Anti-Virus Comparative

Business Security Test

Language: English
March-June 2018

Last revision: 16th July 2018

https://www.av-comparatives.org

Table of content

Introduction 3

Tested Products 4

Settings 5

Management Summary 6

AV-Comparatives' Approved Business Product Award 8

Real-World Protection Test (March-June) 9

Malware Protection Test (March) 14

Performance Test (June) 16

Reviews 21

Avast Business Antivirus Pro Plus 22

Bitdefender Endpoint Security Elite (GravityZone Elite Security HD) 25

CrowdStrike Endpoint Protection Platform Standard Bundle 29

Emsisoft Anti-Malware with Enterprise Console 32

Endgame Protection Platform 35

eScan Corporate 360 with MDM & Hybrid Network Support 38

ESET Endpoint Security and Remote Administrator 41

FireEye Endpoint Security 44

Fortinet FortiClient with Enterprise Management Server & FortiSandbox 47

Kaspersky Endpoint Security for Business Select 50

McAfee Endpoint Security with ATP and ePolicy Orchestrator Cloud 53

Microsoft Windows Defender Antivirus for Business with Intune 56

Panda Endpoint Protection Plus on Aether 59

Saint Security MAX Anti-Virus 62

Trend Micro OfficeScan XG 64

VIPRE Endpoint Security Cloud 67

Feature list 71

Copyright and Disclaimer 72

Introduction

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

Products of 16 different vendors are included in this public test report. The test series consists of three main parts:

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

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

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

In addition to each of the protection tests, a false-positives test is conducted, to check whether any products falsely identify legitimate software as harmful.

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

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. Each vendor decided themselves which product to submit for this test-series.

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

Tested Products

The following business products[2] were tested and reviewed under Microsoft Windows 10 RS3 64-bit:

Vendor	Product	Version March	Version April	Version May	Version June
Avast	Business Antivirus Pro Plus	18.1	18.2	18.2	18.4
Bitdefender	Endpoint Security Elite (GravityZone Elite HD)	6.2	6.2	6.2	6.6
CrowdStrike	Endpoint Protection Platform Standard Bundle	4.0	4.0	4.4	4.7
Emsisoft	Anti-Malware & Enterprise Console	2018.2	2018.3	2018.4	2018.5
Endgame	Endpoint Protection Platform	2.5	2.5	2.6	2.7
eScan	Corporate 360 with MDM & Hybrid Network Support	14.0	14.0	14.0	14.0
ESET	Endpoint Security & Remote Administrator	6.6	6.6	6.6	6.6
FireEye	Endpoint Security	4.0	4.0	4.0	4.0
Fortinet	FortiClient with EMS & FortiSandbox	5.6	5.6	5.6	6.0
Kaspersky Lab	Endpoint Security for Business Select	10.3	10.3	11.0	11.0
McAfee	Endpoint Security with ATP and ePO Cloud	10.5	10.5	10.5	10.5
Microsoft	Windows Defender Antivirus for Business with Intune	4.12	4.12	4.14	4.16
Panda	Endpoint Protection Plus on Aether	7.90	7.90	7.90	7.90
Saint Security	MAX Antivirus	1.0	1.0	1.0	1.0
Trend Micro	OfficeScan XG	12.0	12.0	12.0	12.0
VIPRE	Endpoint Security Cloud	10.1	10.1	10.1	10.1

We congratulate the 16 vendors who are participating in the Business Main-Test Series for having their business products publicly tested by an independent lab, showing their commitment to improving their products, being transparent to their customers and having confidence in their product quality.

[2] Information about additional third-party engines/signatures used by some of the products: **Emsisoft**, **eScan**, **FireEye** and **VIPRE** use the **Bitdefender** engine.

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 allowed 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 did therefore not change any settings. Cloud and PUA[3] detection have been activated in all products.

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

Bitdefender: HyperDetect disabled, Sandbox enabled.

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

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

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

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

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

Microsoft: Cloud protection level set to "High blocking level.

Trend Micro: Behaviour monitoring: "Monitor news 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, **Emsisoft**, **eScan**, **ESET**, **Kaspersky Lab**, **Panda**, **Saint Security**, **VIPRE**: default settings.

---

[3] We do not include any PUA in our malware tests.

Management Summary

AV security software is available for all sizes and types of business. What fits well at the smaller end of the SME (small to medium enterprise) market is probably not going to be quite so appropriate to the larger corporates.

Before deciding on appropriate software to investigate, it is critical to understand the business environment in which it will be used, so that correct and informed choices can be made.

Let's start at the smaller end of the marketplace. These are environments that have often grown out of micro businesses, where domestic-grade AV products might well have been appropriate. But as soon as you start to scale beyond a few machines, the role of AV management comes into sharp focus. This is especially true when you consider the business and reputational damage that could result from a significant, and uncontained/uncontrolled malware outbreak.

However, in the smaller end of the SME space, there is rarely an onsite IT manager or operative. Often the role of "looking after the computers" falls to an interested amateur, whose main role in the business is that of senior partner. This model is often found in retail, accountancy and legal professions. In this space, it is critical to have a managed overview of all the computing assets, and to have instant clarity about the status of the protection delivered in way that is clear and simple. Remediation can be done by taking a machine offline, moving the user to a spare device, and waiting for an IT professional to arrive on site to perform clean-up and integrity checking tasks. Although users might be informed of status, managing the platform is a task for one, or at most, a few, senior people within the organization, often driven by overriding needs for data confidentiality within the company.

In the larger organization, it is expected to have onsite specialist IT staff, and, at the bigger end, staff whose role is explicitly that of network security. Here, the CTO role will be looking for straightforward, but real-time statistics and a management overview which allows for drilling into the data to focus on problems when they arise. There will almost be an explicit role for the software installation engineers, responsible for ensuring the AV package is correctly and appropriately loaded and deployed onto new machines. Knowing when machines "drop off grid" is almost as important here, to ensure that there are no rogue, unprotected devices on the LAN. Finally, there will almost certainly be a help desk role, as a first-line defence, who will be responsible for monitoring and tracking malware activity, and escalating it appropriately. They might, for example, initiate a wipe-and-restart on a compromised computer.

Finally, in this larger, more layered hierarchy, there is a task of remediation and tracking. Knowing that you have a malware infection is just the start. Handling it, and being able to trace its infection route back to the original point of infection, is arguably the most important function in a larger organization. If a weakness in the network security and operational procedure design cannot be clearly identified, then it is likely that such a breach will occur again at some point in the future. For this role, comprehensive analysis and forensic tools are required, with a heavy emphasis on understanding the timeline of an attack or infection from a compromised computer. Providing this information in a coherent way is not easy – it requires the handling of huge amounts of data, and the tools to filter, categorize and highlight issues as they are unfolding, often in real time.

Because of these fundamental differences, it is critically important to identify the appropriate tool for the organization, and the risk profile it is exposed to. Under-specifying this will result in breaches that will be hard to manage. Over-specifying will result in a system of such complexity that no-one truly understands how to deploy, use and maintain it, and the business is then open to attack simply because of the fog of misunderstanding and lack of compliance.

You need to make choices between going for a local-network, server-installed package, or looking at a whole 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.

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

VIPRE's simplicity and clarity make it a very good choice for smaller businesses with limited IT staff resources, although it allows plenty of room to grow. It is limited to the Windows platform, however. **Emsisoft** would be work for companies big enough to have their own full-time IT staff, and going up to larger organisations. It covers Windows devices only. **eScan** and **Trend Micro** are larger, more comprehensive packages that require more learning, deployment and planning.

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.

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

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

The **Saint Security** product would currently only be usable by micro-businesses with half-a-dozen staff in a single office, due to the lack of a central cloud management function. We await the introduction of its cloud-based console, currently under development, to see how it might cope with anything larger.

AV-Comparatives' Approved Business Product Award

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

To be certified in July 2018 as an "Approved Business Product" by AV-Comparatives, the tested products must score at least 90% in the Malware Protection Test, and at least 90% in the overall Real-World Protection Test (i.e. over the course of four months), 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.

Unfortunately, FireEye did not meet the requirements for the July 2018 Approved Award. However, we have been working with the vendor to identify the reasons for this, and hope to see the issues resolved in the second round of tests this year (due in December 2018). All the other participating vendors receive the July 2018 Approved Business Product award.

Real-World Protection Test (March-June)

Malicious software poses an ever-increasing threat, not only due to the number of malware programs increasing, but also due to the nature of the threats. Infection vectors are changing from simple file-based methods to distribution via the Internet. Malware is increasingly focussing 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 of 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 also conventional and non-cloud features such as the signature-based and heuristic detection abilities of antivirus programs 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 Whole-Product Dynamic "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. Some further installed software includes: Adobe Flash, Adobe Acrobat Reader, Apple QuickTime, Google Chrome, Oracle Java and VideoLAN VLC Media Player. 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 perform 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).

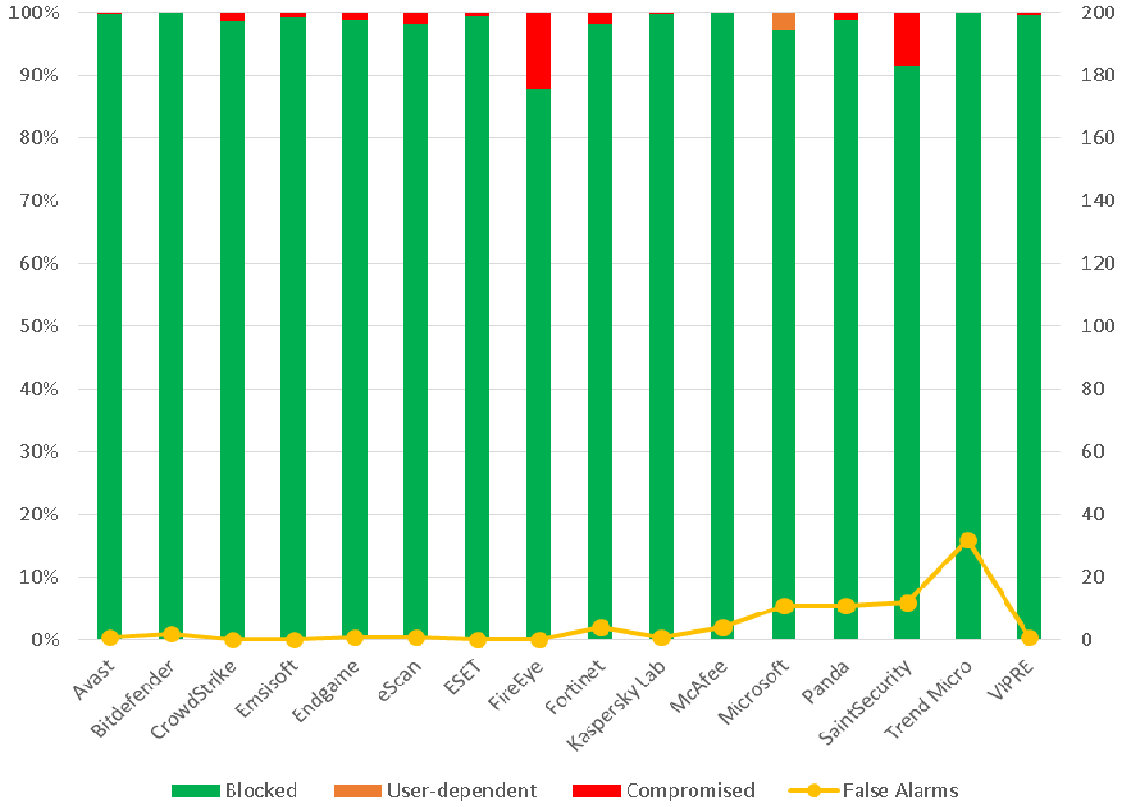
Due to the dynamic nature of the test, i.e. mimicking real-world conditions, and because of the way several different technologies (such as cloud scanners, reputation services, etc.) work, it is a matter of fact that such tests cannot be repeated or replicated in the way that e.g. static detection rate tests can. Anyway, we log as much data as reasonably possible to support our findings and results. Vendors are invited to provide 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 maybe some 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 would mean the PCs are being exposed to higher risks.

Test Set

We aim to use visible and relevant malicious websites/malware that are currently out there, and 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 **1163** test cases (such as malicious URLs), tested from the beginning of March till the end of June[4].



	Blocked	User dependent	Compromised	PROTECTION RATE [Blocked % + (User dependent %)/2][5]	False Alarms
Bitdefender	1163	-	-	**100%**	2
McAfee	1163	-	-	**100%**	4
Trend Micro	1163	-	-	**100%**	32
Kaspersky Lab	1161	-	2	**99.8%**	1
Avast	1160	-	3	**99.7%**	1
VIPRE	1159	-	4	**99.7%**	1
ESET	1156	-	7	**99.4%**	0
Emsisoft	1155	-	8	**99.3%**	0
Endgame	1151	-	12	**99.0%**	1
Panda	1150	-	13	**98.9%**	11
CrowdStrike	1149	-	14	**98.8%**	0
Microsoft	1132	31	-	**98.7%**	11
eScan	1142	-	21	**98.2%**	1
Fortinet	1142	-	21	**98.2%**	4
Saint Security	1065	-	98	**91.6%**	12
FireEye	1021	-	142	**87.8%**	0

[4] During May testing, Panda had a bug in their products, which caused some few malware samples to be reported in the logs, but not being blocked or warned about – the bug was rapidly fixed.

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

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

The false-alarm test in the Whole-Product Dynamic "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 not only risk 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 do not care whether they are infected by malware that affects only them, just as they do not care if the FP count 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.

Microsoft, **Panda**, **Saint Security** and **Trend Micro** had an above-average number of FPs in the Real-World Protection Test.

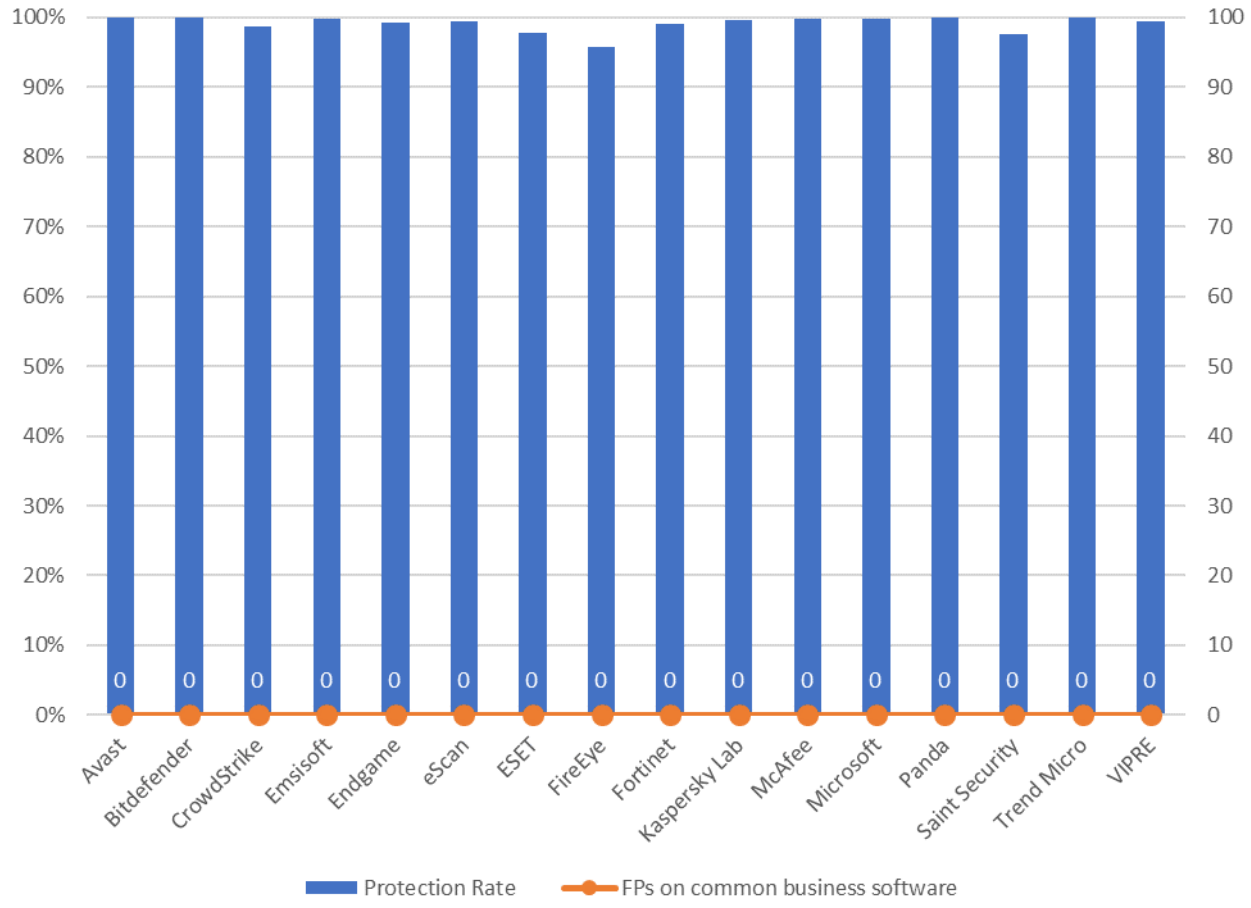
Malware Protection Test (March)

The Malware Protection Test assesses a security program's ability to protect a system against infection by malicious files before, during or after execution. The methodology used for each product tested is as follows. Prior to execution, all the test samples are subjected to on-access scans (if this feature is available) by the security program (e.g. while copying the files over the network or from a USB device, or saving from webmail). 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, **1,470** recent malware samples were used.

False positive (false alarm) test with common business software

A false alarm test done with common business software was also performed. As expected, all the tested products had ***zero*** false alarms on common business software.

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



	Malware Protection Rate	False Alarms on common business software
Avast, Bitdefender, Panda, Trend Micro	100%	0
Microsoft	99.9%	0
Emsisoft, McAfee, Kaspersky Lab	99.7%	0
eScan, VIPRE	99.5%	0
Endgame	99.3%	0
Fortinet	99.0%	0
CrowdStrike	98.8%	0
ESET	97.8%	0
Saint Security	97.6%	0
FireEye	95.9%	0

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

FP rate	Number of FPs on non-business software
Very low	0 - 10
Low	11 – 50
High	51 – 100
Very high	101 - 500
Remarkably high	> 500

	FP rate on non-business software
Avast, Bitdefender, Emsisoft, eScan, ESET, FireEye, Fortinet, Kaspersky Lab, McAfee, VIPRE	Very low
Saint Security	Low
Endgame, Microsoft	High
CrowdStrike, Panda, Trend Micro	Very high
-	Remarkably high

Performance Test (June)

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

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

The following activities/tests were performed under an up-to-date **Windows 10 RS3 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 a Lenovo G50 machine with an Intel Core i3-4005U CPU, 4GB of RAM and HDD hard disks. We consider this machine configuration as "**low-end**". The performance tests were done on a clean Windows 10 RS3 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[6] different types of clean files from one place to another, archiving and unarchiving files, downloading files from the Internet and launching applications (opening documents).

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

We believe that increasing the number of iterations increases our statistical precision. This is especially true for performance testing, as some noise is always present on real machines. We perform each test multiple times and provide the median as result.

We also used a third-party, industry-recognized performance testing suite (PC Mark 10 Professional) to measure the system impact during real-world product usage. We used the predefined *PCMark 10 Extended* test. Readers are invited to evaluate the various products themselves, to see what impact they have on their systems (due to e.g. software conflicts and/or user preferences, as well as different system configurations that may lead to varying results).

Test cases

File copying: Some anti-virus products ignore some types of files by design/default (e.g. based on their file extensions), or use fingerprinting technologies, which may skip already scanned files in order to increase the speed (see comments on page 5). We copied a set of various common file types from one physical hard disk to another physical hard disk.

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. The results already consider the fingerprinting/optimization technologies of the anti-virus products, as most users usually make archives of files they have on their disk.

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, and 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, and afterwards to close, 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 and a public server.

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

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

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

Overview of single AV-C performance scores

Vendor	**File copying**		**Archiving/ unarchiving**	**Installing/ uninstalling applications**	**Launching applications**		**Downloading files**	**Browsing Websites**
	On first run	On subsequent runs			On first run	**On subsequent runs**		
Avast								
Bitdefender								
CrowdStrike								
Emsisoft								
Endgame								
eScan								
ESET								
FireEye								
Fortinet								
Kaspersky Lab								
McAfee								
Microsoft								
Panda								
Saint Security								
Trend Micro								
VIPRE								

Key: Slow mediocre fast very fast

PC Mark Tests

In order to provide an industry-recognized performance test, we used the PC Mark 10 Professional Edition[7] testing suite. Users using PC Mark 10 benchmark[8] 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[9].

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

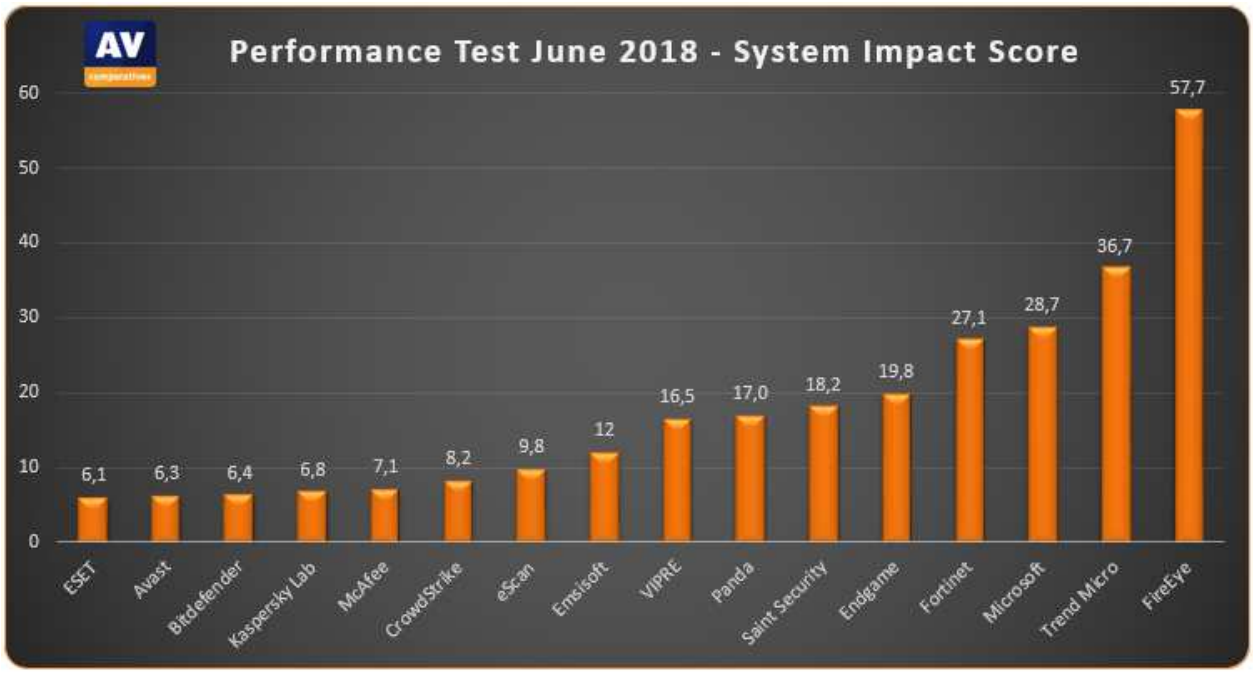
	PC Mark Score
Baseline	*100*
ESET	98.9
Avast	98.7
Bitdefender	98.6
VIPRE	98.5
Kaspersky Lab	98.2
Emsisoft	98.0
Panda	
Fortinet	97.9
McAfee	
CrowdStrike	96.8
Microsoft	96.3
Endgame	95.2
eScan	
Saint Security	93.8
Trend Micro	93.3
FireEye	92.3

[7] For more information, see https://www.futuremark.com/benchmarks/pcmark
[8] PCMark® is a registered trademark of Futuremark Corporation.
[9] http://s3.amazonaws.com/download-aws.futuremark.com/PCMark_10_Technical_Guide.pdf (PDF)
[10] Baseline system: Intel Core i3-4005U machine with 4GB RAM and HDD drive

Summarized results

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

	AV-C Score	PC Mark Score	TOTAL	Impact Score
ESET	85	98.9	183.9	6.1
Avast	85	98.7	183.7	6.3
Bitdefender	85	98.6	183.6	6.4
Kaspersky Lab	85	98.2	183.2	6.8
McAfee	85	97.9	182.9	7.1
CrowdStrike	85	96.8	181.8	8.2
eScan	85	95.2	180.2	9.8
Emsisoft	80	98.0	178.0	12.0
VIPRE	75	98.5	173.5	16.5
Panda	75	98.0	173.0	17.0
Saint Security	78	93.8	171.8	18.2
Endgame	75	95.2	170.2	19.8
Fortinet	65	97.9	162.9	27.1
Microsoft	65	96.3	161.3	28.7
Trend Micro	60	93.3	153.3	36.7
FireEye	40	92.3	132.3	57.7



Reviews

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

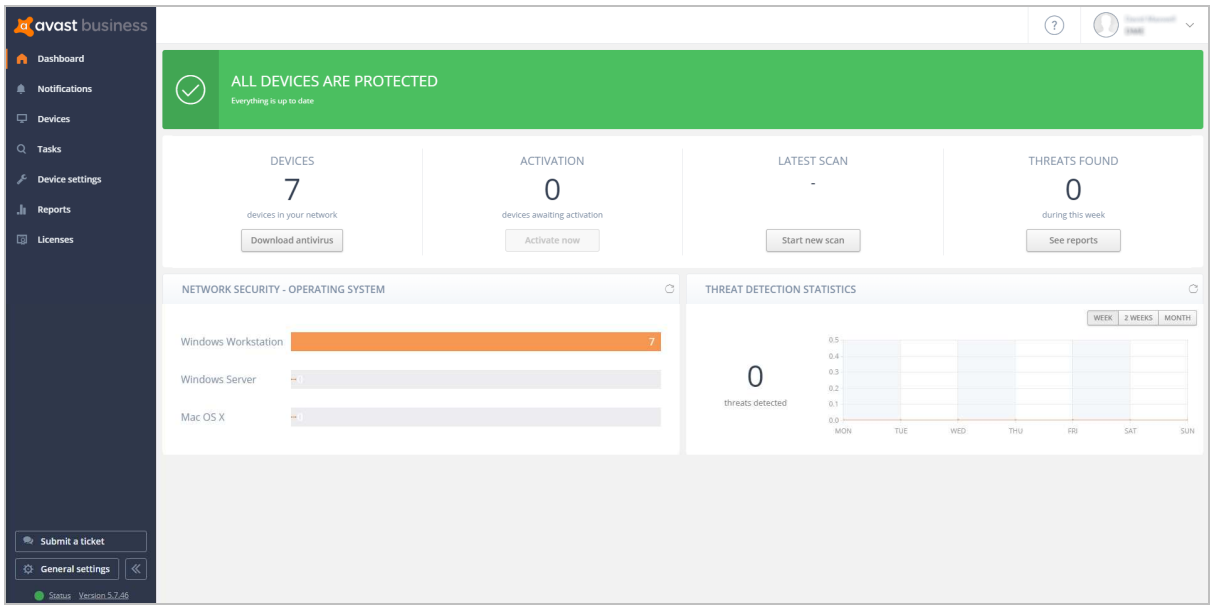
We first look at the type of product, i.e. whether the console is cloud based or server based, and what sort of devices/operating systems can be protected and managed.

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 consider remediation and outbreak containment. That is to say, how the product deals with individual malware detections/infections, how it warns of any spreading malware attacks, and what the administrator can do to keep these under control.

Avast Business Antivirus Pro Plus



What is it?

Cloud-console managed endpoint protection solutions. The portfolio consists of three products: Antivirus, Antivirus Pro, and Antivirus Pro Plus. Antivirus is a full-featured antivirus solution for SMBs; Antivirus Pro additionally includes automatic software updates, data shredding to permanently delete files, and extra security for Exchange and SharePoint servers. Antivirus Pro Plus provides additional data and identity protection to secure users and connections in open and public networks. The product is available for Windows client, server and macOS. There is no mobile device support available.

Product information on the vendor's website: https://www.avast.com/managed-antivirus

Online support: https://www.avast.com/business-support

Summary

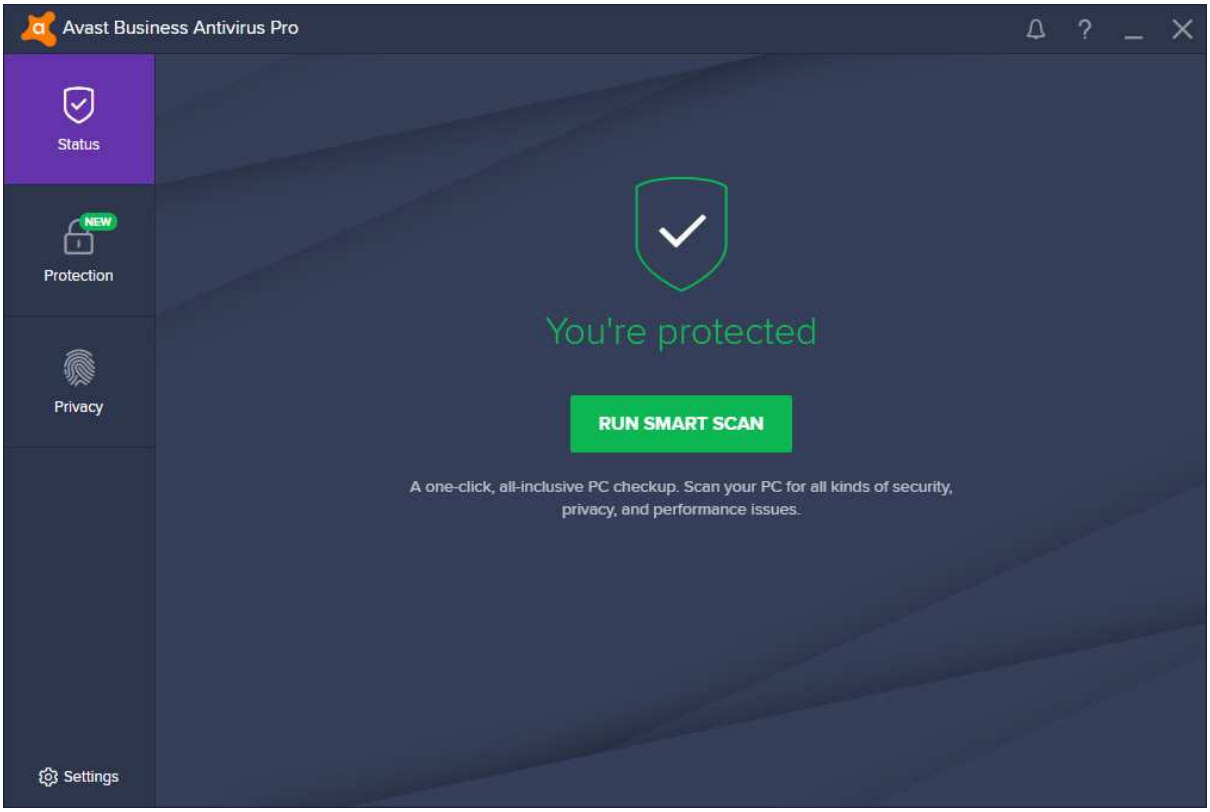
A strong product aimed at the small to medium-sized business looking for a solution that requires no onsite server component. It focusses on the Windows client and server, and the macOS client, but doesn't offer mobile support. The UI is clear and clean, and the defaults are sensible for the smaller organisation. A non-technical user should not have any problems deploying this to their collection of Windows desktops, servers and macOS devices within their organisation and then keeping track of what happens. It's probably aimed more at the smaller end of the organisational size, but still has grouping and profile capabilities to protect the larger estates. The product was liked as a straightforward platform. The lack of integrated control of Android devices is probably the only significant limitation compared to other small business products.

Part 1: Product installation and deployment

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 is via an installer package which can be downloaded for manual sharing and installation, or by sending a download link via email. The installer is offered in two sizes – a Light version which is around 6MB which then pulls the rest of the install from the cloud when running; or the full version, around 300MB, which has no subsequent download requirement to complete. The former is ideal for smaller networks, the latter is better for larger deployments to minimise internet traffic. The client installs a straightforward client onto the machine. The user can interact with the client to run daily tasks.

Part 2 – Ongoing use

Starting with the client, it offers a wide range of capabilities, very similar to a normal end-user desktop solution. There is a Status panel, and then a Protection panel which contains a range of tools. Scans, Wi-Fi Inspector, Firewall, Core Shields, Software Updater, Virus Chest and Sandbox are found here. The central policies determine what can be changed or adjusted, but there are still useful functions here.



On the server console, there is a clear set of main menus down the left-hand side: Dashboard, Notifications, Devices, Tasks, Device Settings, Reports and Licenses. The main Dashboard view 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, how many threats have been found and some graphical views of this information too. It is a straightforward, reassuring overview for the non-expert administrator.

Notifications collates all the main event information into one place, and you can take a malware event and go through to the Virus Chest on the affected computer from here too. The settings panel in Notifications is comprehensive, and 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, and means you can ensure that you are not swamped with information that is not immediately relevant.

The Devices tab gives access to each device configuration, its current licensing and when it was last seen. You can group devices into groups, and apply settings and policy through that group.

Tasks is a powerful scheduler area which is initially empty, although by default it says, "You haven't created any task yet, why don't you start with a scan?". It is here that an administrator can create tasks to run particular events. For example, do a quick scan every day at 2pm. You can also use it to send a short message to your devices, to update the device and to shut it down too. It is a simple task manager, but has useful capabilities for the small office and organisation.

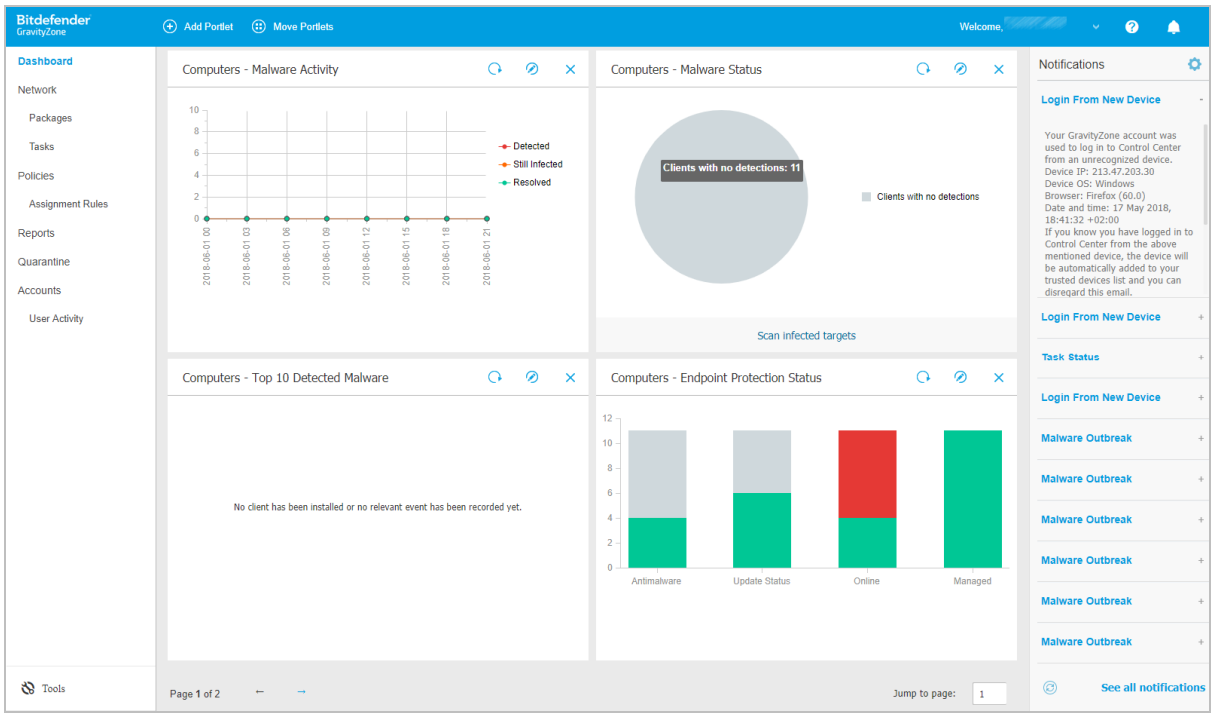
Device Settings allows you to create a settings template which is then applied to a group of devices. In here, you have access to all the control functionality for the device. So, you can determine that file scanning is on, Antispam is running, the firewall must be applied, and so forth. From these templates,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

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

Part 3: Remediation and outbreak containment

There is little here on the cloud management console to remediate an outbreak, although you can instruct all clients to update and run a scan. The reporting is strong but doesn't really handle the task of forensically analysing a large population outbreak. However, this is almost certainly beyond the intended deployment size of the product anyway.

Bitdefender Endpoint Security Elite (GravityZone Elite Security HD)



What is it?

Cloud-based management platform with local device clients. Clients can be Windows, macOS or Linux, and can be desktops, servers or virtual machines. There are various versions of the GravityZone product, and its management can be cloud based or local server based. It can be purchased with the HD component, which adds in the "Hyper Detect" engine, an endpoint integrated sandbox, and visibility of suspicious activities. There is no built-in support for Android or iOS mobile devices in the cloud console, although this is available with the on-premises server-based version.

Product information on the vendor's website: https://www.bitdefender.co.uk/business/elite-security.html

Online support: https://www.bitdefender.com/support/business/

Summary

There is much to like in this solution. The clarity and clear thinking of the design of the management console, the way the tasks are grouped together, the initial walkthrough wizard, plus the strong help and support, all contribute to a sense of calm and understanding of what is happening. We particularly liked the Dashboard capability, and felt that the policies and endpoint management allowed for a coherent and clear understanding of the rules that are being applied to endpoints. The addition of mobile device management would make it an excellent all-round solution for a modern diverse environment.

Part 1: Product installation and deployment

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 from, and to send email invites for multiple installs to your user base. Or you can use the Remote Installation capability to remotely install the endpoint client onto other targets in the network. To enable this, the first deployment must be a "Relay" deployment, to act as the bridgehead. You can also deploy to a security server here if you wish to do so.

Step 2 is to define the Security Policies in use at 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 not accounts for ordinary users, but administrative accounts for the management of the platform. The roles here can be Company Administrator, Network Administrator, Reporter and Custom. A "reporter" user might be on a help-desk role, for example, and can see reports of activity without being able to manage users or the company structure.

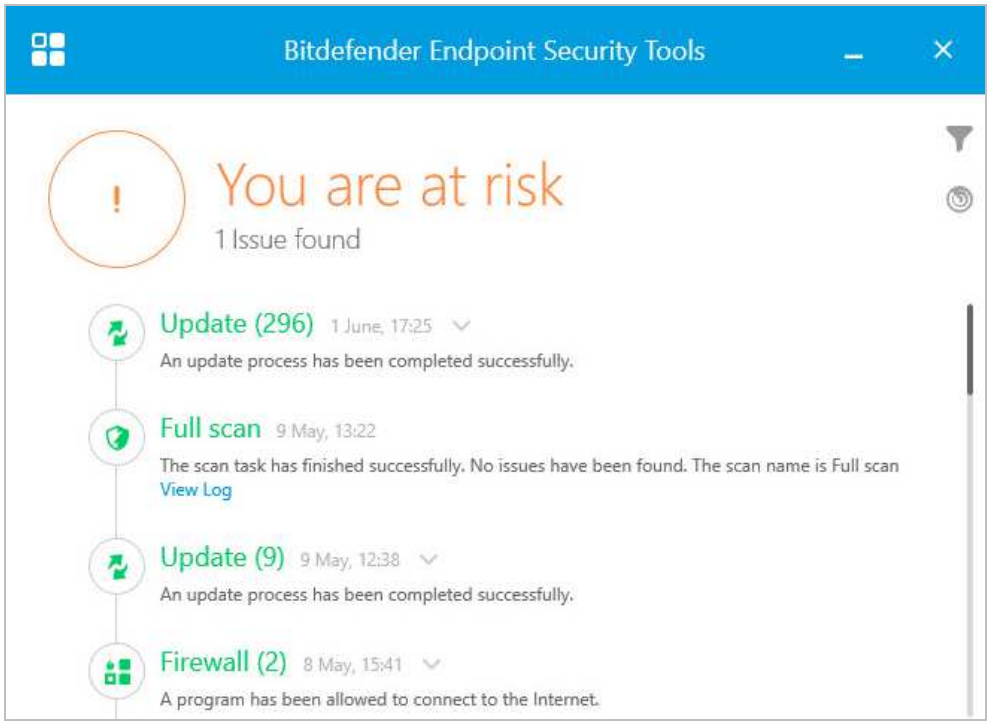
Step 4 is Reporting where it shows you how to create appropriate reports of activity on your network.

Having gone through these steps, you should have a deployed and managed network.

The client package offers a reporting window but no real functionality if the default lockdowns are applied. It will report what is going on and what has happened, but it is intended that most users are hands-off here. Of course, this could be enabled from central policy if required, and might be needed for a specialist role in the company, like a software development and testing role, for example. The user interface does allow the user to initiate a scan if required, or check for updates, but again this is determined by policy.

Part 2 – Ongoing use

Starting with the client, this is a simple application with a clean interface. It clearly shows what is going on, but is designed to have minimal footprint on the user experience. Indeed, one policy setting is to make the whole UI invisible to the user. This might be beneficial in a heavily locked-down environment. Others might prefer to offer the end user the opportunity to do an update or run a scan, which might be more applicable to a roaming user, a travelling salesman away from the office, for example.



The server console is particularly clear and clean. The initial walkthrough wizard is an excellent idea because it helps you focus on the necessary tasks in a clear and coherent fashion. This helps make the product eminently suitable to a smaller, less IT-skilled workplace as well as a larger, more IT-literate infrastructure.

The main console has a menu structure down the left-hand side which is clear and clean. Dashboard, Network, Policies, Reports, Quarantine, Accounts.

Dashboard gives you an instant overview of the installation and the performance of the clients. Each panel here is called a "portlet" and can be clicked on to drill into more information. We particularly liked the way that the Portlets can be rearranged, added to, and laid out to your preferences. The strong capabilities of Dashboard mean that you get to the information you require very quickly, with the minimum of digging through the UI.

The Network menu item lets you configure deployment packages, and then tasks which can be run once or multiple times.

Policies is where you define the operational groups within your organisation, and then apply those policies to computers, thus imprinting onto the client machine the functional roles that the IT department requires. As you would expect, there is a wealth of capability here, including full control of the firewall, application operation, device control (including disallowing access to various hardware components on the desktop, like USB drives) and 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.

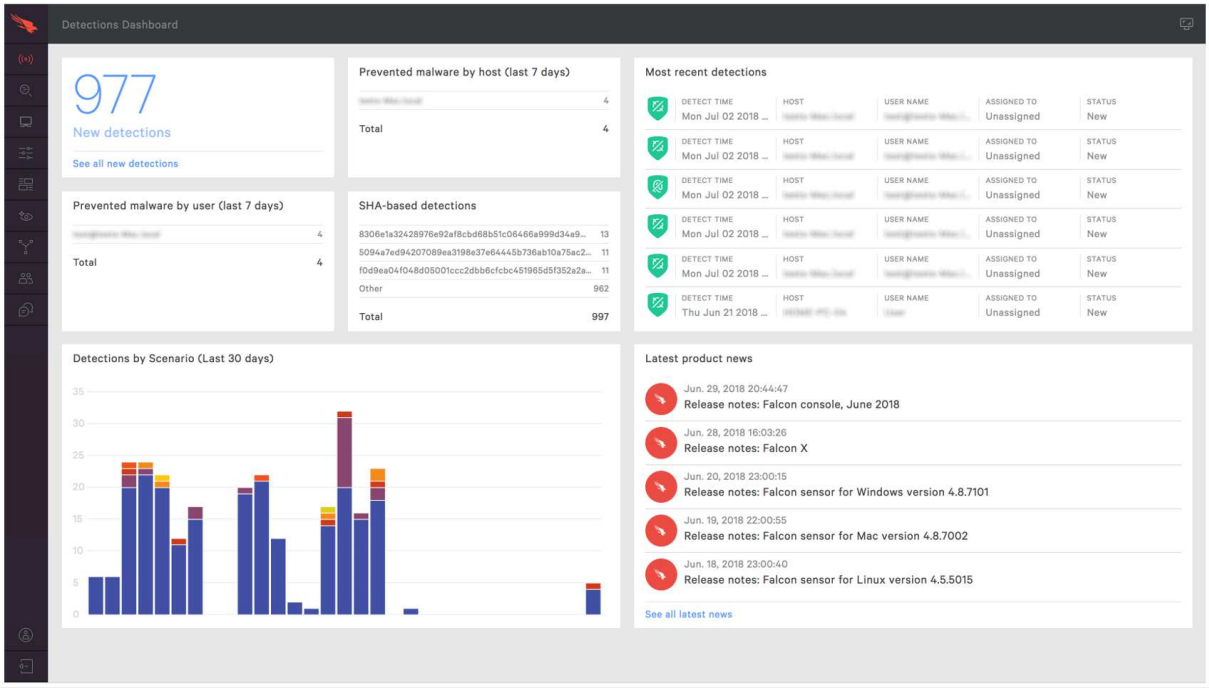
Accounts lets you monitor the activities of the user accounts that have been set up.

On the right-hand side there is a vertical list of Notifications. Drilling into each gives a clear explanation of the problem and a description of what happened. We particularly liked the reporting of a malware outbreak which informed use that "at least 28% from a total number of X endpoints were found infected with" a piece of malware, making it much easier to separate out isolated incidents from a network-wide pandemic.

Part 3: Remediation and outbreak containment

The clarity and careful design of the user interface makes it relatively easy to get a comprehensive view of the status of the network and all end points. The reporting of multiple incidents clustered into one report helps understand what is happening when there is a network-wide event. And the clarity of the UI helps ensure that settings have been applied appropriately, even by a relatively inexperienced system administrator.

CrowdStrike Endpoint Protection Platform Standard Bundle



What is it?

Cloud management console with client AV packages. The product is called CrowdStrike Falcon and the cloud-based management console can be run from the cloud on any modern browser." Clients are provided for Windows, macOS and RedHat, Ubuntu and Amazon Linux platforms. There doesn't appear to be provision for mobile clients.

Product information vendor's website: https://www.crowdstrike.com/products/

Online support: https://falcon/crowdstrike.com/support

Summary

CrowdStrike Falcon is a very comprehensive platform, providing not only AV services within an organisation, but also a comprehensive set of detection and analysis services. It is aimed at the larger organisation, and is not really a "fit and forget" product. Basic everyday monitoring and management tasks are simple enough; however, to get the best out of it, some investment of time for learning is needed, possibly coupled with external consultancy. Its range of capabilities is sufficiently deep that it would be unwise to have only a minimal understanding of its operation.

Part 1: Product Installation and deployment

It is simple to deploy the cloud infrastructure, because it comes pre-packaged for you in a cloud console, which can be run from any modern browser. Deployment of the client "sensor" is quite simple here, and relies on the download of the installation package appropriate to the target platform. There is a checksum ID to be copied into the installation routine. On Windows, you can use an automatic sensor deployment like Windows System Center Configuration Manager.

On the Mac platform, we were a little surprised to see that a command line execution is required. Nevertheless, deployment is straightforward. Once you have installed onto Windows, it registers with the platform as the AV provider and disables Windows Defender.

Once installed on Windows, the Falcon Sensor is almost invisible to the end user.

Deployment across an organisation will take planning and appropriate tools, with preparation for the appropriate layers of policy to be applied to users. Once this work has been done, deployment should be quite straightforward. Because of the capability of the platform, this is not a product aimed at the smaller end of the SME marketplace, although it could most certainly be used there if appropriate skills were available, and the data risk was sufficiently high.

Part 2: Ongoing use

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

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

The Investigate menu takes you into a comprehensive search facility, covering hosts, hashes, users, IP addresses, domain and event searching. This is aimed at locating specific issues across the network estate in the recent history – the default is 24 hours, and it recommends limiting your search to no more than 3 days. Pre-set filters for up to 30 days are provided.

The Hosts menu gives a dashboard of all the host installations, by version and platform, and allows 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 and Mac clients here too.

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

The Discover menu allows you to discover the network by application inventory, asset, mac address, accounts and other app/process-based inventory.

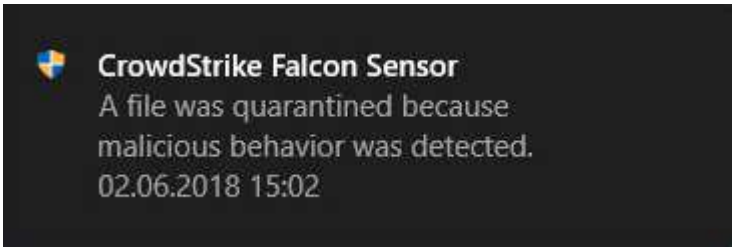
The Intelligence menu takes you into an overview of the current landscape threat as perceived by CrowdStrike. This can be categorised by geographical origin of threat, target industry, target country, and motivation (espionage/criminal/Hactivist and destruction). Each threat is detailed by these parameters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

The User menu allows you to create the usual user profiles for administrators and other activities within the platform. There are pre-built roles already created for Endpoint manager, event viewer, Administrator, Analyst, Investigator, Real time responder, and others, allowing you to map these roles onto existing internal working structures, or to custom build new roles as required.

The management console has five key menu choices on the left-hand side. Dashboard gives an overview of the status of the entire estate of client devices, and reports how many alerts are in play at any one time. It also gives a clear top-view of top alerts, exploits, malware and fileless alerts, allowing for a comprehensive view of what is happening. Each of these can be clicked through to drill into more information. Two-factor authentication appears to be mandatory for all logins here, and this needs to be considered as part of the deployment design.

Finally, there is a comprehensive help and support role within the product, in addition to the Intelligence capability.

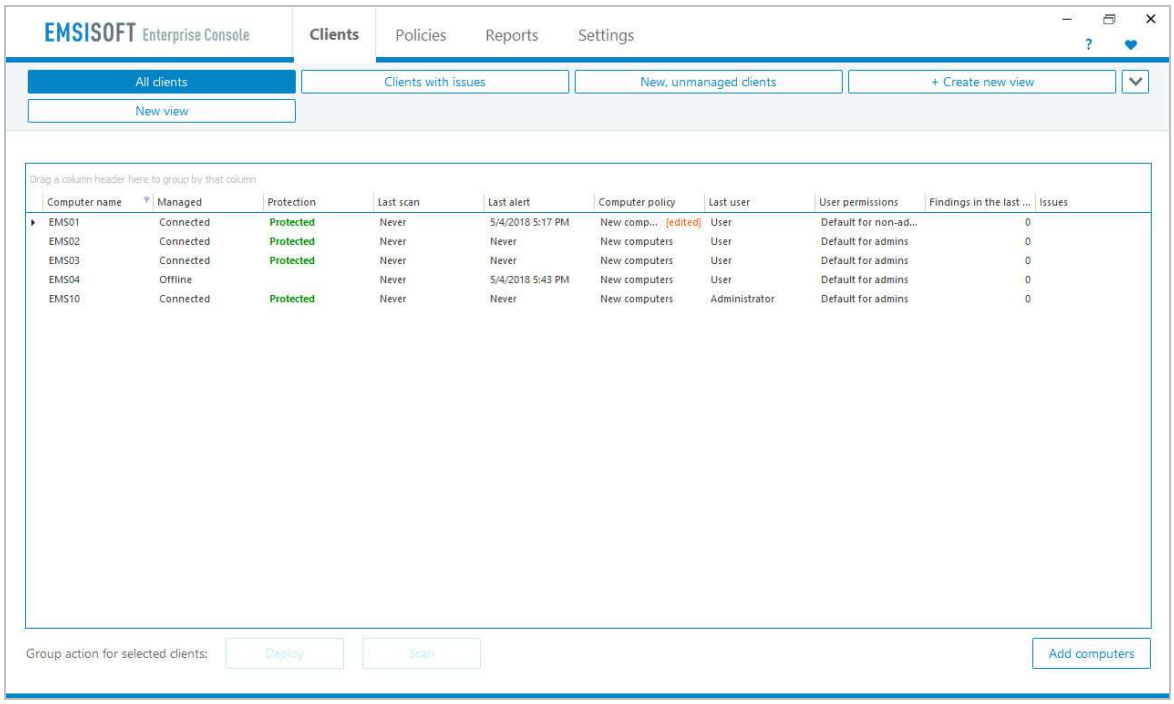
On the end-user client, the default settings is to have the client invisible to the user (aside from malware alerts – please see screenshot below). However, this can be enabled and adjusted through user policy if required.



Part 3: Remediation and outbreak containment

Understanding what is happening across a large installation base is the core functionality of CrowdStrike. It offers all the power you need to clearly understand, review, audit and control an outbreak in a comprehensive layered fashion. This power comes with a need to thoroughly understand the platform, and it requires a layered multi-user security approach to its daily management. However, it is clear that this will reward a serious and comprehensive implementation with excellent power, control and auditing.

Emsisoft Anti-Malware with Enterprise Console



What is it?

Local server-based engine with device clients. The product is available for Windows client and server. There is no mobile device support available, nor MacOS.

Product information on the vendor's website: https://www.emsisoft.com/en/business/antimalware/

Online support: https://support.emsisoft.com/

Summary

A fairly traditional on-premises client/server AV implementation. The client support is for Windows only, so companies wanting to protect Mac or mobile devices would need another solution for these. The console and client software both use a very clean, modern design, which we found very easy to navigate. For an experienced admin, installing the console and deploying the client software is very straightforward. We would suggest the product is well suited to a business large enough to have its own full-time IT administrator, and is powerful enough to cope with larger organisations too.

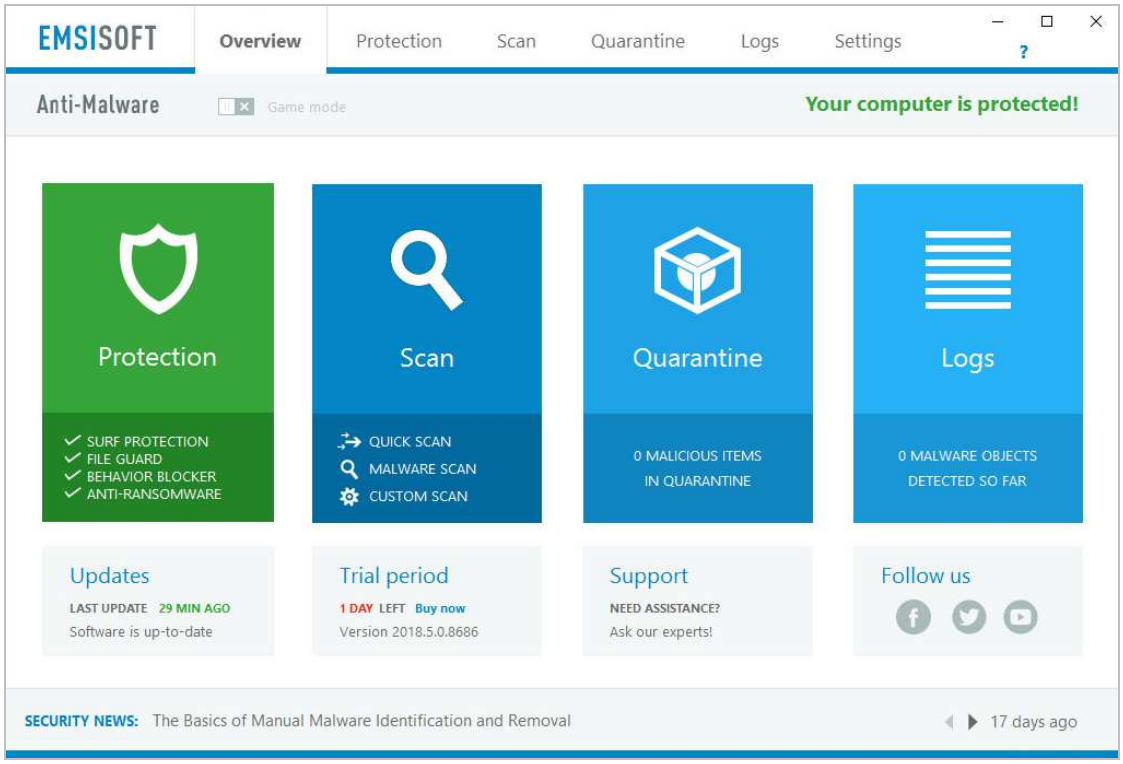
Part 1: Product installation and deployment

Deploying the server component is unproblematic and requires little user intervention. Once it is up and running, you apply appropriate licenses to it to prepare for deployment. Getting the client onto a device is relatively straightforward: the easiest route is to do a remote login to the target using admin rights, and the run the packages.

The client itself looks like a fully featured AV package. The user can run scans and updates from the System Tray icon or main program window.

Part 2 – ongoing use

The client looks like a regular AV client, with a good Overview tab showing the status of the product. The Protection tab has three selection tabs – Surf Protection, File Guard and Behaviour Blocker. Surf Protection is a rather quaint term for web filtering. Behaviour Blocker allows control over running processes on the machine. The Scan tab offers the usual Quick/Malware/Custom scans, scheduling, settings for the scanner and a download link for building an emergency kit for scanning an infected machine. Quarantine shows what has been detected and placed into the quarantine area, and Logs shows the event status of the client. Settings has a range of configuration settings for the client. It is only possible to make any configuration changes using a Windows administrator account. Standard Windows users will see settings controls greyed out.



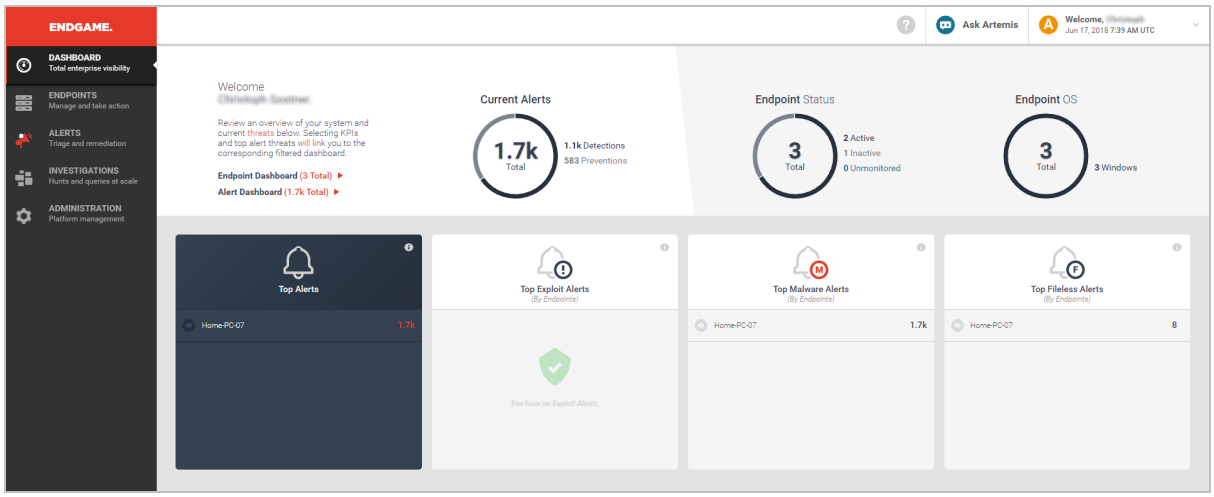
Moving to the server, it is a rather clean design here. There are four main tabs. Clients lists the clients by grouping (all, Clients with Issues etc), Policies allows you to define and deploy policies to the clients. The settings here are split between Computer policies and User policies. Computer policies lets you set organisational groups and then define default settings for that group (e.g. start on Windows startup, Windows Explorer integration and so forth). User policies lets you define user profiles, with defaults set to either Read-only access, Basic access (default for standard users) or Full Access (for administrators). This area supports drag and drop, so you can move a client from "Default for admins" to "Default for non-admins" easily enough.

The Reports tab has a set of standard reporting views. You can build your own reports easily enough in this area, by selecting New Report. Reports support save to PDF and send via email, and you can schedule a pdf report to be sent by email by clicking on Settings, Notifications. Finally, the Settings tab allows control of the various underlying processes and configurations within the server product.

Part 3: Remediation and outbreak containment

The Clients page of the console shows the protection status of the clients as text (e.g. Protected/Not Protected), along with green, orange or red colour as appropriate. If a computer is shown as Not Protected, there will be a Solve link in the Issues column of the same page. To test this, we locally disabled all the protection features on one of the client PCs. The client's status was immediately shown as Not Protected in the console, and clicking Solve instantly reactivated the protection and updated the status in the console to Protected. We did notice one minor bug here: the console displays a message box that states "Protection of Emsisoft Anti-Malware was not enabled", but we verified that this was a false alarm. We have notified Emsisoft of the bug, and they are working on a fix for it.

Endgame Protection Platform



What is it?

The Endgame endpoint protection platform provides prevention, detection and response measures, and threat hunting capabilities aimed at stopping targeted attacks. Their management console can be run from the cloud on any modern browser. A hosted option is also available. The platform supports Windows, Linux, Mac, and Solaris endpoints (although we felt this was not made very clear on the vendor's website). There is no provision for mobile clients.

Product information vendor's website: https://www.endgame.com/platform

Summary

Endgame is aimed at larger organizations that require prevention and EDR capabilities. Deploying it will require some planning and training, meaning that it is not a solution that you can just install and forget about. However, for organisations with the resources to make full use of it, it provides a comprehensive and coherent set of tools and capabilities. Administrators might want to consider disabling Windows Defender via Group Policy.

Part 1: Product Installation and deployment

We used Endgame's cloud-based infrastructure, which simply requires you to log in with your correct credentials to gain access 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 deployment is currently only supported by Windows, while out-of-band supports Windows, Mac OS, Solaris, and Linux clients. For in-band deployment, a system administrator installs the sensor directly onto the Windows client from the Endgame management platform. With out-of-band, customers can deploy via the platform or use a management tool of their choice – this could be Microsoft System Centre Configuration Manager or equivalent.

In our installation, we downloaded a zip file from the Administrator/Sensor page. From this, you extract the installer and configuration file, then run the installer from an elevated command prompt using the configuration file. You have to search the documentation to find the necessary command-line syntax to do this. Double-clicking the .exe file simply deletes it.

Once installed on Windows, the Endgame agent is largely invisible to the end user. It does not register as an Antivirus platform in Security Center. The Endgame platform includes a wide variety of protection features, with many available configuration options and customizations. Users may find it complex to deploy for the first time. The platform is designed to be run either by trained internal security teams or as part of a services offering. It is definitely a product aimed at the medium to larger end of the deployment size, and is not really a product for smaller businesses.

Part 2: Ongoing use

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

The Endpoints menu gives a view of all of the estate of the clients that are currently monitored, and allows you to select and sort by name, IP address, OS version, Endpoint policy that has been applied, the sensor version, alerts and tags. From here, you can choose a range of endpoints and then apply tasks to them – apply a new policy, discover new endpoints, tag/uninstall/delete endpoints from the catalogue.

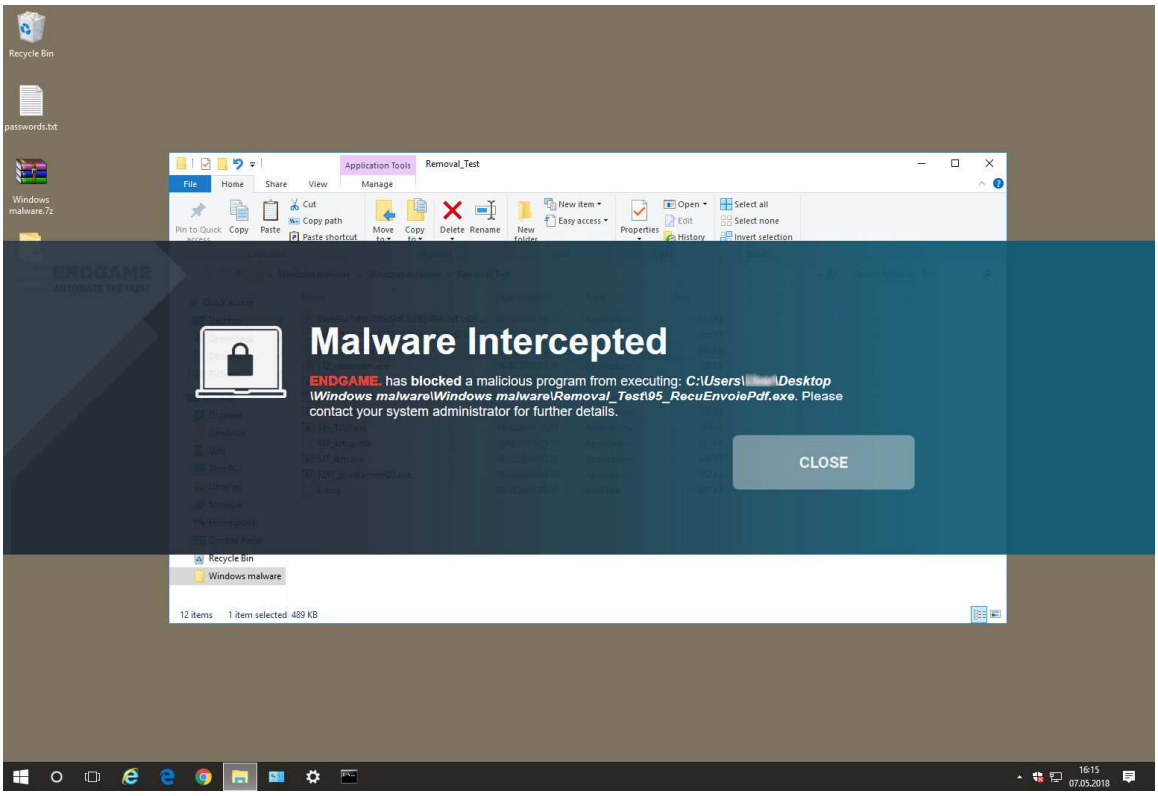
Alerts takes you into the heart of the platform. Here you get a list of current event types which could be, for example, a malicious file execution prevention, a file detection and so forth. The catalogue of events can be sorted and categorised by platform, OS, IP address, Host and date. Most important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

If you click on an event, it takes you to the Alert Details page for that event. Here you can see much more detail about the event, where it started, what it has done and the analysis of the malware if appropriate. Here you can choose to Take Action: the options include download alert, download timeline, resolve, dismiss, start investigation, download file, delete file or whitelist items. Of particular interest here is the Start Investigation feature which lets you create a “hunt”. A hunt can cover multiple information sources – firewall rules, drivers, network, persistence, process, registry, media, system configuration and so forth, and allows you to reach out into the estate to locate information relevant to your enquiry. A key component here is also 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 it is assigned to, what endpoints were involved and so forth. This is very important for understanding how the current analysis is progressing.

Finally, the Administration menu item gives access to the Policy settings, Users, Sensors, Alerts, Whitelist and Platform capabilities. Of particular interest here is the policy settings page, which allows defined policy to be set for items such as command and control, discovery, execution, lateral movement and so forth. As an example, you can choose what policy to apply when there is a process injection – 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.

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

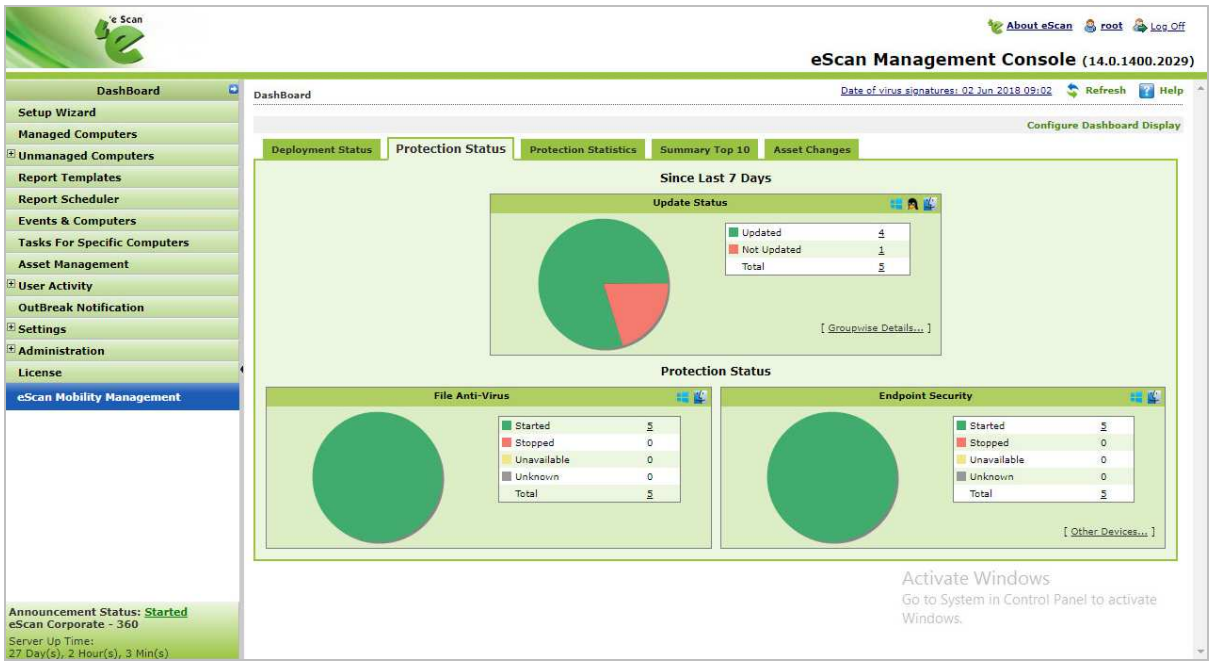


Because Endgame does not register as an AV package in Windows. Endgame tell us that their product is designed to be compatible with Windows Defender or any other "traditional" AV product, and detects and prevents malicious activity before such an AV product springs into action. However, they also say that their software provides all the protection needed, and so running an antivirus product as well as the Endgame product is not necessary. Administrators not deploying an additional AV product might like to disable Windows Defender via group policy, to prevent any possibility of conflicts, or Defender taking action against threats (as this would not show up in the Endgame console).

Part 3: Remediation and outbreak containment

The management console is designed specifically to handle large estates of clients, possibly on a global scale. Because of this, malware issues are expected to be happening, and Endgame offers a very strong set of analytics and remediation to handle such an outcome. The ability to track the progress of an outbreak appears to be strong and thorough, along with the tools to manage and contain it.

eScan Corporate 360 with MDM & Hybrid Network Support



What is it?

Local server-based engine with device clients. The server runs on Windows Server. The clients support Windows, macOS and Linux devices. Mobile support is available through the "eScan Corporate 360 (With MDM and Hybrid Network Support)" edition and supports Android.

Product information on the vendor's website: https://www.escanav.com/en/windows-antivirus/corporate-360.asp

Online support: https://www.escanav.com/en/support/escan-tech-support.asp

Summary

We suggest that the product is best suited to experienced IT professionals in larger corporate networks, for a number of reasons. For example, the remote installation function requires Active Directory. The opening page of the console provides a good status overview, with a very standard, MMC-style menu panel on the left-hand side. However, navigating other areas of the console might not be immediately obvious for inexperienced administrators. We had the feeling that the console design was not consistent throughout, and indeed the MDM component (mobile device management) runs as a separate interface in a separate browser page. Whilst the functionality available from the console is very good, in some areas the GUI could be improved to make it easier to use.

Part 1: Product installation and deployment

Deploying the server component is straightforward and needs little user intervention. It requires a Microsoft SQL Server installation; eScan will install SQL Server Express if necessary.

Once it is up and running, a malware scan is run on the server to ensure it is clean. The deployment wizard starts automatically when you first open the console. Choosing the target clients and pushing out the client installation should be simplicity itself.

You apply appropriate licenses to it to prepare for deployment (full functionality is available in the 30-day trial version). The product supports only Windows clients (no MacOS, or mobile) so deployment is limited to those targets. Getting the client onto a device is relatively straightforward: the easiest route is to do a remote login to the target using admin rights, and the run the packages.

The client itself looks like a fully-featured AV package. It can be started from the shield icon in the Taskbar, or by running the "escanpro.exe shortcut" on the desktop. It has quite a straightforward status view along with appropriate tools for scanning.

Part 2 – ongoing use

The client looks like a regular AV client, and the front window has clear areas highlighted in red and green to indicate that the services were running. There is a little confusion here over the use of colour, because we could have the "file antivirus" panel in green despite it also saying "Dangerous Objects Detected: 18". Some clarity over the meaning of the colours would help. The green colour is intended to demonstrate "protection working as it should".

At the bottom of the screen are Scan and Update buttons, which function as you would expect. Once you choose one of the coloured panels, you are taken into a specific task area, with a list of the other panels at the top of the screen, so you can directly jump from one to another. Again, there is confusion here: our Web Protection panel is in green and states "Started" but once you click into it we have "Web Protection Status" reporting as Stopped, as is Web Phishing Filter Status. The green colour here means that some sub-component of a module is started.

By default, almost all the settings here are controlled via centralised policy and hence are greyed out. If the admin sets up password-controlled access, temporary changes can be made on the client software. These will be undone the next time the client synchronises with the server. Over on the server side, it is a web-based interface despite being a server hosted solution and not cloud. It uses a local web server and a high port number, so typically the URL will be "localhost:10443/ewconsole/ewconsole.dll/homepage". Alternatively, "http://localhost:10443" could be used. The layout of the console will be very familiar to anyone who has used Windows' Microsoft Management Consoles such as Device Manager. All the functionality can be accessed from a single menu panel on the left-hand side, with content shown in the main right-hand panel. Any menu item which has sub-menus is clearly marked with a "+" sign. The familiar Windows look extends to other areas of the GUI. For example, the tree structure and icons used in the Managed Computers page is very consistent with the design of Windows' File Explorer.

A wealth of information about client computers is provided. There are over 20 items, including IP address, name of logged-on user, installed product and its status, installation directory, last policy applied, last connection, and client OS. Whilst this ensures the administrator is very well informed, anyone with a smaller monitor will inevitably have to scroll a lot to the right to see all the items displayed. However, it is possible to customise the page by hiding any items you do not require. The left-hand menu column can be hidden, to provide more space for content, although the very small arrow button that does this was not immediately obvious to us. There is a setup wizard which lets you deploy the endpoint protection software to client computers. Logically enough, this is at the very top of the menu panel. Whilst it is very straightforward to use, we note that Active Directory credentials have to be provided in order to access client computers. As a result, another installation method has to be used in a Windows Workgroup environment.

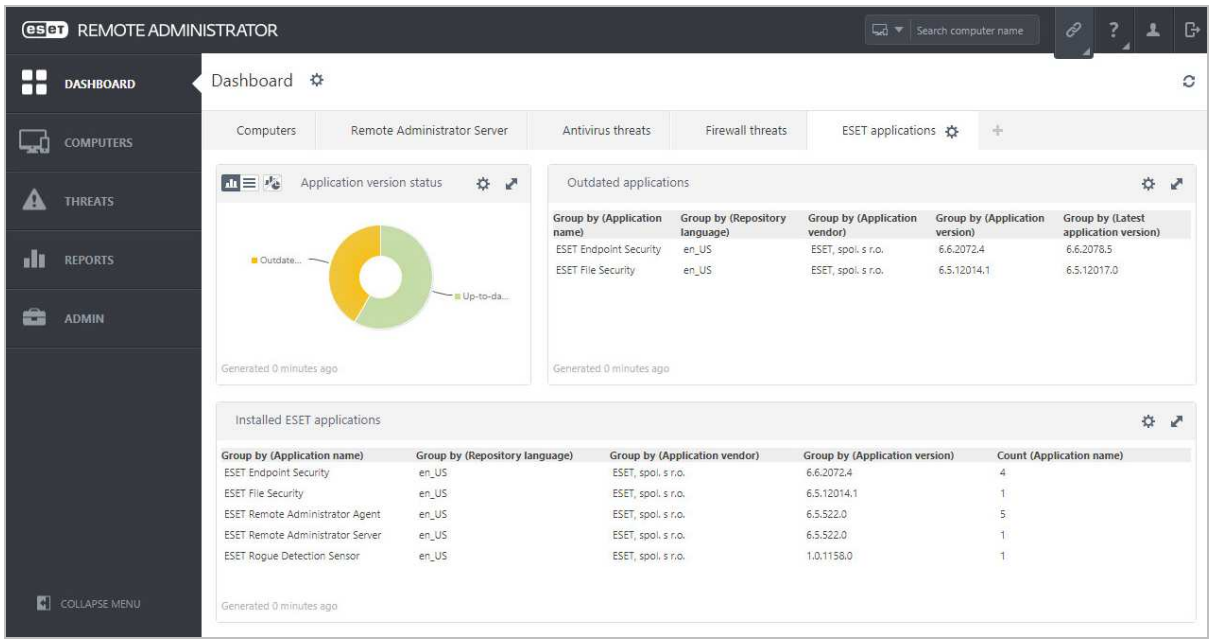
The Report Templates page provides a wide variety of possibilities, including Update Report, Scan Report, USB Control Report and File Activity Report. All of these are available for Windows clients, with a slightly smaller selection for Mac and Linux clients. The logo(s) next to the text indicate(s) which platforms are supported for each report type. We note that reports can be scheduled and emailed. This small subsection of the system has its own SMTP email settings, which are quite separate from the email settings found in OutBreak Notification, for example.

The menu item for the MDM component (mobile device management) stands out, as it uses a different colour scheme. This is in keeping with the fact that it opens in a new window, and is essentially an independent console. This uses a very similar layout to the main console, although there is a different colour scheme. The separate email settings for reports and outbreak notifications, and the separate interface for the MDM component, rather gave us the impression that the product had been assembled from a number of existing components, rather than having an overall design.

Part 3: Remediation and outbreak containment

There is basic help here to help remediate an outbreak in the "Outbreak Notification" menu item, which allows you to generate email notifications when the number of viruses detected exceeds the default of 25 in 1 day. However, all of this is disabled, and requires access to an SMTP server. We expected this to be part of the service provided by eScan, at least as a default backstop to get you up and running.

ESET Endpoint Security and Remote Administrator



What is it?

Local server-based management console with client AV packages. The management console is called ESET Remote Administrator and can be run on Windows or Linux servers. It is also available as a virtual appliance. Clients are provided for Windows, macOS and Linux, and there is support for mobile devices on Android and iOS too. The Windows client is called ESET Endpoint Security. However, there are multiple products to choose from according to the website, and it is important to know the differences. For Windows, you can choose Endpoint Security or Endpoint Antivirus. For macOS, there is Endpoint Security, and Endpoint Antivirus (which is just the AV component). For Linux, there is the NOD32 Antivirus Business Edition for Linux Desktop, which is the core AV product. ESET also provides antivirus software for virtual machines (Azure VM, agentless ESET Virtualization Security), file servers (ESET File Security for Windows Server, Linux/FreeBSD) and SharePoint, gateway and email servers. All of these products can be managed from the Remote Administrator console.

Product information vendor's website: https://www.eset.com/int/business/endpoint-protection/

Online support: https://support.eset.com/en_EN/setupera/ which also offers live chat directly from the management console.

Summary

It is obvious that this is a comprehensive and well-considered platform. The choice of going for an internal server-hosted platform will appeal to many, as will its broad selection of client capabilities across many OS's. It is powerful and capable, and certainly able to scale up. Its reach to the smaller sites might be limited both by its local server requirement, and the slightly geeky/technical nature of the product. However, it is quite obvious once you have learned a few of the main daily tasks, and it is clear that ESET have put a lot of effort into this platform to make it accessible.

Part 1: Product Installation and deployment

Because this is a locally hosted server-based solution, it is best to get the server side working first. Installation is not without some issues however. Depending on your server configuration, you might find that the installer stops and demands the installation of .NET 2.0 and Java. Download links are provided for this. You have to stop the installation, do these separate installations and then restart the main installer.

Once this is completed, opening the console takes you to an introductory wizard which covers off the main points of getting the clients installed, and the management system running. From here, you can create installer files for the endpoints and either choose to run the installer at the endpoint itself, or use a push installation. The management interface is reasonable obvious although it does suffer from a lot of information on the screen. It most definitely benefits from a large high-resolution display, and this should be taken into consideration. Running it on a normal resolution and size of desktop means that many items are rather cramped.

On the console, there is a main menu down the left-hand side, covering Dashboard, Computers, Threats, Reports and Admin. Depending on which area you choose, you might get a secondary menu for additional choices. Getting agents onto the clients is not completely obvious here. It is not accessed through these side menus, but through a small icon on the top right corner. Indeed, this is where most of the setup and management functions are found. Add new computer, add new mobile device, add new user, generate report, new client task, create the installers, the section relating to policy, and server management are all in this somewhat small area.

Creating new devices is simple, and allows you to import a CSV definition list here. Adding a mobile device requires enrolment via email (server settings required here for your own SMTP server) or via a link or QR code.

Creation of the new policy takes you firstly away from the direct server product, because it asks which ESET product you are wanting to create policy for. The list is populated by all the server products that ESET makes. Prepopulating it with those actually on this licensed server would help. Once the endpoint product is chosen, you can then make all the selections to create the policy definition. Then you can use the Assign Policy function to push policy out to clients. There is a wide range of predefined policies here for you to choose from. For example, “Antivirus – Balanced”, “Antivirus Maximum Security”, “Firewall – Block all traffic”, “Visibility – Balanced” and so forth.

As a UI it is reasonably easy to set up and get deployed to a range of client devices. It is not the simplest to use, nor the most obvious, but time spent learning the UI is rewarded.

Part 2: Ongoing use

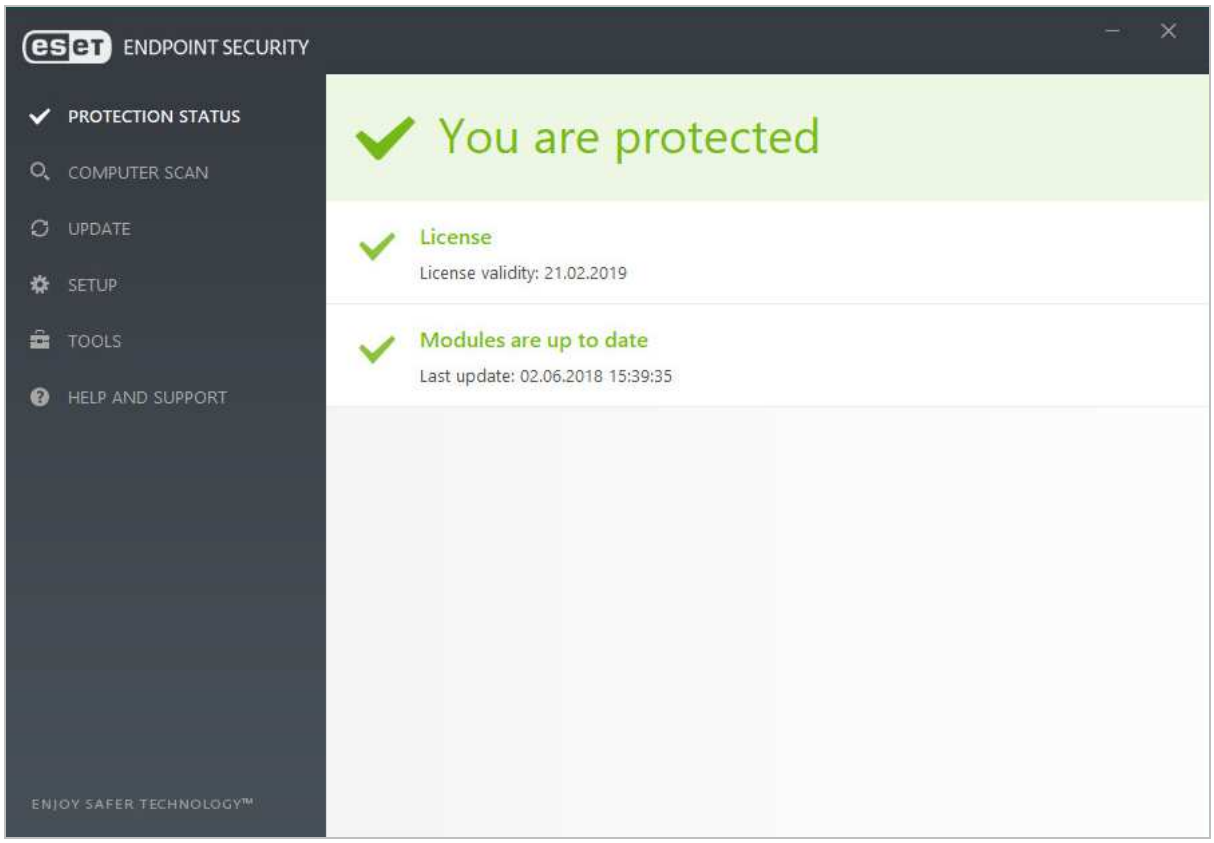
The Remote Administrator console is designed to handle a lot of devices, tasks and processes. Despite this, it is still reasonably clear and obvious. Dashboard gives a strong overview of the current set of managed hardware. You can click onto segments of the graphical data and drill down into the underlying data. There are multiple paged views here, covering Client computers, Server, Antivirus Threats, Firewall Threats, and ESET applications. You can add more tabs here if you wish, and then populate the structure with the desired collection of data. Overall it works well.

Handling the day-to-day operations of clients is quite simple. The product automatically groups clients by type, and you can also add in additional groups as required. This should allow you to manage a large estate of devices, across geographical locations and platforms.

The Threats menu takes you to a strong set of onscreen reporting. Again, a larger screen helps here.

The Reports menu is particularly strong, with a long list of predefined report types. For each you can decide to generate it now, run it on a schedule, download it in a variety of formats, and deliver it via email and to file. This is a very comprehensive set of reporting capabilities and is doubtless one of the strengths of the platform.

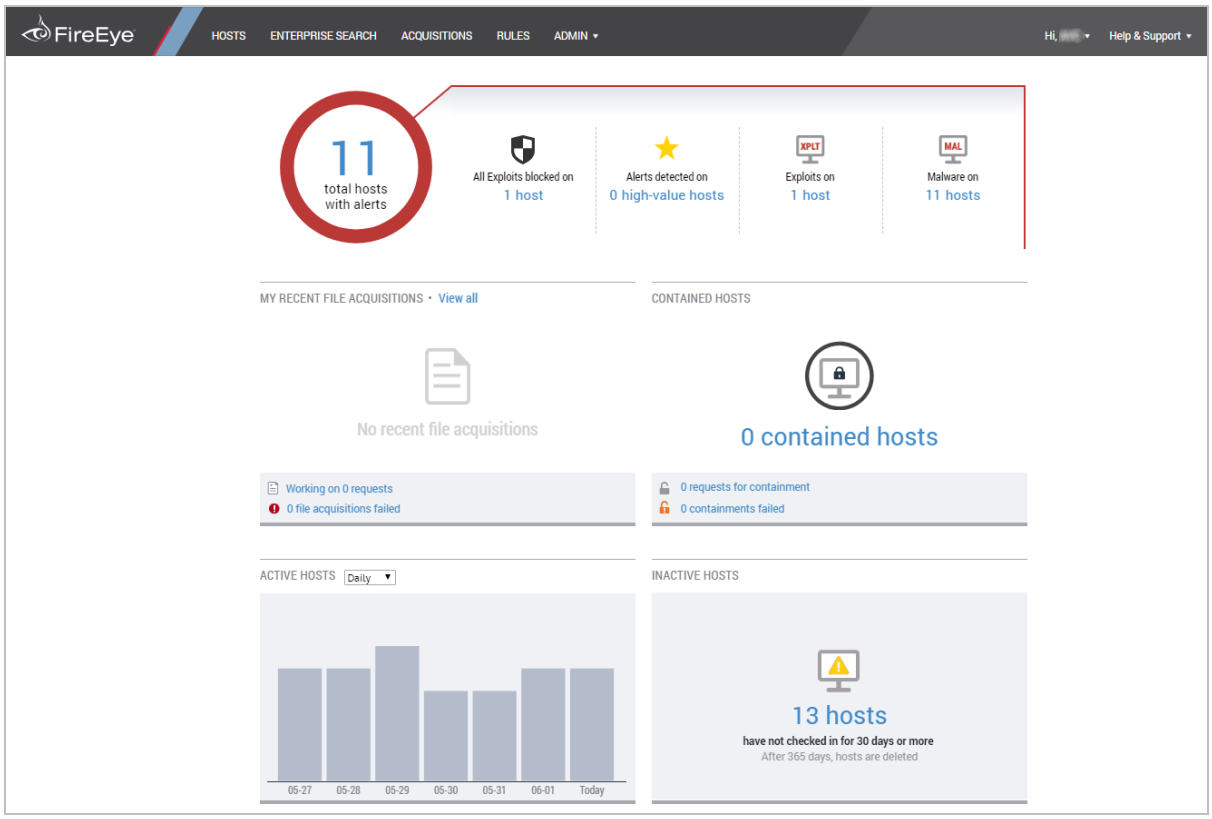
On the client side, by default the user gets a quite comprehensive Endpoint Security client. Capabilities here are, of course, determined by policy from the central server. But the user can do useful tasks here if required, like scanning the computer, updating and so forth. The Tools menu is particularly effective, offering a range of useful overview data and statistics, which can be helpful when viewed through a remote management tools from a helpdesk, for example.



Part 3: Remediation and outbreak containment

The management console is easily up to the task of handling and remediating a significant outbreak. It should be possible to identify which machines are compromised, and how you wish to proceed. The policy management allows you to lock down devices to help prevent, and contain, issues when they arise. There is a lot of power here, which is not too scary for a smaller organisation, but which clearly can scale up to a larger one.

FireEye Endpoint Security



What is it?

Cloud-based management console with client AV packages. The server component can be deployed either to the cloud, or as a virtual or on-premises hardware appliance. It is designed to handle the largest of organisations, with support for up to 100,000 endpoints. There are clients available for Windows, macOS and Red Hat Enterprise Linux. There is no support for mobile platforms.

Product information vendor's website: https://www.fireeye.com/endpoint

Online support: https://www.fireeye.com/support/contacts.html including live chat support.

Summary

FireEye Endpoint Security is a highly powerful platform. Its core strength is in the acquisition of data from the agent for analysis and subsequent decision-making process. This deep insight into the operations of the endpoint estate enables analysis and remediation across the largest of enterprises. With such power comes a significant entry cost in terms of training, both for initial configuration and for ongoing operational effectiveness. To get the most out of FireEye Endpoint Security, security operations teams should have a 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.

Part 1: Product Installation and deployment

The cloud console requires no significant installation. Once in the management console, the client installers can be downloaded from Admin/Agent Settings to install onto the client machines.

There is no user interface provided by default on the Windows client, not even a status icon. Windows pops up a warning window when malware is found. Otherwise the client is designed to be wholly managed from the centralised console with no user input.

The management console is quite different from a conventional centralised AV product. The emphasis here is clearly on acquisition of data from clients, analysis of it, and then responses to the data acquired.

From this perspective, the platform has an extremely powerful and extensive set of information gathering tools, allowing 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.

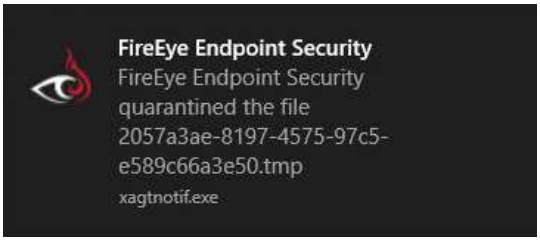
Because of this, although you could treat FireEye as a straightforward AV package, allowing the engines to process malware as it is found, the real strength comes in the analysis and containment capabilities.

There is little work required to configure the platform once the agents are deployed. Of course, you can build custom policies if you wish, or create different settings for groups that diverge from the default. 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 which will have had training and consultancy for deployment.

Part 2: Ongoing use

The desktop client is essentially invisible to the user unless something has been detected. Even then, the client is informational rather than allowing the user to interact with the software. There is no equivalent to "Scan with FireEye" available to the user. The platform relies on its information gathering and threat analysis.



The management console is not a tool to be dipped into occasionally. It offers a huge amount of power, but that comes with the need for considerable understanding of what the platform offers and how to achieve it. There is little handholding here, and the product is squarely into the large corporate space where training and consultancy will be demanded. 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, both from its information gathering, analysis and threat detection capabilities, along with the "behind the scenes" operation on the client. The emphasis here is solidly on information acquisition, analysis and reporting. This goes way beyond a conventional AV product, and allows the central administrators to initiate information gathering from a wide array of client machines, processing of the resultant information and then taking actions based upon it.

Whilst you could use the product as a straightforward AV platform, that would be to overlook its core strengths.

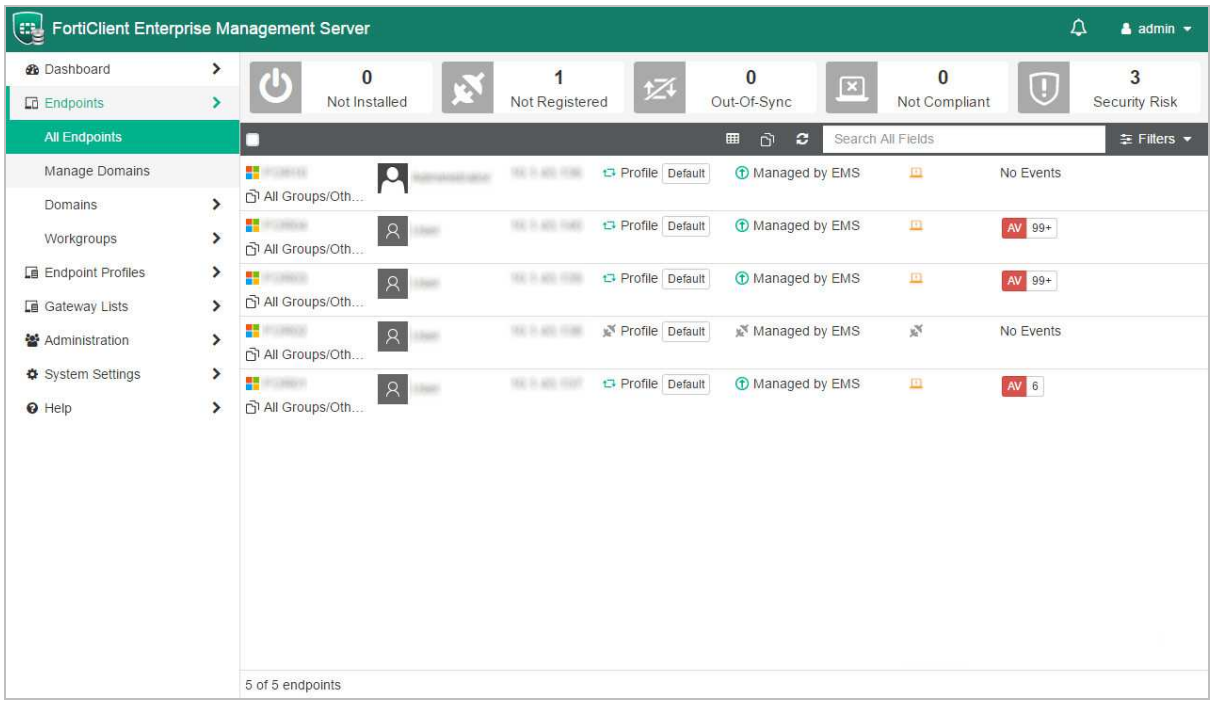
There is a basic front-page overview of the status of the deployed agents, which allows you to drill down into more detail. As an ongoing view, this is probably sufficient. But it is once you drill into the Hosts, Enterprise Search, Acquisitions and Rules sections that the power comes through. The essential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

However, 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 over such a large estate of end user computers.

Part 3: Remediation and outbreak containment

This is the key to FireEye. The ability to see what is happening, to contain and manage the devices, and then to analyse what has happened, is exceptionally powerful. But the power requires deep understanding of both the platform and of the deployed installation. This is not for the faint of heart, but it gives tools that should allow for fast and effective identification, remediation and containment.

Fortinet FortiClient with Enterprise Management Server & FortiSandbox



What is it?

Server-based management console with client AV packages. The server is called Fortinet FortiClient Enterprise Management Server, and the client is called FortiClient. The server runs on Windows Server 2008 R2 or later. There are clients for Windows, Mac OS X and Linux, with limited support on Android and iOS. Only Windows offers Advanced Threat Protection Components. There is a client for Windows Mobile, but this is for SSL VPN only, and there is a web-filtering client for Chromebook.

Product information vendor's website: https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiClient.pdf

Online support: https://www.fortinet.com/support-and-training.html

Summary

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

Part 1: Product Installation and deployment

This is a local server-based product with clients that are deployed to the desktop. Installing the management console is very simple and requires almost no user interaction. Once up and running, there are some tasks you need to perform before the client can be deployed. By default, antivirus functionality is not enabled, and so this needs to be enabled under Endpoint Profiles/Default.

Once you have done this, you can then deploy the client to the desktop, usually by browsing to the server URL and downloading the installer. After the client installer has been deployed, it fully takes over the Windows AV security role. The functionality available to the client user depends upon policy, but can allow for file/right click/Scan with FortiClient Antivirus for example, which can be useful in an environment where users are encouraged to be part of the AV strategy. The client app is somewhat modular in design, depending on what functionality has been configured and deployed.

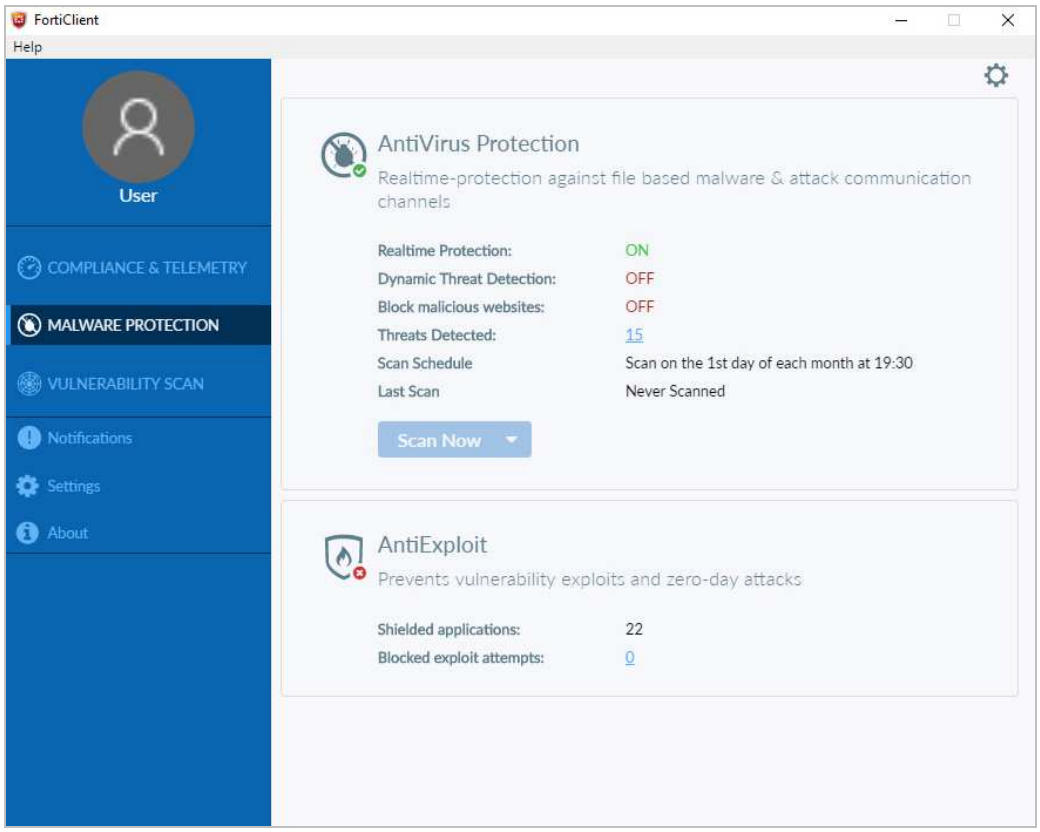
On the server side, there are good reports for devices discovered which are not part of the management structure, and it is easy to remediate this. There is a clear and clean view of the status of the network through the Dashboard/FortiClient Status view.

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

There isn't much in the way of handholding in the initial setup process for the smaller organisation. Clearly the product is aimed at the more professional, larger organisation which will have had training and consultancy for deployment.

Part 2: Ongoing use

The desktop client offers little of day-to-day use to the average user. Being able to initiate a scan is useful for some levels of users, but the client is mostly a status and version reporting tool for the administrators.



Over on the server, there is a fairly clear UI. It definitely benefits from a larger screen.

The Enterprise Management Server app has a menu system down the left-hand side, and choosing from here populates the right-hand side of the window. Starting with Dashboard, there is a fairly graphical overview of the status of the platform and clients. One criticism here is the lack of colour used to highlight issues. For example, our status screen shows "2 infected endpoints" but this is in the same grey design as other status objects reporting no issues. A little more boldness in UI design would help here.

You can click through from the items to get more data, but it sometimes is not particularly obvious what detail has been uncovered. For example, taking our "2 infected endpoints", we click through and get a view of the two devices. But again, there is little here to tell me what is actually wrong with these devices. More clarity here would help when dealing with problems and outbreaks.

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

The Endpoints menu 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 profile 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.

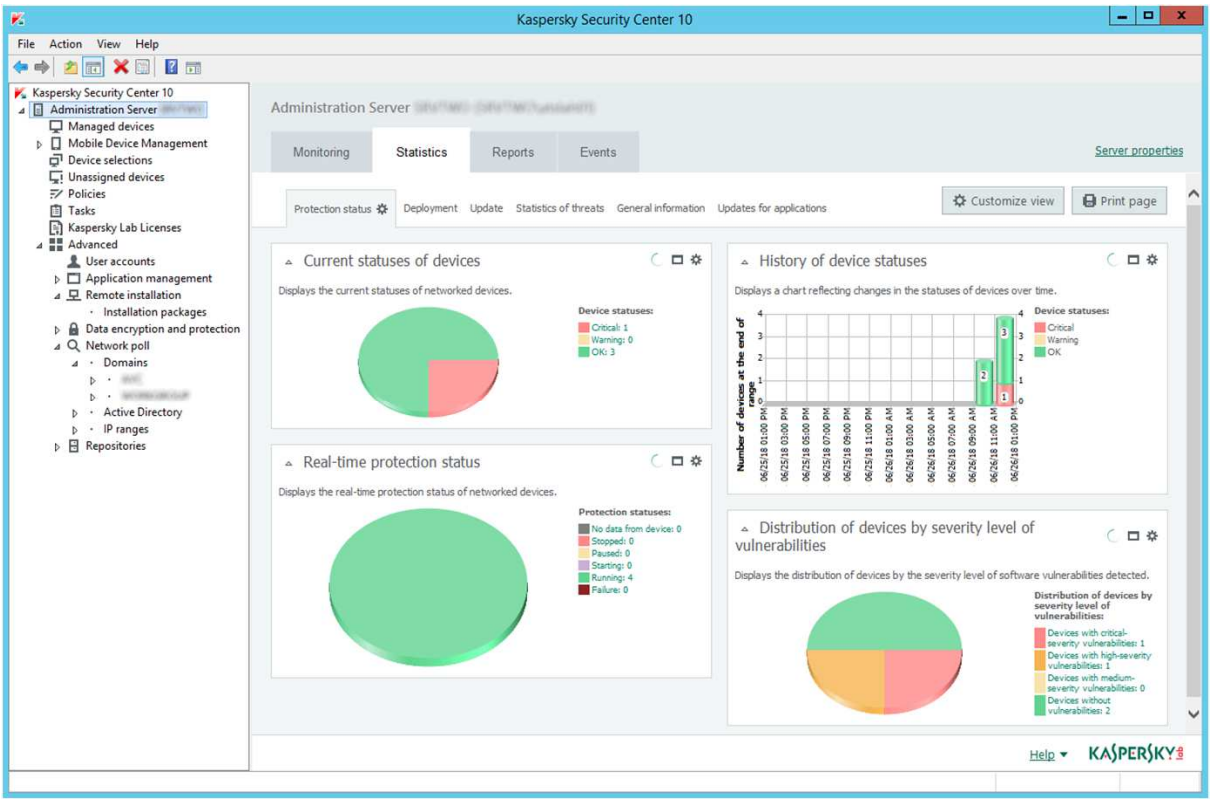
Gateway Lists allows you to manage this aspect. Finally, Administration and System Settings allows control of the underlying settings of the platform.

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

Part 3: Remediation and outbreak containment

The Enterprise Management Server lets you view the status of what is happening on the network, and to focus on those devices where there are issues that need remediation. It is a fairly standard set of tools here, and there is not a lot of deep analysis of what has happened, and where it has spread. Nevertheless, it should be fairly straightforward to handle an outbreak and ensure that the affected clients are identified and/or cleaned depending on policy and internal processes.

Kaspersky Endpoint Security for Business Select



What is it?

Server-based management console. Targeted at medium to large enterprises and organizations. Supports management of endpoint security clients for Windows, Mac, and Linux desktops, Windows and Linux servers, Android and iOS mobile devices.

Product information on vendor's website: https://www.kaspersky.com/small-to-medium-business-security/endpoint-select

Online support: https://support.kaspersky.com/kes11

Summary

A strong product aimed at medium-sized and larger businesses. Very good cross-platform support, a well-designed and customisable administrative console and management processes that will be familiar and straightforward to Windows system admins. For the purposes of this review, we used the MMC console running on the server. The product also includes a web-based console that can be accessed from any device on the local area network. Please note that Kaspersky Lab also provide a cloud-based management platform, Kaspersky Endpoint Security Cloud. This uses the same endpoint clients but provides different management capabilities, and is aimed more at smaller organisations. The Kaspersky Endpoint Security client software is also used in other Kaspersky Lab enterprise solutions such as Kaspersky Anti Targeted Attack and Kaspersky Endpoint Detection and Response.

Part 1: Product Installation and deployment

Installing the management console on the server is a straightforward process for an experienced administrator. An SQL database is required; if this has not already been set up, the admin can download the free Microsoft SQL Server Express 2014 or MySQL from links provided in the setup wizard. When installation is complete, the Protection Deployment Wizard starts. This automatically discovers devices on the network, and allows the mass installation of the network agent and endpoint protection software to desktop and server computers by remote push, and is simple to use. So far it is possible to discover desktop or server devices by leveraging on their IP subnet, Microsoft Active Directory membership, domain names and Amazon AWS API. The wizard can be rerun by clicking Advanced\Remote Installation in the console tree to add new devices at a later stage. Kaspersky Security Center additionally offers an auto-deployment policy, which means that when devices are discovered and placed into a managed group, the appropriate endpoint protection software will be installed automatically. It is also possible to create an installation package, which can be distributed via web link, network share or USB device, for individual installations. The home page of the console (Kaspersky Security Center 10) is subtitled "First steps: devices, tasks, policies and reports. Interface configuration". It provides a comprehensive range of instructions and descriptions to help the admin with everyday tasks, including "How to find your devices", "Where to view a list of all tasks", and "Where to view summary information about Administration Server operation".

Part 2: Ongoing use

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

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

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

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

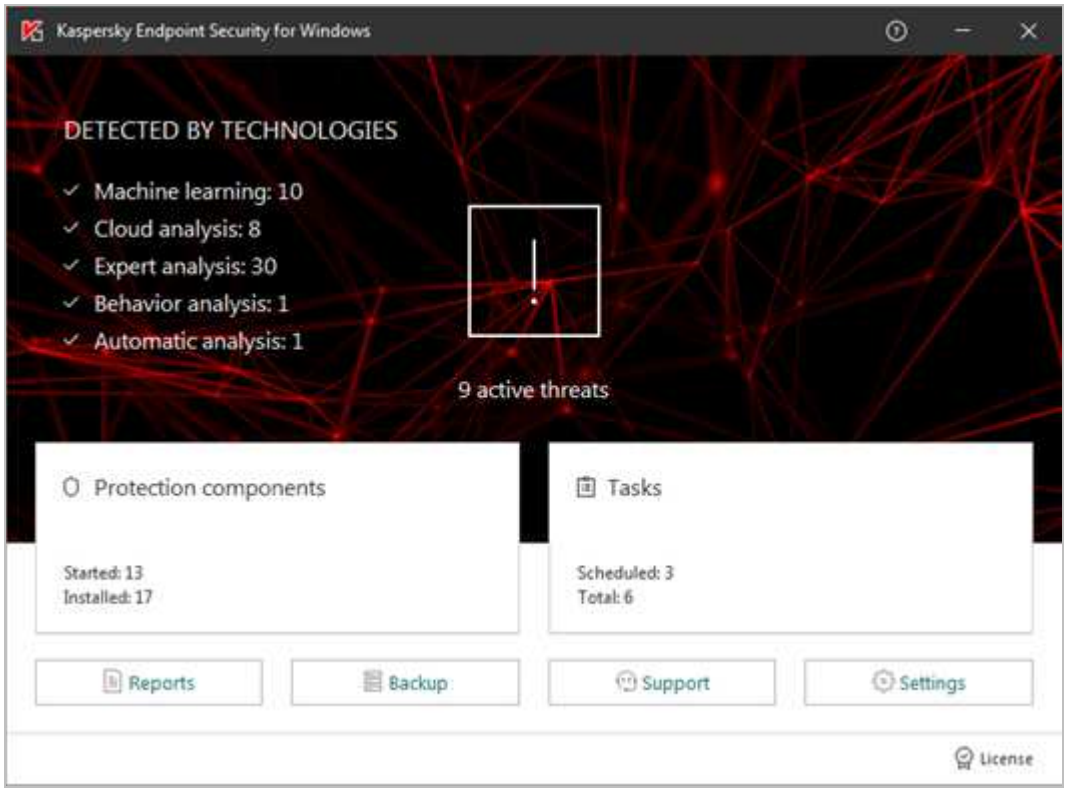
Reporting options can be found under Administration Server\Reports.

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

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

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

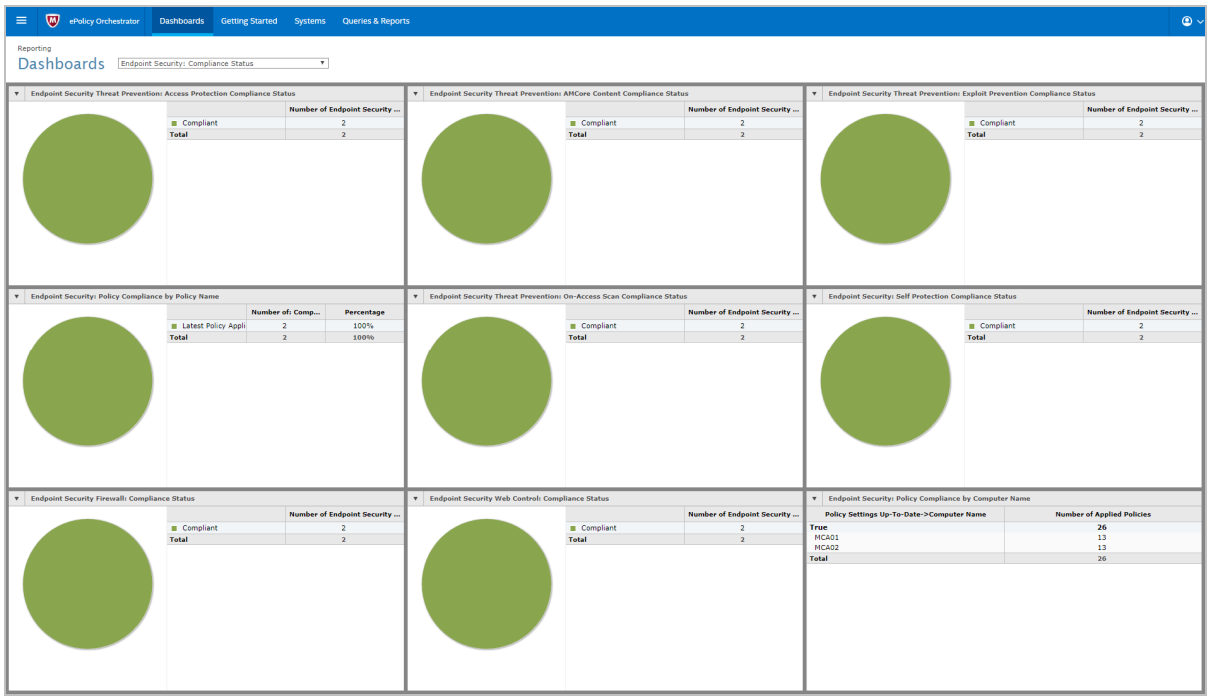
In keeping with its target group of larger enterprises, the product's philosophy is that the endpoint software should be managed by the IT staff, without any distractions for the end user. The program window is essentially a comprehensive status display, which shows security status and detection statistics for the different technologies involved, such as machine learning. Although there is a Settings button, by default the configuration is locked, and the admin makes changes to the settings from the console by using a policy. However, users can run scans of drives, folders or files by means of the context menu in Windows Explorer.



Part 3: Remediation and outbreak containment

The Statistics tab of Administration Server is an obvious place to start in the event of a malware outbreak. This will show the proportion of computers with Warning or Critical status, and lets the admin see a list of all affected computers with a single click. It is then easy to select all the computers from this list, and run an appropriate task, such as scan or update. Running a Threats Report from Administration Server\Reports will rapidly produce a very detailed report of the specific detections, locations and times. It is also possible to set event notifications in the applicable policy. This allows the admin to receive alerts by e.g. email or SMS text message for critical events, errors and warnings etc.

McAfee Endpoint Security with ATP and ePolicy Orchestrator Cloud



What is it?

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 1-10,000 users. There is also a server-based version of ePO available as an option, which has additional capabilities. However, we felt that the McAfee website is unclear as to their various offerings, and finding information about this product is not easy. There are clients for Windows and macOS.

Product information vendor's website: https://www.mcafee.com/us/solutions/cloud-security.aspx

Online support: https://community.mcafee.com/t5/Business-Product-Support/ct-p/mcafee-business

Summary

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

Part 1: Product Installation and deployment

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 main menu starting with a full menu dropdown picker. 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 fairly 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, with the selected protection components then being downloaded and installed automatically over a time period of 20 minutes or so.

Once installed, there is a program window for the client endpoint software that you can address if you wish to. It picks up the installation locale and sets the language of its UI to this automatically. This can be changed by policy, although we feel it is not immediately obvious to first-time users how to do this.

There is an icon in the System Tray area. Clicking on this offers Update Security, the main app window, Show security status, the Status monitor, and an info page.

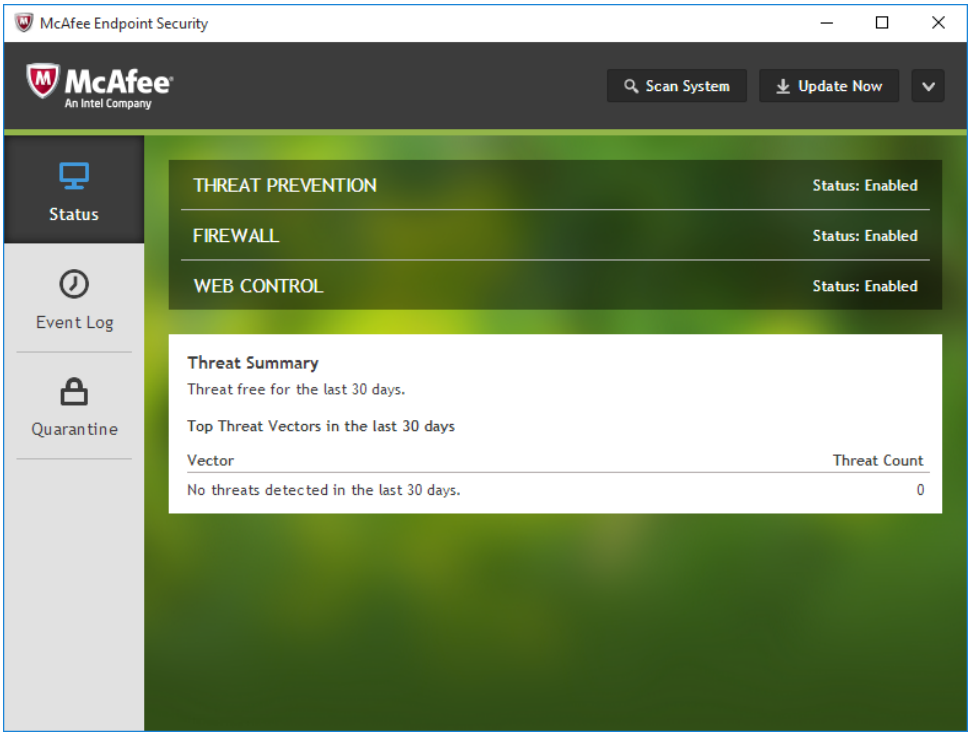
The main desktop client window is quite clear and clean, offering scanning, updating, and the status of each component.

Part 2: Ongoing use

On the endpoint client, the default policy allows the user to run scans and updates, and see component status. Most other controls – such as the event logs and quarantine – are disabled by default for standard users. However, the admin has fine-grained control of this from the console, so any or all of the controls can be enabled or disabled as desired.

Rather unusually, the main client window is resizable but the content doesn't resize to fit.

The user can right click on a file to initiate a scan for threats.



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

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

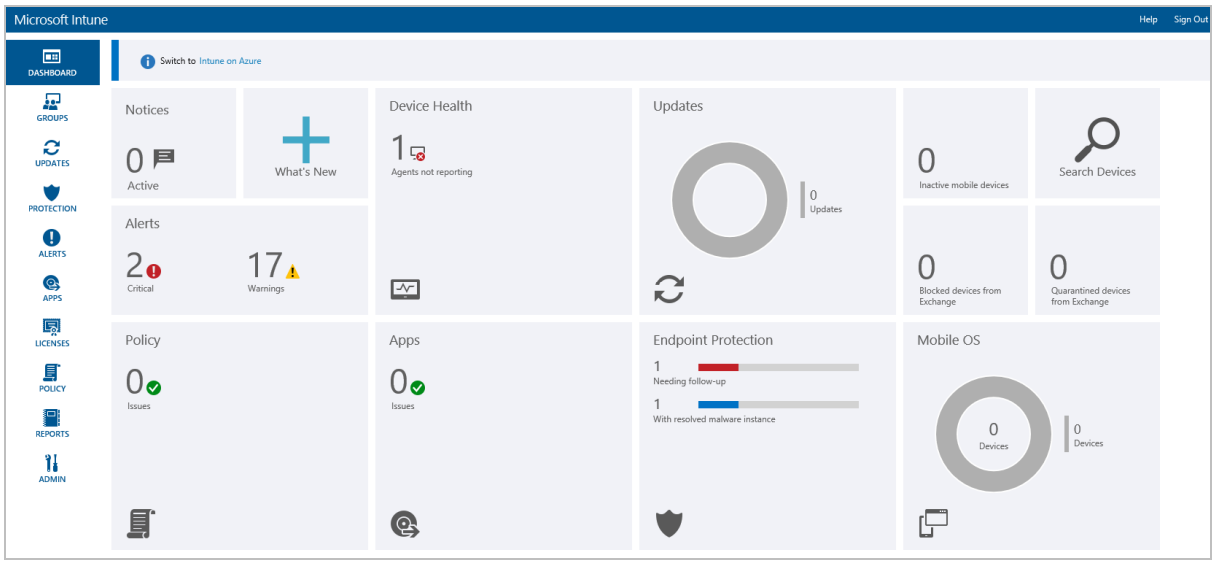
The Dashboards tab has a wide range of reports and views available, and each of them allows you to click through to more data. We found this functionality to be useable, although not quite as intuitive as we would have liked.

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

Part 3: Remediation and outbreak containment

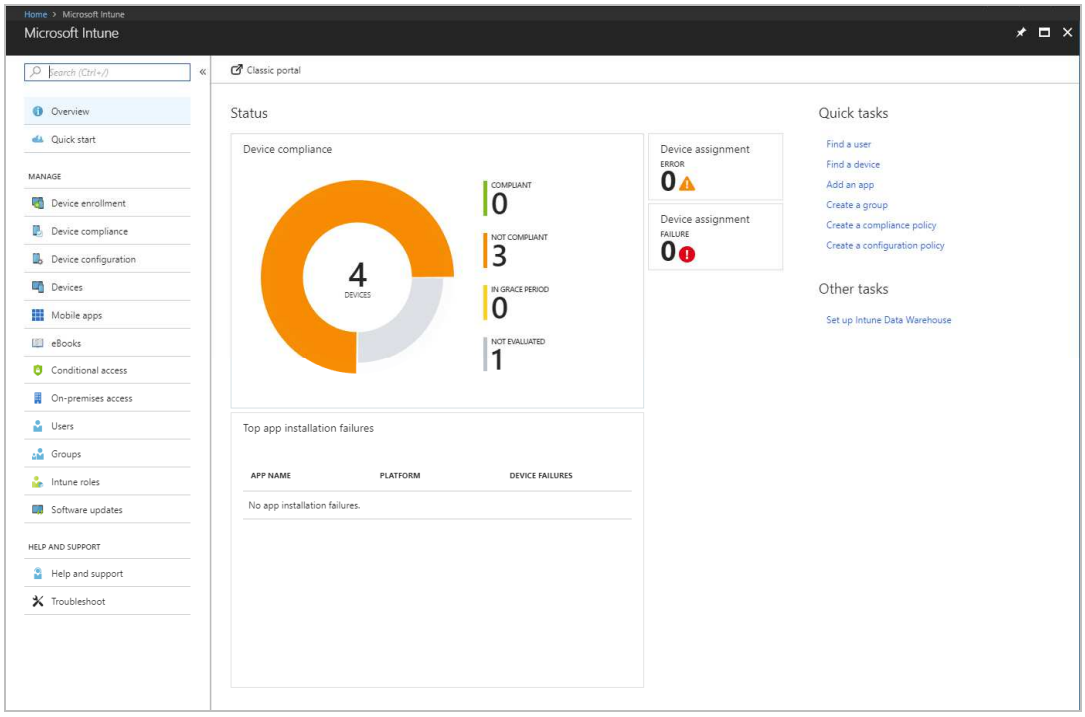
The remediation and outbreak containment area must be considered from two angles. There is a lot of information here, and a lot of deployment and management power. There is even a set of reports covering Threat Event Origins which can highlight the primary vectors of attack, the top infected users and so forth. All of this is admirable, even if the admin will have to spend some time learning how to use the features optimally.

Microsoft Windows Defender Antivirus for Business with Intune



What is it?

Intune is a cloud-based service that provides companies with security management for their devices, apps and data. Platforms covered are Windows Desktop, Windows Mobile, macOS, iOS and Android. This review covers the use of Microsoft Intune to manage Microsoft's out-of-box antivirus and security features in Windows desktop operating systems. Please note that a dual management interface is available. In this review, we have covered the Classic interface, shown above. The alternative Azure interface, which we will be reviewing in the December 2018 report, is shown below:



Product information on vendor's website: https://www.microsoft.com/en-ie/cloud-platform/microsoft-intune

Online support: https://docs.microsoft.com/en-us/intune/?WT.mc_id=UI

Summary

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

Part 1: Product Installation and deployment

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

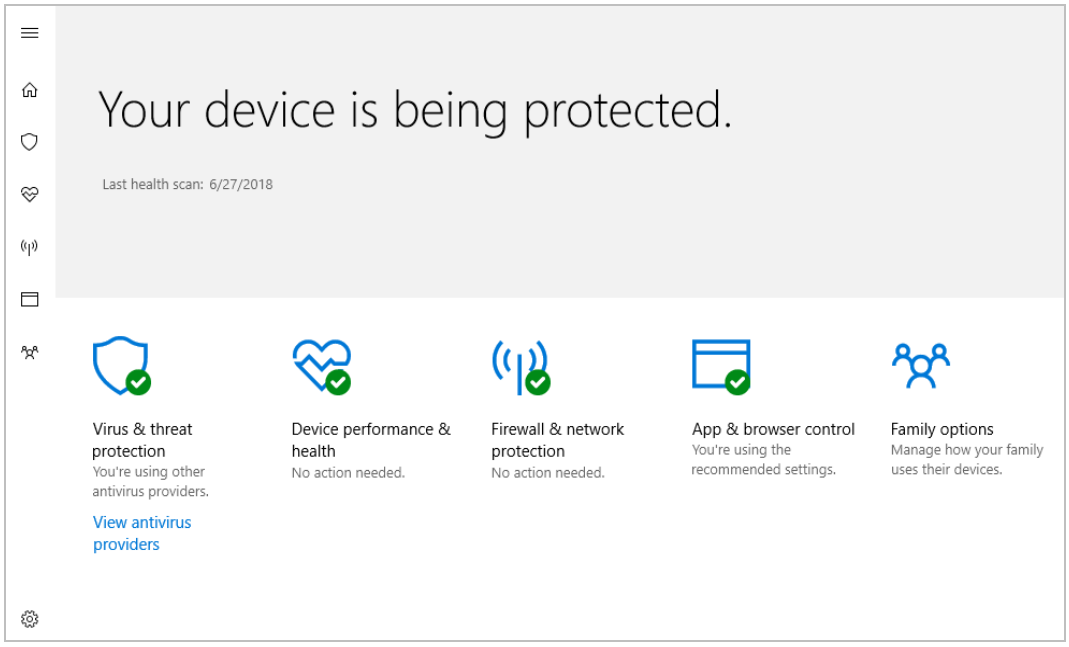
In the case of Windows 10 and Windows 8.1 clients, Microsoft's antivirus client is already incorporated into the operating system, and so no further software installation is required. With Windows 7 PCs, however, the antivirus client is not pre-installed, but is available as an update. If the Intune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

Part 2: Ongoing use

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

Under Groups\Devices, managed computers are listed, along with details such as operating system and date & time of last update. The Protection page provides a more detailed overview of malware detections, device status and most frequently detected malware, along with 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.

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

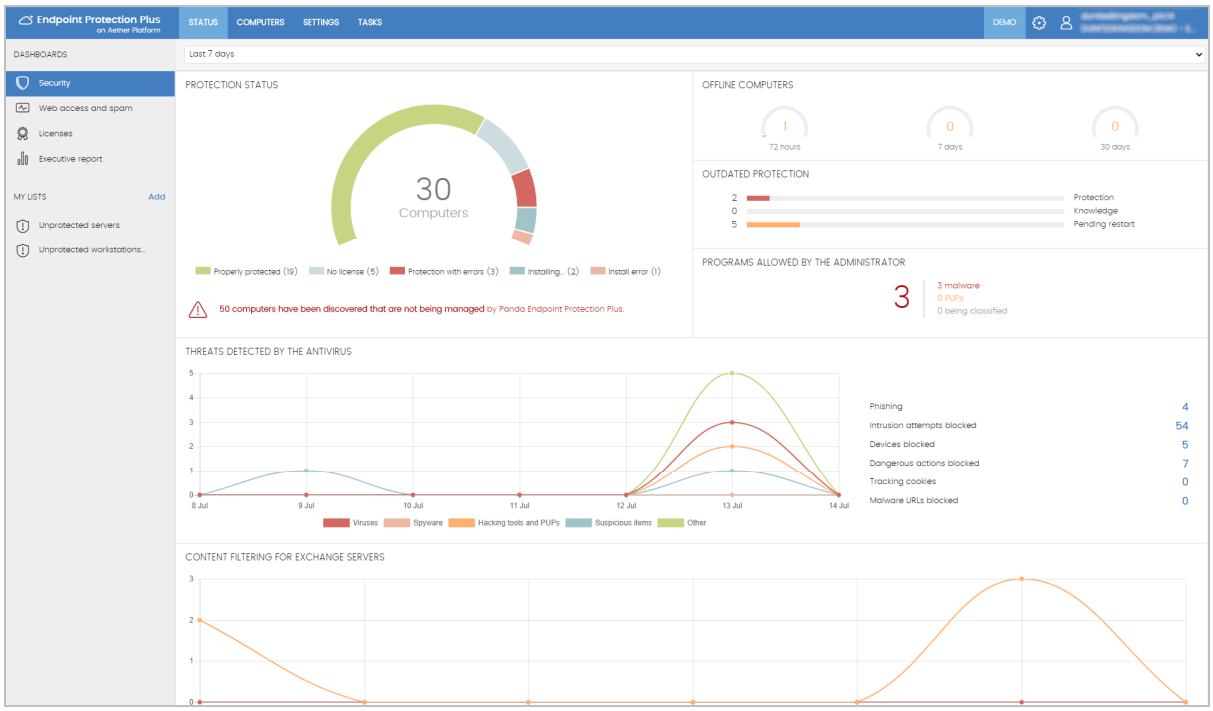


Older versions of Windows, including Windows 7 and 8.1, use the same GUI as Microsoft Security Essentials, which is similar to that of a typical consumer antivirus program. Regardless of the GUI, all variants allow the user to update malware definitions, and run full, quick, custom and context-menu scans.

Part 3: Remediation and outbreak containment

The alerts shown in the Live Tiles on the Dashboard page provide links to the relevant details pages, from which the administrator can take the necessary action. For example, clicking on the "Needing follow-up" alert in the Endpoint Protection tile opens the details page of the computer concerned. From here, the admin can use the Remote Tasks menu to run malware scans, update malware definitions or restart the computer.

Panda Endpoint Protection Plus on Aether



What is it?

Cloud-console managed system with device clients. Client software has a simple interface, which allows users to run updates and various scans. Aimed at organisations of all sizes. Support for servers, desktops and mobile devices.

With regard to information and support pages on the vendor's website, there was very little specific information about the Aether platform when we reviewed it. The only relevant page we could find about Aether was a brief description in the support section, please see link below.

https://www.pandasecurity.com/usa/support/card?id=700005

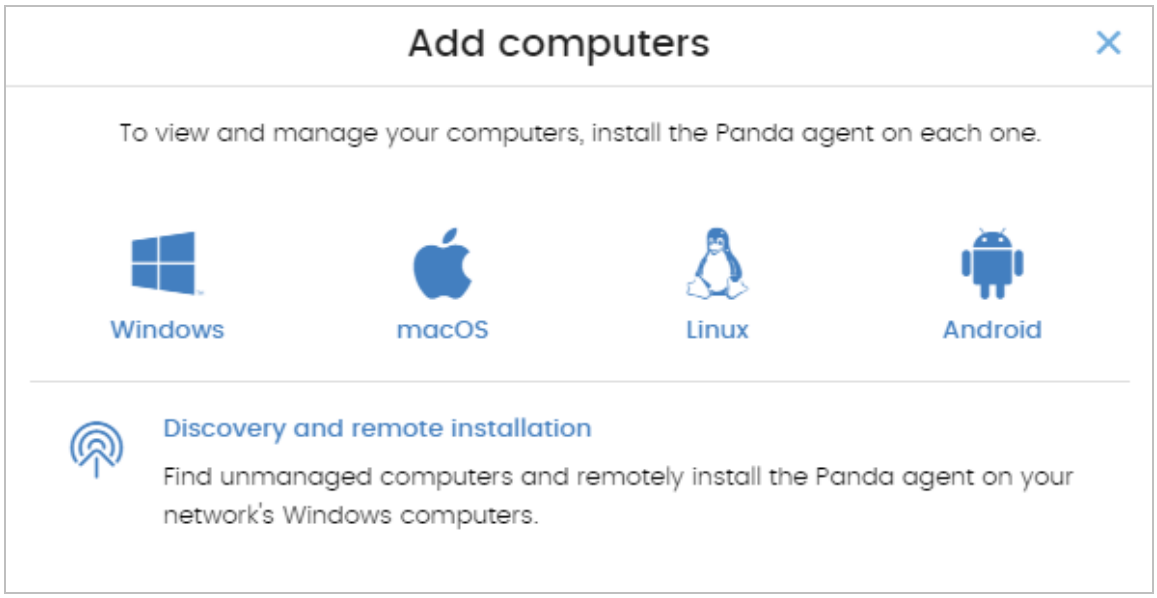
Panda tell us that more comprehensive information about Aether will be added to their website in due course.

Summary

A very strong product, powerful enough for larger organisations but simple enough for smaller businesses too. Very easy to set up as it requires no on-site server component. It has an excellent, very clear and useful administrative console, with a clear installation and deployment workflow and which delivers a strong ongoing operational platform. We were particularly impressed with the clean and obvious design of the user interface, and the speed at which it could be mastered. There is support for Windows servers, Windows/macOS/Linux PCs, and Android mobile devices.

Part 1: Product Installation and deployment

The product is wholly managed from a cloud-based console. Client deployment can be email based, where you issue a link for download and installation. This works on Windows, macOS, Linux and Android. The user clicks on the provided link to install the client, and this is then automatically licensed. Local and remote installations are also available from the Add Computers dialog.



Once a client device has connected to the management console, you can allocate it to a management group. This can be done manually, by IP address range or by Active Directory integration, and obviously helps with a multi-site organisation or one which might be split by IP address/VLAN into teams (sales, accounts etc).

Part 2: Ongoing use

Protection status and threat detection history are provided on the Status page, and this will be the first place an administrator will visit.

There are excellent graphics for detected threats, including malware types, detection origin, phishing and blocked URLs here, and it provides a solid daily overview of issues.

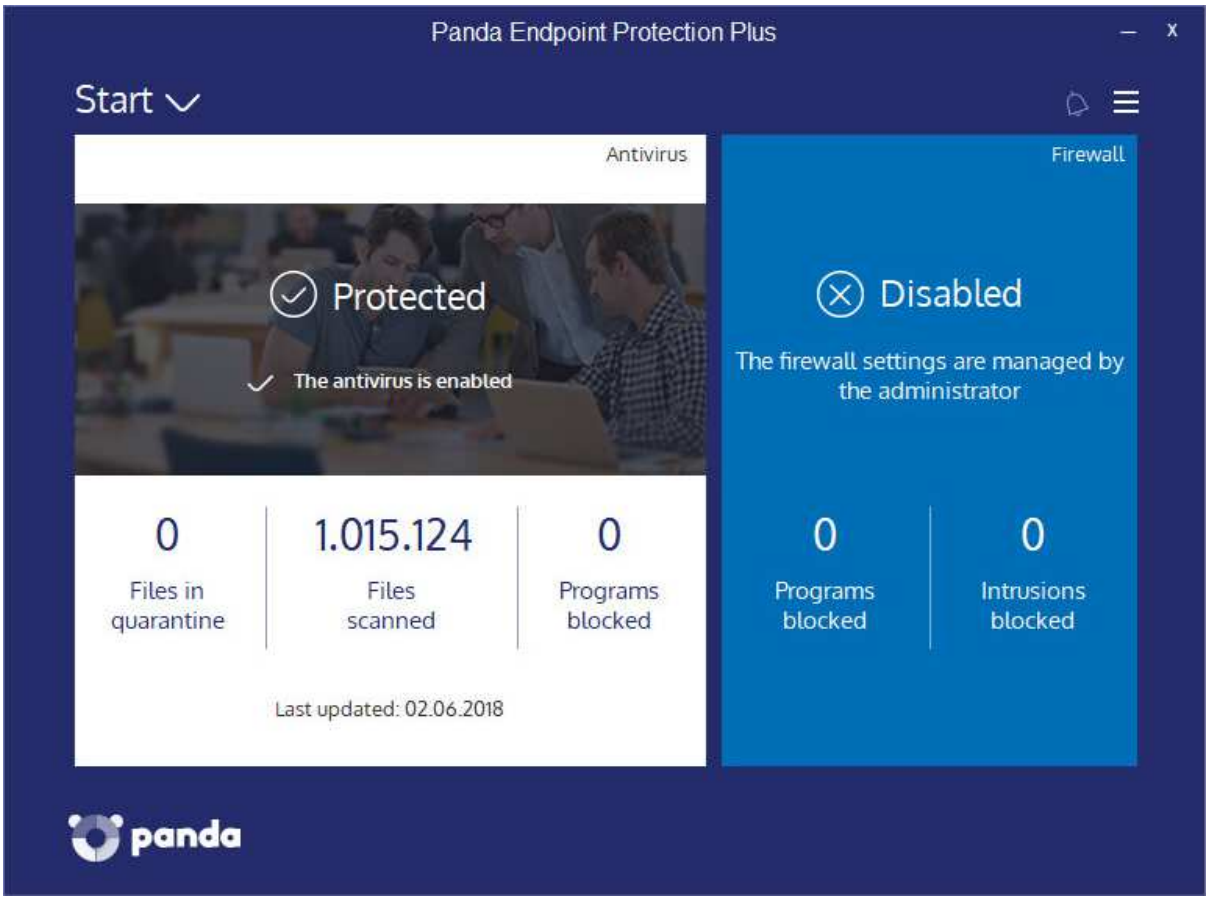
The Status page is particularly liked because it provides a headline view of the status, but allows you to click through for more detailed information. For example, clicking on the main Protection Status graphic takes you to the Computer Protection Status page. This is very clearly laid out, and shows three status categories – Antivirus, Updated Protection and Knowledge – as simple colour-coded icons. Our only criticism of the page is that we could not find a direct link to it – this would be a small but useful addition.

Sub-pages of the Status tab include Web Access and Spam, Licences, and Executive Report. The Executive Report page generates overview reports that can be emailed out on a daily, weekly or monthly routine. You can specify all computers or specific groups, and include any or all of the topics License Status, Protection Status, Detections, Web Access & Spam.

The Computers tab shows all the protected devices; despite the name, mobile devices are also included. A very simple Windows-like folder tree on the left lets you show devices by group. Basic information including IP address, operating system/version, and last connection date/time are shown.

Using the Settings tab, you can see the default configuration policies, and also create new ones. The Tasks tab allows the admin to run scheduled scans.

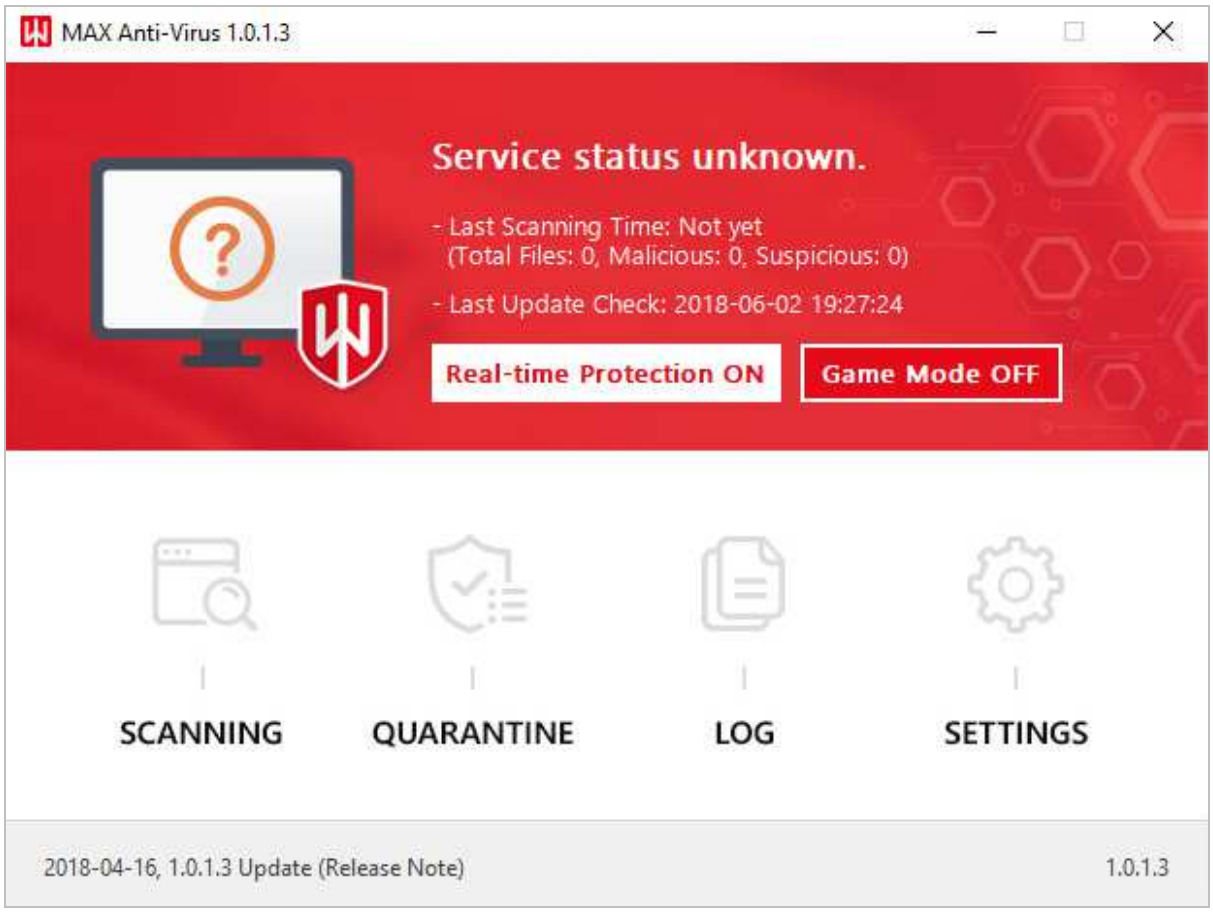
On the Windows client itself, there is a clean and clear application which pops up and allows access to solid end-user capabilities like Full Scan, Critical Areas Scan and Custom Scan. The user can force a synchronisation of the updates here too. This is a useful, clear and obvious tool which should be within the capabilities of most any user.



Part 3: Remediation and outbreak containment

The management console essentially uses the desktop client component for remediation and outbreak containment. We liked the strong graphical overview of the status of all clients, and this provided a clear indication of what was happening. This overview, with its detailed drill down, alongside the reporting capabilities, should be sufficient for an administrator to understand what has happened.

Saint Security MAX Anti-Virus



What is it?

Desktop AV package with a cloud-based deployment page. Max Anti-Virus is a desktop AV package which runs on Windows. There is a web-based console from which the client software can be downloaded, but this currently has no management or reporting capabilities. However, we are told that Saint are developing a management console which is to be released with version 2 of the product, due later this year. In its current form, the product is only suited to very small businesses. Licensing is unclear – the user account has a membership joining date, and a last access date. But it is wholly unclear as to how many seats are licensed or how this is paid for. There are clients for Windows only, with no client for macOS or mobile.

Product information vendor's website: https://www.malwares.com/maxantivirus

Online support: https://www.malwares.com/maxantivirus

Summary

There is currently no central cloud management, it is controlled entirely from the client. The promised future release of a cloud management console will hopefully improve matters considerably.

Part 1: Product Installation and deployment

Having logged into the www.malwares.com site and chosen MAX Anti-Virus tab, you can download the latest version of the Windows client. There is no macOS client nor mobile client.

Installation of the Windows client onto a Windows desktop is simple enough.

Max Anti-Virus has an icon in the System Tray area. Clicking on this offers the options to open the console, perform a scan, turn on/off real-time protection or to enable game mode.

The main program window is straightforward in its layout and use, and the user some basic tools. Turn real-time protection on/off, game mode on/off, initiate scanning, examine the quarantine, examine the log, and go into more detailed settings.

It is important to note that there is no centralised management console here, either provided by a local server or by a cloud service. Because of that, each installation of the client is effectively stand-alone and entirely independent. There is no lockdown of features and facilities – the user can disable the engine or change settings with no oversight or management from the IT function in a company.

The user would expect to have right-click access to initiate a scan against an unknown file. However, there is no shell integration provided here for Max Anti-Virus, and only the concurrently running "Scan with Windows Defender" is found by the user.

Part 2: Ongoing use

Since there is no centralised management at all, there cannot be any reporting, statistics or control. The client installation should be viewed as being entirely self-managed on the desktop.

The MAX Anti-Virus client app is straightforward to use, but has very limited reporting capabilities. You are limited to looking at the Security Threat Log which is a simple listing of the malware events that have happened on that machine.

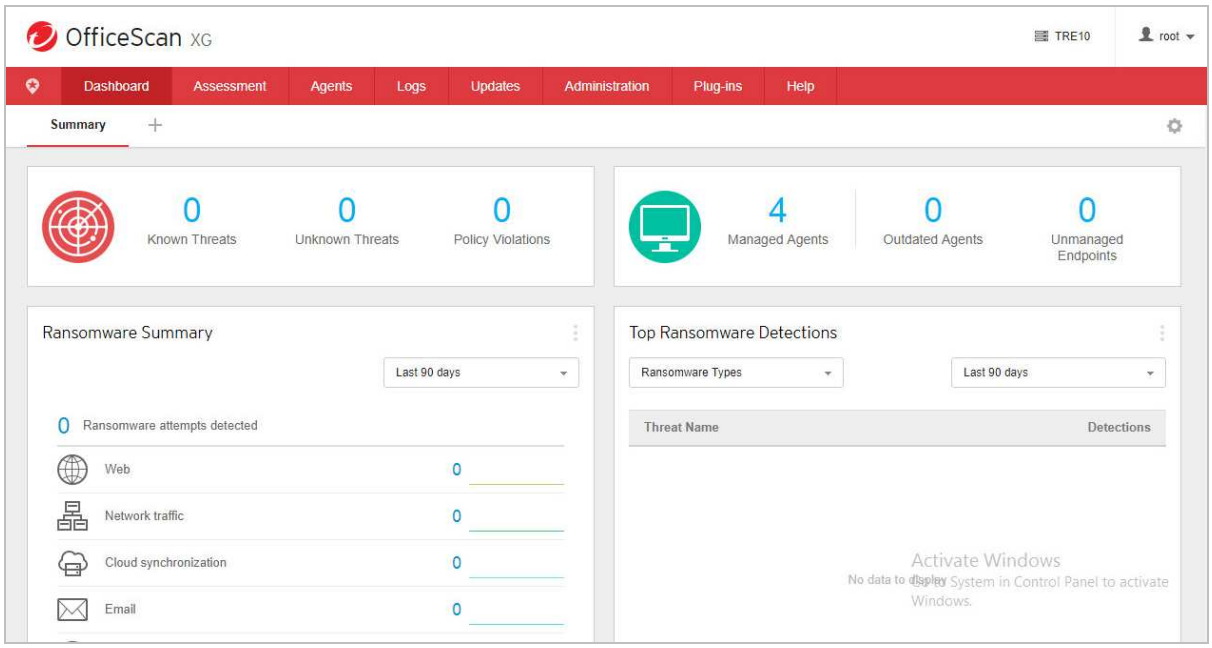
You can also view the Quarantine folder in the usual way. We were confused that the default background colour for this application is bright red, even when there is no threat.

In terms of ongoing operation in a business context, the lack of centralised management, deployment, policy and oversight means it can only be used by the smallest of businesses, until such time as centralised management functionality is provided.

Part 3: Remediation and outbreak containment

Control of outbreaks and remediation can currently only be tackled on a machine-by-machine basis, but we hope that the upcoming management console will allow both of these to be tackled centrally.

Trend Micro OfficeScan XG



What is it?

Local server-based management platform with client AV packages. The server component is installed onto a Windows Server which needs to be Server 2008 or later. Clients are available for Windows and macOS, although there is limited information on the Mac client on the TrendMicro OfficeScan website. There is no support for mobile platforms.

Product information vendor's website: https://www.trendmicro.com/en_gb/business/products/user-protection/sps/endpoint/officescan.html#

Online support: https://success.trendmicro.com/contact-support-europe

Summary

A local server-based solution to AV management. The server product is clear and relatively obvious to use, and it would scale well both up to the larger Active Directory installations and down to the smaller SME sites. Although the UI is quick to learn, it does benefit from some training and ongoing expertise to get the best from the product. However, we liked the good defaults and the clear client tool with its sensible end-user operational capabilities.

Part 1: Product Installation and deployment

Installing the server component follows the standard methodologies. It takes some time, but presents no roadblocks. Deploying Windows clients can be done in a variety of ways. You can email a download link, or use a share to the OfficeXG server from where the installer can be run by executing AutoPccP.exe. Installation of client is straightforward, but it does take some time, partly due to the enforced client scan that occurs as part of the installation process. This cannot be cancelled, but is probably a wise check when deploying into an unknown client estate.

On Windows, the client registers as an AV package and disables Windows Defender.

By default, the client installation presents the user with a wide range of capabilities. These can, of course, be managed by centralised policy. The client app has a clean interface presenting a clear overview of the status of the client and any recent events of note. There are two buttons – one offers Scan, and the other allows an immediate update. There is no right-click scan initiation facility in File Manager, but the Scan function within the OfficeScan client allows you to choose any folder or file.

There are also a few small icons on the client. You can unlock the client by supplying an administrative password, which is useful for a help desk function. The logs window gives a detailed breakdown of past events. The Settings button has configuration items, but these are usually under central policy control.

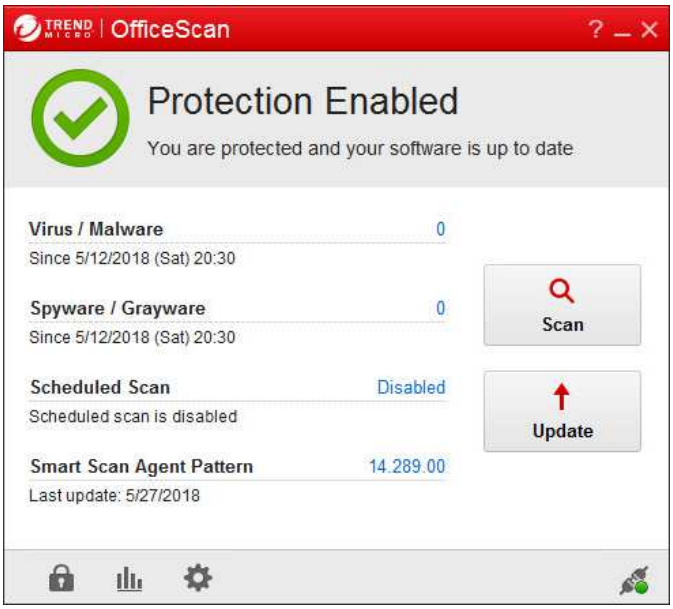
The administration console does not have a walkthrough for setting up the product. However, it is well laid-out with a clear and obvious workflow across the top-level menu items. Dashboard, Assessment, Agents, Logs, Updates, Administration, Plugins and Help

Creating users is quite straightforward, and there is a fine-grained UI here to allow specific permissions to be given to a particular role. Creating a help-desk role was quite straightforward. There is integration with Active Directory too if required.

Although there isn't much support here for a smaller organisation, it would not be beyond the capabilities of an SME or smaller consultancy to get this platform installed and operational.

Part 2: Ongoing use

The desktop client is clear, clean and easy to use. It encourages the user to interact with it, and to run updates and scans at will. Obviously, these will be managed through default policy, but it is useful for a user to have some access here, especially in the smaller workplace.



The management console immediately impresses with its clear and clean design. Dashboard gives an overview of the estate of clients, immediately informing you about key metrics like number of known threats found, how many agents are deployed and so forth. They provide a good overview of what is happening, and the default time window is a reasonable 7 days, with 14 and 30-day options too.

The Assessment menu gives access to the underlying reports. These can be run on demand or can be scheduled. Reports can be emailed out to a list of administrators. It would be a useful improvement for reports to be auto-saved to a shared file location too.

The Agents menu expands to cover all aspects of the agent configuration. You can cluster agents into groups either by NetBIOS domain, active directory or DNS, or create a custom grouping here. Global Agent Settings allows policy control of the client agents. For example, the Agent Control sub-tab here allows you to "add manual scan to the windows shortcut menu on endpoints". The firewall menu defines the policy applied to the clients, and again is policy defined. Agent Installation gives the tools to deploy the agent onto clients.

Outbreak Prevention opens a new window which covers the tools you can use to manage an outbreak.

Logs, Updates, Administration, Plug-ins and Help provide the expected functionality.

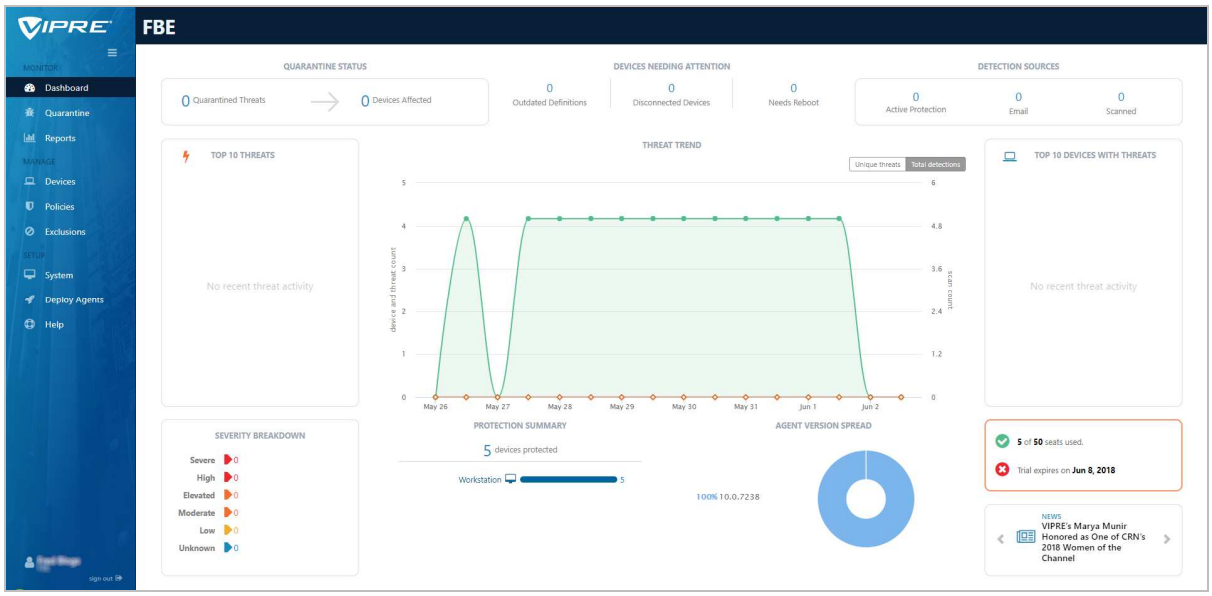
Operationally, the user interface is quite logically designed and obvious to use. The dashboard is clear, and the tasks that you can manage are placed where you would expect. Although the UI is fairly complex, and could benefit from more simplification, even a smaller SME should have little problem managing this on a day to day basis. And we are confident it should scale well with a larger Active Directory-driven installation.

Part 3: Remediation and outbreak containment

Unusually, OfficeScan XG has a dedicated panel to handle outbreaks. Firstly, you define the proportion of the installed base that you wish to manage, and then you start the Outbreak Prevention settings. This allows you to apply additional policy immediately to the affected clients. For example, this can include: limit or deny access to shared folders, block ports, deny write access to files and folders, deny access to executable compressed files, create mutex handling on malware processes and files. The user is normally informed that such a protocol is in place and that the administrator is enforcing enhanced policy.

We like this approach because it gives an obvious place for the administrative team to go to in order to apply additional emergency policy in a controlled and coherent way. Undoing this bundle of settings is easy to do, and normal client operation will return.

VIPRE Endpoint Security Cloud



What is it?

Cloud-based management console with desktop AV package. The cloud package, called Endpoint Security Cloud Edition, claims that it "can be purchased, configured and have a site deployed in a matter of three clicks and less than 10 minutes" which is a bold claim. VIPRE Endpoint Security is the client that runs on the desktop. It isn't clear on their website which platforms are supported, but the management console offers a Windows agent. There is no obvious support for macOS or mobile devices. VIPRE claims that its infrastructure runs on the Amazon AWS cloud, and that this brings unparalleled efficiency, scalability and growth.

Product information vendor's website: https://www.vipre.com/cloud/

Online support: https://businesssupport.vipre.com/support/home which also offers live chat directly from the management console

Summary

This product impresses with its clear and clean design, its simple operational processes and the strong reporting features. Even a relatively inexperienced user should have little difficulty in getting the platform running well, and to have the agent deployed successfully onto the target desktop machines. We would have liked better clarity about the range of clients supported. It is clear from the product that there is a Windows agent, but not others, and the website doesn't help. Nevertheless, the product both in its cloud implementation shows what clear thinking and good deployment flow can bring, along with strong reporting and an obvious process for day-to-day operation.

Part 1: Product Installation and deployment

Access to the web portal is straightforward via a standard username/password login combination.

The user interface immediately impresses with its clean and clear design. The first page you see has a Getting Started area, which covers deploying of agents, creation of users and the setting of appropriate policies. The next section deals with more advanced post-setup topics, such as Dashboard, Devices, Exclusions, Notifications and Reports.

Once you are up and running, 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.

The next section is Manage which covers Devices, an area which shows which devices are in play, and their operational status. For any device or collection of devices, you can easily choose to assign policy, run a scan, update the definitions, reboot the device, delete the agent and other management functions.

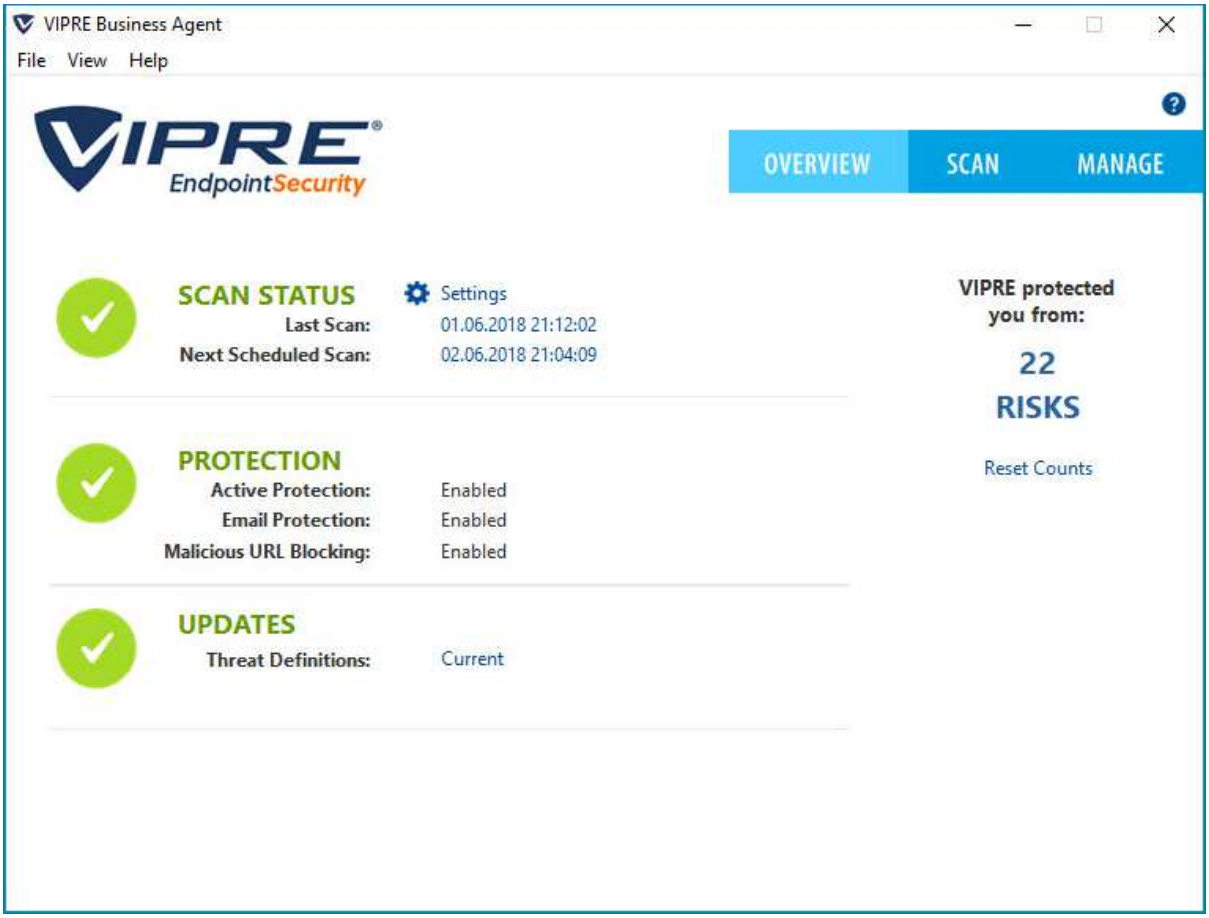
Policies enables the creation of policy definitions controlling how the clients are allowed to operate, and the security policies that they will deploy. There is a wide range of customisation here, but the “Default Enterprise” settings will probably be appropriate for most users. It is here, of course, that you can allow users to interact with the VIPRE client, allowing them to scan items via a right click, or forcing USB devices to be scanned on insertion.

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

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

Part 2: Ongoing use

Starting with the client, the available capability here will depend on the deployed policy. By default, we had the opportunity for the user to right click on items of concern, which always strikes us as a good balance. The user can see basic reporting, and have a daily operational relationship with the platform.



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 who are allowed to interact with the system is simple, and they can have the role of Admin or Analyst, which might be appropriate for 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 can easily imagine this platform being appropriate for any size of organisation, from a small business deployment covering a few seats through to a larger organisation. The UI of the management console was always responsive under testing, although it is not known how well it would fare with thousands of desktops and large numbers of events. We suspect it will scale well.

Part 3: Remediation and outbreak containment

The clarity of the management console is a significant plus point here, showing clearly what is happening and on which devices. The ability to set policy in a visible way, with sensible defaults and clear explanations, is also important, as is the ability to easily get client machines to perform the required updating and scanning in the event of an incident. The reporting helps here too, allowing you to easily discover what happened, when and on which machines.

Features (as of June 2018)	Avast Business Antivirus Pro Plus	Bitdefender Endpoint Security Elite (GravityZone Elite HD)	CrowdStrike Endpoint Protection Platform Standard Bundle	Emsisoft Anti-Malware & Enterprise Console	Endgame Protection Platform	eScan Corporate 360 with MDM & Hybrid Network Support	ESET Endpoint Security & Remote Administrator	FireEye Endpoint Security	FortiClient with EMS & FortiSandbox	Kaspersky Endpoint Security for Business Select	McAfee Endpoint Security with ePO & ATP	Microsoft Windows Defender Antivirus for Business with Intune	Panda Endpoint Protection Plus on Aether	Saint Security MAX Antivirus	Trend Micro OfficeScan XG	VIPRE Endpoint Security Cloud
Available Console Types																
Cloud-based console	•	•	•		•	•		•		•	•	•	•		•	•
On-premise server-based console	•			•	•	•	•	•	•	•	•			•	•	•
Virtual appliance	•	•			•		•	•			•				•	
Client software deployment methods																
Creation of .exe or .msi installer package	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•
Email a link to remote users to install the software themselves	•	•	•		•	•			•	•	•	•	•	•	•	•
Push installation from the console		•		•	•	•	•		•	•	•	•	•		•	•
Supported Operating Systems																
Microsoft Windows	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•
Virtual environments (such as VMware, HyperV)		•	•		•	•	•	•		•	•	•	•	•	•	•
Apple macOS	•	•	•		•		•	•	•	•	•	•	•		•	•
Linux		•	•		•	•	•	•	•	•	•	•	•			
Google Android						•	•		•	•	•	•	•			•
Apple iOS		•				•	•		•	•						•
Windows Features																
Anti-Malware	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•
Phishing protection	•	•		•		•	•		•	•	•	•	•		•	•
Web access control / webfilter (custom blacklisting of URLs / site categories)	•	•		•		•	•		•	•	•	•	•		•	•
Firewall	•	•				•	•			•	•	•	•		•	•
Anti-Spam	•	•				•	•				•	•	•		•	•
Data or Email encryption		•				•					•					
Data backup						•	•				•					
Detection notifications are shown on the client	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•
Settings & Uninstall protection	•	•	•	•	•	•	•	•	•	•	•	•	•		•	•
Registers as AV product in Windows Security Center	•	•	•	•		•	•	•	•	•	•	•	•		•	•
Has capabilities to clean-up an already infected system (remove IOC)	•	•		•		•	•	•	•	•	•	•	•		•	•
Protection settings are enabled by default (out-of-the-box-protection)	•	•		•	•	•	•			•	•	•	•	•	•	•
Cross-platform central management	•	•	•		•	•	•	•	•	•	•	•	•			
Right-click on-demand scan of files/folders	•	•		•		•	•		•	•	•	•	•		•	•
Splunk support		•	•		•	•	•	•	•		•					
The online malware detection rate is the same as offline		•		•		•		•								•
EDR (Endpoint Detection and Response)			•		•			•								
Scans files only on execution			•							•	•					
Languages																
Which languages can be used to contact support?	English, Spanish, French, German, Italian, Portuguese, Russian, Norwegian	English, Spanish, German, Romanian, French	English	English, German, French, Russian, Italian	English	English	All	English, Japanese, French, Italian, Spanish, Portuguese, Arabic, Turkish, Herbrew	English, French, German, Japanese, Chinese	English, German, Dutch, French, Danish, Finnish, Italian, Norwegian, Portuguese, 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, Korean	English	English, Swedish, Danish
Which interface languages is the product available in?		English, Spanish, German, Romanian, French, Italian, Portuguese, Polish, Russian		English, German, French, Russian, Italian, Spanish, Arabic, Catalan, Persian, Finnish, Greek, Hungarian, Japanese, Korean, Dutch, Polish, Portuguese, Slovenian, Swedish, Thai, Turkish, Vietnamese, Chinese		English, German, French, Russian, Spanish, Korean	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, 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, Spanish, French, Italian, Japanese, Korean, Polish, Russian, Chinese	
Which languages are the manuals available in?				English, German, French		English			English			English, Arabic, Bulgarian, Chinese, Croatian, Czech, Danish, Dutch, Estonian, Finnish, French, German, Greek, Hebrew, Hungarian, Italian, Japanese, Korean, Latvian, Lithuanian, Norwegian, Polish, Portuguese, Romanian, Russian, Serbian, Slovak, Slovenian, Spanish, Swedish, Thai, Turkish, Ukrainian	English, Spanish			
Pricing (approximate List Prices as of June 2018; depending on the number of agents purchased, deal size or term, country/region, volume discounts will apply/vary)																
1,000 clients, 3 years, $ US / € DE																
Cloud-based console	$ 43200 / 36300 €	$ 68700 / 52500 €	$ 205800 / 176900 €	N/A	$ 72900 / 72900 €	$ 41600 / 35500 €	N/A	$ 93000 / 120900 €	N/A	$ 43700 / 40000 €	$ 45900 / 45900 €	$ 216000 / 183600 €	$ 42000 / 42000 €	N/A	$ 22700 / 22700 €	$ 51300 / 43200 €
On-premise Windows-based console		N/A	N/A	$ 23900 / 23900 €		N/A	$ 38000 / 31600 €		$ 21000 / 21000 €	$ 48600 / 41400 €	$ 108200 / 108200 €	N/A	N/A	$ 9600 / € 8400 €		N/A
Virtual appliance		$ 68700 / 52500 €		N/A					N/A	N/A	$ 157800 / 157800 €			N/A		
Minimum number of seats																
Seats	1	5	130	1	250	5	5	100	100	5	10	1	1	1	5	5

Copyright and Disclaimer

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

AV-Comparatives (July 2018)