GUIDE

2025 MITRE ATT&CK® Evaluations

Exploring Cynet's Continued Strength in Prevention, Visibility, and Accuracy

Cynet achieved exemplary results in the MITRE ATT&CK® Enterprise Evaluations for three years running, showcasing sustained strength across prevention, detection clarity, false-positive reduction, and out-of-the-box readiness.

The consistency reflects a platform engineered for real-world resilience, built for security teams to scale security operations without sacrificing speed, visibility, or protection.

100%
Detection Visibility in Initial Run

100%
Technique-Level Coverage in Initial Run

100%
Protection in Initial Run

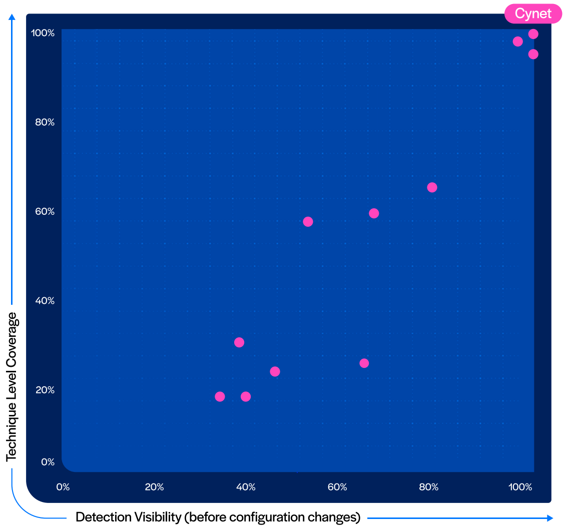
Zero
Detection False Positives in Inital Run

Zero
Configuration Changes

3 CONSECUTIVE YEARS OF PROVEN PERFORMANCE

What the 2025 MITRE ATT&CK Evaluations Measure

The 2025 MITRE ATT&CK Evaluations measures how well security solutions detect and protect against real-world adversary behavior using the ATT&CK framework as a reference. MITRE runs an adversary emulation (this year based on Scattered Spider and Mustang Panda) across multiple platforms and attack stages. Solutions are evaluated on the quality, depth, and accuracy of their detections, including whether they identify activity at the technique level, tactic level, or through general alerts. Solutions are also assessed for what they don't report, as MITRE seeks to identify which participants generate accurate alerts, report false positives, or miss alerts altogether. The ATT&CK Evaluations ultimately aim to help security teams assess participating vendors' visibility, detection accuracy, protection capabilities, and consistency across the full attack lifecycle. Results are evaluated and reported before configuration changes (Initial Run) and after adjustments to configurations (Configuration Change).



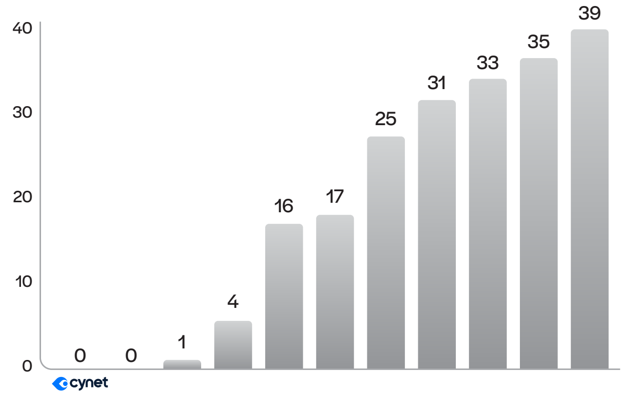
Detection Visibility vs. Technique-Level Coverage

MITRE evaluates each platforms' ability to collect all pertinent telemetry during simulated attacks (Detection Visibility) and create actionable, contextual alerts based on those inputs (Technique-Level Coverage). This Detection Visibility vs. Technique-Level Coverage chart demonstrates how Cynet performed in this year's evaluation in regard to data collection and accuracy of alerting. Strong overall results demonstrate a balanced and capable security platform that delivers protection, clarity, and operational efficiency against emulated real-world adversaries.

Number of Configuration Changes

Number of Configuration Changes data represents the adjustments a vendor must make to its product during testing to detect or respond to simulated adversary behaviors. Fewer required changes indicate stronger default protection and out-of-the-box readiness. For the third year in a row, Cynet was able to detect and respond to emulated attacks without configuration changes.

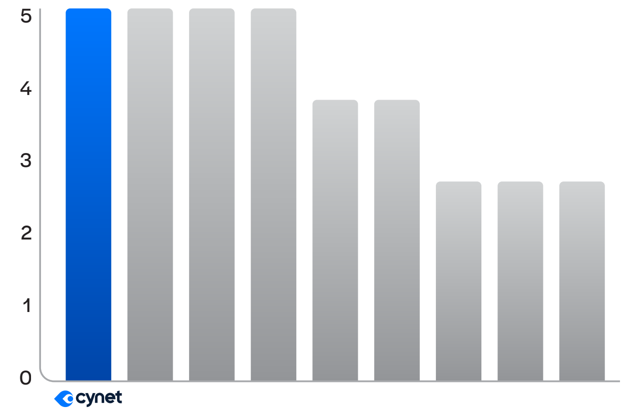
A low confirguration change count signals a platform that performs without heavy customization, intensive tuning, or expert intervention.



Protection Rate

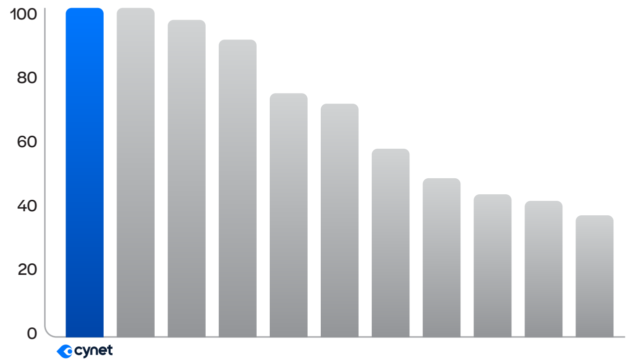
The Protection Rate reflects how often a solution automatically prevented adversary actions during the test scenarios. Higher protection rates demonstrate the platform's ability to block threats proactively, rather than just detecting or reporting them. Cynet participated in ALL 5 malicious test scenarios and successfully blocked each.

A high protection rate shows the solution can stop attacks in real time, reducing reliance on manual response.



Detection Visibility (Before Configuration Changes)

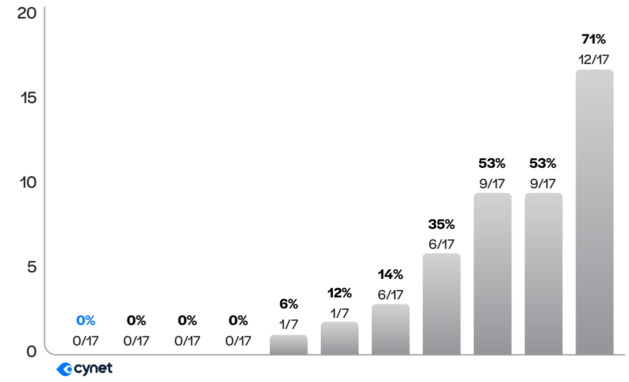
Detection Visibility (Before Configuration Changes) reflects how many adversary techniques the solution was able to observe in its default state, without tuning, customization, or configuration adjustments. Strong pre-configuration visibility shows how well the platform surfaces malicious activity right out of the box, minimizing implementation and maintenance work, and accelerating time-to-value.



Detection False-Positive Rate

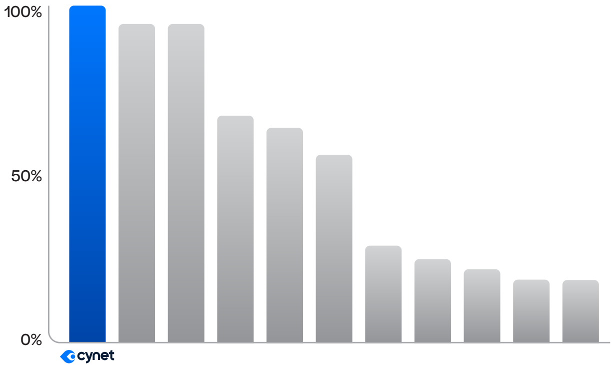
The Detection False-Positive rate reflects how often benign activity is incorrectly flagged as malicious during evaluation. A lower rate means greater accuracy, less noise, and fewer distractions for analysts, allowing security teams to focus on real threats and operational improvements rather than chasing alerts.

Cynet's low false positive rate means greater accuracy in detections, without disrupting operations or overwhelming security teams.



Technique-Level Coverage (Before Configuration Changes)

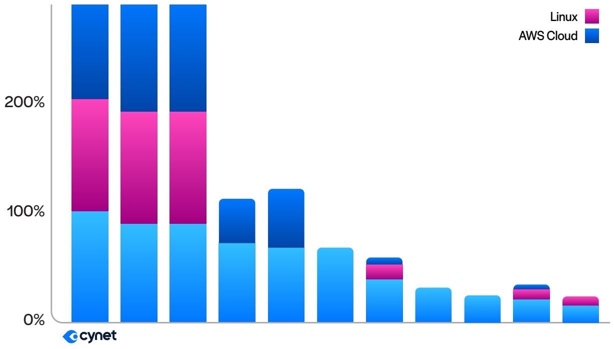
Technique-Level Coverage shows how many of the 90 malicious sub-steps the platform successfully detected without modifying default settings. Strong default coverage indicates a solution capable of recognizing sophisticated behaviors as-is, reducing dependency on expert configuration or specialized tuning.



Technique-Level Coverage (Per Platform)

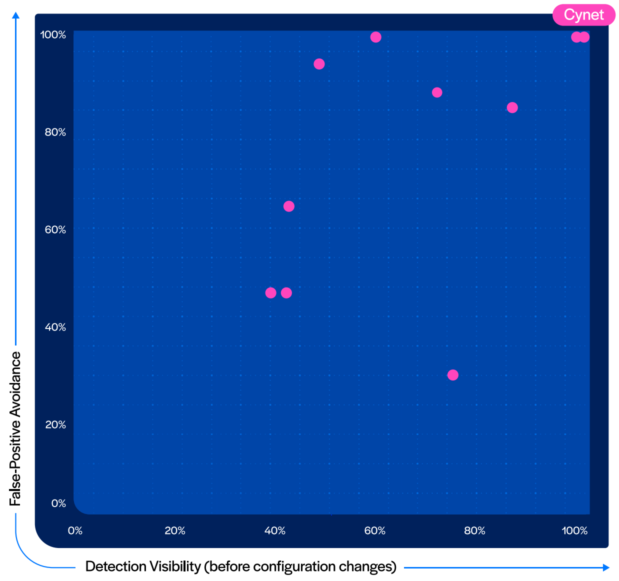
Technique-Level Coverage (Per Platform) highlights Cynet's unmatched 100% technique-level coverage before configuration changes across Windows, Linux, and AWS in the 2025 evaluation. Cynet detected and protected against every technique executed across all three platforms, demonstrating complete visibility and consistent performance regardless of environment.

With full coverage across traditional endpoints, modern Linux servers, and AWS cloud workloads, Cynet shows that organizations can rely on a single, unified platform to identify and stop threats across their entire attack surface. The results underscore Cynet's ability to deliver comprehensive, multi-platform detection



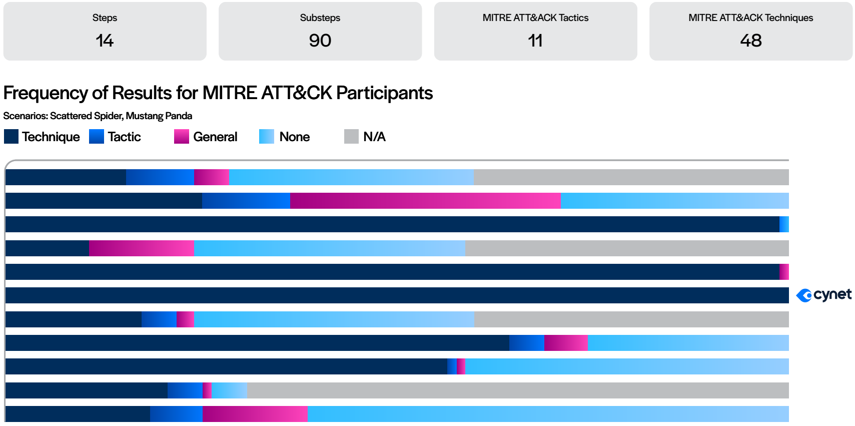
Visibility vs. False-Positive Avoidance (Before Configuration Changes)

This comparison demonstrates a balance between seeing more adversary activity and avoiding unnecessary alerting. High visibility with low false positives reflects a mature detection engine, one that gives security teams better clarity, even before configuration changes are applied.



Detection Summary

MITRE's summary graphic highlights significant variance between vendors in their ability to produce high-fidelity, technique-level detections. While many vendors show mixed results—combining tactic-level, general, and missed detections—Cynet stands out with full coverage of Technique detections across all 90 sub steps, indicating 100% Technique-Level Coverage (before configuration changes) with no gaps, general alerts, or higher-level fallbacks.



This chart demonstrates not only Cynet's consistency but also the depth of its detection capabilities across every stage of the adversary emulation, setting it apart from the broader field where detection quality varies widely.

Performance Worth Proving

Cynet participates in the MITRE ATT&CK® Evaluation because our customers deserve proof, not claims. Even as other vendors cited customer priorities as a reason not to take part in the 2025 evaluation, we believe independent testing IS a critical customer priority as it's a core part of delivering a safer, more trusted security experience.

Cynet's ability to deliver consistent results three years running demonstrates a focus on execution and outcomes. Our unified detection-and-prevention architecture correlates signals across the attack chain, delivers high-fidelity, ATT&CK-mapped detections out of the box, and converts them into fast, reliable protections with minimal tuning. Cynet embeds AI capabilities to help cut noise and prioritize what matters, so outcomes stay consistent at scale.

As demonstrated by our MITRE 2025 performance, our commitment is clear: transparent, validated outcomes that our customers can rely on, year after year.

About Cynet

Cynet is a unified, AI-powered cybersecurity platform purpose-built for security teams. Delivered through a global partner network, Cynet protects against advanced threats across endpoints, users, networks, identity, cloud, mobile, and email. Backed 24x7 by CyOps security experts, Cynet reduces tool sprawl, alert fatigue, and response times, so your team can focus on what matters.

Learn more at www.cynet.com