Independent Tests of
Cybersecurity Solutions

Factsheet Business Test

TEST PERIOD: AUGUST – SEPTEMBER 2026

LAST REVISION: 12TH OCTOBER 2026

WWW.AV-COMPARATIVES.ORG

Contents

INTRODUCTION	3
TESTED PRODUCTS	3
SETTINGS	4
TEST RESULTS	6
COPYRIGHT AND DISCLAIMER	9

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 2026 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 11 64-bit and are included in this factsheet:

Vendor	Product	Version August	Version September
Avast	Ultimate Business Security	26.6	26.6
Bitdefender	GravityZone Business Security Premium	8.26	8.26
Cisco	Secure Client	8.6	8.6
CrowdStrike	Falcon Enterprise	7.40	8.10
Elastic	Security	9.4	9.5
ESET	PROTECT Entry with ESET PROTECT Cloud	13.0	13.0
G Data	Endpoint Protection Business	15.9	15.9
K7	On-Premises Enterprise Security Advanced	14.2	14.2
Kaspersky	Endpoint Security for Business[3] (Select, with KSC)	14.0	14.0
ManageEngine	Endpoint Central with Malware Protection	11.5	11.5
Microsoft	Defender Antivirus with Microsoft Endpoint Manager	4.18	4.18
Norton	Small Business	26.7	26.8
SenseOn	Platform with EPP	7.0	7.0
Sophos	Intercept X Advanced	2026.2	2026.2
Trellix	Endpoint Security (ENS)[4]	10.7	10.7
VIPRE	Endpoint Security	13.4	13.4

[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**, **G Data**, **SenseOn** and **VIPRE** use the **Bitdefender** engine (in addition to their own protection features). **Norton** uses the **Avast** engine.

[3] The product might also be known as "Kaspersky Next EDR Foundations".

[4] 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):

Avast, Norton: "Patch Management" and "WebControl" features were disabled.

Bitdefender: "Sandbox Analyzer" (for Applications, Documents, Scripts, Archives and Emails) enabled. "Analysis mode" set to "Monitoring". "Scan actions for PUA" was set to "Remediate". "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". Under "Network Protection", in "Additional processes" was activated and the following processes were added: powershell.exe, wscript.exe, cscript.exe, pwsh.exe.

Cisco: In "Secure Client", "Umbrella" was enabled. In "Secure Endpoint", the "On Execute File and Process Scan" set to Active; "Exploit Prevention: Script Control" set to "Block"; "TETRA Deep Scan File" enabled; "Detect expanded threat types" enabled; "Exclusions" set to "Microsoft Windows Default"; Engines "ETHOS" and "SPERO" disabled. "Exploit Prevention" set to "Aggressive". "Submit Files for Malware Analysis" set to "Active". "MaxScanFileSize" increased to 250 MB; "MaxArchiveScanFileSize" increased to 500MB; "Cisco Secure Access" enabled and configured to block the following categories: Malware, Command and Control Callbacks, Phishing Attacks, Potentially Harmful Domains, Newly Seen Domains, Dynamic DNS, DNS Tunneling VPN, Cryptomining.

CrowdStrike: everything enabled and set to maximum, i.e. “Extra Aggressive”. “On Write Script File Visibility” and “Unknown detection-related executable analysis” enabled. “On-demand Scans” and “Unknown executables analysis” disabled. “Early adopter sensor builds” enabled. “Redacted HTTP detection details”, “Enhanced exploitation visibility”, “Enhanced DLL load visibility” and “WSL2 visibility” were enabled”. “Boot configuration database protection”, “Vulnerable driver protection” and “File system containment” were also enabled. All “File Detection and Remediation Playbooks” were enabled in Falcon Fusion.

Elastic: MalwareScore (“windows.advanced.malware.threshold”) set to “aggressive”, and Rollback-SelfHealing (“windows.advanced.alerts.rollback.self_healing.enabled”) enabled. “Credential hardening” enabled.

ESET: Under “Protections” all “Detection responses” were set to “Aggressive”. “Detection of potentially unwanted programs” enabled.

G Data: “BEAST Behavior Monitoring” set to “Halt program and move to quarantine”. “BEAST Automatic Whitelisting” deactivated. “G DATA WebProtection” add-on for Google Chrome installed and activated. “Malware Information Initiative” enabled.

K7: default settings.

Kaspersky: “Adaptive Anomaly Control” disabled; “Detect other software that can be used by criminals to damage your computer or personal data” enabled.

ManageEngine: In the Ransomware Detection Settings, the Detection Policy was set to “Kill Process”, and the Detection Sensitivity was set to “Standard”. In the Next-Gen Antivirus section, the Detection Trigger “Enable On Write and Enable On DLL Load” was enabled, and the Detection Policy was set to “Kill & Quarantine”, also for the “Behavior Detection Engine”.

Microsoft: “CloudExtendedTimeOut” set to 50; “PuaProtection” enabled. “SubmitSamplesConsent” set to “SendAllSamples”. Google Chrome extension “Windows Defender Browser Protection” installed and enabled.

SenseOn: Under “Endpoint Protection”, the “Protection Level” was set to “Respond”. “Real Time Process Protection” was enabled, and the sensitivity set to “Medium”.

Sophos: “Threat Graph creation”, “Event journals”, “Web Control” and “Event logging” disabled.

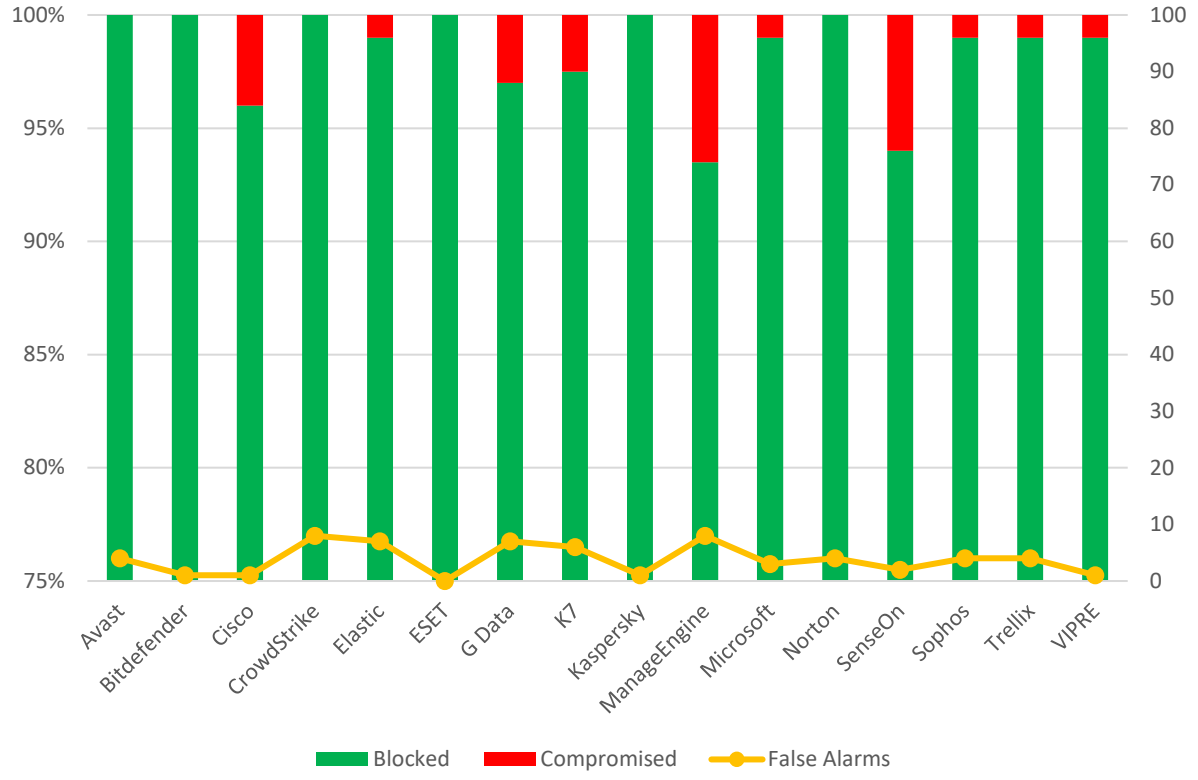
Trellix: “Trellix Endpoint Security Web Control” add-on for Google Chrome enabled. “Access Protection”, “Firewall” and “Exploit Prevention” disabled.

VIPRE: “Incompatible Software Handling” disabled. In "Active Protection", "Disinfect on ATC code buffer detections of intra-process injections" was enabled. "Network Attack Protection" was enabled and set to "Block" for all categories. "Enhanced Detections" and "Inspect Encrypted Domain Controller Traffic" were also enabled. “Firewall” enabled.

Test 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 2026. 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 200 test cases (such as malicious URLs), tested from the beginning of August till the end of September.



Vendor	Blocked	User dependent	Compromised	Protection Rate[5]	False Alarms
ESET	200	-	0	100%	0
Bitdefender, Kaspersky	200	-	0	100%	1
Avast, Norton	200	-	0	100%	4
CrowdStrike	200	-	0	100%	8
VIPRE	198	-	2	99.0%	1
Microsoft	198	-	2	99.0%	3
Sophos, Trellix	198	-	2	99.0%	4
Elastic	198	-	2	99.0%	7
K7	195	-	5	97.5%	6
G Data	194	-	6	97.0%	7
Cisco	192	-	8	96.0%	1
SenseOn	188	-	12	94.0%	2
ManageEngine	187	-	13	93.5%	8

[5] 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.

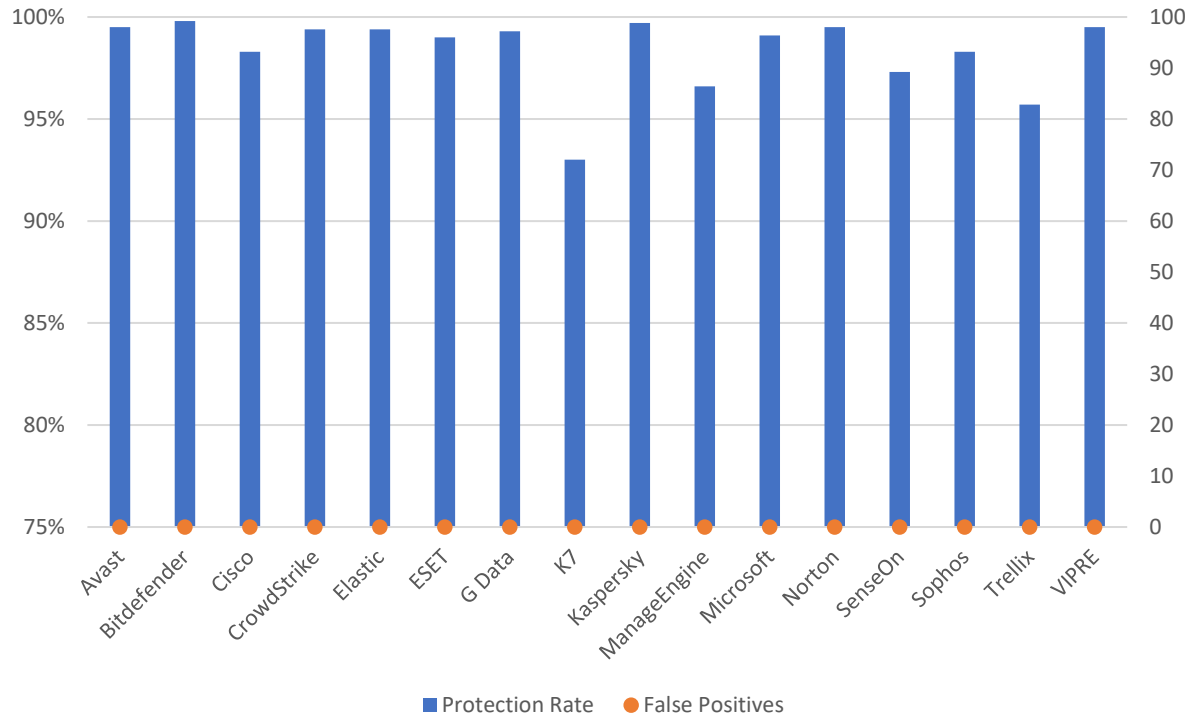
Malware Protection Test (September)

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. All samples are 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, **1,000** 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:



Vendor	Malware Protection Rate	False Alarms on common business software
Bitdefender	99.8%	0
Kaspersky	99.7%	0
Avast, Norton, VIPRE	99.5%	0
CrowdStrike, Elastic	99.4%	0
G Data	99.3%	0
Microsoft	99.1%	0
ESET	99.0%	0
Cisco, Sophos	98.3%	0
SenseOn	97.3%	0
ManageEngine	96.6%	0
Trellix	95.7%	0
K7	93.0%	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

Vendor	FP Rate on Non-Business Files
Bitdefender, ESET, G Data, Kaspersky, VIPRE	Very Low
K7, SenseOn	Low
Avast, Microsoft, Norton	Medium/Average
Cisco, CrowdStrike, Elastic, ManageEngine, Sophos, Trellix	High
-	Very High
-	Remarkably High

Copyright and Disclaimer

This publication is Copyright © 2026 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 2026)