AV-Comparatives Certifies EDR XDR MDR Solutions: Real-World Detection, Proven Performance

The EDR test simulates complex attack scenarios to assess how well a product detects and logs each stage of an intrusion, providing deep insights.

EDR Detection Validation 2025 - AV-Comparatives - Featured Image

INNSBRUCK, TIROL, AUSTRIA, June 15, 2025 /EINPresswire.com/ -- After launching the pilot earlier this year, AV-Comparatives has now completed the 2025 round of the EDR Detection Validation Test. This independent evaluation put seven enterprise cybersecurity solutions to the test under advanced threat scenarios. The goal: to assess their ability to detect and report real-world attacks with precision and visibility.

Read the full test here: https://www.av-comparatives.org/news/edr-detection-validation-2025/

> As cyberattacks evolve, detection can't be a checkbox. Our 2025 EDR/XDR Certification helps CISOs assess how effectively their tools uncover stealthy, real-world threats."
>
> *Andreas Clementi, ceo and founder, AV-Comparatives*

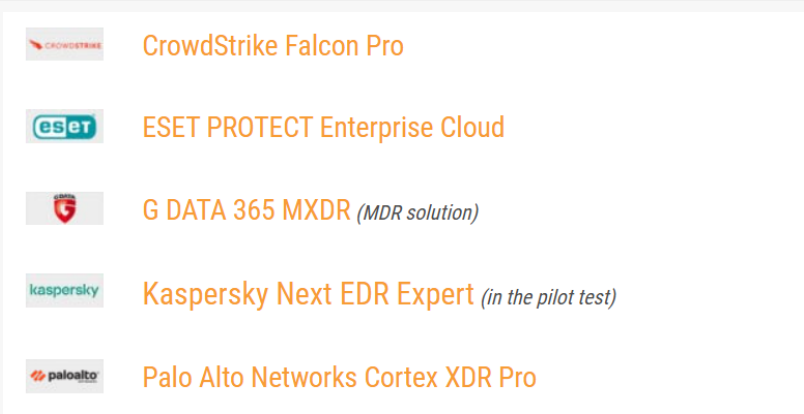
Unlike, e.g. the EPR Test, which focuses on prevention, the EDR test simulates complex attack scenarios to assess how well a product detects and logs each stage of an intrusion, providing insights into its visibility, telemetry quality, and threat detection precision. Threat visibility based on threat hunting capabilities is also considered.

We are pleased to announce that a total of five solutions have achieved certification so far — four in the recent 2025 certification test, and one in the earlier pilot phase — under our transparent and rigorous methodology.

Certified Products – EDR, XDR and MDR Solutions

The following products earned certification in the 2025 test round:

- CrowdStrike Falcon Pro
- ESET PROTECT Enterprise Cloud
- G DATA 365 MXDR (MDR solution)
- Kaspersky Next EDR Expert (in the pilot test)
- Palo Alto Networks Cortex XDR Pro



EDR Detection Validation 2025 - AV-Comparatives - Participants

EDR Detection Validation 2025 - AV-Comparatives - Certificate

One Methodology – EDR, XDR, and MDR
While initially designed to evaluate EDR and XDR capabilities, the test can equally be applied to MDR (Managed Detection and Response) offerings. In this round, G DATA successfully participated with their MDR solution, demonstrating that even managed offerings can be assessed under realistic, controlled attack conditions.

A Focus on Real-World Visibility
This evaluation simulates Advanced Persistent Threat (APT) attacks, using known Tactics, Techniques, and Procedures (TTPs) from frameworks such as MITRE ATT&CK. All products were tested in monitoring mode only, meaning prevention features were disabled. The goal: to measure how well threats are detected and reported, not blocked.

Highlights of the methodology:

- Execution of complex attack chains
- Validation of detections via alerts in the management console or through manual threat hunting in telemetry
- Transparent certification model: only products meeting the detection threshold are certified and publicly listed
- Methodological Improvements and the Road Ahead

The 2025 test incorporated feedback from independent analysts, resulting in greater transparency, enhanced scoring, and deeper telemetry validation. Further enhancements are planned for the 2026 certification test.

Interested in submitting a product to the certification?
The EDR Detection Validation Test is open to EPP, EDR, XDR, and MDR vendors seeking independent validation of their detection capabilities. Certification offers vendors both industry recognition and deep technical insight into their solution's real-world performance.

Contact us to participate in the next test cycle. https://www.av-comparatives.org/contact/

Cybersecurity and Antivirus Test Results available at https://www.av-comparatives.org for the following vendors:
Avast, AVG, Avira, Bitdefender, Checkpoint, Cisco, CrowdStrike, Elastic, Fortinet, F-Secure, ESET, G DATA, Gen Digital. Google, Intego, K7 Computing, Kaspersky, Malwarebytes, ManageEngine, McAfee, Microsoft, NetSecurity, Nordsec, Norton, Palo Alto Networks, Rapid7, SenseOn, Sophos, Total Defense, TotalAV, Trellix, TrendMicro, VIPRE, WithSecure and many more

Peter Stelzhammer
AV-Comparatives
+43 512 287788
email us here
Visit us on social media:
LinkedIn
Facebook
X