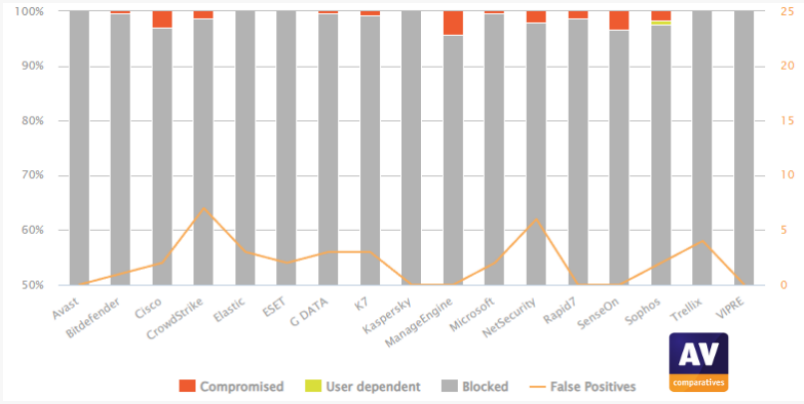
AV-Comparatives Releases Business Security Test Results for August–September 2025

Critical Insights for CISOs: Which Endpoint Security Solutions Can Stop Real Attacks?



AV-Comparatives Real-World Protection Test August-September 2025

INNSBRUCK, TYROL, AUSTRIA, October 17, 2025 /EINPresswire.com/ -- AV-Comparatives, the leading independent authority in cybersecurity testing, has published the results of its latest Business Main-Test Series, covering the Real-World Protection Test (August–September) and the Malware Protection Test (September 2025).

The evaluations provide critical insights into how well endpoint protection platforms defend against real-world threats—ranging from malicious URLs to file-based attacks—within enterprise environments configured to reflect actual deployment scenarios.

> Our enterprise tests deliver independent, real-world insights that help CISOs and security teams choose solutions they can trust to protect their organisations against modern threats."
> *Andreas Clementi, co-founder, AV-Comparatives*

Key Aspects of the Tests:
The Real-World Protection Test evaluated live test cases under Windows 11 64-bit, assessing how effectively each product blocked threats while maintaining usability and low false alarm rates.

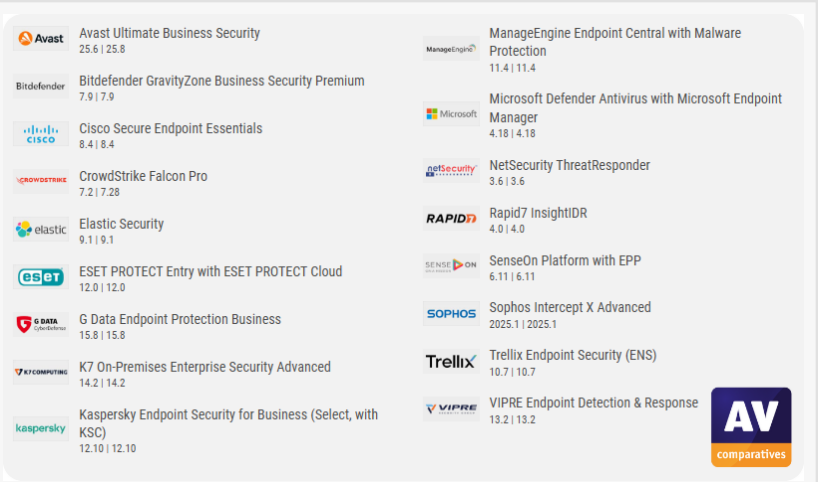
The Malware Protection Test challenged products with a wide range of prevalent malicious files to measure core detection capabilities under cloud-assisted and offline conditions.

All participating vendors were invited to configure their solutions according to best practices, ensuring a fair and realistic assessment across the board.

These results provide valuable guidance for IT security teams and decision-makers seeking

trusted data to inform procurement, policy, and defence strategies in today's rapidly evolving threat landscape.

Full details, charts, and methodologies are available at:
[Business Security Test August–September 2025]



AV-Comparatives Real-World Protection Test August-September 2025

Logo AV-Comparatives

Avast (Ultimate Business Security): Avast demonstrated strong and consistent threat-blocking capabilities across both malware and real-world testing scenarios.
Bitdefender (GravityZone Business Security Premium): Bitdefender showed solid overall performance in preventing threats, with reliable malware detection and minimal operational disruptions.
Cisco (Secure Endpoint Essentials): Cisco Secure Endpoint delivered dependable protection in live attack scenarios and performed efficiently in the malware detection assessment.
CrowdStrike (Falcon Pro): CrowdStrike's platform exhibited stable prevention results with effective handling of common and targeted enterprise threats.
Elastic (Elastic Security): Elastic Security provided full-spectrum protection during the test period, combining proactive detection with operational accuracy.
ESET (PROTECT Entry + PROTECT Cloud): ESET achieved uninterrupted threat prevention across multiple vectors and maintained stability and usability in business environments.
G Data (Endpoint Protection Business): G Data maintained consistent defence across both test areas, offering dependable protection
K7 (On-Premises Enterprise Security Advanced): K7's business solution performed well in real-world scenarios and maintained a straightforward and responsive operational profile.
Kaspersky (Endpoint Security for Business): Kaspersky showed consistent strength in blocking real-world attacks.
ManageEngine (Endpoint Central with Malware Protection): ManageEngine's integrated malware protection added effective detection to its broader IT management features during the test.
Microsoft (Defender Antivirus via Endpoint Manager): Microsoft Defender offered robust, built-in protection for enterprise systems
NetSecurity (ThreatResponder): NetSecurity ThreatResponder handled diverse threats

confidently and provided actionable insights via its enterprise console.
Rapid7 (InsightIDR): Rapid7 delivered competent threat identification and detection.
SenseOn (Platform with EPP): SenseOn responded well to test threats with practical, real-time monitoring.
Sophos (Intercept X Advanced): Sophos combined reliable prevention with intuitive central management.
Trellix (Endpoint Security): Trellix maintained full functionality during testing and effectively blocked a wide range of attacks in business-relevant scenarios.
VIPRE (Endpoint Detection and Response): VIPRE provided dependable protection while keeping user notifications low.

Thomas Uhlemann
AV-Comparatives
+43 512 28778813
email us here
Visit us on social media:
LinkedIn
Facebook
X
