Independent Tests of
Anti-Virus Software

Factsheet Business Test

TEST PERIOD: AUGUST – SEPTEMBER 2019
LANGUAGE: ENGLISH
LAST REVISION: 14TH OCTOBER 2019

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 1903 64-bit and are included in this factsheet:

Vendor	Product	Version August	Version September
Avast	Business Antivirus Pro Plus	19.6	19.6
Bitdefender	GravityZone Elite Security	6.6	6.6
Cisco	AMP for Endpoints	6.3	6.3
CrowdStrike	Endpoint Protection Platform Standard Bundle	5.14	5.16
Endgame	Endpoint Protection Platform[3]	3.50	3.51
ESET	Endpoint Protection Advanced Cloud & Cloud Administrator	7.0	7.0
FireEye	Endpoint Security	30.19	30.19
Fortinet	FortiClient with EMS & FortiSandbox	6.0	6.0
K7	Enterprise Security	14.2	14.2
Kaspersky	Endpoint Security for Business Select	11.1	11.1
McAfee	Endpoint Security with ATP and ePO Cloud	10.6	10.6
Microsoft	Defender ATP's Antivirus	4.18	4.18
Panda	Endpoint Protection Plus on Aether	8.0	8.0
Seqrite	Endpoint Security	17.0	17.0
Sophos	Intercept X Advanced	10.8	10.8
SparkCognition	DeepArmor Endpoint Protection Platform	2.1	2.1
Symantec	Endpoint Protection	14.2	14.2
Trend Micro	OfficeScan XG	12.0	12.0
VIPRE	Endpoint Security Cloud	11.0	11.0

[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**, **FireEye**, **Seqrite** and **VIPRE** use the **Bitdefender** engine (in addition to their own protection features).
[3] Endgame was acquired by Elastic N.V. on Oct 8, 2019. The product is now called Elastic Endpoint Security.

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. About half of the vendors provide their products with optimal default settings which are ready to use, and did therefore not change any settings. Cloud and PUA[4] detection have been activated in all products. Below we have listed relevant deviations from default settings (i.e. setting changes applied by the vendors):

Bitdefender: "HyperDetect", "Device Sensor" and "EDR Sensor" disabled.

Cisco: everything enabled.

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

Endgame[5]: Enabled Software and Hardware protection options: all enabled; Protected Applications: "Browser", "Microsoft Suite" (incl. Fltdr.exe and EQNEDT32.exe), "Java" and "Adobe". Malware (on-execution and on-write): "On – Prevent mode"; Process Injection: "On – Prevent mode"; Options: all enabled; "Aggressive" threshold. Adversary behaviors: all enabled; Credential dumping: enabled; Ransomware: disabled.

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

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

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

Microsoft: Cloud protection level set to "High".

Sophos: "Web Control" and "Protect against data loss" disabled.

SparkCognition: all "Policy Settings" and all "Attack Vectors" settings enabled.

Trend Micro: Behaviour monitoring: "Monitor new encountered programs downloaded through web" enabled; "Certified Safe Software Service for Behaviour monitoring" enabled; "Smart Protection Service Proxy" enabled; "Use HTTPS for scan queries" enabled; Web Reputation Security Level set to Medium; "Send queries to Smart Protection Servers" disabled; "Block pages containing malicious script" enabled; Real-Time Scan set to scan "All scannable files", "Scan compressed files to Maximum layers 6"; "CVE exploit scanning for downloaded files" enabled; "ActiveAction for probable virus/malware" set to Quarantine; Cleanup type set to "Advanced cleanup" and "Run cleanup when probable virus/malware is detected" enabled; "Block processes commonly associated with ransomware" enabled; "Anti-Exploit Protection" enabled; all "Suspicious Connection Settings" enabled and set to Block.

Avast, ESET, K7, Kaspersky, Panda, Seqrite, Symantec, VIPRE: default settings.

---

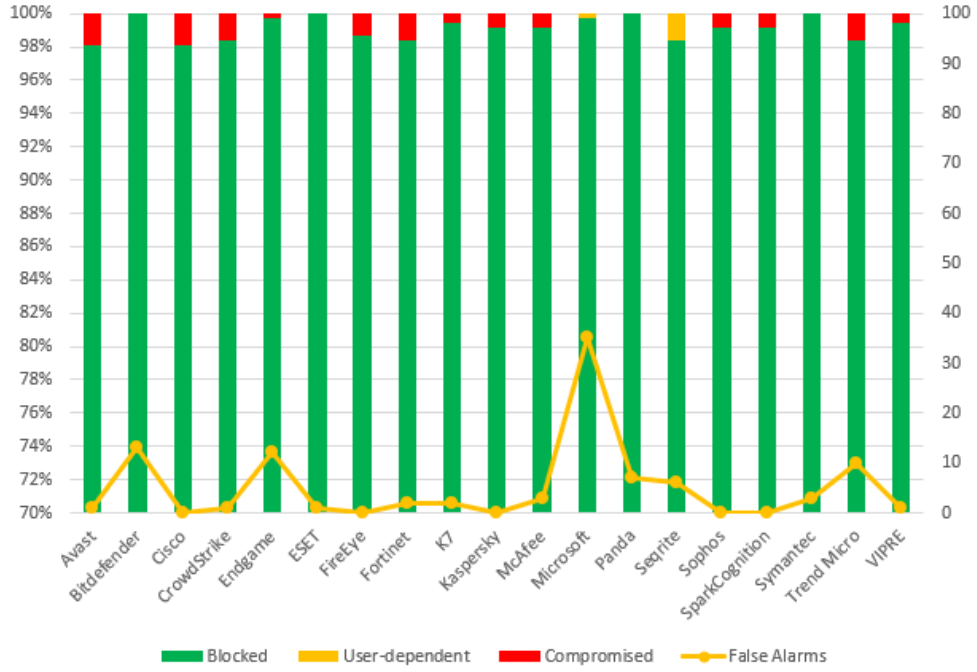
[4] We currently do not include any PUA in our malware tests.

[5] Settings were renamed in the newer version.

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 2019. 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 **371** test cases (such as malicious URLs), tested from the beginning of August till the end of September.



	Blocked	User dependent	Compromised	PROTECTION RATE [Blocked % + (User dependent %)/2] [6]	False Alarms
ESET	371	-	-	**100%**	1
Symantec	371	-	-	**100%**	3
Panda	371	-	-	**100%**	7
Bitdefender	371	-	-	**100%**	13
Microsoft	370	1	-	**99.9%**	35
Endgame	370	-	1	**99.7%**	12
VIPRE	369	-	2	**99.5%**	1
K7	369	-	2	**99.5%**	2
Kaspersky, Sophos, SparkCognition	368	-	3	**99.2%**	0
McAfee	368	-	3	**99.2%**	3
Seqrite	365	6	-	**99.2%**	6
FireEye	366	-	5	**98.7%**	0
CrowdStrike	365	-	6	**98.4%**	1
Fortinet	365	-	6	**98.4%**	2
Trend Micro	365	-	6	**98.4%**	10
Cisco	364	-	7	**98.1%**	0
Avast	364	-	7	**98.1%**	1

[6] 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.

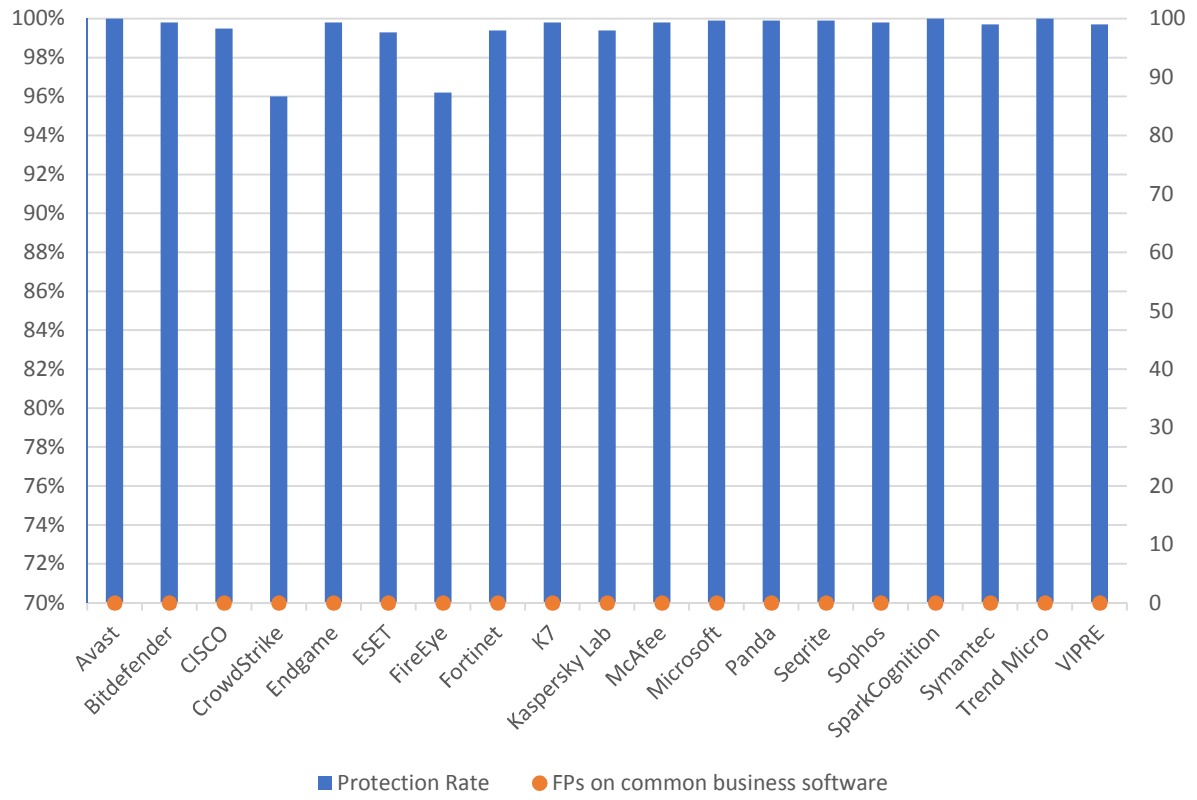
Malware Protection Test (September)

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, **1,278** recent malware samples were used.

False positive (false alarm) test with common business software

A false alarm test done with common business software was also performed. As expected, all the tested products hat ***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, SparkCognition, Trend Micro	100%	0
Microsoft, Panda, Seqrite	99.9%	0
Bitdefender, Endgame, K7, McAfee, Sophos	99.8%	0
Symantec, VIPRE	99.7%	0
Cisco	99.5%	0
Fortinet, Kaspersky	99.4%	0
ESET	99.3%	0
FireEye[7]	96.2%	0
CrowdStrike	96.0%	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	6-25
Medium	26-50
High	51-100
Very High	101-200
Remarkably High	>200

	FP rate on non-business software
Avast, Bitdefender, Cisco, ESET, Fortinet, K7, Kaspersky, Seqrite, Symantec	Very low
CrowdStrike, FireEye, McAfee, Microsoft, Panda, Sophos	Low
Endgame, Trend Micro, VIPRE	Medium
SparkCognition	High
-	Very high
-	Remarkably high

[7] A FireEye product issue was uncovered during the Malware Protection Test which led to some missed detections. The bug has now been fixed.

Copyright and Disclaimer

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

AV-Comparatives
(October 2019)