

Competitive Analysis: Cynet vs. Cisco

Last update: May 2024



Companies today are turning to Cynet and newer, more comprehensive cybersecurity solutions that provide expanded visibility across your environment, preventing and detecting endpoint, network, user, and cloud-based threats on a single platform. Cynet also provides extended automated response capabilities to greatly reduce the burden on your security team and ensure threats are quickly and properly addressed before damage can be done.

Cynet has many advantages over Cisco, especially for companies with lean security teams that can't afford the large staff required to leverage multiple focused solutions that cater to very large corporations. Cisco is well known for world-class networking and firewall products but has not been as strong a provider in the cybersecurity market.

Cisco's solutions are designed to be used by a large team of expert users that are looking for copious data and flexible search tools. This approach, however, is overwhelming for leaner security teams that do not have the bandwidth to appropriately support the tools. A highly complex and time-consuming configuration, user complaints about system slowdowns and limited remediation capabilities are just some of the issues with Cisco.

Summary



		
Time & Resources	✓ Fast, simple deployment. Automated investigation and response. Unified platform with one console and one vendor. 24x7 security experts and expert IR Team included.	✗ Cisco provides a disjointed, complex platform that requires multiple add-on technologies that become challenging for smaller companies to operate.
Pricing & Margins	✓ Natively built, unified solution avoids multiple technologies and integrations from multiple vendors. Less headcount required to deploy and manage solution. 24x7 security experts included.	✗ Disparate technologies integrated in the platform with multiple, expensive add-ons required to achieve full protection. Optional services can get expensive.
Threat Protection	✓ Top performing MITRE ATT&CK solution. All-in-One solution purposed built to protect entire environment. Automated investigation and response. 24x7 security experts and IR Team included.	✗ Cisco AMP provides basic endpoint protection.

Compare Cynet to Cisco



Platform	<p>✓ All-in-one, unified platform with full visibility and automated response across your environment (endpoint, network, users, mobile, cloud) and 24x7 MDR services.</p>	<p>✗ Cisco AMP is a basic EPP / EDR platform, but requires purchase of additional Cisco or 3rd party capabilities to achieve full visibility and automated response with optional, expensive MDR services.</p>
Effectiveness	<p>✓ Top 2023 MITRE ATT&CK Evaluation performer, enterprise-grade protections.</p>	<p>✗ Did not participate 2023 MITRE ATT&CK Evaluation, as did virtually all leading endpoint protection solution providers. Mediocre performance in the 2021 and 2022 MITRE ATT&CK Evaluation for endpoint protection.</p>
Ease of Use	<p>✓ Natively built, single pane of glass, designed to be easy to learn and intuitive to operate</p>	<p>✗ Amalgamation of technologies accessed via multiple interfaces. Third party solutions additionally required to attain similar capabilities as Cynet.</p>
Cost	<p>✓ \$90 list price per user per year for Cynet All-in-one platform, including all capabilities listed below, with full 24x7 MDR service included.</p>	<p>✗ \$100 per user per year for Cisco AMP and full 24x7 MDR service. This does not include UBA, NDR, email, Deception, XDR, CLM, CSPM/SSPM, and SOAR capabilities which must be purchased separately.</p>

Endpoint Protection Platform (EPP)	✓ Full, robust Next-Generation Antivirus, including device control and application control.	✓ Full, robust Next-Generation Antivirus, including device control and application control.
Endpoint Detection and Response (EDR)	✓ Multilayer malware protection and detection, including static and behavioral AI to detect zero-day exploits, malicious scripts and fileless attacks.	✓ Multilayer malware protection and detection, including static and behavioral AI to detect zero-day exploits, malicious scripts and fileless attacks.
2023 MITRE Engenuity ATT&CK® Evaluations	✓ Top performer in 2023 MITRE Engenuity ATT&CK® Evaluations for Endpoint Protection with 100% Visibility and 100% Analytic Coverage before configuration changes. You can trust Cynet to protect your organization.	✗ Did not participate in 2023 MITRE ATT&CK Evaluation.
Email Security	✓ Full email security to protect against malware infiltration, malicious links and phishing attacks included with Cynet All-in-One.	✓ Cisco email security solution can be purchased as an add-on.
User Behavior Analytics (UBA)	✓ Cynet can detect anomalous user behaviors that may be indicative of account takeover or a malicious insider threat.	✗ Not available.
Network Detection and Response (NDR)	✓ Cynet can detect malicious network behaviors such as reconnaissance scanning, DNS and ICMP tunneling, lateral movement and responder attacks.	✓ Cisco Secure Network Analytics can detect and respond to network-based threats as an add-on component.
Mobile protection	✓ Cynet 360 Mobile provides continuous detection and mitigation of malicious events affecting mobile devices with a centralized console to configure policies and manage threat events.	✗ Cisco provides Mobile Device Management (MDM) and Mobile VPN capabilities as an add on, but does not provide mobile threat detection.

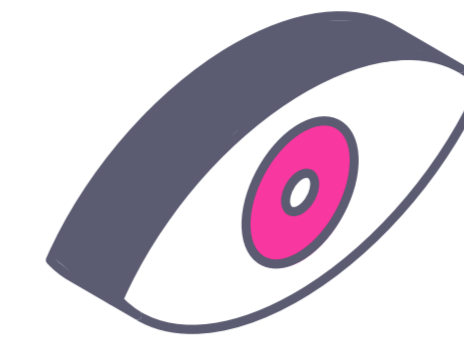
Extended Detection and Response (XDR)	<p>✓ Cynet provides visibility into endpoints, user behavior, network activity and leverages deception technology to protect your entire environment.</p>	<p>✓ Cisco XDR can be purchased as an add on to integrate other Cisco and 3rd party components.</p>
Security Orchestration Automation & Response (SOAR)	<p>✓ Cynet response automation allow you to orchestrate incident response actions across your environment and get all the benefits of SOAR, including pre-built and customized response playbooks.</p>	<p>✗ Not available.</p>
Deception	<p>✓ Cynet Deception lures attackers to reveal their presence using multiple types of decoys, including fake files, hosts, users and networks.</p>	<p>✗ Not available.</p>
Cloud & SaaS Security Posture Management (CSPM & SSPM)	<p>✓ Cynet CSPM & SSPM reduce the risk associated with Cloud & SaaS configuration errors and oversights, allowing you correct errors with a single click.</p>	<p>✗ Cisco offers CSPM as part of its Cloud Application Security Suite for an additional fee, but lacks SSPM.</p>
Centralized Log Management (CLM)	<p>✓ Cynet CLM automatically collects the highest priority log data needed to quickly and accurately uncover threats across your environment.</p>	<p>✗ Cisco Security Analytics and Logging can be added for an additional fee, but only collects data from Cisco firewalls and network devices.</p>
Managed Detection and Response (MDR)	<p>✓ Full 24x7 MDR with threat hunting, investigation and response services, including unlimited expert advice. Includes Cynet All-in-on platform with all capabilities listed above.</p>	<p>✓ Full 24x7 MDR service that can be packaged with Cisco products at significantly higher cost than Cynet.</p>

Cynet 2023 MITRE Engenuity ATT&CK® Evaluations Results



100% Detection

19 of 19 Attack Steps with no configuration changes



100% Visibility

143 of 143 Attack Sub-Steps with no configuration changes



100% Analytic Coverage

143 of 143 Detections with no configuration changes



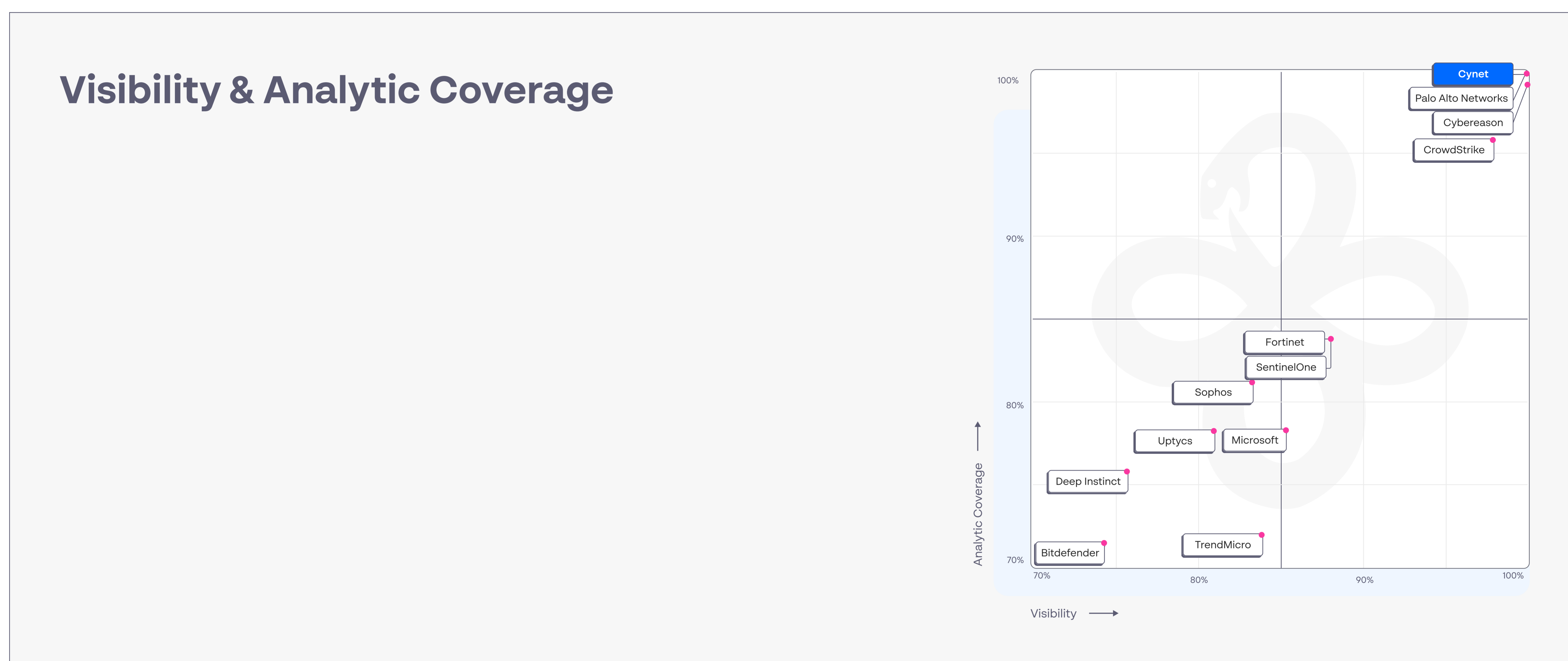
100% Real-Time Detection

0 Delays

MITRE ATT&CK Evaluation

After participating in both the 2021 and 2022 MITRE ATT&CK Evaluation: Enterprise for endpoint protection platforms, Cisco decided not to participate in the 2023 MITRE evaluation. Twenty-nine of the leading endpoint protection platform vendors participated in the 2023 Evaluation, so it's curious that Cisco chose not to participate given the increasing emphasis placed on the MITRE Evaluation results.

The decision to not participate could be due to the mediocre results Cisco achieved in both the 2021 and 2022 MITRE Evaluation. In both of these evaluations, Cynet outperformed Cisco on virtually every measure.



2023 MITRE ATT&CK Evaluation Results

For the first time ever in MITRE ATT&CK Evaluation testing, Cynet achieved a perfect 100% score for both Visibility (detection of the 143 unique threats tested) and Analytic Coverage (the number of alerts that contained actionable threat intelligence) before Configuration Changes.

It's very important to understand what Configuration Changes are in the MITRE ATT&CK Evaluation. After the main threat detection evaluations are performed, MITRE allowed vendors to make changes to their systems and retest the entire attack sequence. Many vendors that perform poorly in the main evaluation report their results after the make configuration changes, which is not representative of real-world performance. Always evaluate MITRE performance before configuration changes.

Learn more: cynet.com

