

Independent Tests of Anti-Virus Software



Business Security Test

TEST PERIOD: MARCH – JUNE 2019
LANGUAGE: ENGLISH
LAST REVISION: 11TH JULY 2019

WWW.AV-COMPARATIVES.ORG

Contents

INTRODUCTION	3
TESTED PRODUCTS	4
SETTINGS	5
MANAGEMENT SUMMARY	6
AV-COMPARATIVES' APPROVED BUSINESS PRODUCT AWARD	8
REAL-WORLD PROTECTION TEST (MARCH-JUNE)	9
MALWARE PROTECTION TEST (MARCH)	14
PERFORMANCE TEST (JUNE)	16
REVIEWS	21
FEATURE LIST	69
COPYRIGHT AND DISCLAIMER	70

Introduction

This is the first half-year report of our Business Main-Test Series¹ of 2019, containing the results of the Business Real-World Protection Test (March-June), Business Malware Protection Test (March), Business Performance Test (June), 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 enters the test system via e.g. the local area network or removable device, rather than directly from the Internet.

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.

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.

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

The second half-year report of 2019 will also include the results of the new **Enhanced Real-World Test** (protection against Advanced Persistent Threats), which evaluates the products for their abilities to block sophisticated attacks such as file-less threats and exploits. Enterprises in particular are frequently targeted by such attacks. This kind of audit has often been requested by analysts and CISOs. Consequently, it will be a valuable indicator of whether business security products live up to their claims.

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 1809 64-bit:

Vendor	Product	Version March	Version April	Version May	Version June
Avast	Business Antivirus Pro Plus	18.8	18.8	19.3	19.5
Bitdefender	GravityZone Elite Security	6.6	6.6	6.6	6.6
Cisco	AMP for Endpoints	6.2	6.2	6.3	6.3
CrowdStrike	Endpoint Protection Platform Standard Bundle	4.22	4.24	4.26	5.10
Endgame	Endpoint Protection Platform	3.50	3.50	3.50	3.50
ESET	Endpoint Protection Advanced Cloud & CA	7.0	7.0	7.0	7.0
FireEye	Endpoint Security	29.7	29.7	29.7	29.7
Fortinet	FortiClient with EMS & FortiSandbox	6.0	6.0	6.0	6.0
K7	Enterprise Security	14.2	14.2	14.2	14.2
Kaspersky	Endpoint Security for Business Select	11.0	11.0	11.1	11.1
McAfee	Endpoint Security with ATP and ePO Cloud	10.6	10.6	10.6	10.6
Microsoft	Defender ATP's Antivirus	4.18	4.18	4.18	4.18
Panda	Endpoint Protection Plus on Aether	7.90	7.90	7.90	7.90
Seqrite	Endpoint Security	17.0	17.0	17.0	17.0
Sophos	Intercept X Advanced	10.8	10.8	10.8	10.8
SparkCognition	DeepArmor Endpoint Protection Platform	1.47	2.0	2.0	2.0
Symantec	Endpoint Protection	14.2	14.2	14.2	14.2
Trend Micro	OfficeScan XG	12.0	12.0	12.0	12.0
VIPRE	Endpoint Security Cloud	10.1	11.0	11.0	11.0

We congratulate the vendors who are participating in the Business Main-Test Series for having their business products publicly³ 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: **Cisco**, **FireEye**, **Seqrite** and **VIPRE** use the **Bitdefender** engine (in addition to their own protection features).

³ Enterprises and analysts interested in the review and full results of **Symantec** and **Trend Micro** can contact us for a quote.

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. About half of the vendors provide their products with optimal default settings which are ready to use, and therefore did not change any settings. Cloud and PUA⁴ detection were activated in all products. Below we have listed relevant deviations from default settings (i.e. setting changes applied by the vendors):

Bitdefender: "HyperDetect", "Device Sensor" and "EDR Sensor" disabled.

Cisco: everything enabled.

CrowdStrike: everything enabled and set to maximum, i.e. "Extra Aggressive".

Endgame: Enabled Software and Hardware protection options: "Critical API Filtering", "Header Protection", "Malicious Macros", "Stack Memory", "Stack Pivot" and "UNC Path"; Protected Applications: "Browser", "Microsoft Suite", "Java" and "Adobe". Exploit Protection: "On – Prevent mode"; Malicious File Configuration: "On" – Protection at File Execution "On"; Options: "Prevent", "Process execution and loaded modules", Malware Detection for created and modified files "On"; "Aggressive" threshold.

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

Fortinet: Real-Time protection, FortiSandbox, Webfilter and Application Firewall (in order to use Detect & Block Exploits) enabled.

McAfee: "Email attachment scanning" enabled; "Real Protect" enabled and set to "high" sensitivity, "read/write scan of Shadow Copy Volumes" disabled, "Access Protection" and "Exploit Prevention" disabled.

Microsoft: Cloud protection level set to "High".

Sophos: "Web Control" and "Protect against data loss" disabled.

SparkCognition: all "Policy Settings" and all "Attack Vectors" settings enabled.

Trend Micro: Behaviour monitoring: "Monitor new encountered programs downloaded through web" enabled; "Certified Safe Software Service for Behaviour monitoring" enabled; "Smart Protection Service Proxy" enabled; "Use HTTPS for scan queries" enabled; Web Reputation Security Level set to Medium; "Send queries to Smart Protection Servers" disabled; "Block pages containing malicious script" enabled; Real-Time Scan set to scan "All scannable files", "Scan compressed files to Maximum layers 6"; "CVE exploit scanning for downloaded files" enabled; "ActiveAction for probable virus/malware" set to Quarantine; Cleanup type set to "Advanced cleanup" and "Run cleanup when probable virus/malware is detected" enabled; "Block processes commonly associated with ransomware" enabled; "Anti-Exploit Protection" enabled; all "Suspicious Connection Settings" enabled and set to Block.

Avast, ESET, K7, Kaspersky, Panda, Seqrite, Symantec, VIPRE: default settings.

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

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.

You need to make choices between going for a local-network, server-installed package, or looking at a wholly cloud-based solution. There are advantages and disadvantages to both, and much will depend upon your existing infrastructure and working practices. There is no reason why one approach is inherently better than another.

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

McAfee provide a console with huge functionality that can be used to manage many other products in addition to endpoint protection. This means that some training and orientation will be needed to get the best out of it, but the time invested will be rewarded. Consequently, it is best used in organisations with the appropriate IT resources to take full advantage of it.

Microsoft's Intune spans the range from the SME market to the largest global corporation, as you would expect, since Microsoft deploys it internally. It has a clean, easy-to-understand user interface, and integrates extremely well with Active Directory and the whole suite of AD policy driven solutions. For many customers who are focused on the Microsoft corporate platform, there are significant advantages to this solution as part of an overall fully managed deployment.

Cisco offers a product with a wealth of functionality. Finding the essentials is made easy in the well-designed console, although getting the most out of the product would take some learning.

SparkCognition presents sophisticated features in a straightforward, easy-to-navigate console.

Kaspersky and Sophos offer strong, easy-to-manage products that are equally at home in SMEs and larger organisations.

For the smaller end of the business, **Avast**, **Bitdefender**, **ESET**, **Fortinet**, **K7**, **Panda** and **Seqrite** all offer strong and coherent solutions. These would all work well with larger companies too, and so allow the business to grow.

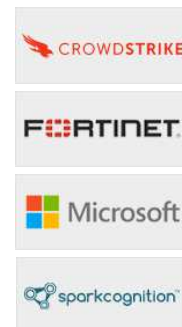
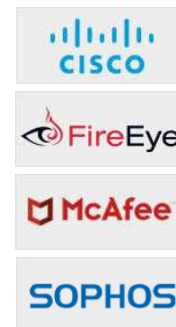
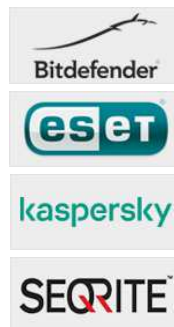
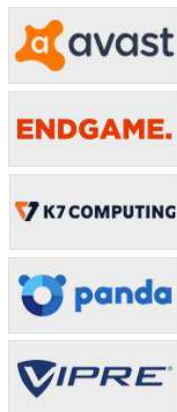
VIPRE's simplicity and clarity make it a very good choice for smaller businesses with limited IT staff resources, although it allows plenty of room to grow. It is limited to the Windows platform, however.

AV-Comparatives' Approved Business Product Award

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

To be certified in July 2019 as an "Approved Business Product" by AV-Comparatives, the tested products must score at least 90% in the Malware Protection Test with zero false alarms on common business software, and at least 90% in the overall Real-World Protection Test (i.e. over the course of four months), with less than one hundred false alarms on any clean software/websites (and with zero false alarms on common business software). Tested products must also avoid major performance issues and have fixed all reported bugs in order to gain certification.

We congratulate the vendors shown below, whose products met the certification criteria, and are thus given the AV-Comparatives Approved Business Security Product Award for July 2019:



Real-World Protection Test (March-June)

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

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

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

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



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

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



Test Procedure

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

Lab Setup

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

Software

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

Preparation for every testing day

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

Testing Cycle for each malicious URL

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

Protection

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

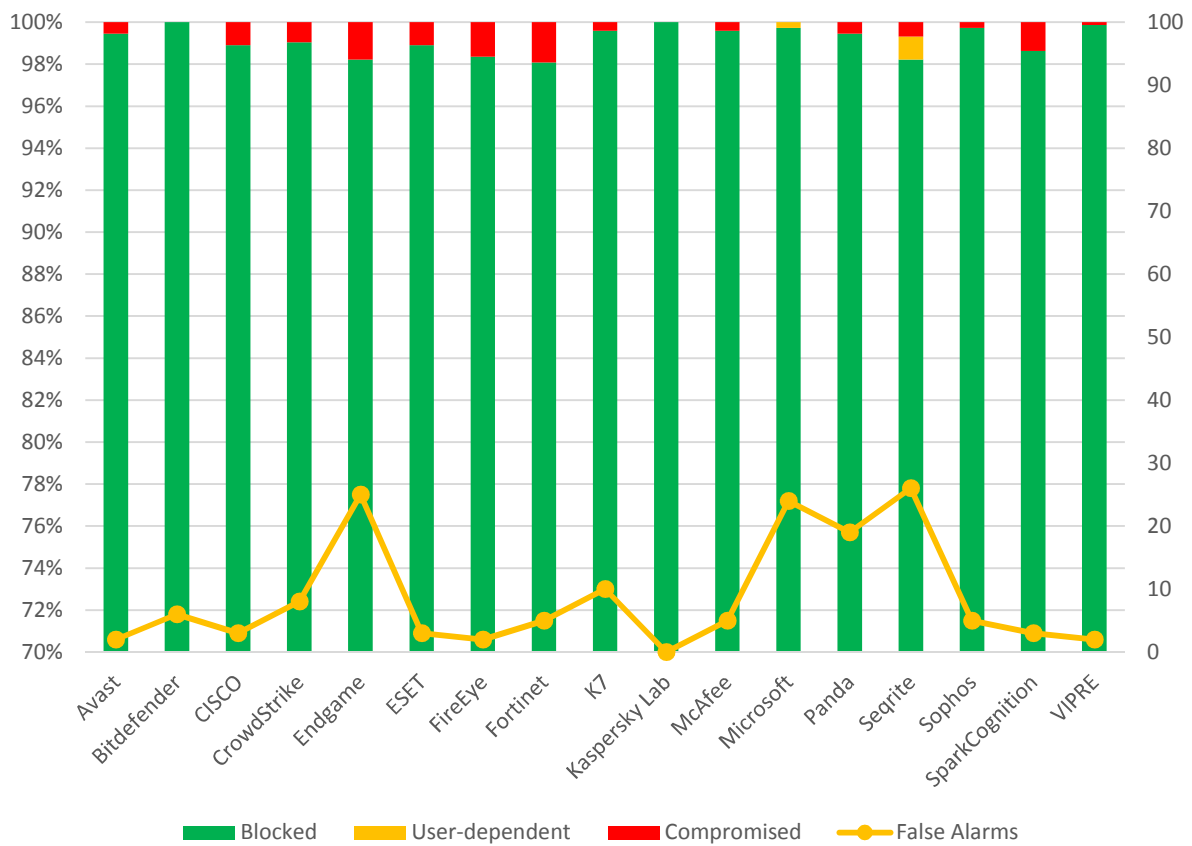
Due to the dynamic nature of the test, i.e. mimicking real-world conditions, and because of the way several different technologies (such as cloud scanners, reputation services, etc.) work, it is a matter of fact that such tests cannot be repeated or replicated in the way that e.g. static detection rate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

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

Test Set

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

The results below are based on a test set consisting of 732 test cases (such as malicious URLs), tested from the beginning of March 2019 till the end of June 2019.



	Blocked	User dependent	Compromised	PROTECTION RATE [Blocked % + (User dependent %)/2] ⁵	False Alarms
Kaspersky	732	-	-	100%	0
Bitdefender	732	-	-	100%	6
VIPRE	731	-	1	99.9	2
Microsoft	730	2	-	99.9	24
Sophos	730	-	2	99.7	5
McAfee	729	-	3	99.6	5
K7	729	-	3	99.6	10
Avast	728	-	4	99.5	2
Panda	728	-	4	99.5	19
CrowdStrike	725	-	7	99.0	8
Cisco, ESET	724	-	8	98.9	3
SparkCognition	722	-	10	98.6	3
Seqrite	719	8	5	98.6	26
FireEye	720	-	12	98.4	2
Endgame	719	-	13	98.2	25
Fortinet	718	-	14	98.0	5

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

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

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

a) Wrongly blocked domains (while browsing)

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

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

b) Wrongly blocked files (while downloading/installing)

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

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

Endgame, K7, Microsoft, Panda and Seqrite and had an above-average number of FPs in the Real-World Protection Test.

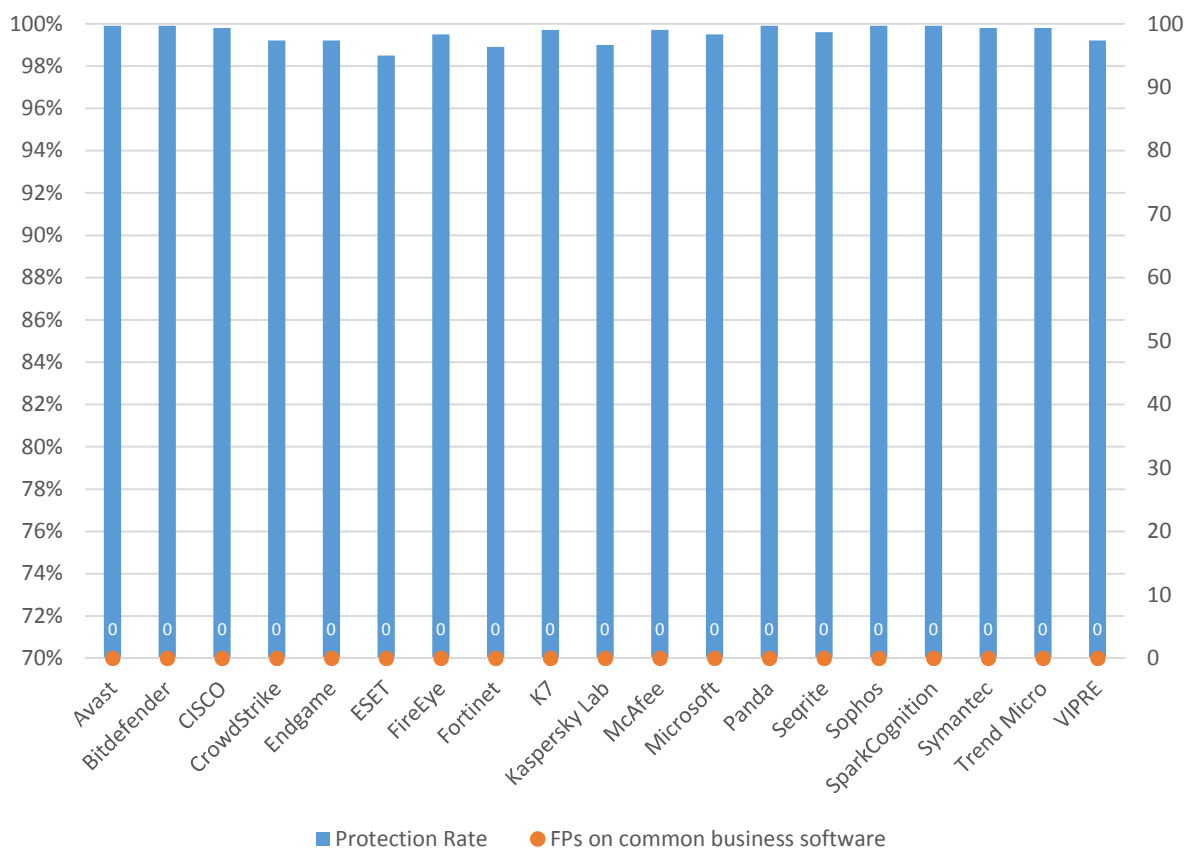
Malware Protection Test (March)

The Malware Protection Test assesses a security program’s ability to protect a system against infection by malicious files before, during or after execution. The methodology used for each product tested is as follows. Prior to execution, all the test samples are subjected to on-access scans (if this feature is available) by the security program (e.g. while copying the files over the network). Any samples that have not been detected by the on-access scanner are then executed on the test system, with Internet/cloud access available, to allow e.g. 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, **1,311** 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. As expected, all the tested products had **zero** false alarms on common business software.

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



	Malware Protection Rate	False Alarms on common business software
Avast, Bitdefender, Panda, Sophos, SparkCognition	99.9%	0
Cisco, Symantec, Trend Micro	99.8%	0
K7, McAfee	99.7%	0
Seqrite	99.6%	0
FireEye, Microsoft	99.5%	0
CrowdStrike, Endgame, VIPRE	99.2%	0
Kaspersky	99.0%	0
Fortinet	98.9%	0
ESET	98.5%	0

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

FP rate	Number of FPs on non-business software
Very low	0-5
Low	6-25
Medium	26-50
High	51-100
Very High	101-200
Remarkably High	>200

	FP rate on non-business software
Cisco, ESET, FireEye, Fortinet, Kaspersky, McAfee, Microsoft, Seqrite, Symantec	Very low
-	Low
Avast, Bitdefender, K7, Sophos, Trend Micro, VIPRE	Medium
Panda, SparkCognition	High
CrowdStrike, Endgame	Very high
-	Remarkably high

Performance Test (June)

We want to make clear that the results in this report are intended only to give an indication of the impact on system performance (mainly by the real-time/on-access components) of the business security products in these specific tests. Users are encouraged to try out the software on their own PC's and see how it performs on their own systems.

We have tested the product that each manufacturer submits for the protection tests in the Business Main Test Series. Please note that the results in this report apply only to the specific product versions listed above (i.e. to the exact version numbers and to 64-bit systems). Also, keep in mind that different vendors offer different (and differing numbers of) features in their products.

The following activities/tests were performed under an up-to-date **Windows 10 1809 64-Bit system**:

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

Test methods

The tests were performed on an Intel Core i3-6006U CPU system with 4GB of RAM and SSD system drives. We consider this machine configuration as “**low-end**”. The performance tests were done on a clean Windows 10 1809 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: copying⁶ different types of clean files from one place to another, archiving and unarchiving files, downloading files from the Internet and launching applications (opening documents).

⁶ We use around 5GB of data consisting of various file types and sizes (pictures, movies, audio files, MS Office documents, PDF documents, business applications/executables, Windows operating system files, archives, etc.).

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).

Test cases

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

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

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

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

Downloading files: The content of several common websites is fetched via wget from a local server and public webserver.

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

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

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

Overview of single AV-C performance scores



PC Mark Tests

In order to provide an industry-recognized performance test, we used the PC Mark 10 Professional Edition⁷ testing suite. Users using PC Mark 10 benchmark⁸ 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 website⁹.

“No security software” is tested on a baseline¹⁰ system without any security software installed, which scores 100 points in the PC Mark 10 benchmark.

	PC Mark Score
Baseline	100
K7	99.3
ESET	99.2
VIPRE	99.0
Endgame	98.6
Seqrite	98.4
Kaspersky	98.3
Bitdefender	98.1
Panda	97.8
Avast	97.5
Cisco	97.5
SparkCognition	97.3
McAfee	97.2
CrowdStrike	97.1
Sophos	96.5
Microsoft	96.4
FireEye	95.4
Fortinet	95.2

⁷ For more information, see <https://benchmarks.ul.com>

⁸ PC Mark® is a registered trademark of Futuremark Corporation / UL.

⁹ http://s3.amazonaws.com/download-aws.futuremark.com/PCMark_10_Technical_Guide.pdf (PDF)

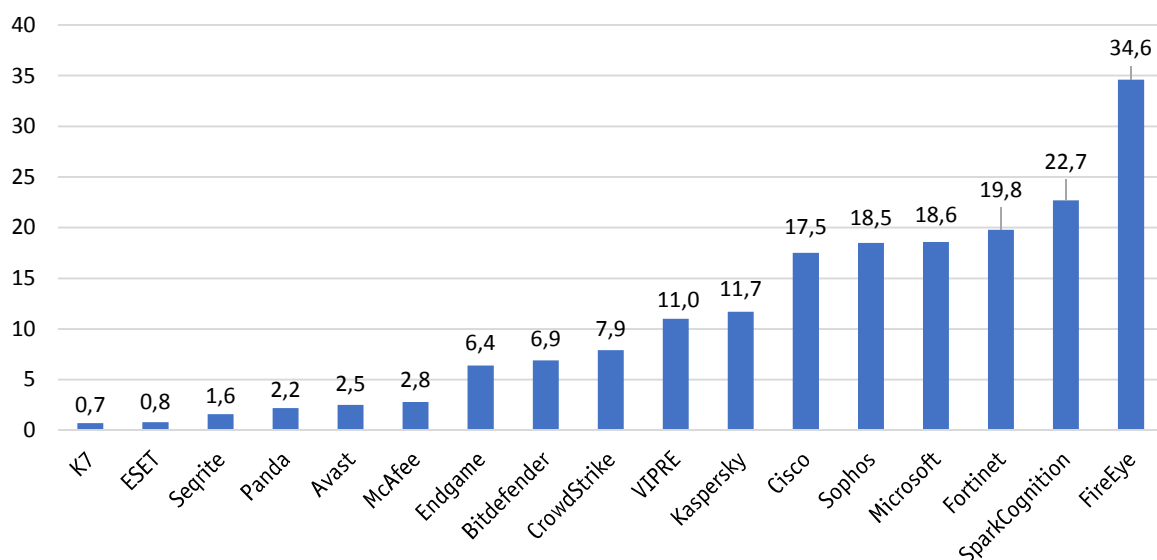
¹⁰ Baseline system: Intel Core i3-6006U machine with 4GB RAM and SSD drive

Summarized results

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

	AV-C Score	PC Mark Score	TOTAL	Impact Score
K7	90	99.3	189.3	0.7
ESET	90	99.2	189.2	0.8
Seqrite	90	98.4	188.4	1.6
Panda	90	97.8	187.8	2.2
Avast	90	97.5	187.5	2.5
McAfee	90	97.2	187.2	2.8
Endgame	85	98.6	183.6	6.4
Bitdefender	85	98.1	183.1	6.9
CrowdStrike	85	97.1	182.1	7.9
VIPRE	80	99.0	179.0	11.0
Kaspersky	80	98.3	178.3	11.7
Cisco	75	97.5	172.5	17.5
Sophos	75	96.5	171.5	18.5
Microsoft	75	96.4	171.4	18.6
Fortinet	75	95.2	170.2	19.8
SparkCognition	70	97.3	167.3	22.7
FireEye	60	95.4	155.4	34.6

Performance Test June 2019 - System Impact Score



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.

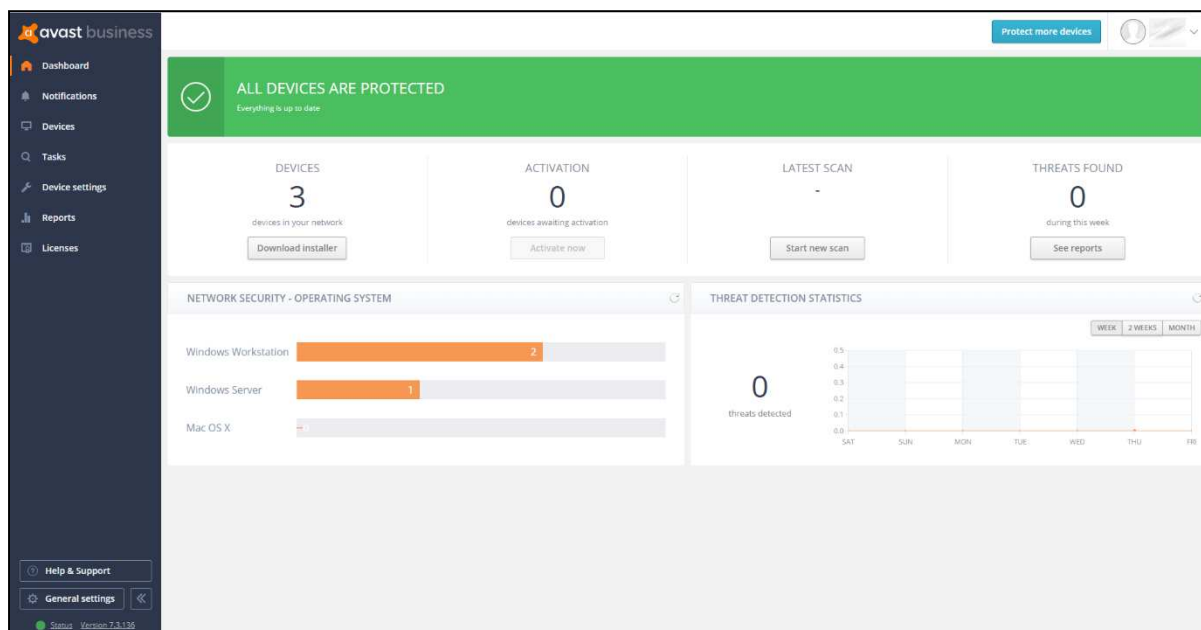
We first look at the type of product, i.e. whether the console is cloud based or server based, and what sort of devices/operating systems can be protected and managed.

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

The review then moves on to ongoing use, i.e. day-to-day management tasks such as monitoring and maintenance that need to be carried out.

Finally, we take a look at the endpoint protection software installed on the client. Here we consider whether the endpoint user can perform any tasks such as scans and updates themselves, or whether such tasks are controlled exclusively by the administrator using the central management console.

Avast Business Antivirus Pro Plus



Verdict

Avast Business Antivirus Pro Plus is a strong product aimed at the small to medium-sized business looking for a solution that requires no onsite server component. The UI is clear and clean, and the defaults are sensible for the smaller organisation. A non-technical user should not have any problems deploying this and keeping track of events. It's probably aimed more at the smaller end of the organisational size. However, it still has grouping and profile capabilities to protect the larger estates. The product was liked as a straightforward platform.

About the product

Avast Business Antivirus Pro Plus uses a cloud-based console to manage endpoint protection solutions. The product protects Windows clients, Windows servers and macOS devices. Features include automatic software updates, data shredding, Exchange and SharePoint security, and data and identity protection.

Getting up and running

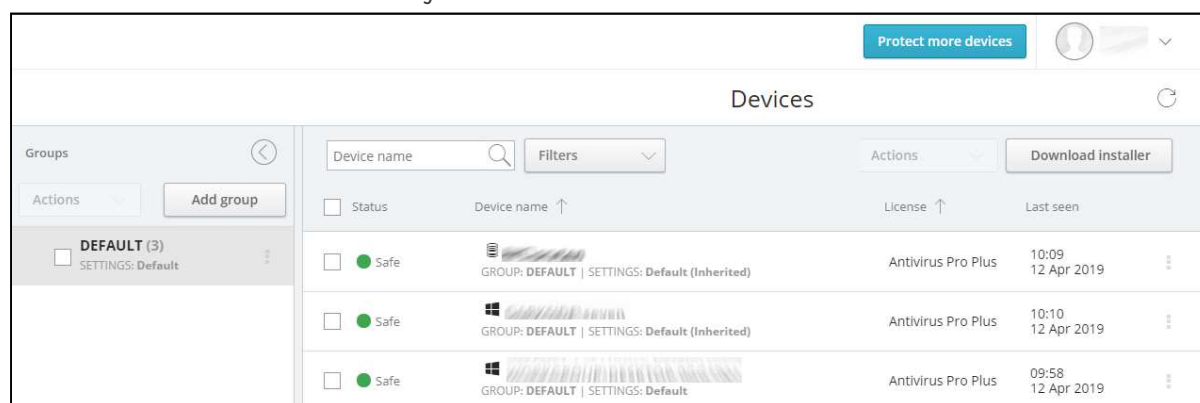
There is no server component to install because it is run from a cloud-based console. You create the account, apply appropriate licensing, and then add devices. Deployment can be carried out via remote push, downloading an installer package, or by sending a download link via email. The installer is offered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

Everyday management

On the server console, there is a clear set of main menus down the left-hand side. These are *Dashboard*, *Notifications*, *Devices*, *Tasks*, *Device Settings*, *Reports* and *Licenses*.

The default *Dashboard* page gives a comprehensive and clear overview of the installation and how it is running. You see how many licenses you have deployed, how many are awaiting activation, and how many threats have been found. There are some graphical views of this information too. It is a straightforward and reassuring overview for the non-expert administrator.

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



The *Devices* tab (screenshot above) shows each device’s configuration, licensing and last-seen time. You can group devices into groups, and apply settings and policy through that group.

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

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

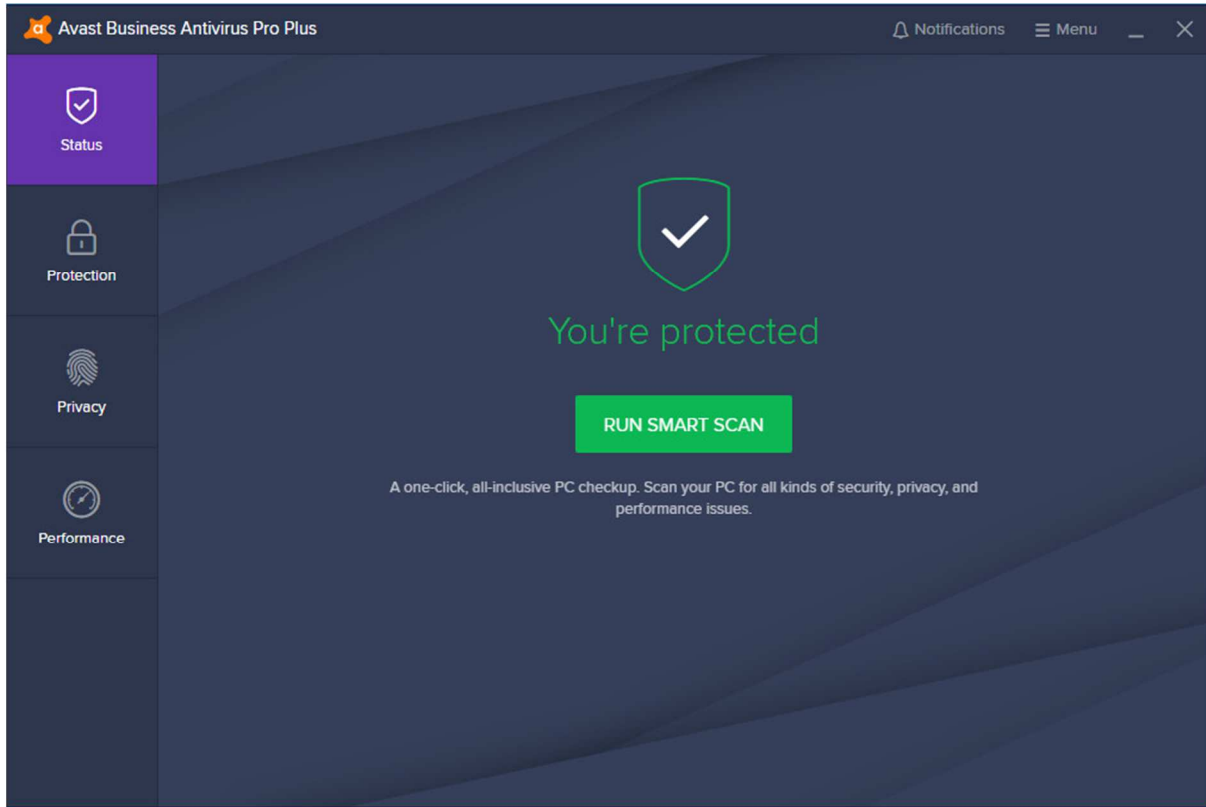
The *Reports* tab gives access to all the statistics about the system and its collection of users. You can drill through here to get a view, and it is a better and more comprehensive overview than the *Dashboard* view. Our only criticism here is that we found no way to either email a PDF of this page nor save it to a file location, which would have been a useful daily report.

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

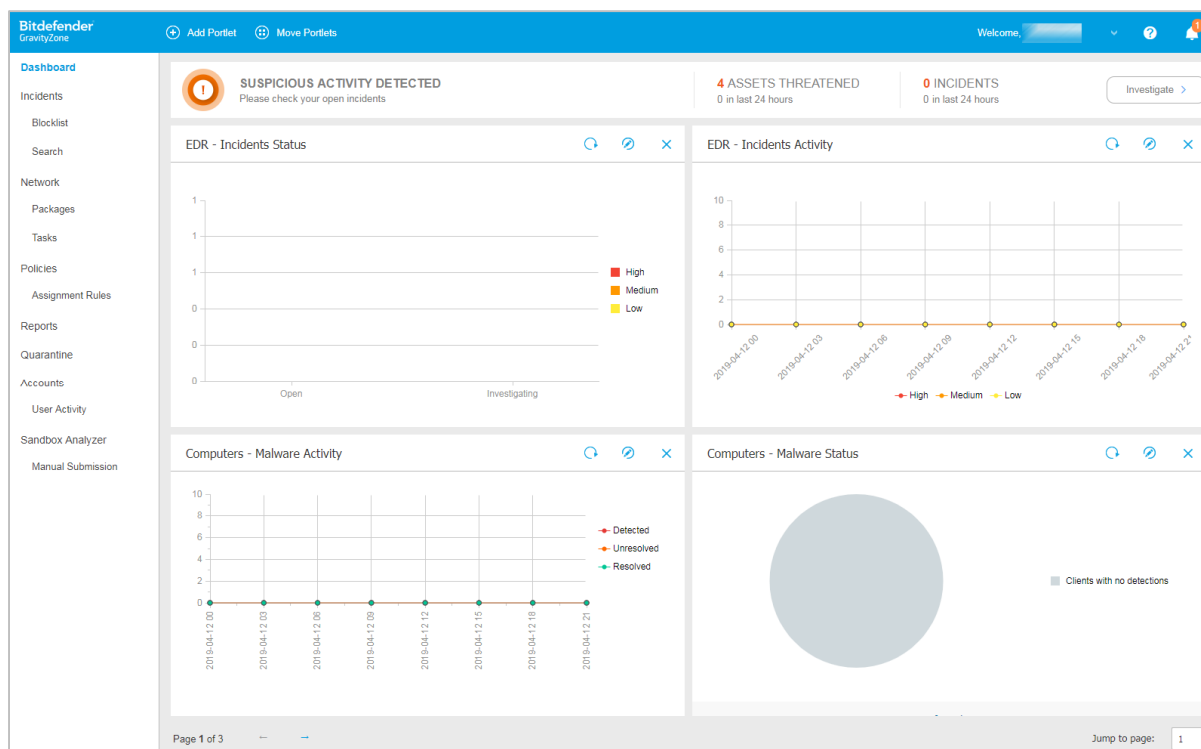
General Settings lets you change the system time zone. You can also create a local server for deployments and updates, and import the database of another Avast console.

Windows endpoint protection software

The client offers a wide range of capabilities, very similar to a normal end-user desktop solution. Users can run scans and updates. The central policies determine what can be changed or adjusted. By default, Windows Standard User Accounts can disable all protection features. Admins may want to prevent this by enabling the password protection feature in the console.



Bitdefender Endpoint Security Elite



Verdict

There is much to like in Bitdefender Endpoint Security Elite. The design of the management console is very clear. Relevant tasks are grouped together, and the initial walkthrough wizard makes deployment easy. We particularly liked the *Dashboard* functionality. The *Policies* feature gives a clear understanding of the rules applied to endpoints.

About the product

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

Getting up and running

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

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

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

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

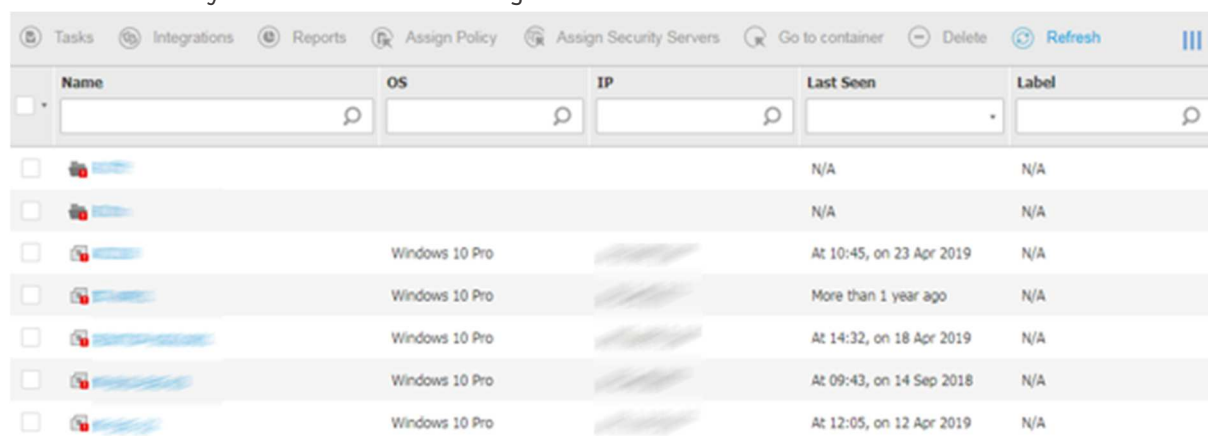
Step 3 is to create appropriate *User Accounts*. These are administrative accounts for the management of the platform. The roles here can be *Company Administrator*, *Network Administrator*, *Reporter* and *Custom*. A *Reporter* might be e.g. a help-desk role, and can see reports of activity without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

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

Everyday management

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

Dashboard gives you an instant overview of the installation and the performance of the clients. Each panel here is called a “portlet” and can be clicked on to drill into more information. We particularly liked the way that the Portlets can be rearranged, added to, and laid out to your preferences. The strong capabilities of *Dashboard* mean that you can quickly and easily find the information you need. *Incidents* allows you to review and investigate threats detected on the network.



Name	OS	IP	Last Seen	Label
			N/A	N/A
			N/A	N/A
	Windows 10 Pro		At 10:45, on 23 Apr 2019	N/A
	Windows 10 Pro		More than 1 year ago	N/A
	Windows 10 Pro		At 14:32, on 18 Apr 2019	N/A
	Windows 10 Pro		At 09:43, on 14 Sep 2018	N/A
	Windows 10 Pro		At 12:05, on 12 Apr 2019	N/A

The *Network* page (shown above) lets you configure deployment packages. You can also create tasks, which can be run once or multiple times.

Policies is where you define the operational groups within your organisation, and then apply policies to them. There is a wealth of capability here. You can control the firewall functionality, application operation, and device access (e.g. blocking USB drives). You can set rules for Exchange Server too.

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

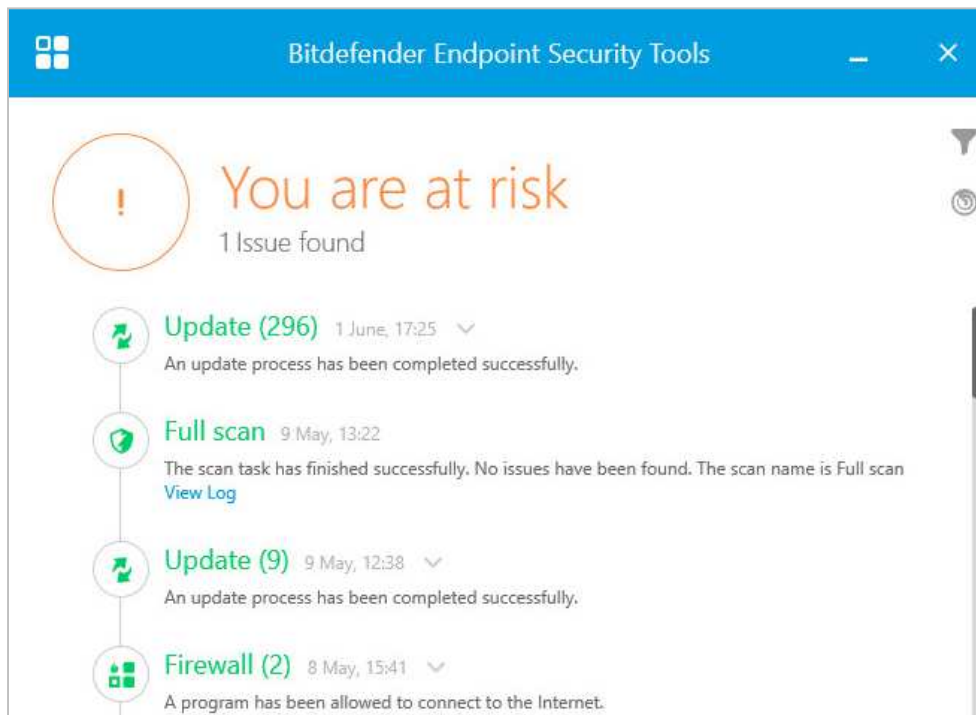
Quarantine gives you an overview of all the malware that has been quarantined on the network, and the ability to choose what to do with those files.

Accounts lets you monitor the activities of the user accounts that have been set up.

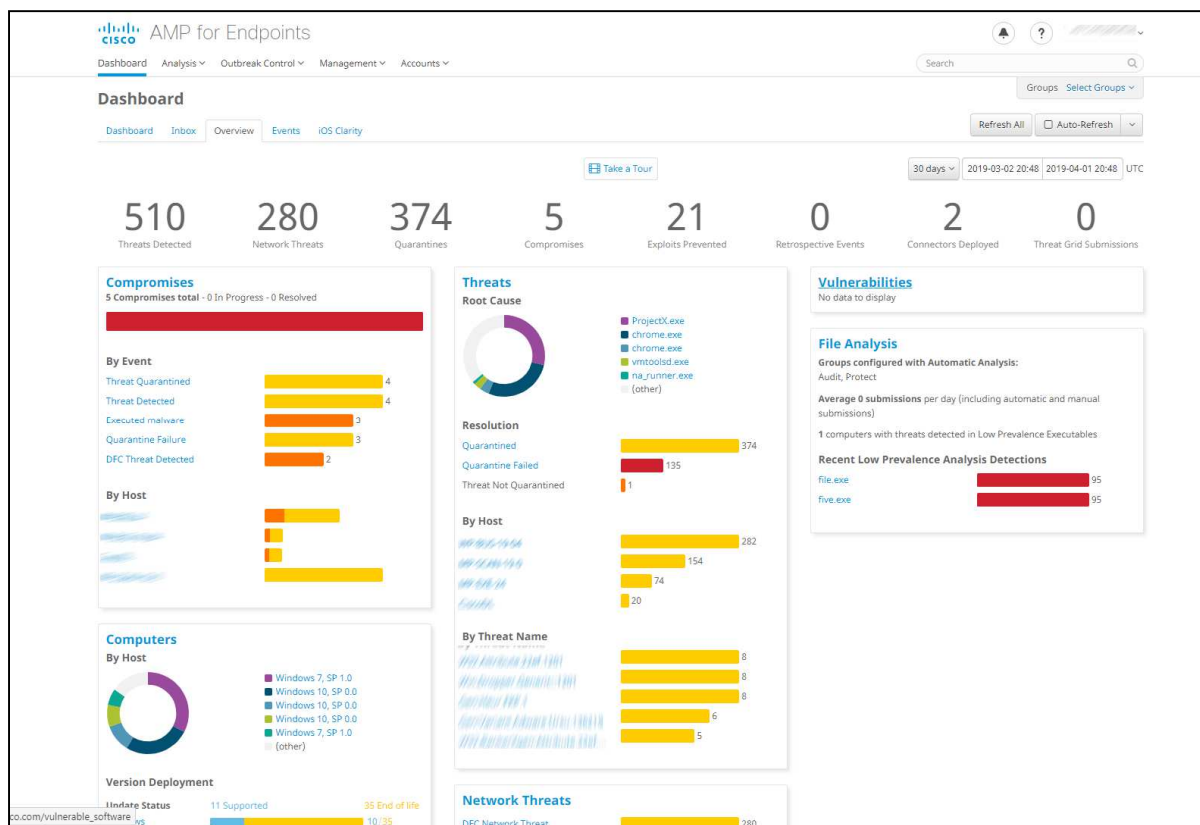
Clicking the bell icon in the top right-hand corner opens the *Notifications* panel. This displays a list of events such as logins and detections. Drilling into an item gives a clear description of what happened. We particularly liked the reporting of a malware outbreak. This informed us that “at least 28% from a total number of X endpoints were found infected with Y malware”. This makes it easy to separate out isolated incidents from a network-wide pandemic.

Windows endpoint protection software

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



Cisco Advanced Malware Protection for Endpoints



Verdict

Getting started with Cisco Advanced Malware Protection for Endpoints is very straightforward. The console requires no setup, and deploying the client software is quick and easy. Clear and colourful bar and doughnut charts summarise the most important information. As regards more advanced monitoring and management, there is a lot of functionality available here. Although the console design makes the different features easy to access, unlocking the product's full potential would clearly take some time. For organisations with appropriate IT staff resources, it provides a wealth of features for monitoring, investigating and blocking security threats.

About the product

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

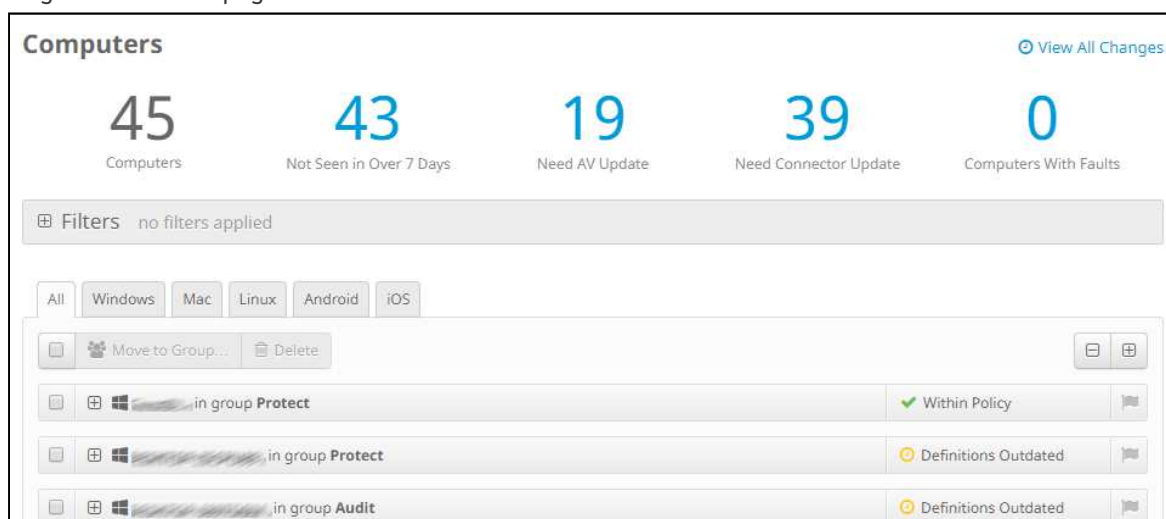
Getting up and running

As the console is cloud-based, no installation is necessary. You just browse to the URL and log in. Installers for desktop systems can be found by clicking *Management\Download Connector*. The setup process is very quick and simple and only takes a couple of clicks.

Everyday management

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

The *Overview* page of the *Dashboard* is probably the best place to start to get a summary of important information. This is shown in the screenshot above. A row of numbers along the top shows statistics for items such as detected threats, quarantined items and compromised devices. Below this, a number of panels with coloured bar and doughnut charts show compromises, threats, vulnerabilities, file analysis, OS distribution, network threats and AV definition status. This provides a very clear summary of the most important information. Very conveniently, you can click on the title of any of these panels to go to a details page for that item.



The *Computers* page, shown above, is accessed from the *Management* menu. This also provides a row of statistics along the top, with items such as computers with faults or needing updates. Below this is a list of individual devices, with a status summary for each one. Clicking on the plus sign for a device displays a detailed information panel, showing information such as OS version, definitions version, internal and external IP addresses, and date and time last seen. The device list can be narrowed by OS type, using the tabs at the top. You can also filter the device list using various details such as specific OS version, group, or definitions status, by clicking on *Filters* at the top.

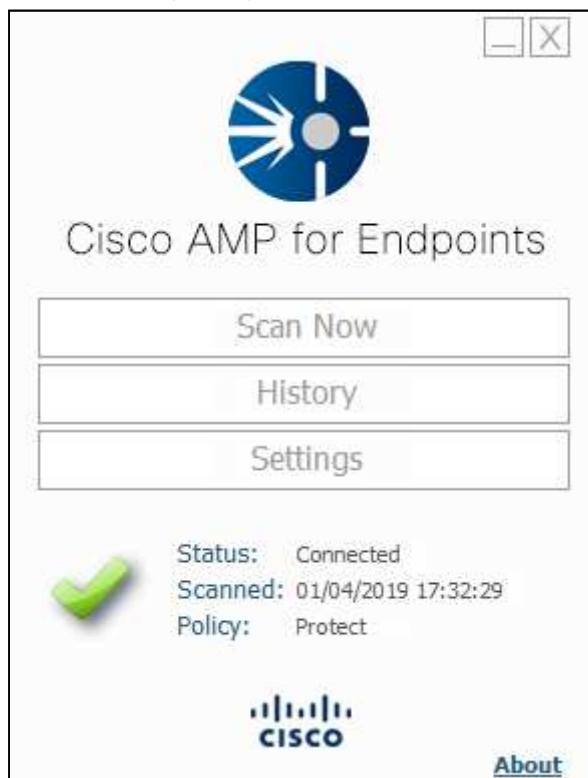
The *Management* menu contains a number of other standard features, such as *Groups*, *Policies*, *Exclusions*, and deployment options. There is also a *Quick Start* guide, in the form of a video explaining the product's features and usage.

In the *Analysis* menu you can find features for investigating attacks. *Events* shows a list of threats encountered by protected devices. These include access to risky websites, malicious file downloads, and attempts to quarantine suspected malware. Clicking on an item displays more details, such as the IP address and port of the threat website, and the hash of the malicious file. This lets you take action against the threats, such as blacklisting the file or website. If you right-click a file's hash here, you have the option *Investigate in Cisco Threat Response*. This opens a separate console, which provides additional analysis data. Cisco tell us that this includes information from 3rd-party security services as well as their own. The *Detections/Quarantine* page is similar, but filters the information down to actual malware encounters.

You can drill down even further on the *File Analysis* page, which 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, along with CVE-ID and CVSS info to help identify and resolve the problem. Finally, *Reports* provides a very detailed weekly report, covering numerous items such as threats, compromises and vulnerabilities. These are illustrated with coloured bar and doughnut charts.

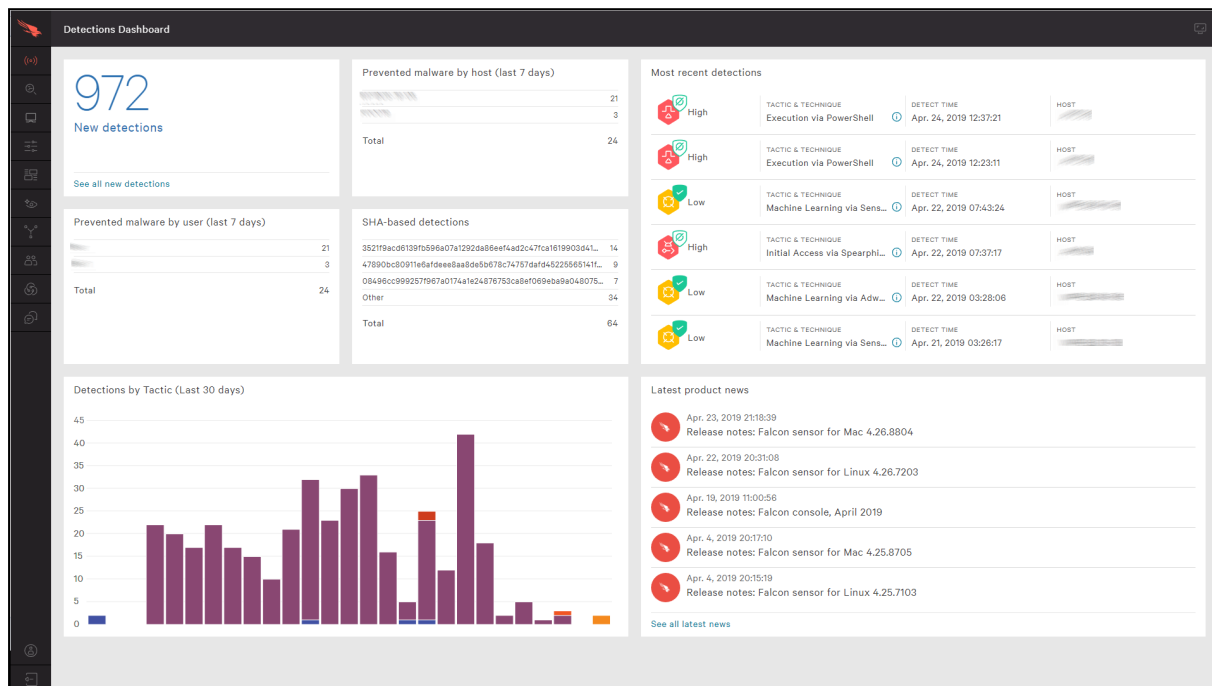
The *Outbreak Control* menu provides options for blocking or whitelisting specific applications and IP addresses. There are also custom detection options, which mean you can block the installation of any program you consider to be harmful or unwanted anywhere on the network. You can also run IOC (indicator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

Windows endpoint protection software



The Windows endpoint client has a very simple GUI, which allows users to run scans and view the logs. Both of these functions open in separate, larger windows. Users can also view settings, but by default these are locked down. Users have a choice of scans they can run. Options are *Flash Scan* (running processes), *Custom Scan*, *Full Scan* and *Rootkit Scan*. By default, malware copied to the system is silently detected and deleted, i.e. without an alert being shown. However, this can be configured by policy to show notifications.

CrowdStrike Endpoint Protection Platform Standard Bundle



Verdict

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

About the product

Crowdstrike Falcon is an endpoint protection platform. It is responsible for proactively looking for malicious activities and adversaries (nation state, eCrime, or hacktivist actors). The cloud-based management console can be run from the cloud on any modern browser. Endpoint protection software is provided for Windows clients and servers, macOS, and specific Linux client and server distributions.

Getting up and running

The management infrastructure comes pre-packaged for you in a cloud console and requires no on-premise equipment – only a modern browser. Deployment of the client “sensor” is quite simple here. It relies on the download of the installation package appropriate to the target platform. On Windows, you can use an automatic sensor deployment like Windows System Center Configuration Manager. Once installed, the Falcon Sensor is almost invisible to the end user. Docker support allows the installation of the Falcon agent on hosts running Docker. Deployment across an organisation will take planning and appropriate tools. This includes preparation for the appropriate layers of policy to be applied to users. Once this work has been done, deployment should be quite straightforward.

Everyday management

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

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

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

The screenshot shows the 'Hosts' page in the CrowdStrike Falcon management console. At the top, there is a search bar with the text 'Type to filter' and a result count of '2,029 hosts found'. Below this is a summary table with columns: Platform, OS Version, OU, Site Name, Type, and Status. The summary table shows 2,028 Windows and 1 Mac. The main table below has columns: Hostname, Last Seen, First Seen, OS Version, OU, Prevention Policy, Response Policy, Sensor Update P..., Status, and Sensor Version. Three host entries are visible, all with 'Normal' status and 'platform_default' policies.

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

Hostname	Last Seen	First Seen	OS Version	OU	Prevention Policy	Response Policy	Sensor Update P...	Status	Sensor Version
[REDACTED]	Apr. 2, 2019 13:38...	Apr. 1, 2019 14:50...	Windows 10		platform_default Apr. 1, 2019 14:50...	platform_default Apr. 1, 2019 14:50...	platform_default Changes pending	Normal	4.24.8702.0
[REDACTED]	Apr. 16, 2019 10:0...	Apr. 15, 2019 10:3...	Windows 10		platform_default Apr. 15, 2019 10:3...	platform_default Apr. 15, 2019 10:3...	platform_default Changes pending	Normal	4.25.8802.0
[REDACTED]	Mar. 6, 2019 20:5...	Mar. 6, 2019 20:5...	Windows 10		platform_default Mar. 6, 2019 20:5...	platform_default Mar. 6, 2019 20:5...	platform_default Changes pending	Normal	4.21.8408.0

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

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

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

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

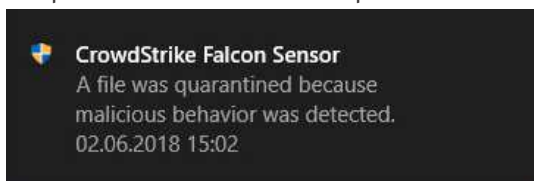
The *Intelligence* menu takes you into an overview of the current landscape threat as perceived by CrowdStrike. This can be categorised by different factors. Examples include geographical origin of threat, target industry, target country, and motivation (espionage/criminal/Hactivist and destruction).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

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

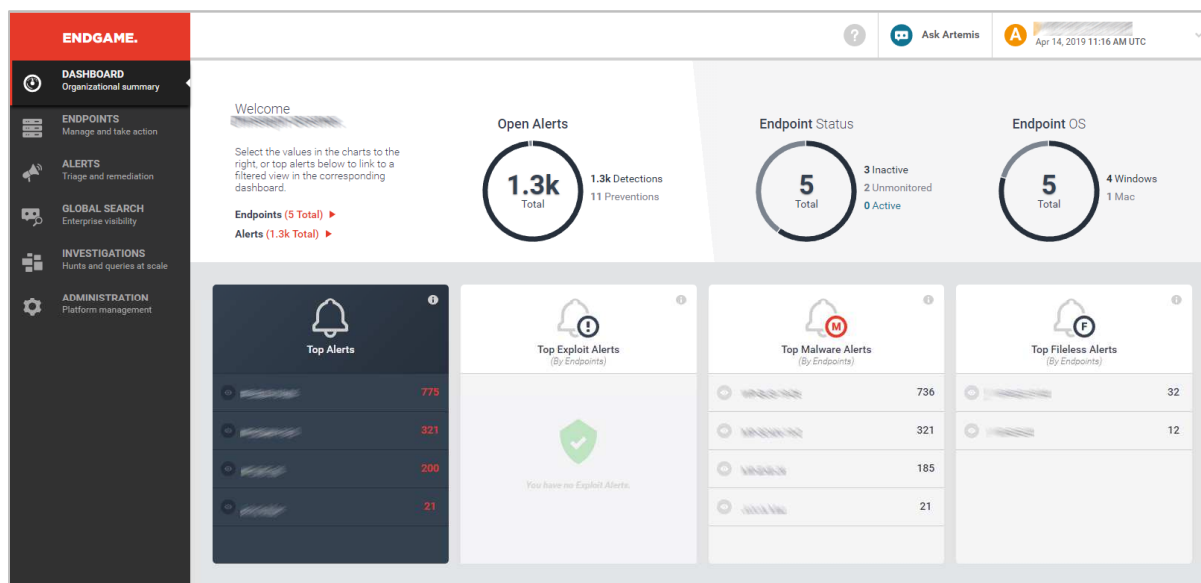
The *CrowdStrike Store* allows you to extend the capabilities of the Falcon platform with a host of ready-to-go partner apps and add-ons.

Windows endpoint protection software

On the end-user client, the default setting is to have the client invisible to the user. The only exception is malware alerts – please see screenshot below.



Endgame Protection Platform



Verdict

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

About the product

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

Getting up and running

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

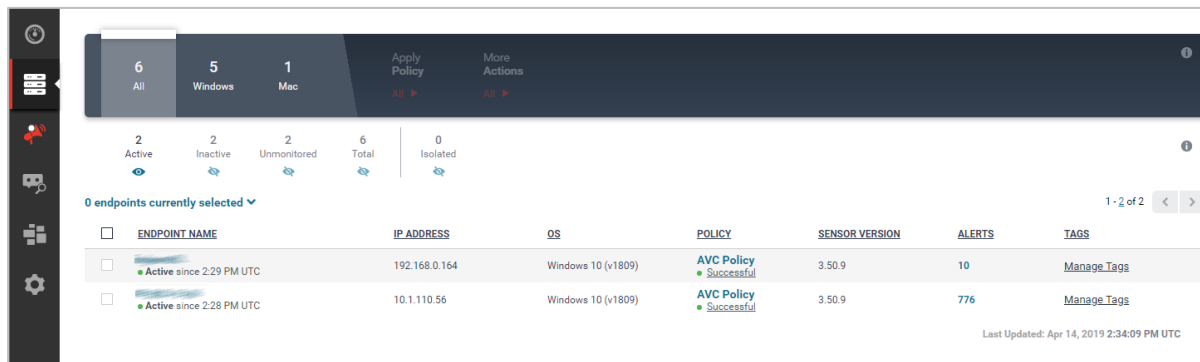
In-band is currently only for Windows. The administrator installs the sensor directly onto Windows clients or servers from the Endgame management platform. The administrator can scan the network for unmonitored endpoints and install the sensor after entering credentials for that endpoint.

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

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

Everyday management

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



The screenshot shows a management console interface. At the top, there are filters for 'All' (6), 'Windows' (5), and 'Mac' (1). Below this, there are status indicators: 2 Active, 2 Inactive, 2 Unmonitored, 6 Total, and 0 Isolated. A table lists endpoints with columns for Endpoint Name, IP Address, OS, Policy, Sensor Version, Alerts, and Tags. Two endpoints are shown, both running AVC Policy (Successful) on Windows 10 (v1809) with sensor version 3.50.9. The first endpoint has 10 alerts, and the second has 776 alerts. The interface also includes a sidebar with navigation icons and a 'Last Updated' timestamp of Apr 14, 2019 2:34:09 PM UTC.

Endpoint Name	IP Address	OS	Policy	Sensor Version	Alerts	Tags
Active since 2:29 PM UTC	192.168.0.164	Windows 10 (v1809)	AVC Policy Successful	3.50.9	10	Manage Tags
Active since 2:28 PM UTC	10.1.110.56	Windows 10 (v1809)	AVC Policy Successful	3.50.9	776	Manage Tags

The *Endpoints* menu gives a view of all the managed clients. You can select and sort by name, IP address, OS version, policy applied, sensor version, alerts and tags. From here, you can choose a range of endpoints and then run tasks on them. These include applying a new policy, discovering new endpoints, and tagging/uninstalling/deleting endpoints from the catalogue.

Alerts takes you into the heart of the platform. Here you get a list of current event types such as malicious file execution prevention or file detection. The catalogue of events can be sorted and categorised by platform, OS, IP address, host and date. Most important is the ability to assign an event to a user to manage that alert, and ensure it is appropriately dealt with.

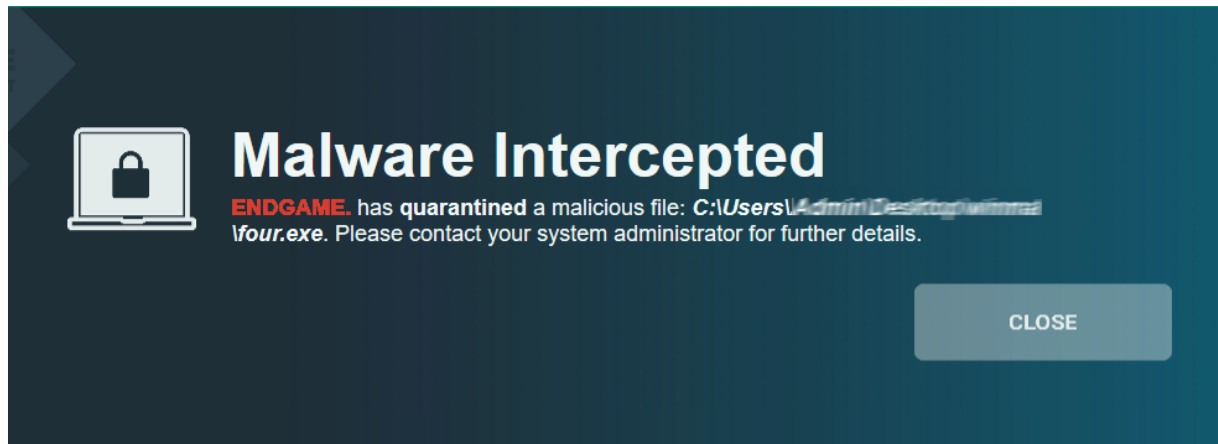
If you click on an event, it takes you to the *Alert Details* page for that event. Here you can see much more detail about the event, where it started, what it has done and the analysis of the malware if appropriate. Here you can choose *Take Action*: the options include *Download Alert*, *Download Timeline*, *Resolve*, *Dismiss*, *Start Investigation*, *Download File*, *Delete File* or *Whitelist Items*. Of particular interest here is the *Start Investigation* feature which lets you create a *Hunt*. A *Hunt* can cover multiple information sources, e.g. firewall rules, drivers, network, persistence, process, registry, media, or system configuration. It allows you to search the network for information relevant to your enquiry. A key component here is the *Ask Artemis* feature, which is a natural language query engine. You can simply type in a question, and Artemis will attempt to resolve it.

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

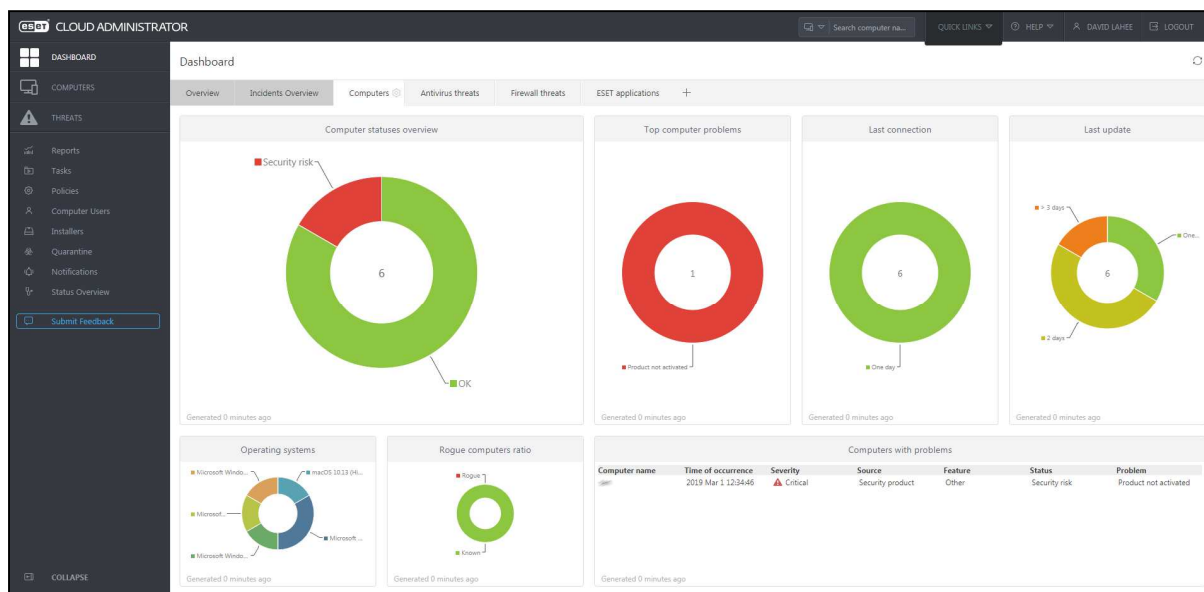
Finally, the *Administration* menu item gives access to the *Policy Settings*, *Users*, *Sensors*, *Alerts*, *Whitelist* and *Platform* features. The *Policy Settings* page lets you define policy for events such as privilege escalation, process injection, and credential access. As an example, you can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

Windows endpoint protection software

On the client side, there is effectively nothing to see unless the system detects an issue. At this point, a large banner appears on the screen telling them what has happened. From a user perspective, the Endgame platform is essentially invisible and there is nothing here for the user to interact with.



ESET Endpoint Protection Advanced Cloud with ESET Cloud Administrator



Verdict

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

About the product

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

Getting up and running

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

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

Everyday management

You can find all the main functions of the console in a single menu column on the left-hand side. The console opens on the *Dashboard/Computers* page, shown in the screenshot above. This provides an at-a-glance overview of the network, in the form of colour-coded doughnut charts. You can see the security status of the network, along with details of any problems and rogue computers. The time of last connection and last update are also shown, as is the distribution of different operating systems. You can easily get more details for any item just by clicking on its graphic. Similar links to details and solutions are provided throughout the console. The panels of the dashboard are very customisable. You can move them around, resize them, and change the chart type, among other things. Other tabs on the *Dashboard* page let you zoom in on antivirus or firewall threats, ESET applications, and incidents.

Groups	COMPUTER NAME	STATUS	MUTI	MODULES	LAST CONNECTED	ALER	THRE	SECURITY PRODUCT	SECURITY
CUSTOM GROUPS	All (6)								
Lost & found (5)	192.168.0.227	✓		Updated	2019 Feb 28 23:02:27	0	90	ESET Endpoint Security	7.0.2100.4
DYNAMIC GROUPS	192.168.0.108	✓		Updated	2019 Mar 1 14:02:23	0	0	ESET Endpoint Security	7.0.2100.4
Windows computers	192.168.0.73	✓		Updated	2019 Mar 1 14:03:00	0	85	ESET Endpoint Antivirus	7.0.2091.0
Windows (desktops)	192.168.0.122	✓		Updated	2019 Mar 1 14:02:20	0	219	ESET Endpoint Security	6.7.654.0
Windows (servers)	192.168.0.200	✓		Updated	2019 Mar 1 14:02:40	0	2	ESET File Security	7.0.12018.0
Mac computers	192.168.0.164	⚠		Updated	2019 Mar 1 13:22:48	3		ESET Endpoint Security	7.0.2100.4
Computers with outdated modules									
Computers with outdated operating system									
Problematic computers									
Not activated security product									

The *Computers* page is shown above. It gives you an overview of all the managed devices on the network; you can click on a computer's entry to get more detailed information about that device. This includes a detailed hardware inventory, amongst other things. You can also organise computers into groups, and carry out tasks such as scans and updates. There are some pre-configured dynamic groups, for example *Computers with outdated operating system*. These make it easy to find all the devices that need your attention.

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

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

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

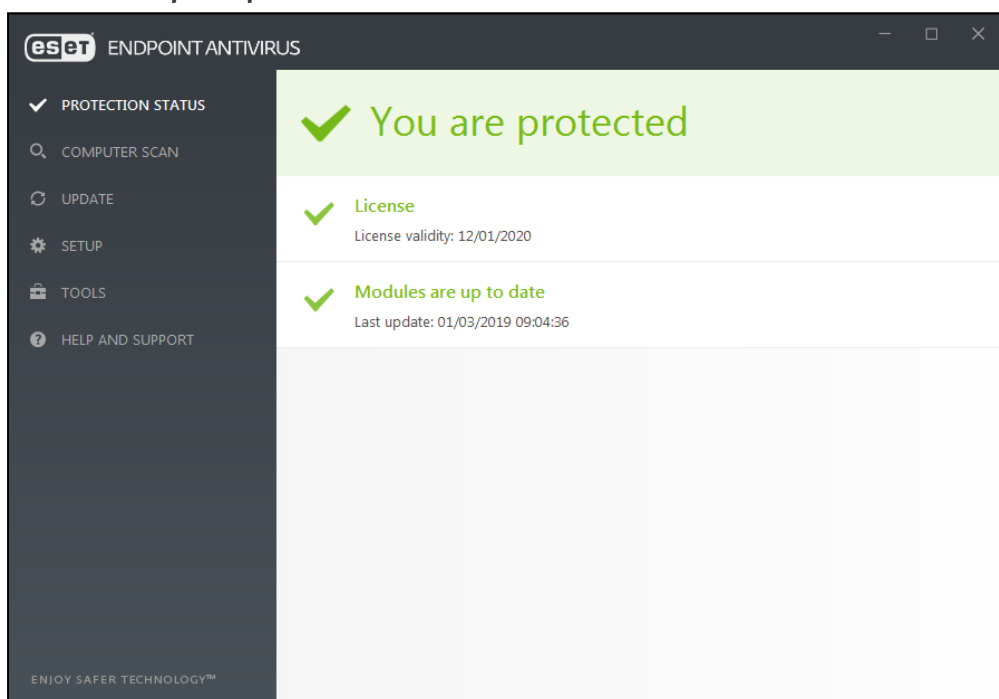
Policies has a convenient list of preconfigured policies that you can apply. These include different security levels, device control options, and how much of the user interface to show to users. You can also create your own custom policies if you want.

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

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

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

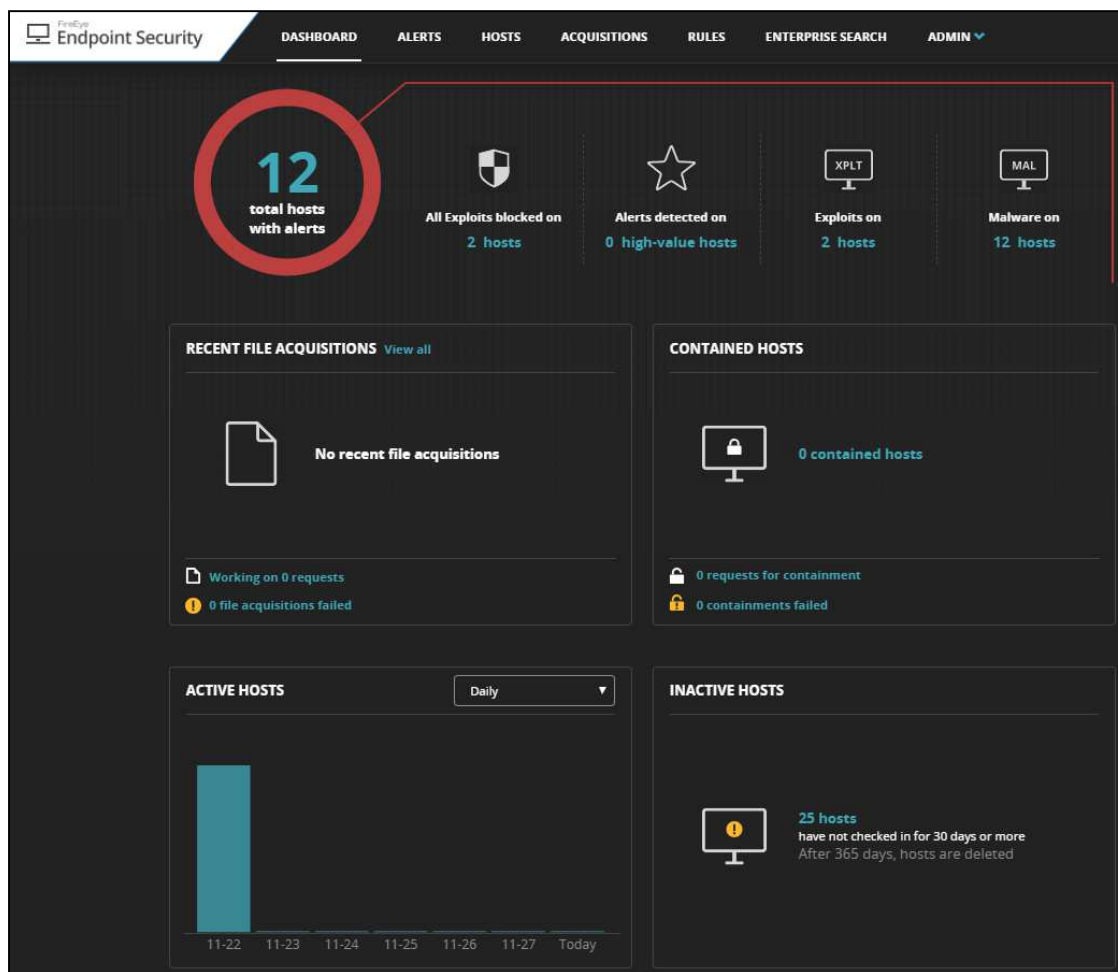
Windows endpoint protection client



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

There is an auto-update feature for the client software, which can be set by policy. This ensures the endpoint protection client is always up to date, by automatically downloading and installing the latest version of the software as soon as it becomes available.

FireEye Endpoint Security



Verdict

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

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

About the product

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

Getting up and running

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

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

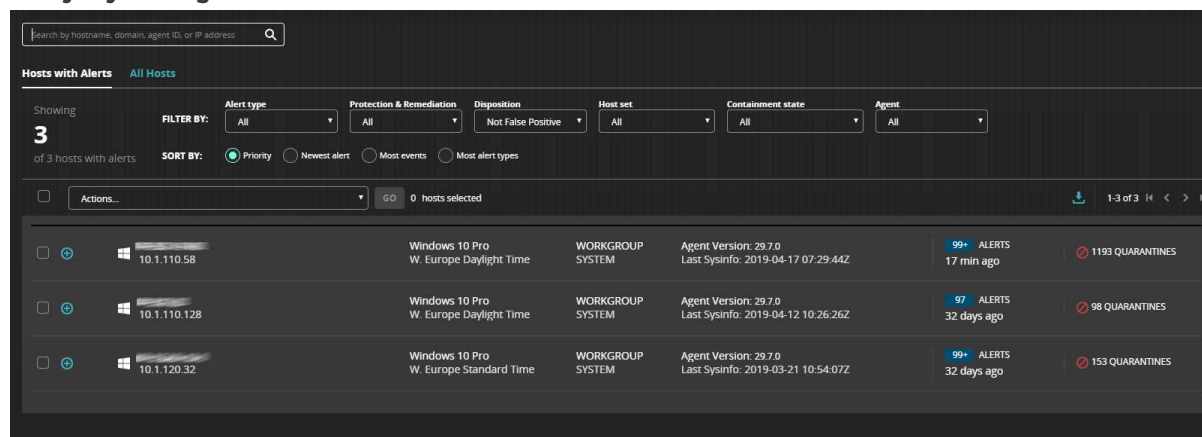
The platform has an extremely powerful and extensive set of information gathering tools. These allow you to build comprehensive queries of almost any type. These are then dispatched to the clients. Analysing this information is the core of the server product.

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

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

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

Everyday management



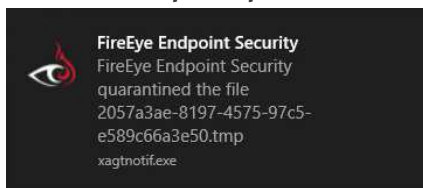
The management console is not a tool to be dipped into occasionally. Unlocking its huge power needs considerable understanding of what the platform offers and how to achieve it. There is little handholding here. The product is aimed squarely at the large corporate space, where training and consultancy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

Firstly, you need to understand what FireEye is trying to achieve. It relies on gathering and analysing, threat-detection capabilities, and “behind the scenes” operation on the client. The emphasis here is solidly on information acquisition, analysis and reporting. This allows the central administrators to initiate information gathering from a wide array of client machines. The information can then be processed, allowing you to take actions based upon it.

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

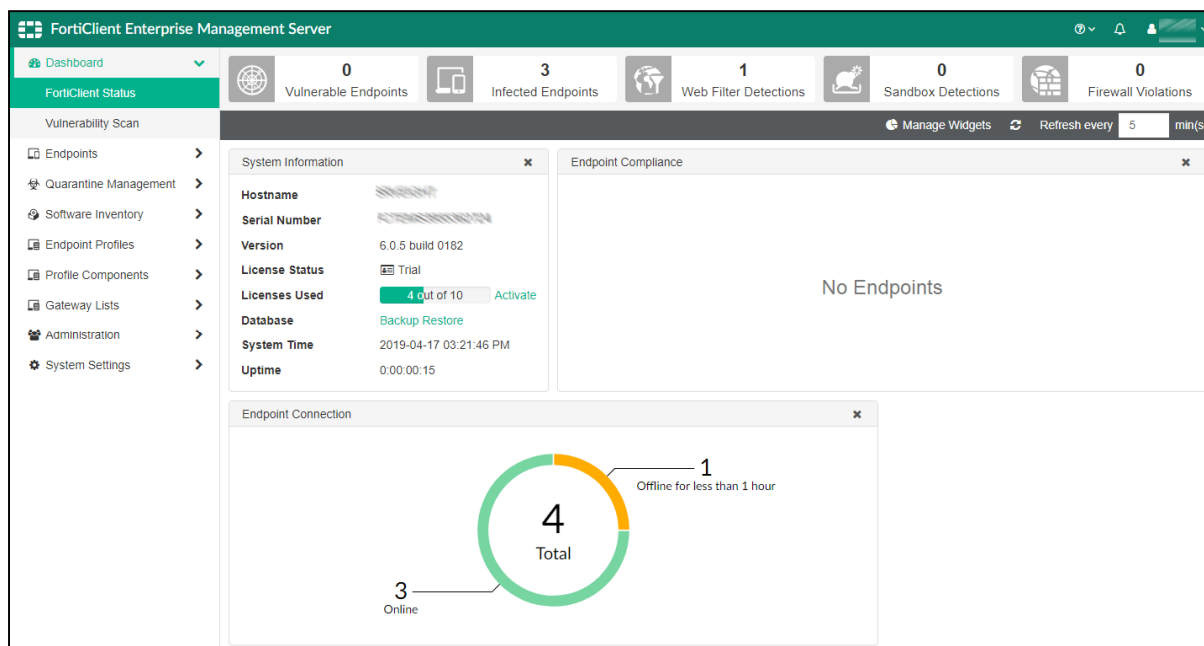
It should not be underestimated how much technical and systems knowledge is required to get the best from this. This is not a criticism. Indeed, for a hard-core IT administrator, it is a great strength to have access to this level of query and analysis of the network.

Windows endpoint protection software



The Windows client does not provide any user interface. There is not even a status icon or a context-menu scan function. FireEye does pop up a warning message when malware is found (screenshot above). However, the client is otherwise invisible to the end user. It is designed to be wholly managed from the centralised console with no user input.

Fortinet FortiClient with Enterprise Management Server & FortiSandbox



Verdict

The Fortinet Enterprise Management Server package is a strong product aimed at the larger organisation. It is relatively straightforward to install and deploy, but would benefit from more handholding for the smaller organisation. There is some welcome graphical reporting, but we felt that more could be done here, especially helping the administrator dig through the status of the network. Nevertheless, the day-to-day operation would benefit from training and time spent learning, in order to extract the full understanding and performance.

About the product

The server-based console is called FortiClient Enterprise Management Server (EMS), and the client is called FortiClient. The console requires a Windows Server OS (2008 R2) or later. There is endpoint protection software for Windows clients and servers, Mac OS X and Linux.

Getting up and running

EMS is a local server-based product. Installing the management console is very simple and requires almost no user interaction. Once up and running, there are some tasks you need to perform before the client can be deployed. The real-time protection feature of the endpoint protection software is disabled in the default policy. However, it is very simple to switch it on *Endpoint Profiles/Default*.

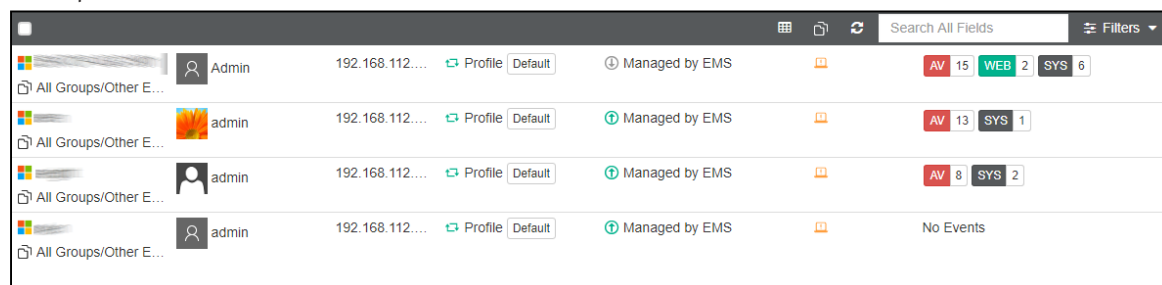
Once you have done this, you can then deploy the client to the desktop. The installer can be downloaded by browsing to the server's URL or www.forticlient.com. You will need to connect the endpoint client on each machine to the server. This just involves typing in the server's IP address and clicking *Connect*. On the server side, there are good reports for devices discovered which are not part of the management structure, and it is easy to remediate this. There is a clear and clean view of the status of the network through the *Dashboard/FortiClient Status* view.

Creating users for the management console is fairly easy. A user can be assigned granular permissions, including creation, update and deleting of various settings, and the abilities to manage endpoints. Finally, you can assign permissions for policy management here too. So, an organisation should be able to create a relatively fine-grained set of permissions here for various levels of administrative role. There isn't much in the way of handholding in the initial setup process for the smaller organisation. Clearly the product is aimed at the more professional, larger organisation which will have had training and consultancy for deployment.

Everyday management

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

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



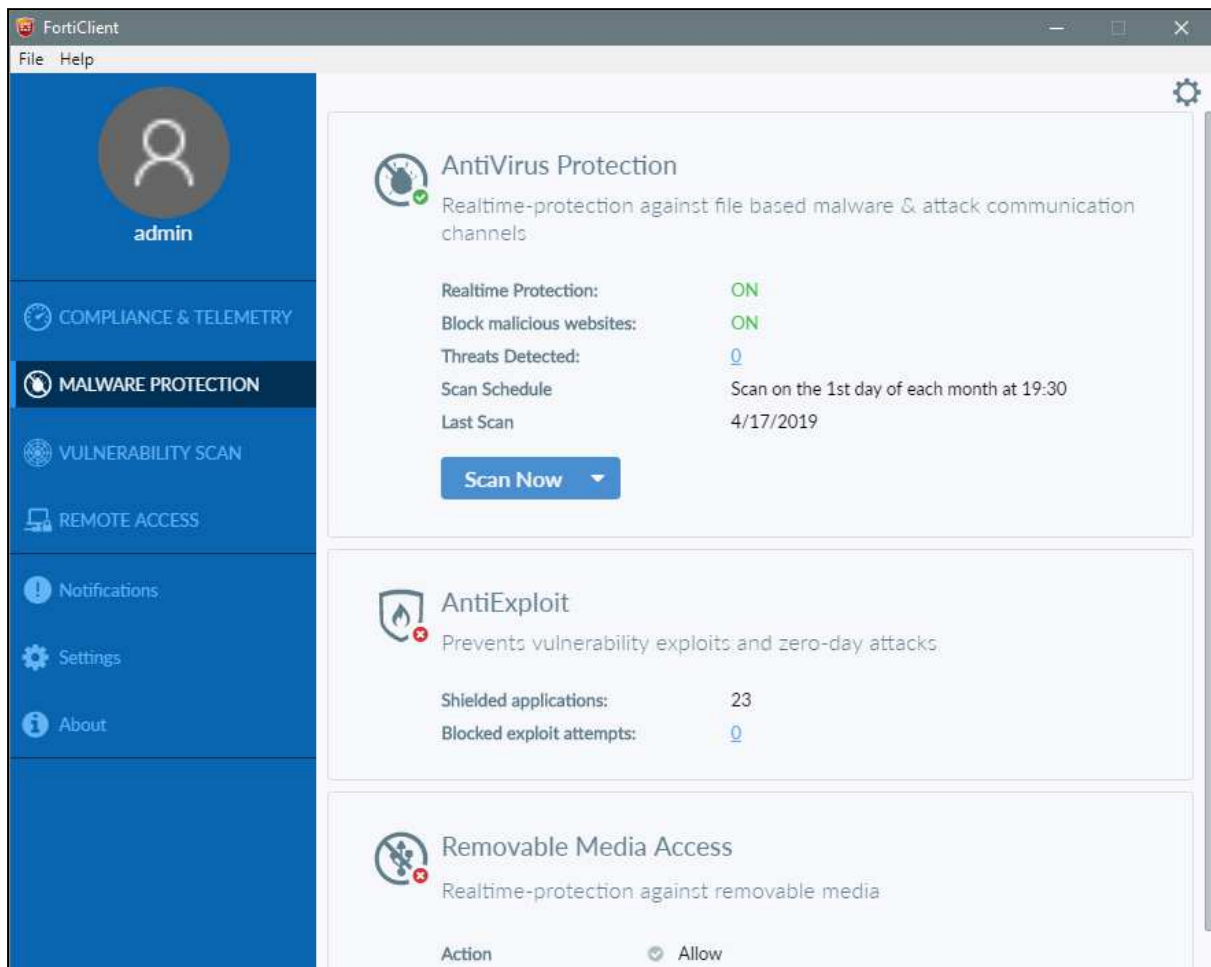
Endpoint	IP Address	Profile	Managed by EMS	AV	WEB	SYS
Admin	192.168.112....	Default	Managed by EMS	15	2	6
admin	192.168.112....	Default	Managed by EMS	13	1	1
admin	192.168.112....	Default	Managed by EMS	8	2	2
admin	192.168.112....	Default	Managed by EMS	No Events		

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

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

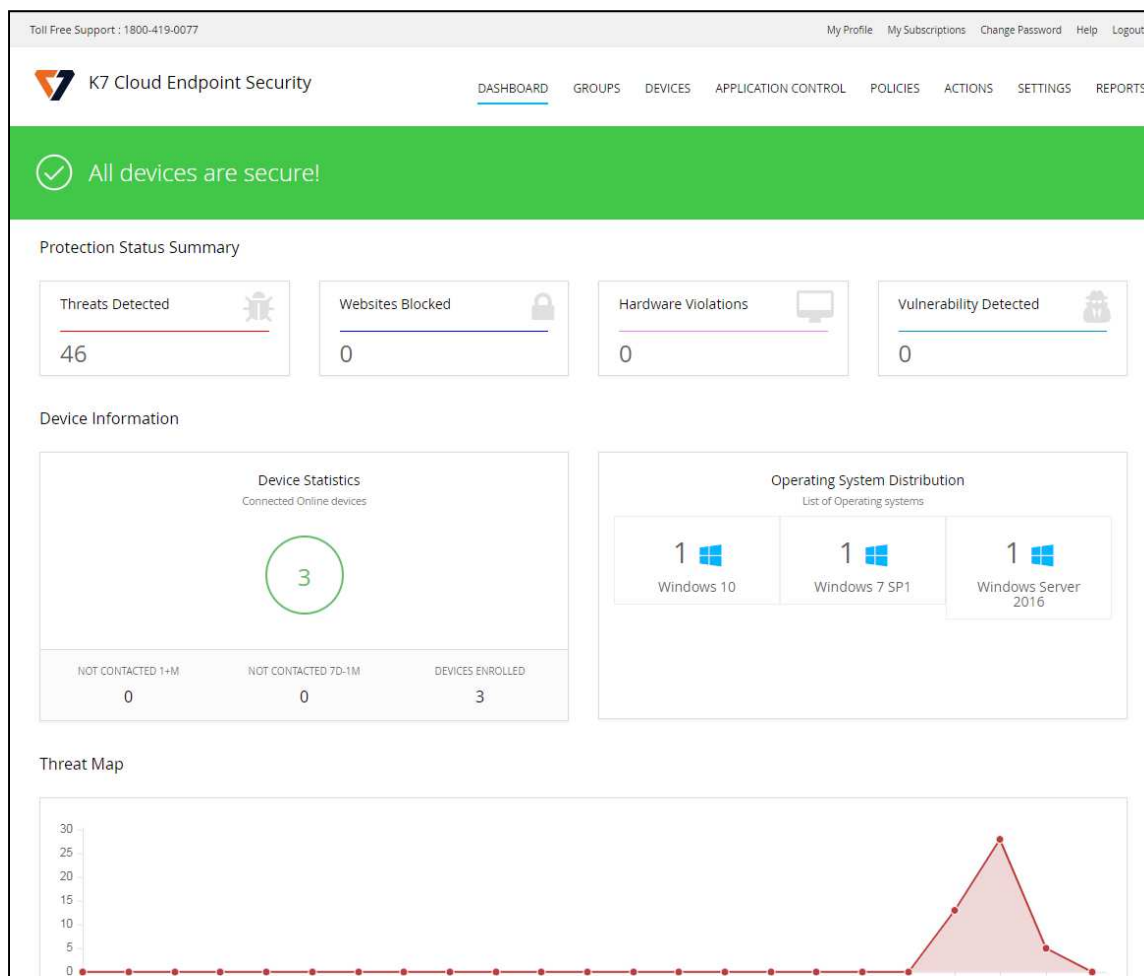
Finally, *Administration* and *System Settings* allows control of the underlying settings of the platform. It is fairly straightforward to use the platform on a day to day basis, both getting reports of what is happening and initiating scans or remedial actions as required. The UI is quite well designed, but would benefit from some final polish to make it more obvious. A stronger splitting of setup from day-to-day and from system administration would help too.

Windows endpoint protection software



After the client installer has been deployed, it fully takes over the Windows AV security role. The functionality available to the client user depends upon policy, but by default allows the user to run scans. This can be useful in an environment where users are encouraged to be part of the AV strategy. Users can see some basic settings, but not change them. The client app is modular in design, and what you see depends on the functionality enabled by the policy.

K7 Cloud Endpoint Security



Verdict

K7 Cloud Endpoint Security is designed for enterprises of all sizes, but its ease of use makes it particularly suitable for smaller businesses. It is very quick and easy to set up, due to the cloud-based console and very simple installation process. The management console is very easy to navigate, and the endpoint client lets users carry out scans and updates very simply. One minor suggestion for improvement would be to include links from the *Dashboard* panels to the relevant details pages. However, overall it is very straightforward and intuitive to use.

About the product

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

Getting up and running

As the console is cloud-based, no installation is necessary. You just browse to the URL and log on. Deploying endpoint protection software is almost as simple. All you need to do is go to the *Settings* page and download an installation package, then run this. The setup wizard is very simple, with no choices to be made. Thus, you can install the client with just a couple of clicks.

Everyday management

All the console's functionality can be accessed from a single menu strip at the top of the window. When you log in, the console opens on the *Dashboard* page, which shows an overview of the system status. There are various detail panels, showing detected threats, blocked websites, violations of hardware policy, device connection statistics, numbers of devices running specific Windows versions, and a timeline of threats discovered. Unfortunately, there are no links to further information. If you want to find more details of any of these items, you have to browse to other pages.

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

The *Devices* page, shown in the screenshot below, lists individual computers on the network. The links in the *Actions* column let you change a computer's group, remove it from the management console, or view its details.

Device Name	Group	OS	Actions
[Redacted]	Default Group	Windows 10	[Eye] [Edit] [Delete]
[Redacted]	Default Group	Windows 7 SP1	[Eye] [Edit] [Delete]
[Redacted]	Default Group	Windows Server 2016	[Eye] [Edit] [Delete]

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

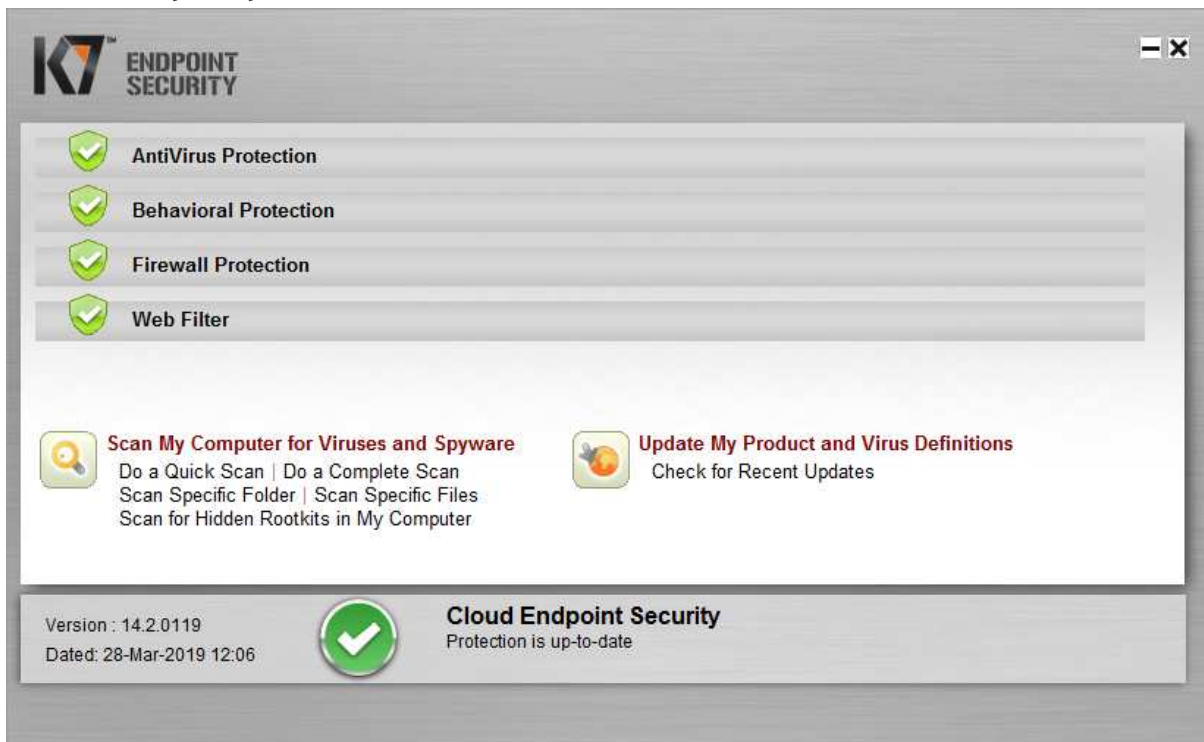
The *Policies* page lets you control settings for the endpoint software. These are conveniently ordered into groups such as *Antivirus*, *Behaviour Protection* and *Firewall*.

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

The *Settings* page might better be called "Installation", as its only function is to let you download installation packages for the endpoint protection software.

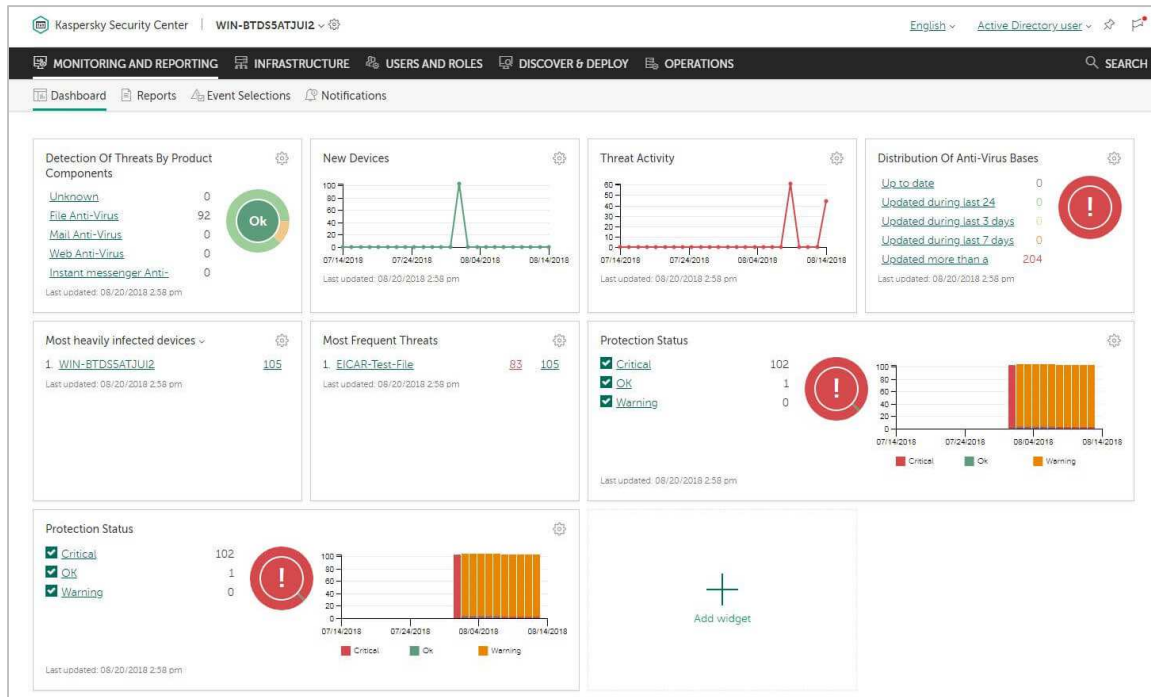
Reports page provides a very simple means of running reports on items such as detected threats and vulnerabilities, and scan results.

Windows endpoint protection software

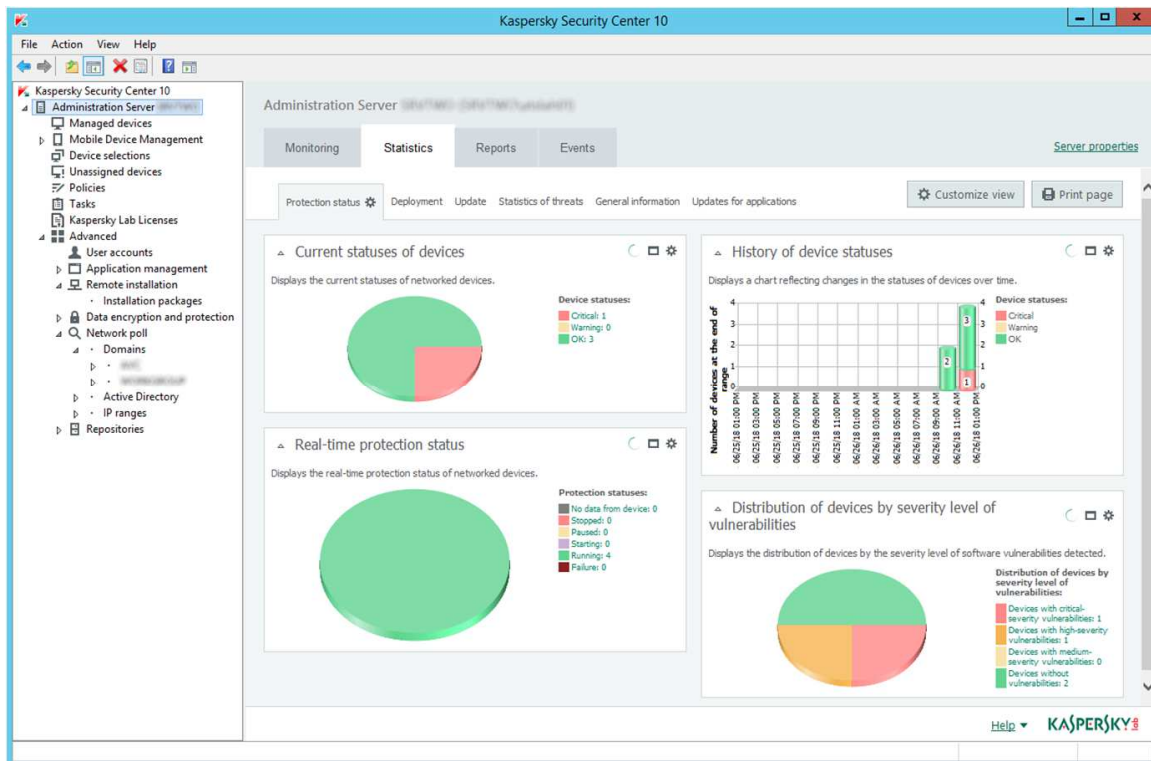


Under default settings, users have access to a fairly standard-looking endpoint client window with a component status display. This lets users run definition updates and a wide variety of scans. However, no settings are accessible. Admins can increase or decrease GUI functionality by means of policy. The endpoint software includes K7's own firewall, which replaces the Windows Firewall. As with the malware protection, users have no access to its settings.

Kaspersky Endpoint Security for Business Select



THE SCREENSHOT ABOVE SHOWS THE WEB-BASED MANAGEMENT CONSOLE; THE SCREENSHOT BELOW IS THE MMC-BASED MANAGEMENT CONSOLE



Verdict

Kaspersky Endpoint Security for Business Select is a strong product aimed at medium-sized and enterprise businesses. There is very good cross-platform support, and a dual interface.

About the product

Kaspersky Endpoint Security for Business Select uses server-based management functionality. It supports management of endpoint security clients for Windows, Mac, and Linux desktops, Windows and Linux servers, plus Android and iOS mobile devices. A dual management interface is provided: you can use a web-based console (upper screenshot on the page above), or an MMC-based console (lower screenshot on the page above). In this review, we have described the MMC-based version of Kaspersky Security Center. We hope to review the web-based console in the second Business Report of 2019.

Getting up and running

Installing the management console is a straightforward process for an experienced administrator. An SQL database is required. If this has not already been set up, the admin can download the free Microsoft SQL Server Express, Microsoft SQL Server or MySQL from links provided in the setup wizard. When installation is complete, the Protection Deployment Wizard starts. This automatically discovers network clients and servers, and lets you install them by remote push. It is simple to use. You can discover desktops and servers using their IP subnet, Microsoft Active Directory membership, domain names and Amazon AWS API.

The wizard can be rerun by clicking *Advanced\Remote Installation* in the console tree to add new devices at a later stage. Kaspersky Security Center additionally offers an auto-deployment policy. This means that when devices are discovered and placed into a managed group, the appropriate endpoint protection software will be installed automatically. You can also create an installation package, which you can distribute via web link, network share or USB device, for individual installations. The home page of the console (Kaspersky Security Center 11) is subtitled *Getting started: devices, tasks, policies and reports. Interface configuration*. It provides a comprehensive range of instructions and descriptions to help the admin with everyday tasks. These include *How to find your devices*, *Where to view a list of all tasks*, and *Where to view summary information about Administration Server operation*.

Everyday management

Kaspersky make use of the Microsoft Management Console framework for the administration interface. This will be familiar to anyone with experience of Windows administration, and makes navigation very simple. Daily operational tasks are carried out using the *Administration Server\Statistics, Managed Devices, Device Selections, Policies, Tasks* and *User Accounts* items in the console tree.

Administration Server/Statistics tab shows a clear overview of network security using pie charts, with a traffic-light colour-coding scheme for *OK, Critical* and *Warning* states. This is shown in the screenshot above. You can customise the page to show different items or change the chart style.

Managed Devices shows a list of the computers on the network, along with status and device information. There are very useful customisation options here. The admin can add and sort columns such as operating system and architecture, real-time protection status, IP address, last update, and malware detected.

Device Selections uses a simple report-like function to search for computers that need attention. The feature is extremely easy to use. There is a list of properties that you might want to search for, such as *Devices with Critical status* and *Many viruses detected*. To run a search, just click on the relevant criterion and then *Run Selection*. The results are shown in a separate *Selection Results* tab.

Reporting options can be found under *Administration Server\Reports*.

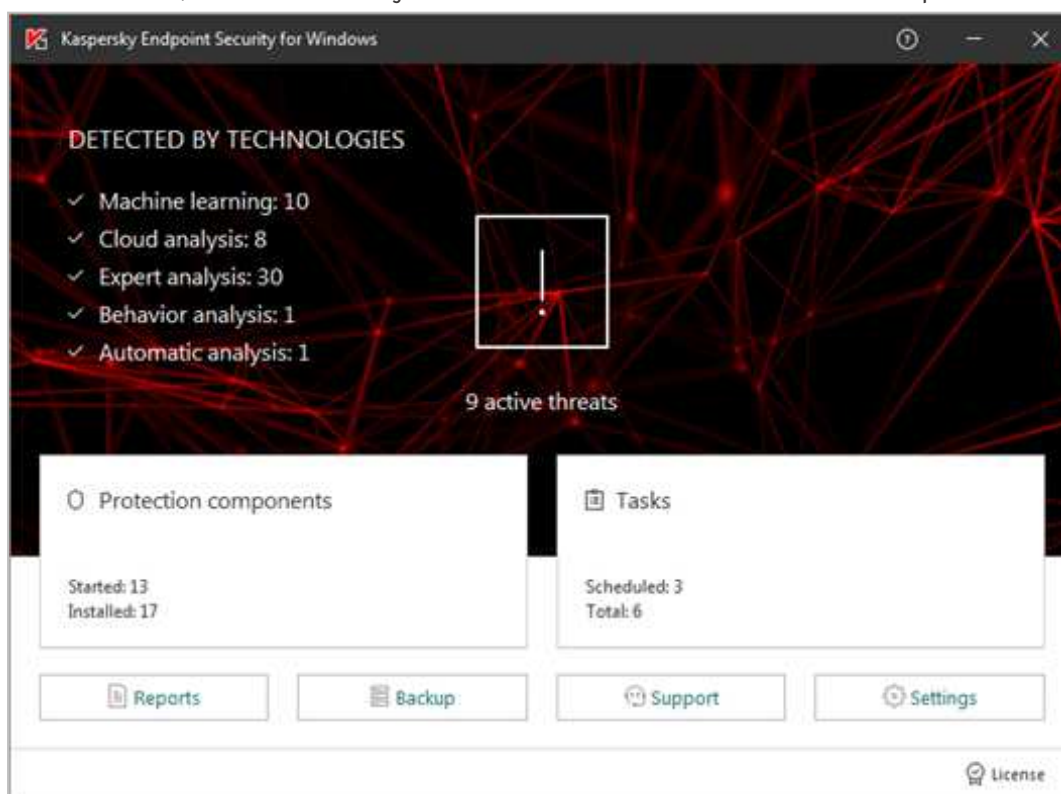
The *Policies* page lets the admin view, create and edit configuration policies for network computers. There are separate policies for the network agent and the endpoint protection software. Again, this is a very straightforward feature to use.

Tasks displays a list of tasks that have already been run. You can also create new ones, or import them from a file. There is a clear and manageable list of jobs such as remote application installation, update, virus scan, and send message to user.

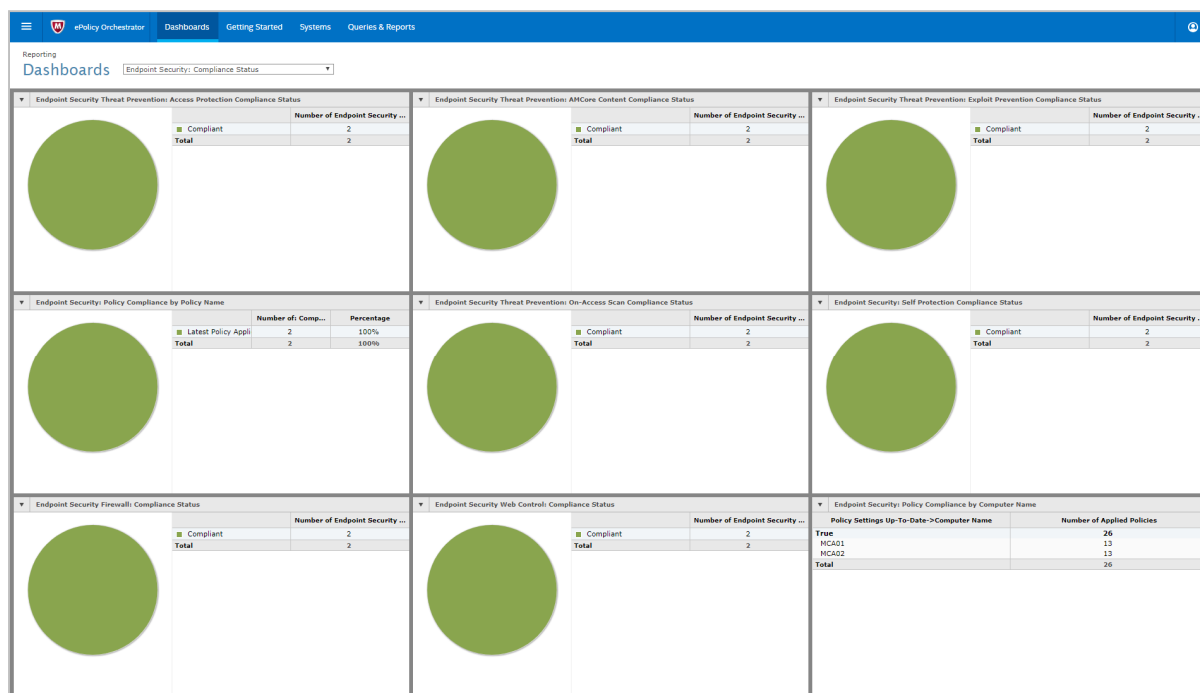
User Accounts in the *Advanced* section of the console tree shows a complete list of all Windows users on the network. Here you can add users and groups, and run a report of users of the most infected devices.

Windows endpoint protection software

The product's philosophy is that the endpoint software should be managed by the IT staff, rather than the end user. The program window is essentially a comprehensive status display. It shows security status and detection statistics for the different technologies involved, such as machine learning. Although there is a *Settings* button, by default the configuration is locked. However, users can run scans of drives, folders or files by means of the context menu in Windows Explorer.



McAfee Endpoint Security with ATP and ePolicy Orchestrator Cloud



Verdict

McAfee’s ePolicy Orchestrator Cloud is undoubtedly powerful, and as part of a wider McAfee managed platform it offers a lot. However, the management of the ePolicy Orchestrator Cloud console requires some training. We felt that the range of functionality within the product means that items required for day-to-day AV management are not as easy to find as in less-sophisticated products. However, it is a product which will reward the initial learning phase with easier management procedures later on.

About the product

This is a cloud-based management console with desktop AV package. Endpoint Security is a client that runs on the desktop, with clients provided for macOS and Windows. There is a web-based console called ePolicy Orchestrator Cloud. The cloud-based product is aimed at businesses of up to 10,000 users. There are clients for Windows clients and servers, and macOS. A generous 60-day trial period is provided, so you can evaluate the product at length before purchasing.

Getting up and running

Access to the web portal is straightforward via a standard username/password login combination. The user interface is quite modular, depending on your current task. Across the top is a dropdown menu. Then there are main menu items of *Dashboards*, *Getting Started*, *Systems*, and *Queries & Reports*. The best place to start is at the *Getting Started* menu. Here you get a very simple page where you can download the installation client package for the platform which you are currently running. Running the endpoint protection setup package is quick and easy. Initially, just the agent itself is installed. The selected protection components are then downloaded and installed automatically over a time period of 20 minutes or so.

Everyday management

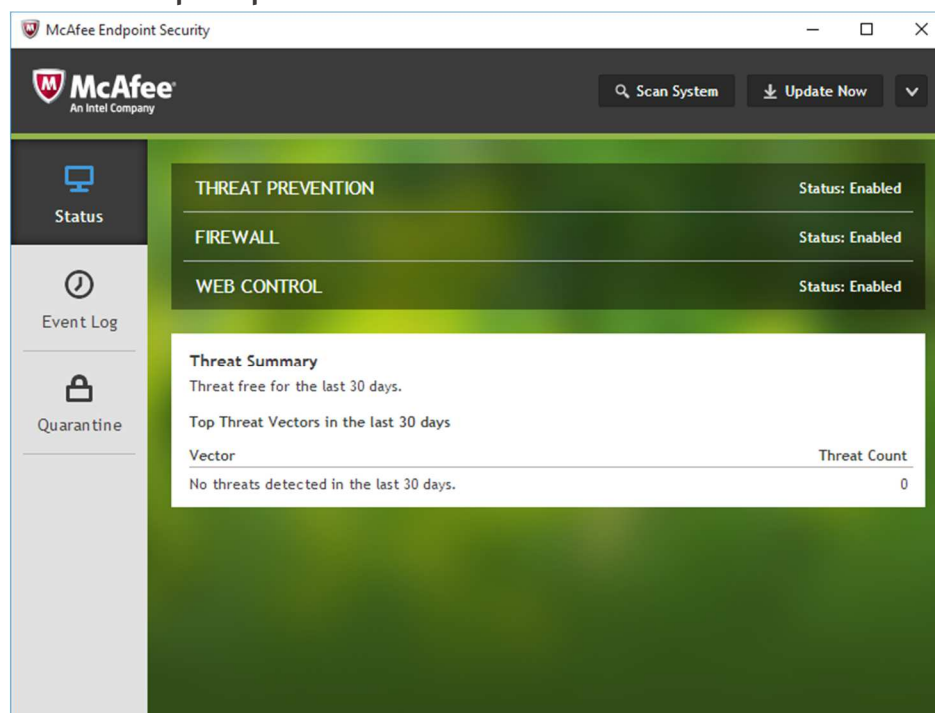
The web console is usefully split into several main working areas. The default *Dashboards* page offers a wide range of reports and views, covering areas such a *Compliance Status*, *Protection Summary*, *Web Control Activity* and so forth. The *Systems* tab lists all installations together with their status and last communication timestamp.

We found one aspect of the GUI to be unclear here. All of the date/time stamps in the management console appear to be on Mountain Time zone, because the headquarters for McAfee's datacentre is apparently in Denver, Colorado. We feel it is far from obvious to the first-time user how to change the time zone to a local one.

The *Dashboards* tab has a wide range of reports and views available, and each of them allows you to click through to more data. We found this functionality to be useable, although not quite as intuitive as we would have liked.

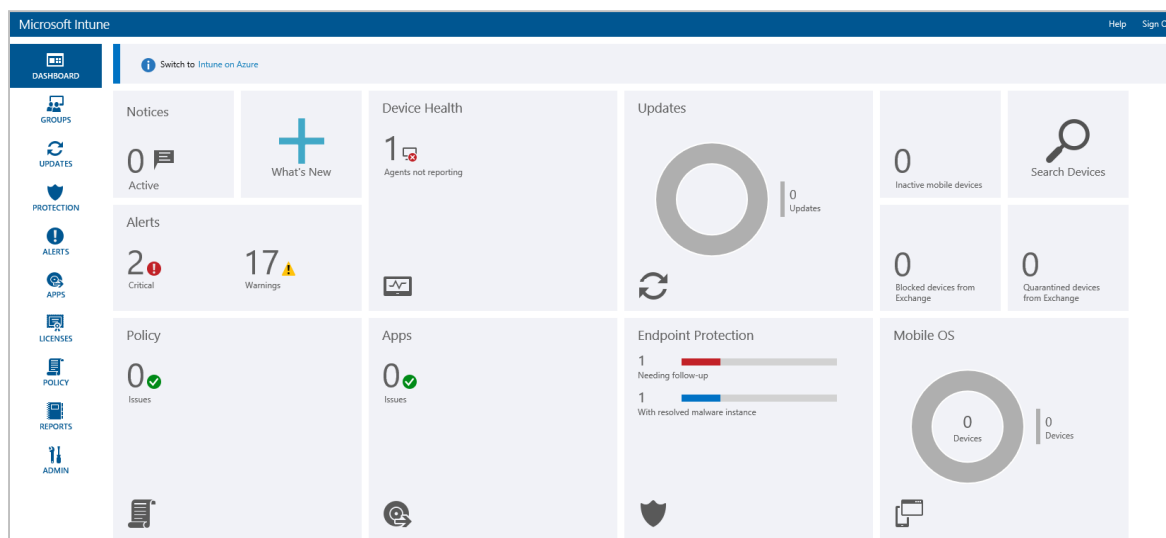
It should be noted that in general, ePO Cloud becomes easier to use the more you become familiar with it. Admins using ePO Cloud for the first time should bear in mind that time spent learning about how it works will pay dividends later on. There are a number of ways that daily tasks can be made easier by automatization. You can also customize the interface, e.g. by adding commonly used functions to the quick-links bar at the top.

Windows endpoint protection software



The main desktop client window is quite clear and clean, offering scanning, updating, and showing the status of each component. Most other controls – such as the event logs and quarantine – are disabled by default for standard users. However, the admin has fine-grained control of this from the console, so any or all of the controls can be enabled or disabled as desired. There is an icon in the System Tray area. Clicking on this offers Update Security, the main app window, Show security status, the Status monitor, and an info page.

Microsoft Windows Defender Antivirus for Business with Intune



Verdict

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

About the product

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

Getting up and running

As the management console is cloud based, no installation is necessary. A management agent has to be deployed to the clients to enable them to be monitored and controlled from the console. This is easily found under Admin/Client Software Download, and can be installed manually on the client with just a couple of clicks. For larger networks, the admin can use Group Policy to deploy the software automatically.

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

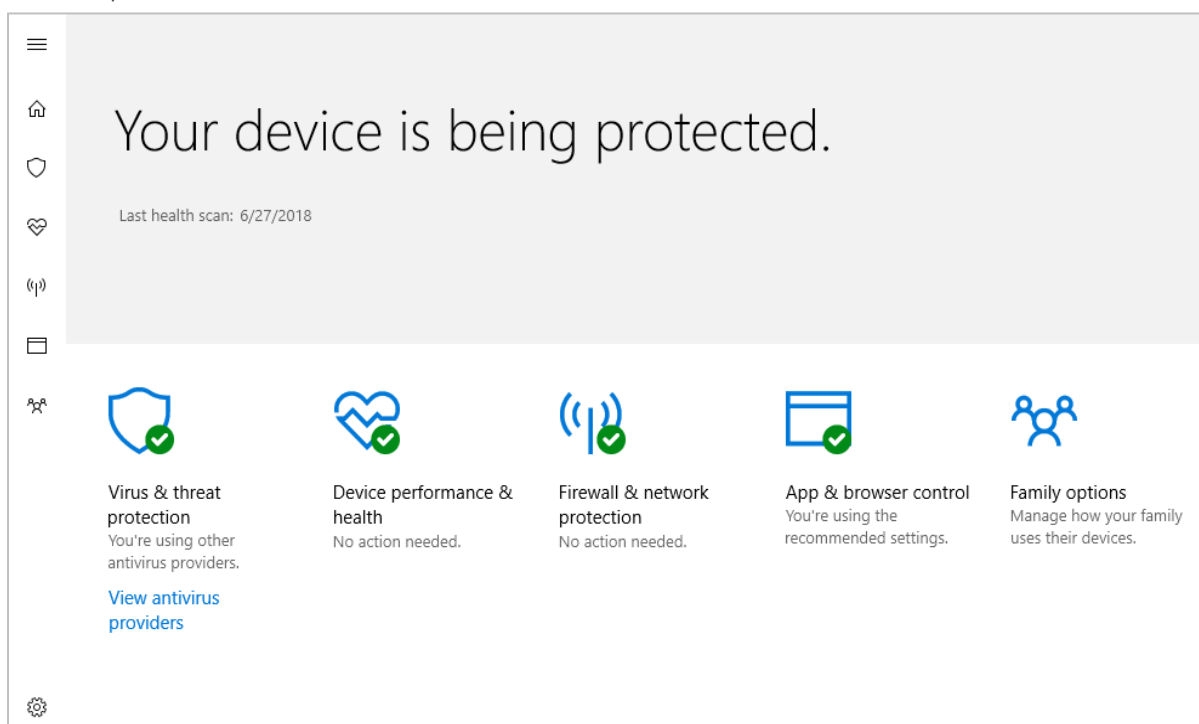
Everyday management

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

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

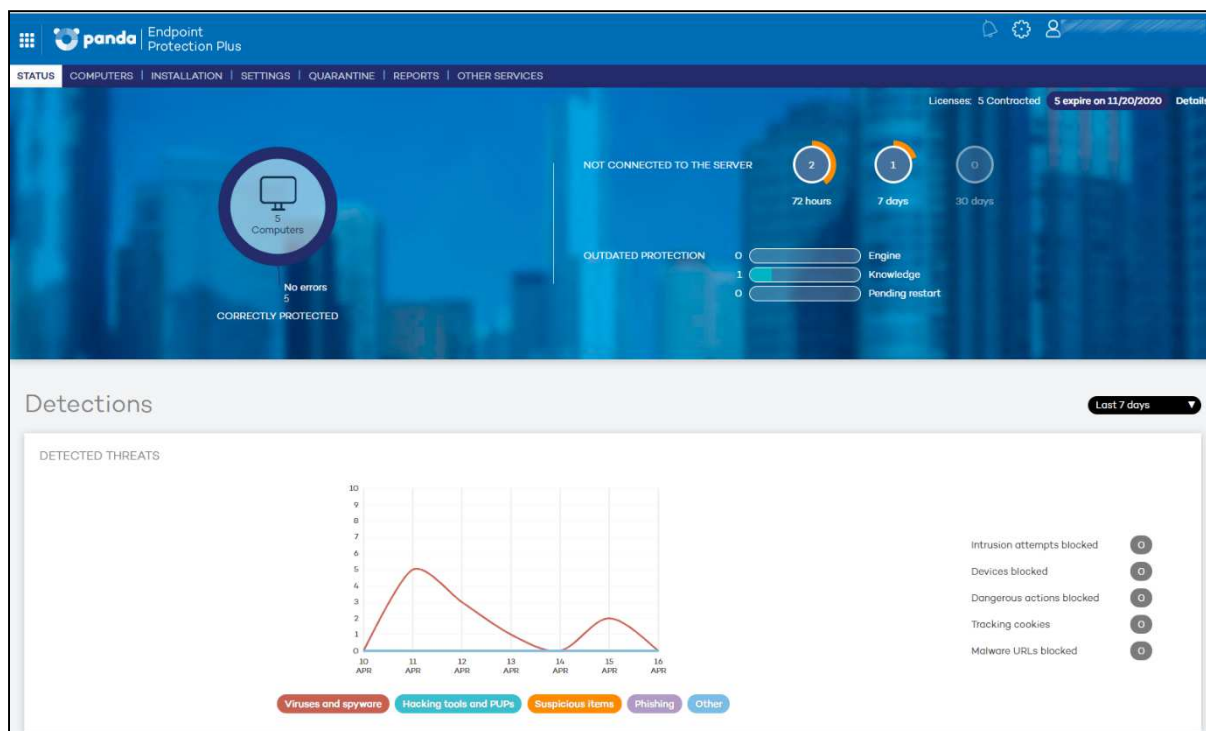
Endpoint protection software

The precise nature of the client protection software GUI is dependent on the version of Windows installed on the PC. Up-to-date Windows 10 clients have the Windows Defender Security Center interface, shown below:



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

Panda Endpoint Protection Plus on Aether



Verdict

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

About the product

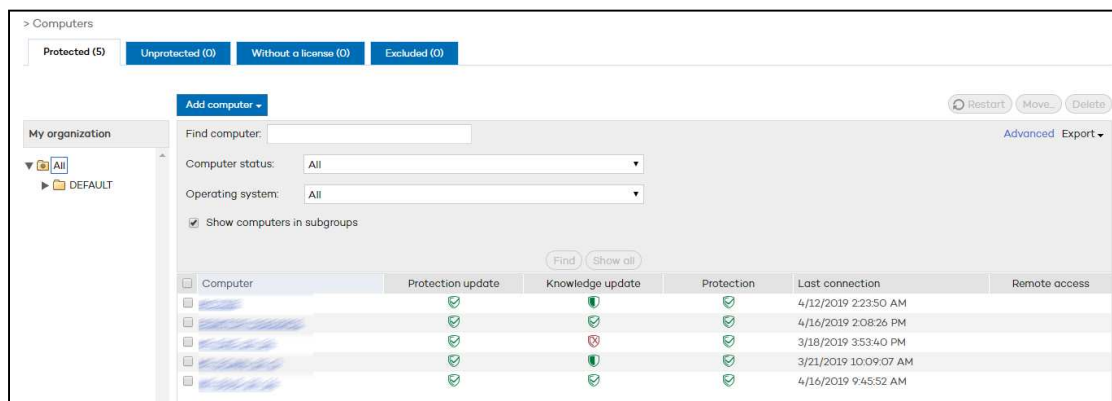
This is a cloud-console managed system with device clients for Windows servers, Windows/Linux PCs, and Android mobile devices. The desktop client software has a simple interface, which allows users to run updates and various scans. It is suitable for organisations of all sizes.

Getting up and running

The product is managed from a cloud-based console, which requires no installation. Deployment is carried out from the *Installation* page. A single click on *Send by email* opens an email message with a link for download and installation. This works for Windows, Linux and Android. The user clicks on the provided link to install the client, and this is then automatically licensed. Alternatively, you can download an installer file directly from the console. This can then be installed locally, or distributed by network share or removable device. Once a client device has connected to the management console, you can allocate it to a management group. This can be done manually, by IP address range or by Active Directory integration, and obviously helps with a multi-site organisation or one which might be split by IP address/VLAN into teams (sales, accounts etc.).

Everyday management

Protection status and threat detection history are provided on the *Status* page, which opens by default. There are excellent graphics for detected threats, including malware types, detection origin, and blocked URLs here. This provides a solid daily overview of issues. We particularly like it because it provides a headline view of the status, but allows you to click through for more detailed information. For example, clicking on the main *Protection Status* graphic takes you to the *Computers* page, shown below.



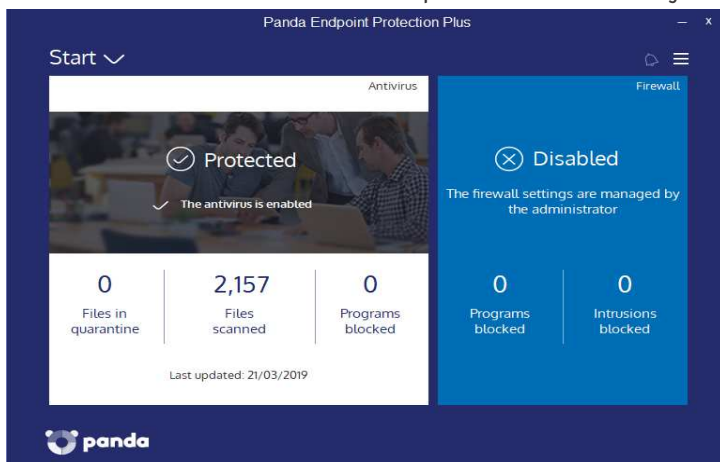
This page shows all the protected computers and mobile devices. It is very clearly laid out, and shows three status categories – *Protection Update*, *Knowledge Update* and *Protection*– as simple colour-coded icons. A Windows-like folder tree on the left lets you show devices by group.

The *Reports* page generates overview reports that can be emailed out on a daily, weekly or monthly routine. You can specify all computers or specific groups, and include *License Status* in addition to the default *Protection Status* and *Detections*.

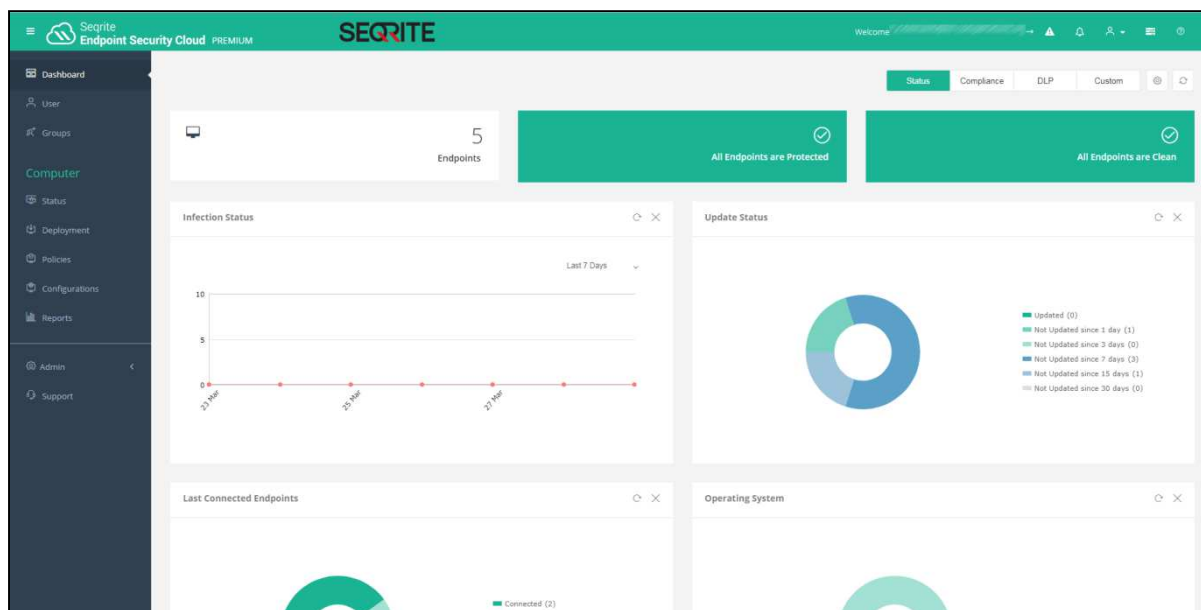
Using the *Settings* tab, you can see the default configuration policies, and also create new ones. As you would expect, you can find quarantined items on the *Quarantine* page. *Other Services* includes a link to the support pages on the vendor's website.

Windows endpoint protection software

On the Windows client itself, there is a clean and clear application. It allows access to solid end-user capabilities like Full Scan, Critical Areas Scan and Custom Scan. The user can force a synchronisation of the updates here too. However, there is no access to any settings. This is a useful, clear and obvious tool which should be within the capabilities of most any user.



Seqrite Endpoint Security Cloud



Verdict

Seqrite Endpoint Security Cloud provides an easy-to-navigate cloud console and a choice of straightforward deployment methods. This makes it simple to use for small businesses, but there is enough functionality for larger enterprises too. It would be a good choice for small companies with plans to expand.

About the product

Seqrite Endpoint Security Cloud provides endpoint protection for Windows, macOS and Linux clients, and Windows servers. Additional features include data-loss prevention and asset management. As the name implies, the management console is cloud-based, and hence allows the service to be accessible from the cloud using any modern browser.

Getting up and running

No setup is required for the console, as it is cloud based. You just browse to the URL and log in. Three options are provided for deploying the endpoint protection software to clients. All of these are conveniently accessible from the same page. You can download an installer package from the console, and run it on client PCs. Alternatively, you can send an installer link to users by email, directly from the console. The third option is to download and run a remote installer package, to deploy the software to clients on the LAN.

Everyday management

All the main functionality of the console is found in a single menu panel on the left-hand side. This can be expanded to show the text of the menu items, or collapsed so show just the icons. The console opens on the *Dashboard* page. This provides an at-a-glance overview of the system security status. Panels at the top show the total number of endpoints on the network, and how many of these are protected and infection-free. Other panels use line or doughnut charts to show infections status, updated status, last connection time of endpoints, and OS distribution.

You can move or delete individual panels to make your own customised dashboard. Clicking on a section of one of the charts (e.g. recently connected endpoints) conveniently displays a details panel for that item.

Columns		Q Filter by		Endpoint Name Search		
<input type="checkbox"/>	Endpoint Name	IP Address	Domain Name	Policy	Virus DB Date (GMT+5:30)	Last Connected
<input type="checkbox"/>	[icon] [blurred]	[blurred]	WORKGROUP	Default_MSSP	14 Mar 2019 [16:50:33]	18 Mar 2019 [21:49:22]
<input type="checkbox"/>	[icon] [blurred]	[blurred]	WORKGROUP	Default_MSSP	20 Mar 2019 [12:43:06]	21 Mar 2019 [16:22:02]
<input type="checkbox"/>	[icon] [blurred]	[blurred]	WORKGROUP	Default_MSSP	28 Mar 2019 [16:49:13]	29 Mar 2019 [18:03:35]
<input type="checkbox"/>	[icon] [blurred]	[blurred]		Default_MSSP	13 Nov 2018 [10:07:00]	29 Mar 2019 [18:17:16]
<input type="checkbox"/>	[icon] [blurred]	[blurred]	WORKGROUP	Default_MSSP	18 Mar 2019 [11:45:20]	29 Mar 2019 [08:30:44]
<input type="checkbox"/>	[icon] [blurred]	[blurred]	WORKGROUP	Default_MSSP	11 Mar 2019 [10:27:52]	12 Mar 2019 [07:13:57]

Under the *Computer* heading, (shown above) *Status* lists individual devices and shows key information such as the policy applied, update status and last connection time. You can easily carry out tasks from this page, by selecting computers and then using the *Client Actions* menu to run scans and updates etc.

On the *Deployment* page, you can download preconfigured installers for the different supported operating systems/architectures. You can also create your own customised installers or use the email/remote install options on the same page.

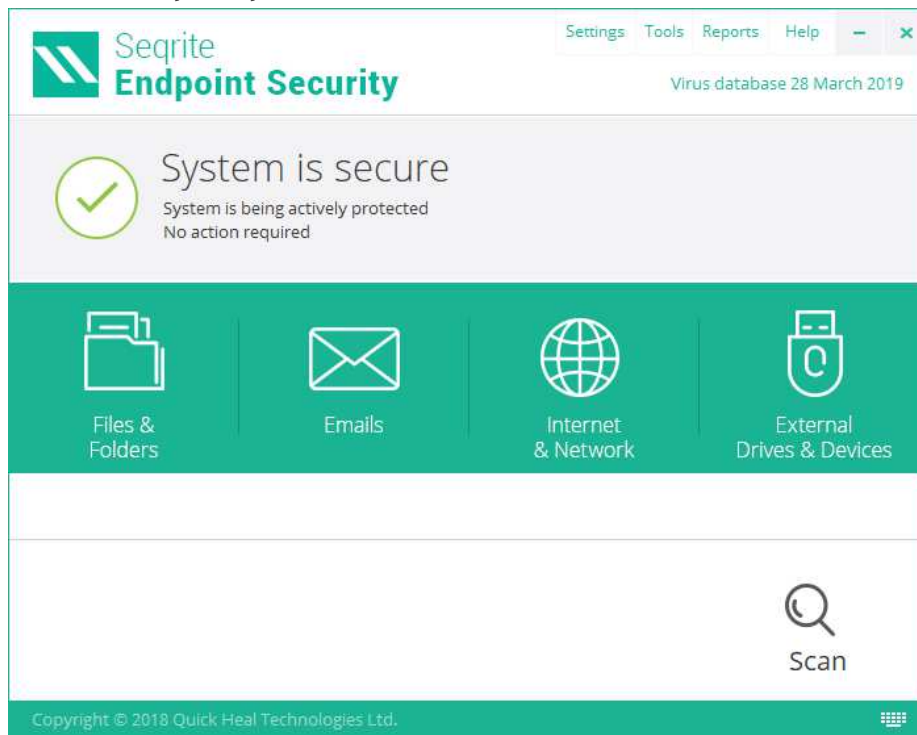
Policies lets you see existing policies and the devices that apply them. You can also see the details of each policy, and duplicate any policy as a basis for customisation.

Under *Configurations*, there are options for the device control and application control features. You can also specify the installation path for Windows clients.

Reports provides a number of preconfigured reports, such as *Virus Scan*, *Web Security* and *Firewall*. You can also create your own custom report from scratch.

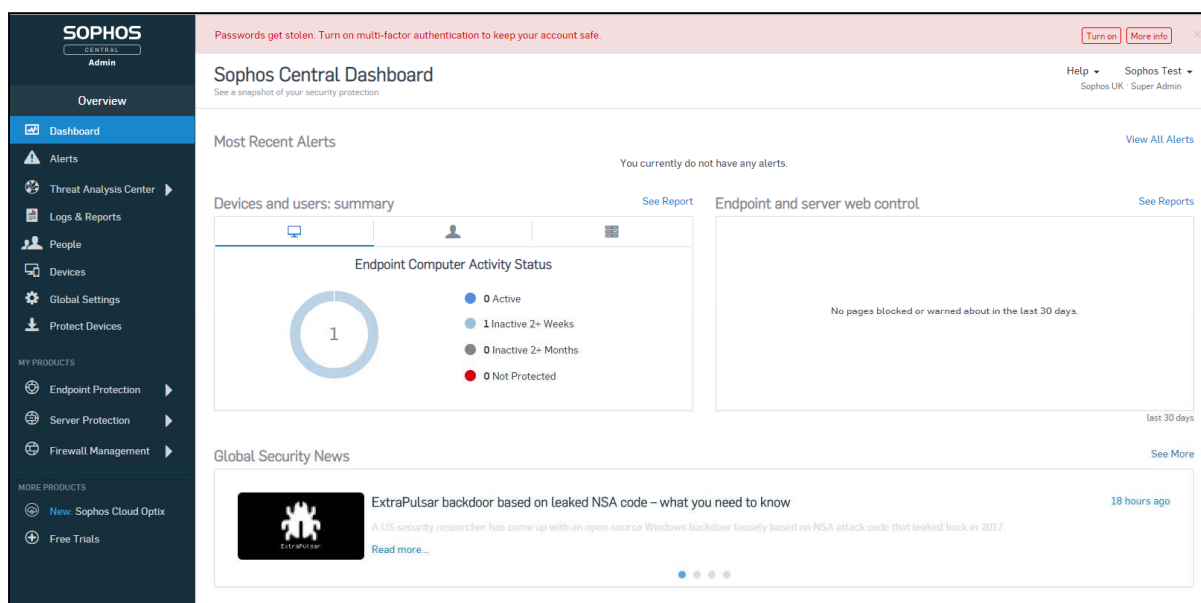
The *Admin* section covers things like licences, console users and notifications.

Windows endpoint protection software



Seqrite Endpoint Security has a fully-featured Windows endpoint protection client, with the same functionality and GUI as a typical consumer antivirus program. The design is clear and modern, with a single row of tiles for major functions. Users can run full, custom, memory and boot-time scans. However, standard users are not able to change any of the program's settings.

Sophos Intercept X Advanced



About the product

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

Verdict

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

Getting up and running

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

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

Everyday management

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

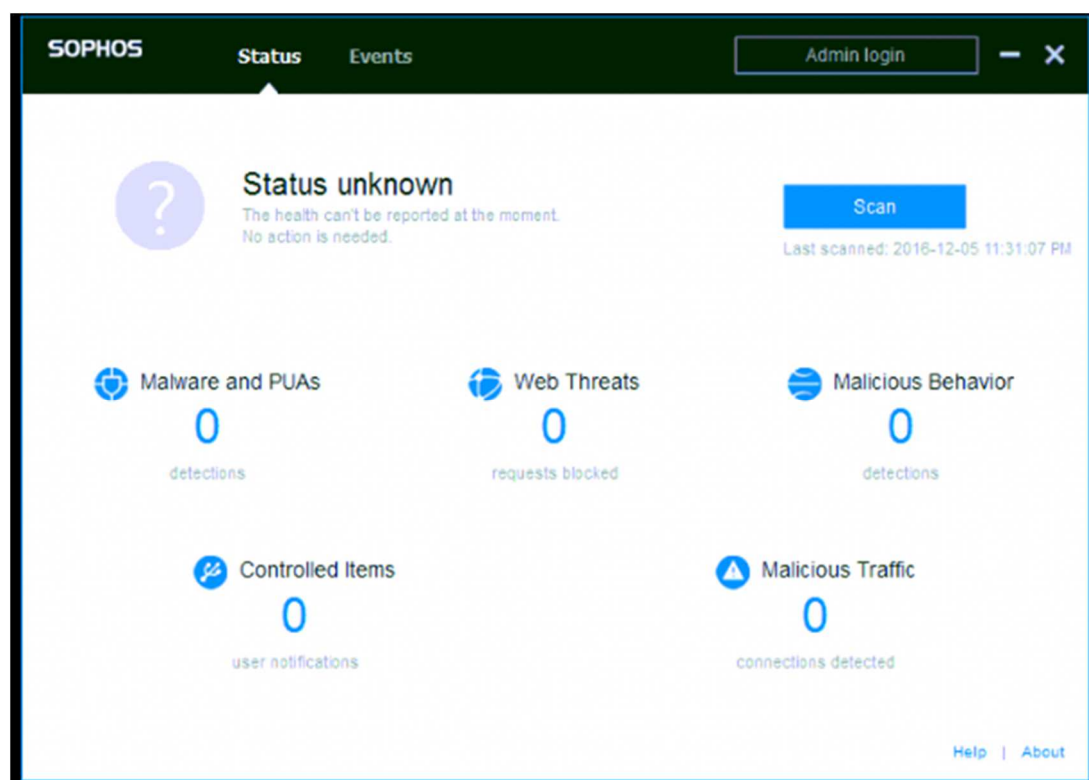
The *Alerts* item gives you a list of all the alerts which have occurred. You can sort by *Description*, *Count* and *Actions*.

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

People (computer users), *Devices* and *Global Settings* do what you would expect.

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

Windows Endpoint Protection Software



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

SparkCognition DeepArmor Endpoint Protection Platform



Verdict

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

About the product

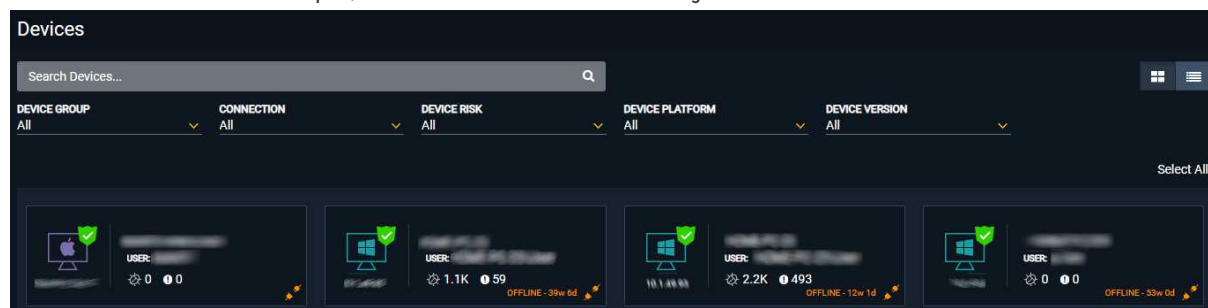
SparkCognition uses a cloud-based console to manage endpoint protection for Windows, Mac and Linux systems.

Getting up and running

The console does not require any installation, as it is cloud-based. Deployment of endpoint protection software is essentially the same for all operating system types. The appropriate installer can be obtained from the *Downloads* page of the console, and run on the respective client device. This is a very straightforward process. For Windows clients, installation by System Centre Configuration Manager or PowerShell command line is also possible.

Everyday management

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



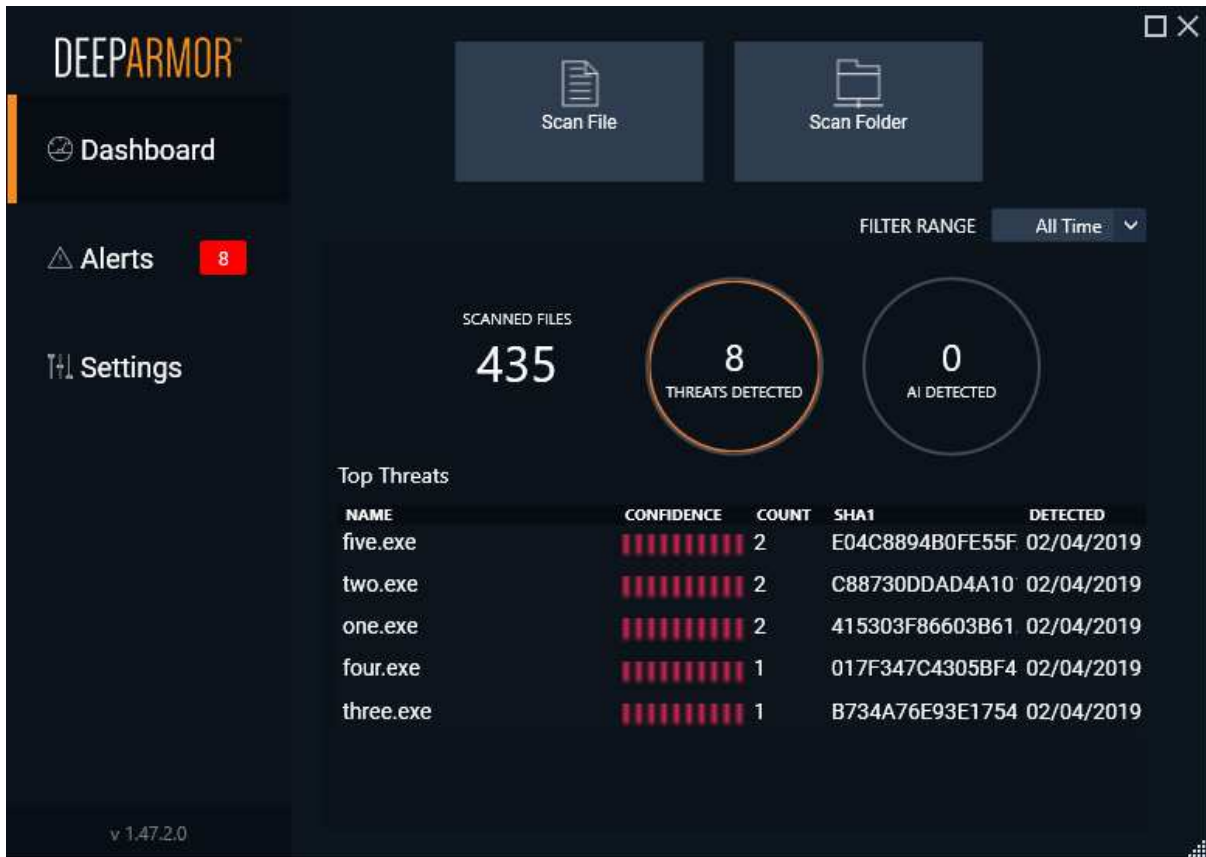
On the *Devices* page, you can see individual computers on your network. These can be displayed as tiles, as shown above, or as a simple list. By selecting a device or devices, you can run scans, change group membership, or remove from the console. It is possible to filter the devices displayed by using drop-down lists at the top of the page. You can filter by device group, connection, device risk, device platform or device version.

The *Alerts* page shows recent alerts, along with details of the file name of the malware, how it was detected, detection name, “confidence” (probability that the file really is malicious), name of affected device, time of detection, action taken or required, and file hash. Sub-tabs of each file’s details page show all detections of the file across the network (*Occurrences*), and further details of the file, including certificate information, file metadata, and PE imports (*Static file analysis*). The *Take Action* button provides the options *Remote Remediate*, *Remote Restore*, and *External Remediate*, allowing the admin to take immediate action.

The *Administration* menu includes the submenus *Users*, *Device Policies*, *Device Groups*, *Global lists*, *Audit logs* and *Reporting*. *Users* lets you add, edit and remove console administrators, who can be assigned varying levels of access (*Admin*, *Manager* or *Auditor*). Under *Device Policies* you can assign preconfigured settings to individual devices or groups. The latter can be managed from the *Device Groups* page. *Device Policies* also lets you define whitelisted folders, i.e. ones that will be excluded from malware protection. You can further create whitelists of files and certificates, and file blacklists, under *Global Lists*. A list of admin logins and logouts can be found under *Audit Logs*. The *Reporting* page lets you create reports for specific groups or all devices. You can choose the time period covered by the report, and who will receive it.

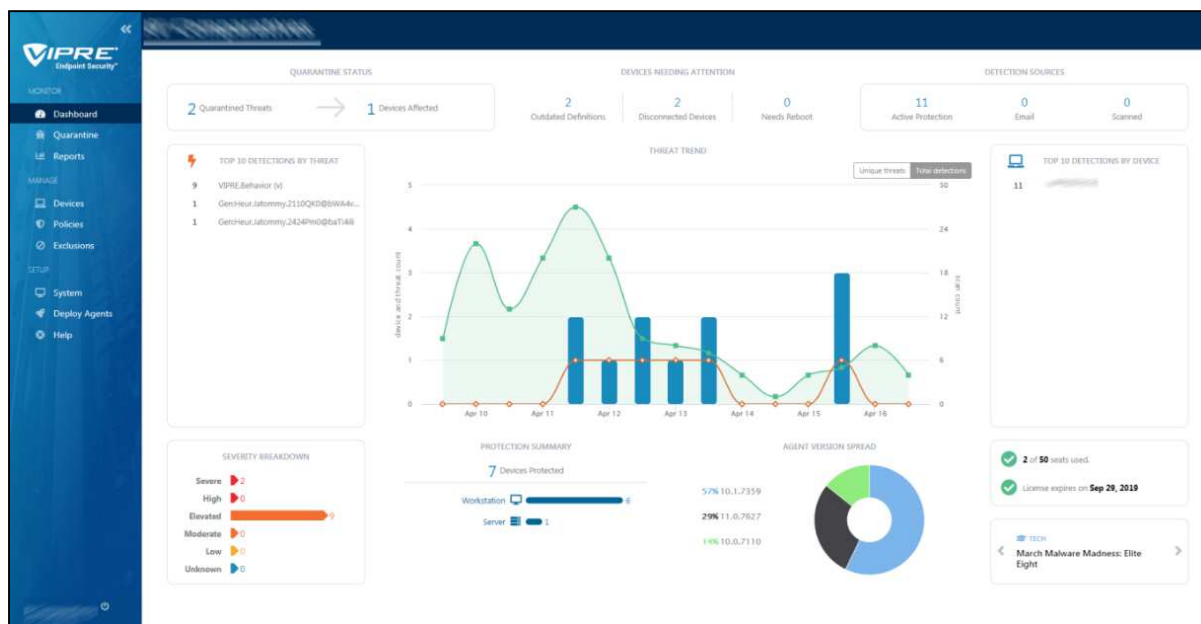
On the *Downloads* page you can find installers for Window, macOS, and various different Linux distributions. Finally, *Support* links to the support page on the vendor’s website.

Windows endpoint protection software



The endpoint protection client has a GUI that allows users to scan individual files and folders. The home page lists the most recent threats discovered, while a more comprehensive list can be seen on the Alerts page. The Settings page has controls for various configuration options for the program, but by default these are deactivated for all users.

VIPRE Endpoint Security Cloud



Verdict

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

About the product

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

Getting up and running

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

Everyday management

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

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

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

HOSTNAME	STATUS	POLICY	TYPE	OS	LAST SEEN	LAST INFECTED	AGENT
[Redacted]	Protected	Default Enterprise	Workstation	Windows 10	4 days ago	Never	11.0.7627
[Redacted]	Shutdown	Default Enterprise	Workstation	Windows 10	a month ago	Never	10.1.7359
[Redacted]	Scanning Files	Default Enterprise	Workstation	Windows 10	a month ago	a month ago	10.1.7359
[Redacted]	Shutdown	Default Enterprise	Workstation	Windows 10	2 months ago	Never	10.1.7359
[Redacted]	Protected	Default Enterprise	Workstation	Windows 10	a month ago	a month ago	10.1.7359
[Redacted]	Shutdown	Default Windows Servers	Server	Windows Server 2016	2 years ago	2 years ago	10.0.7110
[Redacted]	Protected	Default Enterprise	Workstation	Windows 10	an hour ago	a day ago	11.0.7627

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

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

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

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

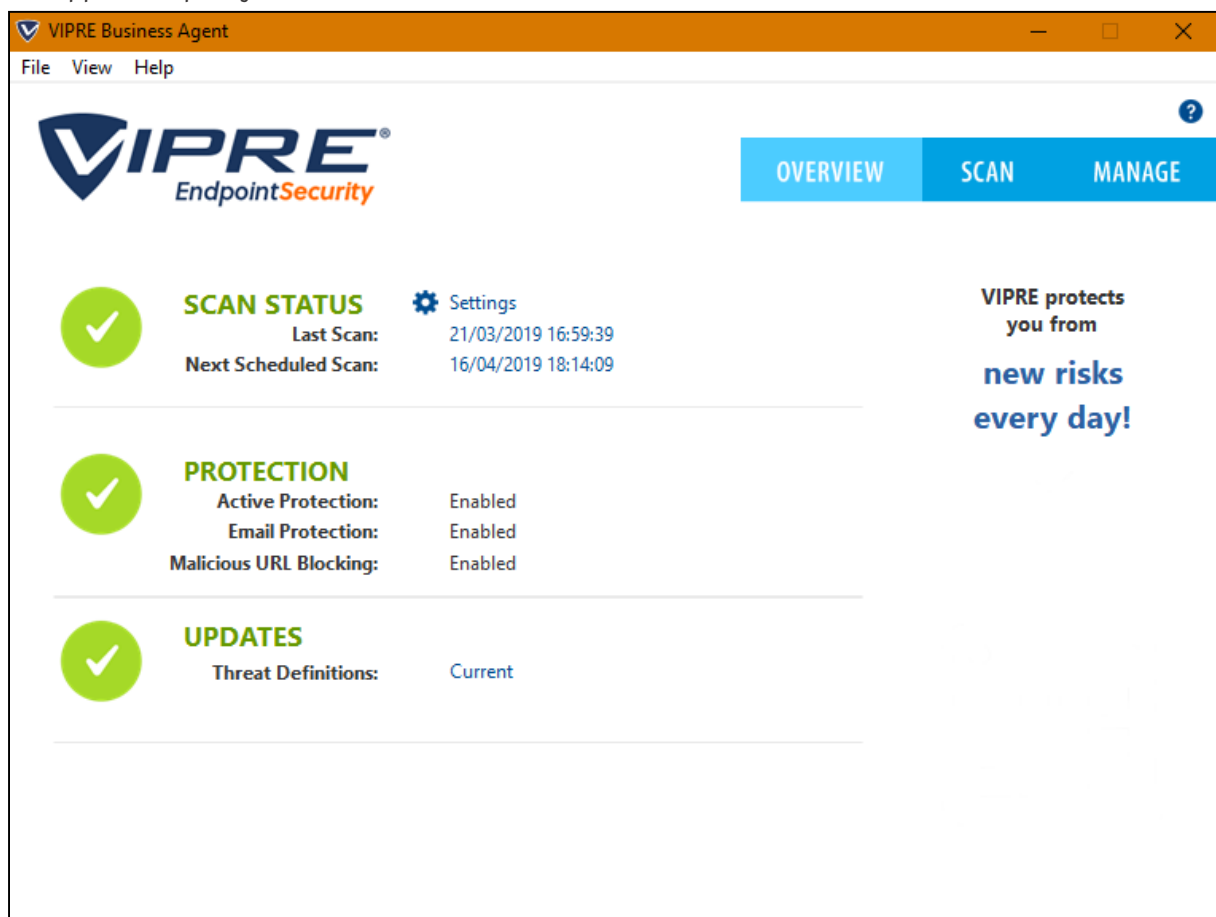
The web console impresses both from the initial setup and deployment through to the ongoing management. The defaults are sensible, the screens clear and clean, and it is obvious what it is reporting and how healthy the clients are. It is simple to get clients to do centrally managed tasks, and the configuration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

It is simple to create ongoing reports, and you don't need to specify a mail server to send it through – this is provided for you.

We would say the platform is appropriate for any size of company, from a small business with a few seats, through to a much larger organisation. The UI of the management console was always responsive under testing. It is built to cope with thousands of desktops and large numbers of events.

Windows endpoint protection software

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



Features (as of June 2019)	Avast Business Antivirus Pro Plus	Bitdefender Endpoint Security Elite (GravityZone Elite HD)	Cisco AMP for Endpoints	CrowdStrike Endpoint Protection Platform Standard Bundle	Endgame Protection Platform	ESET Endpoint Protection Advanced Cloud & ESET Cloud Administrator	FireEye Endpoint Security	FortiClient with EMS & FortiSandbox	K7 Enterprise Security	Kaspersky Endpoint Security for Business Select	McAfee Endpoint Security with ePO & ATP	Microsoft Defender ATP's Antivirus with Intune	Panda Endpoint Protection Plus on Aether	Seqrte Endpoint Security	Sophos Intercept X Advanced	SparkCognition DeepArmor Endpoint Protection Platform	VIPRE Endpoint Security Cloud
Available Console Types																	
Cloud-based console	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*
On-premise server-based console	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*
Virtual appliance	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*
Client software deployment methods																	
Creation of .exe or .msi installer package	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*
Email a link to remote users to install the software themselves	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*
Push installation from the console	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*
Supported Operating Systems																	
Microsoft Windows	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*
Virtual environments (such as VMware, HyperV)	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*
Apple macOS	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*
Linux	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*
Google Android	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*
Apple iOS	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*
Windows Features																	
Anti-Malware	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*
Detection notifications are shown on the client	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*
Web access control / webfilter (custom blacklisting of URLs / site categories)	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*
Phishing protection (blocking of phishing URLs)	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*
Firewall	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*
Anti-Spam	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*
Data or Email encryption	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*
Data backup	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*
Settings & Uninstall protection	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*
Cross-platform central management	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*
Registers as AV product in Windows Security Center	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*
Protection settings are enabled by default (out-of-the-box-protection)	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*
Right-click on-demand scan of files/folders	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*
Can clean-up a previously infected system (incl. registry leftovers and inactive malware)	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*
Splunk support	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*
The online malware detection rate is the same as offline	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*
EDR (Endpoint Detection and Response)	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*
Scans files only on execution	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*
Languages																	
Which languages can be used to contact support?	English, Czech, Japanese, French, German, Portuguese, Norwegian	English, Spanish, German, Romanian, French	All	All	All	All	English, Japanese, French, Italian, Spanish, Portuguese, Arabic, Turkish, Hebrew	English, French, German, Japanese, Chinese	English, Hindi	English, German, Dutch, French, Czech, Hebrew, Danish, Finnish, Italian, Norwegian, Portuguese, Romanian, Spanish, Swedish, Polish, Russian, Turkish, Arabic, Chinese, Japanese, Korean, Hindi, Malay	English, Chinese, Czech, Danish, Dutch, Finnish, French, German, Italian, Japanese, Korean, Norwegian, Polish, Portuguese, Spanish	All	All	English	English, Italian, German, Spanish, French, Japanese	English, Swedish, Danish	
Which interface languages is the product available in?	English, Spanish, French, German, Italian, Portuguese, Russian, Norwegian, Dutch, Bulgarian, Chinese, Czech, Estonian, Finnish, Greek, Hungarian, Japanese, Korean, Polish, Slovak, Slovenian, Swedish, Turkish, Ukrainian, Vietnamese	English, Spanish, German, Romanian, French, Italian, Portuguese, Polish, Russian	English, Japanese, Korean, Chinese	English	English	English, German, Spanish, Greek, Turkish, French, Russian, Polish, Italian, Japanese, Chinese, Arabic, Slovak, Czech, Croatian, Korean	English	English, Chinese, French, German, Japanese, Korean, Portuguese, Spanish	English	English, Arabic, Polish, Korean, Italian, German, French, Chinese, Turkish, Spanish, Russian, Romanian, Portuguese, Dutch, Polish, Hungarian, Vietnamese, Czech, Japan, Kazakh	English, Chinese, Czech, Danish, Dutch, Finnish, French, Hebrew, German, Italian, Japanese, Korean, Norwegian, Polish, Portuguese, Russian, Spanish, Swedish, Turkish	English, French, Dutch, Portuguese, Czech, Danish, German, Spanish, Italian, Norwegian, Polish, Russian, Finnish, Swedish, Turkish, Chinese, Japanese, Korean, Arabic, Hebrew	English, Spanish, French, Italian, Portuguese, Swedish, German, Hungarian, Russian, Polish, Chinese, Japanese, Finnish	English, Japanese	English, German, French, Japanese, Italian, Chinese, Spanish, Portuguese, Korean	English, Spanish	English
Which languages are the manuals available in?	English, Czech						English	English	English	English, Arabic, Bulgarian, Chinese, Croatian, Czech, Danish, Dutch, Estonian, Finnish, French, German, Greek, Hebrew, Hungarian, Italian, Japanese, Korean, Latvian, Lithuanian, Norwegian, Polish, Portuguese, Romanian, Russian, Serbian, Slovak, Slovenian, Spanish, Swedish, Thai, Turkish, Ukrainian		English, Spanish					
Pricing (approximate LIST PRICES as of June 2019; depending on the number of agents purchased, deal size or term, country/region, volume and competitive upgrade discounts will apply/vary)																	
1,000 clients - 3 years, \$ US / € DE																	
Cloud-based console		\$ 68700 / 52500 €	\$ 100800 / 100800 €	\$ 185900 / 166300 €		N/A		N/A	\$ 32900 / 32900 €	\$ 43700 / 40000 €	\$ 45900 / 45900 €	\$ 216000 / 183600 €	\$ 42000 / 42000 €				
On-premise Windows-based console	\$ 43200 / 36300 €	N/A	\$ 506400 / 506400 €		\$ 72900 / 72900 €	\$ 38000 / 31600 €	\$ 93000 / 120900 €	\$ 21000 / 21000 €		\$ 48600 / 41400 €	\$ 108200 / 108200 €			\$ 47200 / 42300 €	\$ 74400 / 74400 €	\$ 86600 / 77500 €	\$ 51300 / 43200 €
Virtual appliance		\$ 68700 / 52500 €	\$ 346800 / 346800 €	N/A				N/A	N/A	N/A	\$ 157800 / 157800 €				N/A	N/A	N/A
Minimum number of seats																	
Seats covered	1	5	25	5	250	5	100	100	5	5	10	1	1	5	5	100	5

Copyright and Disclaimer

This publication is Copyright © 2019 by AV-Comparatives®. Any use of the results, etc. in whole or in part, is ONLY permitted after the explicit written agreement of the management board of AV-Comparatives prior to any publication. AV-Comparatives and its testers cannot be held liable for any damage or loss, which might occur as result of, or in connection with, the use of the information provided in this paper. We take every possible care to ensure the correctness of the basic data, but a liability for the correctness of the test results cannot be taken by any representative of AV-Comparatives. We do not give any guarantee of the correctness, completeness, or suitability for a specific purpose of any of the information/content provided at any given time. No one else involved in creating, producing or delivering test results shall be liable for any indirect, special or consequential damage, or loss of profits, arising out of, or related to, the use or inability to use, the services provided by the website, test documents or any related data.

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

AV-Comparatives
(July 2019)