SentinelOne

MITRE ENGENUITY
A Foundation for Public Good

NCG
National Communications Group

at&t Authorized Agent

2022 MITRE ATT&CK Evaluations

SentinelOne's Stellar Performance Delivers Maximum Cybersecurity Value for the Third Year Running

What is MITRE Engenuity ATT&CK Framework?

The MITRE Engenuity ATT&CK Evaluation is among the world's most respected third-party security tests. It provides organizations with a critical and objective assessment of product performance. The results indicate a solution's ability to provide security analysts a quick, clear picture of how an attack unfolded.

Participating vendors are measured on their ability to detect and address real-world threats through the language and structure of the ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge) Framework.

ATT&CK Framework Components

Adversarial Tactics
What the attacker is trying to do.

Techniques
How the attacker achieves objectives.

Common Knowledge
Who are they? Their behavior.

APT Threat Groups

Wizard Spider

Sandworm

The 2022 Enterprise ATT&CK Evaluation emulates the real attack methods of Wizard Spider and Sandworm, two APT threat groups that conduct ransomware campaigns for financial gain and data destruction.

According to MITRE, these two threat actors were chosen based on their complexity, relevancy to the market, and how well MITRE Engenuity's staff can fittingly emulate the adversary. MITRE Engenuity tested our product, Singularity XDR, evaluating both detection and protection.

Singularity | XDR

SentinelOne

MITRE ENGENUITY
A Foundation for Public Good

NCG
National Communications Group

at&t Authorized Agent

SentinelOne Had Exceptional Results and Excelled in Every Category of the 2022 Enterprise ATT&CK Evaluation

100% Protection

Across Operating Systems

SentinelOne blocked all 9 of 9 MITRE ATT&CK Protection tests. We delivered the fastest and earliest protection with the least amount of permitted actions in the kill-chain for attackers to do damage.

Top Analytic Coverage

Across All Vendors

SentinelOne delivered 108 of 109 high-quality "analytic coverage" defined by MITRE as those "enriched with analytic logic" and thus providing correlation and context around the alerts. We have delivered the highest analytic coverage for three years in a row.

Full Visibility

With Zero Detection Delays

All SentinelOne detections are real-time, with zero delays, reducing incident dwell time through automation. Vendors that have delays are often far more human/linear/slower behind the scenes and lack automation.

Alert Consolidation

To Simplify and Increase SOC Efficiency

SentinelOne Singularity XDR automatically grouped two days of testing into only nine campaign-level console alerts, reducing the amount of manual effort required to understand what's happening. Fewer alerts and more context drives down MTTR.

What Do the Results Mean for My Organization?

SentinelOne's performance in the evaluation demonstrates how we're uniquely positioned to drive business value and help customers excel across major KPIs. SentinelOne delivered:

100%
Protection
9 of 9
MITRE ATT&CK Tests

100%
Detection
19 of 19 Attack Steps

100%
Real-time
0 Delays

99%
Visibility
108 of 109
Attack Sub-Steps

99%
Highest Analytic Coverage
108 of 109 Detections

SentinelOne | NCG National Communications Group | at&t Authorized Agent | MITRE ENGENUITY A Foundation for Public Good

Why SentinelOne?

Aligned to ATT&CK TTPs

SentinelOne solution maps directly to the ATT&CK framework to deliver unparalleled detection of advanced threat actor TTPs. Organizations can immediately benefit from exceptional protection and detection capabilities and autonomous and one-click response options to stop and contain the most advanced cyberattacks.

Actionable Detections

SentinelOne excels at visibility and detection and in the autonomous mapping and correlating of data into fully indexed and correlated stories through Storyline™ technology. Not only SentinelOne automate the creation of context, but it also leverages it to connect all the dots together, so the analyst doesn't have to.

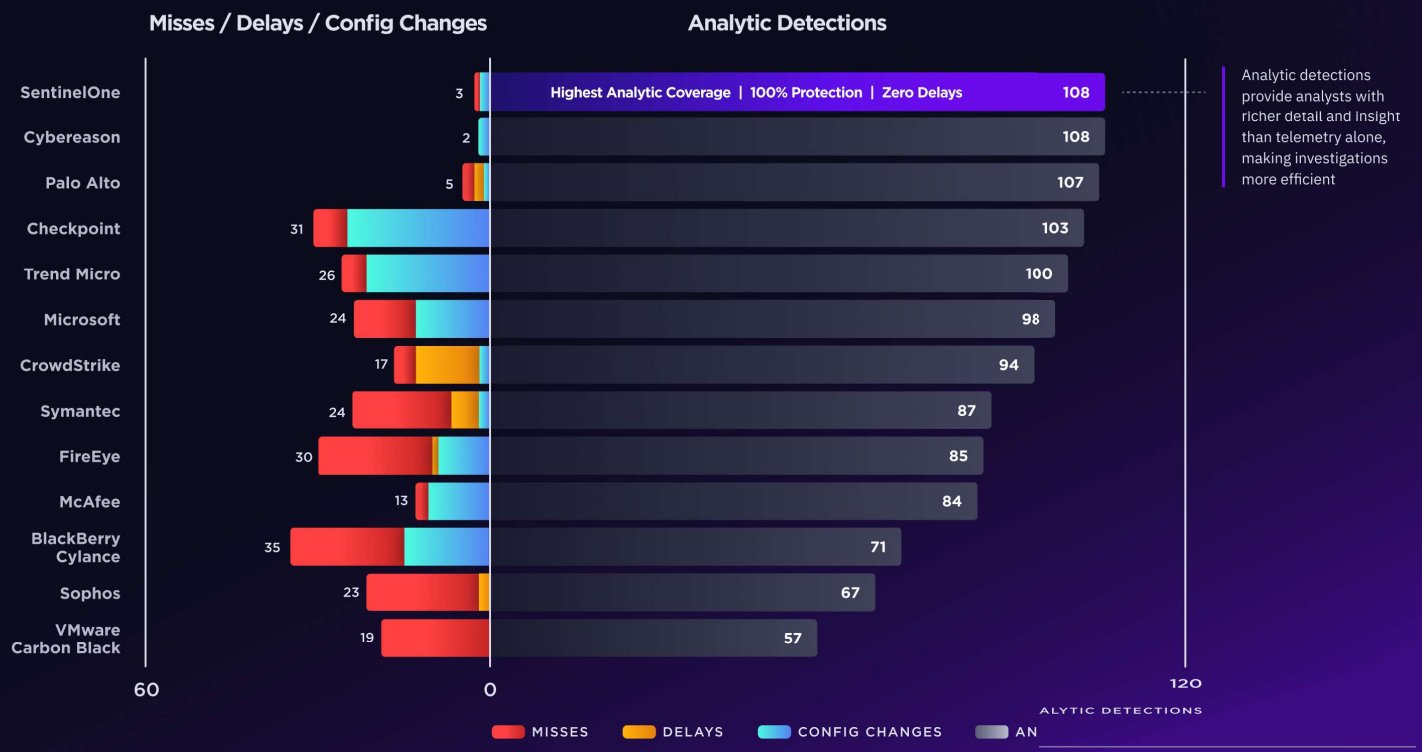
Industry-Leading Protection

SentinelOne delivered the fastest protection in the ATT&CK Evaluation. With its real-time protection, SentinelOne provided the MITRE ATT&CK Evaluation with the least amount of permitted actions in the kill-chain for attackers to do damage. The ATT&CK results display our commitment to preventing and protecting against every possible threat and keeping our customers safe from most adversaries.

One-Click Remediation

SentinelOne empowers security teams to take all the required actions to respond and remediate all affected devices with our patented, one-click remediation. It reverses all unauthorized changes with a single click, simplifying and reducing the Mean Time To Respond (MTTR).

SentinelOne's superior visibility, actionable context, the ability to defeat adversaries in real-time, and out-of-the-box efficacy Singularity XDR provides sets us apart from every other vendor on the market.



Call National Communications Group at 954-424-1235 x1 to learn more.

NCG National Communications Group | at&t Authorized Agent