LOGGED USERS	SECURITY PRODUCT
All (3)									
Companies (0)									
(3)									
Lost & found (0)									
Windows computers									
Linux computers									
Mac computers									
Devices with outdated modules									
Devices with an outdated operating system									
Problematic devices									
Unactivated security product									
Mobile devices									

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 *Devices with an 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 *Computer* menu at the bottom of the page. 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).

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*, *ESET LiveGuard*, *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.

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.

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*.

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*, *Mobile Devices*, *Agents*, *ESET components and security 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\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.

More\Exclusions page

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

More\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 quarantined files.

More\Computer Users page

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

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.

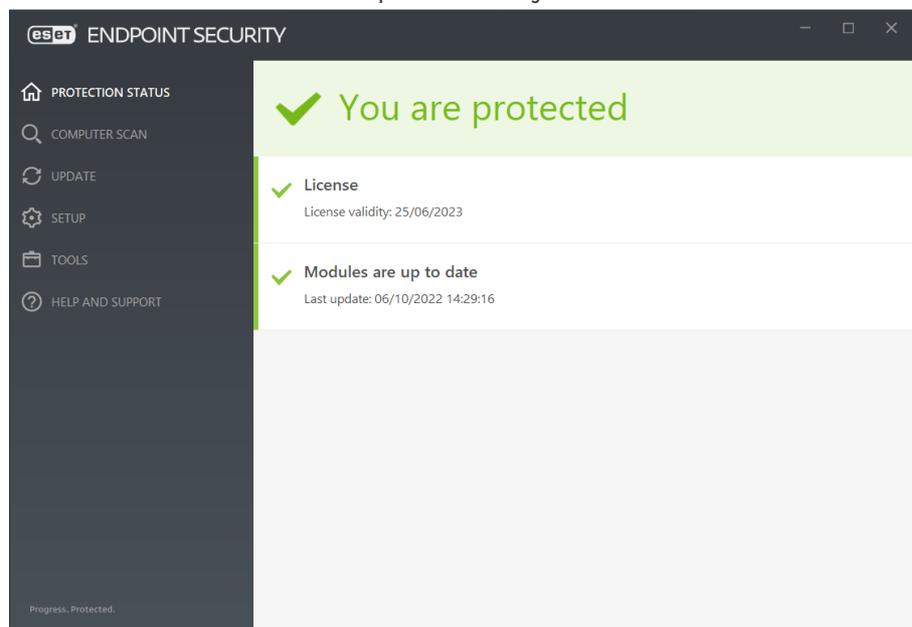
Windows Endpoint Protection Client

Deployment

Installer files in .exe or GPO/SCCM script format can be created and 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. We note that after installation, an initial scan of the endpoint is run automatically.

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 Antivirus and ESET File Security for Windows Servers use a virtually identical interface to ESET Endpoint Security.

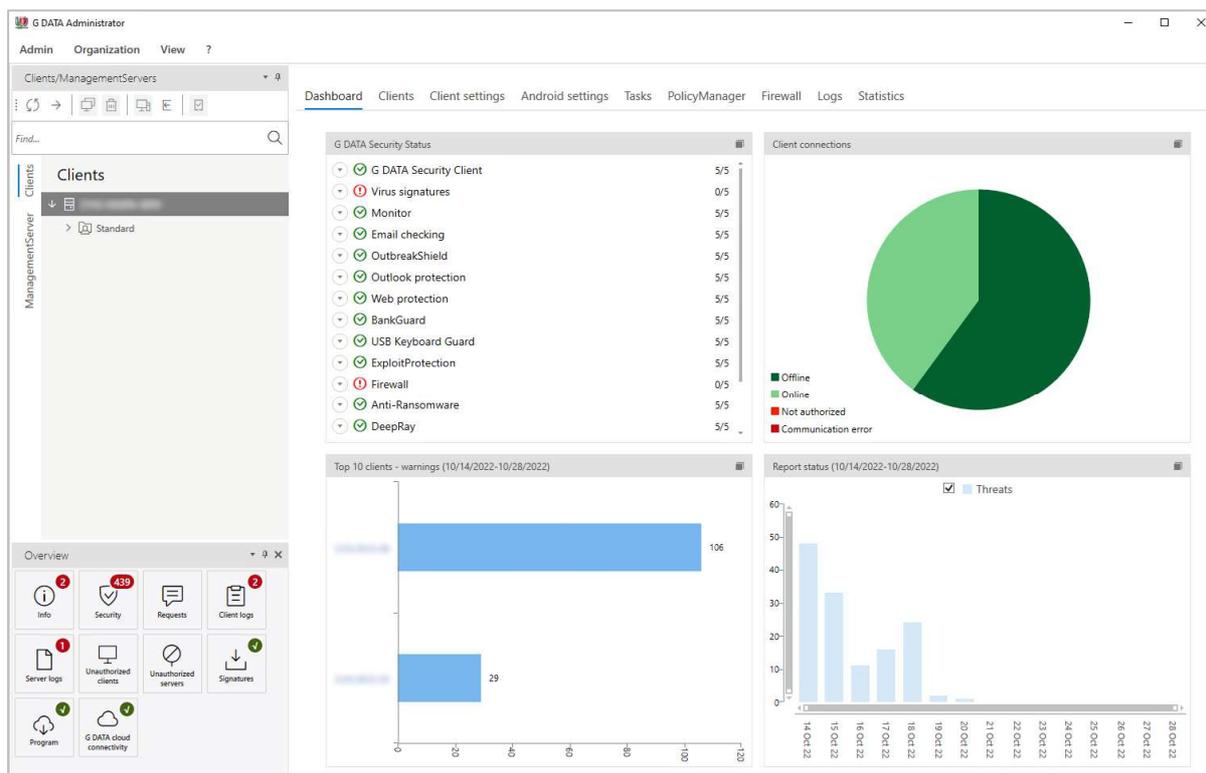


The user can see the protection status and detection logs, run updates, and run full or custom scans. Users can also scan a file, folder or drive using Windows Explorer's right-click menu. If you wish, users with Windows Administrator Accounts can be given full control of the program. Alternatively,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

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.

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 provides 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. An (optional) setup wizard runs when you first log on to the console. This covers items such as computers to be installed, Internet update settings, email notifications, and authentication for Android clients.

Management Console

The main *Dashboard* page of the console is shown in the screenshot above. 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.

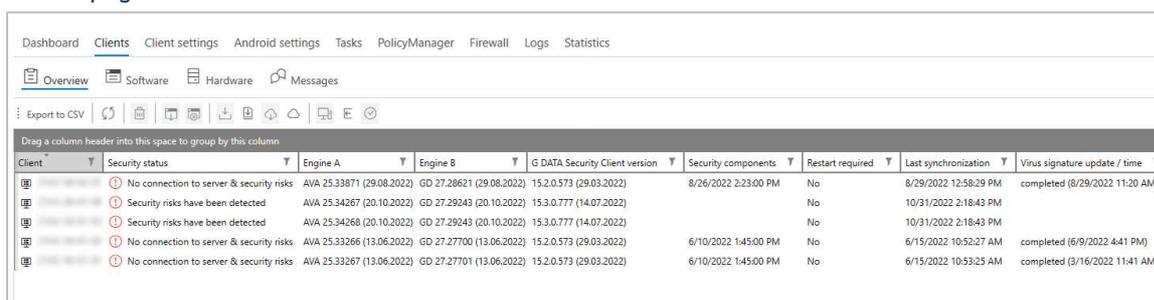
Clients pane

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) on the one hand, and Android mobile devices on the other. 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 provides a graphical display of 4 important status items. The first is the status of individual components, indicating what proportion of devices are correctly configured. Then there is the share of devices that have connected to the console recently. You can also see which clients have had the most detected threats. Finally, there is a timeline of important events.

Clients page



Client	Security status	Engine A	Engine B	G DATA Security Client version	Security components	Restart required	Last synchronization	Virus signature update / time
	No connection to server & security risks	AVA 25.33871 (29.08.2022)	GD 27.28621 (29.08.2022)	15.2.0.573 (29.03.2022)	8/26/2022 2:23:00 PM	No	8/29/2022 12:58:29 PM	completed (8/29/2022 11:20 AM)
	Security risks have been detected	AVA 25.34267 (20.10.2022)	GD 27.29243 (20.10.2022)	15.3.0.777 (14.07.2022)		No	10/31/2022 2:18:43 PM	
	Security risks have been detected	AVA 25.34268 (20.10.2022)	GD 27.29243 (20.10.2022)	15.3.0.777 (14.07.2022)		No	10/31/2022 2:18:43 PM	
	No connection to server & security risks	AVA 25.33266 (13.06.2022)	GD 27.27700 (13.06.2022)	15.2.0.573 (29.03.2022)	6/10/2022 1:45:00 PM	No	6/15/2022 10:52:27 AM	completed (6/9/2022 4:41 PM)
	No connection to server & security risks	AVA 25.33267 (13.06.2022)	GD 27.27701 (13.06.2022)	15.2.0.573 (29.03.2022)	6/10/2022 1:45:00 PM	No	6/15/2022 10:53:25 AM	completed (3/16/2022 11:41 AM)

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 whether a reboot is needed. The columns are customisable. Thus, you could also display the operating system, 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 dark 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 the proxy server and 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 include client name, status (action taken), date and time, detection component, threat name, file name, and logged-on user. The *Details* column displays the source URL of detected malware, where applicable. By selecting one or multiple items, you can take action, such as deleting or restoring quarantined items.

Client	Status	Date/Time	Reported by	Virus	File name/Subject	Details
	Virus found	10/20/2022 9:54:46 AM	HTTP check	Win32.Heur.7E6050EF	Status: Access denied.	Address: https://
	Quarantine: file moved to quarantine	10/19/2022 11:11:25 PM	DeepRay	Win32.Heur.7E6050EF	Ref:	Ref:
	Quarantine: file moved to quarantine	10/18/2022 4:25:11 PM	DeepRay	Win32.Heur.7E6050EF	Ref:	Ref:
	Quarantine: file moved to quarantine	10/18/2022 4:24:34 PM	DeepRay	Win32.Heur.7E6050EF	Ref:	Ref:
	Virus found	10/18/2022 12:00:22 PM	HTTP check	Win32.Heur.7E6050EF	Status: Access denied.	Address: http:

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

Windows Endpoint Protection Client

Deployment

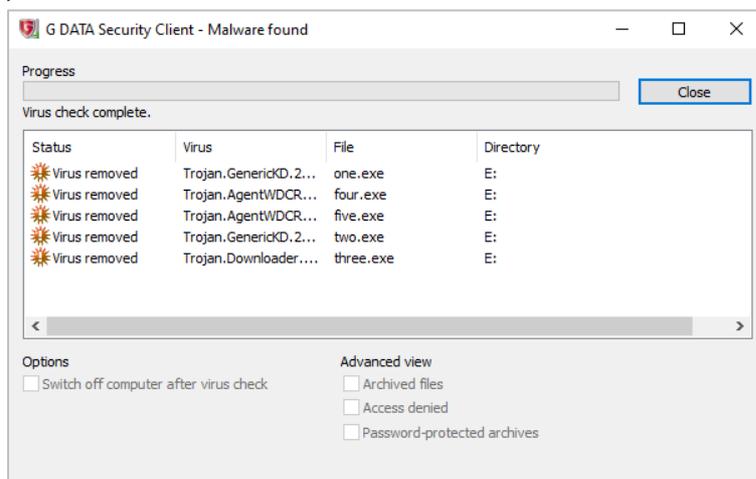
Before deploying endpoint protection software to clients, you may need to adjust Windows Firewall settings on both server and clients to enable communication between them. When the console is first used, a deployment wizard runs, allowing you to push the endpoint software to clients over the network. 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

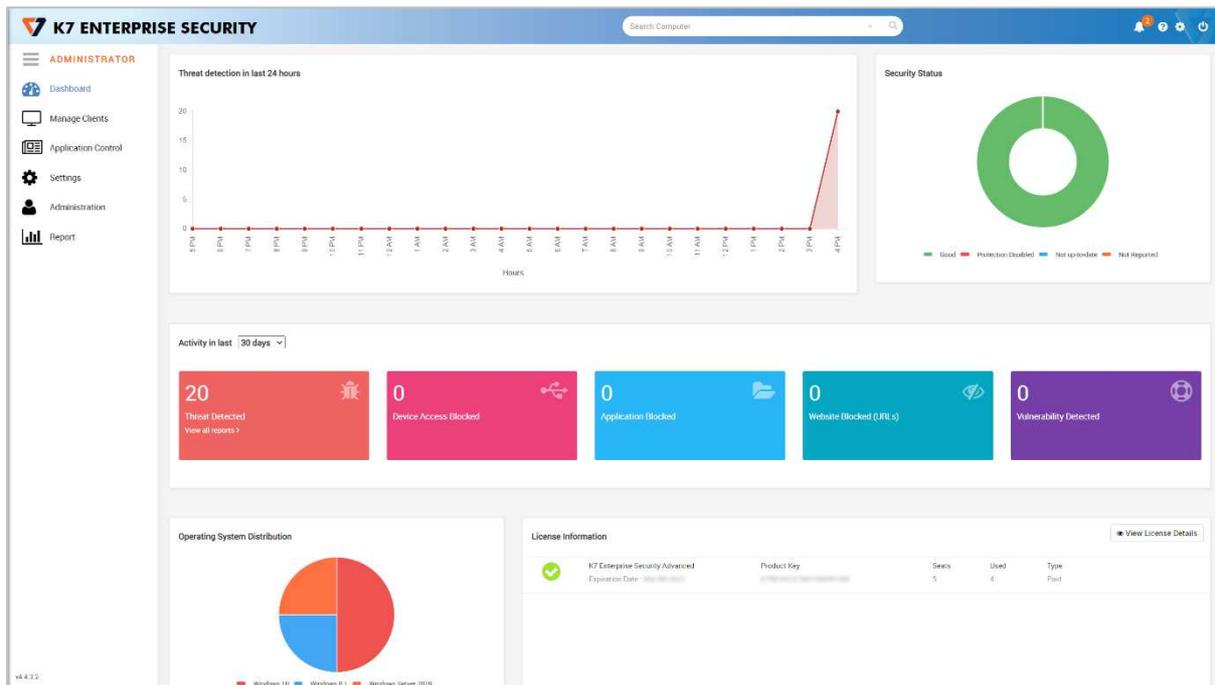
The user interface on protected endpoints consists simply of a System Tray icon. This can be used to run definition updates and display program information. By default, no other functionality is provided. However, by changing the policy, you could allow users to run scans (quick, full, custom and right-click); 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.

Malware detection scenario

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 On-Premises Enterprise Security



About the product

As its name suggests, K7 On-Premises Enterprise Security provides a server-based console for managing the endpoint protection software. This is accessed via a web browser. The product is designed for enterprises of all sizes. We feel it is particularly suitable for smaller businesses and less-experienced administrators, due to the very simple and easy-to-use console design.

Advantages

- Suitable for micro-businesses upwards
- Easy-to-navigate console
- Rapid communication between console and LAN clients
- Easy-to-use application control feature
- Granular control of functionality shown in endpoint protection client

Server Installation

The management console is installed on the server by running the provided .EXE file. You can choose to install Microsoft SQL Server 2014 as part of the installation wizard, or use an existing MS SQL Server instance if you have one. The wizard then lets you set console administrator credentials, proxy server settings, and port number to be used for web access. Email details for notifications can optionally be set up too. We found the server setup to be very straightforward and unproblematic.

Management console

All the console's main functionality can be accessed from a single menu panel on the left-hand side. The main entries here are *Dashboard*, *Manage Clients*, *Application Control*, *Settings*, *Administration*, and *Report*. Mousing over any of these items displays its sub-menus.

Dashboard page

After login, the console opens on the *Dashboard* page (screenshot above), which shows an overview of the system status. There are various detail panels, including a timeline of threats detected in the last 24 hours, security status of devices on the network, proportions of devices running specific Windows versions, and licence information. You can also see the numbers of threats and vulnerabilities detected, and numbers of devices/applications/websites blocked over the last day, week or month. There is a link from the *Security Status* panel to the *Clients* page, so you can get more details just by clicking on it.

Manage Clients\Clients page

Computer	IP Address	Group	Antivirus	Firewall	Last Update	Virus Definitions	Product Version	Last Contact
[Green icon]	[Redacted]	Default Group	Enabled	Enabled	Nov-03-2022 04:16 PM	12.46.45134	14.2.0757	Nov-03-2022 04:28 PM
[Green icon]	[Redacted]	Default Group	Enabled	Enabled	Nov-03-2022 04:38 PM	12.46.45134	14.2.0757	Nov-03-2022 04:38 PM
[Green icon]	[Redacted]	Default Group	Enabled	Enabled	Nov-03-2022 03:57 PM	12.46.45134	14.2.0757	Nov-03-2022 04:27 PM

The *Clients* page lists individual computers on the network. Details include hostname, IP address, group, status of antivirus and firewall components, malware definitions and product version numbers, and date/time of last update/last contact. You can customise the details columns, so you could add e.g. OS or domain information, or date and time of last scan. Mousing over the hostname of a computer displays a menu, from which you can view that device's details, change group membership, enable or temporarily disable protection components, run scans and updates, restart the computer, or uninstall the product.

Manage Clients\Group page

The *Group* page of the console lets you manage device groups. You can add, delete and edit groups, whereby the latter command can be used to apply a specific policy.

Manage Clients\Tasks page

From this page you can run a variety of tasks on selected computers. These include full, quick, custom, vulnerability and rootkit scans, along with client updates. Creating a task is very easy; you just need to select an action from the drop-down list, and then choose the computer(s) or group(s) you want it applied to.

Manage Clients\Policy page

The screenshot shows the 'ANTIVIRUS AND SPYWARE' configuration page. On the left is a navigation menu with categories: BEHAVIOUR PROTECTION, FIREWALL, INTRUSION DETECTION, WEB FILTERING, DEVICE CONTROL, UPDATE, and CLIENT PRIVILEGES. The main area is divided into four tabs: On Access, Schedule Scan, Exclusion, and Mail protection. The 'On Access' tab is active, showing settings for 'Enable On Access' (checked), 'What to scan' (All files, Automatic Identification, Scan only executable and vulnerable files, Detect spyware and Adware, Scan files on network, Concede resources to operating system when the computer starts, Perform background scan on running programs), 'Action for executable' (Clean automatically, Quarantine if clean fails, Report only, Don't take any action), and 'Action for document' (Clean automatically, Quarantine if clean fails, Report only, Don't take any action).

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

Application Control\Block Rule page

The screenshot shows the 'New Rule' dialog box in the Application Control section. It has a breadcrumb trail: Rule > Computer selection > Block access. The 'Rule Name' field is empty. The 'File Type' is set to 'File Path' (selected) with 'File Hash(MD5)' as an alternative. The 'Folder' field is empty, with a link to 'Show me the list of environment variables'. The 'File Name' field contains 'Ex. freecell.exe,*.exe' and a checkbox for 'This file may be found anywhere under the folder' is unchecked. 'cancel' and 'Next' buttons are at the bottom right.

From this page, you can easily regulate which applications are allowed to run or access the LAN/Internet. This can be done very simply by entering the folder path and file name, and then specifying which computers or groups the block should apply to. In a final step, you can specify one of the following: *Block from running*; *Block Internet Access*; *Block Network Access*.

Settings section

This lets you configure system-wide configurations, such as notifications, console updates, proxy settings, and licences.

Administration section

Under this main menu item, you can manage console users, administration roles, and relevant settings such as session timeout time and password complexity.

Report section

This provides a very easy means of running either summary or detailed reports on items such as detected threats, applications/websites blocked, device access violations, computers with incidents, hardware assets, and scan results. You can specify day, week, month, year or as the time interval for the report, or use a custom time period.

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. On the *Manage Clients\Install Protection* page you can download an installation package in .exe format. You can also create your own installer, and specify the group that installed computers 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. The default policy settings prevent users (even those with admin accounts) from disabling or uninstalling the software.

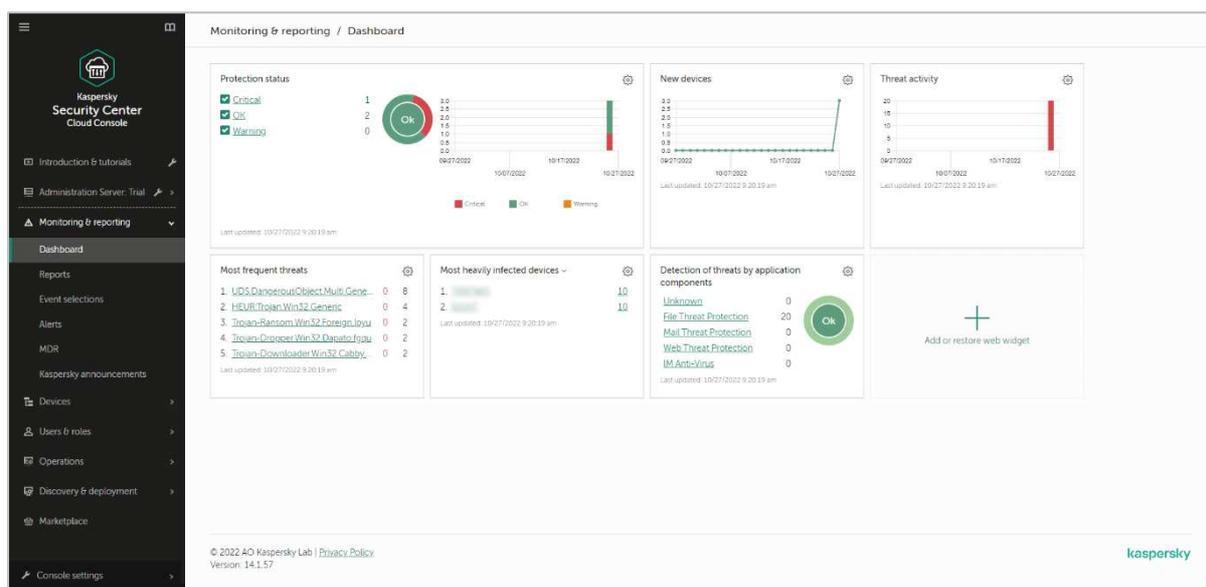
User interface

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 could 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



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
- Customisable web interface
- Granular role-based access controls

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 to devices/device groups. On the *Tasks* page you can carry out everyday maintenance and backup tasks, such as remote installation and updates.

Name	Visible	Last connected to Administration Server	Network Agent is installed	Network Agent is running	Status	Status description	Parent group	Real-time protection
[Redacted]	⊙	10/27/2022 9:35:01 am	⊙	⊙	⊙	The Kaspersky Security Network... >>	Managed devices	⊙
[Redacted]	⊠	10/26/2022 3:57:17 pm	⊙	⊠	⊙		Managed devices	⊙
[Redacted]	⊙	10/27/2022 9:38:11 am	⊙	⊙	⊙		Managed devices	⊙

The *Managed Devices* page, shown above, lists managed computers, along with the status of major components. You can sort and 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:

Time	Event	Description	Application	Version number	Importance level	Task
10/27/2022 9:07:08 am	Object deleted	Result description: Deleted Name: UDS.DangerousObject.Multi.Generic User: [Redacted] (Initiator) Object: [Redacted].exe SHA256: [Redacted] MD5: [Redacted]	Kaspersky Endpoint Security for Windows (11.10.0)	11.10.0.399	Warning	File Tr
10/27/2022 9:07:07 am	A backup copy of the object was created	Event type: A backup copy of the object was created Name: explorer.exe Application path: C:\Windows Process ID: 7024 User: [Redacted] (Initiator) Component: File Threat Protection Result description: Backup copy created Name: UDS.DangerousObject.Multi.Generic Threat level: Exactly Precision: High Object type: File Path to object: [Redacted] Object name: 1.exe SHA256: [Redacted] MD5: [Redacted]	Kaspersky Endpoint Security for Windows (11.10.0)	11.10.0.399	Info	File Tr
10/27/2022 9:07:07 am	Malicious object detected	Result description: Detected Name: UDS.DangerousObject.Multi.Generic User: [Redacted] (Initiator) Object: [Redacted].exe	Kaspersky Endpoint Security for Windows (11.10.0)	11.10.0.399	Critical	File Tr

The *Device Selections* page lets you find devices in pre-configured groups. Examples include *Databases are outdated* and *Devices with Critical Status*. These allow you to easily identify any devices on the network that need your attention.

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, console users can be assigned one of 15 different management roles, 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 Updates* you can see missing Windows Updates (amongst other things):

Operations / Patch management / Software updates

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

Preset filters: Requires action

<input type="checkbox"/>	Name	Application	Application version	Importance level	Registered	Update approval status	Not assigned for installation	Not
<input type="checkbox"/>	2022-07 Cumulative Update Pre	Windows 11		Unknown	10/26/2022 3:58:29 pm	Undefined	1	0
<input type="checkbox"/>	2022-08 Cumulative Update Pre	Windows 11		Unknown	10/26/2022 3:58:29 pm	Undefined	1	0
<input type="checkbox"/>	2022-08 Cumulative Update Pre	Windows 11		Unknown	10/26/2022 3:58:29 pm	Undefined	1	0
<input type="checkbox"/>	2022-08 Security Update for Win	Windows 11		Unknown	10/26/2022 3:58:29 pm	Undefined	1	0
<input type="checkbox"/>	2022-09 Cumulative Update Pre	Windows 11		Unknown	10/26/2022 3:58:29 pm	Undefined	1	0
<input type="checkbox"/>	2022-09 Cumulative Update Pre	Windows 11		Unknown	10/26/2022 3:58:29 pm	Undefined	1	0
<input type="checkbox"/>	2022-10 Cumulative Update Pre	Windows 11		Unknown	10/26/2022 3:58:29 pm	Undefined	1	0

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 using various categories such as domain membership or IP address range. *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, which guides you through the steps needed 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*.

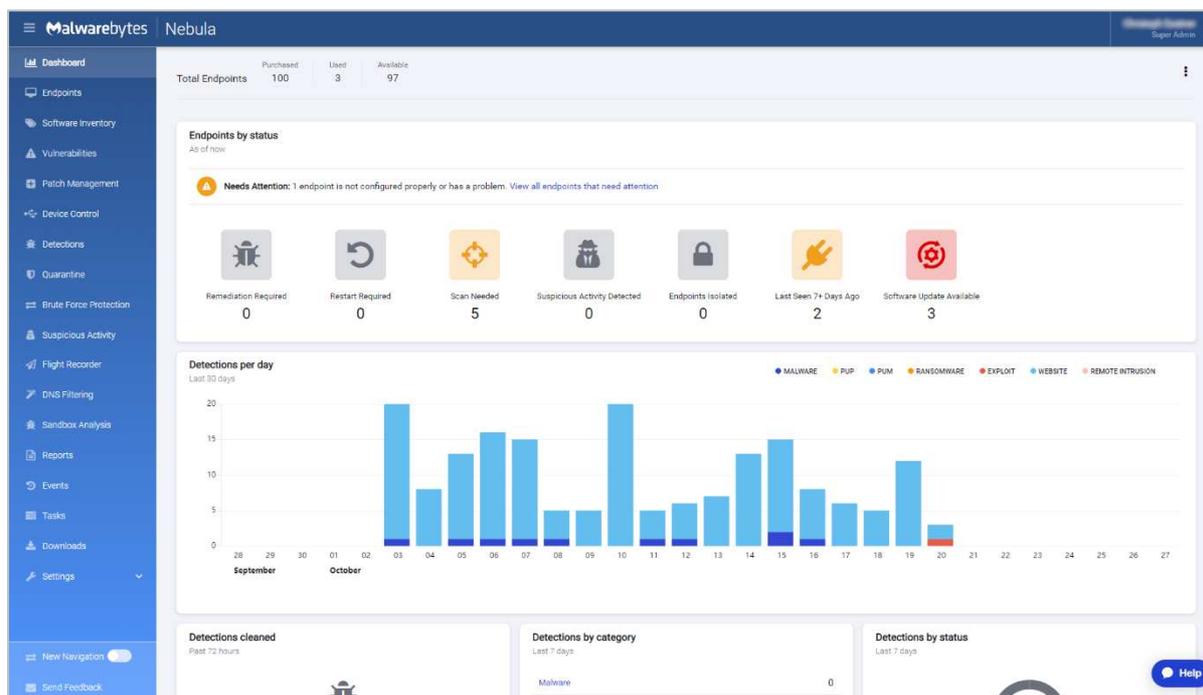
User interface

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

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*, *Software Inventory*, *Vulnerabilities*, *Patch Management*, *Device Control*, *Detections*, *Quarantine*, *Brute Force Protection*, *Suspicious Activity*, *Flight Recorder*, *DNS Filtering*, *Sandbox Analysis*, *Reports*, *Events*, *Tasks*, *Downloads*, and *Settings*.

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

Endpoint	Group	Last seen	Last user	OS platform	Policy	Status
[Green dot]	Default Group	Today	[Redacted]	Windows	MainTest	
[Grey dot]	Default Group	1 month ago	[Redacted]	Windows	MainTest	⊕ ⊗
[Green dot]	Default Group	Today	[Redacted]	Windows	MainTest	⊕ ⊗

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

Software Inventory page

Here you can see all the software installed on each computers in your network. For each application, you can see the version number, date installed, name of the endpoint, and operating system. This data can be exported in .CSV or .XLSX format.

Detections page

As you would expect, this displays instances of malware found on network computers. You can see the threat name, action taken, threat category (e.g. ransomware), threat type (e.g. file), 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, including file hashes.

Threat name	Action taken	Category	Type	Endpoint	Location	Date
Malware.Sandbox.12	Quarantined	Malware	File	[Green dot]	[Redacted]	10/27/2022 4:28:29 PM
Malware.AI.4106007299	Quarantined	Malware	File	[Green dot]	[Redacted]	10/27/2022 4:28:29 PM
Trojan.Agent.JV	Quarantined	Malware	File	[Green dot]	[Redacted]	10/27/2022 4:28:29 PM
Malware.Sandbox.12	Quarantined	Malware	File	[Green dot]	[Redacted]	10/27/2022 4:28:29 PM
Trojan.Agent.JV	Quarantined	Malware	File	[Green dot]	[Redacted]	10/27/2022 4:28:29 PM

Quarantine page

This shows quarantined malware that has been detected on protected devices. You can see the threat name and path, threat category and 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*, *Device Control Summary*, *Endpoints Summary*, *Events Summary*, *Quarantine Summary*, *Tasks Summary*, and *Weekly Security Report*. These can be run on-demand, or 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. An information panel at the top conveniently lists the possible deployment methods, such as Active Directory Group Policy.

Settings\Policies page

The screenshot displays the 'Default Policy' configuration page for Malwarebytes. At the top, it shows the policy name 'Default Policy' and an 'Edit' link. Below this, a table provides metadata: 'Updated at' (03/23/2022 1:12:00 AM), 'Updated by' (Malwarebytes), and 'Created at' (07/30/2021 10:50:18 AM). The main content area is divided into a left-hand navigation pane and a right-hand configuration pane. The navigation pane includes links for 'General', 'Endpoint agent', 'Tamper protection', 'Protection settings', 'Scan settings', 'Endpoint Detection and Response' (which is currently selected), 'Brute force protection', and 'Software management'. The configuration pane is titled 'Endpoint agent' and includes OS icons for Windows and Mac. It features several settings: 'User interface options' (expanded), 'Show the Malwarebytes icon in the notification area' (enabled), 'Display real-time protection notifications' (enabled), 'Allow users to run a Threat Scan (all threats will be quarantined automatically)' (enabled), 'Show Malwarebytes shortcuts on Start menu and desktop to run Threat Scans' (disabled, with a note that it requires 'Allow users to run a Threat Scan' to be enabled), 'Show Malwarebytes option in context menus' (checked), 'Allow only Administrator level users to interact with the Malwarebytes Tray' (disabled, with a note that it is not supported in XP or Server 2003), and 'Endpoint agent updates' (expanded). Under 'Endpoint agent updates', 'Automatically download and install Malwarebytes application updates' is checked. A blue banner at the bottom states: 'Automatic endpoint agent updates are always enabled for Mac'.

Here you can configure the policies that dictate the settings applied to protected devices. The screenshot above shows the *Endpoint agent* section of the default policy. On the left-hand side of the page are links to the different policy areas: *Endpoint Agent*, *Tamper Protection*, *Protection Settings*, *Scan Settings*, *Endpoint Detection and Response*, *Brute Force Protection*, and *Software Management*. For Windows devices, you can enable 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.

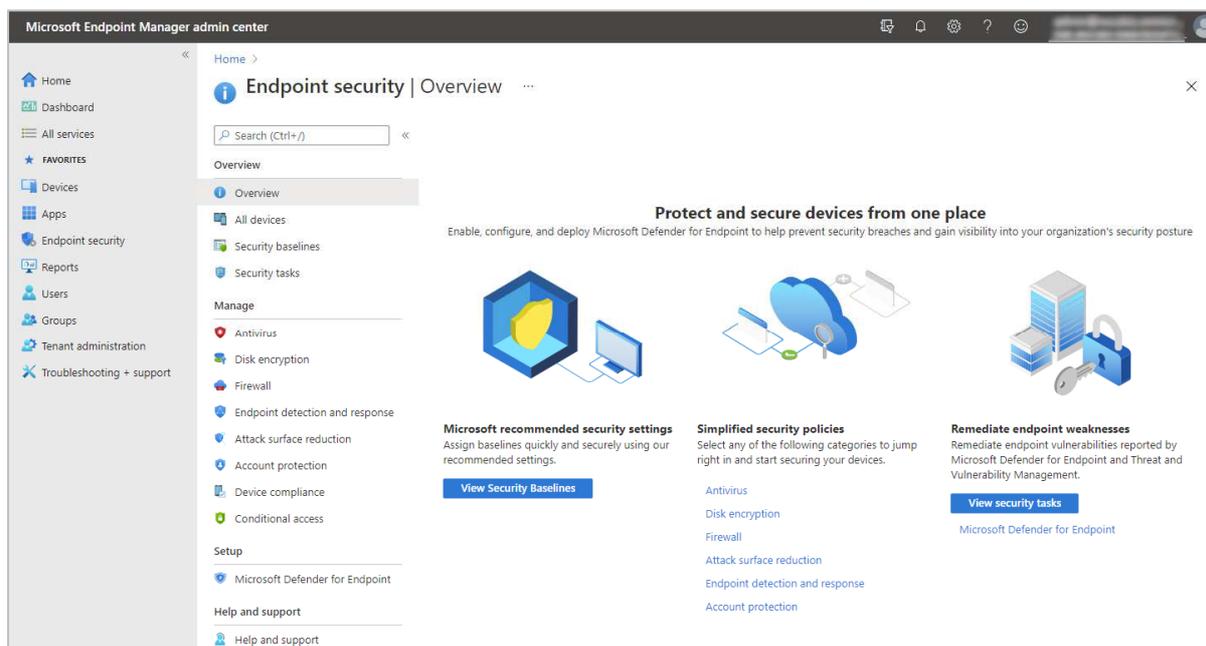
User interface

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 and Windows 11 operating systems.

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

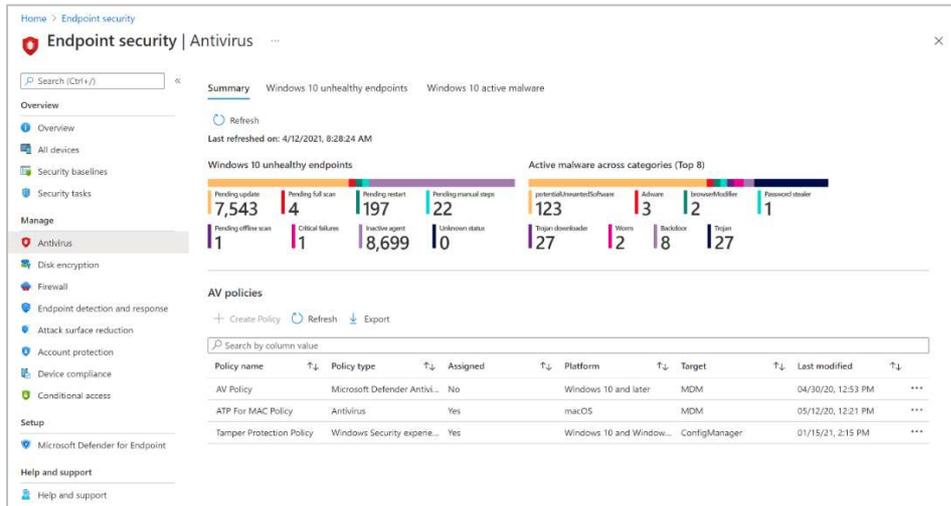
- Controls all Windows security settings
- Console is customisable
- Exceptionally simple client deployment
- Suitable for businesses of all sizes using Microsoft cloud services for business
- Granular control of security options

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

The screenshot shows the 'All devices' page in a management console. The page has a search bar at the top with the text 'Search by IMEI, serial number, email, user principal name, device name, management name, phone number, model, or manufacturer'. Below the search bar, there is a table of devices. The table has columns for Device name, Managed by, Ownership, Compliance, OS, OS version, Last check-in, and Enrolled. There are three rows of data, all showing 'Compliant' status and 'Windows' OS. The sidebar on the left contains navigation options like 'Overview', 'All devices', 'Monitor', 'By platform' (Windows, iOS/iPadOS, macOS, Android), and 'Device enrollment' (Enroll devices).

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

The screenshot shows the 'Device details' page for a specific device. The page has a menu bar at the top with actions like Retire, Wipe, Delete, Remote lock, Sync, Reset passcode, Restart, Fresh Start, Autopilot Reset, Quick scan, and Full scan. Below the menu bar, there is a section for 'Restart: Completed' and a section for 'Essentials' with device information. The 'Essentials' section includes fields for Device name, Management name, Ownership, Serial number, Phone number, Device manufacturer, Primary user (preview), Enrolled by, Compliance, Operating system, Device model, Last check-in time, and Remote assistance.

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

Here you can see the status of recent tasks, along with device-specific information such as manufacturer, model, serial number and primary user. The menu bar along the top of the page provides a number of management options. You can 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.

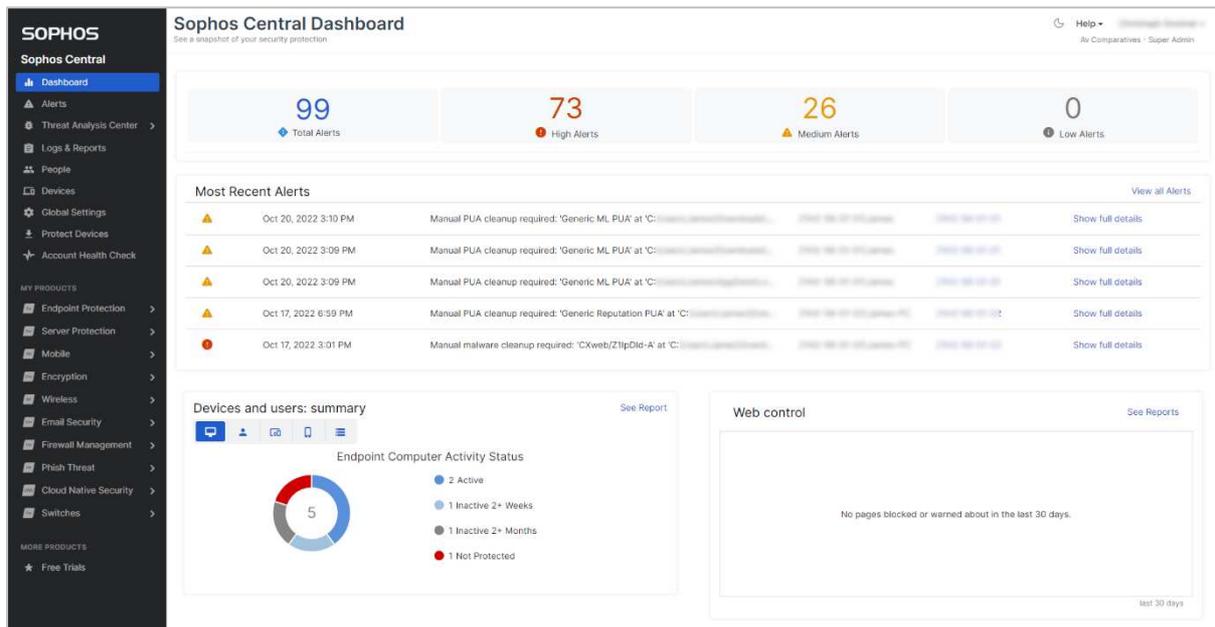
User interface

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.

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 the “back” button 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 screenshot displays the Alerts page interface. At the top, there are four summary cards: Total Alerts (99), High Alerts (73), Medium Alerts (26), and Low Alerts (0). Below these is a table of alerts. The selected alert is expanded to show details:

Description	Occurred	User	Device
Manual malware cleanup required: 'Mal/Generic-S' at 'C:\Users\...-4cea40c26636.tmp'	Oct 16, 2022 7:21 AM	[Redacted]	[Redacted]

Description: Manual malware cleanup required: 'Mal/Generic-S' at 'C:\Users\...-4cea40c26636.tmp'.
More information: We tried to clean up a threat but failed.
What you need to do: Please see knowledge base article 134588 for the steps needed to investigate the threat and clean it up.

Endpoint Type: Computer
OS: Windows
User: [Redacted]
Device: [Redacted]

Actions: Mark As Resolved, Email Alert (Change frequency for "Manual malware cleanup required" email alerts. This will be added to your "Exceptions" list. None)

The *Alerts* page shows you numbers of threat detections, both as a total and by severity category. You can sort the alerts by description, date/time, user or device. 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*.

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 the list of recent threats, along with *Devices and users: Summary*, *Web control* and *Global Security News*.

Logs and Reports page

The *Logs* section shows activity triggered by data-loss prevention rules. In the *Reports* section, you can run a variety of preconfigured reports in the categories *Users*, *Endpoint Protection* and *Web Control*. These include reports on users who have violated policies by trying to access blocked apps or websites.

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, 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. You can remove selected devices from the console with the *Delete* button.

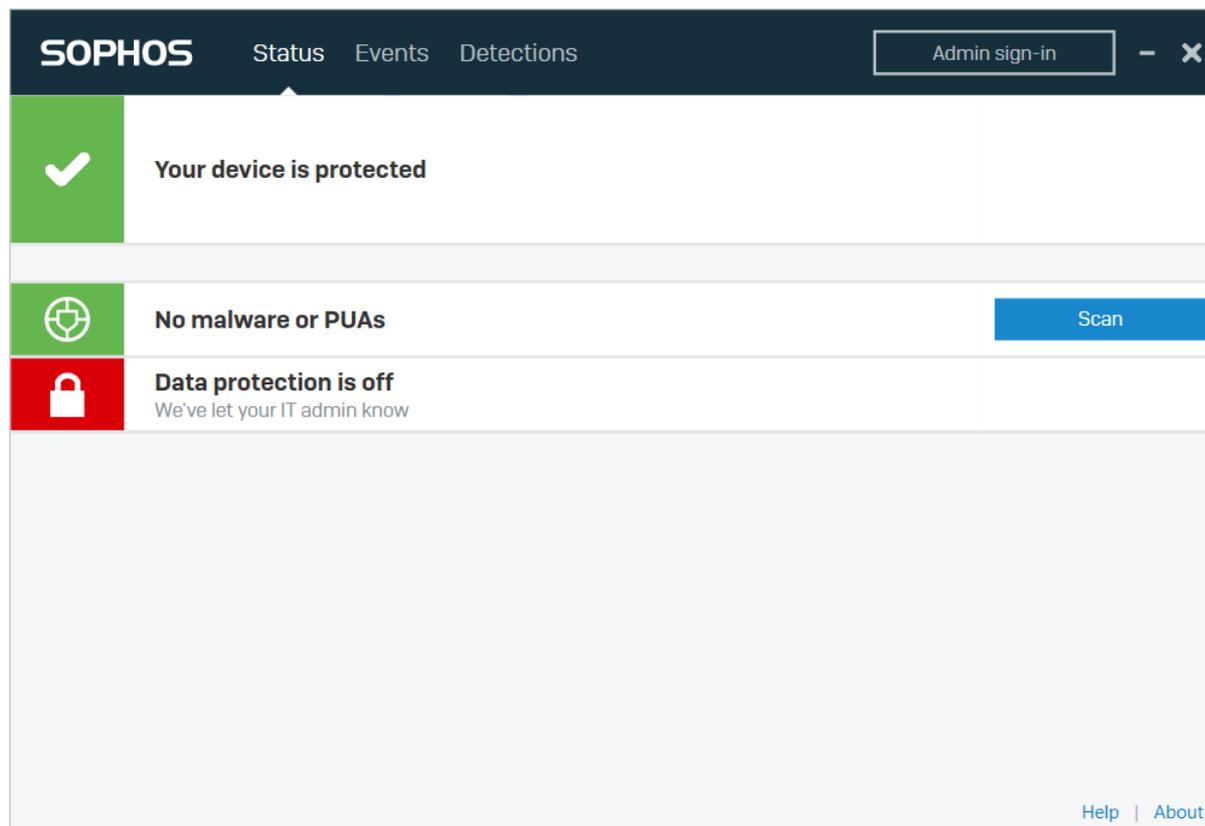
<input type="checkbox"/>	Name	IP	OS	Protection	Encryption	Last user	Last active	Group
<input type="checkbox"/>	[Redacted]	[Redacted]	Windows 10 Pro	✓ Intercept X Advanced	+	[Redacted]	Oct 27, 2022 2:00 PM	
<input type="checkbox"/>	[Redacted]	[Redacted]	Windows 10 Pro	✓ Intercept X Advanced	+	[Redacted]	Oct 27, 2022 1:59 PM	
<input type="checkbox"/>	[Redacted]	[Redacted]	Windows 10 Pro	✓ Intercept X Advanced	✓	[Redacted]	Oct 27, 2022 1:21 PM	

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

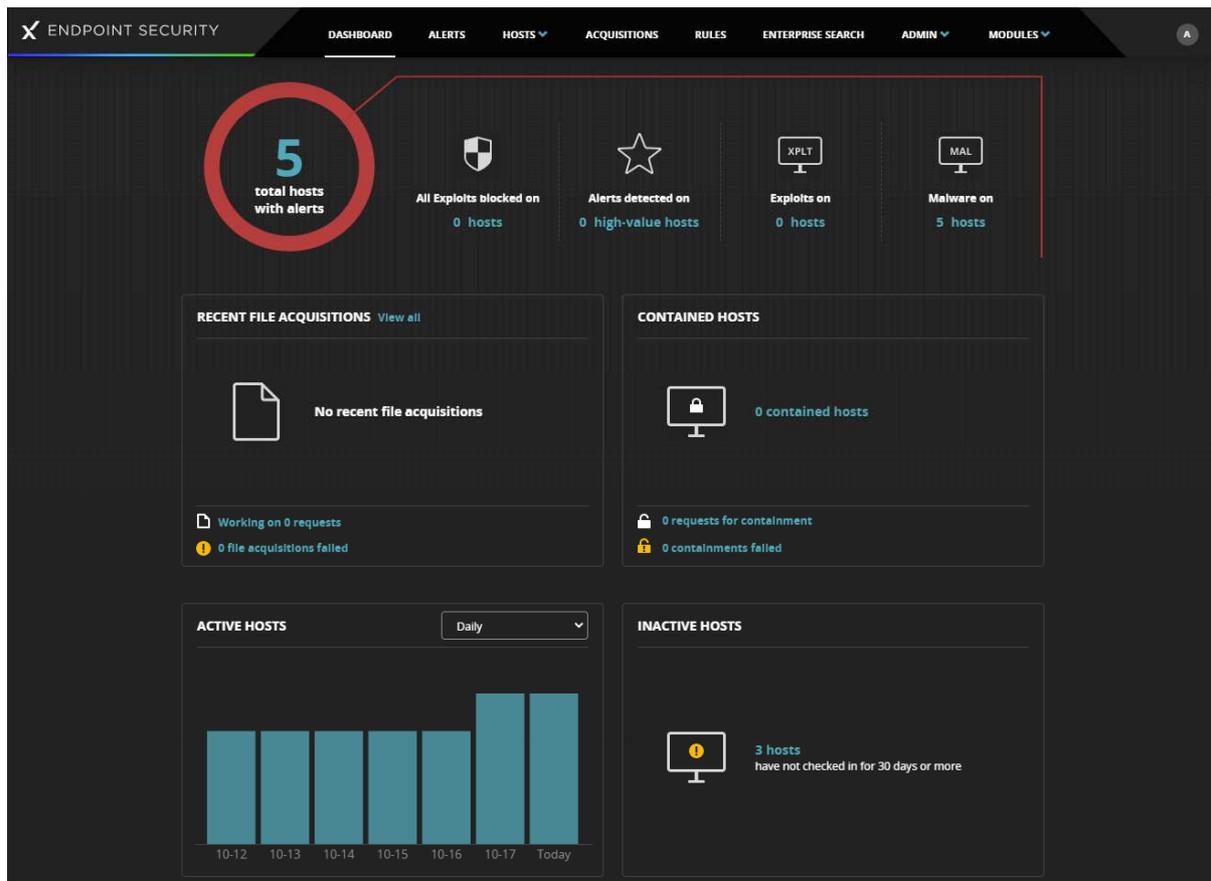


The user interface on protected endpoints consists of a System Tray icon and a program window. Users can see the protection status and detection logs, and run updates and default scans. They can also scan a file, folder or drive using Windows Explorer's right-click menu. Administrators can also change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

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 (visible) 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.

Trellix Endpoint Security (HX)



About the product

Trellix Endpoint Security (HX) 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 isolate 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

The screenshot shows the 'Hosts with Alerts' interface. At the top, there is a search bar and a summary indicating 5 hosts with alerts. Below the summary are filter and sort options. The main table lists the following hosts:

Host ID	OS & Timezone	Agent Version	Last Sysinfo	Alerts	Quarantines
WORKGROUP	Windows 10 Pro W. Europe Daylight Time	34.28.6	2022-10-18 13:07:52Z	99+ ALERTS (4 hours ago)	1605 QUARANTINES
WORKGROUP	Windows 10 Pro W. Europe Daylight Time	34.28.6	2022-10-18 13:06:32Z	99+ ALERTS (19 hours ago)	1718 QUARANTINES
STOVOKOR	Windows 10 Pro GMT Summer Time	35.31.0	2022-10-18 13:06:57Z	10 ALERTS (21 hours ago)	10 QUARANTINES

As the name suggests, this page displays details of protected devices with alerts that have not yet been dealt with. If you click on the plus sign for a device, you can see a list of alerts for that device, in chronological order. With malware alerts, a wealth of detail is provided for each one. This includes status (e.g. quarantined), 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

The screenshot shows the 'Alerts' page with a table of threat details. The table has the following columns: Acknowledged, Protection and Remediation, Alert Type, File Full Path, First Event, and Last Event. The data rows are as follows:

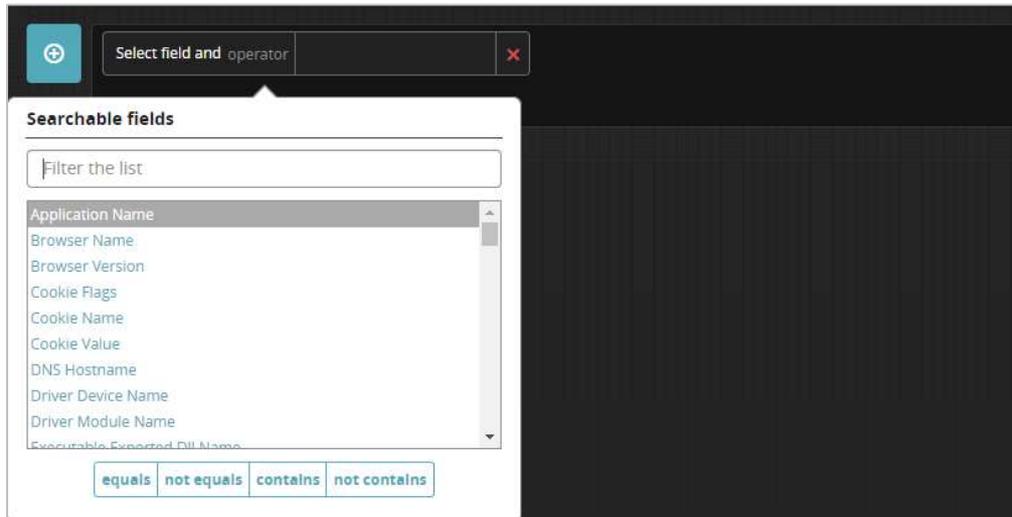
Acknowledged	Protection and Remediation	Alert Type	File Full Path	First Event	Last Event
No	QUARANTINED	MAL	[Redacted]	2022-10-18T09:03:27.473Z	2022-10-18T09:03:27.473Z
No	QUARANTINED	MAL	[Redacted]	2022-10-18T09:03:19.623Z	2022-10-18T09:03:19.623Z
No	QUARANTINED	MAL	[Redacted]	2022-10-18T07:22:51.096Z	2022-10-18T07:22:51.096Z
No	QUARANTINED	MAL	[Redacted]	2022-10-18T07:22:48.358Z	2022-10-18T07:22:48.358Z
No	QUARANTINED	MAL	[Redacted]	2022-10-18T03:47:41.441Z	2022-10-18T03:47:41.441Z

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

Acquisitions

From the *Hosts with Alerts* 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/paths, IP address, port, process name, registry key, service name/status/type/mode, timestamp, URL, username and Windows Event Message.

Admin\Policies

Here you can configure numerous different aspects of the client protection policy. Examples are scans, whether to show the endpoint client GUI on the endpoints, 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.

Admin\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.

Admin\Agent Versions

This lets you download current and older versions of the endpoint agent for Windows and Mac systems. The admin can thus e.g. avoid compatibility problems with a particular agent version on specific systems.

Admin\Appliance Settings

This page allows you to change settings for the management console itself. 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 five or so earlier versions of the client are provided. The installer file can be run manually, via a systems management product, or using an AD script.

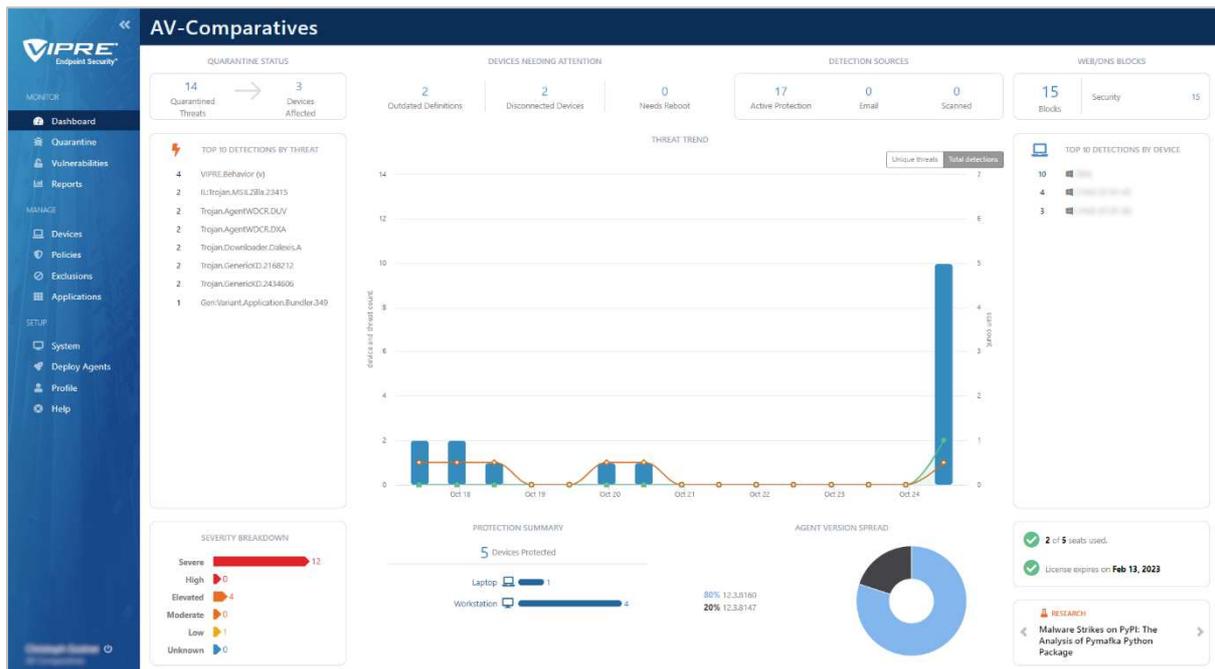
User interface

A System Tray icon is provided, from which users can open a simple program window. This lets you see the event log, quarantined items, and program version information.

Malware detection scenario

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

VIPRE Endpoint Protection Cloud



About the product

VIPRE Endpoint Cloud provides a cloud-based console for managing the endpoint protection software, as you would expect. In addition to malware protection, vulnerability and patch management features are included. 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*, licensing information, and a security blog. Every item is clickable, and links to the respective details page.

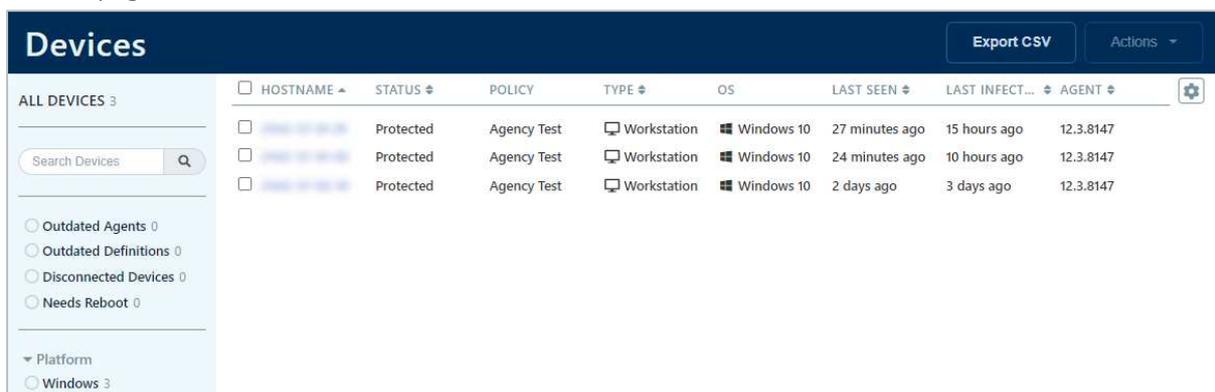
Quarantine page

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 ordered by time, name, severity, or number of devices. 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*, *License Summary* and *Applications Update*. *Threat Summary* uses a timeline, bar and pie charts to visualise threats found in the last week.

Devices page



Devices									Export CSV	Actions
ALL DEVICES 3	HOSTNAME	STATUS	POLICY	TYPE	OS	LAST SEEN	LAST INFECT...	AGENT		
<input type="checkbox"/>	...	Protected	Agency Test	Workstation	Windows 10	27 minutes ago	15 hours ago	12.3.8147		
<input type="checkbox"/>	...	Protected	Agency Test	Workstation	Windows 10	24 minutes ago	10 hours ago	12.3.8147		
<input type="checkbox"/>	...	Protected	Agency Test	Workstation	Windows 10	2 days ago	3 days ago	12.3.8147		

- Outdated Agents 0
- Outdated Definitions 0
- Disconnected Devices 0
- Needs Reboot 0

Platform

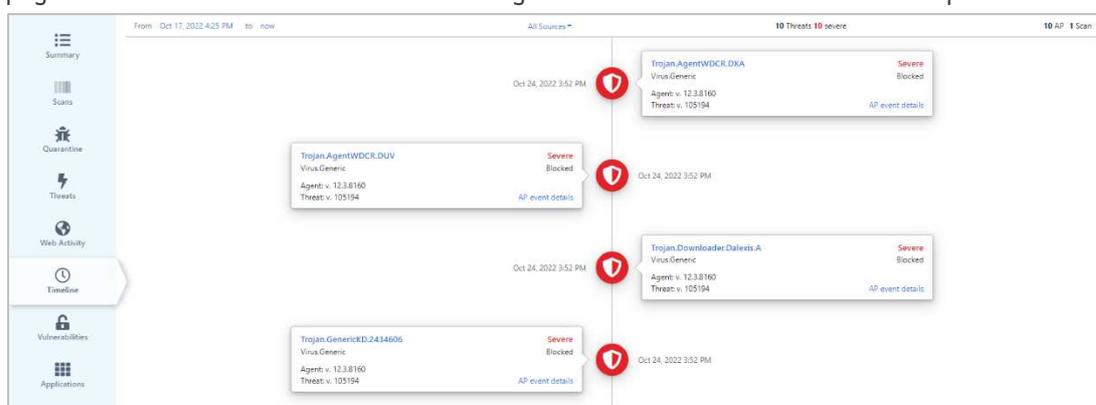
- Windows 3

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 sort the list of devices shown by hostname, OS version, status, 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*, *Scan Applications*, *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); *Vulnerabilities*; *Applications*.

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 encounters with the threat in the last week, the protection component involved, threat severity, 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*; *Patching*; *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.

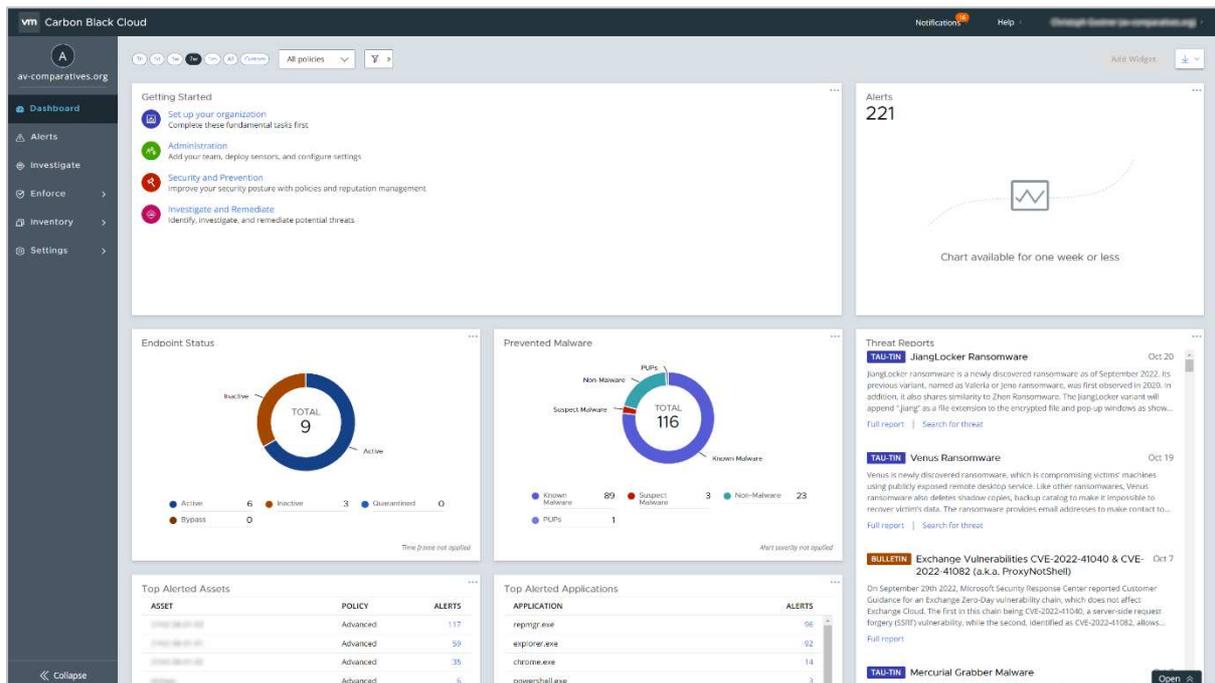
User interface

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 deploying the endpoint software and adding console administrators. You can customise the dashboard by moving panels around and removing any you don't need.

Alerts page

STATUS	FIRST SEEN	REASON	SEVERITY	VALUE	DEVICE	ACTIONS
<input type="checkbox"/>	9:37:15 am Oct 25, 2022	A known virus (Dropper: Delph) was detected.	3	Medium		[Icons]
<input type="checkbox"/>	9:37:14 am Oct 25, 2022	A known virus (Trojan: Nymalm) was detected.	3	Medium		[Icons]
<input checked="" type="checkbox"/> Policy Applied	9:37:12 am Oct 25, 2022	A known virus was detected running. A Deny Policy Action was applied.	4	Medium		[Icons]

The *Alerts* page shows you a list of threats encountered on all devices, in chronological order. You can filter the list using a wide variety of criteria, using the 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

TIME	TYPE	EVENT	ACTIONS
9:37:15 am Oct 25, 2022	filemod	The file [redacted] was first detected on removable media. The device was off the corporate network using the public address [redacted] (Location: Dublin L, Ireland). The file is not signed. The file was accessed by the application C:\windows\explorer.exe.	[Icons]

ALERT DETAILS
Alert ID: 00097c44-9d05-1547-7a-e4-78905d24c7ad
Reason: A known virus (Dropper: Delph) was detected.
First seen: 9:37:15 am Oct 25, 2022
Policy: No policy applied

PARENT PROCESS
userinit.exe
CMD: C:\Windows\system32\userinit.exe

PROCESS
explorer.exe
CMD: C:\Windows\Explorer.EXE
Effective Reputation: LOCAL_WHITE
Run by: [redacted]
Signed: Microsoft Windows
Techniques: detected_malware_app, known_dropper

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 (screenshot above). 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-demand scans, frequency of updates and the servers to use, 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 screenshot shows the 'ENDPOINTS' page with the following data:

STATUS	NAME	USER	OS	GROUP/POLICY	S...	SENSOR	T	LAST CHECK-IN	ACTIONS
✓	Windows 10 x64	Manually Assigned Advanced	●	3.8.0.722	Medium	1:46:06 pm Oct 25, 2022	[Icons]
✓	Windows 10 x64	Manually Assigned Advanced	●	3.8.0.684	Medium	1:46:01 pm Oct 25, 2022	[Icons]
✓	Windows 10 x64	Advanced (Default AVC Testing) Advanced	●	3.8.0.684	Medium	1:45:13 pm Oct 25, 2022	[Icons]
✓	Windows 10 x64	Unassigned Advanced	●	3.8.0.722	Medium	9:53:45 pm Oct 22, 2022	[Icons]

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, device name, 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. By selecting a device or devices, you can carry out actions, such as scans, policy assignments 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 e.g. 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 *Inventory\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.

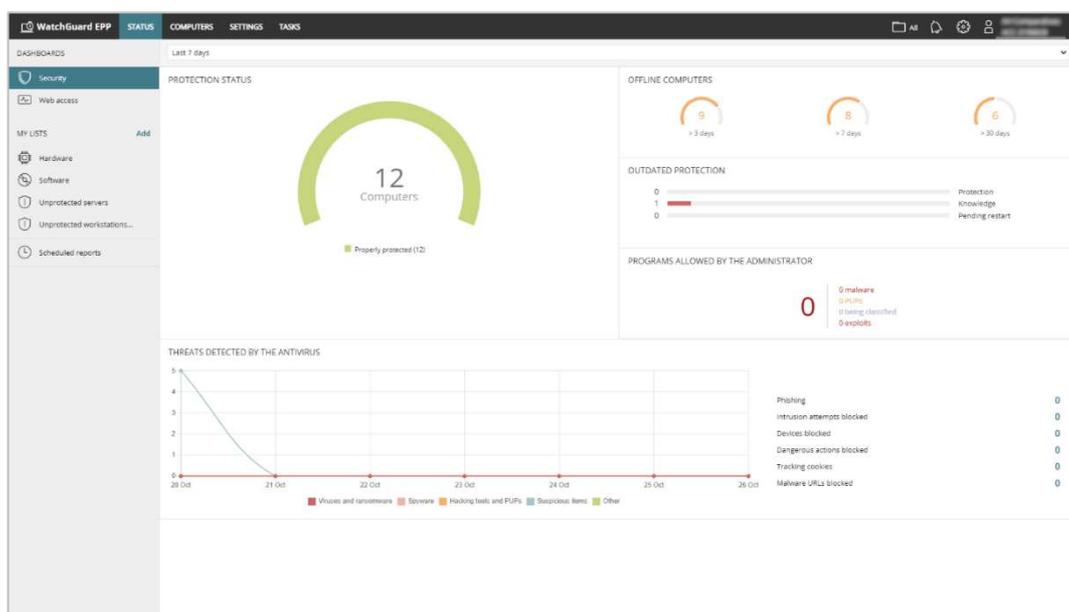
User interface

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.

Malware detection scenario

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.

WatchGuard Endpoint Protection Platform



About the product

WatchGuard Endpoint Protection Platform (EPP) 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* shows categories of website, such as webmail, games and business, which users have accessed. 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.

Computers tab

The *Computers* tab, shown below, lists all the protected computers and mobile devices on the network. You can sort by various criteria, including hostname, IP address, OS, management group, and date/time of last connection. It's possible to customise the columns shown, so you can add e.g. domain membership and last logged-on user. A Windows-Explorer-like folder tree on the left lets you filter devices by OS (including Windows for ARM processors), 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, restarting the computer, moving it to another group, or deleting it.

Computer	IP address	Group	Operating system	Last connection
...	...	Avcomparatives	Windows 10 Pro 64 (21H2)	5/13/2022 2:45:16 PM
...	...	Avcomparatives	Windows 10 Pro 64 (21H2)	5/13/2022 8:00:21 PM
...	...	Avcomparatives	Windows 10 Pro 64 (21H2)	10/26/2022 1:05:32 PM
...	...	Avcomparatives	Windows 10 Pro 64 (21H2)	10/26/2022 12:30:48 PM
...	...	Avcomparatives	Windows 10 Pro 64 (21H2)	10/20/2022 4:18:02 PM
...	...	Avcomparatives	Windows 10 Pro 64 (21H2)	3/14/2022 9:14:01 AM
...	...	Avcomparatives	Windows 10 Pro 64 (21H2)	10/3/2022 11:26:55 AM
...	...	Avcomparatives	Windows 10 Pro 64 (21H2)	3/14/2022 9:14:07 AM
...	...	Avcomparatives	Windows 10 Pro 64 (21H2)	10/3/2022 11:01:37 AM
...	...	Avcomparatives	Windows 10 Pro 64 (21H2)	9/8/2022 3:00:30 PM
...	...	Avcomparatives	Windows 10 Pro 64 (21H2)	9/7/2022 8:06:28 AM
...	...	All	Windows 10 Pro 64 (21H2)	10/26/2022 1:24:24 PM

By clicking the folder icon at the top of the left-hand pane, and clicking the three-dots icon to the right of "All", you can create and manage computer groups, which can be synchronised with Active Directory.

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, WatchGuard 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 applicable 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 the management agent or protection software, and reboot the computer.

Computer

Name: [redacted]

Description: [redacted] [Change](#)

IP addresses: [redacted]

Public IP address: [redacted]

Physical addresses (MAC): [redacted]

Domain: [redacted]

Active Directory path: [redacted]

Group: [All](#) [Change](#)

Operating system: Windows 10 Pro 64 (Version: 21H2)(Build: 19044.2130)

Virtual machine: Yes

Is a non-persistent computer: No

Licenses: WATCHGUARD EPP

Agent version: 1.19.01.0000

Last bootup date: 10/26/2022 1:01:01 PM

Installation date: 10/26/2022 1:09:15 PM

Last proxy used: No proxy

Last connection: 10/26/2022 1:24:24 PM

Last settings check: 10/26/2022 1:14:04 PM

Shadow Copies: Disabled

Last logged-in user: [redacted]

Settings tab

The *Settings/Security* pages let you define separate security policies for computers on the one hand, and Android mobile devices on the other. 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 WatchGuard 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

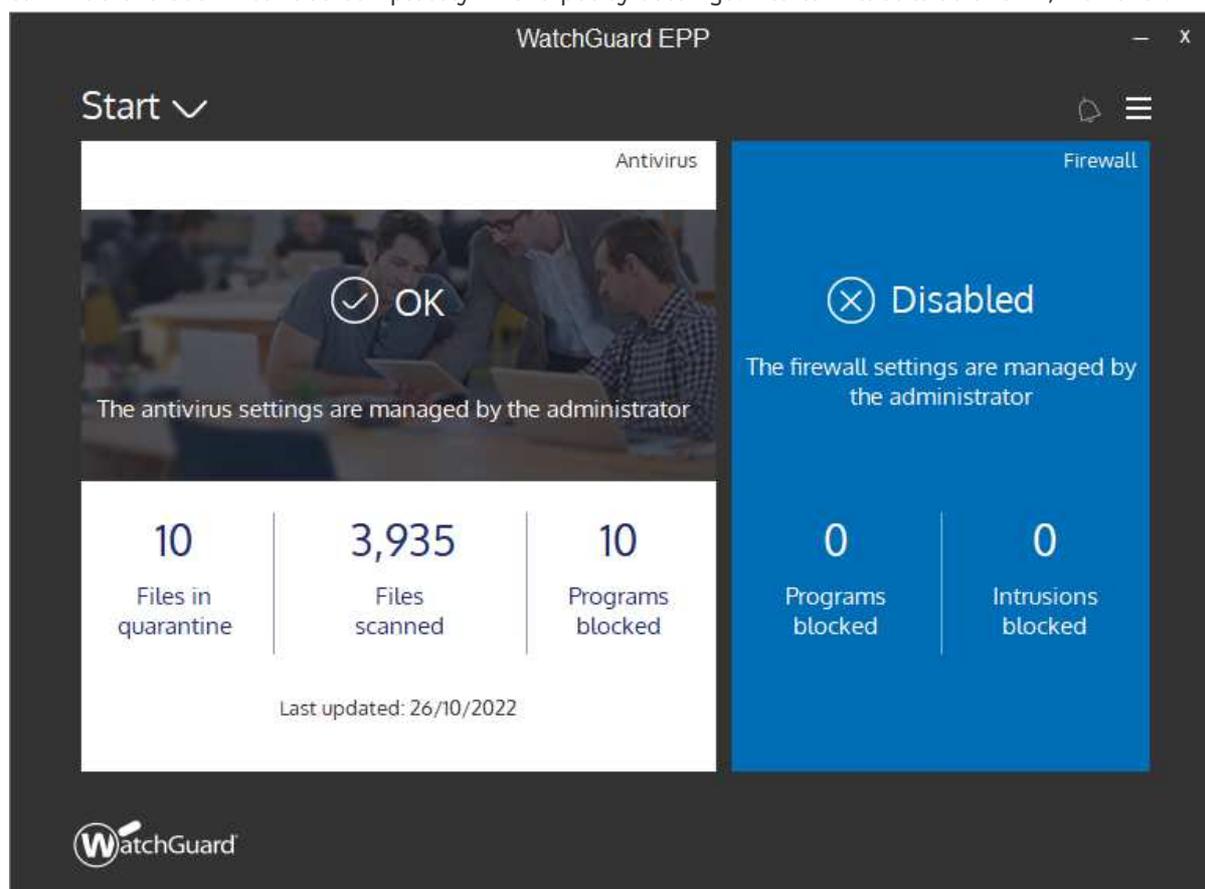
Deployment

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 WatchGuard 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.



Malware detection scenario

When we connected a flash drive containing malware samples to our test PC, and opened the drive in Windows Explorer, WatchGuard 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.



Copyright and Disclaimer

This publication is Copyright © 2022 by AV-Comparatives®. Any use of the results, etc. in whole or in part, is ONLY permitted after the explicit written agreement of the management board of AV-Comparatives prior to any publication. AV-Comparatives and its testers cannot be held liable for any damage or loss, which might occur as result of, or in connection with, the use of the information provided in this paper. We take every possible care to ensure the correctness of the basic data, but a liability for the correctness of the test results cannot be taken by any representative of AV-Comparatives. We do not give any guarantee of the correctness, completeness, or suitability for a specific purpose of any of the information/content provided at any given time. No one else involved in creating, producing or delivering test results shall be liable for any indirect, special or consequential damage, or loss of profits, arising out of, or related to, the use or inability to use, the services provided by the website, test documents or any related data.

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

AV-Comparatives
(December 2022)