Independent Tests of
Anti-Virus Software

Business Security Test

TEST PERIOD: AUGUST – NOVEMBER 2023
LAST REVISION: 6TH DECEMBER 2023

WWW.AV-COMPARATIVES.ORG

Contents

Introduction

This is the second half-year report of our Business Main-Test Series[1] of 2023, containing the results of the Business Real-World Protection Test (August-October), Business Malware Protection Test (September), Business Performance Test (November), as well as the product descriptions.

The test-series consists of three main parts:

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

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

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

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

To complete the picture of each product's key capabilities, there is a **product description** 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[2]. In such cases, other products in the range may have a different type of management console (server-based as opposed to cloud-based, or vice-versa); they may also include additional features not included in the tested product, such as endpoint detection and response (EDR). Readers should not assume that the test results for one product in a vendor's business range will necessarily be the same for another product from the same vendor.

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

[2] For additional tests, please also have a look at the "Endpoint Prevention and Response (EPR) Tests" https://www.av-comparatives.org/enterprise/testmethod/endpoint-prevention-response-tests/ and "Advanced Threat Protection (ATP) Tests" https://www.av-comparatives.org/enterprise/testmethod/advanced-threat-protection-tests/

Tested Products

The following business products[3] were tested under Microsoft Windows 10 64-bit:

Vendor	Product	Version August	Version September	Version October	Version November
Avast	Ultimate Business Security	23.7	23.8	23.9	23.10
Bitdefender	GravityZone Business Security Premium	7.9	7.9	7.9	7.9
CISCO	Secure Endpoint Essentials	8.1	8.1	8.1	8.2
CrowdStrike	Falcon Pro	6.58	7.01	7.04	7.04
Cybereason	NGAV	22.1	22.1	22.1	22.1
Elastic	Security	8.9	8.9	8.10	8.10
ESET	PROTECT Entry with ESET PROTECT Cloud	10.1	10.1	10.1	10.1
G Data	Endpoint Protection Business	15.6	15.6	15.6	15.6
K7	On-Premises Enterprise Security Advanced	14.2	14.2	14.2	14.2
Kaspersky	Endpoint Security for Business – Select, with KSC	12.1	12.2	12.2	12.3
Microsoft	Defender Antivirus with MEM	4.18	4.18	4.18	4.18
Sophos	Intercept X Advanced	2023.1	2023.1	2023.1	2023.1
Trellix	Endpoint Security (ENS)[4]	10.7	10.7	10.7	10.7
VIPRE	Endpoint Detection & Response	13.0	13.1	13.1	13.1
VMware	Carbon Black Cloud Endpoint Standard	3.9	3.9	3.9	3.9
WatchGuard	Endpoint Protection Platform	8.0	8.0	8.0	8.0

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

[3] Information about additional third-party engines/signatures used by some of the products: **CISCO**, **Cybereason**, **G Data** and **VIPRE** use the **Bitdefender** engine (in addition to their own protection features). **CISCO** uses also the **ClamAV** engine. **VMware** uses the **Avira** engine (in addition to their own protection features). **G Data**'s OutbreakShield is based on Data443.

[4] The "ENS" version of **Trellix** in this test uses the erstwhile **McAfee** engine (now owned by Trellix), opposed to the "HX" version which uses the FireEye engine (McAfee Enterprise and FireEye were merged into Trellix in 2022).

Settings

In business environments, and with business products in general, it is usual for products to be configured by the system administrator, in accordance with vendor’s guidelines, and so we invited all vendors to configure their respective products.

Only a few vendors provide their products with optimal default settings which are ready to use, and did therefore not change any settings.

Please keep in mind that the results reached in the Enterprise Main-Test Series were only achieved by applying the respective product configurations described here. Any setting listed here as enabled might be disabled in your environment, and vice versa. This influences the protection rates, false alarm rates and system impact. The applied settings are used across all our Enterprise Tests over the year. That is to say, we do not allow a vendor to change settings depending on the test. Otherwise, vendors could e.g. configure their respective products for maximum protection in the protection tests (which would reduce performance and increase false alarms), and maximum speed in the performance tests (thus reducing protection and false alarms). Please not that some enterprise products have all their protection features disabled by default, so the admin has to configure the product to get any protection.

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

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

CISCO: “On Execute File and Process Scan” set to Active; “Exploit Prevention: Script Control” set to “Block”; “TETRA Deep Scan File” disabled; “Exclusions” set to “Microsoft Windows Default”; Engines “ETHIS”, “ETHOS”, “SPERO” and “Step-Up” disabled. “MaxScanFileSize” increased to 500 MB.

CrowdStrike: everything enabled and set to maximum, i.e. “Extra Aggressive”. “On-demand Scans” and Uploading of “Unknown Detection-Related Executables” and “Unknown Executables” disabled.

Cybereason: “Anti-Malware” enabled; “Signatures mode” set to “Quarantine”; “Artificial intelligence” set to “Moderate”; “Fileless protection” enabled and set to “Prevent”; Update interval set to 1 minute.

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

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

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

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

Microsoft: “CloudExtendedTimeOut” set to 55; “PuaMode” enabled.

Sophos: “Threat Graph creation”, “Web Control” and “Event logging” disabled.

Trellix: “Web Control” add-on for Google Chrome enabled. “Firewall” and “Exploit Prevention” disabled.

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

VMware: policy set to “Advanced”.

Avast, K7, WatchGuard: default settings.

Management Summary

AV security software caters to businesses of all sizes and types. However, the suitability of a particular software solution varies depending on the scale of operations. Before selecting an appropriate software, it is crucial to understand the business environment in which it will be deployed, enabling informed decision-making.

Let's focus on the smaller end of the market. These environments typically emerge from micro businesses where consumer-grade AV products might have sufficed. However, as the business expands beyond a few machines, the importance of AV management becomes evident. This is particularly critical when considering the potential business and reputational damage that can result from a significant, uncontained malware outbreak.

In the smaller SME segment, on-site IT managers or professionals are often absent. Instead, the responsibility of "computer maintenance" falls on an interested non-expert, usually a senior partner with other primary roles in the business. This model is commonly found in retail, accountancy, and legal professions. In such cases, it is essential to have a centralized overview of all computing assets and instant clarity regarding the protection status in a straightforward manner. If necessary, remediation can involve temporarily disconnecting a machine, transferring the user to a spare device, and waiting for an IT professional to arrive on-site for cleanup and integrity checks. While users may be kept informed about the status, managing the platform remains the responsibility of one or a few senior individuals within the organization. These decisions are often driven by the company's overriding need for data confidentiality.

In larger organizations, having dedicated on-site IT specialists, including network security professionals, is expected. The Chief Technology Officer (CTO) in such organizations seeks straightforward, real-time statistics and a management overview that allows for detailed analysis of data to address emerging issues. Software installation engineers play a vital role in ensuring correct and appropriate deployment of the AV package on new machines. It is crucial to monitor and detect when machines become disconnected from the network to prevent the presence of rogue and unprotected devices on the LAN. Additionally, a help desk role serves as the first line of defense, responsible for monitoring and tracking malware activity and taking appropriate actions, such as initiating a wipe-and-restart process on compromised computers.

In this larger organizational structure with multiple layers, remediation and tracking become key tasks. Identifying a malware infection is only the beginning; effectively handling and tracing the infection back to its original point are essential functions in larger organizations. If weaknesses in network security and operational procedures cannot be clearly identified, the risk of future breaches remains high. To fulfil this role, comprehensive analysis and forensic tools are required, with a focus on understanding the timeline of an attack or infection originating from a compromised computer. However, presenting this information coherently is challenging, as it involves processing vast amounts of data and employing tools to filter, categorize, and highlight unfolding issues, often in real time.

Due to these significant differences, it is crucial to accurately assess the organization's needs and risk profile to identify the appropriate security tool. Under-specifying can lead to breaches that are difficult to manage, while over-specifying results in a system so complex that it becomes challenging to deploy, use, and maintain effectively. The business becomes vulnerable to attacks due to the confusion and lack of compliance resulting from an overly complex system.

One crucial consideration for businesses is choosing between a cloud-based or server-based console. Cloud-based consoles are quick to set up and generally do not require additional configuration of client devices. On the other hand, server-based consoles require more initial setup work, including configuring clients and the company firewall. However, they provide the advantage of having the entire setup on the company's premises and under the direct control of the administrator. For smaller businesses with limited IT staff, cloud-based consoles may be a more accessible option. It's important to note that manufacturers often offer both cloud-based and server-based options for managing their products. The console types mentioned here refer specifically to the product used in our tests. It is recommended to consult the respective vendor to explore other console types that may be available.

Avast and **VIPRE** offer user-friendly cloud consoles that are well-suited for smaller businesses without dedicated IT staff. These solutions are also suitable for larger companies, allowing for business growth. **G Data** and **K7** utilize server-based consoles that are straightforward for experienced Windows professionals and can be used by SMEs and beyond.

For businesses of the same size seeking cloud-based management solutions, **Bitdefender**, **ESET**, **Kaspersky**, **Microsoft**, **Sophos**, and **WatchGuard** provide robust and comprehensive options. **Cybereason** and **VMware** may require a slightly steeper learning curve but are also suitable for this category of business.

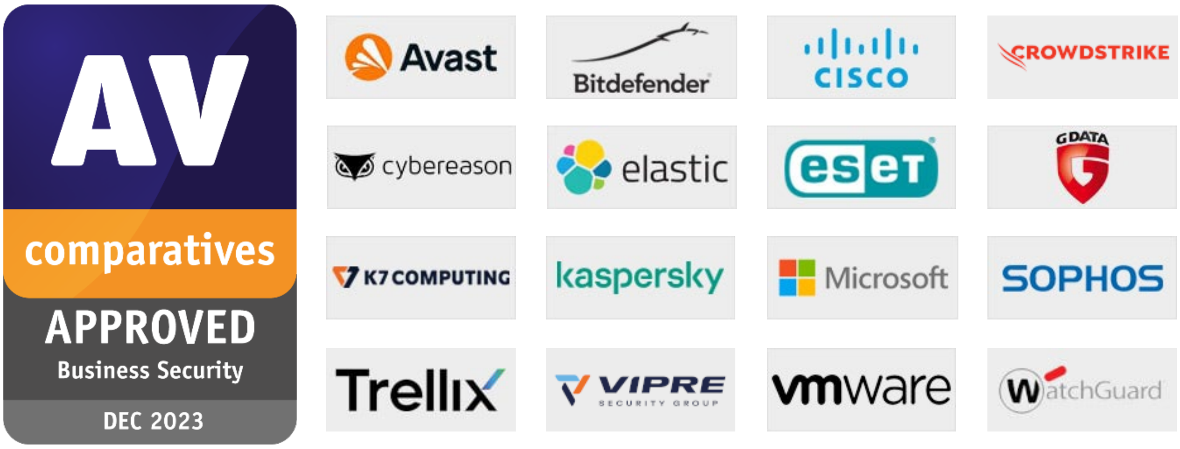
At the larger end of the market, **CISCO**, **CrowdStrike**, **Elastic**, and **Trellix** offer exceptionally powerful tools. However, their suitability for your organization, both in its current state and future growth plans over the next five years, should be carefully planned. Seeking external expertise and consultancy is recommended during the planning and deployment stages, as these tools require significant training and ongoing support. Nonetheless, they offer capabilities that surpass those of smaller packages.

AV-Comparatives' Approved Business Product Award

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

To be certified in December 2023 as an "Approved Business Product" by AV-Comparatives, the tested products must score at least 90% in the Malware Protection Test, with zero false alarms on common business software, and an FP rate on non-business files below the *Remarkably High* threshold. Additionally, products must score at least 90% in the overall Real-World Protection Test (i.e. over the course of four months), with less than fifty false alarms on any clean software/websites, and zero false alarms on common business software. Tested products must also avoid major performance issues (impact score must be below 40) and have fixed all reported bugs in order to gain certification.

We congratulate the vendors shown below, whose products met the certification criteria, and are thus given the AV-Comparatives Approved Business Security Product Award for December 2023:



Real-World Protection Test (August-November)

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

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

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

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

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

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

Test Procedure

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

Lab Setup

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

Software

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

Preparation for every testing day

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

Testing Cycle for each malicious URL

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

Protection

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

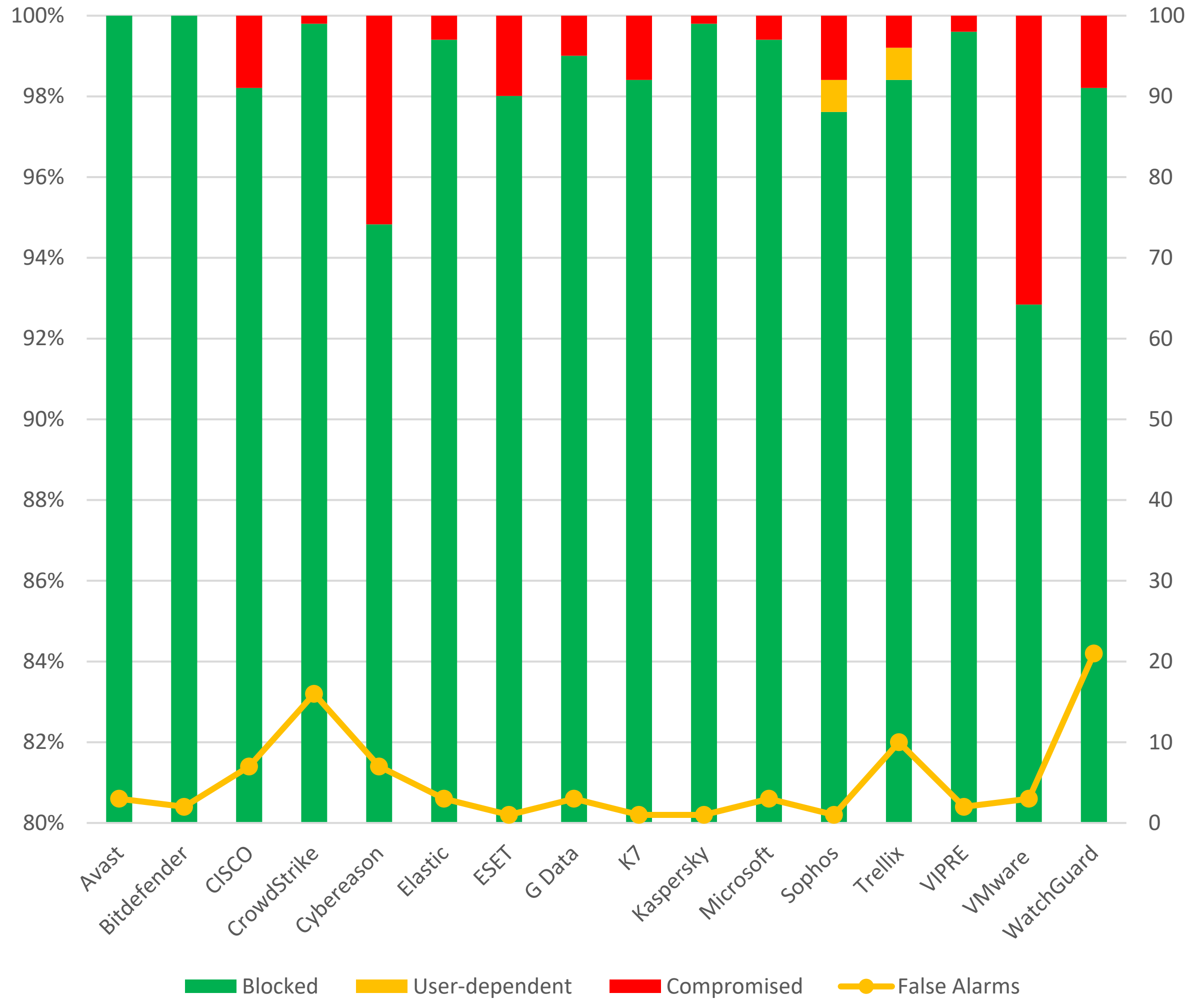
Due to the dynamic nature of the test, i.e. mimicking real-world conditions, and because of the way several different technologies (such as cloud scanners, reputation services, etc.) work, it is a matter of fact that such tests cannot be repeated or replicated in the way that e.g. static detection rate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

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

Test Set

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

The results below are based on a test set consisting of **503** test cases (such as malicious URLs), tested from the beginning of August 2023 till the end of November 2023.



	Blocked	User dependent	Compromised	PROTECTION RATE [Blocked % + (User dependent %)/2][5]	False Alarms
Bitdefender	503	-	-	100%	2
Avast	503	-	-	100%	3
Kaspersky	502	-	1	99.8%	1
CrowdStrike	502	-	1	99.8%	16
VIPRE	501	-	2	99.6%	2
Elastic, Microsoft	500	-	3	99.4%	3
G Data	498	-	5	99.0%	3
Trellix	495	4	4	98.8%	10
K7	495	-	8	98.4%	1
CISCO	494	-	9	98.2%	7
WatchGuard	494	-	9	98.2%	21
ESET	493	-	10	98.0%	1
Sophos	491	4	8	98.0%	1
Cybereason	477	-	26	94.8%	7
VMware	467	-	36	92.8%	3

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

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

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

a) Wrongly blocked domains (while browsing)

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

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

b) Wrongly blocked files (while downloading/installing)

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

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

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

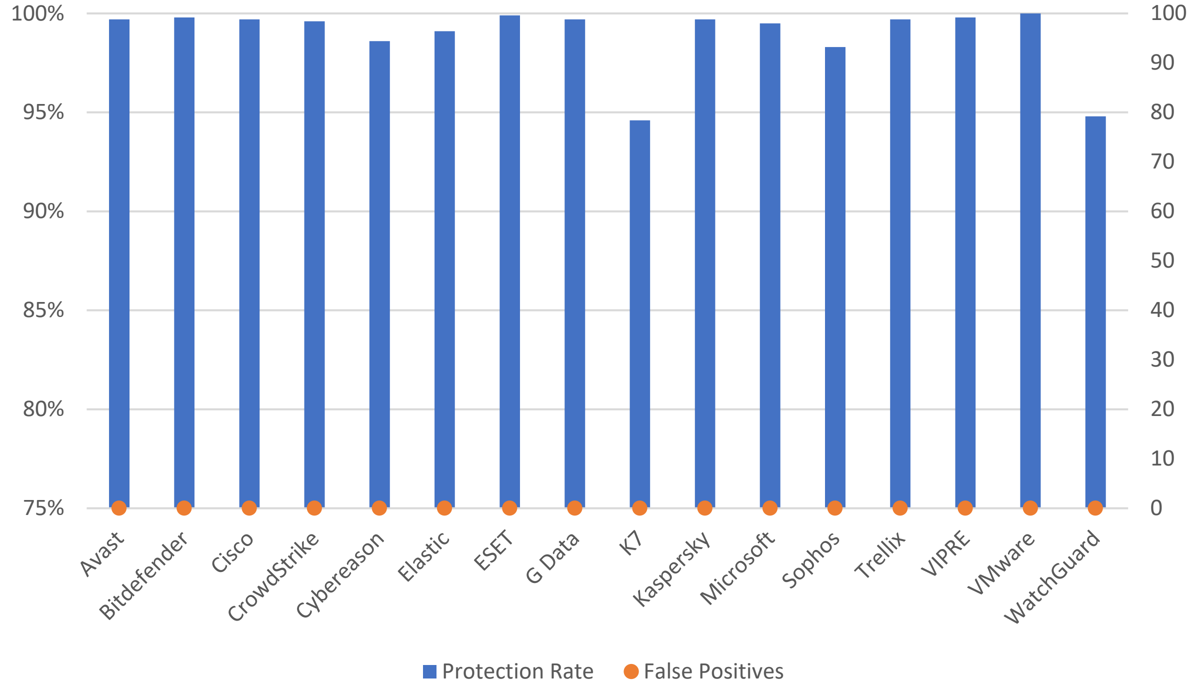
Malware Protection Test (September)

The Malware Protection Test assesses a security program's ability to protect a system against infection by malicious files before, during or after execution. The methodology used for each product tested is as follows. Prior to execution, all the test samples are subjected to on-access scans (if this feature is available) by the security program (e.g. while copying the files over the network). Any samples that have not been detected by the on-access scanner are then executed on the test system, with Internet/cloud access available, to allow e.g. behavioural detection features to come into play. If a product does not prevent or reverse all the changes made by a particular malware sample within a given time period, that test case is considered to be a miss. For this test, **1,009** recent malware samples were used.

False positive (false alarm) test with common business software

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

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



	Malware Protection Rate	False Alarms on common business software
VMware	100%	0
ESET	99.9%	0
Bitdefender, VIPRE	99.8%	0
Avast, CISCO, G Data, Kaspersky, Trellix	99.7%	0
CrowdStrike	99.6%	0
Microsoft	99.5%	0
Elastic	99.1%	0
Cybereason	98.6%	0
Sophos	98.3%	0
WatchGuard	94.8%	0
K7	94.6%	0

In order to better evaluate the products' detection accuracy and file detection capabilities (ability to distinguish benign files from malicious files), we also performed a false alarm test on non-business software and uncommon files. Results are shown in the tables below; the false alarms found were promptly fixed by the respective vendors. However, organisations which often use uncommon or non-business software, or their own self-developed software, might like to consider these results. Products are required to have an FP rate on non-business files below the *Remarkably High* threshold in order to be approved. This is to ensure that tested products do not achieve higher protection scores by using settings that might cause excessive levels of false positives.

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

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

Performance Test (November)

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

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

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

Test methods

The tests were performed on an Intel Core i7 CPU system with 8GB of RAM and SSD system drives. We consider this machine configuration as "**high-end**". The performance tests were done on a clean Windows 10 64-Bit system (English) and then with the installed business security client software. The tests were done with an active Internet connection to allow for the real-world impact of cloud services/features. Care was taken to minimize other factors that could influence the measurements and/or comparability of the systems. Optimizing[6] 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[7] different types of clean files from one place to another, archiving and unarchiving files, downloading files from the Internet and launching applications (opening documents). We believe that increasing the number of iterations increases our statistical precision. This is especially true for performance testing, as some noise is always present on real machines. We perform each test multiple times and provide the median as result. We also used a third-party, industry-recognized performance testing suite (PC Mark 10 Professional) to measure the system impact during real-world product usage. We used the predefined *PC Mark 10 Extended* test. Readers are invited to evaluate the various products themselves, to see what impact they have on their systems (due to e.g. software conflicts and/or user preferences, as well as different system configurations that may lead to varying results).

[6] https://www.av-comparatives.org/the-balance-between-performance-low-speed-impact-and-real-time-detection-enterprise-products/

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

Test cases

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

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

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

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

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

Downloading files: Common files are downloaded from a webserver on the Internet.

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

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

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

Overview of single AV-C performance scores

Vendor	File copying		Archiving/ unarchiving	Installing applications	Launching applications		Downloading files	Browsing Websites
	On first run	On subsequent runs			On first run	On subsequent runs		
Avast	very fast	very fast	very fast	very fast	very fast	very fast	very fast	very fast
Bitdefender	very fast	very fast	fast	very fast	mediocre	fast	fast	very fast
CISCO	very fast	very fast	fast	mediocre	fast	very fast	very fast	very fast
CrowdStrike	fast	very fast	very fast	mediocre	mediocre	fast	very fast	very fast
Cybereason	mediocre	very fast	fast	fast	very fast	very fast	very fast	very fast
Elastic	very fast	very fast	very fast	fast	mediocre	mediocre	very fast	very fast
ESET	fast	fast	very fast	very fast	very fast	very fast	very fast	very fast
G Data	very fast	very fast	fast	very fast	very fast	very fast	fast	very fast
K7	very fast	very fast	very fast	very fast	very fast	very fast	very fast	very fast
Kaspersky	mediocre	very fast	very fast	very fast	very fast	very fast	very fast	very fast
Microsoft	very fast	very fast	mediocre	fast	fast	very fast	very fast	very fast
Sophos	mediocre	very fast	fast	fast	mediocre	fast	very fast	very fast
Trellix	mediocre	fast	very fast	very fast	mediocre	fast	very fast	very fast
VIPRE	very fast	very fast	very fast	very fast	fast	fast	fast	very fast
VMware	fast	very fast	very fast	mediocre	mediocre	fast	very fast	very fast
WatchGuard	very fast	very fast	very fast	fast	very fast	very fast	very fast	very fast

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[8] testing suite. Users using PC Mark 10 benchmark[9] 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[10].

"No security software" is tested on a baseline[11] system without any security software installed, which scores 100 points in the PC Mark 10 benchmark.

	PC Mark Score
Baseline	*100*
ESET	98.5
K7	98.4
Avast	98.2
G Data	98.1
Cybereason	98.0
WatchGuard	97.9
Bitdefender	97.8
Kaspersky	97.6
VIPRE	97.4
Trellix	97.2
Microsoft	96.5
Elastic	96.4
CrowdStrike	96.1
VMware	95.9
CISCO	94.8
Sophos	94.5

[8] For more information, see https://benchmarks.ul.com

[9] PC Mark® is a registered trademark of Futuremark Corporation / UL.

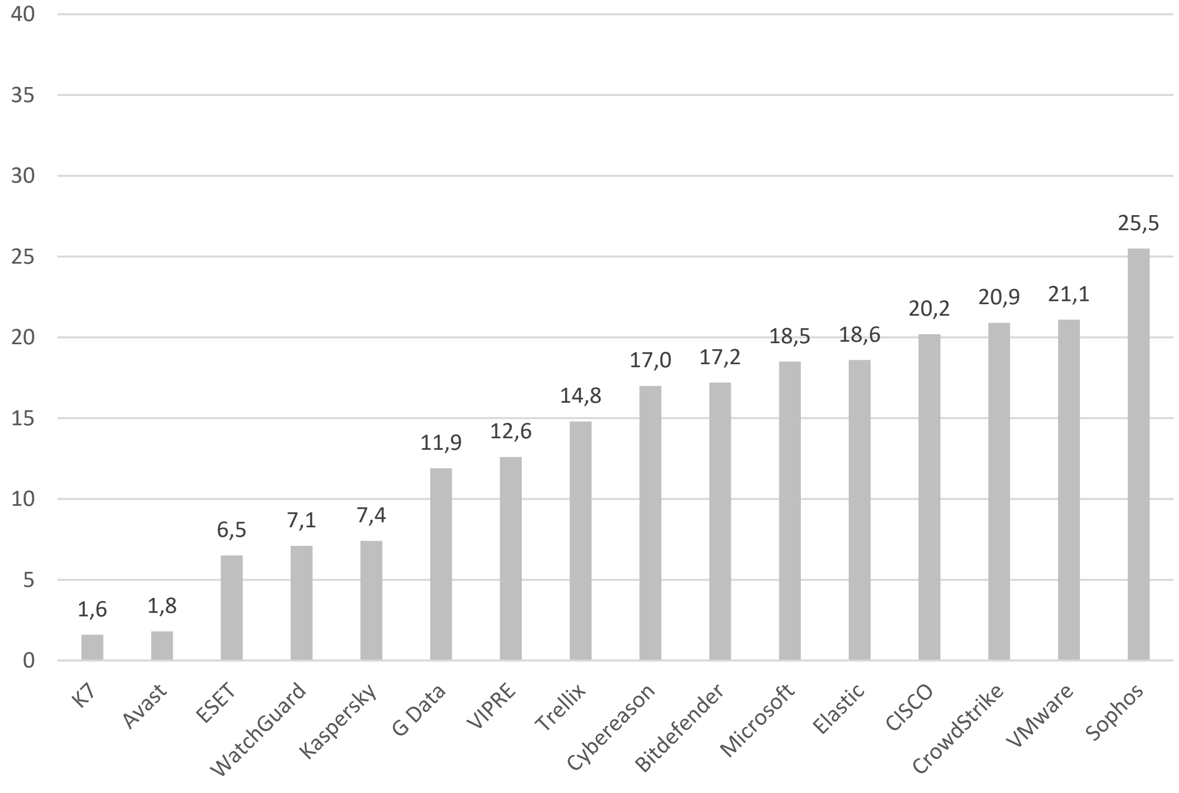
[10] http://s3.amazonaws.com/download-aws.futuremark.com/PCMark_10_Technical_Guide.pdf (PDF)

[11] Baseline system: Intel Core i7 machine with 8GB RAM and SSD drive

Summarized results

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

	AV-C Score	PC Mark Score	TOTAL	Impact Score
K7	90	98.4	188.4	1.6
Avast	90	98.2	188.2	1.8
ESET	85	98.5	183.5	6.5
WatchGuard	85	97.9	182.9	7.1
Kaspersky	85	97.6	182.6	7.4
G Data	90	98.1	178.1	11.9
VIPRE	90	97.4	177.4	12.6
Trellix	78	97.2	175.2	14.8
Cybereason	75	98.0	173.0	17.0
Bitdefender	75	97.8	172.8	17.2
Microsoft	75	96.5	171.5	18.5
Elastic	75	96.4	171.4	18.6
CISCO	75	94.8	169.8	20.2
CrowdStrike	73	96.1	169.1	20.9
VMware	73	95.9	168.9	21.1
Sophos	70	94.5	164.5	25.5



Product Descriptions

On the following pages, you will find product descriptions of the tested enterprise products. Please note that the product descriptions are based on information provided by vendors. For more detailed and current information, please visit the vendors' websites.

Avast Ultimate Business Security:
https://www.avast.com/de-de/business/products/ultimate#pc

Bitdefender GravityZone Business Security Premium:
https://download.bitdefender.com/resources/media/materials/business/en/bitdefender-business-security-datasheet.pdf

Cisco Secure Endpoint Essentials:
https://www.cisco.com/c/en/us/products/collateral/security/fireamp-endpoints/datasheet-c78-733181.html

CrowdStrike Falcon Pro:
https://www.crowdstrike.com/wp-content/uploads/2019/02/crowdstrike-falcon-pro-bundle-data-sheet.pdf

Cybereason NGAV:
https://www.cybereason.com/hubfs/dam/collateral/data-sheets/cr-ngav-redefined-data-sheet.pdf

Elastic Security:
https://www.elastic.co/guide/en/security/current/index.html

ESET PROTECT Entry with ESET PROTECT Cloud:
https://www.eset.com/fileadmin/ESET/US/product-overviews/business/ESET-PROTECT-B2B-offering.pdf

G DATA Endpoint Protection Business:
https://www.gdata.help/display/BS/Business+Solutions

K7 On-Premises Enterprise Security Advanced:
https://www.k7computing.com/us/pdf/k7-enterprise-brochure.pdf

Kaspersky Endpoint Security for Business – Select, with KSC:
https://content.kaspersky-labs.com/se/media/de/business-security/KESB_Product_Datasheet_Advanced_Customer.pdf

Microsoft Defender Antivirus with Microsoft Endpoint Manager:
https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/?view=o365-worldwide

Sophos Intercept X Advanced:
https://assets.sophos.com/X24WTUEQ/at/2b38x8h3fjg68jmm7tvbsp8m/sophos-intercept-x-ds.pdf

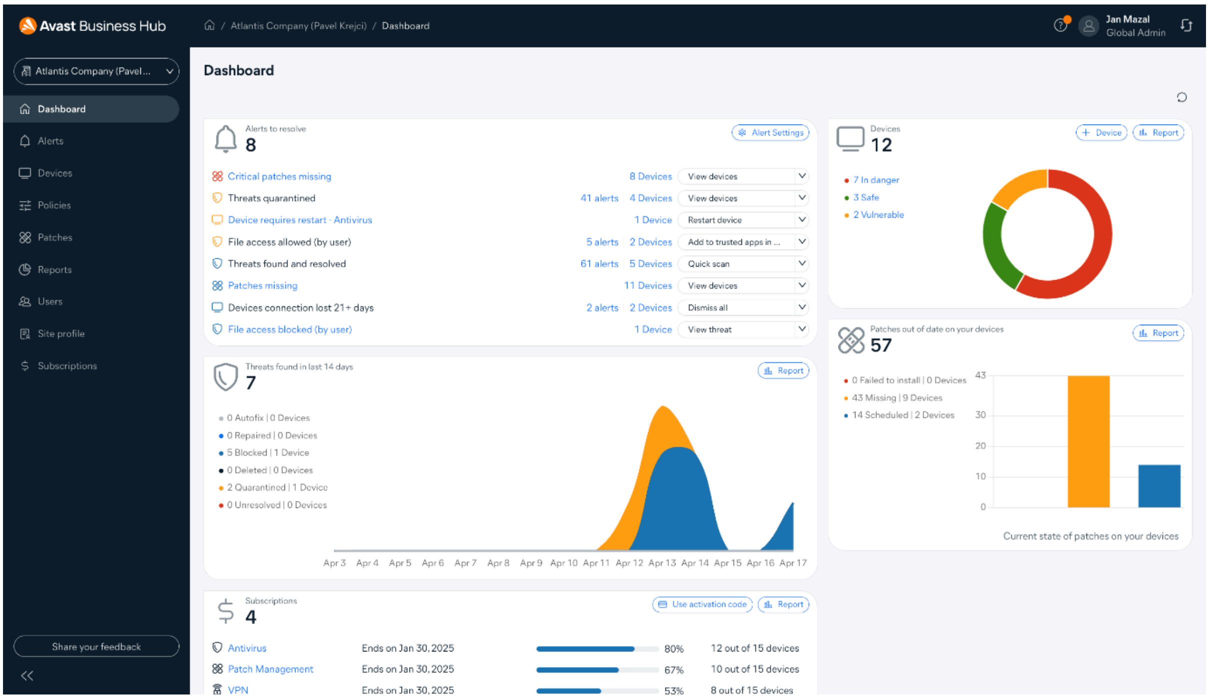
Trellix Endpoint Security (ENS):
https://www.trellix.com/en-us/assets/solution-briefs/trellix-endpoint-protection-platform-solution-brief.pdf

VIPRE Endpoint Detection & Response:
https://www.vipre.com/wp-content/uploads/2023/01/VIPRE_2022_DS_ENDPOINT-DETECTION-AND-RESPONSE_Jan_2023.pdf

VMware Carbon Black Cloud Endpoint Standard:
https://carbonblack.vmware.com/resource/carbon-black-cloud-endpoint-standard-technical-overview#section2

WatchGuard Endpoint Protection Platform (EPP):
https://www.watchguard.com/de/wgrd-resource-center/docs/watchguard-epp

Avast Ultimate Business Security



Dashboard

Alerts to resolve
8

Critical patches missing		8 Devices	View devices
Threats quarantined	41 alerts	4 Devices	View devices
Device requires restart - Antivirus		1 Device	Restart device
File access allowed (by user)	5 alerts	2 Devices	Add to trusted apps in ...
Threats found and resolved	61 alerts	5 Devices	Quick scan
Patches missing		11 Devices	View devices
Devices connection lost 21+ days	2 alerts	2 Devices	Dismiss all
File access blocked (by user)		1 Device	View threat

Devices
12

- 7 In danger
- 3 Safe
- 2 Vulnerable

Threats found in last 14 days
7

- 0 Autofix | 0 Devices
- 0 Repaired | 0 Devices
- 5 Blocked | 1 Device
- 0 Deleted | 0 Devices
- 2 Quarantined | 1 Device
- 0 Unresolved | 0 Devices

Patches out of date on your devices
57

- 0 Failed to install | 0 Devices
- 43 Missing | 9 Devices
- 14 Scheduled | 2 Devices

Current state of patches on your devices

Subscriptions
4

Antivirus	Ends on Jan 30, 2025	80%	12 out of 15 devices
Patch Management	Ends on Jan 30, 2025	67%	10 out of 15 devices
VPN	Ends on Jan 30, 2025	53%	8 out of 15 devices

Avast Ultimate Business Security includes a next-gen antivirus with online privacy tools and patch management automation software to help keep business devices, data, and applications updated and secure.

Key Features

Online Management Platform: Get real-time visibility of cyberthreats, comprehensive reporting, and administrative capabilities - right from your web browser. A cloud-based console lets you centrally manage your Avast Business security services and their subscriptions.

Next-gen Antivirus: Next-gen endpoint protection with File Shield, Web Shield, Mail Shield, real-time Behaviour Monitoring, and Cloud Sandbox help secure users' devices against malware infections and zero-day threats.

Advanced Firewall: Monitor network traffic between your employees' devices and the internet. Improve blocking of dangerous or superfluous data transmissions for better protection of your business against malicious data manipulation.

Ransomware Shield: Reinforce the protection of your sensitive data and other critical business documents against modification, deletion, or encryption by ransomware attacks. Choose which applications have permission to access your protected folders and block the rest.

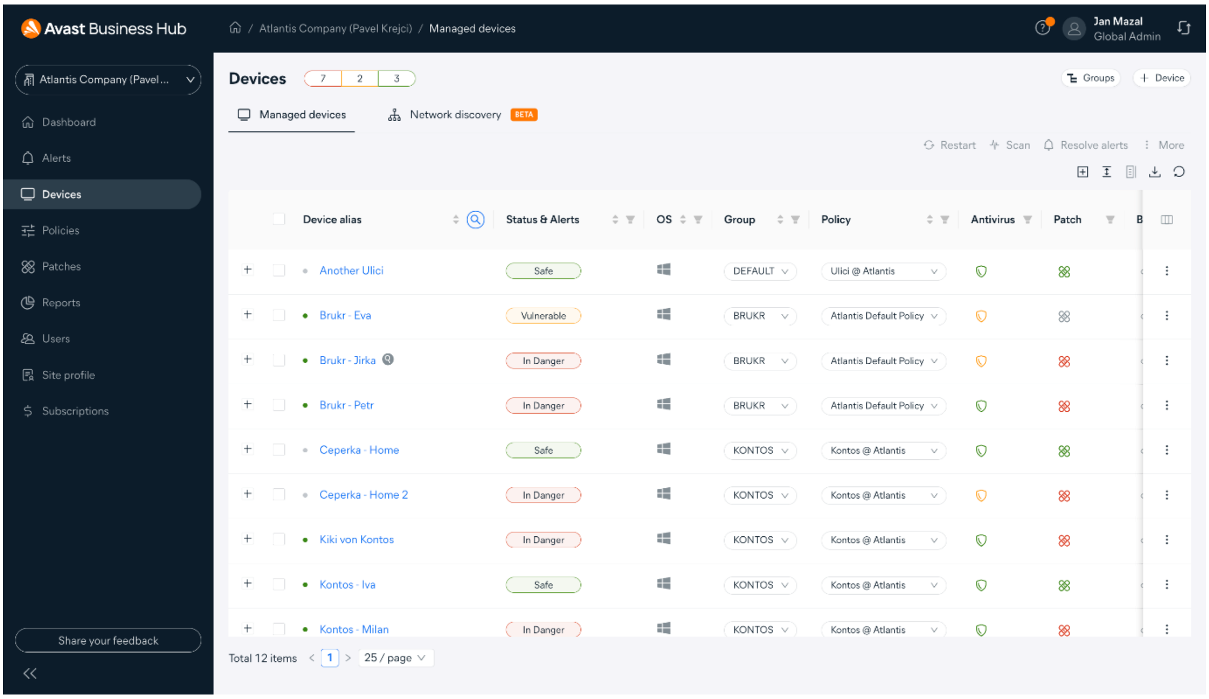
Real Site: Real Site supports safer web browsing and banking by helping your employees avoid fake websites created to steal sensitive data such as usernames, passwords, and credit card details. It is designed to secure users against DNS (Domain Name System) hijacking.

Password Protection: Help safeguard your employees' login information that is stored in web browsers from being stolen and misused. Password Protection is designed to prevent applications and malware from tampering with passwords that are saved in Google Chrome, Mozilla Firefox, Microsoft Edge, and Avast Secure Browser browsers.

VPN: Built-in personal VPN with no data limits encrypts your data traffic over the internet to help protect your employees' data, making them also private when using public Wi-Fi networks, such as those in cafes or the airport.

USB Protection: Prevent employees from using unauthorized removable storage devices, including flash drives, external drives, and memory cards to avoid data theft, data loss, and malware infections.

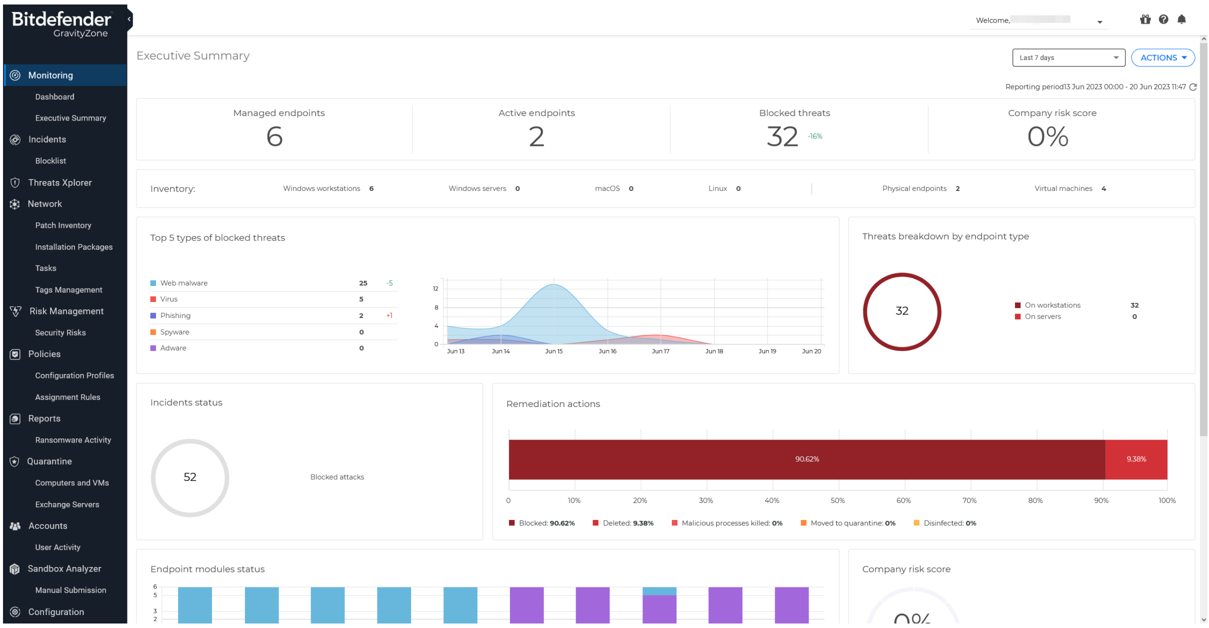
Patch Management: Automatically fix vulnerabilities in Windows and third-party applications that are susceptible to cyberattacks by remotely patching devices, no matter where they are. Patch Management helps you distribute tested patches to hundreds of devices in minutes, with minimal impact on your network.



Device alias	Status & Alerts	OS	Group	Policy	Antivirus	Patch	B
Another Ulici	Safe		DEFAULT	Ulici @ Atlantis			
Brukr - Eva	Vulnerable		BRUKR	Atlantis Default Policy			
Brukr - Jirka	In Danger		BRUKR	Atlantis Default Policy			
Brukr - Petr	In Danger		BRUKR	Atlantis Default Policy			
Ceperka - Home	Safe		KONTOS	Kontos @ Atlantis			
Ceperka - Home 2	In Danger		KONTOS	Kontos @ Atlantis			
Kiki von Kontos	In Danger		KONTOS	Kontos @ Atlantis			
Kontos - Iva	Safe		KONTOS	Kontos @ Atlantis			
Kontos - Milan	In Danger		KONTOS	Kontos @ Atlantis			

Total 12 items < 1 > 25 / page

Bitdefender GravityZone Business Security Premium



Welcome, [redacted]

Executive Summary

Last 7 days

Reporting period13 Jun 2023 00:00 - 20 Jun 2023 11:47

Managed endpoints 6

Active endpoints 2

Blocked threats 32 -16%

Company risk score 0%

Inventory: Windows workstations 6 Windows servers 0 macOS 0 Linux 0 | Physical endpoints 2 Virtual machines 4

Top 5 types of blocked threats

Web malware	25	-5
Virus	5	
Phishing	2	+1
Spyware	0	
Adware	0	

Threats breakdown by endpoint type

32

On workstations	32
On servers	0

Incidents status

52 Blocked attacks

Remediation actions

90.62% 9.38%

Blocked: **90.62%** Deleted: **9.38%** Malicious processes killed: **0%** Moved to quarantine: **0%** Disinfected: **0%**

Endpoint modules status

Company risk score

0%

GravityZone Business Security Premium is designed to protect small to medium organizations, covering any number of file servers, desktops, laptops, physical or virtual machines. It is based on a layered next-gen endpoint protection platform with prevention, detection and blocking capabilities, using machine learning techniques, behavioural analysis, and continuous monitoring of running processes.

Key Features

Machine Learning Anti-Malware: Bitdefender's machine learning models utilize 40,000 features and billions of file samples to predict and block advanced attacks effectively, improving malware detection accuracy while minimizing false positives.

Process Inspector: Operating in zero-trust mode, Process Inspector continuously monitors all processes in the system, detecting suspicious activities and anomalous behaviours. It effectively identifies unknown advanced malware, including ransomware, and takes remediation actions such as termination and undoing changes.

Advanced Anti-Exploit: This technology protects memory and vulnerable applications by detecting and blocking exploit techniques like API caller verification, stack pivot, and return-oriented-programming (ROP).

Endpoint Control and Hardening: Policy-based controls include firewall management, USB scanning for device control, and web content filtering with URL categorization.

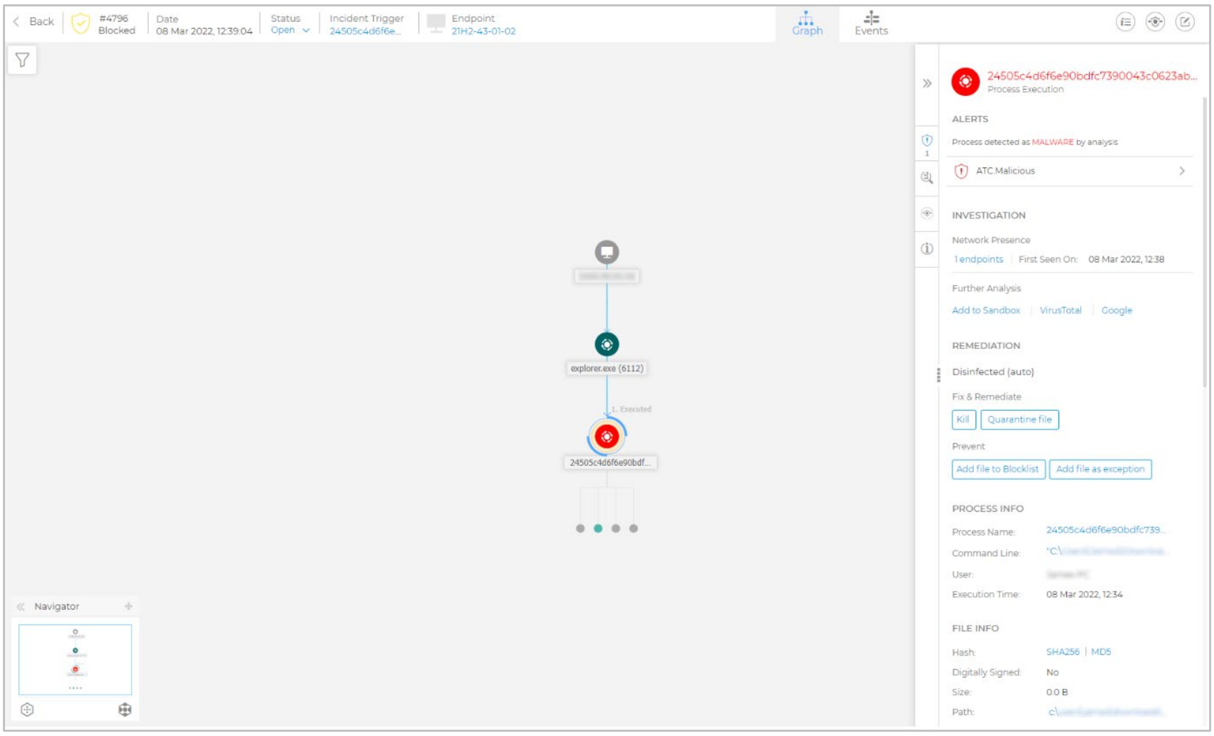
Anti-Phishing and Web Security Filtering: Real-time scanning of web traffic, including SSL, http, and https, prevents the download of malware. Anti-phishing protection automatically blocks fraudulent web pages.

Response and Containment: GravityZone automatically blocks and contains threats, terminates malicious processes, and rolls back unauthorized changes.

Ransomware Protection: Bitdefender can detect new ransomware patterns, offering robust protection against evolving threats.

Automate Threat Remediation and Response: GravityZone neutralizes threats through actions such as process terminations, quarantine, removal, and rollback. Real-time threat information sharing with Bitdefender's cloud-based threat intelligence service prevents similar attacks globally.

GravityZone Control Center: GravityZone Control Center is an integrated and centralized management console that provides a view for all security management components. It can be cloud-hosted or deployed locally. GravityZone management center incorporates multiple roles and contains the database server, communication server, update server and web console.



#4796 Blocked | Date 08 Mar 2022, 12:39:04 | Status Open | Incident Trigger 24505c4d6f6e... | Endpoint 21H2-43-01-02

24505c4d6f6e90bdfc7390043c0623ab...
Process Execution

ALERTS
Process detected as MALWARE by analysis
ATC.Malicious

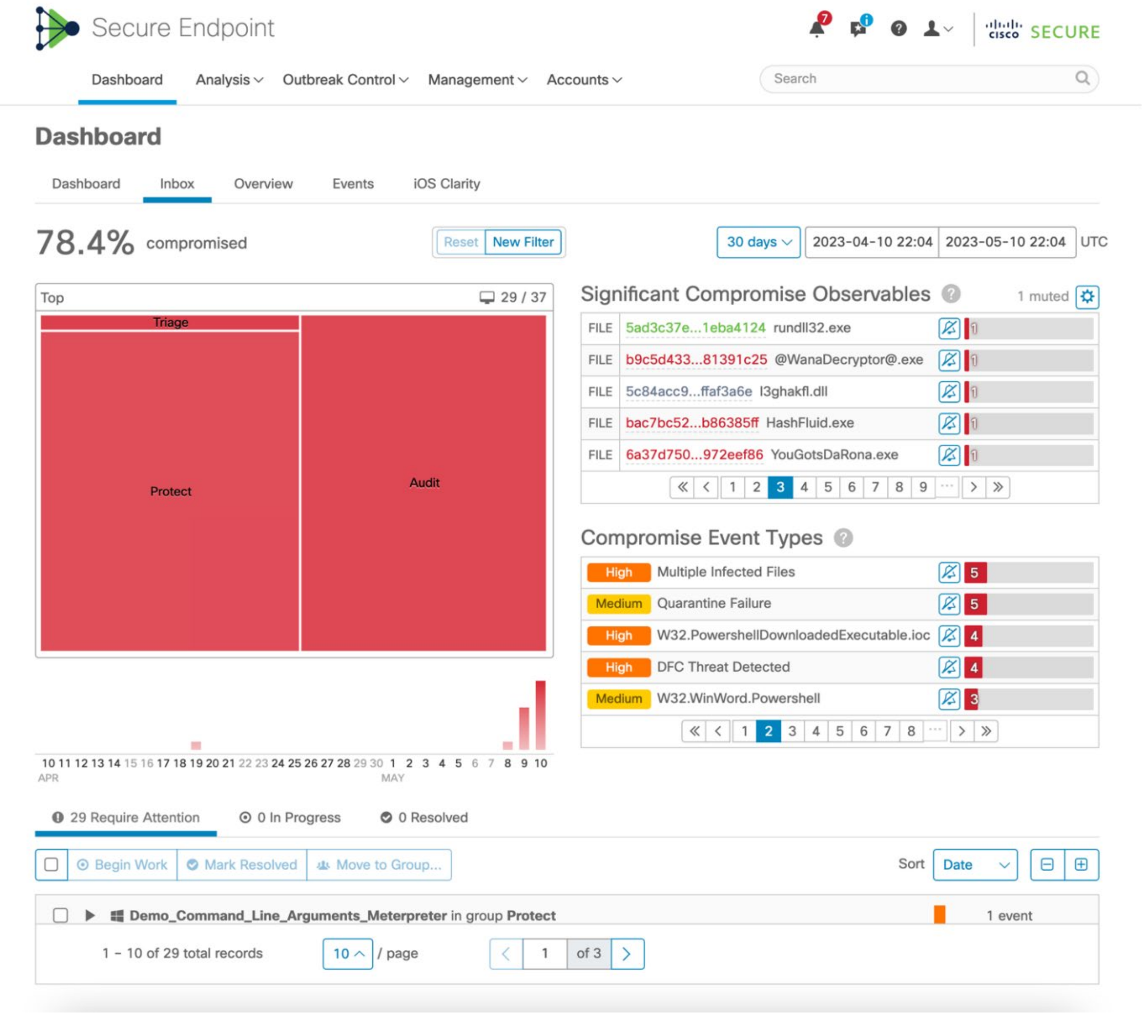
INVESTIGATION
Network Presence
1 endpoints | First Seen On: 08 Mar 2022, 12:38
Further Analysis
Add to Sandbox | VirusTotal | Google

REMEDIATION
Disinfected (auto)
Fix & Remediate
Prevent

PROCESS INFO
Process Name: 24505c4d6f6e90bdfc739...
Command Line: "C:\[redacted]
User: [redacted]
Execution Time: 08 Mar 2022, 12:34

FILE INFO
Hash: SHA256 | MD5
Digitally Signed: No
Size: 0.0 B
Path: c:\[redacted]

Cisco Secure Endpoint Essentials



Significant Compromise Observables

1 muted

FILE	5ad3c37e...1eba4124 rundll32.exe	1
FILE	b9c5d433...81391c25 @WanaDecryptor@.exe	1
FILE	5c84acc9...ffaf3a6e l3ghakfl.dll	1
FILE	bac7bc52...b86385ff HashFluid.exe	1
FILE	6a37d750...972eef86 YouGotsDaRona.exe	1

Compromise Event Types

High	Multiple Infected Files	5
Medium	Quarantine Failure	5
High	W32.PowershellDownloadedExecutable.ioc	4
High	DFC Threat Detected	4
Medium	W32.WinWord.Powershell	3

□ ▶ Demo_Command_Line_Arguments_Meterpreter in group Protect 1 event

Cisco Secure Endpoint Essentials is a comprehensive endpoint security solution that provides advanced protection, threat detection and response capabilities in a single agent that offers Endpoint Detection and Response and integrated Extended Detection and Response (XDR) capabilities.

Key Features

Advanced Protection: Cisco Secure Endpoint uses a layered approach consisting of reputation, application, process and command monitoring, machine learning and behavioural analysis to detect and prevent advanced attacks.

Next-Generation Antivirus (NGAV): Preventative technologies to stop malware by leveraging file reputation, exploit prevention, script protections, and signature detection techniques to stop known and unknown threats**.**

Endpoint Detection and Response (EDR): Real-time visibility and control of endpoint activities to enable threat hunting and accelerate incident response.

Threat Intelligence: Cisco Talos Intelligence provides the latest threat intelligence to identify and prevent emerging threats.

Dynamic analysis: Produces detailed runtime insight and analysis, including the severity of behaviours, the original file name, screenshots of the malware executing, and packet captures.

Device Control: Visibility and control over USB mass storage devices.

Secure Endpoint: This prevents breaches, blocks malware at the point of entry, and continuously monitors and analyses file and process activity to rapidly detect, contain, and remediate threats that can evade front-line defences.

Prevention and Detection: Identify and stop threats before compromise. Reduce the attack surface with prevention techniques, risk-based vulnerability management, and posture assessments. Enable hunts for hidden threats, detect malware, and perform advanced investigations.

Rapid Response: The Cisco Secure portfolio provides automatic global outbreak control. Endpoint response ranging from file, application and network control to automated actions and isolation help automate endpoint triage and threat containment to reduce time to respond.

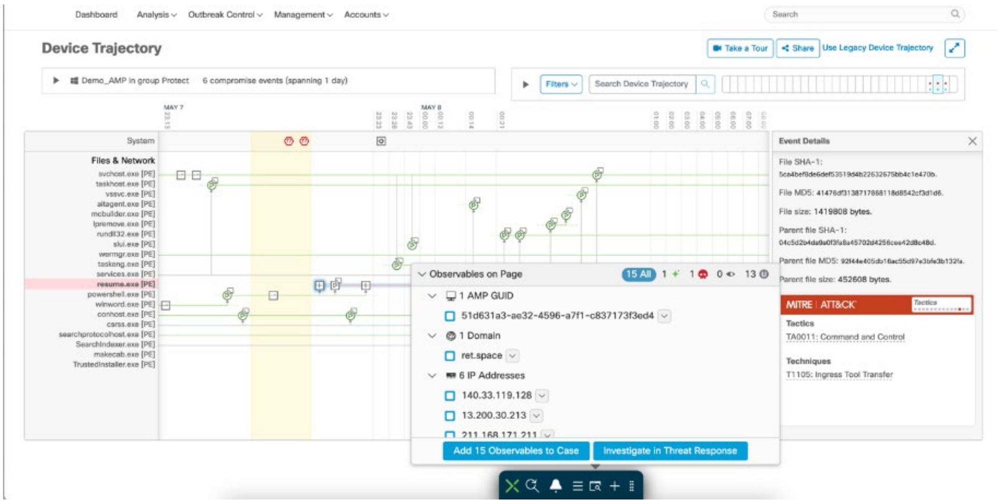
Extended Detection and Response (XDR): Reduce incident detection and response times with Cisco Extended Detection and Response (XDR). Built-in integration with the Cisco Secure portfolio and 3rd party solutions to provide a unified view to simplify and orchestrate incident response across your security control points, for a layered defence against threats.

Flexible Deployment and Simplified Management: The solution is easy to deploy, manage, and scale. It can be deployed on-premises or in the cloud, providing flexibility to meet different organizational needs.

Single Agent: Cisco Secure Endpoint Essentials combines Endpoint Prevention, Detection and Response in a single agent.

Management Console: The solution provides a centralized management console to manage and monitor endpoints and can be deployed on-premises or in the cloud.

Scalability: management console can scale to support businesses as they grow.



Demo_AMP in group Protect 6 compromise events (spanning 1 day)

Observables on Page

- 1 AMP GUID
  - □ 51d631a3-ae32-4596-a7f1-c837173f3ed4
- 1 Domain
  - □ ret.space
- 6 IP Addresses
  - □ 140.33.119.128
  - □ 13.200.30.213
  - □ 211.168.171.211

Event Details

File SHA-1: 5ca4bef8de6def53519d4b22632675bb4c1e470b.

File MD5: 41476df3138717868118d8542cf3d1d6.

File size: 1419808 bytes.

Parent file SHA-1: 04c5d2b4da9a0f3fa8a45702d4256cee42d8c48d.

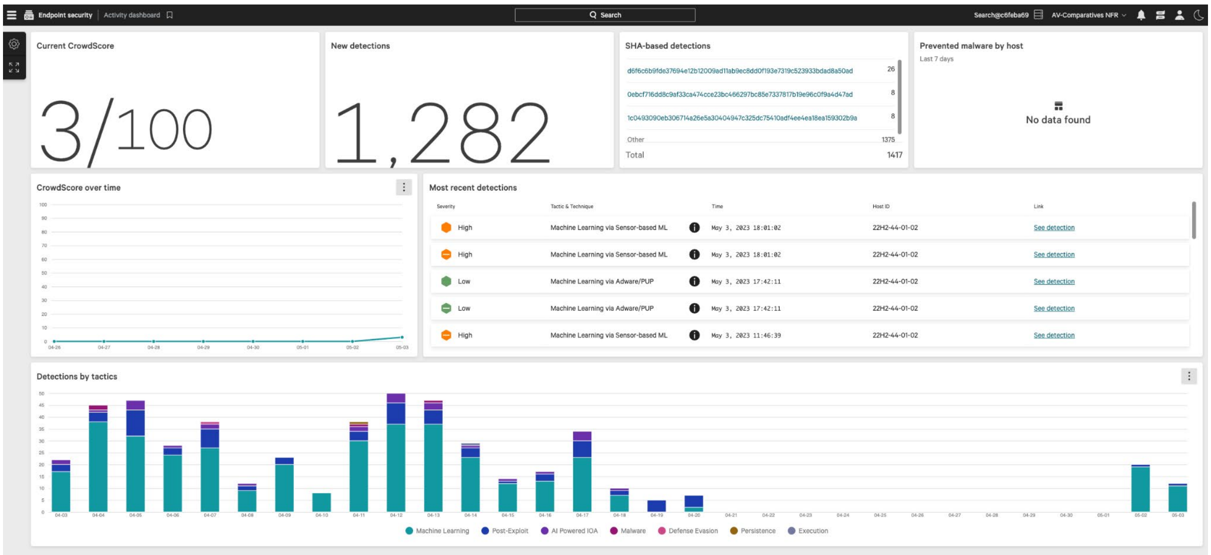
Parent file MD5: 92f44e405db16ac55d97e3bfe3b132fa.

Parent file size: 452608 bytes.

Tactics
TA0011: Command and Control

Techniques
T1105: Ingress Tool Transfer

CrowdStrike Falcon Pro



SHA-based detections

d6f6c6b9fde37694e12b12009ad11ab9ec8dd0f193e7319c523933bdad8a50ad	26
0ebcf716dd8c9af33ca474cce23bc466297bc85e7337817b19e96c0f9a4d47ad	8
1c0493090eb306714a26e5a30404947c325dc75410adf4ee4ea18ea159302b9a	8
Other	1375
Total	1417

Most recent detections

Severity	Tactic & Technique	Time	Host ID	Link
High	Machine Learning via Sensor-based ML	May 3, 2023 18:01:02	22H2-44-01-02	See detection
High	Machine Learning via Sensor-based ML	May 3, 2023 18:01:02	22H2-44-01-02	See detection
Low	Machine Learning via Adware/PUP	May 3, 2023 17:42:11	22H2-44-01-02	See detection
Low	Machine Learning via Adware/PUP	May 3, 2023 17:42:11	22H2-44-01-02	See detection
High	Machine Learning via Sensor-based ML	May 3, 2023 11:46:39	22H2-44-01-02	See detection

CrowdStrike Falcon Pro offers cloud-native capabilities through a lightweight agent and a centralized command center. In addition to threat protection, it provides investigative functions and threat intelligence for analysis and remediation of attacks. The solution is scalable, making it suitable for managing networks with thousands of devices.

Key Features

Easy to deploy: The Falcon agent is easy to deploy at scale, offering instant protection without the need for a reboot or tuning processes.

Advanced Threat Detection: Falcon Pro is designed to detect advanced and unknown threats, including fileless attacks, ransomware, adware, and potentially unwanted programs.

Full Attack Visibility: The solution provides attack visibility through a process tree. It unravels complete attack scenarios, enriches them with contextual threat intelligence, and maps adversary behaviours using MITRE ATT&CK® terminology.

Falcon Fusion: Falcon Pro includes Falcon Fusion, an integrated Security Orchestration, Automation, and Response (SOAR) framework. This enables IT and security teams to streamline workflow orchestration and automation.

Signatureless Approach: Falcon Pro does not rely on signatures, eliminating the need for daily virus definition updates. This reduces the administrative overhead and ensures protection against emerging threats.

Exploit Blocking: The solution proactively blocks the execution and spread of threats through unpatched vulnerabilities, preventing potential exploitation.

On-Write Quarantine: Falcon Pro detects and isolates malicious files as soon as they appear on a host, ensuring they are contained and unable to cause harm.

Custom Indicators of Attack (IOAs): Teams can utilize custom IOAs to create behaviour-based blocking rules tailored to their specific organizational needs, providing enhanced protection against targeted attacks.

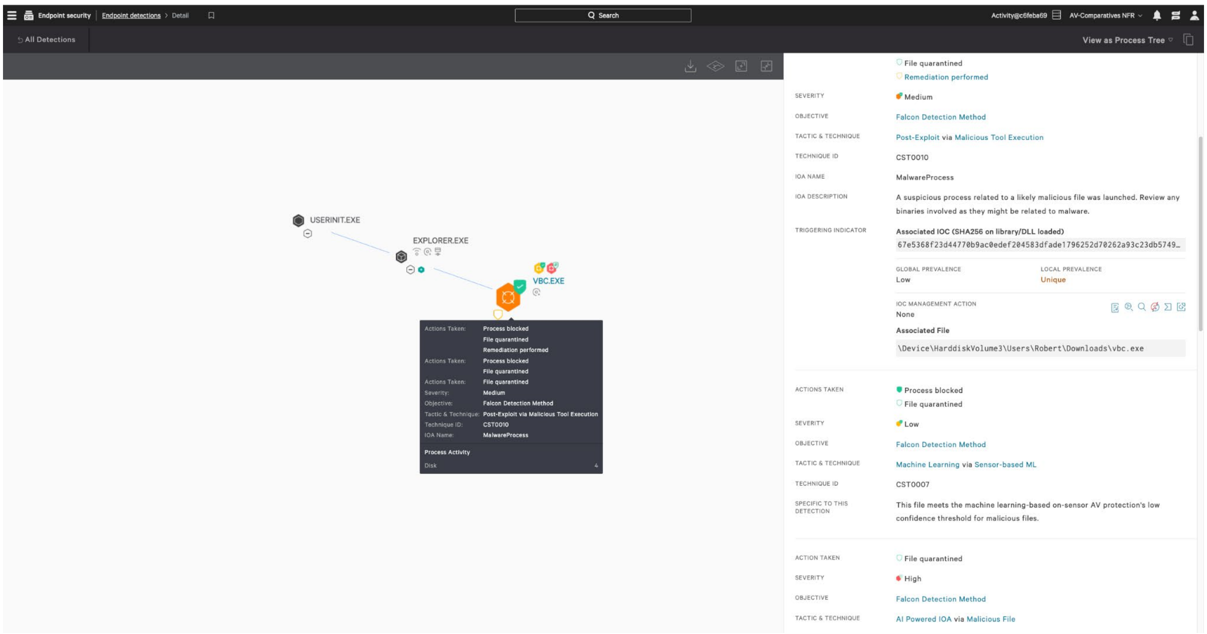
Advanced Memory Scanning: Automated memory scans are performed using behavioural triggers to prevent fileless and memory-based attacks, such as ransomware and the use of dual-purpose tools like Cobalt Strike, earlier in the kill chain.

Quarantine Functionality: Blocked files are quarantined, allowing analysts to access and investigate them for deeper analysis and understanding of the threat landscape.

Script-Based Execution Monitoring: Falcon Pro inspects and blocks malicious office macros, preventing script-based attacks.

Incident Response Acceleration: The solution accelerates incident response workflows by offering automated, scripted, and manual response capabilities. This streamlines the incident management process and enables faster resolution.

Built-in Threat Intelligence: Falcon Pro integrates comprehensive threat intelligence, strengthening detection capabilities and enhancing the efficiency of Security Operations Centers (SOCs). From automatic sandbox submissions of blocked files to actor profiles, analysts can gain valuable insights into threats and adversaries without exposing their local systems and network infrastructure.



Actions Taken: Process blocked
File quarantined
Remediation performed
Actions Taken: Process blocked
File quarantined
Actions Taken: File quarantined
Severity: Medium
Objective: Falcon Detection Method
Tactic & Technique: Post-Exploit via Malicious Tool Execution
Technique ID: CST0010
IOA Name: MalwareProcess

Process Activity
Disk 4

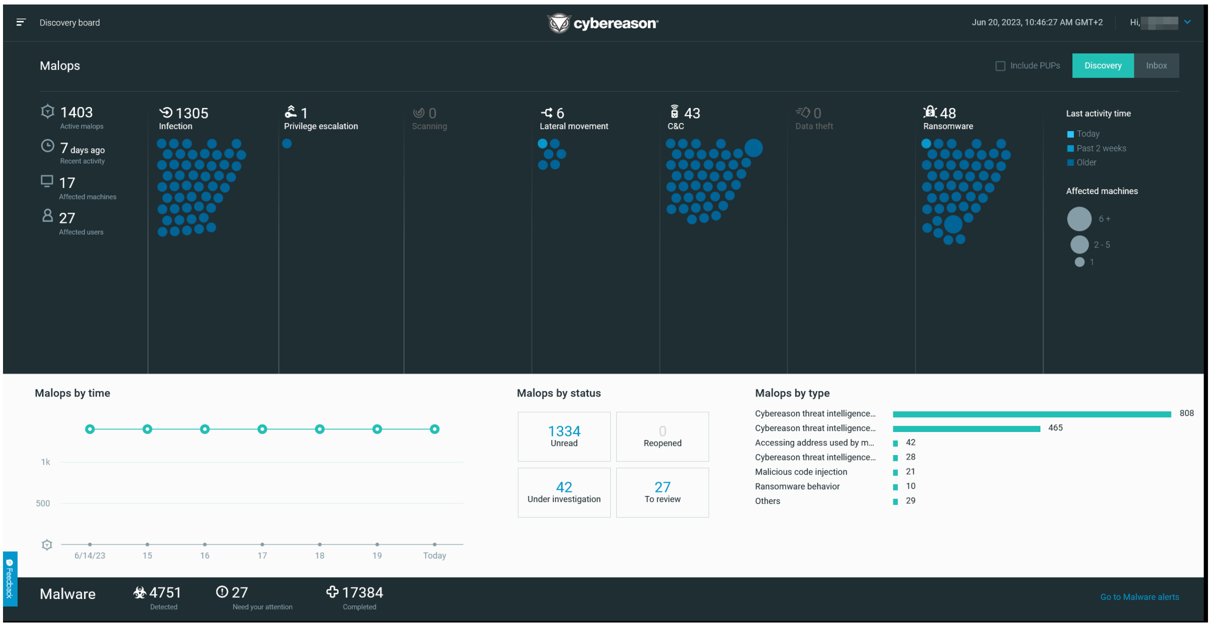
File quarantined
Remediation performed

SEVERITY Medium
OBJECTIVE Falcon Detection Method
TACTIC & TECHNIQUE Post-Exploit via Malicious Tool Execution
TECHNIQUE ID CST0010
IOA NAME MalwareProcess
IOA DESCRIPTION A suspicious process related to a likely malicious file was launched. Review any binaries involved as they might be related to malware.
TRIGGERING INDICATOR Associated IOC (SHA256 on library/DLL loaded)
67e5368f23d44770b9ac0edef204583dfade1796252d70262a93c23db5749…
GLOBAL PREVALENCE Low
LOCAL PREVALENCE Unique
IOC MANAGEMENT ACTION None
Associated File
\Device\HarddiskVolume3\Users\Robert\Downloads\vbc.exe

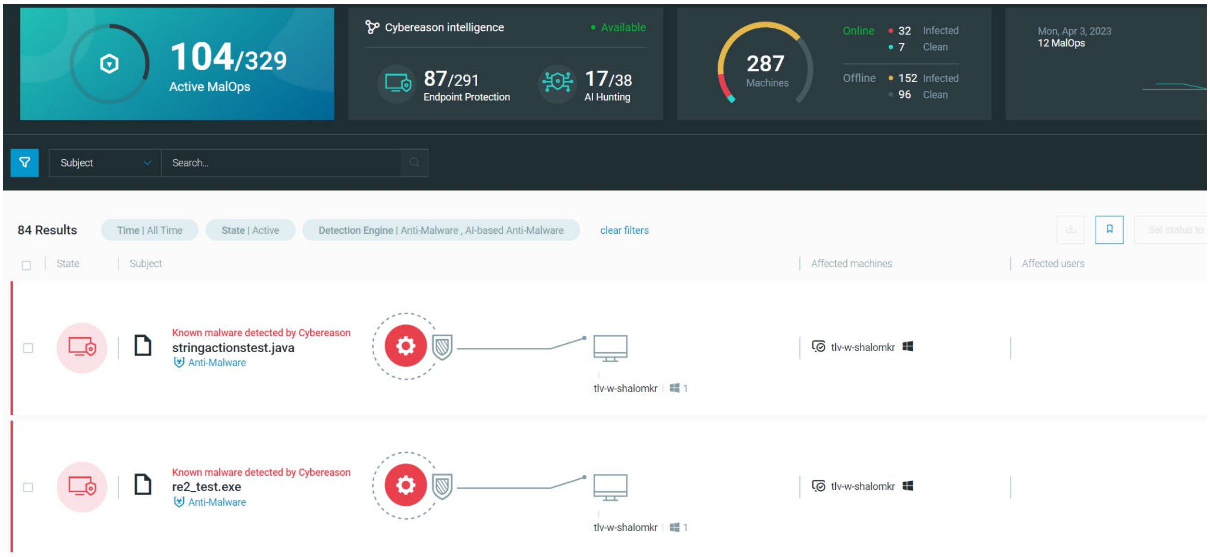
ACTIONS TAKEN Process blocked
File quarantined
SEVERITY Low
OBJECTIVE Falcon Detection Method
TACTIC & TECHNIQUE Machine Learning via Sensor-based ML
TECHNIQUE ID CST0007
SPECIFIC TO THIS DETECTION This file meets the machine learning-based on-sensor AV protection's low confidence threshold for malicious files.

ACTION TAKEN File quarantined
SEVERITY High
OBJECTIVE Falcon Detection Method
TACTIC & TECHNIQUE AI Powered IOA via Malicious File

Cybereason NGAV



Cybereason NGAV: Multiple layers of unparalleled attack protection. Cybereason brings a unique approach of multi-layered NGAV defence, with multiple layers purpose-built to prevent unique attacker techniques. Designed to stop everything from the simplest to the most novel Malware that exists today, even those never before seen. When these independent, yet complimentary, layers are combined, unparalleled attack protection is achieved.

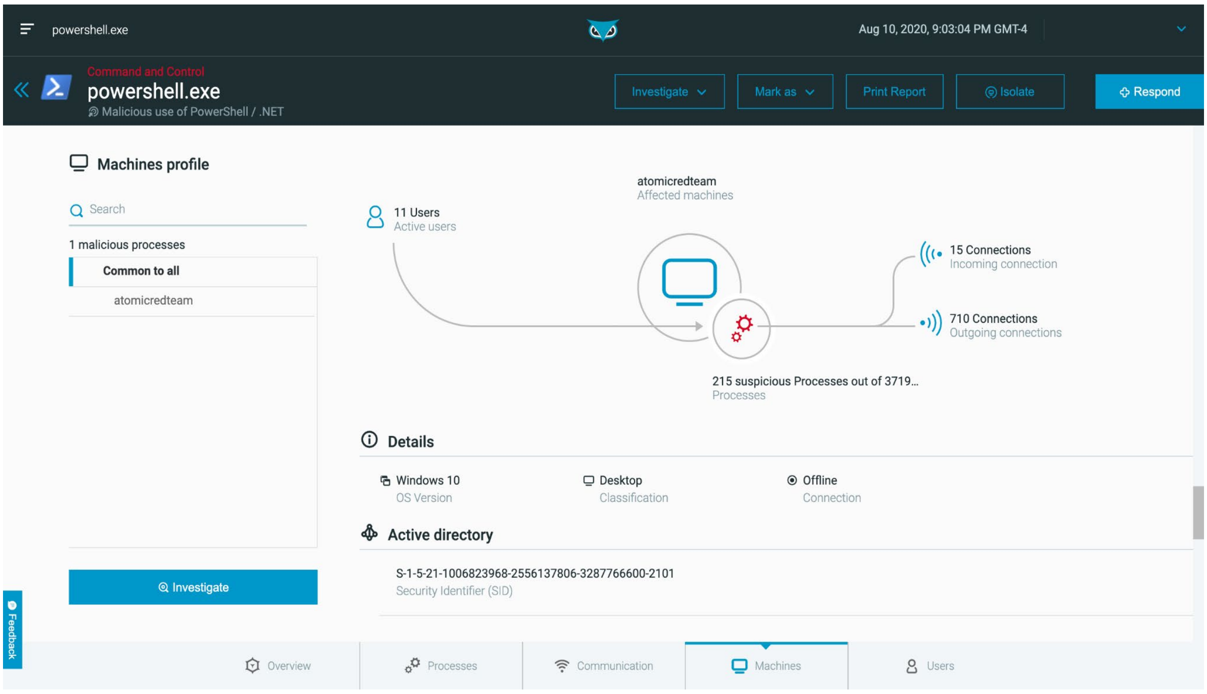


During AV-Comparatives testing, a base configuration of Cybereason NGAV is used where many of these unique layers are enabled. The most unique layers in the Cybereason NGAV product enabled during the testing are *AI-Based Anti-Malware* and *Fileless Malware Prevention*.

Key Features

Anti-Malware: Designed to block malware, the AI-Based anti-malware layer leverages artificial Intelligence to evaluate behaviour occurring across the enterprise as a whole to stop actors in their tracks, even when they're using never before seen malware.

Fileless Malware Prevention: Purpose-built to block in-memory command line and script-based attacks, the Fileless Malware Prevention layer examines the behaviour of the PowerShell engine, .Net, JScript, and VBScript to ensure that attackers are not able to slip by defences by loading malicious code into memory.



Details

Windows 10
OS Version

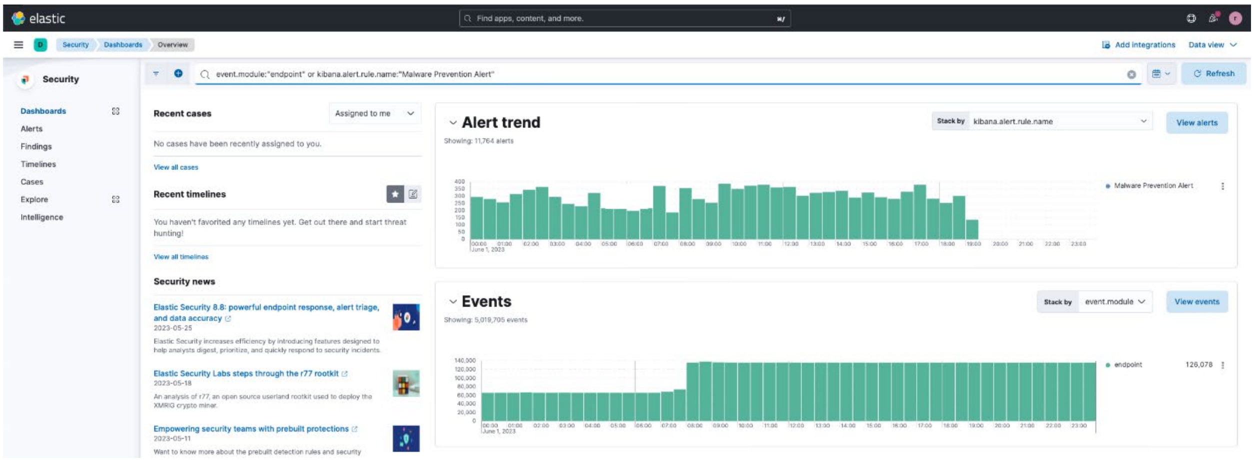
Desktop
Classification

Offline
Connection

Active directory

S-1-5-21-1006823968-2556137806-3287766600-2101
Security Identifier (SID)

Elastic Security



event.module:"endpoint" or kibana.alert.rule.name:"Malware Prevention Alert"

Recent cases

No cases have been recently assigned to you.

View all cases

Recent timelines

You haven't favorited any timelines yet. Get out there and start threat hunting!

View all timelines

Security news

Elastic Security 8.8: powerful endpoint response, alert triage, and data accuracy
2023-05-25
Elastic Security increases efficiency by introducing features designed to help analysts digest, prioritize, and quickly respond to security incidents.

Elastic Security Labs steps through the r77 rootkit
2023-05-18
An analysis of r77, an open source userland rootkit used to deploy the XMRIG crypto miner.

Empowering security teams with prebuilt protections
2023-05-11
Want to know more about the prebuilt detection rules and security

Alert trend

Showing: 11,764 alerts

Stack by: kibana.alert.rule.name

Events

Showing: 5,019,705 events

Stack by: event.module

Elastic Security for endpoint prevents ransomware and malware, detects advanced threats, and arms responders with vital investigative context. Elastic Security provides organizations with prevention, detection, and response capabilities across running on both traditional endpoints and public, private, and hybrid cloud environments.

Elastic Security combines SIEM threat detection features with endpoint prevention and response capabilities in one solution. These analytical and protection capabilities, leveraged by the speed and extensibility of Elasticsearch, enable analysts to defend their organization from threats before damage and loss occur.

Key Features

Prevent complex attacks: Prevent malware and ransomware from executing, and stop advanced threats with malicious behaviour, memory threat, and provides credential hardening protections. All powered by Elastic Labs and the global community.

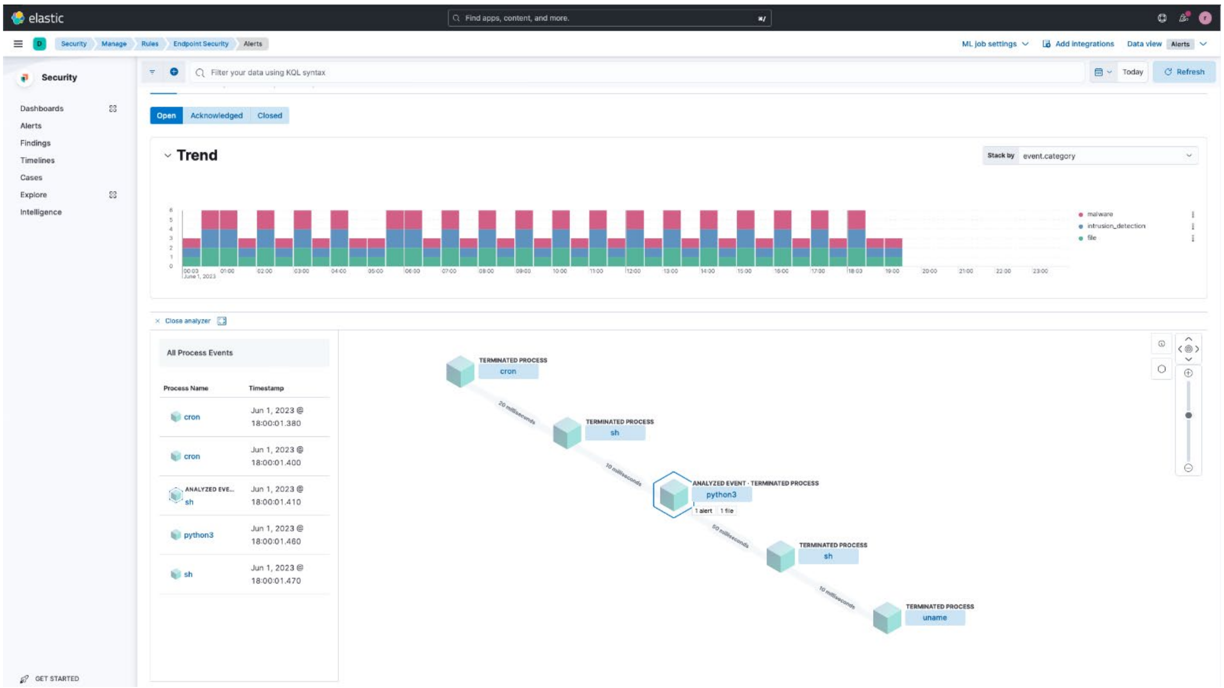
Detect threats in high fidelity: Elastic Defend facilitates deep visibility by instrumenting the process, file, and network data in users' environments with minimal data collection overhead.

Triage and rapid response: Elastic Security allows for detailed analysis of data across hosts and examining of host-based activity with interactive visualizations. It allows users to invoke remote response actions across distributed endpoints. The investigation capabilities can be further extended with the OSquery integration, fully integrated into Elastic Security workflows.

Secure cloud workloads: This allows stopping threats targeting cloud workloads and cloud-native applications. The lightweight user-space agent, powered by eBPF, allows for real-time visibility and control. Automates identification of cloud threats with detection rules and machine learning (ML). MITRE ATT&CK-aligned detections honed by Elastic Security Labs enable a rapid time-to-value.

View terminal sessions: This gives security teams an investigative tool for digital forensics and incident response (DFIR), reducing the mean time to respond (MTTR).

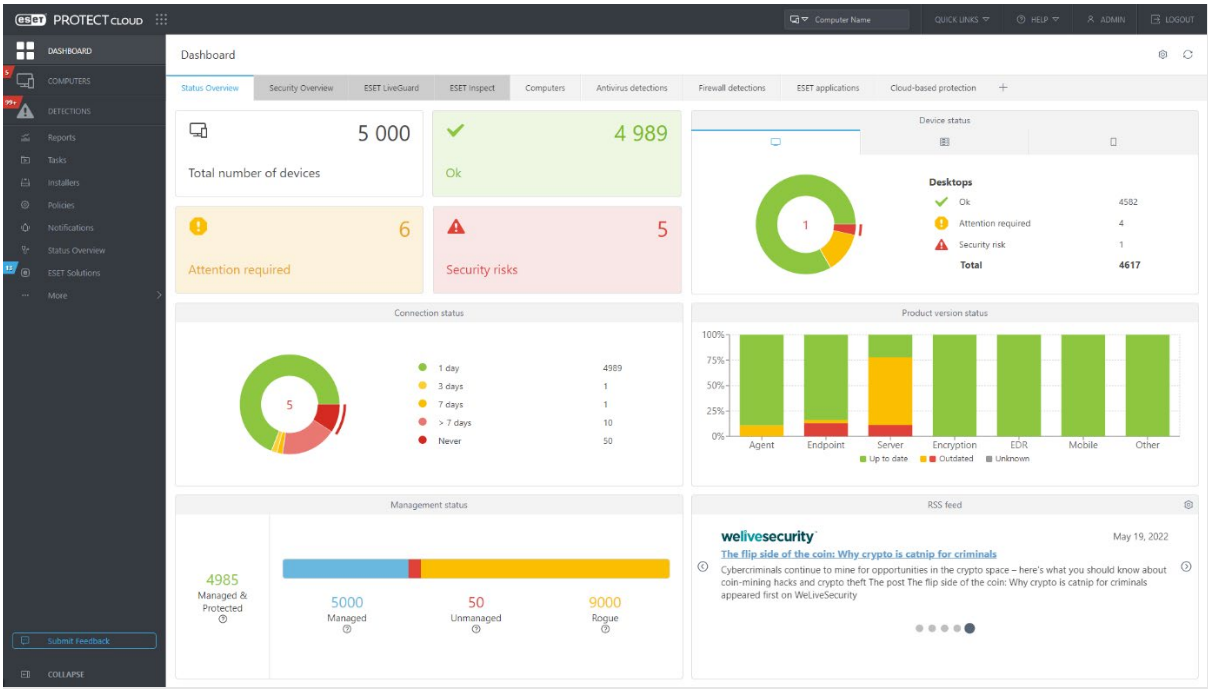
Continuous Monitoring: Including both user and network activity monitoring but also custom security monitoring. This allows the protection of platforms like AWS, GCP, and Azure from data theft, resource hijacking, and sabotage. Allowing users to observe container security and health and to safeguard distributed workplaces by tracking IT and security applications from Azure AD to Zoom.



All Process Events

Process Name	Timestamp
cron	Jun 1, 2023 @ 18:00:01.380
cron	Jun 1, 2023 @ 18:00:01.400
ANALYZED EVE... sh	Jun 1, 2023 @ 18:00:01.410
python3	Jun 1, 2023 @ 18:00:01.460
sh	Jun 1, 2023 @ 18:00:01.470

ESET PROTECT Entry with ESET PROTECT Cloud



Desktops	
Ok	4582
Attention required	4
Security risk	1
Total	4617

1 day	4989
3 days	1
7 days	1
> 7 days	10
Never	50

May 19, 2022

The flip side of the coin: Why crypto is catnip for criminals

Cybercriminals continue to mine for opportunities in the crypto space – here's what you should know about coin-mining hacks and crypto theft The post The flip side of the coin: Why crypto is catnip for criminals appeared first on WeLiveSecurity

ESET PROTECT is powered by ESET LiveSense, ESET's multi-layered technology that combines machine learning and ESET LiveGrid, ESET's global, cloud-based reputation system.

Key Features

Combines cybersecurity needs: ESET PROTECT Platform integrates multiple cybersecurity capabilities under one roof so customers can choose which are most effective for protecting their organization. It is simple, modular, adaptable, and continuously innovated – across all operating systems.

Modern endpoint capabilities and protection tools: ESET uses multi-layered technologies that go far beyond the capabilities of basic antivirus or antimalware. ESET PROTECT Entry provides ESET's multi-layered protection and threat intelligence information, which protects against ransomware and botnets, blocks targeted attacks, prevents data breaches, and detects zero-day threats, fileless attacks, advanced persistent threats and more.

In-house research and development: ESET's teams not only develop its products but also publish research. ESET is also currently among the top 5 contributors and top 10 referenced sources in the MITRE Enterprise Matrix, thus providing much-needed intelligence into TTPs exploited by diverse APT groups.

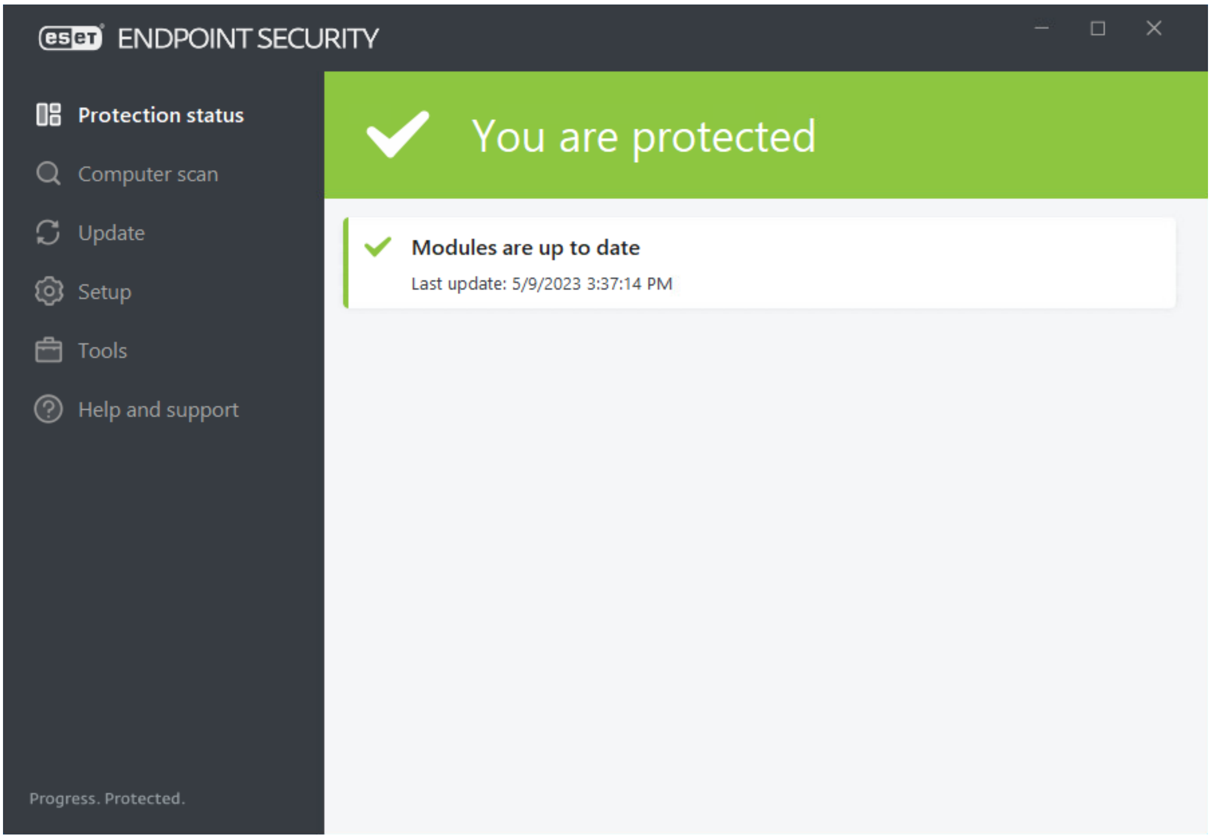
Local language support for users in every corner of the globe: The enterprise management consoles are available in 23 languages, and the endpoint security solution in 37 languages, making ESET's solution one of the most accessible.

Network management with one-click actions: Actions such as isolating the device from the network, creating an exclusion, or initiating a scan are available with a single click in ESET PROTECT console.

Deep-dive insights into the network: ESET PROTECT Platform provides over 120 built-in reports and allows you to create custom reports from over 1000 data points.

Real-time alerts about incidents in your organization: Use pre-defined notifications or create your own. The notification system features a full "what you see is what you get" editor.

Effortless and quick installation: Deploy pre-configured live installers that automatically activate and connect your endpoints to the management console.

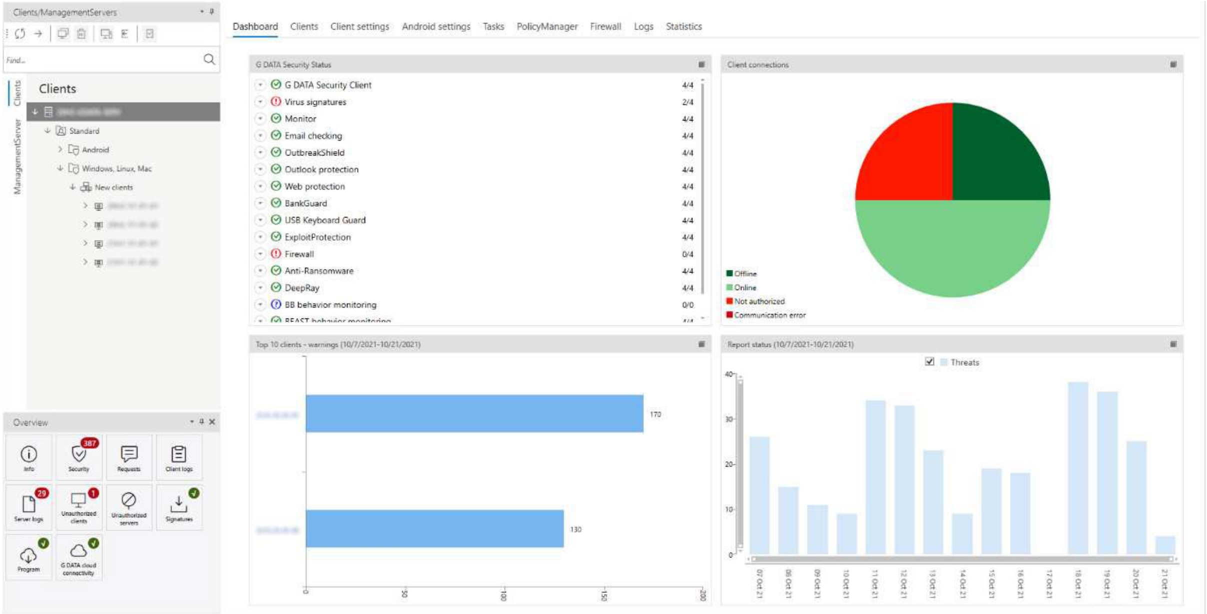


You are protected

Modules are up to date

Last update: 5/9/2023 3:37:14 PM

G DATA Endpoint Protection Business



G DATA Security Status	
G DATA Security Client	4/4
Virus signatures	2/4
Monitor	4/4
Email checking	4/4
OutbreakShield	4/4
Outlook protection	4/4
Web protection	4/4
BankGuard	4/4
USB Keyboard Guard	4/4
ExploitProtection	4/4
Firewall	0/4
Anti-Ransomware	4/4
DeepRay	4/4
BB behavior monitoring	0/0
BEAST behavior monitoring	4/4

G DATA Endpoint Protection Business is a long-standing product line that has developed from a static scanning engine only product into incorporating next generation scanning and heuristic technologies. These technologies help us detect and prevent malware even when normal scanning approaches fail.

Key Features

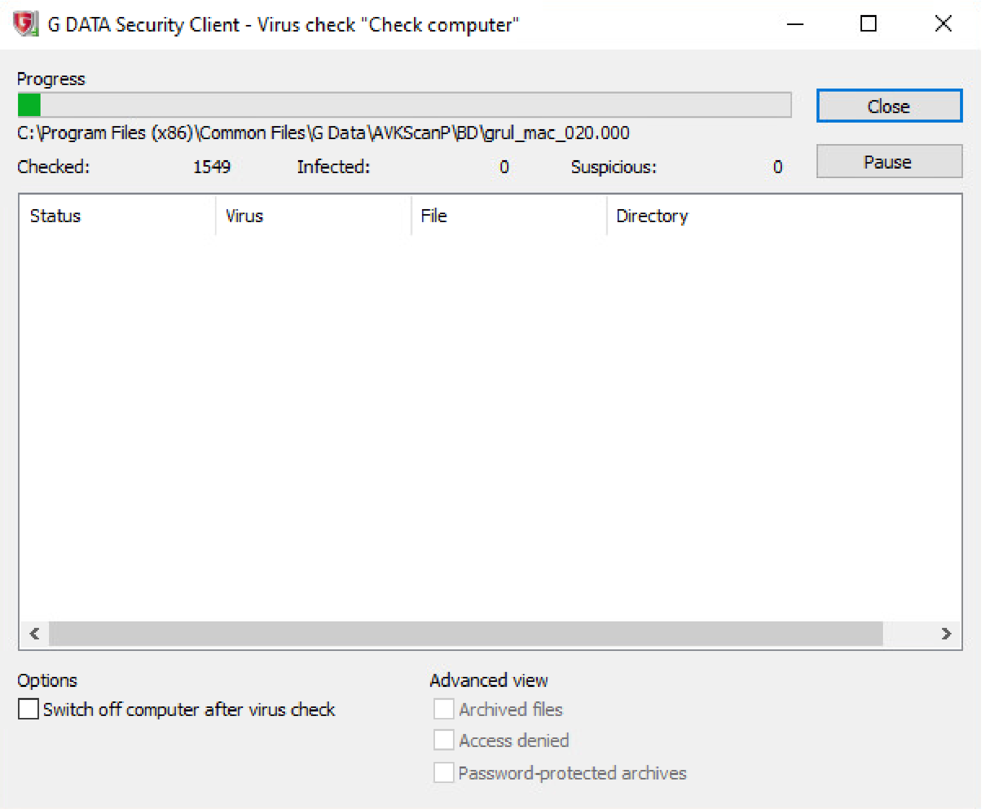
Privacy by design: G Data's development only happens in Germany, which had very strict data privacy laws even before the GDPR, employing strict privacy by design and by default rules in the development of their software.

Online and offline protection: G Data's products offer very strong offline and local protection by design. Protection modules work offline and do not require a cloud connection, although the cloud connection does improve detection against latest and unknown threats.

BehaviorStorage (BEAST) module: This module runs locally on the client and does not transmit user behaviour data into a cloud. BEAST is able to run completely independent of Internet connectivity and can still classify suspicious or malicious activity.

In house support: Support is not outsourced, being involved in the development processes which enables G Data to fix errors reported by customers.

MMC style admin: Allowing for easy use by Windows administrators.



G DATA Security Client - Virus check "Check computer"

Progress

C:\Program Files (x86)\Common Files\G Data\AVKScanP\BD\grul_mac_020.000

Checked: 1549 Infected: 0 Suspicious: 0

Status	Virus	File	Directory

Options

□ Switch off computer after virus check

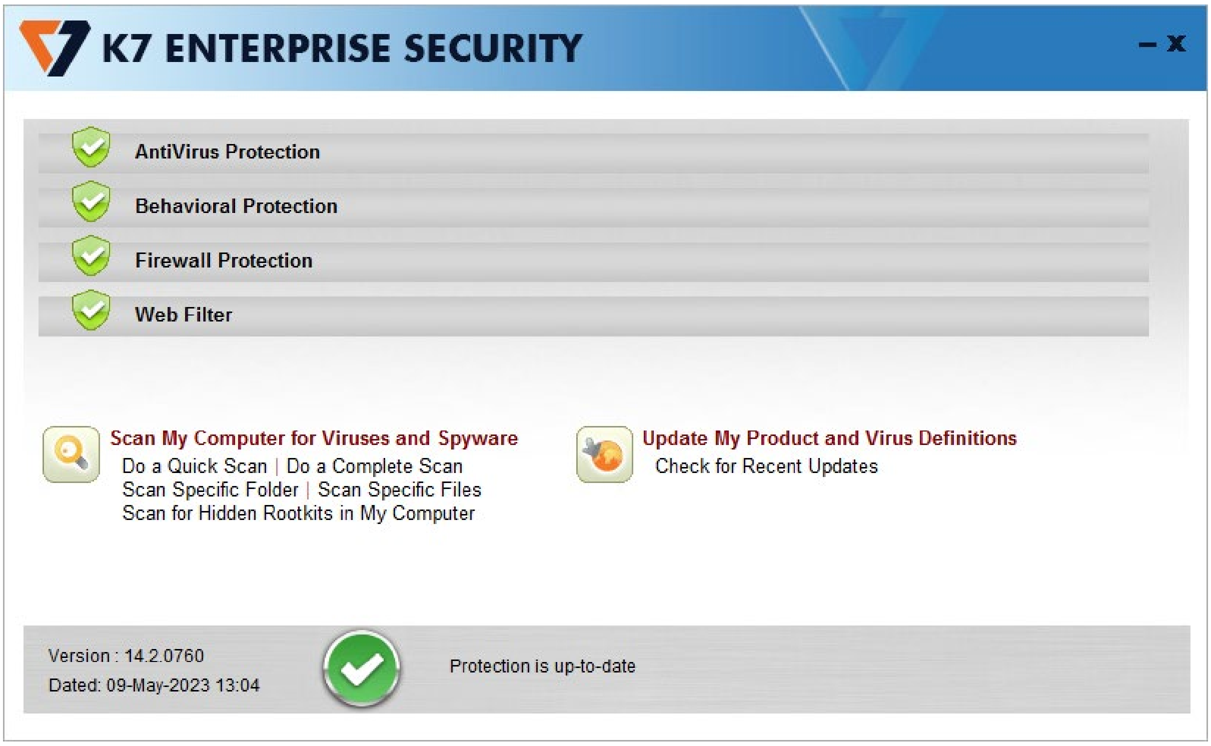
Advanced view

□ Archived files

□ Access denied

□ Password-protected archives

K7 On-Premises Enterprise Security Advanced



K7 ENTERPRISE SECURITY

✓ AntiVirus Protection

✓ Behavioral Protection

✓ Firewall Protection

✓ Web Filter

Scan My Computer for Viruses and Spyware
Do a Quick Scan | Do a Complete Scan
Scan Specific Folder | Scan Specific Files
Scan for Hidden Rootkits in My Computer

Update My Product and Virus Definitions
Check for Recent Updates

Version : 14.2.0760
Dated: 09-May-2023 13:04

✓ Protection is up-to-date

K7 Security simplifies deployment and management, protecting client workstations and critical servers. The Centralised Management Server consolidates threats, implements endpoint security policies, and manages them with fewer IT resources. The web-based console handles K7 software installation on multiple endpoints, user group creation, policy enforcement, task scheduling, updates, and remote management of core capabilities such as Antivirus, Firewall, Application Control, and Web Content Filtering.

Key Features

Admin Console: The web-based interface enables complete security settings management, including client installation, group and policy management, task scheduling, updates, and control over Antivirus, Firewall, Application Control, Web Filtering, and Notifications.

Advanced Malware Detection and Remediation: The Host Intrusion Prevention System collates, analyses and triages various events to effectively detect and deal with malware. This feature deals with analysis of both pre-execution and runtime behaviour of monitored objects in the host.

Anti-Ransomware Protection: Monitors secured devices for ransomware, employing signature-less, behaviour-based detection mechanisms. K7 Ecosystem Threat Intelligence enhances protection against known and new ransomware variants. Real-time security defends against ransomware distribution through shared files and folders on the network.

K7 Device Control: This prevents USB and storage media infections by blocking unauthorized access to unknown devices. Host-level policies enforce device password access, file execution control, and on-demand/automatic device scanning.

K7 SafeSurf: This ensures secure online browsing by identifying and blocking malicious websites through URL analysis and cloud-based reputation services.

K7 Firewall / HIPS: The K7 Firewall, working with the integrated Host Intrusion Prevention System (HIPS), stealths system ports and protects against direct attacks. The Intrusion Detection System (IDS) blocks known malicious network-based exploits before processing.

System Security and Performance: K7 Security prioritizes system performance by utilizing a proprietary lean data-loading algorithm and ordering mechanism, minimizing RAM and CPU usage.

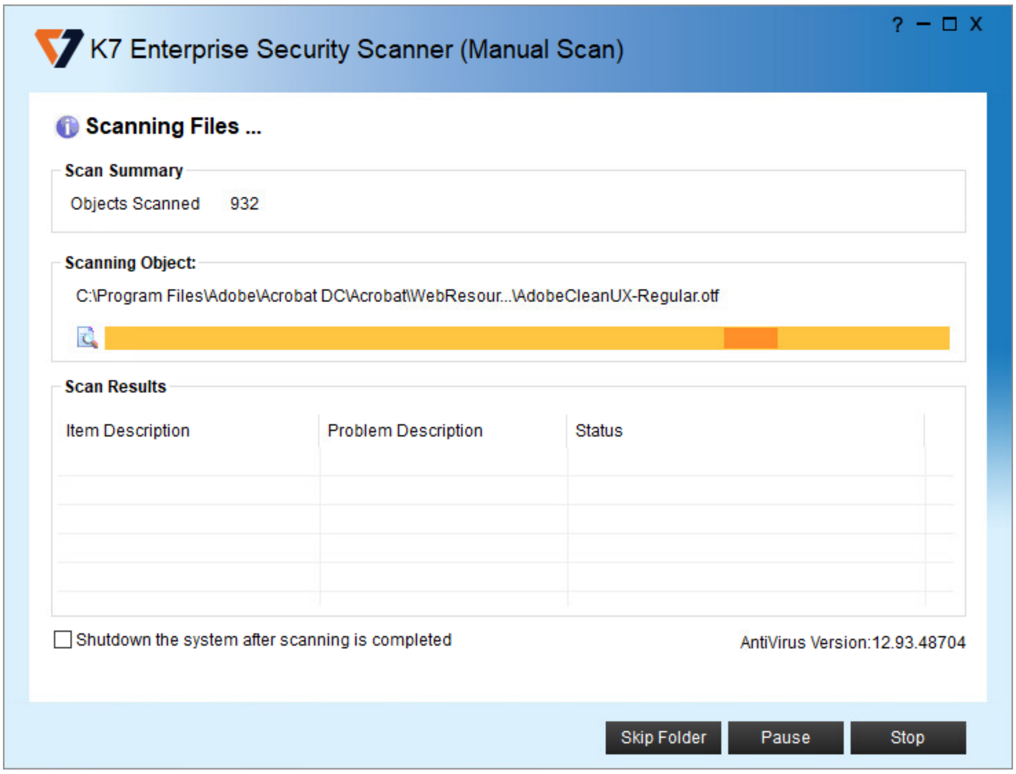
Web Categorisation: Web Categorization allows administrators to define website and content access for company devices, limiting access to unproductive or inappropriate sites.

Groups and Policies: Endpoint security is managed through groups and policies, controlling malware detection, and user settings. Default settings provide optimum security, and end-users are limited to updates and scans.

Application control: This enables automatic reporting and blocking of applications, including version-based blocking.

Fine control of administrative privileges: Administrative privileges can be fine-tuned with custom roles and group-based administration.

Scans: Options include Quick Scan, Full System Scan, and Vulnerability Scan, with patch links. Scans can be scheduled and deployed to desired endpoints.


K7 Enterprise Security Scanner (Manual Scan)

Scanning Files ...

Scan Summary

Objects Scanned 932

Scanning Object:

C:\Program Files\Adobe\Acrobat DC\Acrobat\WebResour...\AdobeCleanUX-Regular.otf

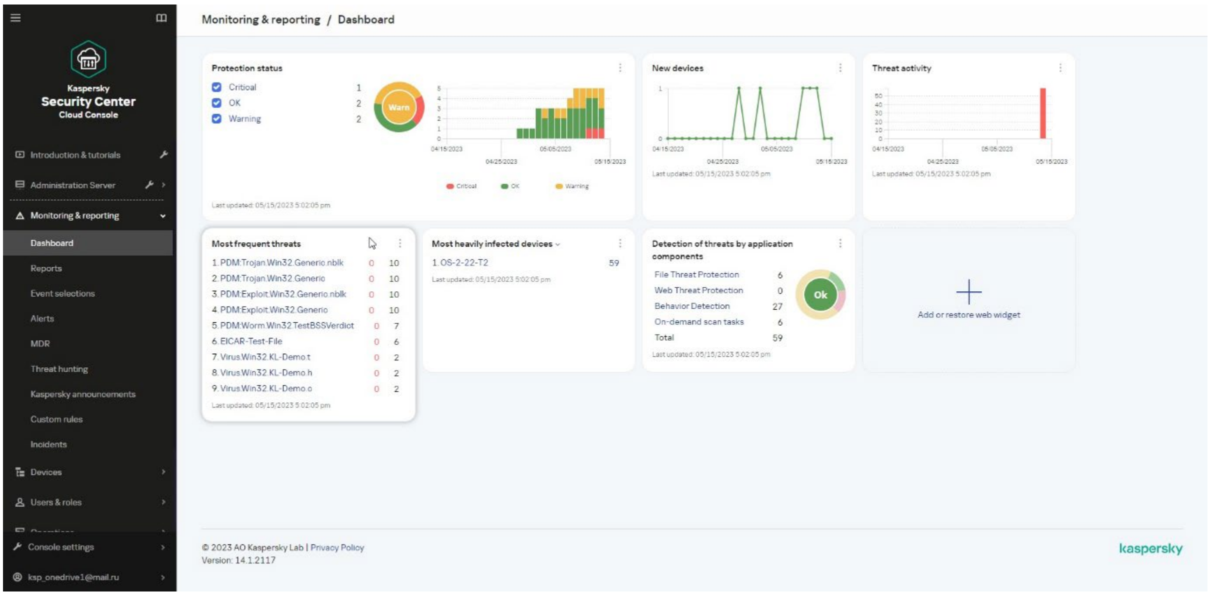
Scan Results

Item Description	Problem Description	Status

□ Shutdown the system after scanning is completed

AntiVirus Version:12.93.48704

Kaspersky Endpoint Security for Business – Select, with KSC



Protection status

☑ Critical	1
☑ OK	2
☑ Warning	2

Last updated: 05/15/2023 5:02:05 pm

New devices — Last updated: 05/15/2023 5:02:05 pm

Threat activity — Last updated: 05/15/2023 5:02:05 pm

Most frequent threats

1. PDM:Trojan.Win32.Generic.nblk	0	10
2. PDM:Trojan.Win32.Generic	0	10
3. PDM:Exploit.Win32.Generic.nblk	0	10
4. PDM:Exploit.Win32.Generic	0	10
5. PDM:Worm.Win32.TestBSSVerdict	0	7
6. EICAR-Test-File	0	6
7. Virus.Win32.KL-Demo.t	0	2
8. Virus.Win32.KL-Demo.h	0	2
9. Virus.Win32.KL-Demo.c	0	2

Last updated: 05/15/2023 5:02:05 pm

Most heavily infected devices

1. OS-2-22-T2	59

Last updated: 05/15/2023 5:02:05 pm

Detection of threats by application components

File Threat Protection	6
Web Threat Protection	0
Behavior Detection	27
On-demand scan tasks	6
Total	59

Last updated: 05/15/2023 5:02:05 pm

© 2023 AO Kaspersky Lab | Privacy Policy
Version: 14.1.2117

Kaspersky Endpoint Security for Business is a next-gen endpoint security solution which can secure organizations against a wide range of threats, from BIOS-related to fileless threats. The solution provides crucial endpoint management and security tools to IT administrators and cybersecurity specialists in organizations of any size and type.

Key Features

Protect user data: Kaspersky Endpoint Security for Business protects all endpoints against widespread and emerging threats, thanks to Kaspersky technologies like behaviour-based protection from advanced threats including fileless ones, ML-based analysis, and specific protection against exploits, ransomware, miners and financial spyware. Recognizing threat behaviour patterns, allows for the neutralizing of unknown threats.

Proactive protection: Stops attacks before they start. System hardening by Adaptive Anomaly Control combines the simplicity of blocking rules with the smartness of automatic tuning, based on behaviour analysis.

Reduced attack surface: This is achieved by controlling what applications, websites and devices can interact with endpoints and users.

Complete ecosystem: Users can grow their IT security maturity. Automated response and analysis leverages integrations with EDR and SIEM solutions

Single solution for any platform: Security for every workstation, server and mobile device that carries user data, regardless of location and ownership.

Cross platform support: A single solution, working from a single console covers every OS in a mixed environment.

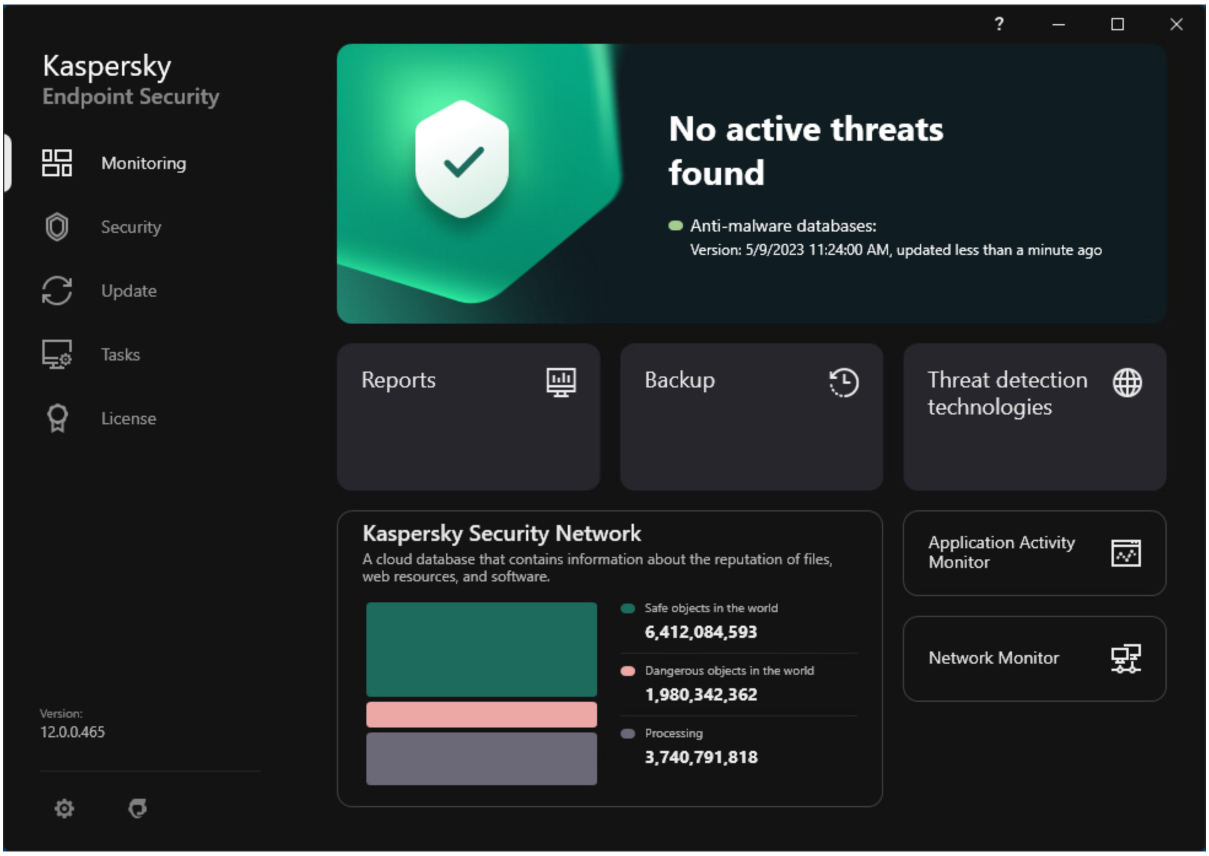
High levels of automation: Particularly for essential but routine tasks such as patching and OS deployment.

Remote management capabilities: Covering different scenarios, like setting up workstations in home offices or securing data with encryption options.

Centralization: Integrated single-screen management, either at the user's perimeter or in the cloud.

Futureproofing: Upgrading is seamless, allowing users to move through the tiers. The fully scalable solution is ready to support thousands of managed devices as companies grow.

Flexibility: Users can choose their preferred deployment option: in the cloud, on-premises, air gapped and in hybrid deployments. Then they can allocate different levels of security systems access to different team members with granular role-based access control (RBAC).



No active threats found

Anti-malware databases:
Version: 5/9/2023 11:24:00 AM, updated less than a minute ago

Kaspersky Security Network
A cloud database that contains information about the reputation of files, web resources, and software.

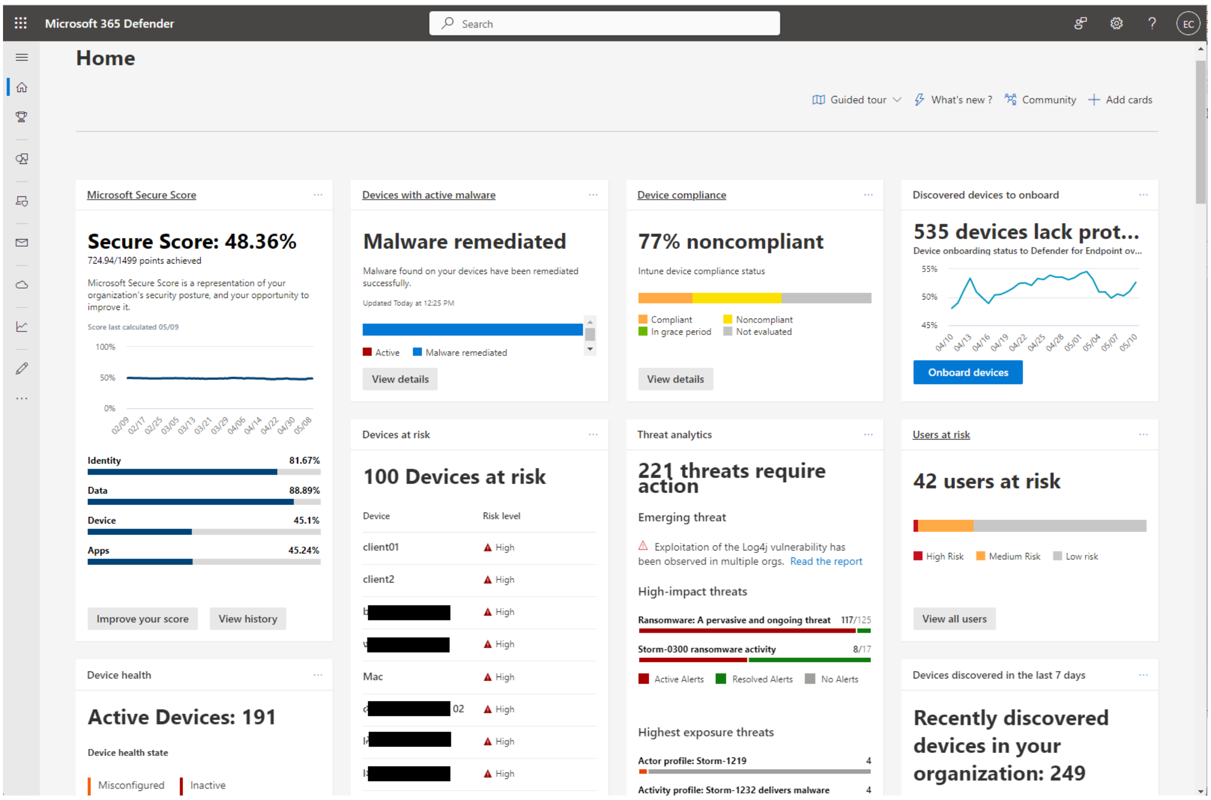
Safe objects in the world
6,412,084,593

Dangerous objects in the world
1,980,342,362

Processing
3,740,791,818

Version:
12.0.0.465

Microsoft Defender Antivirus with Microsoft Endpoint Manager



Microsoft Secure Score

Secure Score: 48.36%

724.94/1499 points achieved

Microsoft Secure Score is a representation of your organization's security posture, and your opportunity to improve it.

Score last calculated 05/09

Identity	81.67%
Data	88.89%
Device	45.1%
Apps	45.24%

Devices with active malware

Malware remediated

Malware found on your devices have been remediated successfully.

Updated Today at 12:25 PM

🟥 Active 🟦 Malware remediated

Device compliance

77% noncompliant

Intune device compliance status

🟧 Compliant 🟨 Noncompliant 🟩 In grace period ⬜ Not evaluated

Discovered devices to onboard

535 devices lack prot...

Device onboarding status to Defender for Endpoint ov...

Devices at risk

100 Devices at risk

Device	Risk level
client01	▲ High
client2	▲ High
[redacted]	▲ High
[redacted]	▲ High
Mac	▲ High
[redacted] 02	▲ High
[redacted]	▲ High
[redacted]	▲ High

Threat analytics

221 threats require action

Emerging threat

⚠ Exploitation of the Log4j vulnerability has been observed in multiple orgs. Read the report

High-impact threats

Ransomware: A pervasive and ongoing threat	117/125
Storm-0300 ransomware activity	8/17

🟥 Active Alerts 🟩 Resolved Alerts ⬜ No Alerts

Highest exposure threats

Actor profile: Storm-1219	4
Activity profile: Storm-1232 delivers malware	4

Users at risk

42 users at risk

🟥 High Risk 🟧 Medium Risk ⬜ Low risk

Device health

Active Devices: 191

Device health state

Devices discovered in the last 7 days

Recently discovered devices in your organization: 249

Microsoft Defender Antivirus is pre-installed on Windows 10/11 systems. In business environments, it can be managed e.g. with Microsoft Defender for Endpoint's P1 plan. Microsoft Defender for Endpoint is an enterprise security product designed to help organizations prevent, detect, and respond to evolving threats across operating systems and network devices. Its antivirus capability combines machine learning models trained on cloud-scale data and behaviour-based detection to protect in real-time against malware and malicious activity.

Key Features

Defender for Endpoint's P1 plan[12] allows security teams to do the following:

Eliminate blind spots in their environment: Discover unmanaged and unauthorized endpoints and network devices. Secure these assets using integrated workflows.

Block sophisticated threats and malware: Examples include novel polymorphic and metamorphic malware, and fileless and file-based threats. With cloud-delivered, next-generation protection, analysts benefit from near-instant detection and blocking of these threats.

Apply manual response actions: Security teams can act on devices or files when threats are detected, such as quarantining them.

[12] https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/defender-endpoint-plan-1

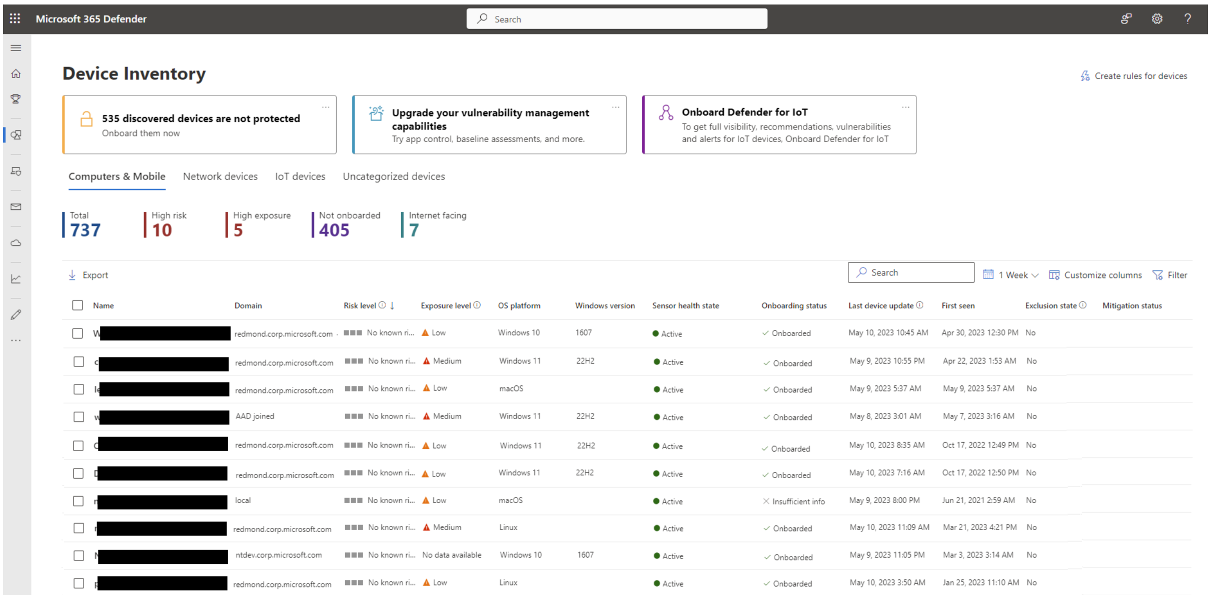
Harness attack surface reduction capabilities: Harden devices, prevent zero-day attacks, and take granular control over endpoint access and behaviours. These capabilities include rules, ransomware mitigation, device control, web protection, network protection, network firewall, and application control.

Access unified security tools and centralized management: Security administrators can use role-based access control from the Microsoft 365 Defender customizable portal to manage which users have access to which assets.

Management console: The Microsoft 365 Defender portal provides security teams access to unified security tools and centralized management. This can be used to monitor and respond to alerts of potential threats and can go beyond protecting endpoints to securing across identities, data, apps, and infrastructure.

Customizable home page: The landing page provides a customizable view that shows at-risk devices, threats detected, alerts/incidents and actionable information depending on which Microsoft Defender capabilities the organization is using. Examples of what you can see:

- **Incidents & alerts:** Lists incidents that were created as a result of triggered alerts generated as threats are detected across devices.
- **Action center:** This lists remediation actions taken. Analysts can see details like investigation package collection, antivirus scan, app restriction, and device isolation.
- **Reports section:** This section includes reports that show threats and their status.
- **Device Inventory**: A list of the devices in the user's network that triggered alerts. This shows domain, risk level, OS platform, and other details for easy identification of devices most at risk.



Device Inventory

535 discovered devices are not protected
Onboard them now

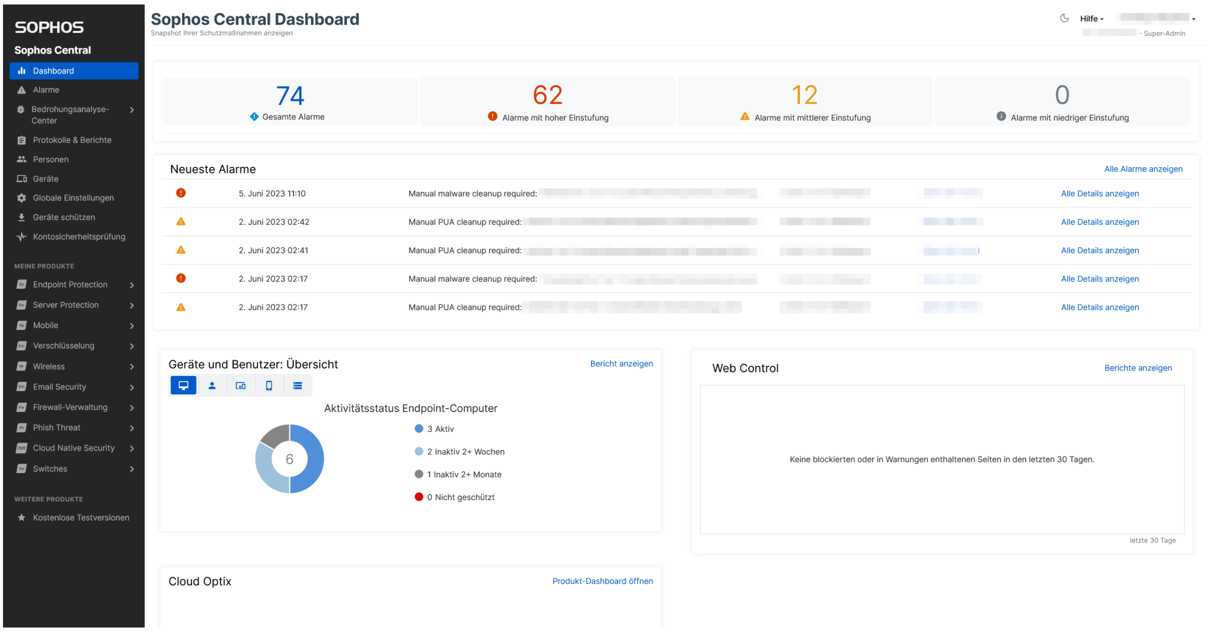
Upgrade your vulnerability management capabilities
Try app control, baseline assessments, and more.

Onboard Defender for IoT
To get full visibility, recommendations, vulnerabilities and alerts for IoT devices, Onboard Defender for IoT

Total 737 | High risk 10 | High exposure 5 | Not onboarded 405 | Internet facing 7

□	Name	Domain	Risk level	Exposure level	OS platform	Windows version	Sensor health state	Onboarding status	Last device update	First seen	Exclusion state	Mitigation status
□	[redacted]	redmond.corp.microsoft.com	No known ri...	Low	Windows 10	1607	● Active	✓ Onboarded	May 10, 2023 10:45 AM	Apr 30, 2023 12:30 PM	No	
□	[redacted]	redmond.corp.microsoft.com	No known ri...	Medium	Windows 11	22H2	● Active	✓ Onboarded	May 9, 2023 10:55 PM	Apr 22, 2023 1:53 AM	No	
□	[redacted]	redmond.corp.microsoft.com	No known ri...	Low	macOS		● Active	✓ Onboarded	May 9, 2023 5:37 AM	May 9, 2023 5:37 AM	No	
□	[redacted]	AAD joined	No known ri...	Medium	Windows 11	22H2	● Active	✓ Onboarded	May 8, 2023 3:01 AM	May 7, 2023 3:16 AM	No	
□	[redacted]	redmond.corp.microsoft.com	No known ri...	Low	Windows 11	22H2	● Active	✓ Onboarded	May 10, 2023 8:35 AM	Oct 17, 2022 12:49 PM	No	
□	[redacted]	redmond.corp.microsoft.com	No known ri...	Low	Windows 11	22H2	● Active	✓ Onboarded	May 10, 2023 7:16 AM	Oct 17, 2022 12:50 PM	No	
□	[redacted]	local	No known ri...	Low	macOS		● Active	✕ Insufficient info	May 9, 2023 8:00 PM	Jun 21, 2021 2:59 AM	No	
□	[redacted]	redmond.corp.microsoft.com	No known ri...	Medium	Linux		● Active	✓ Onboarded	May 10, 2023 11:09 AM	Mar 21, 2023 4:21 PM	No	
□	[redacted]	ntdev.corp.microsoft.com	No known ri...	No data available	Windows 10	1607	● Active	✓ Onboarded	May 9, 2023 11:05 PM	Mar 3, 2023 3:14 AM	No	
□	[redacted]	redmond.corp.microsoft.com	No known ri...	Low	Linux		● Active	✓ Onboarded	May 10, 2023 3:50 AM	Jan 25, 2023 11:10 AM	No	

Sophos Intercept X Advanced



Sophos Central Dashboard

Snapshot Ihrer Schutzmaßnahmen anzeigen

74 Gesamte Alarme | 62 Alarme mit hoher Einstufung | 12 Alarme mit mittlerer Einstufung | 0 Alarme mit niedriger Einstufung

Neueste Alarme — Alle Alarme anzeigen

●	5. Juni 2023 11:10	Manual malware cleanup required: [redacted]	[redacted]	[redacted]	Alle Details anzeigen
⚠	2. Juni 2023 02:42	Manual PUA cleanup required: [redacted]	[redacted]	[redacted]	Alle Details anzeigen
⚠	2. Juni 2023 02:41	Manual PUA cleanup required: [redacted]	[redacted]	[redacted]	Alle Details anzeigen
●	2. Juni 2023 02:17	Manual malware cleanup required: [redacted]	[redacted]	[redacted]	Alle Details anzeigen
⚠	2. Juni 2023 02:17	Manual PUA cleanup required: [redacted]	[redacted]	[redacted]	Alle Details anzeigen

Geräte und Benutzer: Übersicht — Bericht anzeigen

Aktivitätsstatus Endpoint-Computer

- 3 Aktiv
- 2 Inaktiv 2+ Wochen
- 1 Inaktiv 2+ Monate
- 0 Nicht geschützt

Web Control — Berichte anzeigen

Keine blockierten oder in Warnungen enthaltenen Seiten in den letzten 30 Tagen.

letzte 30 Tage

Cloud Optix — Produkt-Dashboard öffnen

Sophos Intercept X Advanced is an endpoint security solution designed to minimize the attack surface and prevent attacks. It combines multiple technologies, including anti-exploit, anti-ransomware, deep learning AI, and control technology to detect and block threats before they can impact users' systems.

Key Features

Stop Unknown Threats: Intercept X utilizes deep learning AI to identify and block malware that hasn't been seen before. It analyses file attributes to detect threats without relying on signatures.

Block Ransomware: Intercept X incorporates anti-ransomware capabilities that identify and block the encryption processes used in ransomware attacks. Encrypted files can be rolled back to a safe state, minimizing the potential impact.

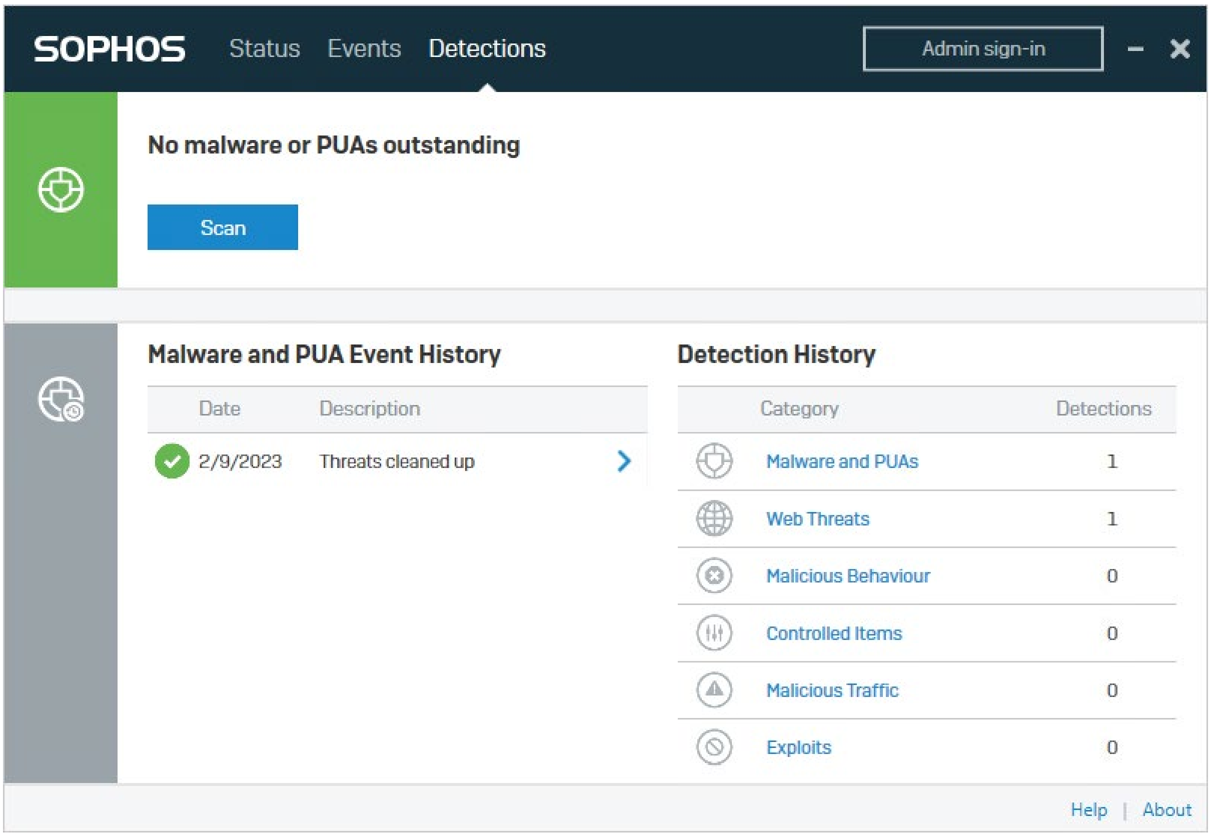
Prevent Exploits: The anti-exploit technology in Intercept X prevents attackers from leveraging exploit techniques to compromise devices, steal credentials, and distribute malware. This protection extends to file-less attacks and zero-day exploits.

Reduce the Attack Surface: Users have control over the apps and devices allowed to run in their environment. Intercept X enables blocking of malicious websites and potentially unwanted apps (PUAs).

Synchronized Security: Sophos solutions work together seamlessly. For instance, Intercept X and Sophos Firewall share data to isolate compromised devices during cleanup, restoring network access once the threat is neutralized, all without requiring admin intervention.

Straightforward Management: Intercept X is managed through Sophos Central, the cloud-based management platform for all Sophos solutions. This centralized management approach simplifies deployment, configuration, and management, including remote working setups.

AI and Expert Powered Data: Intercept X combines the power of deep learning AI with the expertise of SophosLabs cybersecurity professionals to provide robust protection and accurate threat detection.



No malware or PUAs outstanding

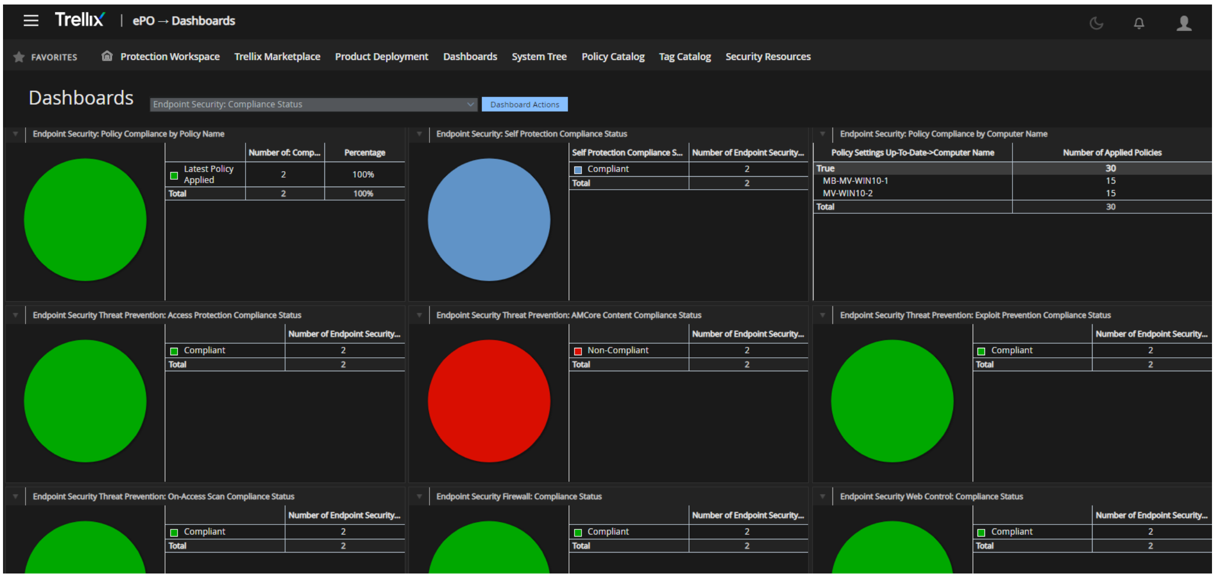
Malware and PUA Event History

Date	Description
✓ 2/9/2023	Threats cleaned up

Detection History

Category	Detections
Malware and PUAs	1
Web Threats	1
Malicious Behaviour	0
Controlled Items	0
Malicious Traffic	0
Exploits	0

Trellix Endpoint Security (ENS)



Endpoint Security: Policy Compliance by Policy Name

	Number of: Comp...	Percentage
🟩 Latest Policy Applied	2	100%
Total	2	100%

Endpoint Security: Self Protection Compliance Status

Self Protection Compliance S...	Number of Endpoint Security...
🟦 Compliant	2
Total	2

Endpoint Security: Policy Compliance by Computer Name

Policy Settings Up-To-Date->Computer Name	Number of Applied Policies
True	30
MB-MV-WIN10-1	15
MV-WIN10-2	15
Total	30

Endpoint Security Threat Prevention: Access Protection Compliance Status

	Number of Endpoint Security...
🟩 Compliant	2
Total	2

Endpoint Security Threat Prevention: AMCore Content Compliance Status

	Number of Endpoint Security...
🟥 Non-Compliant	2
Total	2

Endpoint Security Threat Prevention: Exploit Prevention Compliance Status

	Number of Endpoint Security...
🟩 Compliant	2
Total	2

Endpoint Security Threat Prevention: On-Access Scan Compliance Status

	Number of Endpoint Security...
🟩 Compliant	2
Total	2

Endpoint Security Firewall: Compliance Status

	Number of Endpoint Security...
🟩 Compliant	2
Total	2

Endpoint Security Web Control: Compliance Status

	Number of Endpoint Security...
🟩 Compliant	2
Total	2

Trellix Endpoint Security (ENS) is a comprehensive security solution designed for enterprise networks of all sizes. The ePolicy Orchestrator management console offers flexible options, including both cloud-based and on-premises consoles, for efficient management of the endpoint protection software.

Key Features

Customizable Dashboard: The dashboard and reporting can be tailored to display relevant endpoint status information for each user.

Deployment Flexibility: The console offers a variety of deployment options, including cloud-based, on-premises hosting, and Amazon hosting.

Management Console: The ePolicy Orchestrator console is easily accessed through the primary navigation menu located at the top left of the main dashboard. It provides access to different sections and pages, such as *Dashboard*, *Reporting*, *Policy Management*, *Automation*, and *Software and Systems Administration*. Integration of additional components like DLP, Mobile Security, and Insights Threat Intelligence and EDR is also available.

Real Protect: Through machine learning classification, threats are detected in real time, and behavior classification continually evolves to identify future attacks. Endpoints are restored to the last known good state, preventing infections and reducing administrative burdens.

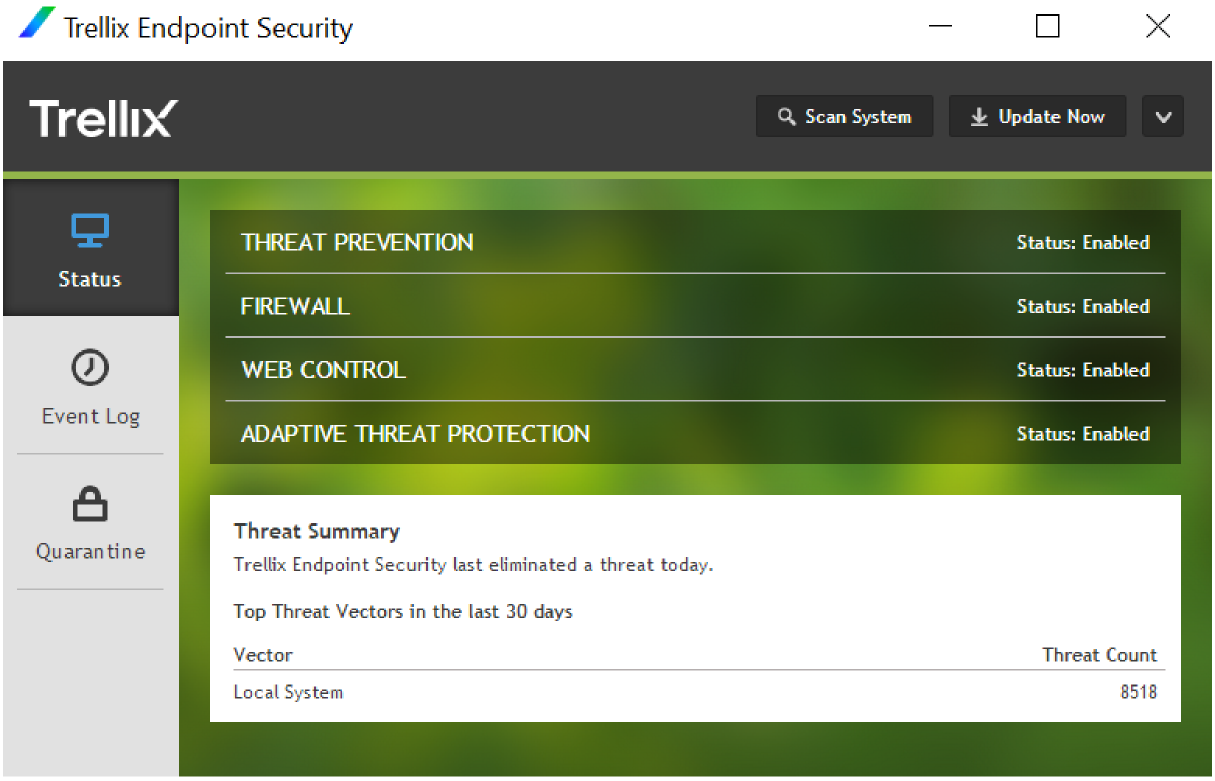
Adaptive Scanning: The system intelligently skips scanning trusted processes and gives priority to suspicious processes and applications during scanning.

Endpoint Client Deployment: Client agent packages can be created on the Product Deployment page. The installer file can be distributed via a web link, manually executed, or deployed through a systems management product. After installation, the agent downloads the necessary protection engine before full protection becomes active. The client interface displays the installed and enabled protection components.

Proactive web security: This feature ensures safe browsing by providing web protection and filtering for endpoints.

Hostile network attack blocking: The integrated firewall utilizes reputation scores based on GTI to safeguard endpoints against botnets, DDoS attacks, advanced persistent threats, and suspicious web connections. During system startup, the firewall only allows outbound traffic, providing protection when endpoints are not connected to the corporate network.

Antimalware protection: Trellix protects, detects, and corrects malware quickly with an antimalware engine that works across multiple devices and operating systems.



THREAT PREVENTION Status: Enabled

FIREWALL Status: Enabled

WEB CONTROL Status: Enabled

ADAPTIVE THREAT PROTECTION Status: Enabled

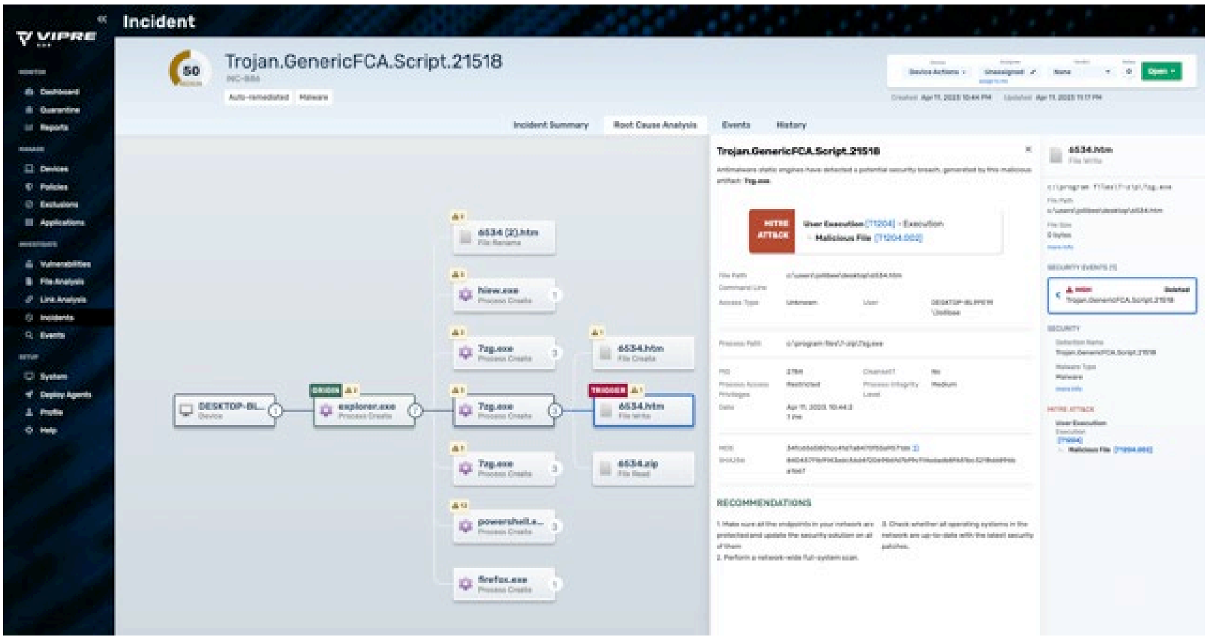
Threat Summary

Trellix Endpoint Security last eliminated a threat today.

Top Threat Vectors in the last 30 days

Vector	Threat Count
Local System	8518

VIPRE Endpoint Detection & Response



VIPRE Endpoint Detection & Response (EDR) provides comprehensive endpoint protection with next-gen antivirus (NGAV) and EDR features combined into a seamless platform. Designed to automatically block the vast majority of threats, and to provide for quick and efficient containment and investigation of potential threats, VIPRE provides everything you need to keep your endpoints and users safe.

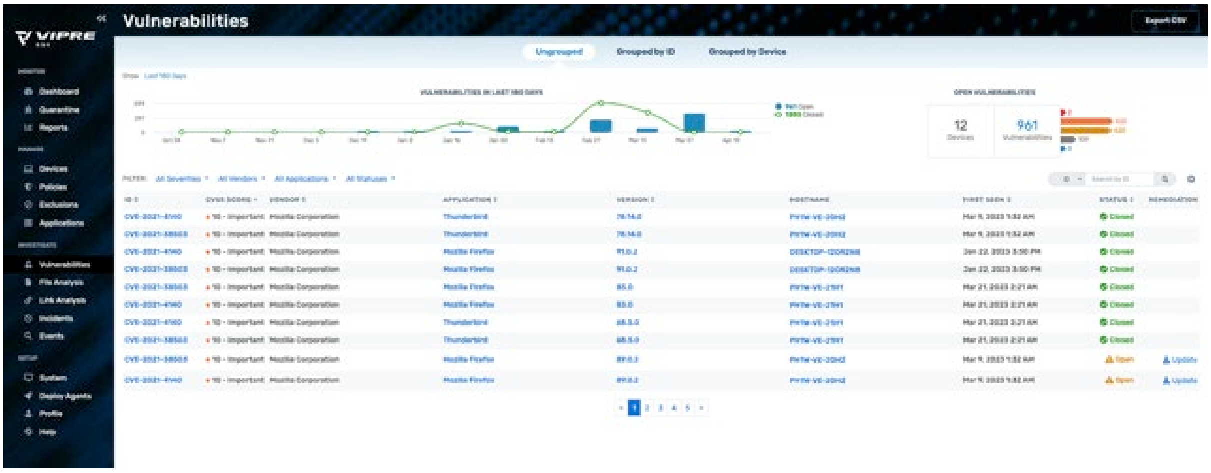
Key Features

Detailed network protection: This includes a full IDS, DNS Protection, and browser exploit prevention. The core NGAV components scan for and remove any latent malware, and behavioural process monitoring ensures that apps and users behave. The EDR layer on top of these core components orchestrates response to zero-day and persistent threats that can't be immediately identified as malicious, but that represent a possible threat.

Supports investigation: EDR bundles in endpoint vulnerability scanning, raw event telemetry, and detailed root cause analysis. VIPRE Endpoint Detection & Response (EDR) includes access to cloud-based malware analysis sandboxes to investigate suspicious files and URLs, with detailed results presented right in the console. It also includes a simple method to isolate endpoints that are misbehaving, to prevent attack spread and give you time to understand what is happening on the endpoint.

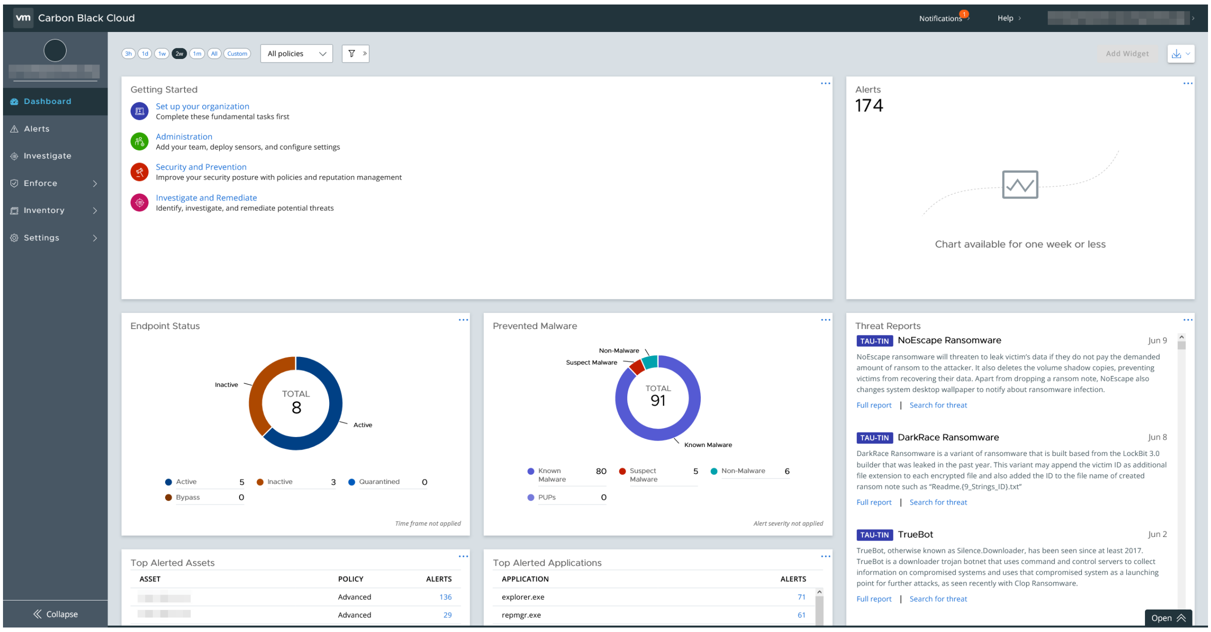
Remediate threats on endpoints: EDR will help patch vulnerable applications automatically and provides for integrated remote access to the endpoint to clean up files, processes, registry keys, and more. Any files corrupted by zero-day ransomware will be restored. Any security gaps identified by your investigation can be closed quickly.

Single Interface: VIPRE EDR combines all these tools into a clean, easy to use interface that helps speed response times and reduce confusion. Mobile responders can access everything from their smartphones, avoiding the expense, annoyance, and delays of having to rush into the office. And with transparent delegated access via VIPRE Site Manager, MSPs, MSSPs, and MDR providers can assist in incident response and investigation with zero friction.



ID	CVSS SCORE	VENDOR	APPLICATION	VERSION	HOSTNAME	FIRST SEEN	STATUS	REMEDIATION
CVE-2021-4140	10 - Important	Mozilla Corporation	Thunderbird	78.14.0	PWIN-VE-20H2	Mar 9, 2023 1:32 AM	Closed	
CVE-2021-38503	10 - Important	Mozilla Corporation	Thunderbird	78.14.0	PWIN-VE-20H2	Mar 9, 2023 1:32 AM	Closed	
CVE-2021-4140	10 - Important	Mozilla Corporation	Mozilla Firefox	91.0.2	DESKTOP-12OR2N8	Jan 22, 2023 3:50 PM	Closed	
CVE-2021-38503	10 - Important	Mozilla Corporation	Mozilla Firefox	91.0.2	DESKTOP-12OR2N8	Jan 22, 2023 3:50 PM	Closed	
CVE-2021-38503	10 - Important	Mozilla Corporation	Mozilla Firefox	85.0	PWIN-VE-21H1	Mar 21, 2023 2:21 AM	Closed	
CVE-2021-4140	10 - Important	Mozilla Corporation	Mozilla Firefox	85.0	PWIN-VE-21H1	Mar 21, 2023 2:21 AM	Closed	
CVE-2021-4140	10 - Important	Mozilla Corporation	Thunderbird	68.5.0	PWIN-VE-21H1	Mar 21, 2023 2:21 AM	Closed	
CVE-2021-38503	10 - Important	Mozilla Corporation	Thunderbird	68.5.0	PWIN-VE-21H1	Mar 21, 2023 2:21 AM	Closed	
CVE-2021-38503	10 - Important	Mozilla Corporation	Mozilla Firefox	89.0.2	PWIN-VE-20H2	Mar 9, 2023 1:32 AM	Open	Update
CVE-2021-4140	10 - Important	Mozilla Corporation	Mozilla Firefox	89.0.2	PWIN-VE-20H2	Mar 9, 2023 1:32 AM	Open	Update

VMware Carbon Black Cloud Endpoint Standard



[redacted]

Getting Started

Set up your organization
Complete these fundamental tasks first

Administration
Add your team, deploy sensors, and configure settings

Security and Prevention
Improve your security posture with policies and reputation management

Investigate and Remediate
Identify, investigate, and remediate potential threats

Chart available for one week or less

● Active	5	● Inactive	3	● Quarantined	0
● Bypass	0				

Time frame not applied

● Known Malware	80	● Suspect Malware	5	● Non-Malware	6
● PUPs	0				

Alert severity not applied

Threat Reports

TAU-TIN NoEscape Ransomware Jun 9

NoEscape ransomware will threaten to leak victim's data if they do not pay the demanded amount of ransom to the attacker. It also deletes the volume shadow copies, preventing victims from recovering their data. Apart from dropping a ransom note, NoEscape also changes system desktop wallpaper to notify about ransomware infection.

Full report | Search for threat

TAU-TIN DarkRace Ransomware Jun 8

DarkRace Ransomware is a variant of ransomware that is built based from the LockBit 3.0 builder that was leaked in the past year. This variant may append the victim ID as additional file extension to each encrypted file and also added the ID to the file name of created ransom note such as "Readme.{9_Strings_ID}.txt"

Full report | Search for threat

TAU-TIN TrueBot Jun 2

TrueBot, otherwise known as Silence.Downloader, has been seen since at least 2017. TrueBot is a downloader trojan botnet that uses command and control servers to collect information on compromised systems and uses that compromised system as a launching point for further attacks, as seen recently with Clop Ransomware.

Full report | Search for threat

Top Alerted Assets

ASSET	POLICY	ALERTS
[redacted]	Advanced	136
[redacted]	Advanced	29

Top Alerted Applications

APPLICATION	ALERTS
explorer.exe	71
repmgr.exe	61

VMware Carbon Black Cloud™ Endpoint Standard is a cloud native endpoint, workload, and container protection platform that combines the intelligent system hardening and behavioural prevention needed to keep emerging threats at bay. The cloud native protection platform enables customers to utilize different modular capabilities to identify risk, prevent, detect and respond to known and unknown threats using a single lightweight agent and an easy-to-use console. Its sensor serves as both a continuous event recorder and preventive action agent. For detection and response purposes, the VMware Carbon Black Cloud captures all process executions and associated metadata, file modifications, registry modifications, network connections, authentication events, module loads, fileless script executions, and cross-process behaviours (i.e., Process injection). All this behavioural activity is captured and streamed live to your cloud instance for visualization, searching, alerting, and blocking. This allows for both real-time and historical threat hunting across your environment. The VMware Carbon Black Cloud also keeps track of every application executed in your environment and its metadata, including a copy of that binary for forensics purposes.

Key Features

Threat prevention updates: Carbon Black deploys updates to prevent the latest attack techniques focused on behavioural attributes quickly without additional effort required by users.

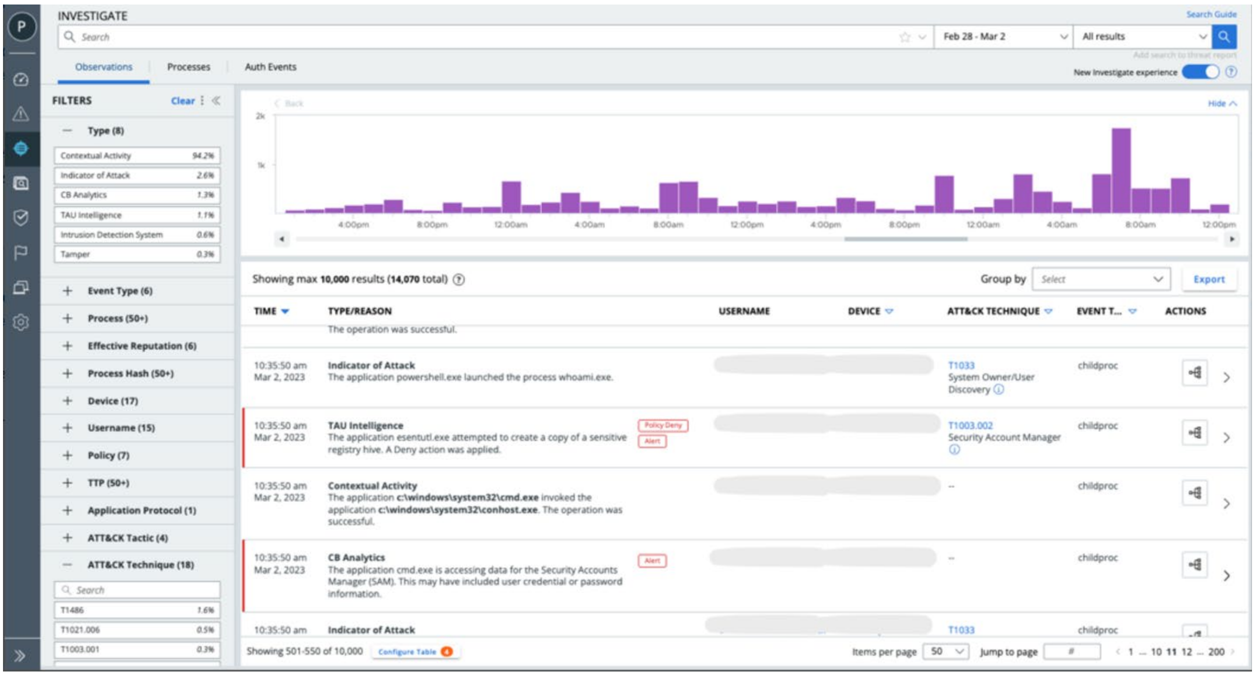
Custom detections: Rapidly deploy custom detections in the form of threat intelligence indicators focusing on the same behavioural attributes.

Alert and detections mapping: Alerts and detection techniques can be directly mapped to MITRE ATT&CK®.

Post analysis tools: Search for binary prevalence, process masquerading, binary signing issuers, and forensic capture for post analysis

Robust and extensible API: Some examples of 3rd party API integrations are:

- YARA
- Out of the box SIEM, SOAR and ITSM API integrations
- Binary Detonation and Sandboxing Uploads
- Network security/service appliances (DNS, IDS, IPS, DHCP)
- File integrity monitoring - VMware Carbon Black Cloud can alert any time files, file paths, registry keys, and registry hives are modified.



Type (8)	
Contextual Activity	94.2%
Indicator of Attack	2.6%
CB Analytics	1.3%
TAU Intelligence	1.1%
Intrusion Detection System	0.6%
Tamper	0.3%

Event Type (6)
Process (50+)
Effective Reputation (6)
Process Hash (50+)
Device (17)
Username (15)
Policy (7)
TTP (50+)
Application Protocol (1)
ATT&CK Tactic (4)

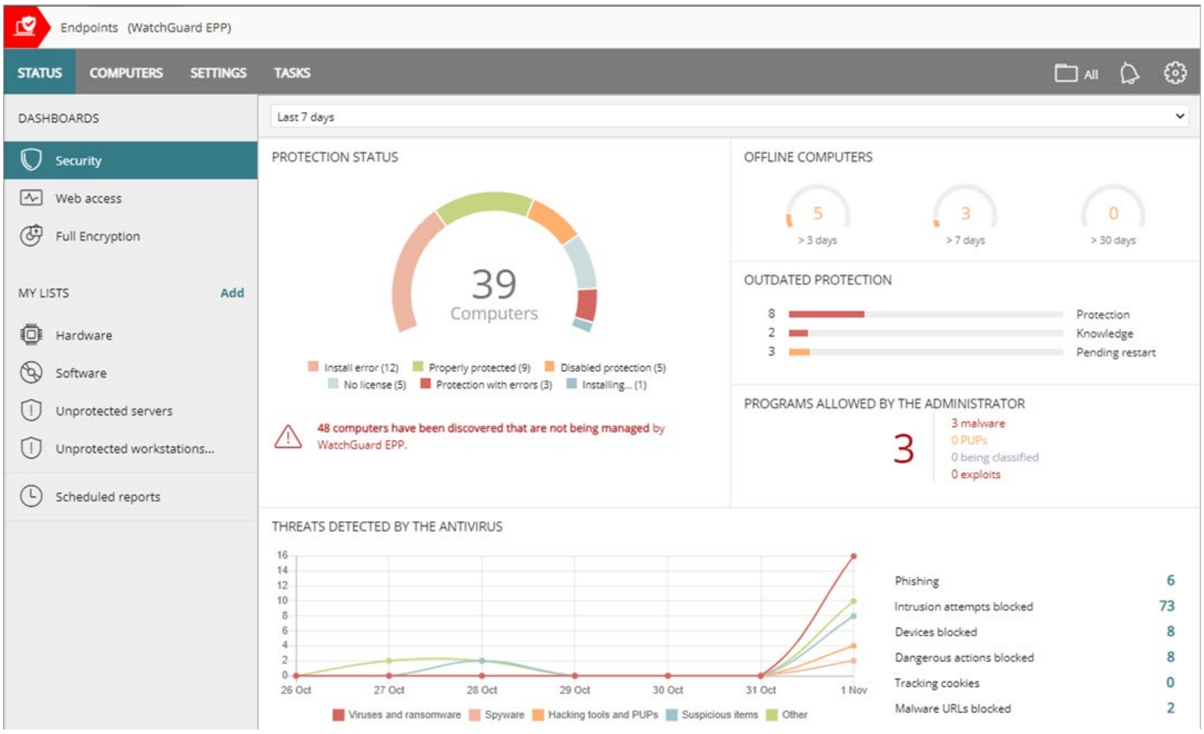
ATT&CK Technique (18)	
T1486	1.6%
T1021.006	0.5%
T1003.001	0.3%

Showing max **10,000** results (**14,070** total)

TIME	TYPE/REASON		USERNAME	DEVICE	ATT&CK TECHNIQUE	EVENT T...	ACTIONS
	The operation was successful.						
10:35:50 am Mar 2, 2023	**Indicator of Attack** The application powershell.exe launched the process whoami.exe.		[redacted]		T1033 System Owner/User Discovery	childproc	
10:35:50 am Mar 2, 2023	**TAU Intelligence** The application esentutl.exe attempted to create a copy of a sensitive registry hive. A Deny action was applied.	Policy Deny Alert	[redacted]		T1003.002 Security Account Manager	childproc	
10:35:50 am Mar 2, 2023	**Contextual Activity** The application **c:\windows\system32\cmd.exe** invoked the application **c:\windows\system32\conhost.exe**. The operation was successful.		[redacted]		--	childproc	
10:35:50 am Mar 2, 2023	**CB Analytics** The application cmd.exe is accessing data for the Security Accounts Manager (SAM). This may have included user credential or password information.	Alert	[redacted]		--	childproc	
10:35:50 am	**Indicator of Attack**		[redacted]		T1033	childproc	

Showing 501-550 of 10,000

WatchGuard Endpoint Protection Platform (EPP)



48 computers have been discovered that are not being managed by WatchGuard EPP.

Phishing	6
Intrusion attempts blocked	73
Devices blocked	8
Dangerous actions blocked	8
Tracking cookies	0
Malware URLs blocked	2

WatchGuard EPP is a cloud-native security solution that centralizes next-gen antivirus with advanced technologies to protect against threats. It offers real-time monitoring, behaviour analysis, and blocking of malware. WatchGuard EPP defends against ransomware attacks with contextual detections, anti-phishing, decoy files, and shadow copies.

Key Features

Multiplatform Security*:* cross-platform security for various systems. Management of licenses belonging to both persistent and non-persistent virtualization infrastructure (VDI).

Management and Installation: Multiple deployment methods available, with automatic uninstallers for other products allowing rapid migration from third-party solutions. Deployment can be done via email and download URL, or silently to selected endpoints via the solution's distribution tool. The MSI installer is compatible with third-party tools (Active Directory, Tivoli, SMS, etc.).

Performance*:* all operations are performed on the Cloud. WatchGuard EPP requires no installation, management, or maintenance of new hardware resources in the organization's infrastructure.

Centralize Device Security: centralized management from a single web-based administration console for all workstations and servers on the corporate network.

Malware and Ransomware Protection: WatchGuard EPP analyses behaviours and hacking techniques to detect and block both known and unknown malware, as well as ransomware, trojans and phishing.

Advanced Disinfection: in the event of a security breach, affected computers can be restored to the state before infection with advanced disinfection tools. Quarantine stores suspicious and deleted items. Administrators can remotely restart workstations and servers to ensure the latest product updates are installed.

Real-time Monitoring and Reports: detailed, real-time security monitoring is delivered via comprehensive dashboards and easy-to-interpret graphs. Reports are automatically generated and delivered on protection status, detections, and improper use of devices.

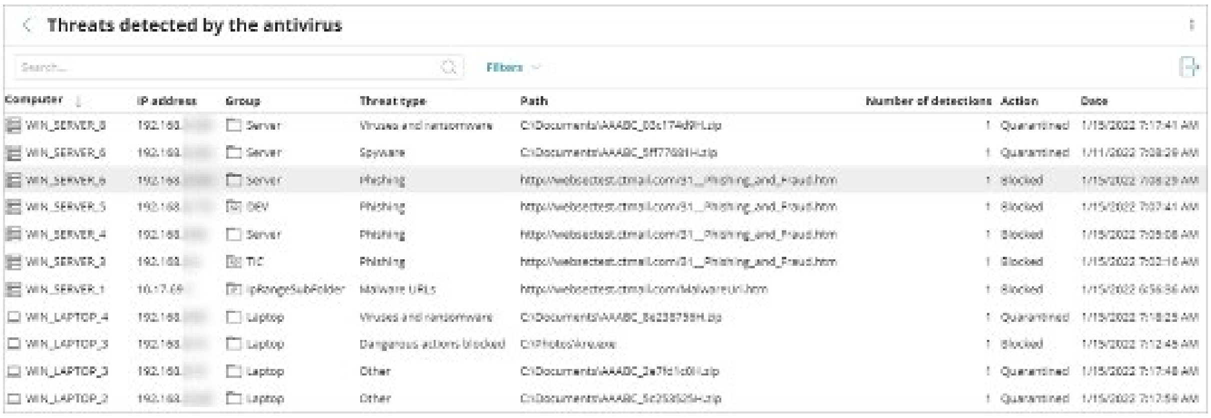
Granular Configuration of Profiles: Assign user profile-based protection policies, ensuring appropriate policies for every user group.

Centralized Device Control: Stop malware and information leaks by blocking device categories (flash drives, USB modems, webcams, DVD/CD, etc.), allowlisting devices or configuring read-only, write-only, and read-and-write access permissions.

Vulnerability Assessment: Vulnerability assessment helps IT teams to identify, evaluate, and prioritize security weaknesses and vulnerabilities in applications and systems.

Malware Freezer: Quarantines malware for seven days and, in the event of a false positive, automatically restores the affected file to the system.

Ransomware Remediation and Recovery: Besides encrypting files, adversaries try to delete backup and VSS files and turn off services designed to help recovery. Files are protected using shadow copies, which can be used to recover ransomware encrypted files.



Computer	IP address	Group	Threat type	Path	Number of detections	Action	Date
WIN_SERVER_8	192.168.[redacted]	Server	Viruses and ransomware	C:\Documents\AAABC_03c174d9H.zip	1	Quarantined	1/15/2022 7:17:41 AM
WIN_SERVER_6	192.168.[redacted]	Server	Spyware	C:\Documents\AAABC_5ff77691H.zip	1	Quarantined	1/11/2022 7:08:29 AM
WIN_SERVER_6	192.168.[redacted]	Server	Phishing	http://websectest.ctmail.com/31__Phishing_and_Fraud.htm	1	Blocked	1/15/2022 7:08:29 AM
WIN_SERVER_5	192.168.[redacted]	DEV	Phishing	http://websectest.ctmail.com/31__Phishing_and_Fraud.htm	1	Blocked	1/15/2022 7:07:41 AM
WIN_SERVER_4	192.168.[redacted]	Server	Phishing	http://websectest.ctmail.com/31__Phishing_and_Fraud.htm	1	Blocked	1/15/2022 7:05:08 AM
WIN_SERVER_3	192.168.[redacted]	TIC	Phishing	http://websectest.ctmail.com/31__Phishing_and_Fraud.htm	1	Blocked	1/15/2022 7:02:16 AM
WIN_SERVER_1	10.17.69.[redacted]	IpRangeSubFolder	Malware URLs	http://websectest.ctmail.com/MalwareUrl.htm	1	Blocked	1/15/2022 6:56:56 AM
WIN_LAPTOP_4	192.168.[redacted]	Laptop	Viruses and ransomware	C:\Documents\AAABC_8e238759H.zip	1	Quarantined	1/15/2022 7:18:25 AM
WIN_LAPTOP_3	192.168.[redacted]	Laptop	Dangerous actions blocked	C:\Photos\Arv.exe	1	Blocked	1/15/2022 7:12:45 AM
WIN_LAPTOP_3	192.168.[redacted]	Laptop	Other	C:\Documents\AAABC_2e7fd1c0H.zip	1	Quarantined	1/15/2022 7:17:48 AM
WIN_LAPTOP_2	192.168.[redacted]	Laptop	Other	C:\Documents\AAABC_5c253525H.zip	1	Quarantined	1/15/2022 7:17:56 AM

WatchGuard EPP is an essential component within WatchGuard EPDR, a comprehensive solution combining a wide range of endpoint protection (EPP) technologies with Endpoint Detection and Response (EDR) capabilities. EPDR seamlessly integrates advanced functionalities, including Zero-Trust Application and Threat Hunting features, to deliver a unified defence against intricate endpoint threats.

Features (as of November 2023)	Avast Ultimate Business Security	Bitdefender GravityZone Business Security Premium	CISCO Secure Endpoint Essentials	CrowdStrike Falcon Pro	Cybereason NGAV	Elastic Security	ESET PROTECT Entry & ESET PROTECT Cloud	G Data Endpoint Protection Business	K7 On-Premises Enterprise Security Advanced	Kaspersky Endpoint Security for Business Select, with KSC	Microsoft Defender Antivirus with MEM	Sophos Intercept X Advanced	Trellix Endpoint Security (ENS)	VIPRE Endpoint Detection & Response	VMware CarbonBlack Cloud Endpoint Standard	WatchGuard Endpoint Protection Platform
Available Console Types																
Cloud-based console	•	•	•	•	•	•	•		•	•	•	•	•	•	•	•
On-premise server-based console	•	•	•		•	•	•	•	•	•			•	•		
Multi-tenancy features for managed service providers included in the licence	•	•	•	•	•	•	•	•	•	•		•		•	•	•
Client software deployment methods																
Creation of .exe or .msi installer package	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•
Share a link to remote users to install the software themselves	•	•	•	•		•	•	•	•	•	•	•	•	•	•	•
Push installation from the console	•	•	•			•	•	•	•	•	•		•	•		•
Supported Operating Systems																
Microsoft Windows																
↪ Windows 7	•	•	•	•	•		•	•	•	•		•	•	•	•	•
↪ Windows 8	•	•	•	•	•	•	•	•	•	•		•	•	•	•	•
↪ Windows 10	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•
↪ Windows 11	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•
Virtual environments (such as VMware, HyperV)		•	•	•	•	•	•	•	•	•	•	•	•	•	•	•
Apple macOS	•	•	•	•	•	•	•	•		•	•	•	•	•	•	•
Linux		•	•	•	•	•	•	•		•	•	•	•		•	•
Google Android		•	•	•	•		•	•		•	•	•		•		•
Apple iOS		•	•	•	•		•	•		•		•		•		•
Windows Features																
Anti-Malware	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•
Registers as AV product in Windows Security Center	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•
Protection settings are enabled by default (out-of-the-box-protection)	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•
Settings & Uninstall protection	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•
Can clean-up a previously infected system (incl. registry leftovers and inactive malware)	•	•	•		•		•	•	•	•	•	•	•	•	•	•
Right-click on-demand scan of files/folders	•	•	•		•		•	•	•	•		•	•	•		•
The online malware detection rate is the same as offline		•	•		•	•	•	•	•				•	•	•	
Scans files ONLY on execution (by default/design)				•												
Phishing protection (blocking of phishing URLs)	•	•	•				•	•	•	•	•	•		•		•
Firewall	•	•	•				•	•	•	•	•	•	•	•	•	•
Web access control / webfilter (custom blacklisting of URLs / site categories)	•	•			•		•	•	•	•	•	•	•	•		•
Device control	•	•	•		•		•	•	•	•		•	•	•	•	•
Anti-Spam		•					•	•			•	•		•		
Data or Email encryption		•					•					•				•
Splunk support		•	•	•	•	•				•		•	•		•	
2-factor authentication: obligatory/optional/not included	Optional	Obligatory	Obligatory	Obligatory	Optional	Optional	Optional	Not included	Not included	Optional	Not included	Obligatory	Optional	Optional	Optional	Optional
Languages																
Which languages can be used to contact support?	English, Czech, French, German, Portuguese	English, Spanish, German, Romanian, French	All	English	English, Japanese	English, French, German, Japanese, Mandarin, Korean, Spanish, Portugese	All	German, English, French, Italian, Spanish, Portuguese, Polish	English, Hindi	English, Russian, Turkish, Chinese, Japanese, Korean, French, Italian, Spanish, Portuguese, German, Arabic, Hebrew, Hindi	All	English, Italian, German, Spanish, French, Japanese	English, Japanese, French, Italian, Spanish, Portuguese, Arabic, Turkish, Herbrew	English, Swedish, Danish	All	All
Which interface languages is the product available in?	English, Spanish, French, German, Italian, Portuguese, Russian, Norwegian, Dutch, Bulgarian, Chinese, Czech, Estonian, Finnish, Greek, Hungarian, Japanese, Korean, Polish, Slovak, Slovenian, Swedish, Turkish, Ukrainian, Vietnamese	English, Spanish, German, Romanian, French, Italian, Portuguese, Polish, Russian, Czech, Chinese, Korean	English, Japanese, Korean, Chinese				English, Arabic, Bulgarian, Chinese, Croatian, Czech, Dutch, Estonian, Finnish, French, German, Greek, Hebrew, Hungarian, Indonesian, Italian, Japanese, Kazakh, Korean, Latvian, Lithnuanian, Norwenian, Polish, Portuguese, Romanian, Russian, Spanish, Swedish, Slovak, Slovenian, Thai, Turkish, Ukrainian, Vietnamese		English	English, Arabic,Polish, Korean, Italian, German, French, Chinese, Turkish, Spanish, Spanish, Russian, Romanian, Portuguese, Dutch, Hungarian, Vietnamese, Czech, Japan, Kazakh	English, French, Dutch, Portuguese, Czech, Danish, German, Spanish, Italian, Norwegian, Polish, Russian, Finnish, Swedish, Turkish, Chinese, Japanese, Korean, Arabic, Hebrew	English, German, French, Japanese, Italian, Chinese, Spanish, Portuguese, Korean	English	English	English, Japanese	English, Spanish, French, German, Japanese
Which languages are the manuals available in?	English, Czech						English, Arabic, Bulgarian, Chinese, Croatian, Czech, Dutch, Estonian, Finnish, French, German, Greek, Hungarian, Italian, Japanese, Kazakh, Korean, Lithnuanian, Norwenian, Polish, Portuguese, Romanian, Russian, Spanish, Swedish, Slovak, Slovenian, Thai, Turkish, Ukrainian				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					

Copyright and Disclaimer

This publication is Copyright © 2023 by AV-Comparatives®. Any use of the results, etc. in whole or in part, is ONLY permitted after the explicit written agreement of the management board of AV-Comparatives prior to any publication. AV-Comparatives and its testers cannot be held liable for any damage or loss, which might occur as result of, or in connection with, the use of the information provided in this paper. We take every possible care to ensure the correctness of the basic data, but a liability for the correctness of the test results cannot be taken by any representative of AV-Comparatives. We do not give any guarantee of the correctness, completeness, or suitability for a specific purpose of any of the information/content provided at any given time. No one else involved in creating, producing or delivering test results shall be liable for any indirect, special or consequential damage, or loss of profits, arising out of, or related to, the use or inability to use, the services provided by the website, test documents or any related data.

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

AV-Comparatives
(December 2023)