

Competitive Analysis:

Cynet vs. Palo Alto

Last update: April 2024

Companies today are turning to Cynet and newer Extended Detection and Response (XDR) solutions that provide expanded visibility across their 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's all-in-one platform approach offers true 360 coverage that extends beyond XDR. On the other hand, Palo Alto's Cortex primarily focuses on XDR functionalities. It offers additional security products like Prisma Cloud and Traps Mobile Security that require separate integration for broader protection.

One major disadvantage of Palo Alto's offering is that it is not a native platform. While it does leverage a range of solutions, some developed in-house and others acquired, this can result in a lack of cohesion and integration across the platform. This can lead to inefficiencies and difficulties in managing the platform. Achieving complete environmental protection using Palo Alto requires purchasing multiple separate product lines and an additional solution to integrate them all. However, with Cynet, you get everything you need in one package, without the need to buy additional products, at a considerably lower cost.

Summary



Time & Resources	<p>✓ Fast, simple deployment. Automated investigation and response. Unified platform with one console and one vendor. 24x7 security experts and expert IR Team included.</p>	<p>✗ Palo Alto's disjointed platform requires significant time and resources for integration due to multiple add-on technologies, making it a poor fit for SMBs with limited resources.</p>
Pricing & Margins	<p>✓ As a comprehensive all in one platform, our pricing model includes all capabilities.</p>	<p>✗ Disparate technologies integrated in the platform with multiple, expensive add-ons required to achieve full protection. Optional services can get expensive.</p>
Threat Protection	<p>✓ 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.</p>	<p>✓ Similar performance in 2023 MITRE ATT&CK Evaluation.</p>

Compare Cynet to Palo Alto



Platform	✓ All-in-one, unified platform with full visibility and automated response across your environment (endpoint, network, users, mobile, cloud) and 24x7 MDR services.	✗ While Palo Alto Cortex requires integrating several modules to function as a complete platform, once operational it can be a strong contender.
Effectiveness	✓ Top 2023 MITRE ATT&CK Evaluation performer, enterprise-grade protections.	✓ Top 2023 MITRE ATT&CK Evaluation performer, enterprise-grade protections.
Ease of Use	✓ Natively built, single pane of glass, designed to be easy to learn and intuitive to operate.	✗ It requires extensive knowledge and a dedicated team to administer, as it is designed and built for enterprise use.
Cost	✓ Cynet All-in-one platform, including all capabilities listed above, with full 24x7 MDR service available for a similar price other's basic EDR offerings.	✗ 2 to 4 times more expensive for Palo Alto Cortex and added components required to reach parity with Cynet and full 24x7 MDR service.

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.
User Behavior Analytics (UBA)	✓ Cynet can detect anomalous user behaviors that may be indicative of account takeover or a malicious insider threat.	✓ Palo Alto Cortex can detect anomalous user behaviors that may be indicative of account takeover or a malicious insider threat.
Network Detection and Response (NDR)	✓ Cynet can detect malicious network behaviors such as reconnaissance scanning, DNS and ICMP tunneling, lateral movement and responder attacks.	✓ Palo Alto offers an NDR capabilities as a part of the Cortex XDR. Cortex XDR provides complete visibility into network traffic, including encrypted traffic.
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.	✗ Available at an add on.

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>✓ Cortex XDR by Palo Alto automates threat hunting across your network and devices.</p>
Security Orchestration Automation & Response (SOAR)	<p>✓ Cynet response automation allows 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>✗ Cortex XDR integrates with Palo Alto Networks' Cortex XSOAR, a security orchestration and automation platform, which comes for an additional fee.</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>✗ Palo Alto requires a combination of Palo Alto Prisma Cloud and Prisma SASE to get similar capabilities, which comes for an additional fee.</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>✗ Not a part of Cortex, it requires Cortex XSIAM, which comes for an additional fee.</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>✗ Requires Unit 42 MDR: Offers a managed service where Palo Alto Networks security experts deploy Cortex XDR and other security tools, and then continuously monitor your network for threats, investigate suspicious activity, and take action to contain and remediate incidents which comes for an additional fee.</p>

Cynet: Comprehensive Cybersecurity Made Easy

Native Platform:

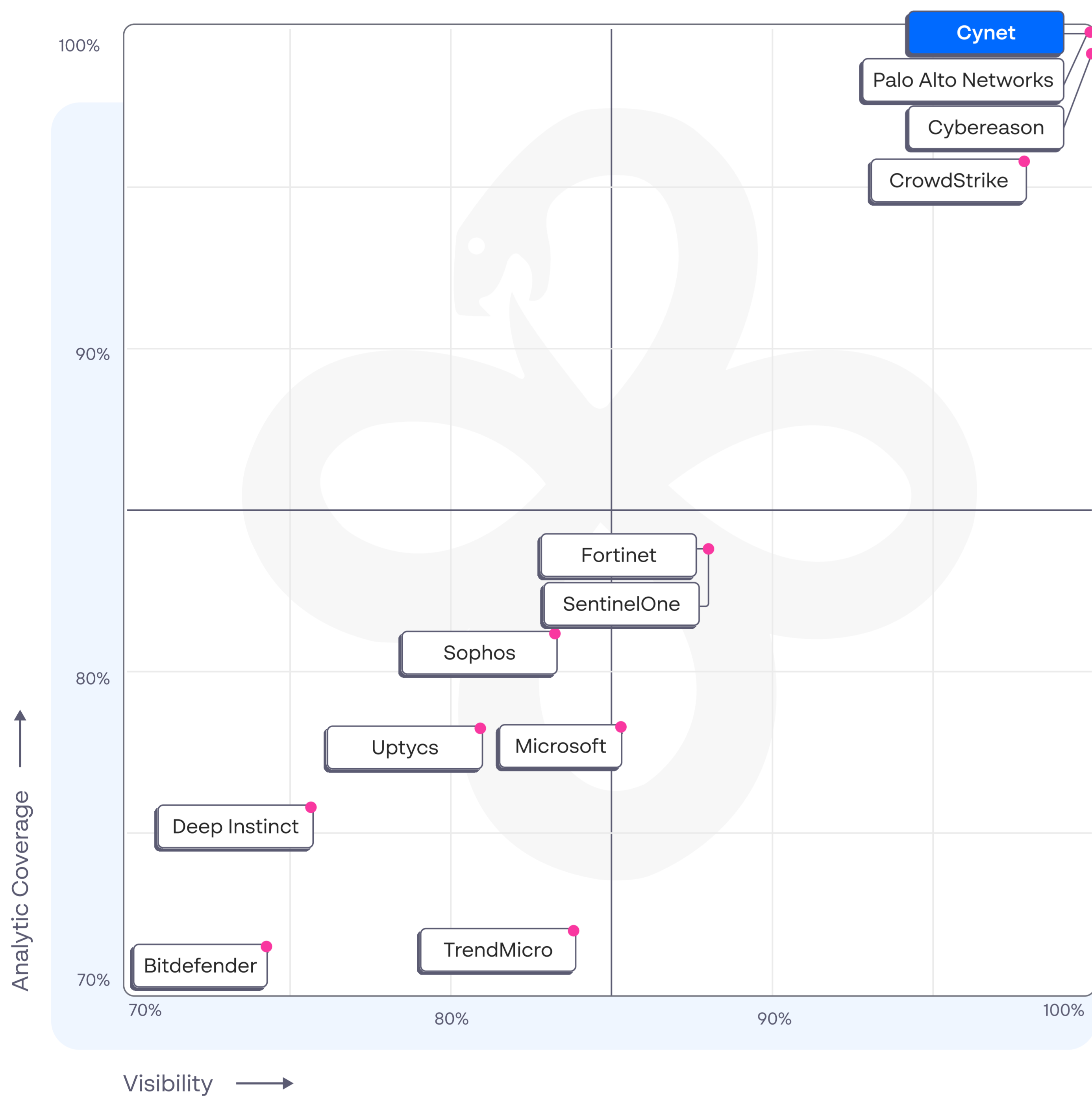
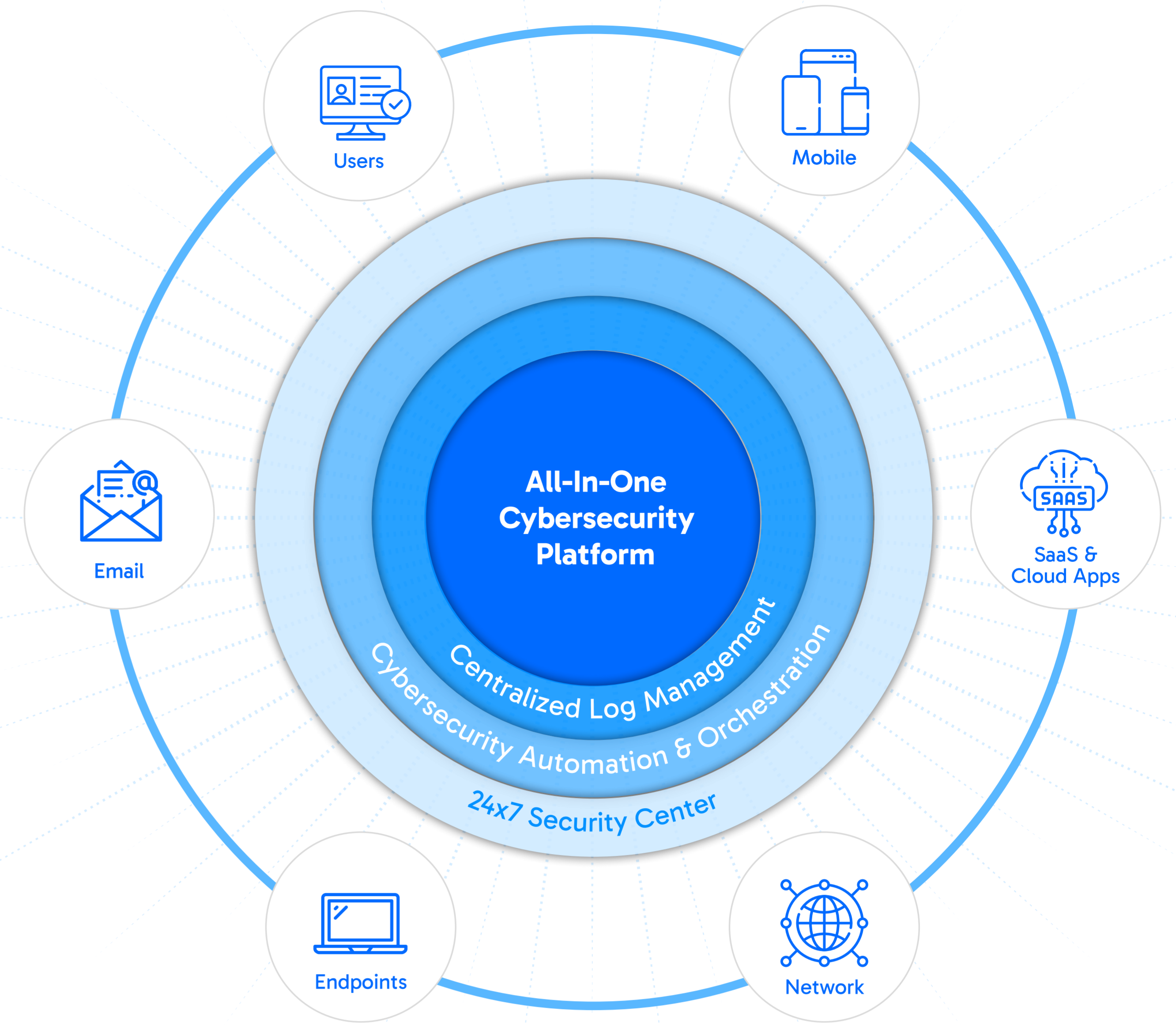
Built from the ground up for unified security.

Best-in-Class:

Delivers comprehensive threat detection and response across endpoints, network, and user activity, mobile, cloud, and email.

Full Coverage & Visibility:

Unifies endpoint security, deception, NDR, and vulnerability management for a complete threat picture.



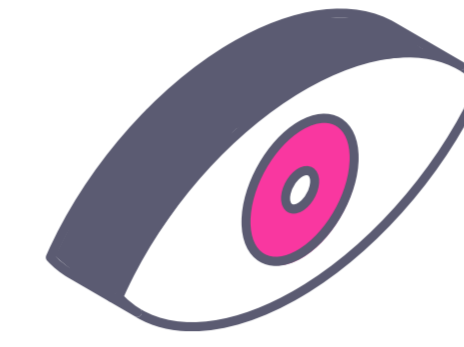
While Palo Alto Networks offers robust security solutions, their enterprise focus can translate to higher costs and complex implementations – ideal for large organizations with dedicated IT security resources. Cynet, on the other hand, delivers comparable threat detection and analytic capabilities at a significantly lower price point. Designed with the needs of small and medium-sized businesses in mind, Cynet offers a user-friendly platform that simplifies security management without compromising effectiveness.

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

Learn more: cynet.com

