

# Independent Tests of Anti-Virus Software



## Business Security Test

TEST PERIOD: AUGUST – NOVEMBER 2019  
LANGUAGE: ENGLISH  
LAST REVISION: 16<sup>TH</sup> DECEMBER 2019

[WWW.AV-COMPARATIVES.ORG](http://WWW.AV-COMPARATIVES.ORG)

# Contents

<b>INTRODUCTION</b>	<b>3</b>
<b>TESTED PRODUCTS</b>	<b>4</b>
<b>SETTINGS</b>	<b>5</b>
<b>MANAGEMENT SUMMARY</b>	<b>6</b>
<b>AV-COMPARATIVES' APPROVED BUSINESS PRODUCT AWARD</b>	<b>8</b>
<b>REAL-WORLD PROTECTION TEST (AUGUST-NOVEMBER)</b>	<b>9</b>
<b>MALWARE PROTECTION TEST (SEPTEMBER)</b>	<b>14</b>
<b>PERFORMANCE TEST (OCTOBER)</b>	<b>16</b>
<b>ENHANCED REAL-WORLD TEST (AUGUST-NOVEMBER)</b>	<b>21</b>
<b>REVIEWS</b>	<b>30</b>
<b>FEATURE LIST</b>	<b>82</b>
<b>COPYRIGHT AND DISCLAIMER</b>	<b>83</b>

## Introduction

This is the second half-year report of our Business Main-Test Series<sup>1</sup> of 2019, containing the results of the Business Real-World Protection Test (August-November), Business Malware Protection Test (September), Business Performance Test (October), as well as the Product Reviews.

The test series consists of three main parts:

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

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

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

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

This second half-year report of 2019 also includes the results of the new **Enhanced Real-World Test** (protection against advanced persistent threats), which evaluates the products as regards their ability 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. In 2020, the Enhanced Real-World Test will be a separate test (not part of the Business Main Test Series), with its own report.

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

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

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

---

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

## Tested Products

The following business products<sup>2</sup> were tested under Microsoft Windows 10 1903 64-bit:

Vendor	Product	Version August	Version September	Version October	Version November
Avast	Business Antivirus Pro Plus	19.6	19.6	19.7	19.7
Bitdefender	GravityZone Elite Security	6.6	6.6	6.6	6.6
Cisco	AMP for Endpoints	6.3	6.3	6.3	6.3
CrowdStrike	Endpoint Protection Platform Standard Bundle	5.14	5.16	5.19	5.19
Elastic <sup>3</sup>	Endpoint Security	3.50	3.51	3.52	3.52
ESET	Endpoint Protection Advanced Cloud & CA	7.0	7.0	7.0	7.0
FireEye	Endpoint Security	30.19	30.19	30.19	30.19
Fortinet	FortiClient with EMS & FortiSandbox	6.0	6.0	6.2	6.2
K7	Enterprise Security	14.2	14.2	14.2	14.2
Kaspersky	Endpoint Security for Business Select	11.1	11.1	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	8.0	8.0	8.0	8.0
Seqrite	Endpoint Security	17.0	17.0	18.0	18.0
Sophos	Intercept X Advanced	10.8	10.8	10.8	10.8
SparkCognition	DeepArmor Endpoint Protection Platform	2.1	2.1	2.1	2.1
Symantec	Endpoint Protection	14.2	14.2	14.2	14.2
Trend Micro	Apex One <sup>4</sup>	12.0	12.0	12.0	12.0
VIPRE	Endpoint Security Cloud	11.0	11.0	11.0	11.0

We congratulate the vendors who are participating in the Business Main-Test Series for having their business products publicly<sup>5</sup> tested by an independent lab, showing their commitment to improving their products, being transparent to their customers and having confidence in their product quality.



<sup>2</sup> 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).

<sup>3</sup> **Endgame** was acquired by **Elastic** N.V. in autumn 2019. The product was formerly known as Endgame Endpoint Protection Platform.

<sup>4</sup> Trend Micro renamed its product in 2019. It was formerly known as Trend Micro OfficeScan XG.

<sup>5</sup> Large 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 PUA<sup>6</sup> 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".

**Elastic**<sup>7</sup>: Enabled Software and Hardware protection options: all enabled; Protected Applications: "Browser", "Microsoft Suite" (incl. Fltdr.exe and EQNEDT32.exe), "Java" and "Adobe". Malware (on-execution and on-write): "On – Prevent mode"; Process Injection: "On – Prevent mode"; Options: all enabled; "Aggressive" threshold. Adversary behaviors: all enabled; Credential dumping: enabled; Ransomware: disabled.

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

**Fortinet**<sup>8</sup>: 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.

---

<sup>6</sup> We currently do not include any PUA in our malware tests.

<sup>7</sup> Settings were renamed/reordered in the newer version.



## 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**, **Elastic** 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. Elastic 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.

## 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 for business products per year, separate awards will be given to qualifying products in July (for March-June tests), and December (for August-November tests).

To be certified in December 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 December 2019:





## Real-World Protection Test (August-November)

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

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

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

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



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

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



## Test Procedure

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

### Lab Setup

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

### Software

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

### Preparation for every testing day

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

### Testing Cycle for each malicious URL

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

## Protection

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

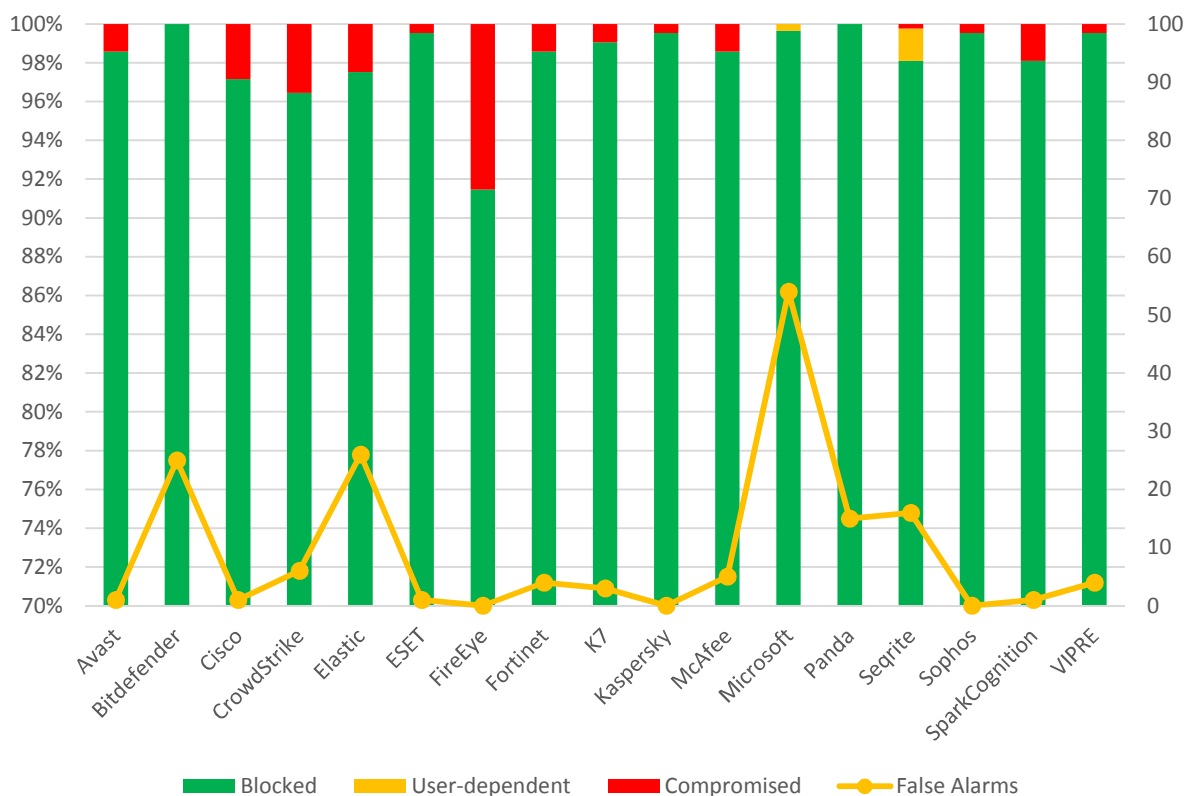
Due to the dynamic nature of the test, i.e. mimicking real-world conditions, and because of the way several different technologies (such as cloud scanners, reputation services, etc.) work, it is a matter of fact that such tests cannot be repeated or replicated in the way that e.g. static detection rate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

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

## Test Set

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

The results below are based on a test set consisting of **844** test cases (such as malicious URLs), tested from the beginning of August 2019 till the end of November 2019.



	Blocked	User dependent	Compromised	PROTECTION RATE [Blocked % + (User dependent %)/2] <sup>8</sup>	False Alarms
<b>Panda</b>	844	-	-	100%	15
<b>Bitdefender</b>	844	-	-	100%	25
<b>Microsoft</b>	841	3	-	99.8%	54
<b>Kaspersky, Sophos</b>	840	-	4	99.5%	0
<b>ESET</b>	840	-	4	99.5%	1
<b>VIPRE</b>	840	-	4	99.5%	4
<b>K7</b>	836	-	8	99.1%	3
<b>Seqrite</b>	828	14	2	98.9%	16
<b>Avast</b>	832	-	12	98.6%	1
<b>Fortinet</b>	832	-	12	98.6%	4
<b>McAfee</b>	832	-	12	98.6%	5
<b>SparkCognition</b>	828	-	16	98.1%	1
<b>Elastic<sup>9</sup></b>	823	-	21	97.5%	26
<b>Cisco</b>	820	-	24	97.2%	1
<b>CrowdStrike</b>	814	-	30	96.4%	6
<b>FireEye</b>	772	-	72	91.5%	0

<sup>8</sup> 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.

<sup>9</sup> Formerly known as Endgame.

## 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.

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



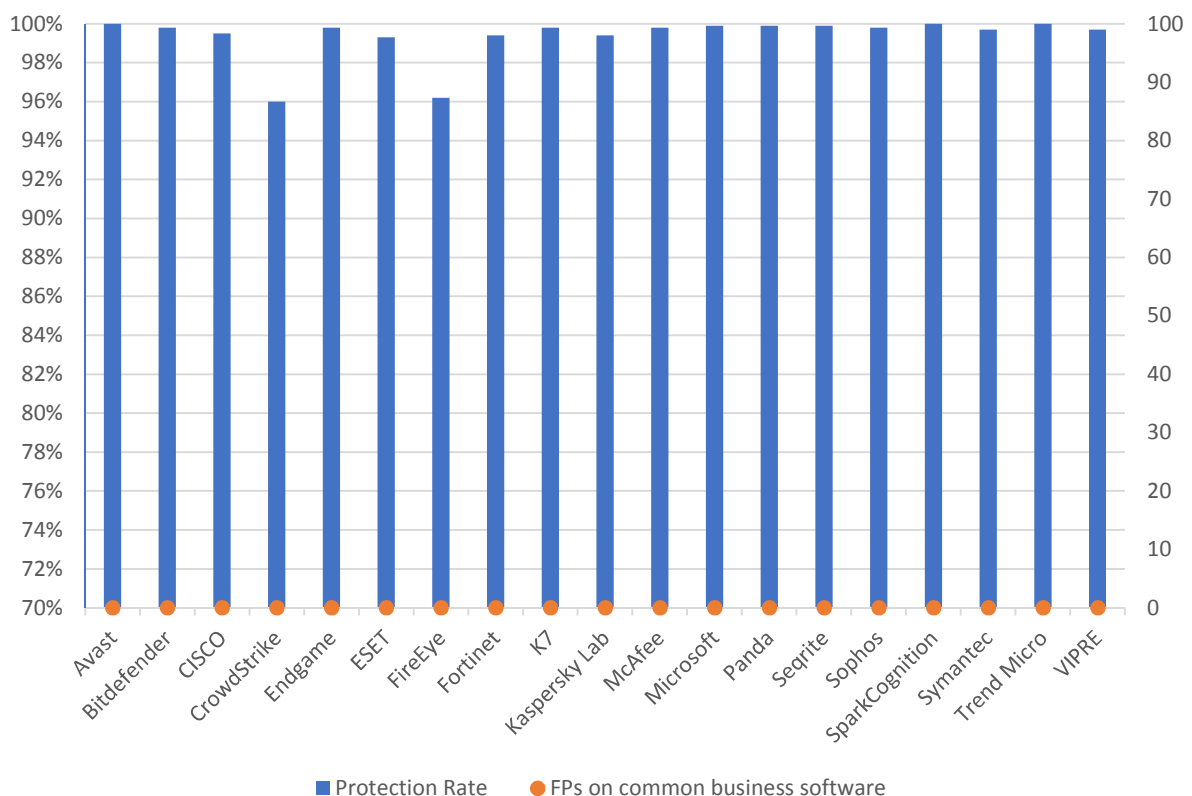
## Malware Protection Test (September)

The Malware Protection Test assesses a security program’s ability to protect a system against infection by malicious files before, during or after execution. The methodology used for each product tested is as follows. Prior to execution, all the test samples are subjected to on-access scans (if this feature is available) by the security program (e.g. while copying the files over the network). Any samples that have not been detected by the on-access scanner are then executed on the test system, with Internet/cloud access available, to allow e.g. behavioural detection features to come into play. If a product does not prevent or reverse all the changes made by a particular malware sample within a given time period, that test case is considered to be a miss. For this test, **1,278** 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, SparkCognition, Trend Micro	100%	0
Microsoft, Panda, Seqrite	99.9%	0
Bitdefender, Elastic, K7, McAfee, Sophos	99.8%	0
Symantec, VIPRE	99.7%	0
Cisco	99.5%	0
Fortinet, Kaspersky	99.4%	0
ESET	99.3%	0
FireEye <sup>10</sup>	96.2%	0
CrowdStrike	96.0%	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
Avast, Bitdefender, Cisco, ESET, Fortinet, K7, Kaspersky, Seqrite, Symantec	Very low
CrowdStrike, FireEye, McAfee, Microsoft, Panda, Sophos	Low
Elastic, Trend Micro, VIPRE	Medium
SparkCognition	High
-	Very high
-	Remarkably high

<sup>10</sup> A FireEye product issue was uncovered during the Malware Protection Test which led to some missed detections. The bug has now been fixed.

## Performance Test (October)

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

The following activities/tests were performed under an up-to-date **Windows 10 1903 64-Bit system**:

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

### Test methods

The tests were performed on an Intel Core i7-8550U CPU system with 8GB of RAM and SSD system drives. We consider this machine configuration as “**high-end**”. The performance tests were done on a clean Windows 10 1903 64-Bit system (English) and then with the installed business security client software. The tests were done with an active Internet connection to allow for the real-world impact of cloud services/features. Care was taken to minimize other factors that could influence the measurements and/or comparability of the systems. Optimizing processes/fingerprinting used by the products were also considered – this means that the results represent the impact on a system which has already been operated by the user for a while. The tests were repeated several times (with and without fingerprinting) in order to get mean values and filter out measurement errors. After each run, the workstation was reverted to the previously created system image and rebooted six times. We simulated various file operations that a computer user would execute: copying<sup>11</sup> different types of clean files from one place to another, archiving and unarchiving files, downloading files from the Internet and launching applications (opening documents). We believe that increasing the number of iterations increases our statistical precision. This is especially true for performance testing, as some noise is always present on real machines. We perform each test multiple times and provide the median as result. We also used a third-party, industry-recognized performance testing suite (PC Mark 10 Professional) to measure the system impact during real-world product usage. We used the predefined *PC Mark 10 Extended* test. Readers are invited to evaluate the various products themselves, to see what impact they have on their systems (due to e.g. software conflicts and/or user preferences, as well as different system configurations that may lead to varying results).

---

<sup>11</sup> We use around 5GB of data consisting of various file types and sizes (pictures, movies, audio files, MS Office documents, PDF documents, business applications/executables, Windows operating system files, archives, etc.).

## Test cases

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

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

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

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

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

**Downloading files:** 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



Key: Slow mediocre fast very fast

<sup>12</sup> Fortinet have told us that bugs in the tested version led to an increased system impact. The ability to change some newly introduced settings in version 6.2.0 (which have increased performance impact) will be added in the next build (6.2.2), as well as the bug fixes.



## PC Mark Tests

In order to provide an industry-recognized performance test, we used the PC Mark 10 Professional Edition<sup>13</sup> testing suite. Users using PC Mark 10 benchmark<sup>14</sup> should take care to minimize all external factors that could affect the testing suite, and strictly follow at least the suggestions documented inside the PC Mark manual, to get consistent and valid/useful results. Furthermore, the tests should be repeated several times to verify them. For more information about the various consumer scenarios tests included in PC Mark, please read the whitepaper on their website<sup>15</sup>.

“No security software” is tested on a baseline<sup>16</sup> system without any security software installed, which scores 100 points in the PC Mark 10 benchmark.

	PC Mark Score
<i>Baseline</i>	100
<b>ESET, K7</b>	99.3
<b>Elastic</b>	99.0
<b>Bitdefender</b>	98.9
<b>Vipre</b>	98.8
<b>Seqrite</b>	98.6
<b>McAfee</b>	98.5
<b>Sophos</b>	98.4
<b>FireEye</b>	98.3
<b>Kaspersky</b>	98.1
<b>Avast</b>	97.9
<b>Panda</b>	97.8
<b>Fortinet, Microsoft</b>	97.6
<b>CrowdStrike</b>	97.5
<b>Cisco</b>	97.2
<b>SparkCognition</b>	97.0

<sup>13</sup> For more information, see <https://benchmarks.ul.com>

<sup>14</sup> PC Mark® is a registered trademark of Futuremark Corporation / UL.

<sup>15</sup> [http://s3.amazonaws.com/download-aws.futuremark.com/PCMark\\_10\\_Technical\\_Guide.pdf](http://s3.amazonaws.com/download-aws.futuremark.com/PCMark_10_Technical_Guide.pdf) (PDF)

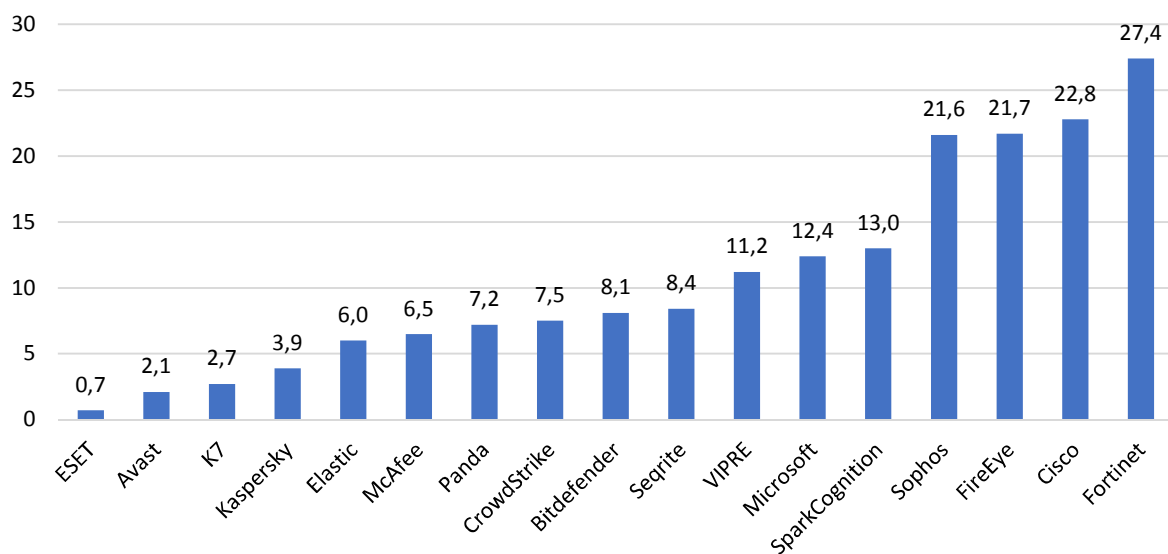
<sup>16</sup> Baseline system: Intel Core i7-8550U machine with 8GB RAM and SSD drive

## Summarized results

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

	AV-C Score	PC Mark Score	TOTAL	Impact Score
<b>ESET</b>	90	99.3	189.3	0.7
<b>Avast</b>	90	97.9	187.9	2.1
<b>K7</b>	88	99.3	187.3	2.7
<b>Kaspersky</b>	88	98.1	186.1	3.9
<b>Elastic</b>	85	99.0	184.0	6.0
<b>McAfee</b>	85	98.5	183.5	6.5
<b>Panda</b>	85	97.8	182.8	7.2
<b>CrowdStrike</b>	85	97.5	182.5	7.5
<b>Bitdefender</b>	83	98.9	181.9	8.1
<b>Seqrite</b>	83	98.6	181.6	8.4
<b>Vipre</b>	80	98.8	178.8	11.2
<b>Microsoft</b>	80	97.6	177.6	12.4
<b>SparkCognition</b>	80	97.0	177.0	13.0
<b>Sophos</b>	70	98.4	168.4	21.6
<b>FireEye</b>	70	98.3	168.3	21.7
<b>Cisco</b>	70	97.2	167.2	22.8
<b>Fortinet</b>	65	97.6	162.6	27.4

Performance Test November 2019 - System Impact Score



## Enhanced Real-World Test (August-November)

Advanced Persistent Threat (APT) is a term commonly used to describe a targeted cyber-attack that employs a complex set of methods and techniques to penetrate information system(s). Different aims of such attacks could be stealing / substituting / damaging confidential information, or establishing sabotage capabilities, the last of which could lead to financial and reputational damage of the targeted organisations. Such attacks are very purposeful, and usually involve highly specialized tools. The tools employed include heavily obfuscated malicious code, the malicious use of benign system tools, and non-file-based malicious code.

In our “Enhanced Real-World Test”, we use hacking and penetration techniques that allow attackers to access internal computer systems. These attacks can be broken down into Lockheed Martin's Cybersecurity Kill Chain, and seven distinct phases - each with unique IOCs (Indicators of Compromise) for the victims. All our tests use a subset of the TTP (Tactics, Techniques, Procedures) listed in the MITRE ATT&CK framework<sup>17</sup>. A false alarm test is also included in the report.

The tests use a range of techniques and resources, mimicking malware used in the real world. Some examples of these are given here. We make use of system programs, in an attempt to bypass signature-based detection. Popular scripting languages (JavaScript, batch files, PowerShell, Visual Basic scripts, etc.) are used. The tests involve both staged and non-staged malware samples, and deploy obfuscation and/or encryption of malicious code before execution (Base64, AES). Different C2 channels are used to connect to the attacker (HTTP, HTTPS, TCP). Use is made of known exploit frameworks (Metasploit Framework, Meterpreter, PowerShell Empire, Puppy, etc.).

To represent the targeted system, we use fully patched 64-bit Windows 10 systems, each with a different AV product installed. In the enterprise test, the target user has a standard user account. In the consumer test, an admin account is targeted. For this reason and others (e.g. possibly different settings), the results of the Consumer Test should not be compared with those of the Enterprise Test.

Once the payload is executed by the victim, a Command and Control Channel (C2) to the attacker's system is opened. For this to happen, a listener has to be running on the attacker's side. For example, this could be a Metasploit Listener on a Kali Linux system. Using the C2 channel, the attacker has full access to the compromised system. The functionality and stability of this established access is verified in each test-case.

The test consists of 15 different attacks. In future tests, we plan to provide additional, more granular information, complexity and coverage in the public report. This test currently focuses on protection, not on detection. It is carried out completely manually.

AV Main-Test-Series vendors were given the opportunity to opt out of this test before the public test started, which is why not all vendors are included in this test.

---

<sup>17</sup> <https://attack.mitre.org/matrices/enterprise/windows/>

## Scope of the test

The Enhanced Real-World Test looks at how well the tested products protect against very specific targeted attack methods. It does not consider the overall security provided by each program, or how well it protects the system against malware downloaded from the Internet or introduced via USB devices. It should be considered as an addition to the Real-World Protection Test and Malware Protection Test, not a replacement for either of these. Consequently, readers should also consider the results of other tests in our Main-Test Series when evaluating the overall protection provided by any individual product. This test focuses on whether the security products protect against specific attack/exploitation techniques used in APTs. Readers who are concerned about such attacks should consider the consumer products participating in this test, whose vendors were confident of their ability to protect against these threats in the test. We expect more vendors to participate in next year's test.

## Differences between the "MITRE test" and our "Enhanced Real-World Test"

Whilst our Enhanced Real-World Test makes use of elements of the MITRE ATT&CK framework, it is a very different sort of test from the "MITRE test". The "MITRE test" evaluates EDR (Endpoint Detection and Response) systems in situations where the respective vendors actively monitor the attack being performed in real time, sometimes also referred as "red and blue team testing". The emphasis is very much on detecting and logging attack processes (visibility), alerting administrators, and providing data to assist with manual threat-hunting and threat-countermeasures.

For the "MITRE test", vendors set their products to "log-only" mode, in order to find out as much as possible about the attack chain. Such tests very definitely have their uses and provide valuable data. However, protecting individual systems against infection, and thus system/data damage, is not the principle aim in such a test. We also note that MITRE does not provide a final scoring or ranking system; rather, it simply provides raw data for analysis.

Our Enhanced Real-World Test, on the other hand, aims to determine how well a security product protects the system on which it is installed in everyday use. The critical question is whether the product protects the system against the attack, whereby it is not important which protection component blocks the attack, or at which stage the attack is stopped, provided the system is not compromised (this sort of granularity might be added in future Enhanced Real-World Test for informational purposes). We also consider false alarms in our test.

## Test procedure

Scripts such as VBS, JS or MS Office macros can execute and install a file-less backdoor on victims' systems and create a control channel (C2) to the attacker, who is usually in a different physical location, and maybe even in a different country. Apart from these well-known scenarios, it is possible to deliver file-less malware using exploits, remote calls (PSexec, wmic), task scheduler, registry entries, Arduino hardware (USB RubberDucky) and WMI calls. This can be done with built-in Windows tools like PowerShell. These methods load the actual malware directly from the Internet into the target system's memory, and continue to expand further into the local area network with native OS tools. They may even become persistent on machines in this way. This test does not make use of portable executable (PE) malware.

## Fileless attacks

In the field of malware there are many (possibly overlapping) classification categories, and amongst other things a distinction can be made between file-based and fileless malware. Since 2017, a significant increase in fileless threats has been recorded. One reason for this is the fact that such attacks have proved very successful from the attackers' point of view. One factor in their effectiveness is the fact that fileless threats operate only in the memory of the compromised system, making it harder for antivirus software to recognize them. It is important that fileless threats are recognised by consumer security programs as well as by business products, for the reasons given below.

## Attack vectors and targets

In penetration tests, we see that certain attack vectors may not yet be well covered by security programs, and many popular AV products still provide insufficient protection. Some business security products are now making improvements in this area, and providing better protection in some scenarios. As mentioned above, we believe that consumer products also need to improve their protection against such malicious attacks; non-business users can be, and are, attacked in the same way. Anyone can be targeted, for a variety of reasons, including "doxing" (publishing confidential personal information) as an act of revenge. Attacking the home computers of businesspeople is also an obvious route into accessing their company data.

## Attack methods

In the Enhanced Real-World Test, we also include several different command-line stacks, CMD/PS commands, which can download malware from the network directly into RAM (staged) or base64 encoded calls. These methods completely avoid disk access, which is (usually) well guarded by security products. We sometimes use simple concealment measures, or change the method of the stager call as well. Once the malware has loaded its 2<sup>nd</sup> stage, an http/https connection to the attacker will be established. This inside-out mechanism has the advantage of establishing a C2 channel to the attacker that is beyond the protection measures of the majority of NAT and firewall products. Once the C2 tunnel has been established, the attacker can use all known control mechanisms of the common C2 products (Meterpreter, PowerShell Empire, etc.). These include e.g. file uploads/downloads, screenshots, keylogging, Windows shell (GUI), and webcam snapshots. All the tools used are freely available. Their source code is open and created for research purposes. However, the bad guys often abuse these tools for criminal purposes.

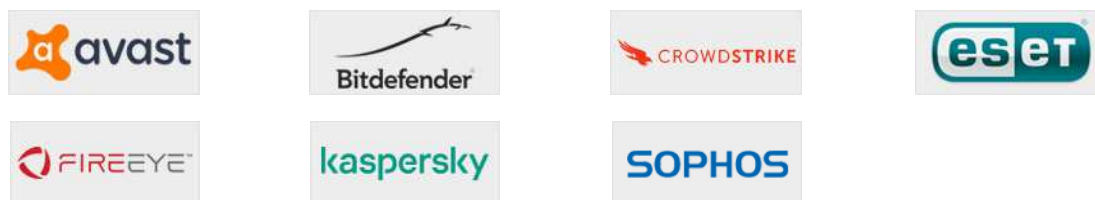
## False Positive (False Alarm) Test

A security product that blocks 100% of malicious attacks, but also blocks legitimate (non-malicious) actions, can be hugely disruptive. Consequently, we conduct a false-positives test as part of the Enhanced Real-World Test, to check whether the tested products are able to distinguish malicious from non-malicious actions. Otherwise a security product could easily block 100% of malicious attacks that e.g. use email attachments, scripts and macros, simply by blocking such functions. For many users, this could make it impossible to carry out their normal daily tasks. Consequently, false-positive scores are taken into account in the product's test score.



## Tested Products

The following vendors participated in the Enhanced Real-World Test. These are the vendors whose products scored well in the internal pre-test, and who were confident enough in the protection capabilities of their products against file-less attacks to take part in this public test. All other vendors in the Enterprise Main-Test Series opted-out of the test.



Vendor	Product	Version
<b>Avast</b>	Business Antivirus Plus	19.7
<b>Bitdefender</b>	GravityZone Elite Security	6.6
<b>CrowdStrike</b>	Endpoint Protection Platform Standard Bundle	5.19
<b>ESET</b>	Endpoint Protection Advanced Cloud	7.0
<b>FireEye</b>	Endpoint Security	30.19
<b>Kaspersky</b>	Endpoint Security for Business Select	11.1
<b>Sophos</b>	Intercept X Advanced	10.8

Most AV vendors did not participate with their respective EDR products, or disabled the EDR components of their participating products (see settings below). This may be explained by the fact that we use the same product and configuration for all the tests within a series; some EDR functions can have a negative impact on performance and false alarms.

Please note that the reached results are valid only for the products tested with their respective settings. With other settings (or products) the scores could be worse or better.

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

**Avast, ESET, Kaspersky:** default settings.

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

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

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

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

## Test Results

Below are the results for the 15 attacks used in this test<sup>18</sup>:

	Test scenarios															FPs	Score
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15		
Avast	✓	✓	✓	✓	✓	🛡️	✓	✓	🛡️	✓	✓	✓	✓	🛡️	✗	N	14
Bitdefender	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	N	15
CrowdStrike	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✗	✗	✗	✓	N	12
ESET	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	N	15
FireEye	✓	✓	✓	✗	✓	✓	✓	✓	✓	✓	🛡️	✗	✓	✓	✗	N	12
Kaspersky	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	N	15
Sophos	✓	✗	✓	✓	✓	✓	✓	✓	✓	✓	✗	✗	✗	✗	✗	N	9

### Key

✓	Threat detected, no C2 session, system protected	1 point
🛡️	No alert shown, but no C2 session established, system protected	1 point
✗	Threat not detected, C2 session established	0 points

In our opinion, the goal of every AV/EPP/EDR system should be to detect and prevent APTs or other malware as soon as possible. In other words, if the APT is detected before, at or soon after execution, thus preventing the opening of a Command and Control Channel, there is no need to prevent post-exploitation activities. A good burglar alarm should go off when somebody breaks into your house, not wait until they start stealing things.

A product that blocked certain functions (e.g. email attachments, scripts) in our FP test, would not be certified. However, none of the tested products exhibited any such behaviour in the false-alarm/functionality-blocking scenarios used in this particular test.

If a user-dependent alert were shown, we would award half a point. However, there were no such cases in this specific test.

### Observations on enterprise products

In this section, we report any additional information of interest to readers. An example might be a program with EDR functions reporting some kind of detection without actually blocking it. Whilst there were no such cases in this test, other points of interest are noted below.

**Avast:** In three cases, there was no alert, but also no stable C2-session.

**Bitdefender:** Almost all detections occurred on-access, i.e. before the threat was executed.

**CrowdStrike:** All detections occurred during execution of the threats. Cases #4, #5 and #11 showed no alert on the client (although blocked), but were reported in the web console.

**ESET, Kaspersky:** All threats were blocked: most of them were blocked during execution, and some few ones before the threat was executed (on-access).

**FireEye:** In one case, there was no alert, but also no stable C2-session.

**Sophos:** Most of the threats were blocked during execution.

<sup>18</sup> Please note that the results apply only for the product versions and settings used.

## Certified Advanced Threat Protection (ATP) Enterprise Products

AV-Comparatives' certification for Advanced Threat Protection is given to Approved Enterprise products which blocked at least 8 of the 15 attacks used in the Enhanced Real-World Test, i.e. a C2-session could not be established. Business security programs are expected to deal with the kind of threat used in this test, so detection of more than half of the test cases is required for certification.



## Test cases employed

We used five different [Initial Access Phases](#), distributed among the 15 test cases (e.g. 3 testcases came via email/spear-phishing attachment).

- a) **Trusted Relationship:** “Adversaries may breach or otherwise leverage organizations who have access to intended victims. Access through trusted third party relationship exploits an existing connection that may not be protected or receives less scrutiny than standard mechanisms of gaining access to a network.” (Source: <https://attack.mitre.org/techniques/T1199/>)
- b) **Valid accounts:** “Adversaries may steal the credentials of a specific user or service account using Credential Access techniques or capture credentials earlier in their reconnaissance process through social engineering [...]” (Source: <https://attack.mitre.org/techniques/T1078/>)
- c) **Replication Through Removable Media:** “Adversaries may move onto systems [...] by copying malware to removable media [...] and renaming it to look like a legitimate file to trick users into executing it on a separate system. [...]” (Source: <https://attack.mitre.org/techniques/T1091/>)
- d) **Spearphishing Attachment:** “Spearphishing attachment is [...] employs the use of malware attached to an email. [...]” (Source: <https://attack.mitre.org/techniques/T1193/>)
- e) **Spearphishing Link:** “Spearphishing with a link [...] employs the use of links to download malware contained in email [...]” (Source: <https://attack.mitre.org/techniques/T1192/>)

The 15 test scenarios (PowerShell-based file-less attacks and file-based exploits) used in this Enhanced Real-World Test are very briefly described below.

- 1) This threat is introduced via Trusted Relationship. MSHTA launches an HTML application, which executes a PowerShell command via the Windows Scripting Host. This test case was created with Unicorn.
- 2) This threat is introduced via Trusted Relationship. A batch file with an encoded PowerShell command gets executed. The PowerShell process injects the payload into memory. This test case was created with Unicorn.
- 3) This threat is introduced via Trusted Relationship. A Microsoft Word document with a malicious macro starts a PowerShell process which loads the payload into memory. This test case was created with Unicorn.
- 4) This threat is introduced through Valid Accounts. A VBScript spawns a PowerShell process and executes the payload. This test case was created with Empire.
- 5) This threat is introduced through Valid Accounts. A Shortcut modification technique is used to generate a backdoor. This test case was created with Empire.
- 6) This threat is introduced through Valid Accounts. MSHTA launches an HTML application, which executes an obfuscated PowerShell command via the Windows Scripting Host. This test case was created with Empire.
- 7) This threat is introduced via Removable Media (USB). A batch file executes an encoded payload through the PowerShell engine. This test case was created with Empire.
- 8) This threat is introduced via Removable Media (USB). An encoded malicious Microsoft Word document macro starts a PowerShell process and loads the payload into memory. This test case was created with Empire.

- 9) This threat is introduced via Removable Media (USB). A PowerShell script executes a PowerShell payload into memory. This test case was created with Unicorn.
- 10) This threat is introduced via Spearphishing Attachment. A VBScript executes an obfuscated payload through the PowerShell engine. This test case was created with Metasploit Meterpreter.
- 11) This threat is introduced via Spearphishing Attachment. An obfuscated Microsoft Word macro-enabled file starts a PowerShell process which loads the payload into memory. This test case was created with Empire.
- 12) This threat is introduced via Spearphishing Attachment. A JavaScript executes a C# code via the Windows Scripting Host. This test case was created with SharpShooter.
- 13) This threat is introduced via Spearphishing Link. A JavaScript executes an obfuscated C# code via the Windows Scripting Host. This test case was created with Metasploit Meterpreter.
- 14) This threat is introduced via Spearphishing Link. A Microsoft Excel macro-enabled file injects obfuscated C# code into memory. This test case was created with Metasploit Meterpreter.
- 15) This threat is introduced via Spearphishing Link. A PowerShell script injects an obfuscated PowerShell payload into memory. This test case was created with Metasploit Meterpreter.

**False Alarm Test:** Various false-alarm scenarios were used in order to see if any product is over-blocking certain actions (e.g. by blocking by policy email attachments, communication, scripts, etc.). None of the tested products showed over-blocking behaviour in the false-alarm test scenarios used.

### What is covered by the various test cases?

Our tests use a subset of the TTP (Tactics, Techniques, Procedures) listed in the [MITRE ATT&CK framework](#). In future, we might cover more [Techniques](#) and [Tactics](#) (such as [Privilege Escalation](#), [Credential Access](#), [Lateral Movement](#) and [Impact](#)) and provide more details of where the attack is stopped (either as part of this report, or in a separate test report). This year, the above 15 test cases cover the items shown in the table below:

<i>Initial Access</i>	<i>Execution</i>	<i>Persistence</i>	<i>Defense Evasion</i>	<i>Discovery</i>	<i>Collection</i>	<i>Command and Control</i>	<i>Exfiltration</i>
<a href="#">Replication Through Removable Media</a>	<a href="#">Mshta</a>	<a href="#">Shortcut Modification</a>	<a href="#">Mshta</a>	<a href="#">System Information Discovery</a>	<a href="#">Data from Local System</a>	<a href="#">Commonly Used Port</a>	<a href="#">Automated Exfiltration</a>
<a href="#">Spearphishing Attachment</a>	<a href="#">PowerShell</a>		<a href="#">Masquerading</a>			<a href="#">Data Encoding</a>	<a href="#">Data compressed Exfiltration</a>
<a href="#">Spearphishing Link</a>	<a href="#">Scripting</a>		<a href="#">Obfuscated Files or Information</a>			<a href="#">Data Obfuscation</a>	<a href="#">Over Command and Control Channel</a>
<a href="#">Trusted Relationship</a>			<a href="#">Scripting</a>			<a href="#">Multi-Stage Channels</a>	
<a href="#">Valid Accounts</a>			<a href="#">Template Injection</a>			<a href="#">Uncommonly Used Port</a>	

For reference purposes, the full MITRE ATT&CK framework for Windows can be seen here: <https://attack.mitre.org/matrices/enterprise/windows/>



## About the Enhanced Real-World Test

The Enhanced Real-World Test for enterprise products is being run for the first time in 2019. This year, it is an optional part of the Public Enterprise Main-Test Series. Next year, it will be an entirely separate test with its own report.

The complex nature of the test means that automation is not possible, and it has to be performed entirely manually, making it cost-intensive to run. However, vendors in the Main-Test Series (both Consumer and Enterprise) had the opportunity to participate in the Public Enhanced Real-World Test of 2019 at no additional cost to themselves.

In the Enterprise Main-Test Series, vendors are allowed to configure the products as they see fit – as is common practice with business security products in the real world. However, precisely the same product and configuration is used for all the tests in the series. If we did not insist on this, a vendor could turn up protection settings or activate features in order to score highly in the Real-World and Malware Protection Tests, but turn them down/deactivate them for the Performance and False Positive Tests, in order to appear faster and less error-prone. In real life, users can only have one configuration at once, so they should be able to see if high protection scores mean slower system performance, or lower false-positive scores mean reduced protection.

Some vendors asked for precise details of the day and time the test would be performed, so that they could monitor the attacks in real time and interact with their products when they thought it beneficial. Because the aim of the test is to measure protection capabilities, rather than analyse the attack methods, we did not provide any vendors with any advance information about when the test would be performed. In real life, attackers do not tell their victims when they are going to attack, so products must provide protection all the time. We also had requests from vendors regarding the attack methods to be used in the test. Again, because the test is about protection rather than analysis/visibility, we did not divulge specific details of the attack methods.

We did however invite all the vendors in the Main-Test Series to take part in an internal pre-test, which demonstrated broad guidelines for how the test would be performed, and invited vendors to provide feedback on how it might be improved. Each vendor was privately provided with the results for their respective product. As a result of the feedback we received, we implemented some changes in the test methodology, where we felt that this was in the genuine interests of users and helped to promote cybersecurity in general.

The test is very challenging, but at the same time it also reflects realistic scenarios. We have had positive feedback from many vendors' technical departments. Penetration testers see the real capabilities of products in their tests every day. Our comparison test tries to create a level playing-field that allows us to compare the protection capabilities of the different products against such attacks. This lets users see how well they are protected, and allows vendors, where necessary, to improve their products in the future. To get an overall picture of the protection capabilities of any of the tested products, readers should look at the results of the other tests in the Main-Test Series too.

## 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.

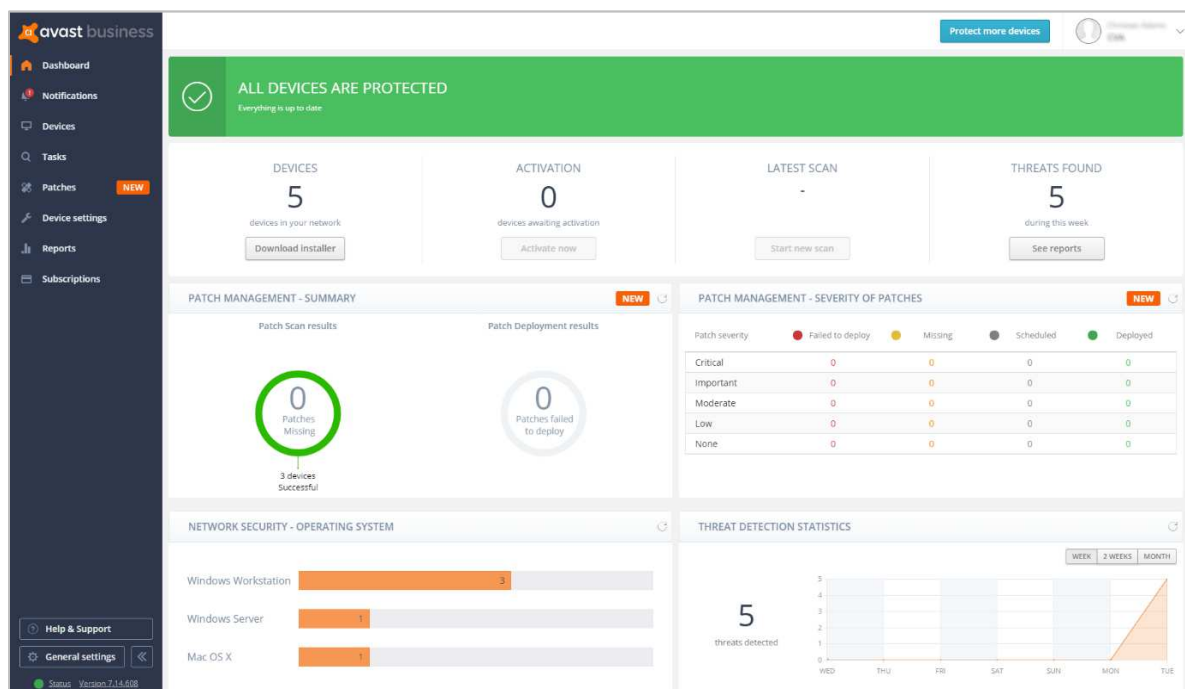
We first look at the type of product, i.e. whether the console is cloud based or server based, and what sort of devices/operating systems can be protected and managed.

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 cloud-based product aimed at the small to medium-sized business. 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. We liked the straightforward nature of the platform.

### About the product

Avast Business Antivirus Pro Plus uses a cloud-based console to manage the endpoint software. The product protects Windows clients, Windows servers and macOS devices. Windows client features include anti-spam, data shredding, a VPN, and data & identity protection. Exchange and SharePoint security are provided for Windows Server. A patch management feature is included for all Windows computers. However, automatic installation of patches requires an Avast Patch Management licence.

### Getting up and running

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

### Everyday management

On the server console, there is a clear set of main menus down the left-hand side. These are: *Dashboard*, *Notifications*, *Devices*, *Tasks*, *Patches*, *Device Settings*, *Reports*, *Subscriptions*. *Help & Support* and *General Settings* are found at the bottom.

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, when the latest scan was run, and how many threats have been found. The status display at the top of the page warns of any problems, such as out-of-date computers or malware detections. It is a straightforward and reassuring overview for the non-expert administrator. There are also summaries of the patch management, OS distribution and threat detection situations.

*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.

Status	Device name	License	Last seen
<input type="checkbox"/> Safe	GROUP-DEFAULT   SETTINGS: Default (Inherited)	Antivirus Pro Plus	11:32 17 Sep 2019
<input type="checkbox"/> In danger	GROUP-DEFAULT   SETTINGS: Default (Inherited)	Antivirus Pro Plus	12:05 17 Sep 2019
<input type="checkbox"/> Safe	GROUP-DEFAULT   SETTINGS: Default (Inherited)	Antivirus Pro Plus	23:16 16 Sep 2019
<input type="checkbox"/> Uninstalling	GROUP-DEFAULT   SETTINGS: Default (Inherited)		09:38 17 Sep 2019
<input type="checkbox"/> Safe	GROUP-DEFAULT   SETTINGS: Default (Inherited)	Antivirus Pro Plus	18:13 16 Sep 2019

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.

At the time of writing (September 2019), *Patches* was marked as a “new” feature in the console menu column. It monitors the state of installed applications, and advises when newer versions are available. Both Microsoft and third-party applications are covered. The status display at the top of the dashboard will warn if any devices are missing critical or non-critical patches. A link here takes you to the *Patches* page, which shows you which devices are affected. Clicking on a device displays a list of the missing patches, together with convenient download links.

*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 or save it to a file location, which would have been a useful daily report.

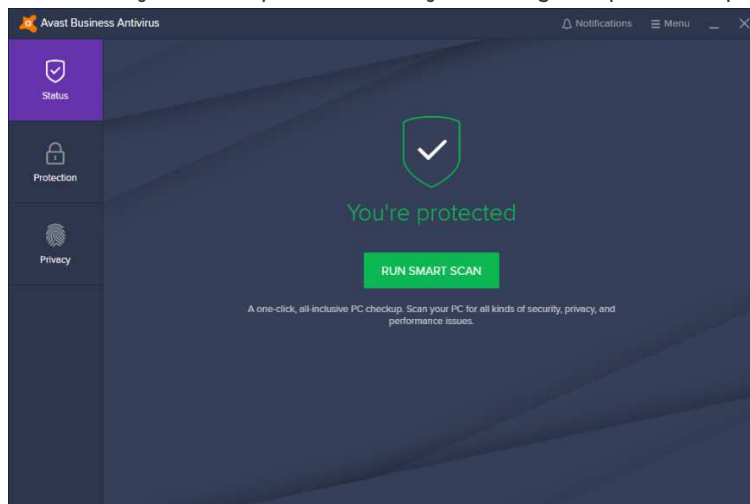
As you would expect, *Subscriptions* shows you the product licences you currently have, and how many of them you have used.

*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.

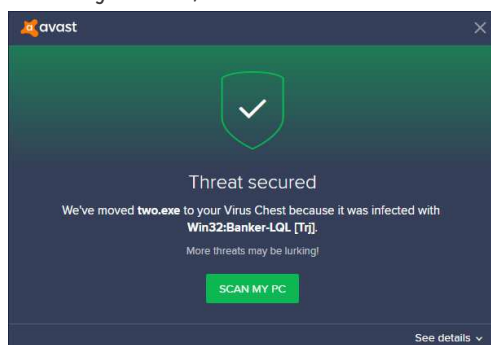
*General Settings* lets you change the system time zone. You can also create a local server for deployments and updates, and import the database of another Avast console.

### Windows endpoint protection software

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

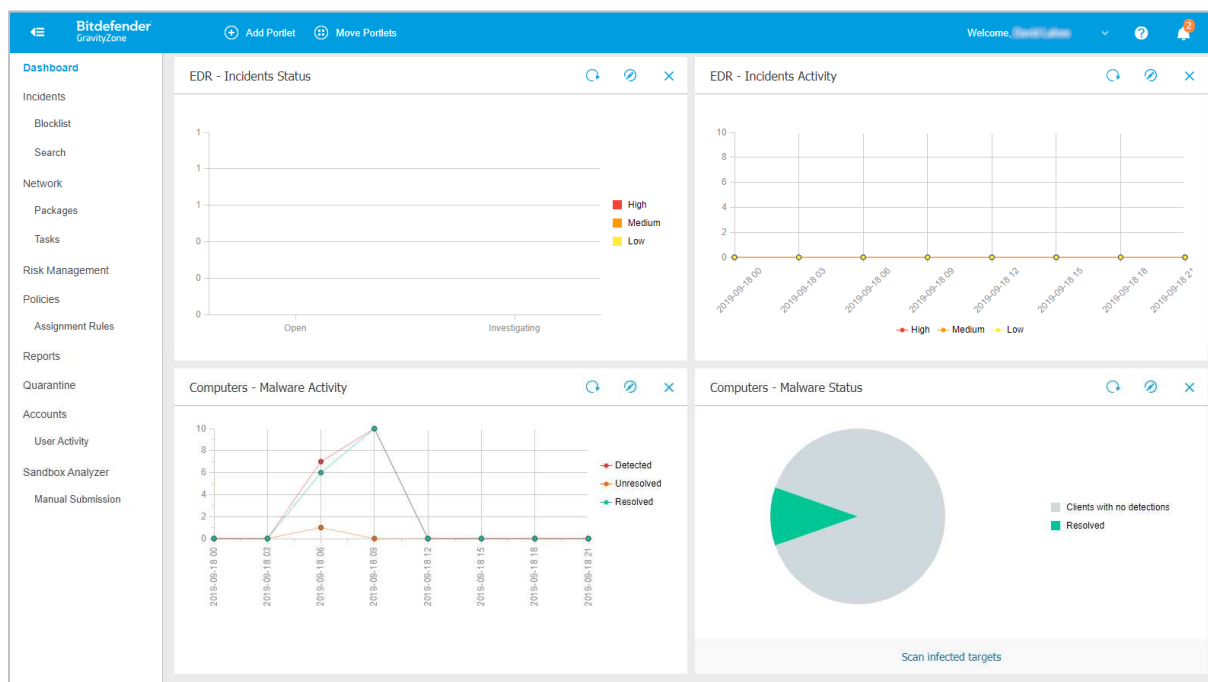


Malware is detected on file copy and quarantined. An example alert is shown below. The user cannot take any action, other than to close the alert.



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

## 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.

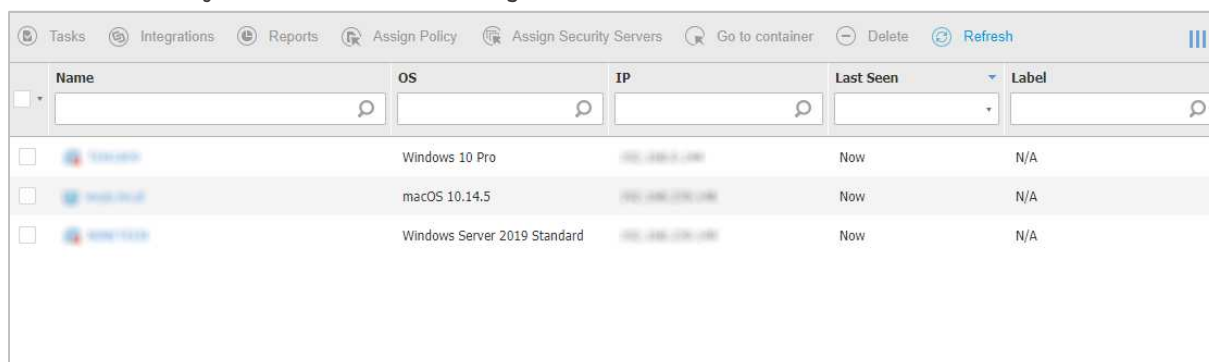
Step 4 is *Reporting*, where it shows you how to create appropriate reports of activity on your network. Having gone through these steps, you should have a deployed and managed network.




### 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. The items are *Dashboard*, *Incidents*, *Network*, *Risk Management*, *Policies*, *Reports*, *Quarantine*, *Accounts* and *Sandbox Analyzer*.

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

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



Name	OS	IP	Last Seen	Label
 Windows 10 Pro	Windows 10 Pro	192.168.1.100	Now	N/A
 macOS 10.14.5	macOS 10.14.5	192.168.1.101	Now	N/A
 Windows Server 2019 Standard	Windows Server 2019 Standard	192.168.1.102	Now	N/A

The main *Network* page shows you all the managed devices on your network, ordered into groups which you can create yourself (screenshot above). The *Packages* sub-page lets you configure deployment packages. On the *Tasks* sub-page you can create tasks such as scans and updates, which can be run once or multiple times on specified devices or groups.

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

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

*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.

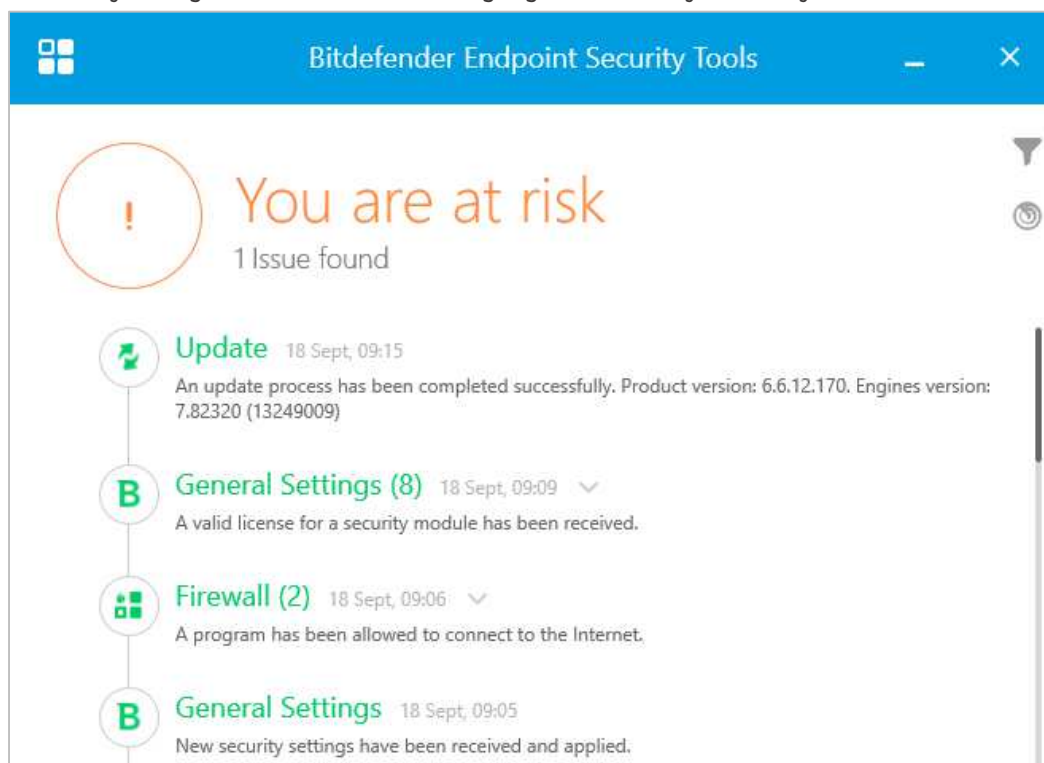
*Accounts* lets you monitor the activities of the user accounts that have been set up.

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

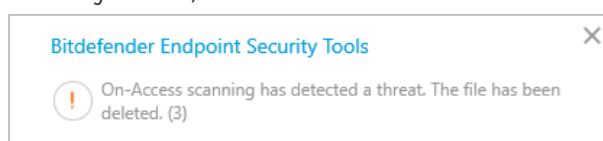
Clicking the bell icon in the top right-hand corner opens the *Notifications* panel. This displays a list of events such as logins and detections. Drilling into an item gives a clear description of what happened. We particularly liked the reporting of a malware outbreak. This informed us that “at least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

### Windows endpoint protection software

The Windows desktop protection software is a simple application with a clean interface. It clearly shows what is going on, with details of updates carried out, modules enabled, and programs allowed through the firewall. The user interface allows the user to check for updates, and initiate 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.

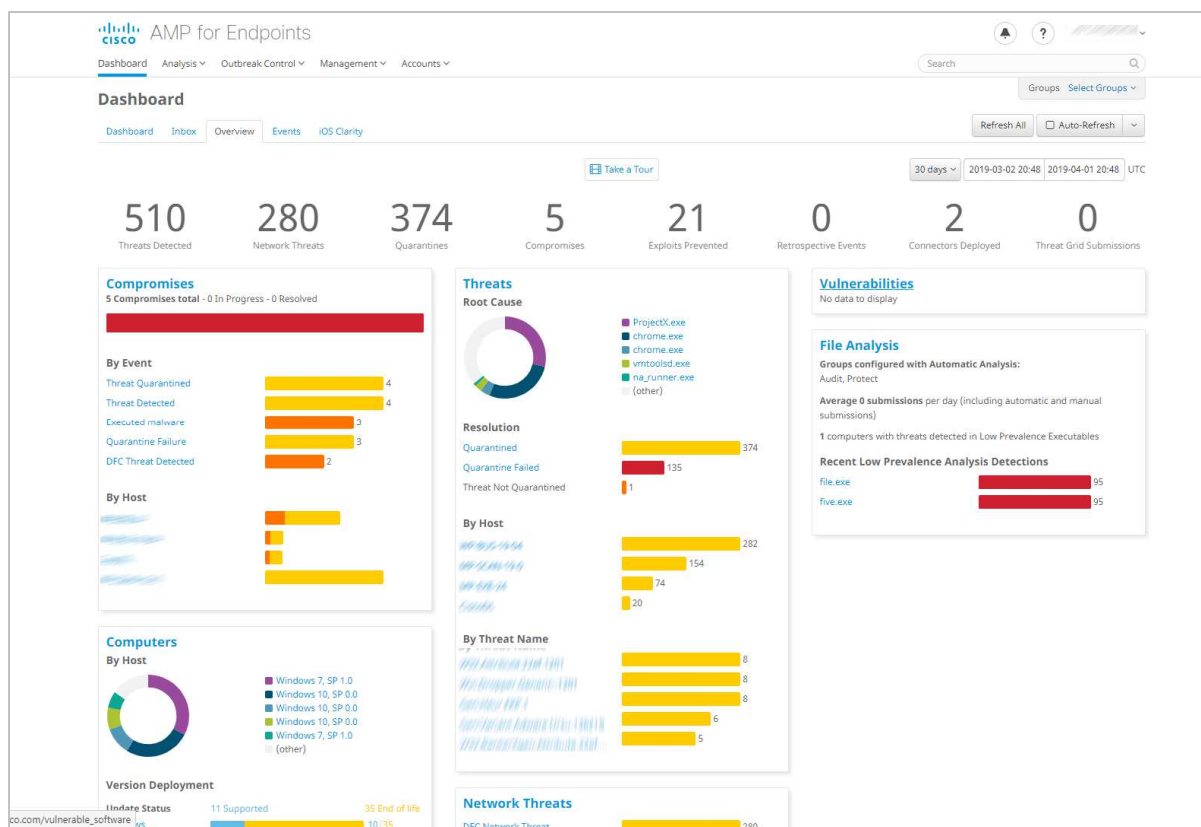


Malware is detected on file copy and quarantined. An example alert is shown below. The user cannot take any action, and the alert closes after a few seconds.



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

## Cisco Advanced Malware Protection for Endpoints



### Verdict

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

### About the product

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

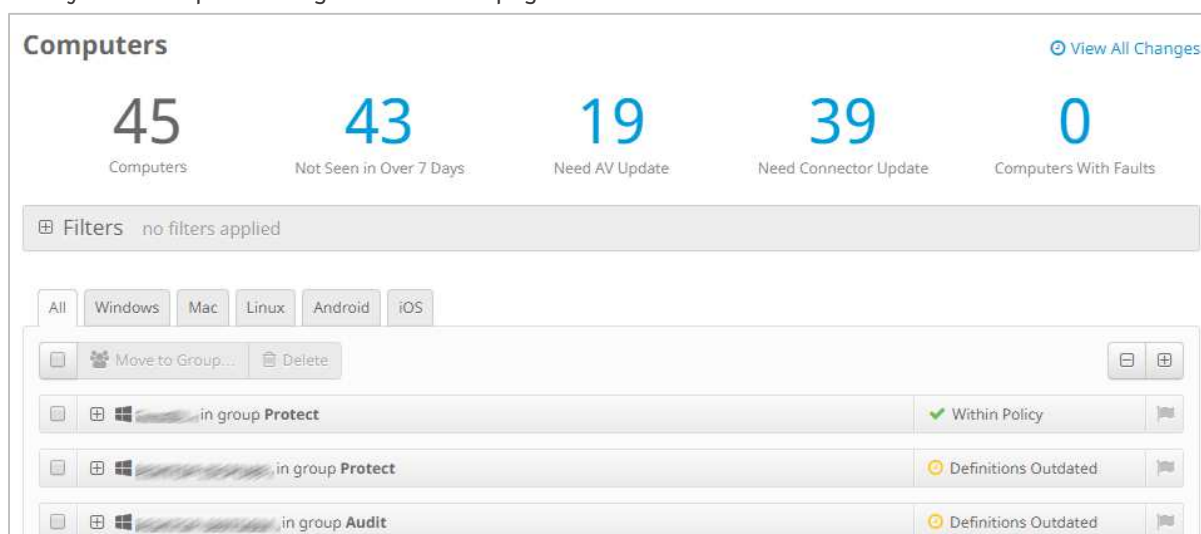
### Getting up and running

As the console is cloud-based, no installation is necessary. You just browse to the URL and log in. Installers for desktop systems can be found by clicking *Management\Download Connector*. The setup process is very quick and simple, and only takes a couple of clicks. We note that Windows Defender is not disabled automatically on Windows desktop systems when the Cisco endpoint software is installed.

## Everyday management

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

The *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 are a number of panels with coloured bar and doughnut charts. These 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, such as computers with faults or that need 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. This shows information such as OS version, definitions version, internal and external IP addresses, and date and time last seen. You can also start or stop the isolation of a computer from here. The device list can be narrowed by OS type, using the tabs at the top. You can also filter the device list using various details. These include specific OS version, group, or definitions status, by clicking on *Filters* at the top.

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

In the *Analysis* menu you can find features for investigating attacks. *Events* shows a list of threats encountered by protected devices. These include access to risky websites, malicious file downloads, and attempts to quarantine suspected malware. Clicking on an item displays more details, such as the IP address and port of the threat website, and the hash of the malicious file. This lets you take action against the threats, such as blacklisting the file or website and/or starting isolation of the endpoint for triage. 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 third-party security services as well as their own. The *Detections/Quarantine* page is similar. However, it filters the information down to actual malware encounters. You can drill down even further on the *File Analysis* page. This shows you the specific behavioural indicators for detecting a file as malicious. To see which legitimate programs have been involved in malware encounters, take a look at the *Threat Root Cause* page. A coloured pie chart shows you the distribution of malware encountered by specific applications, such as chrome.exe or explorer.exe. On the *Prevalence* page, the number of devices affected by a particular threat is shown. Under *Vulnerable Software*, programs with known vulnerabilities are listed. There is also CVE-ID and CVSS info to help identify and resolve the problem. Finally, *Reports* provides a very detailed weekly report. This covers numerous items such as threats, compromises and vulnerabilities. These are illustrated with coloured bar and doughnut charts. The *Outbreak Control* menu provides options for blocking or whitelisting specific applications and IP addresses. There are also custom detection options. These let you block the installation of any program you consider to be harmful or unwanted anywhere on the network. You can also run IOC (indicator of compromise) scans.

#### Windows endpoint protection software

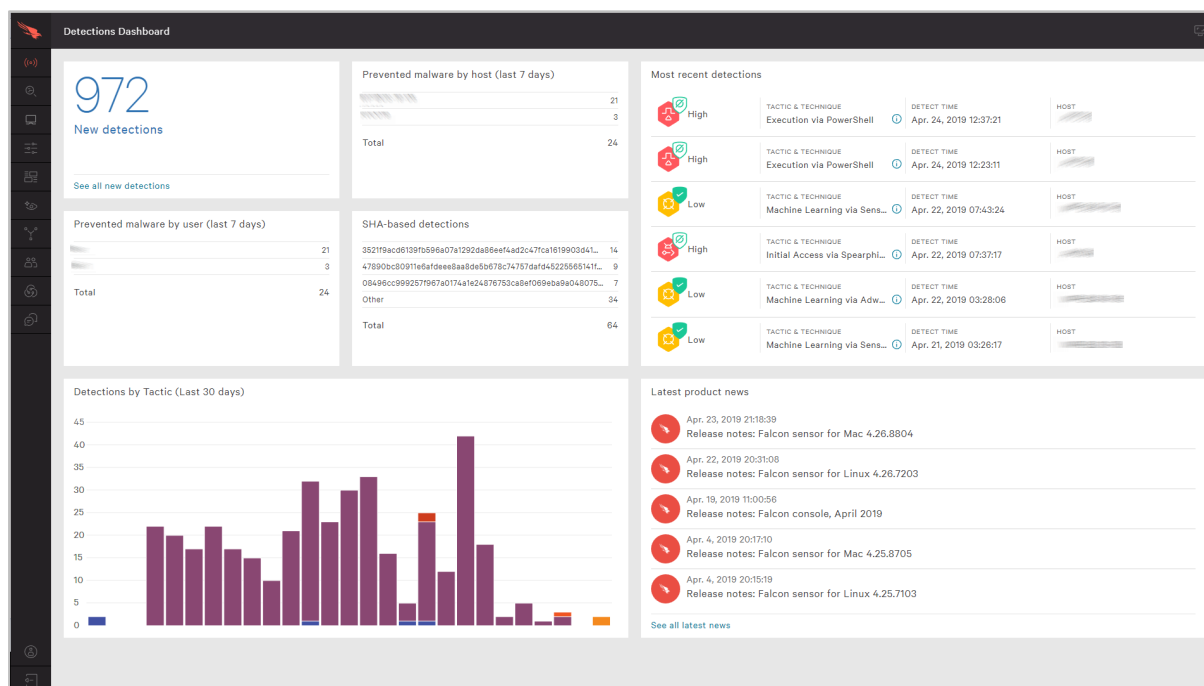
The Windows desktop protection software has a very simple GUI, which allows users to run scans and view the logs. Both of these functions open in separate, larger windows. Users can also view settings, but by default these are locked down. Users have a choice of scans they can run. Options are *Flash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



Malware is detected and quarantined on file copy. By default, detection is silent, i.e. no alert is shown to the user. However, the endpoint software can be configured by policy to show notifications.

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

## CrowdStrike Endpoint Protection Platform Standard Bundle



### Verdict

CrowdStrike Falcon is a very comprehensive platform. It provides AV services within an organisation, and a comprehensive set of detection and analysis services. We note that CrowdStrike Falcon is available as a fully managed service. This would be ideal for organisations that desire a more hands-off solution. Otherwise, it aims at the larger organisation, and is not really a “fit and forget” product. Basic everyday monitoring and management tasks are simple enough, even without detailed knowledge. However, the product’s capabilities are sophisticated enough that investing learning time will pay dividends. CrowdStrike tell us that learning modules are available online or via external consultancy.

### About the product

Crowdstrike Falcon is an endpoint protection platform. It lets you proactively look for malicious activities and adversaries. The cloud-based management console can be run from the cloud on any modern browser. There is endpoint protection software is for Windows/Linux clients and servers, and macOS.

### Getting up and running

Management is via a cloud console, and requires no on-premises equipment. Deployment of the client “sensor” is quite simple here. It relies on the download of the appropriate installation package. Automatic sensor deployment using e.g. Windows System Center Configuration Manager is also possible. On macOS clients, you need to run a terminal command after installation. You can find details of this in the documentation. 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 apply 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. You can expand this 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. 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. You can click through to the *Detections* submenu to view more detail. You get a strong reporting infrastructure, with a good choice of filter options. You can also examine quarantined files and real-time response sessions too.

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

The screenshot shows the 'Hosts' page in the CrowdStrike Falcon console. At the top, there is a search bar with the text 'Type to filter' and a notification '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 hosts, 1 Mac host, and 1 Yosemite (10.10) host. Below the summary table is a table with columns: Hostname, Last Seen, First Seen, OS Version, OU, Prevention Policy, Response Policy, Sensor Update P..., Status, and Sensor Version. The table shows three rows of host data.

Platform	OS Version	OU	Site Name	Type	Status
Windows	Windows 10	N/A	N/A	Workstation	Normal
Mac	Windows	233		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 13:39...	Apr. 1, 2019 14:50...	Windows 10		platform_default Apr. 1, 2019 14:50...	platform_default Apr. 1, 2019 14:50...	platform_default Changes pending	Normal	4.24.8702.0
[REDACTED]	Apr. 16, 2019 10:0...	Apr. 15, 2019 10:3...	Windows 10		platform_default Apr. 15, 2019 10:3...	platform_default Apr. 15, 2019 10:3...	platform_default Changes pending	Normal	4.25.8802.0
[REDACTED]	Mar. 6, 2019 20:5...	Mar. 6, 2019 20:5...	Windows 10		platform_default Mar. 6, 2019 20:5...	platform_default Mar. 6, 2019 20:5...	platform_default Changes pending	Normal	4.21.8406.0

The *Hosts* 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 displays an executive summary. There are detailed graphics for detections by scenario and severity, plus top 10 users, hosts and files with most detections. This is just the tip of a very deep iceberg allowing for comprehensive analysis. You can search by almost anything, and use this to discover what has happened during an outbreak. This includes where something entered, how it attempted to execute, what processes it used, and the containment method. Getting through this is not for the fainthearted, but it certainly provides a very powerful set of audit and analysis tools.

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.



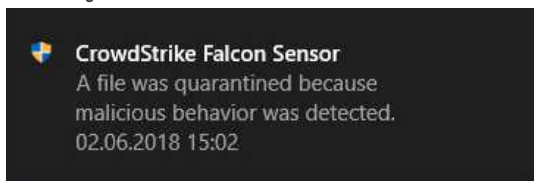
You can also review user account information, including domain/local accounts and their password reset status.

The *Intelligence* menu provides an overview of the current threat landscape. You can categorise this by different factors. Examples include geographical origin of threat, target industry, and target country. You can even see the attackers' motivation, e.g. criminal or hacktivist. Each threat is detailed by these parameters. Clicking *View Profile* on the threat displays a comprehensive analysis and explanation of that specific threat. This is a comprehensive resource which is unusual and most welcome.

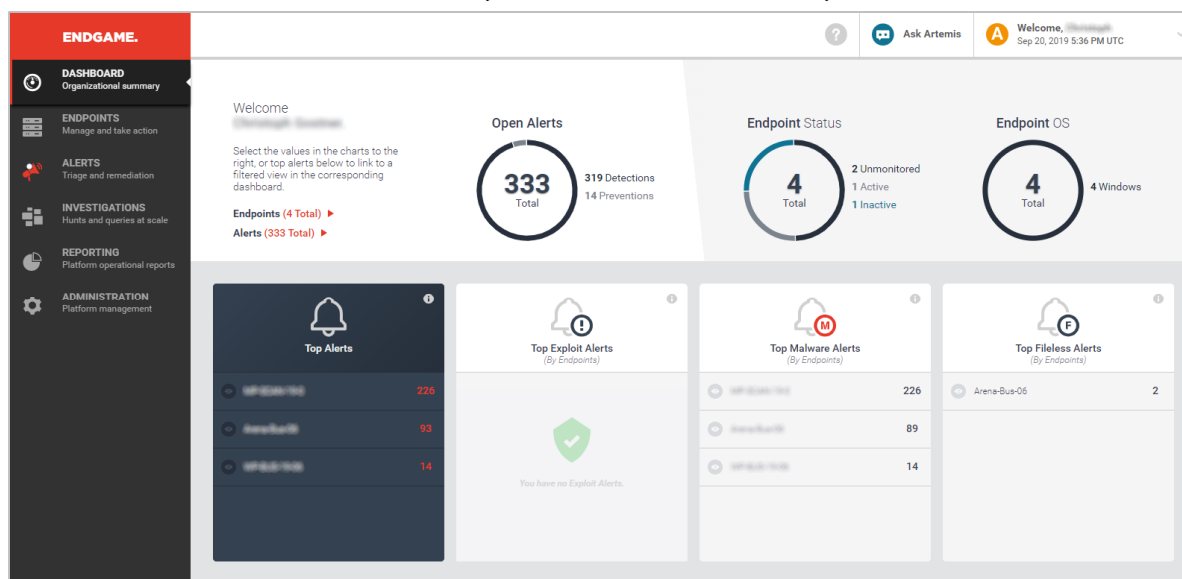
The *User* menu allows you to create profiles for console users. There are pre-built roles already created for *Endpoint Manager*, *Event Viewer*, *Administrator*, *Analyst*, *Investigator*, *Real Time Responder*, and others. You can map these roles to existing working structures, or custom-build new 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

Under default settings, the Windows desktop and server protection software is invisible to the user. Malware is detected on execution, and quarantined. An example alert is shown below. The user cannot take any action, and the alert closes after a few seconds.



## Elastic Endpoint Security (formerly Endgame)



### Verdict

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

### About the product

Endgame was acquired by Elastic in October 2019 and the product is now known as Elastic Endpoint Security. Elastic Endpoint Security provides prevention, detection and response measures. It has threat-hunting capabilities aimed at stopping targeted attacks. The management console can be run from the cloud on any modern browser. On-premises deployment is also an option. Elastic Endpoint Security supports Windows, Linux, Mac, and Solaris clients and servers.

### Getting up and running

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

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

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

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

## Everyday management

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

The screenshot shows a management console interface. At the top, there are navigation tabs: 'All' (4), 'Windows' (4), 'Apply Policy', 'Create Investigation', 'Discover Endpoints', and 'More Actions'. Below this, a summary bar shows: 4 Total, 1 Active, 1 Inactive, 2 Unmonitored, and 0 Isolated. A 'Create Group' button is visible. The main area displays a table of endpoints with the following data:

Endpoint Name	IP Address	Operating System	Policy	Sensor Version	Alerts	AD	Group
Endpoint-100	10.1.1.100	Windows 10 (v1903)	Alert Test Successful	3.51.10	93	-	0 Groups
Endpoint-101	10.1.1.101	Windows 10 (v1903)	Alert Test Unmonitored	3.51.10	0	-	0 Groups
Endpoint-102	10.1.1.102	Windows 10 (v1903)	Alert Test Inactive since Sep 10, 2019	3.51.10	226	-	0 Groups
Endpoint-103	10.1.1.103	Windows 10 (v1809)	Alert Test Unmonitored	3.51.10	14	-	0 Groups

At the bottom right of the screenshot, it says 'Last Updated: Sep 20, 2019 5:46:29 PM UTC'.

The Endpoints page (shown above) gives a view of all the managed clients. You can select and sort by name, IP address, OS version, policy applied, sensor version, alerts and groups. From here, you can choose a range of endpoints and then run tasks on them. These include applying a new policy, 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 event type, 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, Resolve, Dismiss, Start Investigation, Isolate Host, 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 are involved, and so forth. This is very important for understanding how the current analysis is progressing.

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

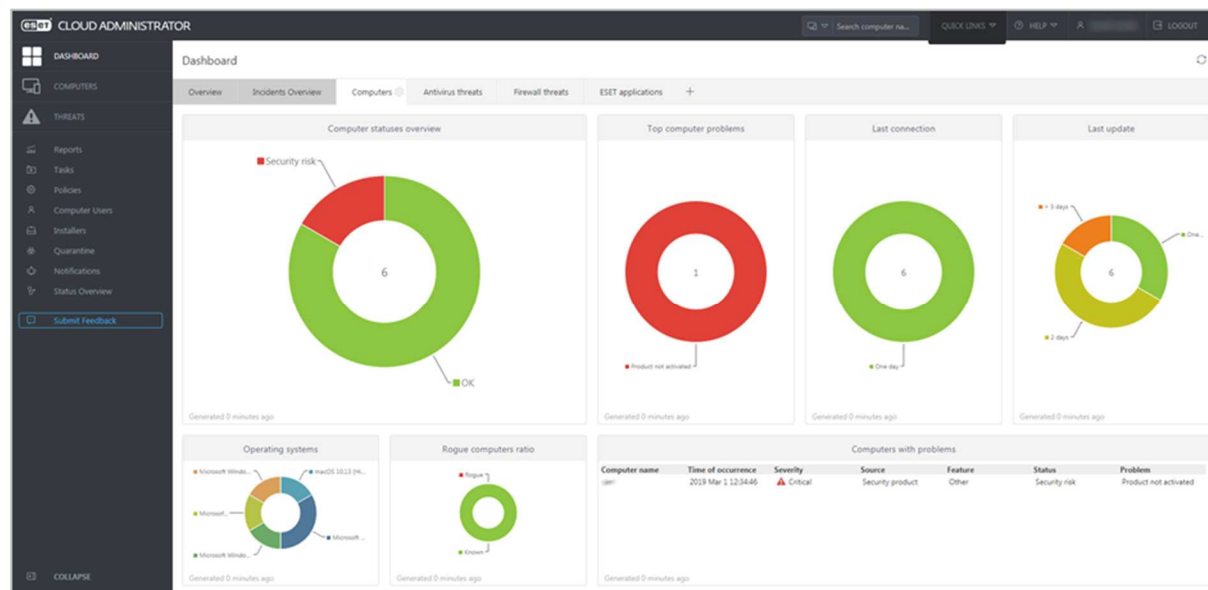
Finally, the Administration menu item gives access to the Policy Settings, Users, Sensors, Alerts, Whitelist and Platform features. The Policy Settings page lets you define policy for events such as privilege escalation, process injection, and credential access. As an example, you can choose what policy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

### Windows endpoint protection software

The Windows desktop and server protection software is essentially invisible to the user. Malware is detected on file copy, and is quarantined. An example alert is shown below. This takes the form of a banner running across the screen. The user cannot take any action, other than to close the alert.



## 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 first 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 (6)	192.168.0.227	✓		Updated	2019 Feb 28 23:02:27	0	90	ESET Endpoint Security	7.0.2100.4
	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	1		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 shutting down the computer.

*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.

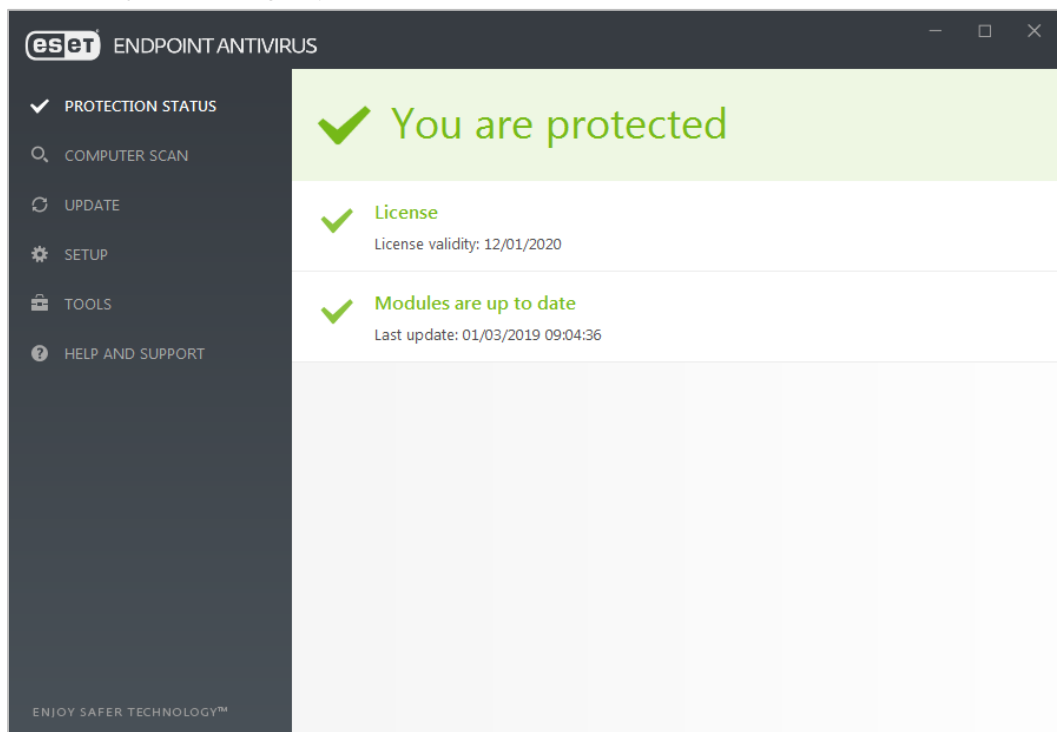
*Computer Users* allows you to create users, add contact details, and link them to devices.

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.

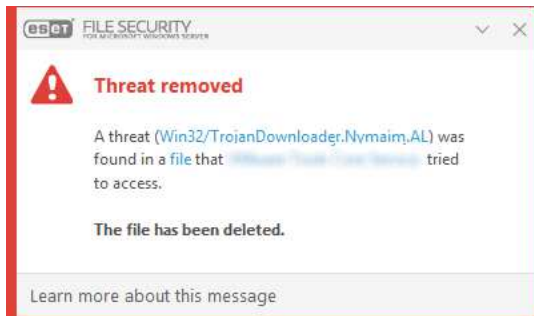
### Windows endpoint protection client

By default, the Windows desktop protection software has a full GUI. 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.

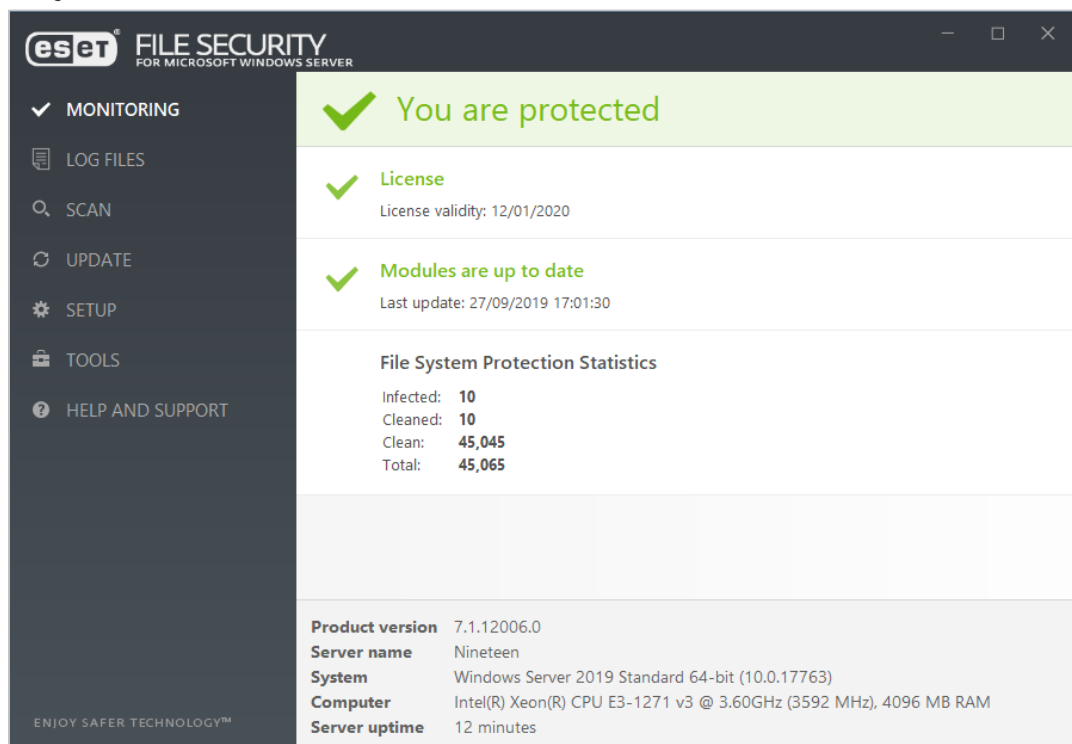




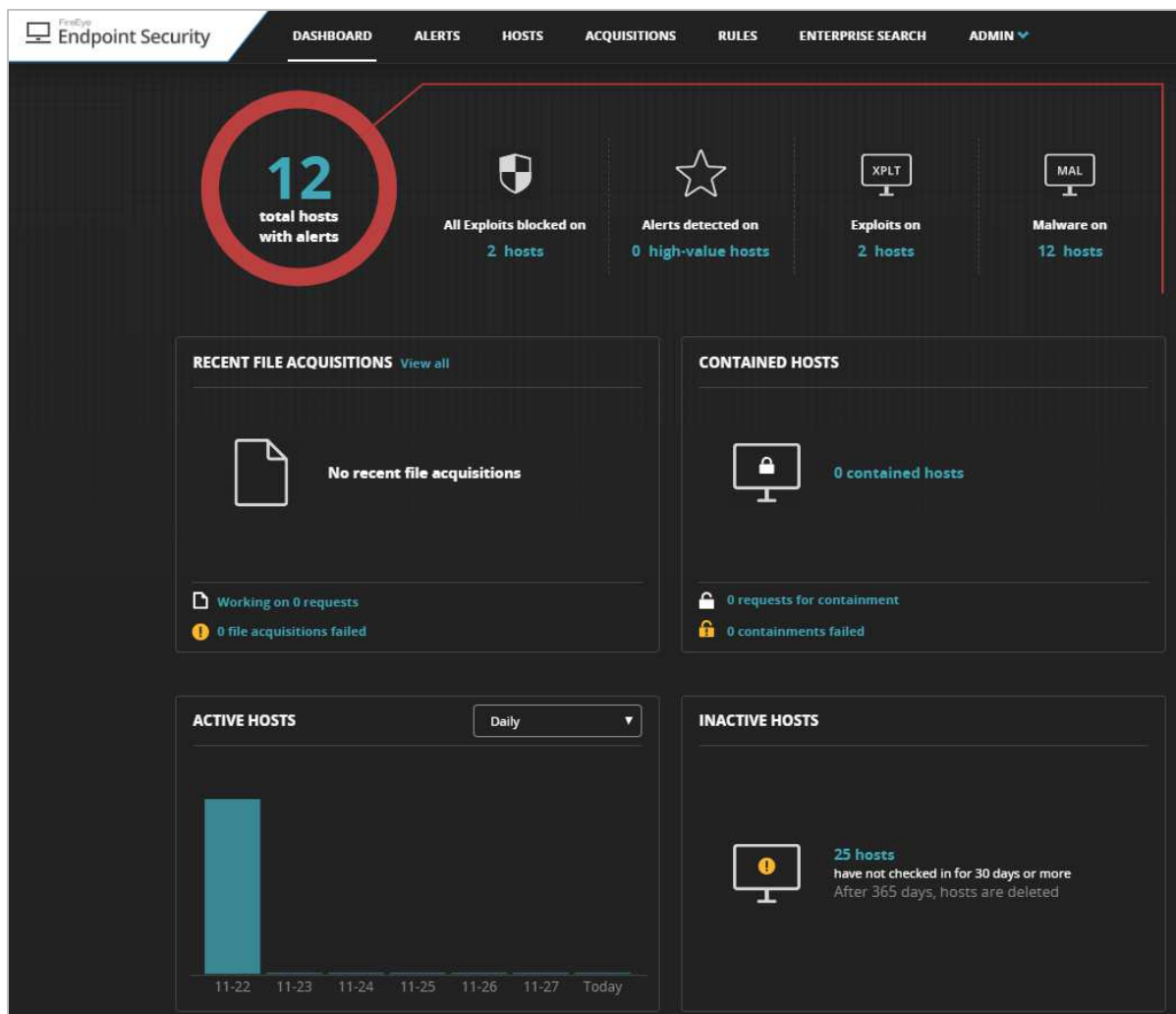
Malware is detected on file copy, and is quarantined. An example alert is shown below. The user cannot take any action, and the alert closes after a few seconds.



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



## FireEye Endpoint Security



### Verdict

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

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

### About the product

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

## Getting up and running

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

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

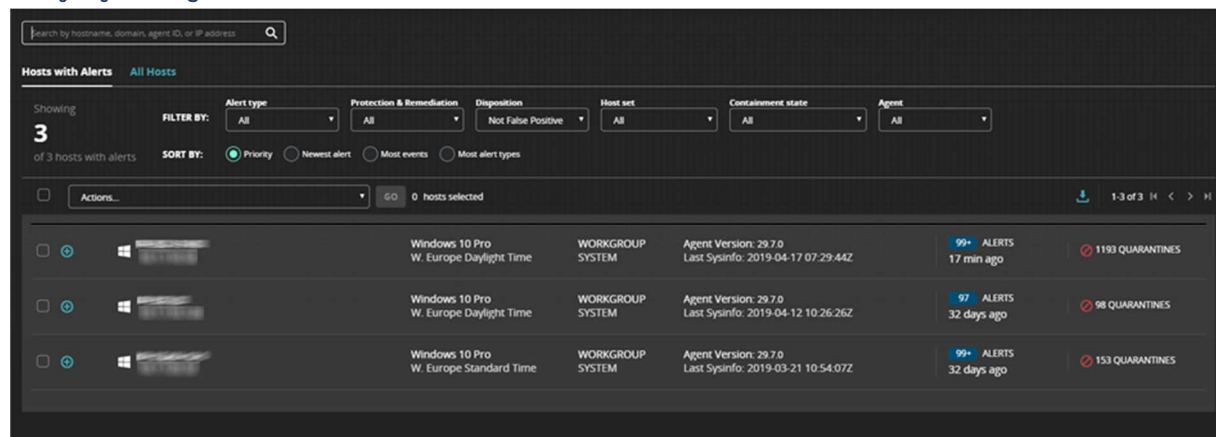
The platform has an extremely powerful and extensive set of information gathering tools. These allow you to build comprehensive queries of almost any type. These are then dispatched to the clients. Analysing this information is the core of the server product.

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

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

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

## Everyday management



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

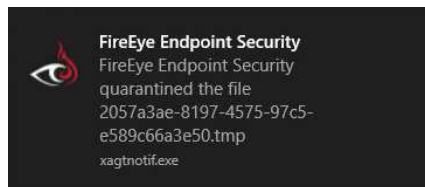
Firstly, you need to understand what FireEye is trying to achieve. It relies on threat detection, plus data gathering and analysis. The emphasis here is solidly on information acquisition, analysis and reporting. This allows the administrator to gather information from a wide array of client machines.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

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

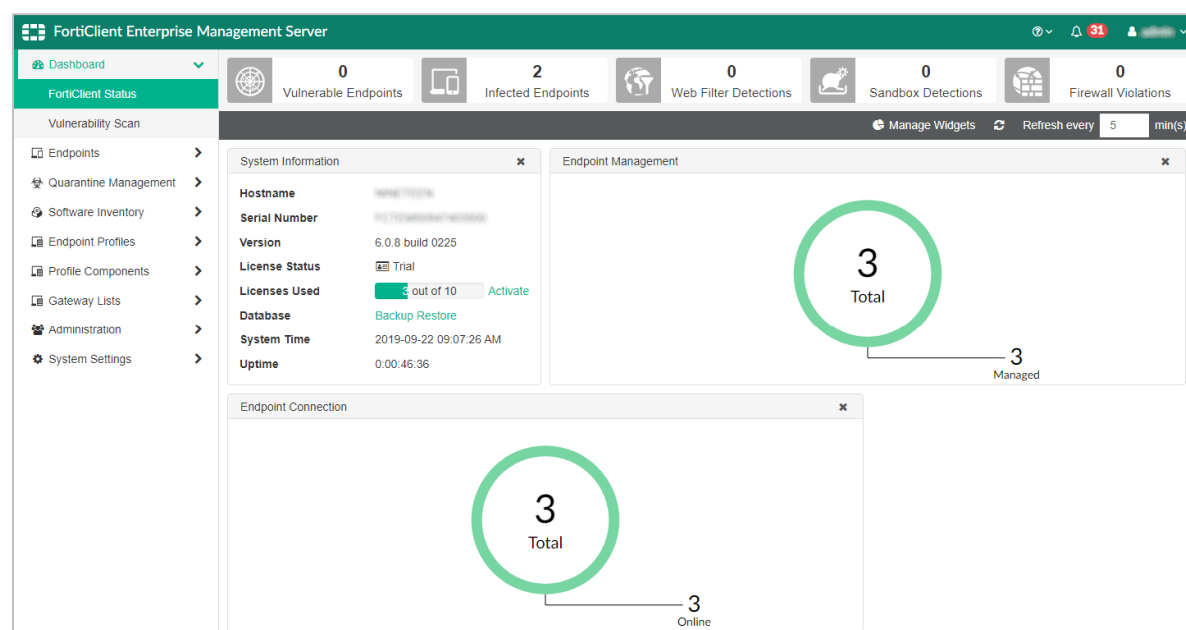
It should not be underestimated how much technical and systems knowledge is required to get the best from this. This is not a criticism. Indeed, for a hard-core IT administrator, it is a great strength to have access to this level of query and analysis of the network.

### Windows endpoint protection software

The Windows desktop and server protection software does not provide any user interface. Malware is detected on file copy, and is quarantined. An example alert is shown below. The user cannot take any action, and the alert closes after a few seconds.



## Fortinet FortiClient with Enterprise Management Server & FortiSandbox



### Verdict

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

### About the product

The server-based console is called FortiClient 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. The console functionality can be accessed from the desktop shortcut (dedicated window), or a web browser. Once up and running, there are some tasks you need to perform before the client can be deployed. The real-time protection feature of the endpoint protection software is disabled in the default policy. However, it is very simple to switch it on under *Endpoint Profiles/Default*.

You can then deploy the client to the desktop. The installer can be downloaded by browsing to the server's URL or [www.forticlient.com](http://www.forticlient.com). If you get the setup file from the server, it will connect automatically to EMS. Otherwise 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 that are not part of the management structure, and it is easy to remediate this. There is a clear and clean view of the status of the network through the *Dashboard/FortiClient Status* view.

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

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

### Everyday management

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

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

Device	User	IP	Profile	Management	AV Status
Apple	[User Icon]	192.168.1.100	Default	Managed by EMS	No Events
Windows	[User Icon]	192.168.1.101	Default	Managed by EMS	AV 11
Windows	[User Icon]	192.168.1.102	Default	Managed by EMS	AV 18

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.

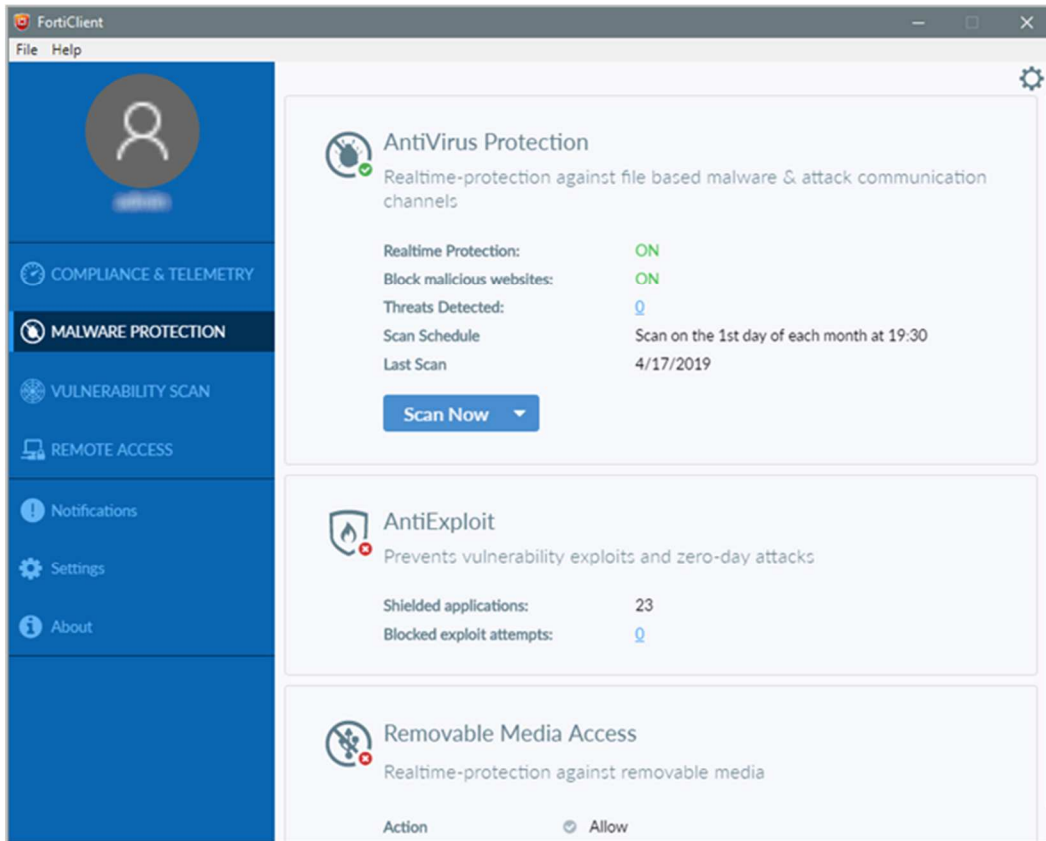
*Endpoint Profile* lets you build up the policy to be pushed to a user's computer. It is quite straightforward and obvious what needs to be done here. There is a *Basic/Advanced* view button which is helpful if you want to dig into the details, or stay with a more simplified view.

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

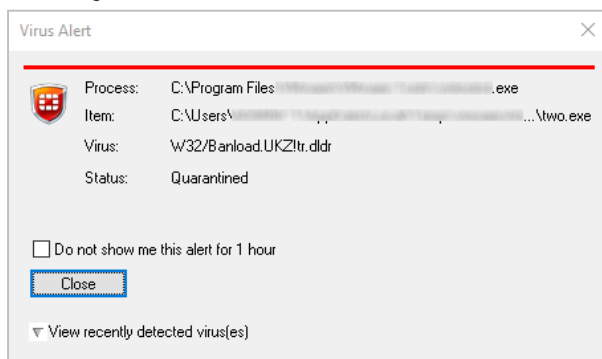
It is fairly straightforward to get reports of what is happening, and initiate scans or remedial actions as required. The UI is quite well designed, but would benefit from some final polish to make it more obvious. A stronger splitting of setup from day-to-day and from system administration would help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

### Windows endpoint protection software

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



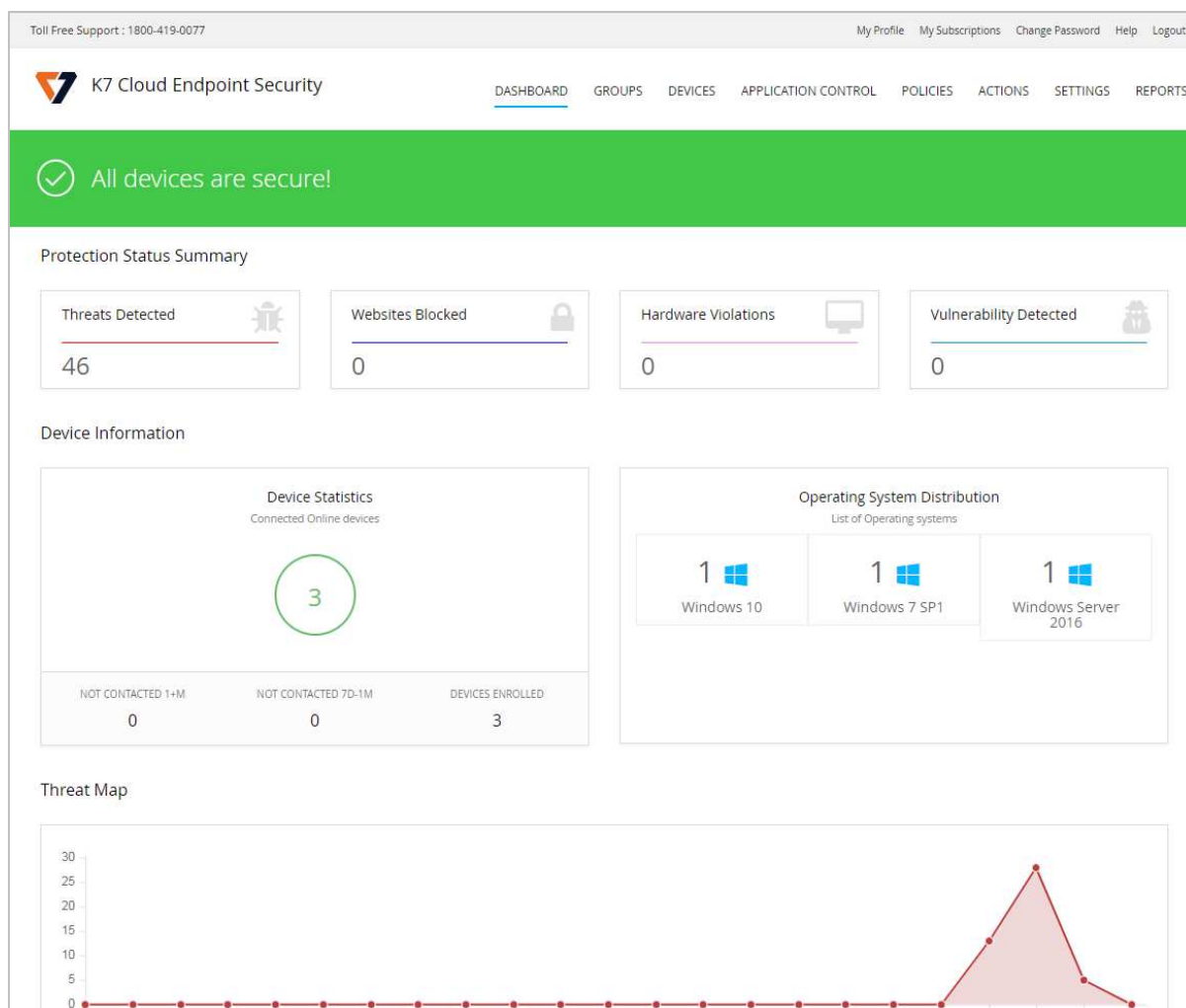
Malware is detected on file copy, and is quarantined. An example alert is shown below. The user cannot take any action, other than to close the alert.



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



## 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, uninstall Endpoint Security on it, or view its details.

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

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

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

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

The *Settings* page 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

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

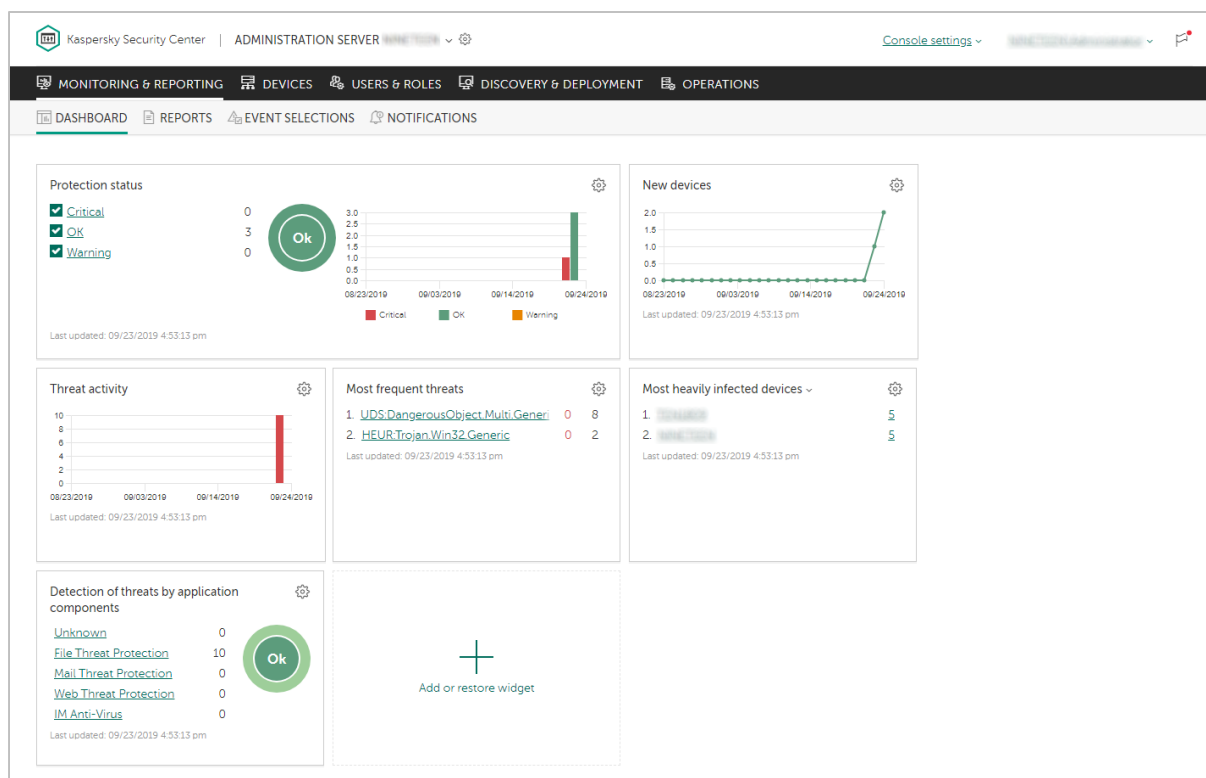


Should the user inadvertently try to copy malware to the system, it is immediately detected on access, and deleted. An example alert is shown below. The user cannot take any action, and the alert closes after a few seconds.



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

## Kaspersky Endpoint Security for Business Select



### Verdict

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

### About the product

Kaspersky Endpoint Security for Business Select uses server-based management functionality. It supports management of endpoint software for Windows, Mac, and Linux desktops, plus Windows and Linux servers. There is also support for Android and iOS mobile devices. A dual management interface is available. Users have the choice of a web-based console (please see screenshot above), or an MMC-based console too. We have looked at the web-based console in this review. You can find a description of the MMC-based console in the report of our July 2019 Business Security Test. Users might like to compare the different interfaces, to decide which one best suits their needs.

### Getting up and running

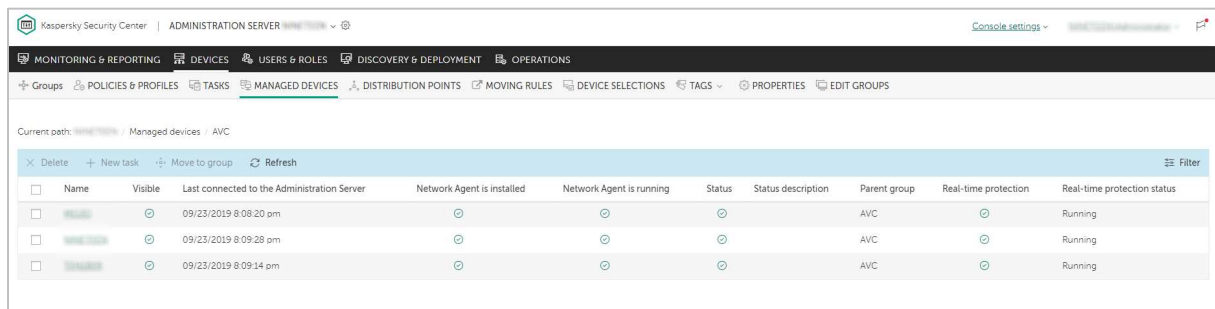
Installing the management console is a straightforward process for an experienced administrator. An SQL database is required, which could be the free Microsoft SQL Server Express. You can use Windows credentials to log in to the console if you want. When you first run the web-based console, an optional brief tutorial is shown. This highlights the most important functions, and provides a brief description of each. Next, the *Quick Start Wizard* takes you through initial configuration. The steps are: product activation, configuration of notifications, and proxy server settings. Finally, the *Protection Deployment Wizard* lets you set up remote push software installation. You can also install clients manually (there are three different methods of doing this).

## Everyday management

The console functions are arranged in two menu bars across the top of the page. The upper menu bar shows the main functionality areas. These are *Monitoring & Reporting*, *Devices*, *Users & Roles*, *Discovery & Deployment*, and *Operations*. The lower menu bar provides access to the sub-pages of each major menu item. In some cases, the items on the lower menu bar open drop-down lists of further items. The *Monitoring and Reporting \ Dashboard* page provides a graphical overview of important items. These include protection status, new devices, plus details of threats and infected devices. Please see the screenshot above. The *Reports* page lets you run a wide variety of reports, on topics such as protection status, deployment, updates and threats. These can be easily accessed from a preconfigured list.

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

The *Devices* tab, *Managed Devices* page lists managed computers, along with the status of major components. You can filter the list using criteria such as operating system, real-time protection or last time seen. By selecting individual devices, you can run tasks on them. These include installation, deinstallation, or changing group membership.



<input type="checkbox"/>	Name	Visible	Last connected to the Administration Server	Network Agent is installed	Network Agent is running	Status	Status description	Parent group	Real-time protection	Real-time protection status
<input type="checkbox"/>	AVC	<input checked="" type="radio"/>	09/23/2019 8:08:20 pm	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>		AVC	<input checked="" type="radio"/>	Running
<input type="checkbox"/>	AVC	<input checked="" type="radio"/>	09/23/2019 8:09:28 pm	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>		AVC	<input checked="" type="radio"/>	Running
<input type="checkbox"/>	AVC	<input checked="" type="radio"/>	09/23/2019 8:09:14 pm	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>		AVC	<input checked="" type="radio"/>	Running

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

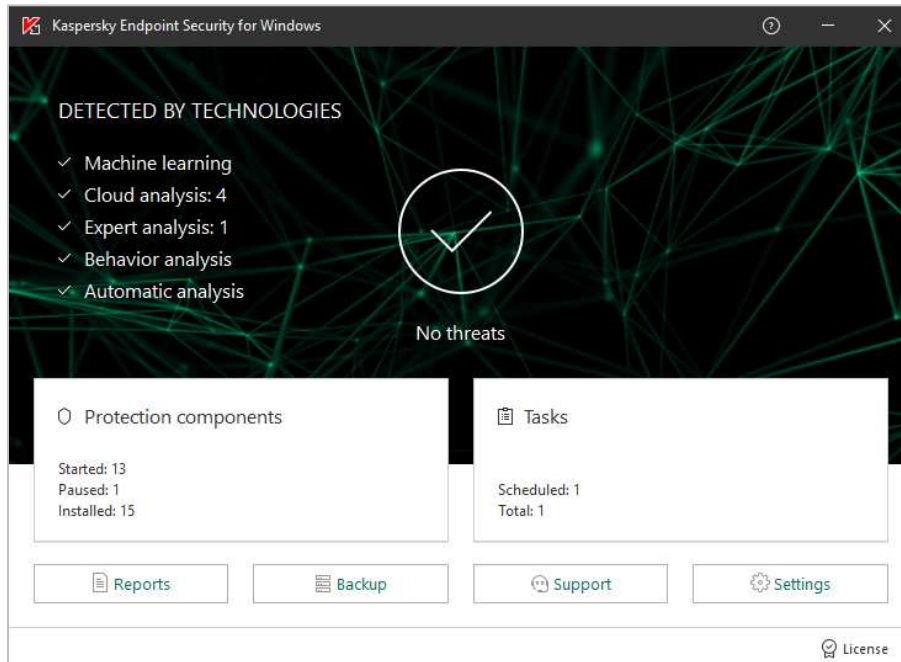
Under *Users & Roles*, you can see a list of predefined console users, along with Windows local and domain accounts for the Windows computers on the network. These can be assigned one of 16 different management roles for the console, allowing very granular access.

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

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

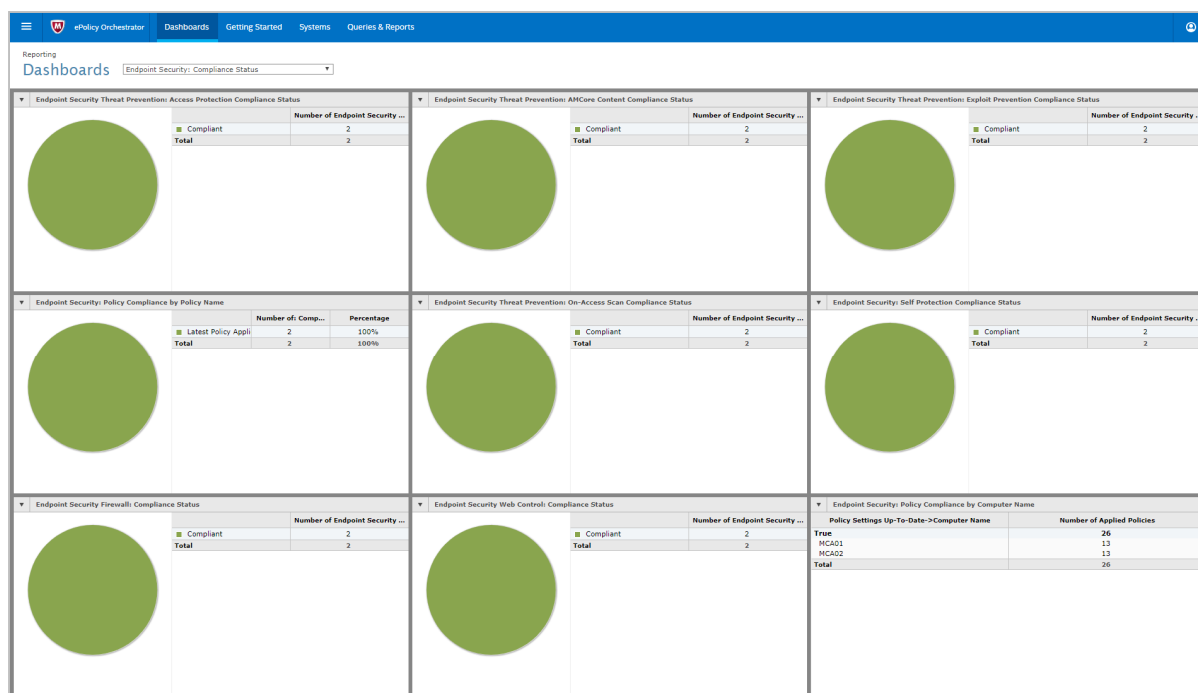
### Windows endpoint protection software

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



Malware is detected on file copy and quarantined. No alert is shown. The GUI of the server protection software is identical to that of the client.

## 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 means that everyday management functions 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. These include areas such a *Compliance Status*, *Protection Summary* and *Web Control Activity*. The *Systems* tab, shown below, lists all installations together with their status, IP address and last communication timestamp.

System Name	Managed State	Tags	IP address	Last Communication
Workstation	Managed	Workstation	192.168.1.100	23/09/19 05:05:08 EDT
Server	Managed	Server	192.168.1.101	27/09/19 14:03:38 EDT
Workstation	Managed	Workstation	192.168.1.102	27/09/19 14:04:09 EDT

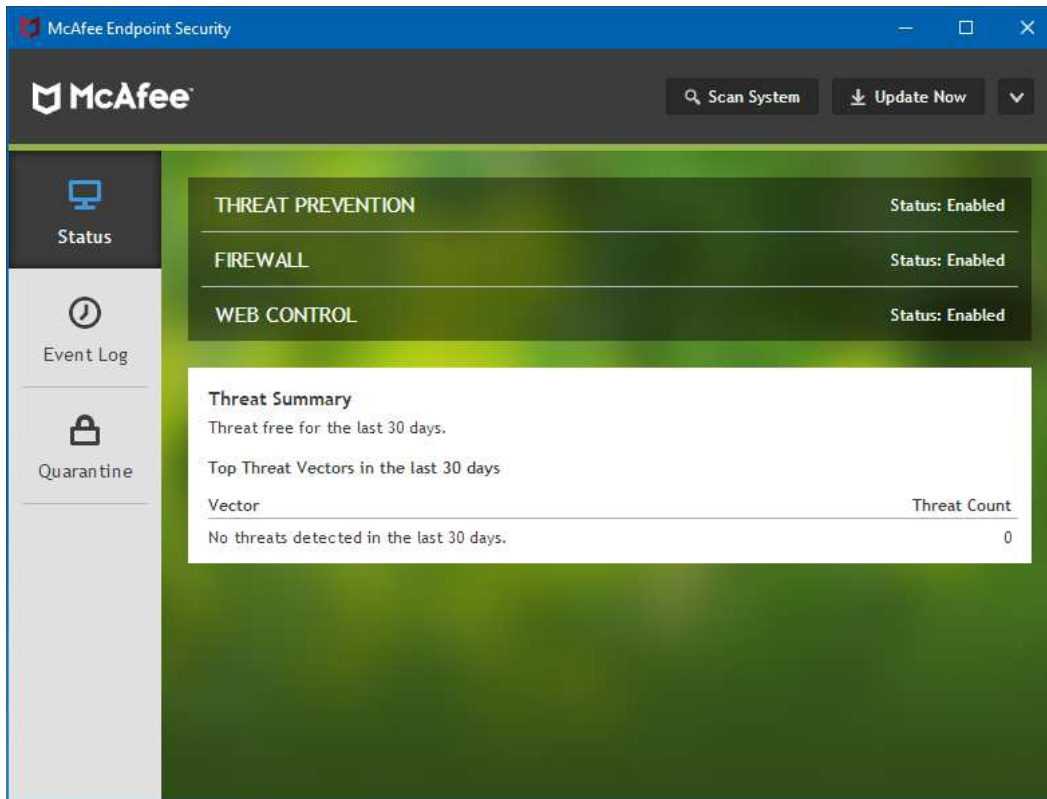
We found one aspect of the GUI to be unclear here. All of the date/time stamps in the management console appear to be on Eastern (Daylight) Time zone. We feel it is far from obvious to the first-time user how to change the time zone to a local one.

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.

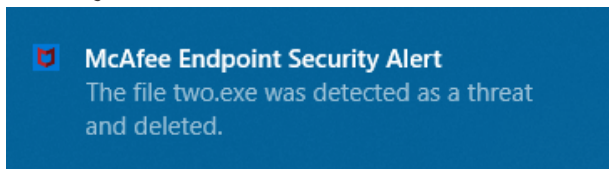
It should be noted that in general, ePO Cloud becomes easier to use the more you become familiar with it. Admins using ePO Cloud for the first time should bear in mind that time spent learning about how it works will pay dividends later on. There are a number of ways that daily tasks can be made easier 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 Windows desktop protection software provides scanning and updating functions, and shows the status of each protection component. Most other controls – such as the event logs and quarantine – are disabled by default for standard users.

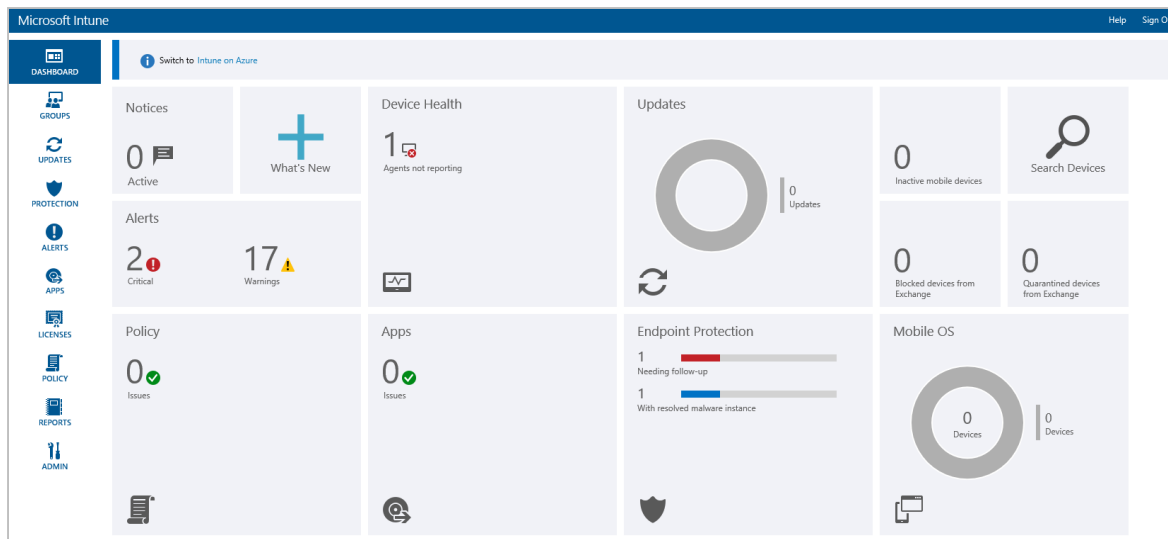


Malware is detected on file copy, and quarantined. An example alert is shown below. The user cannot take any action, and the alert closes after a few seconds.



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

## Microsoft Windows Defender Antivirus for Business with Intune



### Verdict

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

### About the product

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

### Getting up and running

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

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

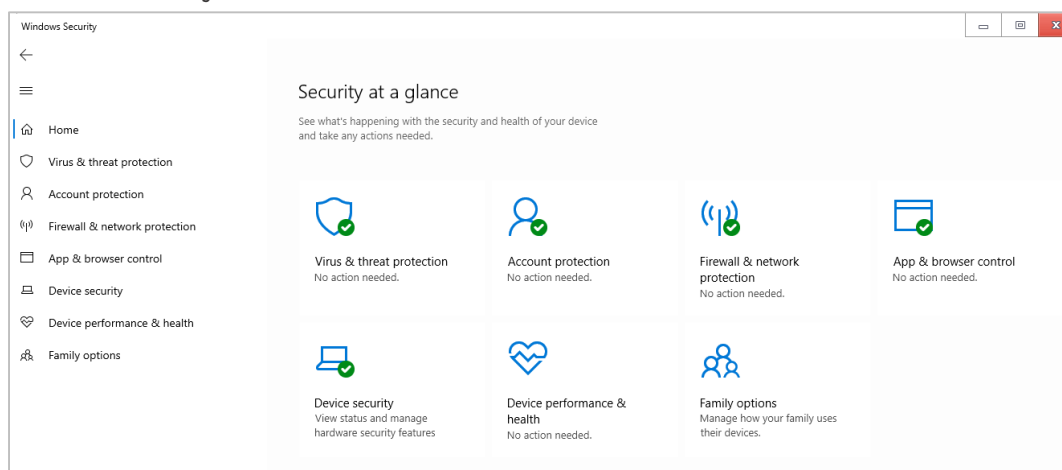
## Everyday management

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

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

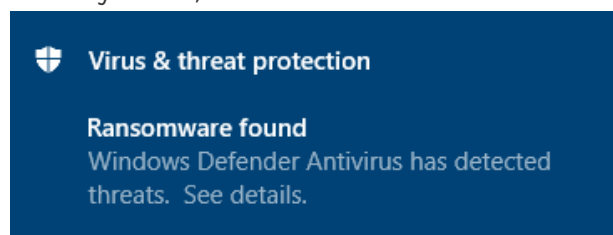
## Endpoint protection software

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



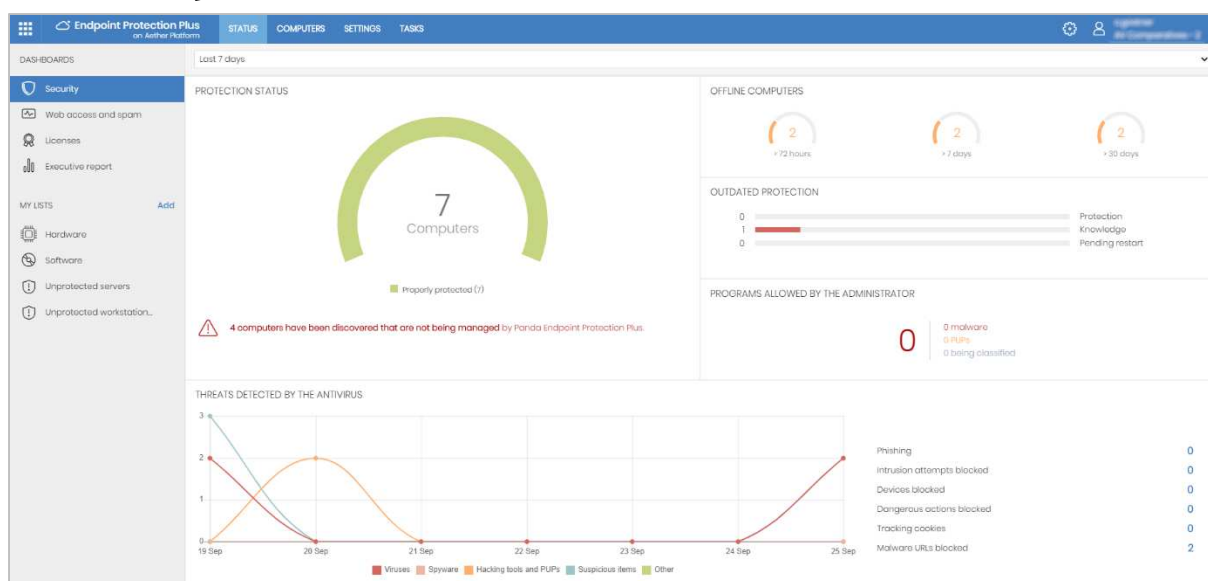
Older versions of Windows, including Windows 7 and 8.1, use the same GUI as Microsoft Security Essentials. This is similar to that of a typical consumer antivirus program. All variants allow the user to update malware definitions, and run full, quick, custom and context-menu scans.

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



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

## Panda Endpoint Protection Plus on Aether



### Verdict

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

### About the product

This is a cloud-console managed system. There are device clients for Windows 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 using the *Add Computers* button on the *Computers* page. You can download the installer directly, or click on *Send by email*. This opens an email message with a link for download and installation. This works for Windows, Linux and Android. The user clicks on the provided link to install the client, and this is then automatically licensed. Either installation method lets you pre-allocate the client to a management group.

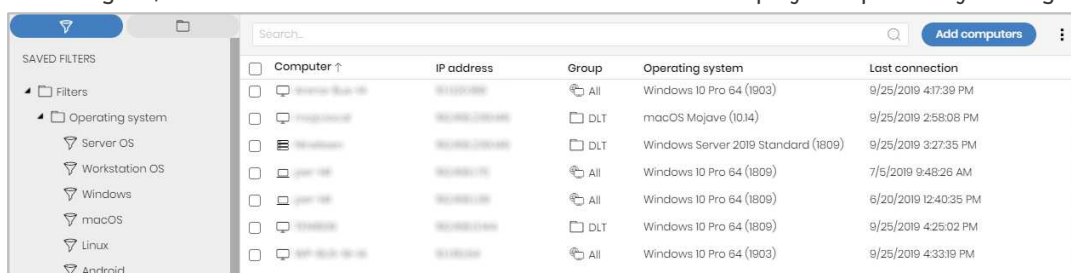
### Everyday management

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

The *Status* tab includes a left-hand menu column, from which you can open additional status pages.

*Web access and spam* shows categories of website, such as webmail, games and business, which users have accessed. *Executive Report* lets you quickly create reports. Subjects include licence status, security status, detections, plus web access and spam. You can choose any or all of these categories, and select the time period and groups of computers. *Licenses* is self-explanatory. A section called *My Lists* provides simple but useful overviews of different aspects of the network. There are links for hardware and software of managed computers, plus lists of unprotected workstations and servers. This list is customisable, and a number of other categories can be added. These include computer protection status, threats detected by AV, and web access by computer.

The *Computers* tab, shown below, lists computers on the network. You can filter by various criteria, including OS, hardware and installed software. You can also display computers by management group.



Computer	IP address	Group	Operating system	Last connection
Windows Server 2019 Standard (1809)	10.10.10.10	All	Windows 10 Pro 64 (1803)	9/25/2019 4:17:39 PM
MacBook Pro	10.10.10.11	DLT	macOS Mojave (10.14)	9/25/2019 2:58:08 PM
Windows Server 2019 Standard (1809)	10.10.10.12	DLT	Windows Server 2019 Standard (1809)	9/25/2019 3:27:35 PM
Lenovo	10.10.10.13	All	Windows 10 Pro 64 (1809)	7/5/2019 9:48:26 AM
Lenovo	10.10.10.14	All	Windows 10 Pro 64 (1809)	6/20/2019 12:40:35 PM
Lenovo	10.10.10.15	DLT	Windows 10 Pro 64 (1809)	9/25/2019 4:25:02 PM
HP EliteBook	10.10.10.16	All	Windows 10 Pro 64 (1803)	9/25/2019 4:33:19 PM

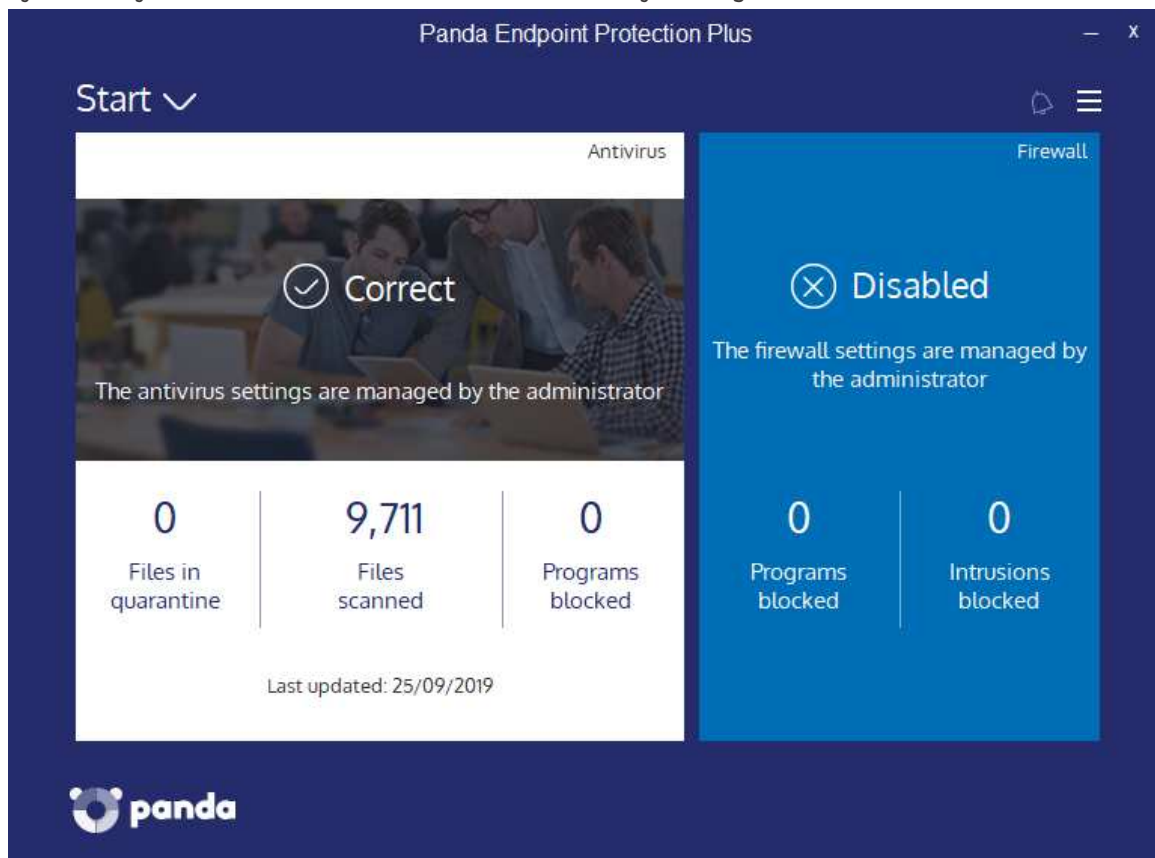
This page shows all the protected computers and mobile devices. It is very clearly laid out, and shows essential information. A Windows-like folder tree on the left lets you show devices by group.

Using the *Settings* tab/*Users* page, you can create console users and assign them full control or read-only access. The *Security* section lets you define separate security policies for computers and Android mobile devices. Under *My Alerts* you can set up email notifications for various items. These include malware and phishing detections, unlicensed/unmanaged/unprotected/unlicensed computers, and installation errors. Other settings pages let you manage updates and proxy servers etc.

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

### Windows endpoint protection software

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



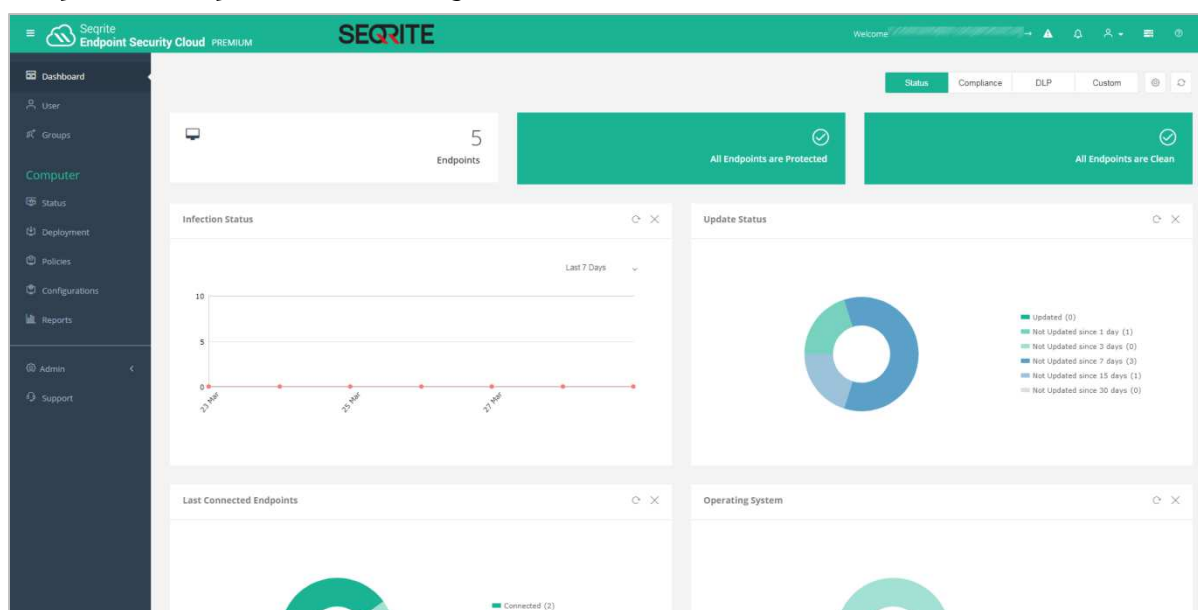
Malware is detected on file copy, and is quarantined. An example alert is shown below. The user cannot take any action, and the alert closes after a few seconds.



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



## Seqrite Endpoint Security Cloud



### Verdict

Seqrite Endpoint Security Cloud provides an easy-to-navigate cloud console. There is 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. Thus, the service is accessible from 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 infection status, update 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		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] [Redacted]	[Redacted]	WORKGROUP	Default_MSSP	14 Mar 2019 [16:50:33]	18 Mar 2019 [21:49:22]
<input type="checkbox"/>	[Icon] [Redacted]	[Redacted]	WORKGROUP	Default_MSSP	20 Mar 2019 [12:43:06]	21 Mar 2019 [16:22:02]
<input type="checkbox"/>	[Icon] [Redacted]	[Redacted]	WORKGROUP	Default_MSSP	28 Mar 2019 [16:49:13]	29 Mar 2019 [18:03:35]
<input type="checkbox"/>	[Icon] [Redacted]	[Redacted]		Default_MSSP	13 Nov 2018 [10:07:00]	29 Mar 2019 [18:17:16]
<input type="checkbox"/>	[Icon] [Redacted]	[Redacted]	WORKGROUP	Default_MSSP	18 Mar 2019 [11:45:20]	29 Mar 2019 [08:30:44]
<input type="checkbox"/>	[Icon] [Redacted]	[Redacted]	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. This includes 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 clients. 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.

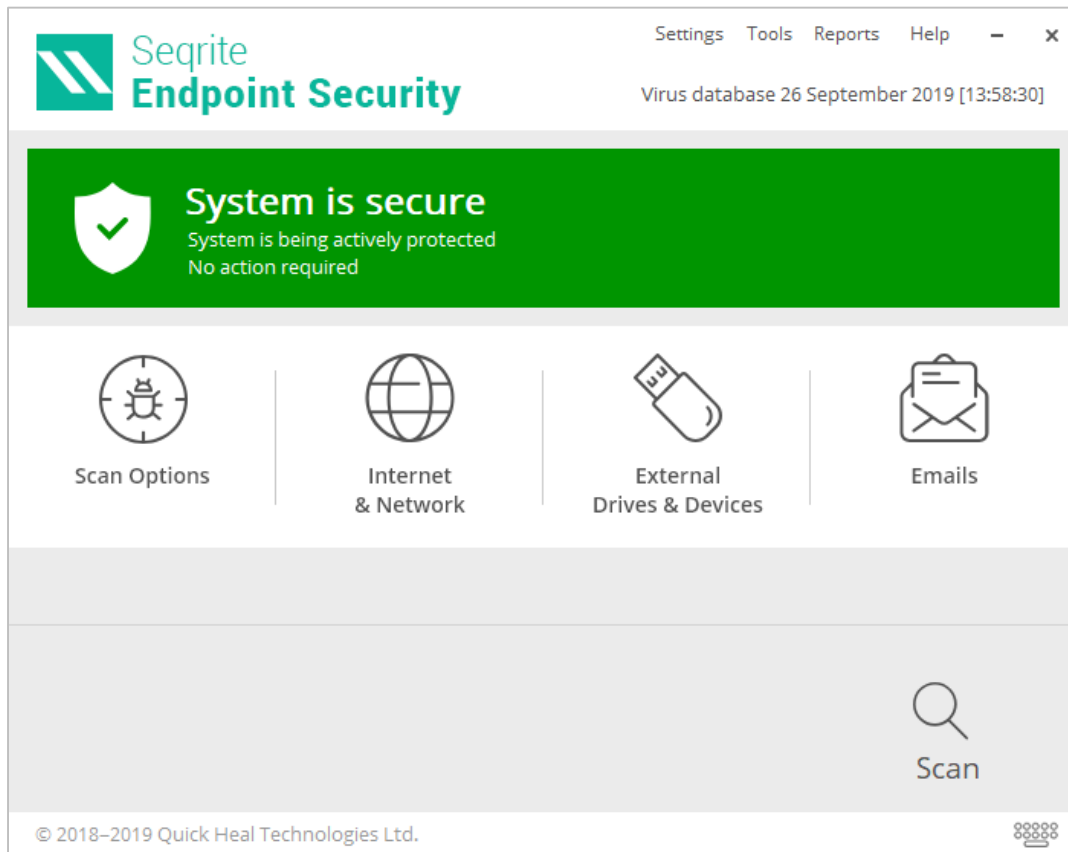
Under *Configurations*, there are options for the device control and application control features. You can also specify the installation path for Windows clients.

*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.

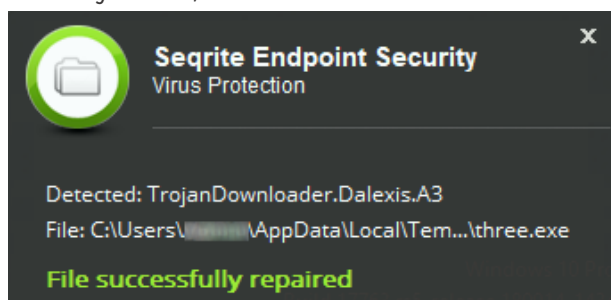
The *Admin* section covers things like licences, console users and their specified roles, plus notifications.

## Windows endpoint protection software

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

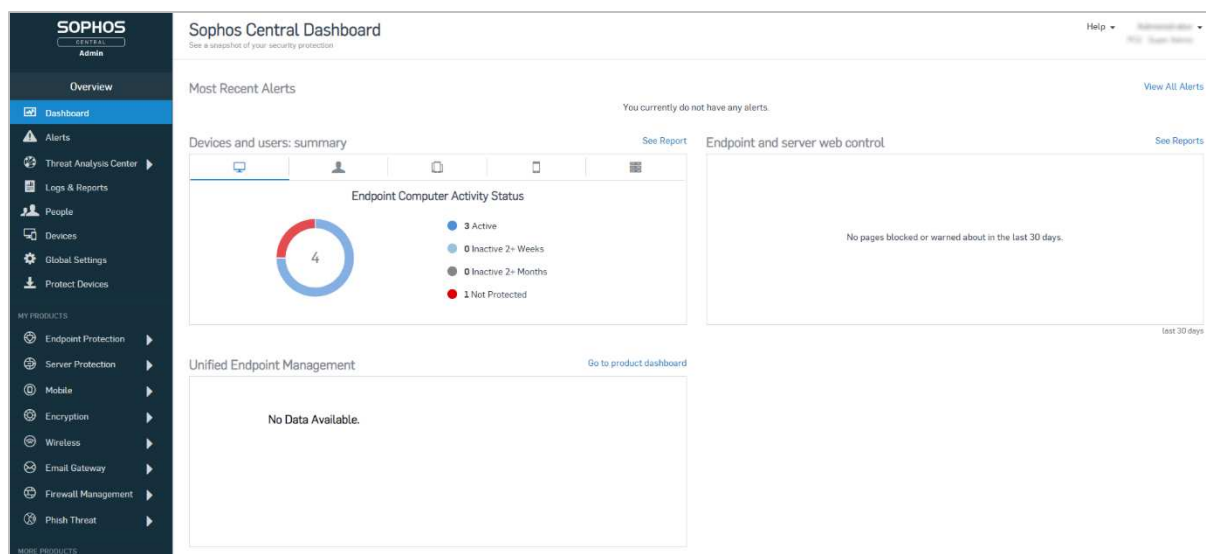


Malware is detected on file copy, and is deleted. An example alert is shown below. The user cannot take any action, and the alert closes after a few seconds.



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

## Sophos Intercept X Advanced



### Verdict

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

### About the product

Sophos Intercept X Advanced uses a cloud console (Sophos Central) to manage Windows clients and servers, 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.

### Getting up and running

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

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

## Everyday management

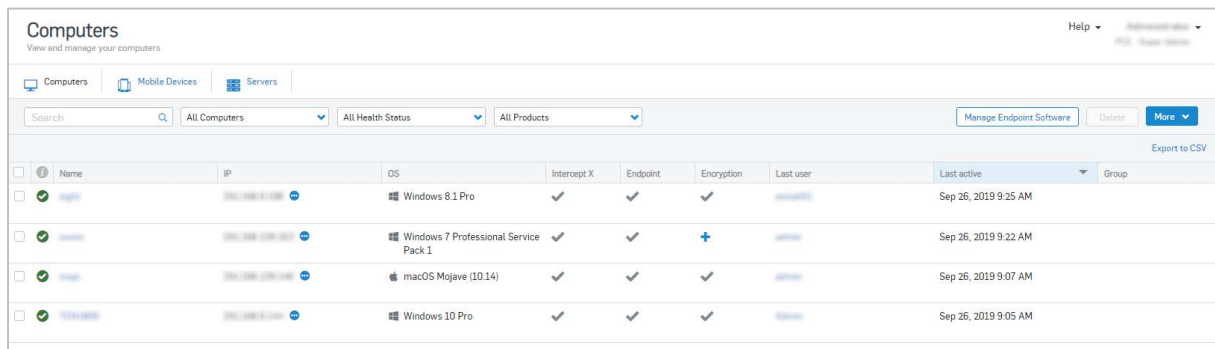
The *Sophos Central Dashboard* view is quite straightforward. It has a clean, uncluttered user interface, offering an overview of all the systems and protection capabilities. Here you can see how many endpoints are active, the most recent alerts, and statistics on the web URL access management.

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

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

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

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

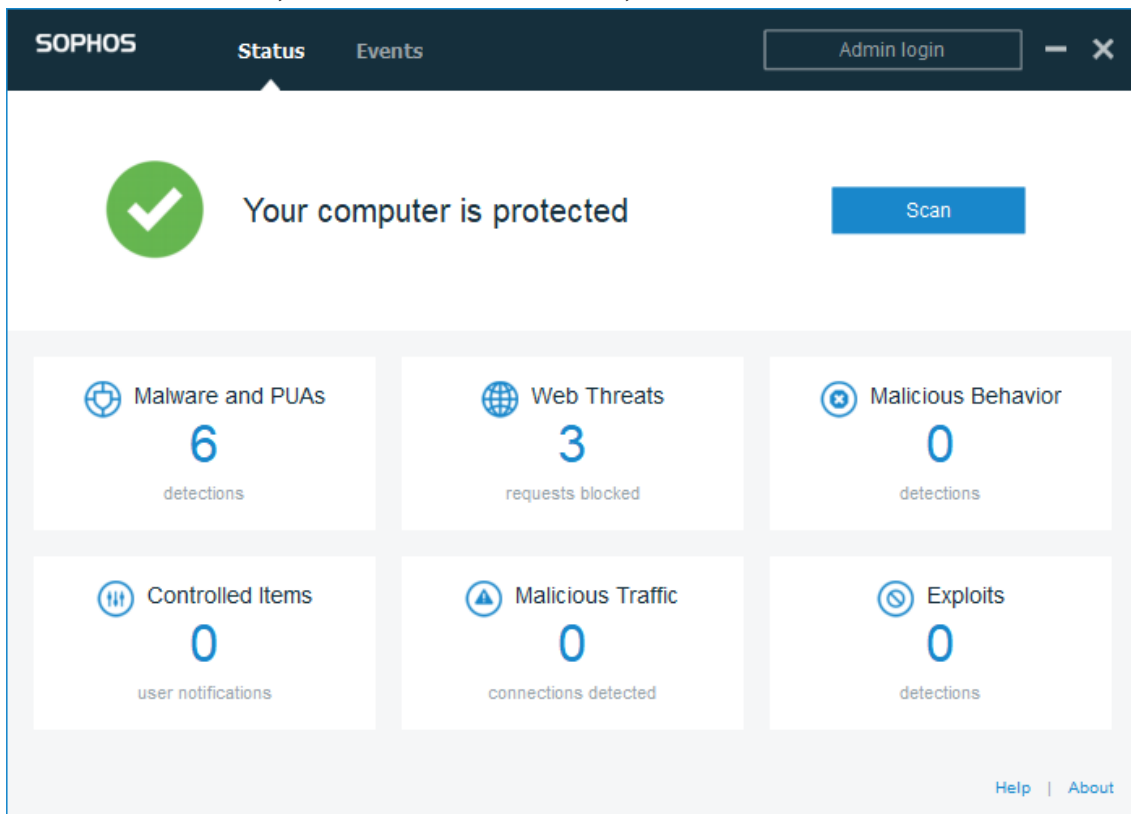


<input type="checkbox"/>	Name	IP	OS	Intercept X	Endpoint	Encryption	Last user	Last active	Group
<input type="checkbox"/>	192.168.1.100	192.168.1.100	Windows 8.1 Pro	✓	✓	✓	admin	Sep 26, 2019 9:25 AM	
<input type="checkbox"/>	192.168.1.101	192.168.1.101	Windows 7 Professional Service Pack 1	✓	✓	+	admin	Sep 26, 2019 9:22 AM	
<input type="checkbox"/>	192.168.1.102	192.168.1.102	macOS Mojave (10.14)	✓	✓	✓	admin	Sep 26, 2019 9:07 AM	
<input type="checkbox"/>	192.168.1.103	192.168.1.103	Windows 10 Pro	✓	✓	✓	admin	Sep 26, 2019 9:05 AM	

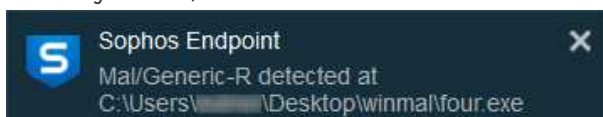
*Endpoint Protection* takes you to another set of user interface and menus. This also has pages for *Dashboard*, *Logs and Reports*, *People* and *Computers* menu items. Here you can also configure policies, settings and download endpoint installation packages.

## Windows Endpoint Protection Software

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

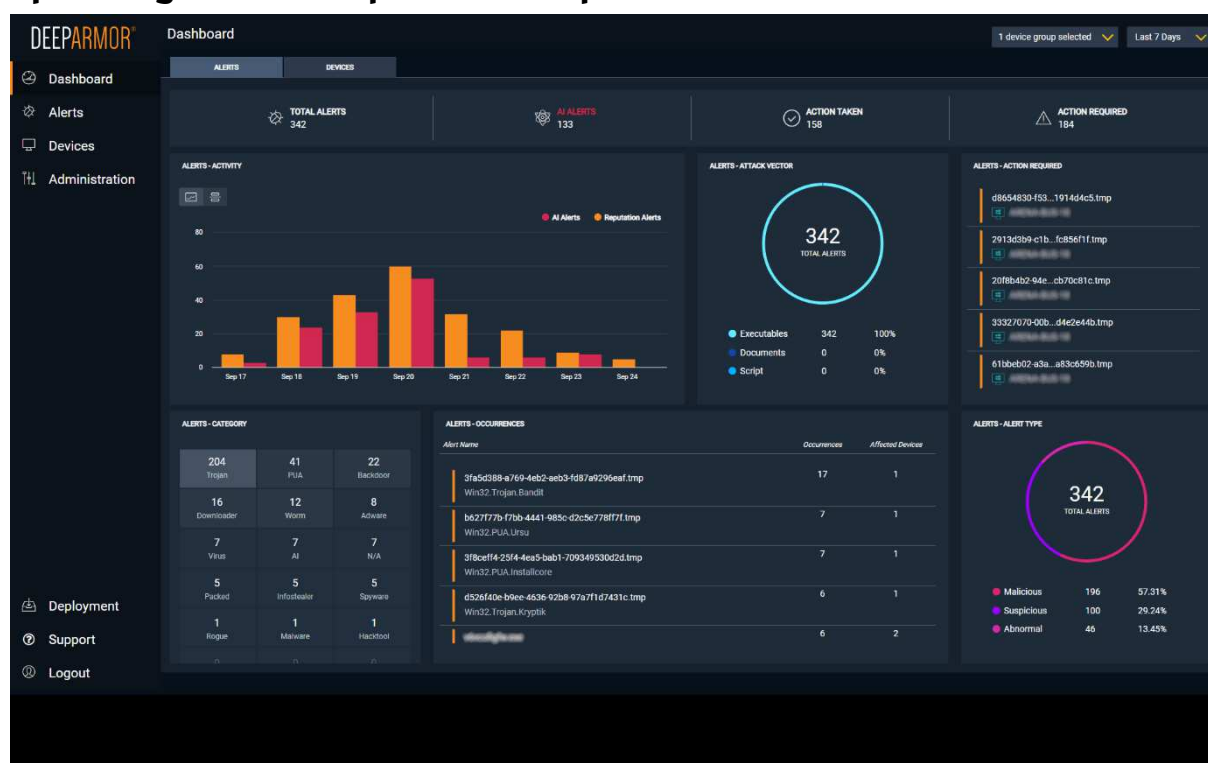


Malware is detected on file copy, and is deleted. An example alert is shown below. The user cannot take any action, and the alert closes after a few seconds.



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

## SparkCognition DeepArmor Endpoint Protection Platform



### Verdict

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

### About the product

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

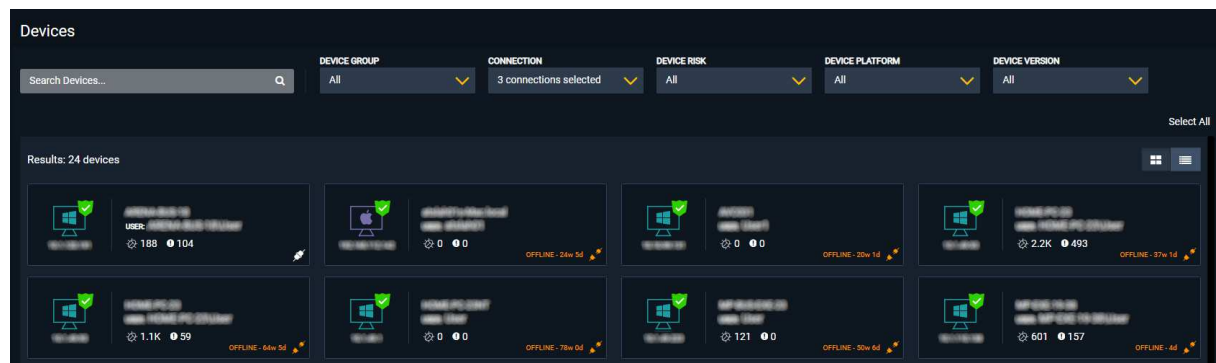
### Getting up and running

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

### Everyday management

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





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

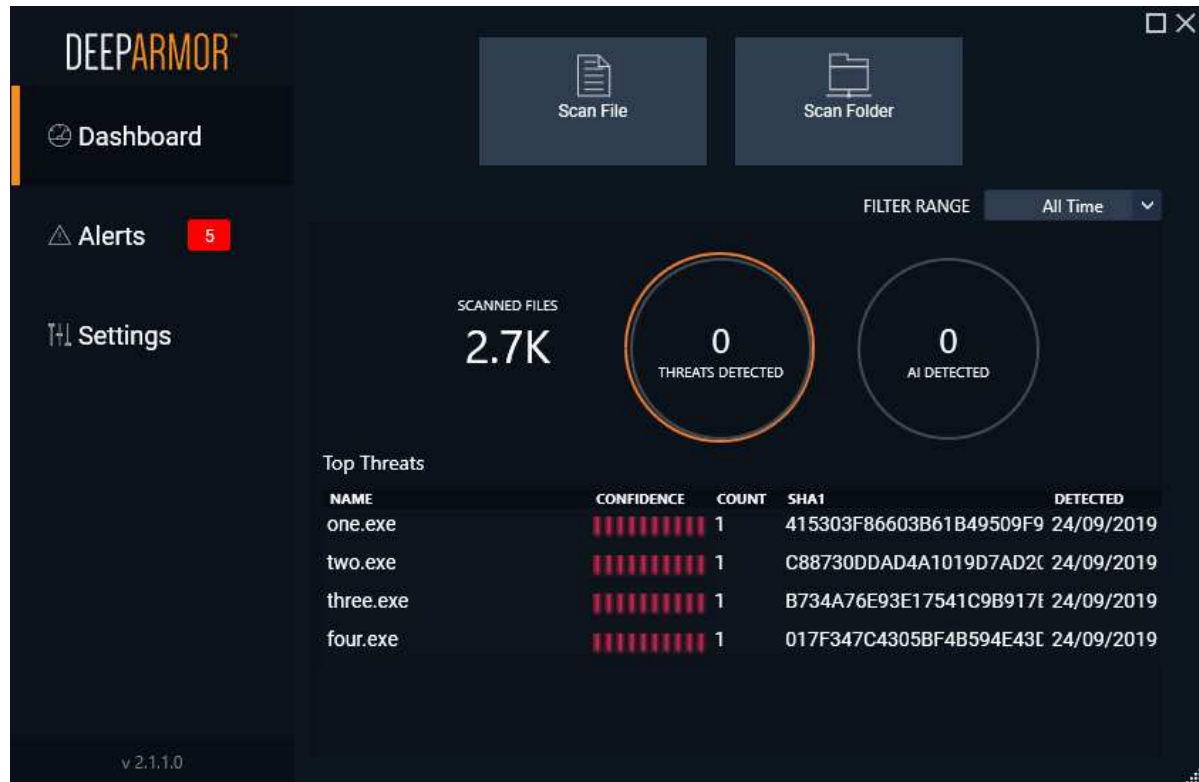
The *Alerts* page shows recent alerts, along with details. These include the file name of the malware, how it was detected, detection name, “confidence” (probability that the file really is malicious), name of affected device, time of detection, action taken or required, and file hash. Sub-tabs of each file’s details page show all detections of the file across the network (*Occurrences*). There are also further details of the file, as well as the device on which it was detected. The *Take Action* button provides the options *Remote Remediate*, *Remote Restore*, and *External Remediate*. These allow the admin to take immediate action.

The *Administration* menu includes the submenus *Users*, *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. You can manage the latter from the *Device Groups* page. *Device Policies* also lets you define whitelisted folders, i.e. ones you want to exclude from malware detection. 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.

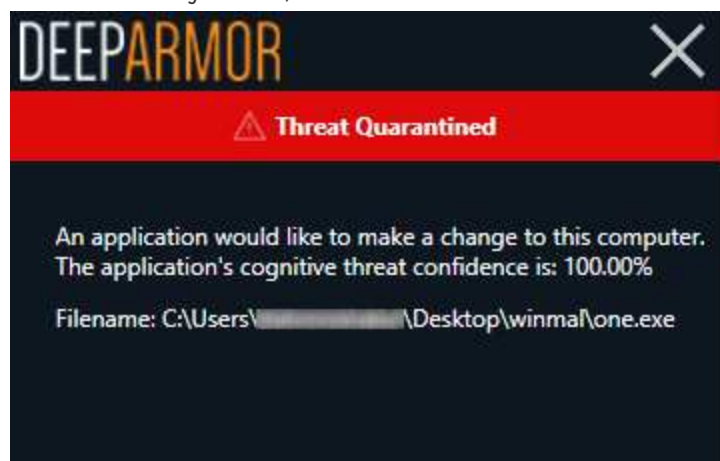
On the *Deployment* page you can find installers for Window, macOS, and various different Linux distributions. The *User Guide* can also be found here. Finally, *Support* links to the support page on the vendor’s website.

### 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 shows the current configuration options for the program. By default, these are deactivated for all users.



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



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

## 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 and macOS clients and Windows servers. VIPRE Endpoint Security is the client that runs on the desktop. VIPRE tell us that the cloud service runs on the Amazon AWS cloud, and that this brings efficiency, scalability and growth.

### Getting up and running

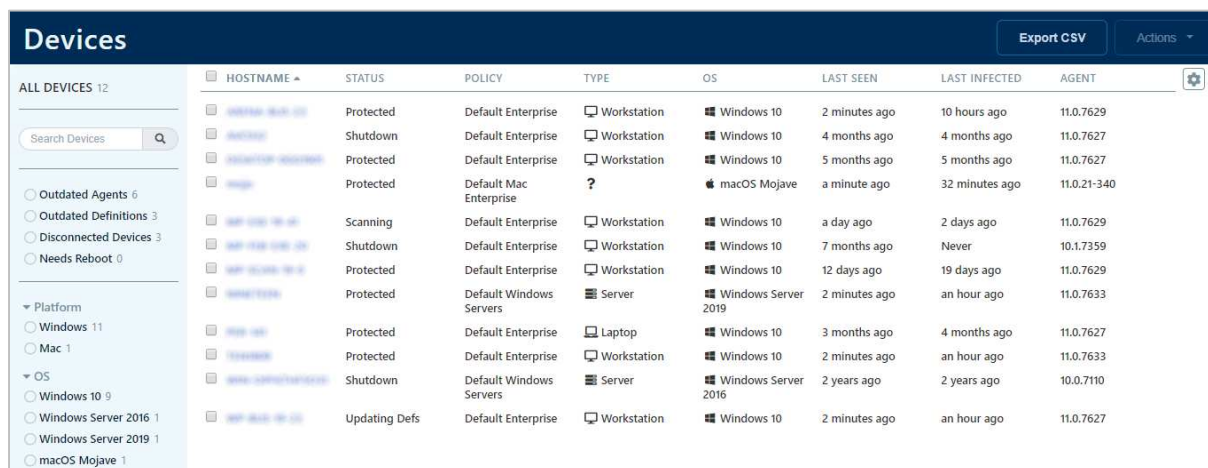
Access to the web portal is straightforward via a standard username/password login combination (two-factor authentication is also available). The user interface immediately impresses with its clean and clear design. The first page you see has a *Getting Started* area. This covers deploying of agents,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

## Everyday management

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

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

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



ALL DEVICES 12		HOSTNAME	STATUS	POLICY	TYPE	OS	LAST SEEN	LAST INFECTED	AGENT
<input type="checkbox"/>	192.168.1.101	Protected	Default Enterprise	Workstation	Windows 10	2 minutes ago	10 hours ago	11.0.7629	
<input type="checkbox"/>	192.168.1.102	Shutdown	Default Enterprise	Workstation	Windows 10	4 months ago	4 months ago	11.0.7627	
<input type="checkbox"/>	192.168.1.103	Protected	Default Enterprise	Workstation	Windows 10	5 months ago	5 months ago	11.0.7627	
<input type="checkbox"/>	192.168.1.104	Protected	Default Mac Enterprise	?	macOS Mojave	a minute ago	32 minutes ago	11.0.21-340	
<input type="checkbox"/>	192.168.1.105	Scanning	Default Enterprise	Workstation	Windows 10	a day ago	2 days ago	11.0.7629	
<input type="checkbox"/>	192.168.1.106	Shutdown	Default Enterprise	Workstation	Windows 10	7 months ago	Never	10.1.7359	
<input type="checkbox"/>	192.168.1.107	Protected	Default Enterprise	Workstation	Windows 10	12 days ago	19 days ago	11.0.7629	
<input type="checkbox"/>	192.168.1.108	Protected	Default Windows Servers	Server	Windows Server 2019	2 minutes ago	an hour ago	11.0.7633	
<input type="checkbox"/>	192.168.1.109	Protected	Default Enterprise	Laptop	Windows 10	3 months ago	4 months ago	11.0.7627	
<input type="checkbox"/>	192.168.1.110	Protected	Default Enterprise	Workstation	Windows 10	2 minutes ago	an hour ago	11.0.7633	
<input type="checkbox"/>	192.168.1.111	Shutdown	Default Windows Servers	Server	Windows Server 2016	2 years ago	2 years ago	10.0.7110	
<input type="checkbox"/>	192.168.1.112	Updating Defs	Default Enterprise	Workstation	Windows 10	2 minutes ago	an hour ago	11.0.7627	

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

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

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

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

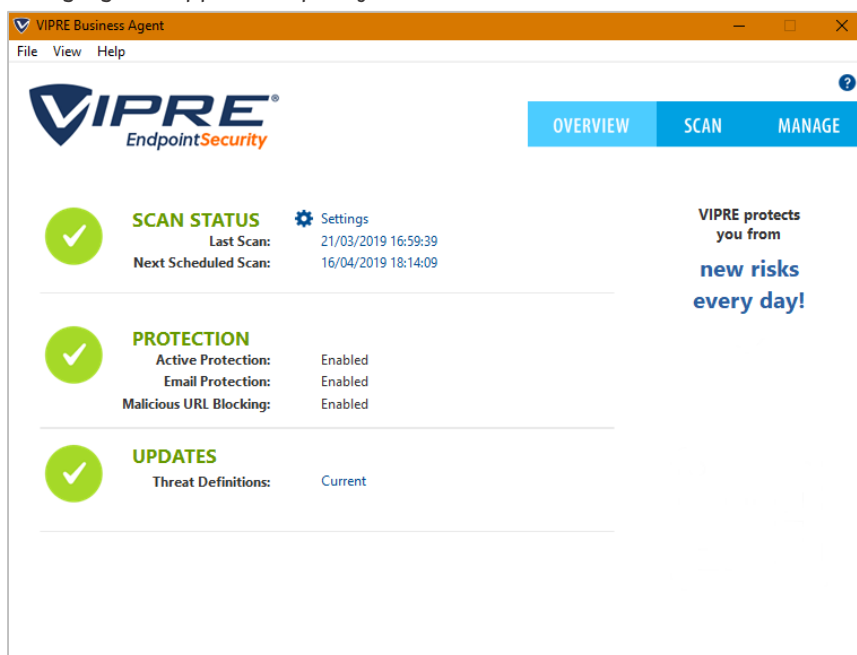
The web console impresses both from the initial setup and deployment through to the ongoing management. The defaults are sensible, the screens clear and clean, and it is obvious what it is reporting and how healthy the clients are. It is simple to get clients to do centrally managed tasks, and the configuration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

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

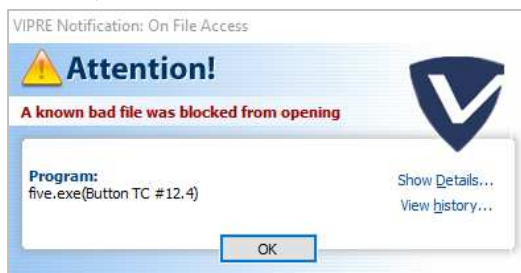
We would say the platform is appropriate for any size of company, from a small business with a few seats, through to a much larger organisation. The UI of the management console was always responsive under testing. It is built to cope with thousands of desktops and large numbers of events.

### Windows endpoint protection software

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



Malware is detected on file copy, and is quarantined. An example alert is shown below. The user cannot take any actions, other than to close the alert.



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

Features (as of November 2019)	Avast Business Antivirus Pro Plus	Bitdefender Endpoint Security Elite (GravityZone Elite HD)	Cisco AMP for Endpoints	CrowdStrike Endpoint Protection Platform Standard Bundle	Elastic Endpoint Security	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	Seqrite Endpoint Security	Sophos Intercept X Advanced	SparkCognition DeepArmor Endpoint Protection Platform	VIPRE Endpoint Security Cloud	
<b>Available Console Types</b>																		
Cloud-based console	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	
On-premise server-based console	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	
Virtual appliance	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	
<b>Client software deployment methods</b>																		
Creation of .exe or .msi installer package	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	
Email a link to remote users to install the software themselves	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	
Push installation from the console	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	
<b>Supported Operating Systems</b>																		
Microsoft Windows	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	
Virtual environments (such as VMware, HyperV)	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	
Apple macOS	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	
Linux	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	
Google Android	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	
Apple iOS	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	
<b>Windows Features</b>																		
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	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	
<b>Languages</b>																		
Which languages can be used to contact support?	English, Czech, Japanese, French, German, Portuguese, Norwegian	English, Spanish, German, Romanian, French	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, 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		English, Japanese			English	
<b>Pricing (based on LIST PRICES as of November 2019; depending on the number of agents purchased, deal size or term, country/region, volume and competitive upgrade, discounts will apply/vary)</b>																		
<b>999 clients, 3 years, Relative Prices (from Very Low to Very High)</b>																		
Cloud-based console		Average	High	High		N/A		N/A	Low	Average	Average	Very High	Average		Average	High	Average	
On-premise Windows-based console	Average	N/A					High											
Virtual appliance		Average	Very High	N/A	Average	Low		N/A	N/A	N/A	High	N/A	N/A	Average	N/A	N/A	N/A	
<b>Minimum number of seats</b>																		
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  
(December 2019)