

Competitive Analysis: Cynet vs. Microsoft

Last update: March 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.

While activating Microsoft Defender for Endpoint is easy on machines running the Windows 10 OS, it's far more onerous to install in Apple environments. With mediocre detection capabilities, dangerous delays in alerting and a disjointed set of management consoles, Defender for Endpoints is not optimized for lean security teams. Perhaps more importantly, does it make sense to use a company that continuously fails to prevent attacks that exploit flaws in its own platforms and software?

Further, Microsoft licensing is complex and confusing. Upgrading to Microsoft E3/E5 plans provides more capabilities, but the platform becomes prohibitively expensive and difficult to operate.

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.	✗ Disjointed platform that requires multiple add-on technologies. Designed for large enterprise customers. SMB service is subpar.
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 2023 MITRE Engenuity ATT&CK® Evaluations solution. All-in-One solution purposed built to protect entire environment. Automated investigation and response. 24x7 security experts and IR Team included.	✗ Mediocre performance in 2023 MITRE Engenuity ATT&CK® Evaluations, Full 24x7 MDR with basic XDR. Does not include UBA, NDR, Deception, CSPM/SSPM, CLM and SOAR capabilities.

Compare Cynet to Microsoft



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>✗ Microsoft XDR platform requires the purchase of at least 5 additional Microsoft or third-party capabilities to achieve full visibility and automated response.</p>
Effectiveness	<p>✓ Top 2023 MITRE Engenuity ATT&CK® Evaluations performer, enterprise-grade protections.</p>	<p>✗ Sup-par performer in the 2023 MITRE Engenuity ATT&CK® Evaluations.</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 separately built technologies. Third party solutions required to attain similar capabilities.</p>
Cost	<p>✓ 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.</p>	<p>✗ 2 to 4 times more expensive for Microsoft XDR and added components required to reach parity with Cynet and full 24x7 MDR service.</p>

Endpoint Protection Platform (EPP)	<p>✓ Full, robust Next-Generation Antivirus, including device control and application control.</p>	<p>✓ Full, robust Next-Generation Antivirus, including device control and application control.</p>
Endpoint Detection and Response (EDR)	<p>✓ Multilayer malware protection and detection, including static and behavioral AI to detect zero-day exploits, malicious scripts and fileless attacks.</p>	<p>✓ Multilayer malware protection and detection, including static and behavioral AI to detect zero-day exploits, malicious scripts and fileless attacks.</p>
2023 MITRE Engenuity ATT&CK® Evaluations	<p>✓ 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.</p>	<p>✗ Sub-par performer in Top 2023 MITRE Engenuity ATT&CK® Evaluations for Endpoint Protection with 85% Visibility and 78% Analytic Coverage before configuration changes. Microsoft may or may not detect dangerous threats in your organization.</p>
Email Security	<p>✓ Full email security to protect against malware infiltration, malicious links and phishing attacks included with Cynet All-in-One.</p>	<p>✓ Requires separate Microsoft Entra license and expensive E5 license upgrade.</p>
User Behavior Analytics (UBA)	<p>✓ Cynet can detect anomalous user behaviors that may be indicative of account takeover or a malicious insider threat.</p>	<p>✓ Full email security to protect against malware infiltration, malicious links and phishing attacks included with Cynet All-in-One</p>
Network Detection and Response (NDR)	<p>✓ Cynet can detect malicious network behaviors such as reconnaissance scanning, DNS and ICMP tunneling lateral movement and responder attacks.</p>	<p>✗ Not available.</p>
Mobile protection	<p>✓ 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.</p>	<p>✗ Available at an add on. Does not defend against rogue apps on IOS devices.</p>

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>✗ Available as an integration layer that requires at least 5 additional Microsoft of third-party add-ons to approach parity with Cynet's out-of-the-box capabilities.</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>✗ Microsoft's investigation function provides minimal context on individual endpoints. You'll need to upgrade to the very expensive E5 to get more robust investigation and response capabilities.</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>✗ Microsoft offers CSPM & SSPM 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>✗ Microsoft Sentinel provides SIEM capabilities, which include CLM, as a considerably expensive add-on.</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-one platform with all capabilities listed above.</p>	<p>✗ Full 24x7 MDR with basic XDR available. Does not include UBA, NDR, Deception, CSPM/SSPM, and SOAR capabilities.</p>

2023 MITRE Engenuity ATT&CK® Evaluations Results: Cynet vs. Microsoft

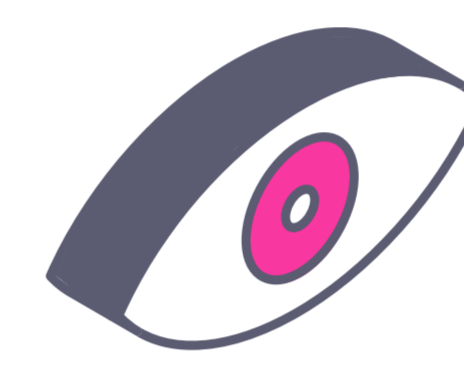
Microsoft, whose operating systems are the focus of most cyberattacks, participated again in the 2023 MITRE Engenuity ATT&CK® Evaluations: Enterprise. Microsoft's blog claimed they achieved "100 percent visibility across all stages of the attack chain in real-time." It also claims Microsoft achieved "100 percent ATT&CK technique-level detections at every attack stage without delay." Unfortunately, both claims are quite misleading.

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

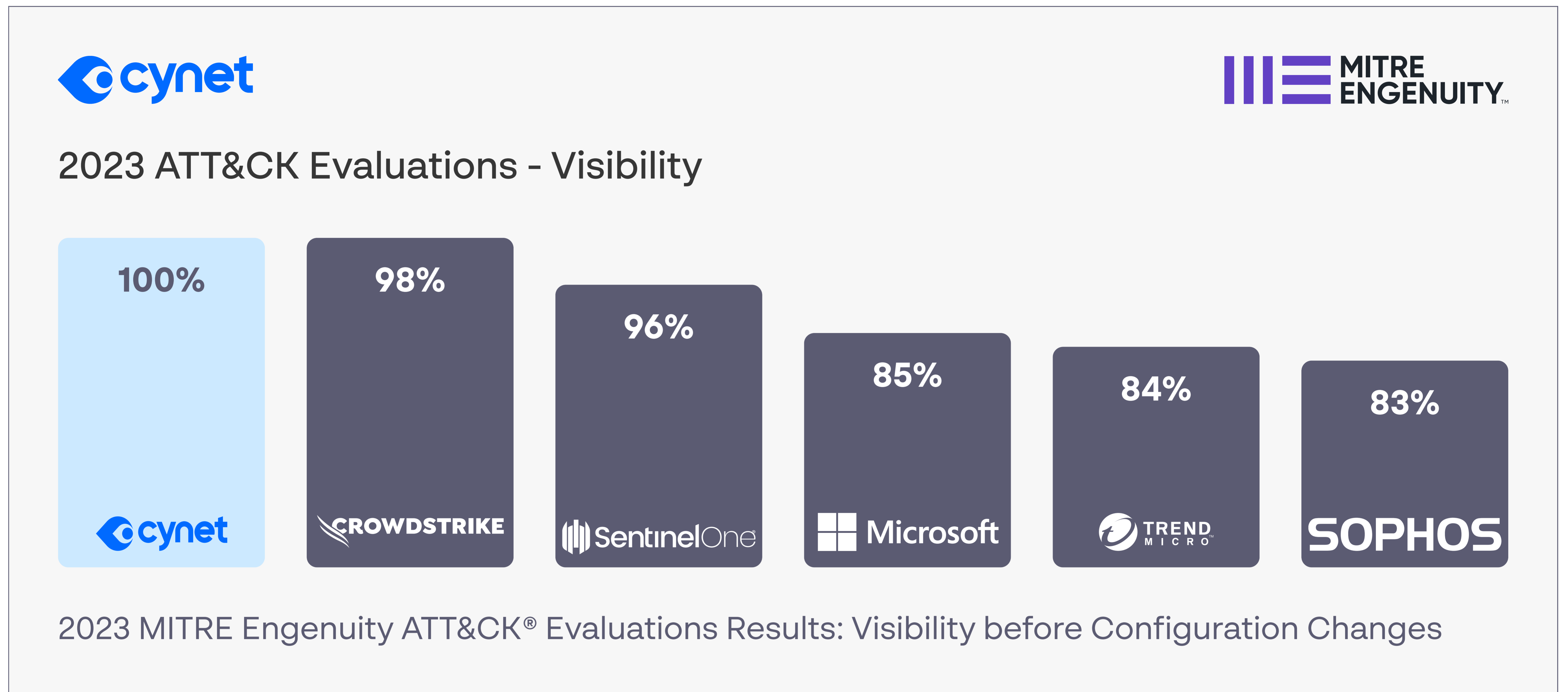


100% Real-Time Detection

0 Delays

Cynet Achieved Superior Visibility

During Days 1 & 2 of testing, Microsoft achieved 85% Visibility across all stages of the attack chain. "Visibility" is universally defined as the number of the 143 threats (aka sub-steps) tested that were detected. On the final day, Microsoft made a whopping 39 Configuration Changes – the fifth highest number of Configuration Changes made by the 29 participating vendors.



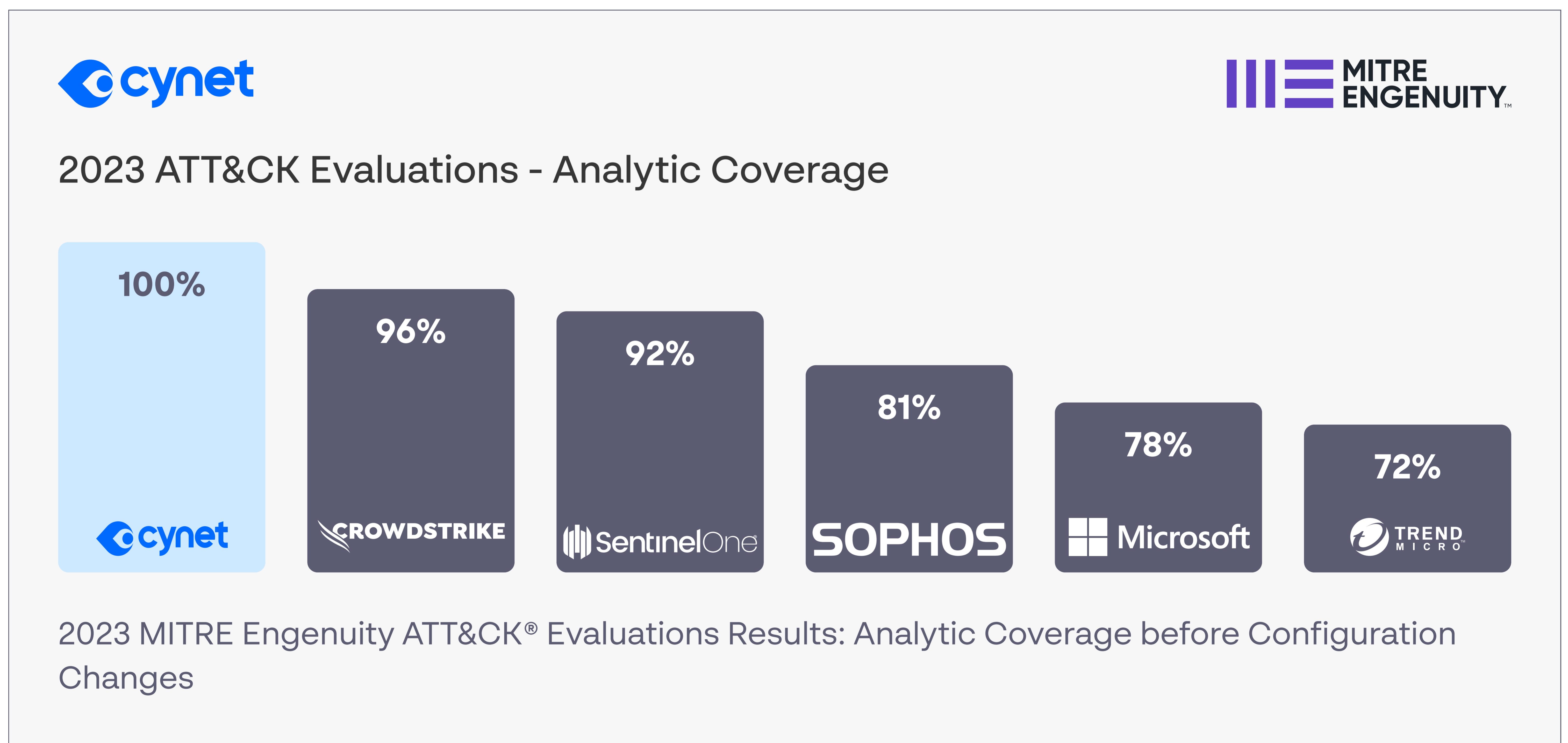
So, after the Configuration Changes were implemented, Microsoft achieved the 100% Visibility results they're promoting. It seems Microsoft forgot to mention the results they advertised were after 39 Configuration Changes, not a trivial detail and not a trivial amount of Configuration Changes. Unfortunately, after a successful attack you won't be able to reconfigure your system and then ask the attacker for a "do over!"

Cynet Achieved Superior Analytic Coverage

Microsoft claimed the achieved “100 percent ATT&CK technique-level detections at every attack stage without delay.” This claim, however, makes no sense. We can see that Microsoft achieved 97 technique-level detections before Configuration Changes. This translates to 68% technique level detections (97 technique-level detections out of the 143 Sub-steps). We can also see that Microsoft achieved 132 technique-level detections after Configuration Changes. This translates to 92% technique-level detections (132 technique-level detections out of the 143 Sub-steps). Microsoft is clearly being misleading with this claim.

Technique-level detections are one component of Analytic Coverage, the number of alerts that contained actionable threat intelligence. Analytic Coverage is the measure of detection quality used by MITRE Engenuity and all participating vendors. It’s important, for the reasons stated in the previous section, to measure Analytic Coverage, before Configuration Changes.

Microsoft achieved 78% Analytic Coverage before Configuration Changes. This means around three quarters of Microsoft’s alerts are accompanied with any useful information. Seven vendors achieved higher Analytic Coverage scores than Microsoft before Configuration Changes, with two vendors achieving 100%.



Learn more: cynet.com

