Anti-Virus Comparative

Factsheet Business Test

Language: English
March-April 2018

Last revision: 11th May 2018

http://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.

We congratulate the 16 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.

To be certified in July 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 RS3 64-bit:

Vendor	Product	Version March	Version April
Avast	Business Antivirus Pro Plus	18.1	18.2
Bitdefender	Endpoint Security Elite	6.2	6.2
CrowdStrike	Falcon Prevent	4.0	4.0
Emsisoft	Anti-Malware	2018.2	2018.3
Endgame	Endpoint Security	2.5	2.5
eScan	Corporate 360	14.0	14.0
ESET	Endpoint Security	6.6	6.6
FireEye	HX Endpoint Threat Protection Platform	4.0	4.0
Fortinet	FortiClient with FortiGate & FortiSandbox	5.6	5.6
Kaspersky Lab	Endpoint Security	10.3	10.3
McAfee	Endpoint Security with Adaptive Threat Protection	10.5	10.5
Microsoft	Windows Defender for Enterprise	4.12	4.12
Panda	Endpoint Protection Plus	7.90	7.90
Saint Security	MAX Antivirus	1.0	1.0
Trend Micro	OfficeScan XG	12.0	12.0
VIPRE	Endpoint Security	10.1	10.1

[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: **Emsisoft**, **eScan**, **FireEye** and **VIPRE** use the **Bitdefender** engine.

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 allowed 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 detection have been activated in all products.

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

Bitdefender: HyperDetect disabled, Sandbox enabled.

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

Endgame: Enabled Software and Hardware protection options: "Critical API Filtering", "Header Protection", "Malicious Macros", "Stack Memory", "Stack Pivot" and "UNC Path"; Protected Applications: "Browser", "Microsoft Suite", "Java" and "Adobe". Exploit Protection: "On – Prevent mode"; Malicious File Configuration: "On" – Protection at File Execution "On"; Options: "Prevent", "Process execution and loaded modules", Malware Detection for created and modified files "On"; "Aggressive" threshold.

FireEye: "Real-Time Indicator Detection" enabled; "Exploit Guard" enabled; "Malware Protection" enabled.

Fortinet: Real-Time protection, FortiProxy, FortiSandbox, Webfilter and Firewall enabled.

McAfee: "Email attachment scanning" enabled; "Real Protect" enabled and set to "high" sensitivity.

Microsoft: Cloud protection level set to "High blocking level.

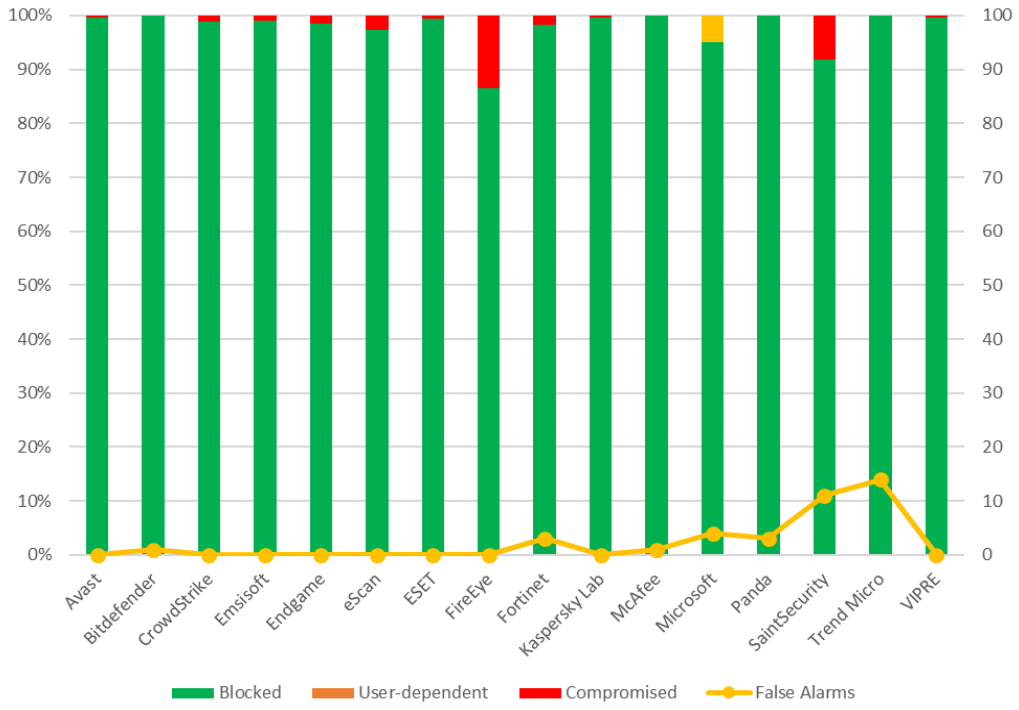
Trend Micro: Behaviour monitoring: "Monitor news encountered programs downloaded through web" enabled; "Certified Safe Software Service for Behaviour monitoring" enabled; "Smart Protection Service Proxy" enabled; "Use HTTPS for scan queries" enabled; Web Reputation Security Level set to Medium; "Send 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, **Emsisoft**, **eScan**, **ESET**, **Kaspersky Lab**, **Panda**, **Saint Security**, **VIPRE**: default settings.

Results

Real-World Protection Test (March-April)

This fact sheet[3] gives a brief overview of the results of the Business Real-World Protection Test run in March and April 2018. 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 http://www.av-comparatives.org. The results are based on a test set consisting of **620** test cases (such as malicious URLs), tested from the beginning of March till the end of April.



	Blocked	User dependent	Compromised	PROTECTION RATE [Blocked % + (User dependent %)/2][4]	False Alarms
Bitdefender, McAfee	620	-	-	**100%**	1
Panda	620	-	-	**100%**	3
Trend Micro	620	-	-	**100%**	14
Avast, Kaspersky Lab, VIPRE	618	-	2	**99.7%**	0
ESET	616	-	4	**99.4%**	0
Emsisoft	614	-	6	**99.0%**	0
CrowdStrike	613	-	7	**98.9%**	0
Endgame	610	-	10	**98.4%**	0
Fortinet	609	-	11	**98.2%**	3
Microsoft	589	31	-	**97.5%**	4
eScan	603	-	17	**97.3%**	0
Saint Security	569	-	51	**91.8%**	11
FireEye	536	-	84	**86.5%**	0

[3] The full report will be released in July.

[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.

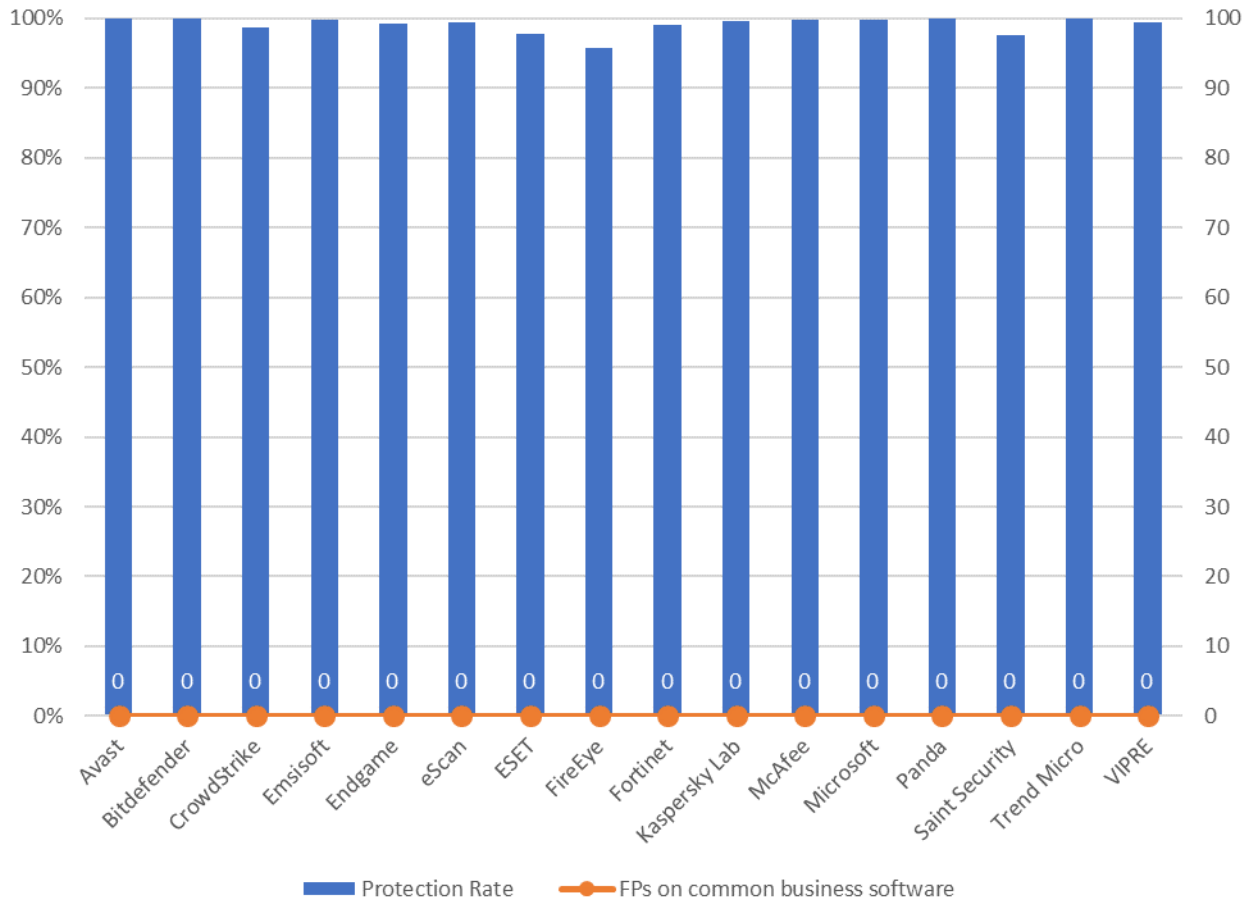
Malware Protection Test

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 or from a USB device, or saving from webmail). 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, **1,470** 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 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, Bitdefender, Panda, Trend Micro	100%	0
Microsoft	99.9%	0
Emsisoft, McAfee, Kaspersky Lab	99.7%	0
eScan, VIPRE	99.5%	0
Endgame	99.3%	0
Fortinet	99.0%	0
CrowdStrike	98.8%	0
ESET	97.8%	0
Saint Security	97.6%	0
FireEye	95.9%	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 - 10
Low	11 – 50
High	51 – 100
Very high	101 - 500
Remarkably high	> 500

	FP rate on non-business software
Avast, Bitdefender, Emsisoft, eScan, ESET, FireEye, Fortinet, Kaspersky Lab, McAfee, VIPRE	Very low
Saint Security	Low
Endgame, Microsoft	High
CrowdStrike, Panda, Trend Micro	Very high
-	Remarkably high

Copyright and Disclaimer

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

AV-Comparatives (May 2018)