Independent Tests of
Anti-Virus Software

Factsheet Business Test

TEST PERIOD: MARCH – APRIL 2023

LAST REVISION: 14TH MAY 2023

WWW.AV-COMPARATIVES.ORG

Introduction

This is a short fact sheet for our Business Main-Test Series[1], containing the results of the Business Malware Protection Test (March) and Business Real-World Protection Test (March-April). The full report, including the Performance Test and product reviews, will be released in July.

To be certified in July 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.

Tested Products

The following products[2] were tested under Windows 10 64-bit and are included in this factsheet:

Vendor	Product	Version March	Version April
Avast	Ultimate Business Security	23.1	23.2
Bitdefender	GravityZone Business Security Premium	7.8	7.8
Cisco	Secure Endpoint Essentials	8.1	8.1
CrowdStrike	Falcon Pro	6.52	6.53
Cybereason	NGAV	22.1	22.1
Elastic	Security	8.6	8.6
ESET	PROTECT Entry with ESET PROTECT Cloud	10.0	10.0
G Data	Endpoint Protection Business	15.4	15.5
K7	On-Premises Enterprise Security Advanced	14.2	14.2
Kaspersky	Endpoint Security for Business – Select, with KSC	12.0	12.0
Microsoft	Defender Antivirus with Microsoft Endpoint Manager	4.18	4.18
Sophos	Intercept X Advanced	2022.1	2022.4
Trellix	Endpoint Security (ENS)[3]	10.7	10.7
VIPRE	Endpoint Detection and Response	13.0	13.0
VMware	Carbon Black Cloud Endpoint Standard	3.9	3.9
WatchGuard	Endpoint Protection Plus on Aether	8.0	8.0

[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] 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). **VMware** uses the **Avira** engine (in addition to their own protection features). **G Data**'s OutbreakShield is based on **Cyren**.
[3] 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.

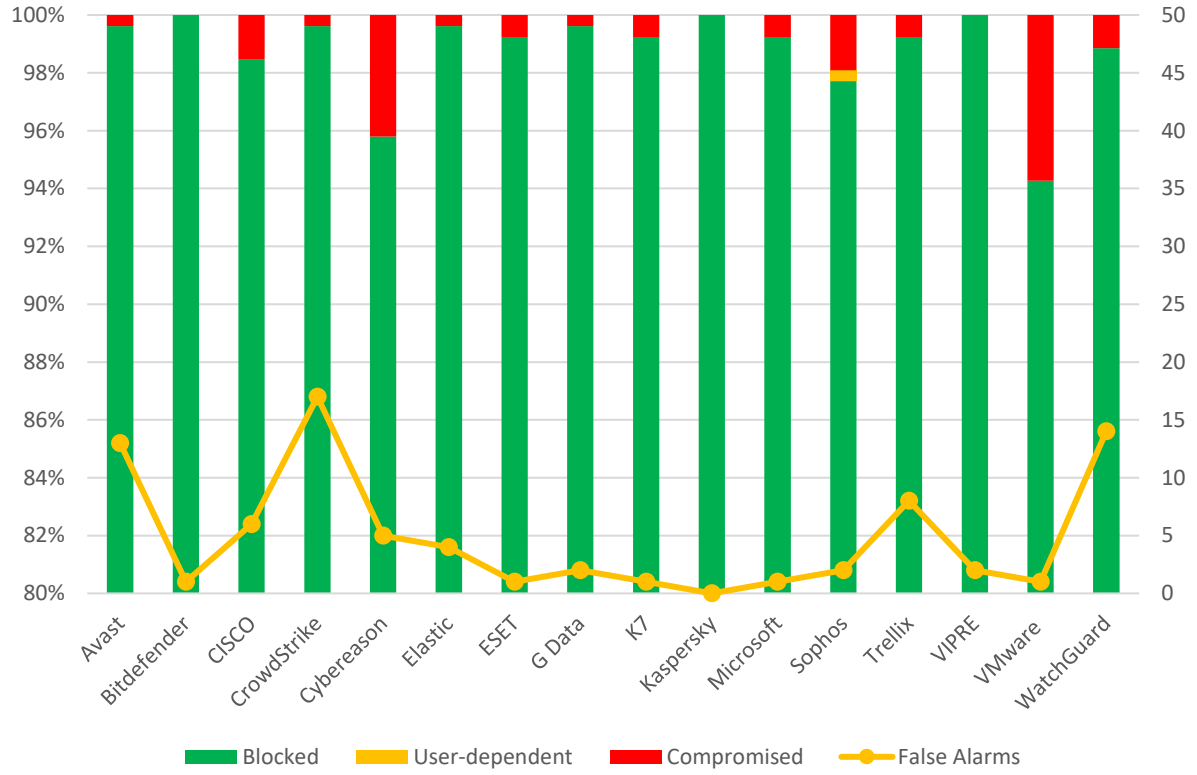
VMware: policy set to “Advanced”.

Avast, K7, WatchGuard: default settings.

Results

Real-World Protection Test (March-April)

This fact sheet gives a brief overview of the results of the Business Real-World Protection Test run in March and April 2023. The overall business product reports (each covering four months) will be released in July and December. For more information about this Real-World Protection Test, please read the details available at https://www.av-comparatives.org. The results are based on a test set consisting of **262** test cases (such as malicious URLs), tested from the beginning of March till the end of April.



	Blocked	User dependent	Compromised	PROTECTION RATE[4]	False Alarms
Kaspersky	262	-	-	100%	0
Bitdefender	262	-	-	100%	1
VIPRE	262	-	-	100%	2
G Data	261	-	1	99.6%	2
Elastic	261	-	1	99.6%	4
Avast	261	-	1	99.6%	13
CrowdStrike	261	-	1	99.6%	18
ESET, K7, Microsoft	260	-	2	99.2%	1
Trellix	260	-	2	99.2%	8
WatchGuard	259	-	3	98.9%	14
CISCO	258	-	4	98.5%	6
Sophos	256	1	5	97.9%	2
Cybereason	251	-	11	95.8%	5
VMware	247	-	15	94.3%	1

[4] 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.

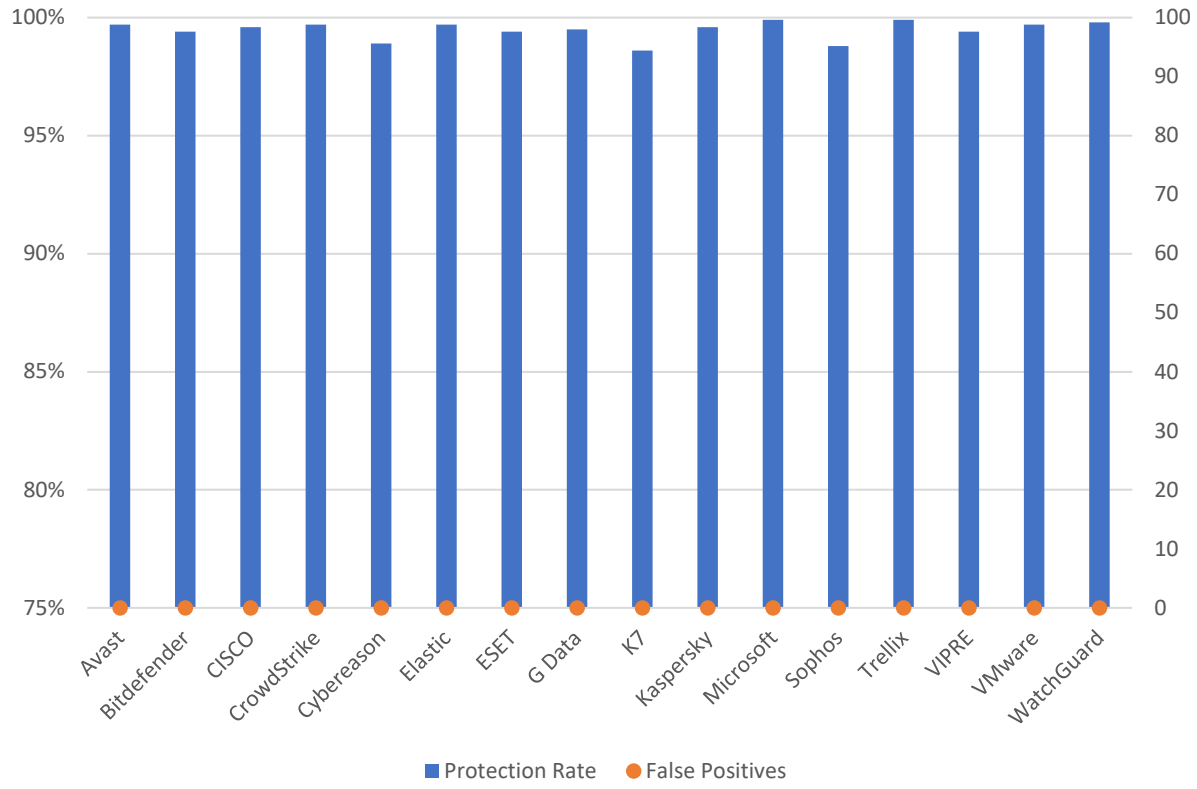
Malware Protection Test (March)

The Malware Protection Test assesses a security program's ability to protect a system against infection by malicious files before, during or after execution. The methodology used for each product tested is as follows. Prior to execution, all the test samples are subjected to on-access scans (if this feature is available) by the security program (e.g. while copying the files over the network). Any samples that have not been detected by the on-access scanner are then executed on the test system, with Internet/cloud access available, to allow e.g. behavioural detection features to come into play. If a product does not prevent or reverse all the changes made by a particular malware sample within a given time period, that test case is considered to be a miss. For this test, **1,011** 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
Microsoft, Trellix	99.9%	0
WatchGuard	99.8%	0
Avast, CrowdStrike, Elastic, VMware	99.7%	0
Cisco, Kaspersky	99.6%	0
G Data	99.5%	0
Bitdefender, ESET, VIPRE	99.4%	0
Cybereason	98.9%	0
Sophos	98.8%	0
K7	98.6%	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
Bitdefender, ESET, G Data, Kaspersky, Trellix, VIPRE, VMware	Very Low
-	Low
Avast, Microsoft	Medium/Average
K7	High
Cisco, CrowdStrike, Sophos, WatchGuard	Very High
Cybereason, Elastic	Remarkably High

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

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
(May 2023)