Independent Tests of
Anti-Virus Software

Factsheet Business Test

TEST PERIOD: AUGUST – SEPTEMBER 2021
LAST REVISION: 11TH OCTOBER 2021

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 2021 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[2] on common business software, and at least 90% in the overall Real-World Protection Test (i.e. over the course of four months), with less than one hundred false alarms on any clean software/websites (and with zero false alarms on common business software). Tested products must also avoid major performance issues (impact score must be below 40) and have fixed all reported bugs in order to gain certification.

Tested Products

The following products[3] were tested under Windows 10 64-bit and are included in this factsheet:

Vendor	Product	Version August	Version September
Acronis	Cyber Protect Cloud with Advanced Security pack	15.0	15.0
Avast	Business Antivirus Pro Plus	21.4	21.6
Bitdefender	GravityZone Elite	7.2	7.2
Cisco	Secure Endpoint Essentials	7.4	7.4
CrowdStrike	Falcon Pro	6.26	6.28
Cybereason	Enterprise	20.2	20.2
Elastic	Security	7.13	7.13
ESET	PROTECT Entry with ESET PROTECT Cloud	8.0	8.0
FireEye	Endpoint Security	33.46	33.46
Fortinet	FortiClient with EMS, FortiSandbox & FortiEDR	6.4	6.4
G Data	Endpoint Protection Business	15.1	15.1
K7	Enterprise Security Advanced	14.2	14.2
Kaspersky	Endpoint Security for Business – Select, with KSC	11.6	11.6
Malwarebytes	EDR	1.2	1.2
Microsoft	Defender Antivirus with Microsoft Endpoint Manager	4.18	4.18
Panda	Endpoint Protection Plus on Aether	8.0	8.0
Sophos	Intercept X Advanced	10.8	10.8
VIPRE	Endpoint Cloud	12.0	12.0
VMware	Carbon Black Cloud Endpoint Standard	3.7	3.7

[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] Starting from 2022, products will be required to have an FP rate on non-business files below the *Remarkably High* threshold.

[3] 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.

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):

Acronis: "Backup", "Vulnerability assessment", "Patch management" and "Data protection map" disabled.

Bitdefender: "Fileless Attack Protection", "Sandbox Analyzer" (for Applications and Documents) and "Scan SSL" enabled. "Encryption" and "Patch Management" add-ons registered and enabled. "HyperDetect" and "Device Sensor" disabled. "Update ring" changed to "Fast ring". "Web Traffic Scan" enabled for HTTP Web traffic and Incoming POP3 emails.

Cisco: "On Execute File and Process Scan" set to Active; "Exploit Prevention: Script Control" and "TETRA Deep Scan File" enabled; "Event Tracing for Windows" enabled.

CrowdStrike: everything enabled and set to maximum, i.e. "Extra Aggressive". "Sensor Visibility" for "Firmware" disabled. Uploading of "Unknown Detection-Related Executables" and "Unknown Executables" disabled.

Cybereason: "Anti-Malware" enabled; "Signatures mode" set to "Disinfect"; "Behavioral document protection" enabled; "Artificial intelligence" and "Anti-Exploit" 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: MalwareScore ("windows.advanced.malware.threshold") set to "aggressive".

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

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

Fortinet: "Sandbox analysis" (FortiSandbox) and FortiEDR enabled. “Submit files from USB Sources” disabled; “Exclude Files from Trusted Sources” for “Sandbox Detection” enabled; in “Execution Prevention”, “Suspicious Script Execution” was disabled and “Unconfirmed File Detected” was enabled; eXtended Detection (XDR) was disabled.

G Data: “BEAST Behavior Monitoring” set to “Halt program and move to quarantine”. “G DATA WebProtection” add-on for Google Chrome installed and activated.

Malwarebytes: “Expert System Algorithms”, “Block penetration testing attacks”, "Disable IE VB Scripting", "Java Malicious Inbound/outbound Shell Protection", "Earlier RTP blocking", "Enhanced sandbox protection" and "Thorough scan" enabled; “RET ROP Gadget detection” and "Malicious LoadLibrary Protection" enabled for all applications; "Protection for MessageBox Payload" enabled for MS Office; “Malwarebytes Browser Guard” Chrome extension enabled.

Microsoft: Google Chrome extension “Windows Defender Browser Protection” installed and enabled.

Sophos: “Threat Case creation” and “Web Control” disabled.

VIPRE: “DNS Traffic Filtering” and “Malicious URL Blocking for HTTPS Traffic” enabled. “Firewall” and “IDS” enabled and set to “Block With Notify”.

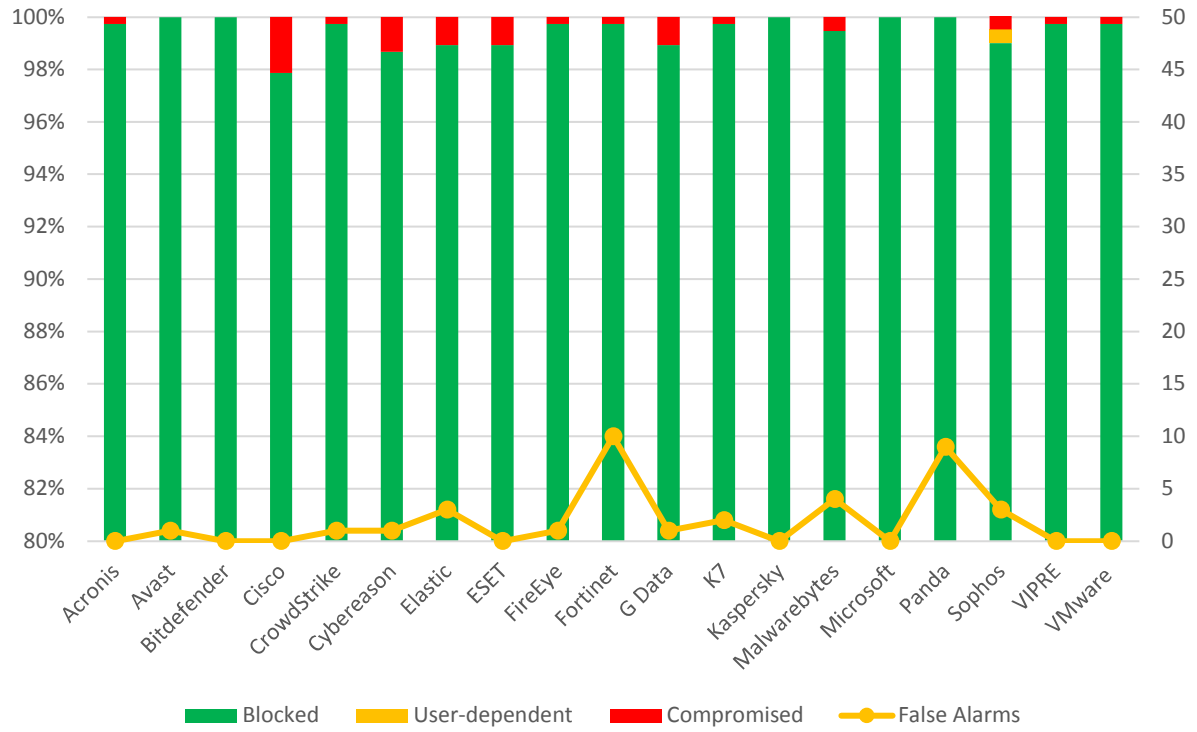
VMware: policy set to “Advanced”.

Avast, K7, Kaspersky, Panda: 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 2021. 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 **375** 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
Bitdefender, Kaspersky, Microsoft	375	-	-	100%	0
Avast	375	-	-	100%	1
Panda	375	-	-	100%	9
Acronis, VIPRE, VMware	374	-	1	99.7%	0
CrowdStrike, FireEye	374	-	1	99.7%	1
K7	374	-	1	99.7%	2
Fortinet	374	-	1	99.7%	10
Malwarebytes	373	-	2	99.5%	4
Sophos	371	2	2	99.2%	3
ESET	371	-	4	98.9%	0
G Data	371	-	4	98.9%	1
Elastic	371	-	4	98.9%	3
Cybereason	370	-	5	98.7%	1
Cisco	367	-	8	97.9%	0

[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.

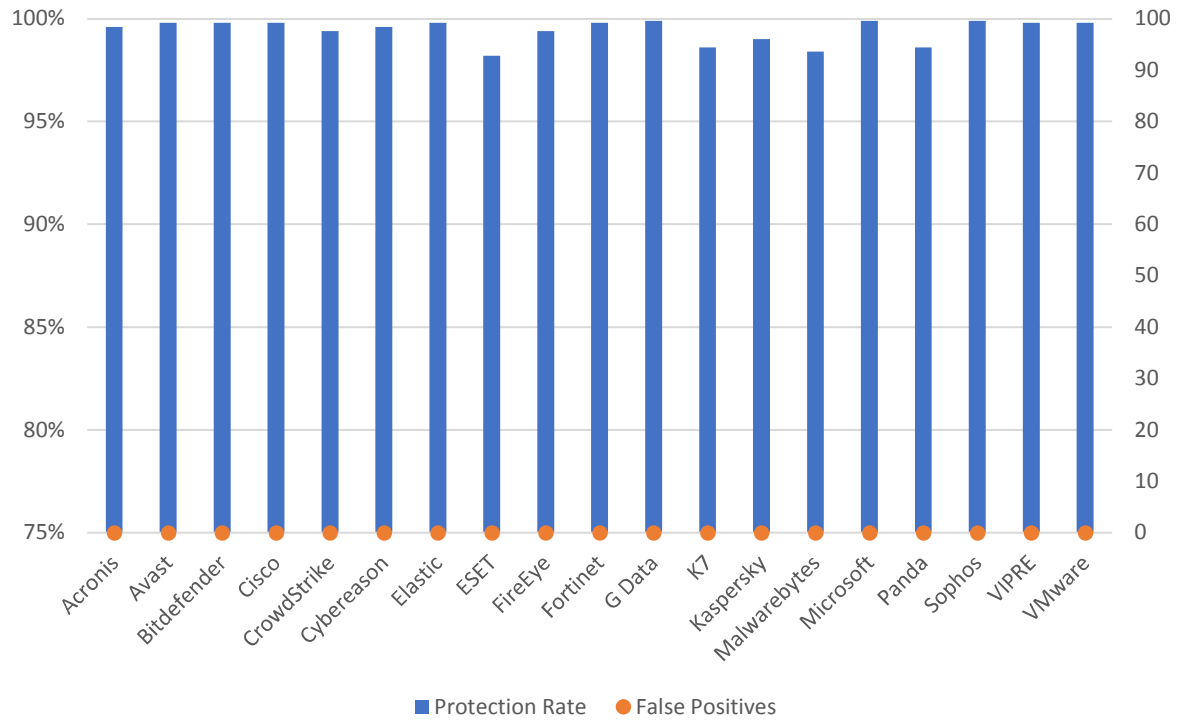
Malware Protection Test (September)

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, **1,016** 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
G Data, Microsoft, Sophos	99.9%	0
Avast, Bitdefender, Cisco, Elastic, Fortinet, VIPRE, VMware	99.8%	0
Acronis, Cybereason	99.6%	0
CrowdStrike, FireEye	99.4%	0
Kaspersky	99.0%	0
K7, Panda	98.6%	0
Malwarebytes	98.4%	0
ESET	98.2%	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, and the results currently do not affect the overall test score or the Approved Business Product award. The false alarms found were promptly fixed by the respective vendors. Organisations which often use uncommon or non-business software, or their own self-developed software, might like to consider these results, however.

FP rate	Number of FPs on non-business software
Very Low	0-5
Low	6-15
Medium/Average	16-35
High	36-80
Very High	81-125
Remarkably High	>125

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

It should be noted that Cybereason and Fortinet had *Remarkably High* levels of false positives on non-business software. Administrators should consider whether this might create problems in their organisation's specific environments. Starting from 2022, products will be 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 excessively restrictive settings that can cause very high levels of false positives.

Copyright and Disclaimer

This publication is Copyright © 2021 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
(October 2021)