Independent Tests of
Anti-Virus Software

Factsheet Business Test

TEST PERIOD: AUGUST – SEPTEMBER 2020
LANGUAGE: ENGLISH
LAST REVISION: 12TH OCTOBER 2020

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 (September) and Business Real-World Protection Test (August-September). The full report, including the Performance Test and product reviews, will be released in December. To be certified in December as an "Approved Business Product" by AV-Comparatives, the tested products must score at least 90% in the Malware Protection Test, and at least 90% in the overall Real-World Protection Test (i.e. over the course of 4 months), with zero false alarms on common business software. Tested products must also avoid major performance issues and have fixed all reported bugs in order to gain certification.

Tested Products

The following products[2] were tested under Windows 10 1909 64-bit and are included in this factsheet:

Vendor	Product	Version August	Version September
Acronis	Cyber Protect – Advanced Edition	12.5	12.5
Avast	Business Antivirus Pro Plus	20.5	20.6
Bitdefender	GravityZone Elite Security	6.6	6.6
Cisco	AMP for Endpoints - Advantage	7.2	7.2
CrowdStrike	Falcon Pro	5.36	5.40
Cybereason	Cybereason	20.1	20.1
Elastic	Endpoint Security	3.53	3.53
ESET	Endpoint Protection Advanced Cloud & Cloud Administrator	7.2	7.2
FireEye	Endpoint Security	32.30	32.30
Fortinet	FortiClient with EMS, FortiSandbox & FortiEDR	6.4	6.4
G DATA	AntiVirus Business	14.3	14.3
K7	Enterprise Security	14.2	14.2
Kaspersky	Endpoint Security for Business Select	11.4	11.4
Microsoft	Defender ATP's Antivirus	4.18	4.18
Panda	Endpoint Protection Plus on Aether	8.0	8.0
Sophos	Intercept X Advanced	10.8	10.8
SparkCognition	DeepArmor Endpoint Protection Platform	3.3	3.3
Vipre	Endpoint Security Cloud	12.0	12.0
VMware	Carbon Black Cloud	3.5	3.5

[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: **Acronis**, **Cisco**, **Cybereason**, **FireEye, 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**.

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. Cloud and PUA[3] detection have been activated in all products.

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" and "Scan SSL" enabled; "HyperDetect", "Device Sensor" and "EDR Sensor" disabled.

Cisco: everything enabled and set to Block.

CrowdStrike: everything enabled and set to maximum, i.e. "Extra Aggressive". "Unknown Detection-Related Executables" and "Unknown Executables" disabled.

Cybereason: "Anti-Malware" enabled; "Signatures mode" set to "Disinfect"; "Behavioral document protection" enabled; "Artificial intelligence" set to "Aggressive"; "Exploit protection", "PowerShell and .NET", "Anti-Ransomware" and "App Control" enabled and set to "Prevent"; all "Collection features" enabled; "Scan archives on access" enabled.

Elastic: "Malware" and "Process Injection" protections enabled; "Blacklist", "Credential Access", "Exploit" and "Ransomware" protections, as well as all "Adversary Behaviors" disabled.

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

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

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

Fortinet: All “AntiVirus Protection” settings enabled and set to “Block”. Additionally, “Anti-Exploit”, “Cloud Based Malware Detection”, “Advanced Heuristic”, “FortiGuard Analytics”, FortiSandbox’s “Sandbox Detection”, “Web Filter”, “Application Firewall”, “Detect and Block Exploits & Botnets” and “FortiEDR” were all enabled; “Exclude Files from Trusted Sources” for “Sandbox Detection” enabled.

G DATA: “Exploit Protection”, “Anti-Ransomware” and “BankGuard” enabled; “BEAST Behavior Monitoring” set to “Pause Program and Quarantine”.

Kaspersky: “Adaptive Anomaly Control” disabled.

Microsoft: Cloud protection level set to "High", Cloud-delivered protection set to "Advanced". Google Chrome extension “Windows Defender Browser Protection” installed and enabled.

Sophos: All options in “Active Adversary Mitigations” enabled. “Web Control” and “Protect against data loss” disabled.

SparkCognition: all “Policy Settings” and all “Attack Vectors” settings enabled and set to “Aggressive”.

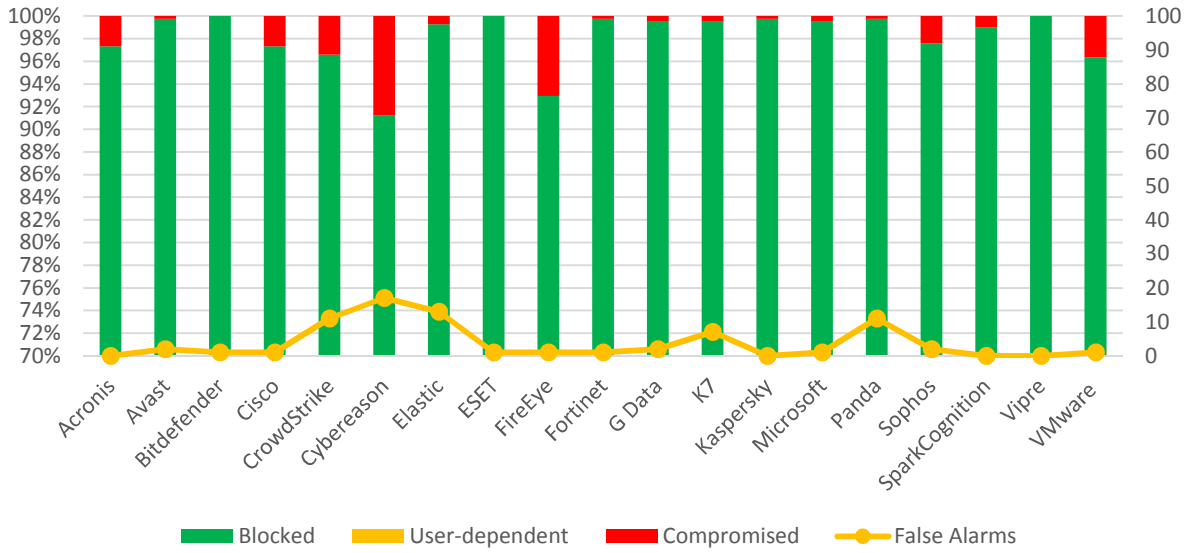
VMware: policy set to “Advanced”.

Acronis, Avast, K7, Panda, Vipre: default settings.

Results

Real-World Protection Test (August-September)

This fact sheet gives a brief overview of the results of the Business Real-World Protection Test run in August and September 2020. 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 **411** test cases (such as malicious URLs), tested from the beginning of August till the end of September.



	Blocked	User dependent	Compromised	PROTECTION RATE[4]	False Alarms
Vipre	411	-	-	100%	0
Bitdefender, ESET	411	-	-	100%	1
Kaspersky	410	-	1	99.8%	0
Fortinet	410	-	1	99.8%	1
Avast	410	-	1	99.8%	2
Panda	410	-	1	99.8%	11
Microsoft	409	-	2	99.5%	1
G Data	409	-	2	99.5%	2
K7	409	-	2	99.5%	7
Elastic	408	-	3	99.3%	13
SparkCognition	407	-	4	99.0%	0
Sophos	401	-	10	97.6%	2
Acronis	400	-	11	97.3%	0
Cisco	400	-	11	97.3%	1
CrowdStrike	397	-	14	96.6%	11
VMware	396	-	15	96.4%	1
FireEye	382	-	29	92.9%	1
Cybereason[5]	375	-	36	91.2%	17

[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.
[5] A Cybereason product issue was uncovered during the Real-World Protection Test which led to some missed detections. The bug has now been fixed.

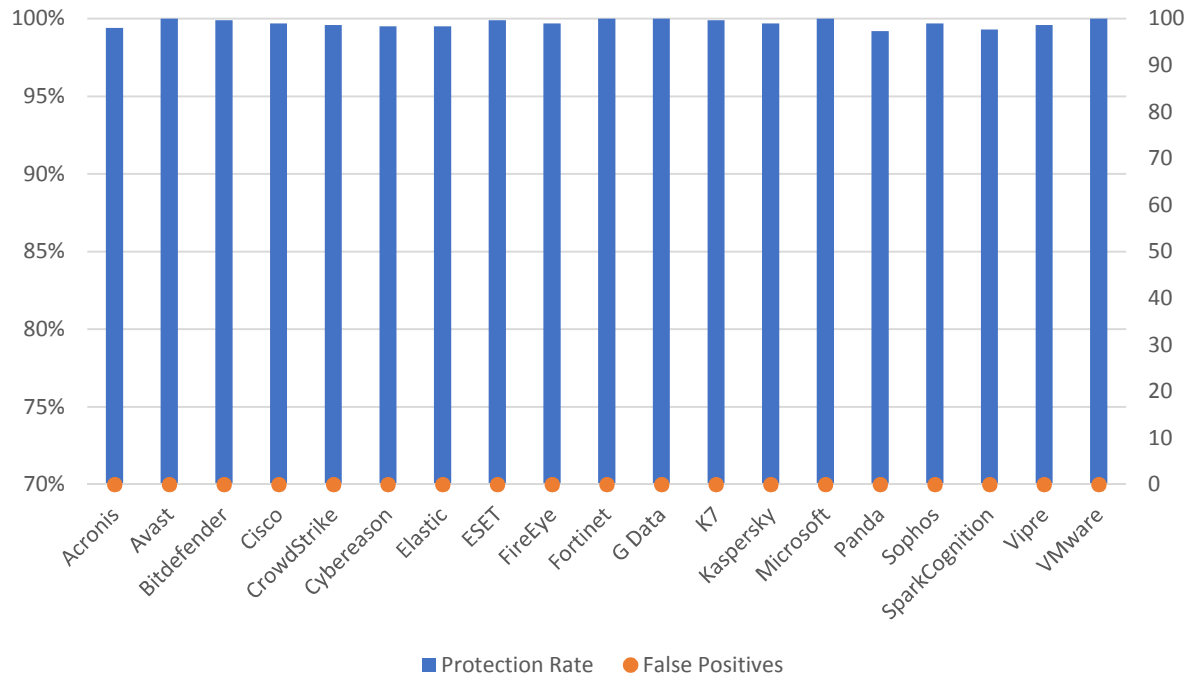
Malware Protection Test (September)

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. behavioral 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, **1,063** 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
Avast, Fortinet, G Data, Microsoft, VMware	100%	0
Bitdefender, ESET, K7	99.9%	0
Cisco, FireEye, Kaspersky, Sophos	99.7%	0
CrowdStrike, Vipre	99.6%	0
Cybereason, Elastic	99.5%	0
Acronis	99.4%	0
SparkCognition	99.3%	0
Panda	99.2%	0

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

FP rate	Number of FPs on non-business software
Very Low	0-5
Low	6-15
Medium/Average	16-25
High	26-50
Very High	51-100
Remarkably High	>100

	FP rate on non-business software
Acronis, Bitdefender, Cisco, ESET, Kaspersky	Very low
Avast, FireEye, G Data, Sophos, Vipre	Low
Elastic, Microsoft, SparkCognition, VMware	Medium/Average
CrowdStrike, Cybereason, Fortinet	High
K7, Panda	Very high
-	Remarkably high

Copyright and Disclaimer

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

AV-Comparatives
(October 2020)