SentinelOne White Paper

SentinelOne

MITRE ENGENUITY

MITRE Engenuity™ ATT&CK® Evaluation

SentinelOne Participates for the Third Year with Record Performance

April 2021

Table of Contents

01

Introduction

MITRE Engenuity continues to drive the cybersecurity industry forward for the better with the third iteration of its ATT&CK evaluations, this one performed in November 2020 with the results released April 2021.

MITRE Engenuity is a not for profit research organization whose stated goals are:

1. Empower end-users with objective insights into how to use specific commercial security products to detect known adversary behaviors.
2. Provide transparency around the true capabilities of security products and services to detect known adversary behaviors.
3. Drive the security vendor community to enhance their capability to detect known adversary behaviors.

SentinelOne remains a steadfast supporter of MITRE Engenuity's objective approach. They are indeed a catalyst for cybersecurity innovation not only in the vendor community but also within 1000's of organizations that now use ATT&CK as a common lexicon for understanding who the adversaries are and their typical game plans. ATT&CK helps industry clearly communicate the exact nature of threats and makes it clear how to enhance defenses to blunt the impact. Overall, ATT&CK serves as a flexible model and invaluable tool for applying intelligence to cybersecurity operations.

02

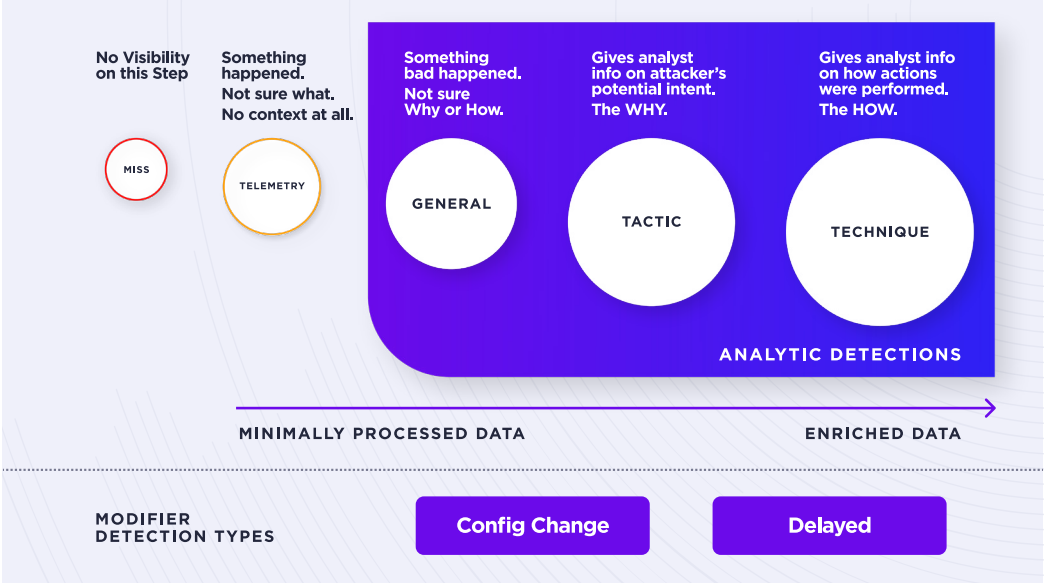
The Evaluation

Though the ATT&CK evaluation is not a competition, the results do help organizations understand relative product performance under emulated adversary conditions. The 2020 test takes place over two day and involves 20 distinct steps comprising 174 sub-steps. This year MITRE Engenuity emulates the Carbanak adversary group in Day 1 and the FIN7 adversary group in Day 2. Their common objective is to steal financial data.

SentinelOne Leads in ATT&CK Evaluation Performance

- Only Vendor with 100% Visibility Across all 174 Sub-Steps & Zero Misses
- Vendor with Highest Analytic Detection Coverage
- Zero Delay Modifiers
- Zero Config Change Modifiers

Arm yourself against exaggerated competing vendor claims by taking time to understand the differences among ATT&CK's detection categories. In summary, not all detections have the same level of quality. On one end of the quality spectrum is "Telemetry" which is simple "minimally processed data." On the other end of quality are "Techniques" that, according to the ATT&CK website, "gives the analyst information on how the action was performed or helps answer the question 'what was done'." The evaluation describes "Analytic Detections" as the sum total of all three higher quality, enriched detection types labeled as General, Tactic, and Technique. Lastly, ATT&CK defines two modifiers, configuration change and delayed. During testing, if the vendor modifies how their product operates to adjust for whatever reason, the evaluation proctors note these as "configuration change." During testing, if a "detection is not immediately available to the analyst due to additional processing unavailable due to some factor that slows or defers its presentation," this detection is labeled as "delayed."



When describing evaluation detection data, SentinelOne echos MITRE Engenuity's detection lexicon. Terminology like miss, telemetry, and analytic detection describe ascending levels of detection value. We also use config change and delayed to note these conditions.

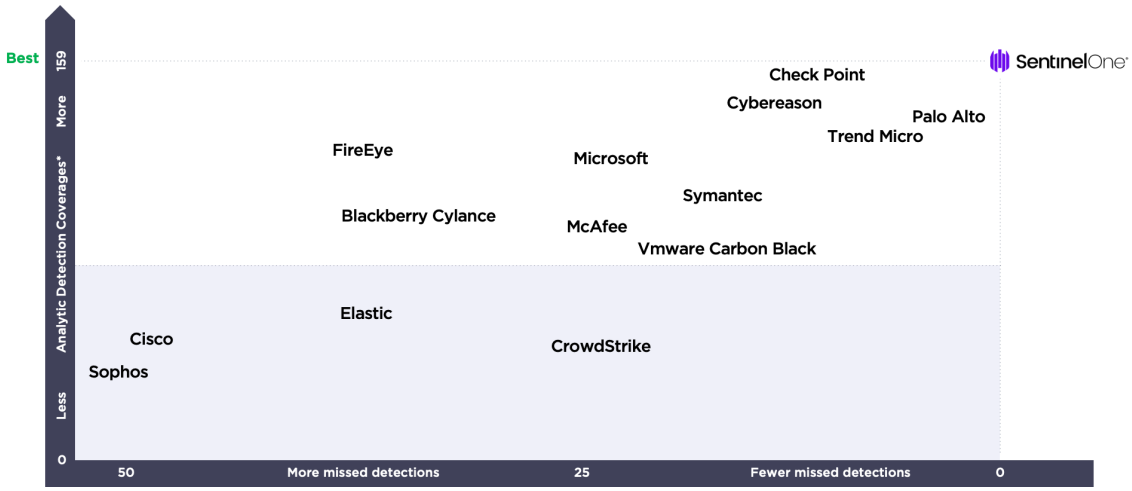
03

Results

SentinelOne is pleased with its performance in the 2020 ATT&CK evaluation. We detected something in each of the 174 sub-steps which means we missed zero. No other vendor achieved zero misses. But what is most striking in our performance is that >91% of the detections were of the high quality "analytic detection" type. SentinelOne is the only participant that exceeded >90% analytic detections in 2020. Furthermore, we were the only participant to achieve >90% in the ATT&CK 2019 evaluation. Our ability to deliver consistency over time is notable.

This graph illustrates participating vendors relative performance by mapping missed detections in descending order on the X axis and analytic detections on the Y axis in ascending order

SentinelOne Leads with Zero Misses & the Most Analytic (high quality) Detection Coverage



SentinelOne is unique among vendors in that it achieved >90% high-quality "analytic detections" in both the ATT&CK 2020 & 2019 evaluations.

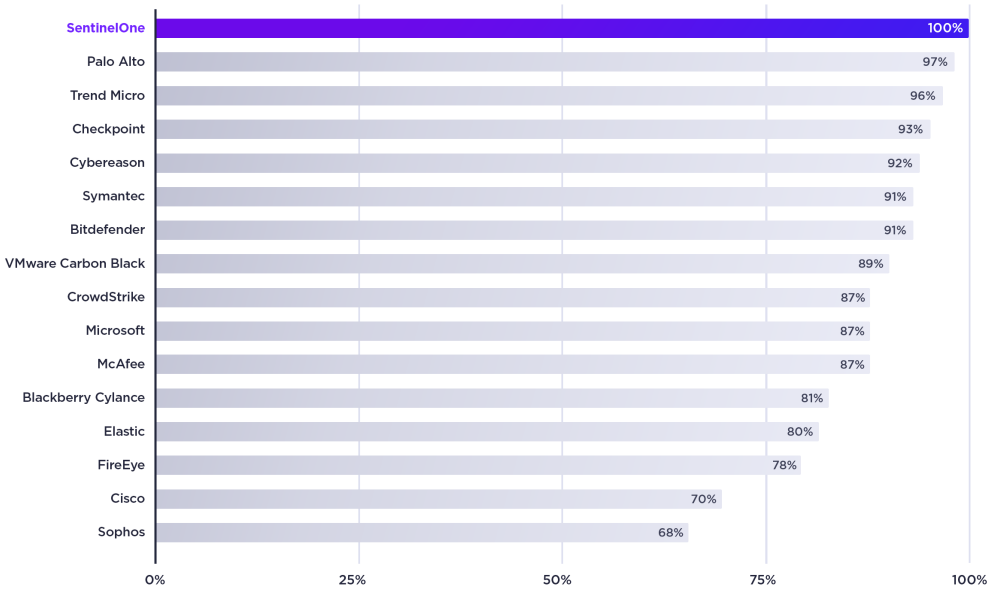
Other highlights of the evaluation detection results follow...

1. SentinelOne is the ONLY vendor to deliver the highest number of high quality analytic detections and have ZERO missed detections. And we do this across all tested operating systems - Windows & Linux.

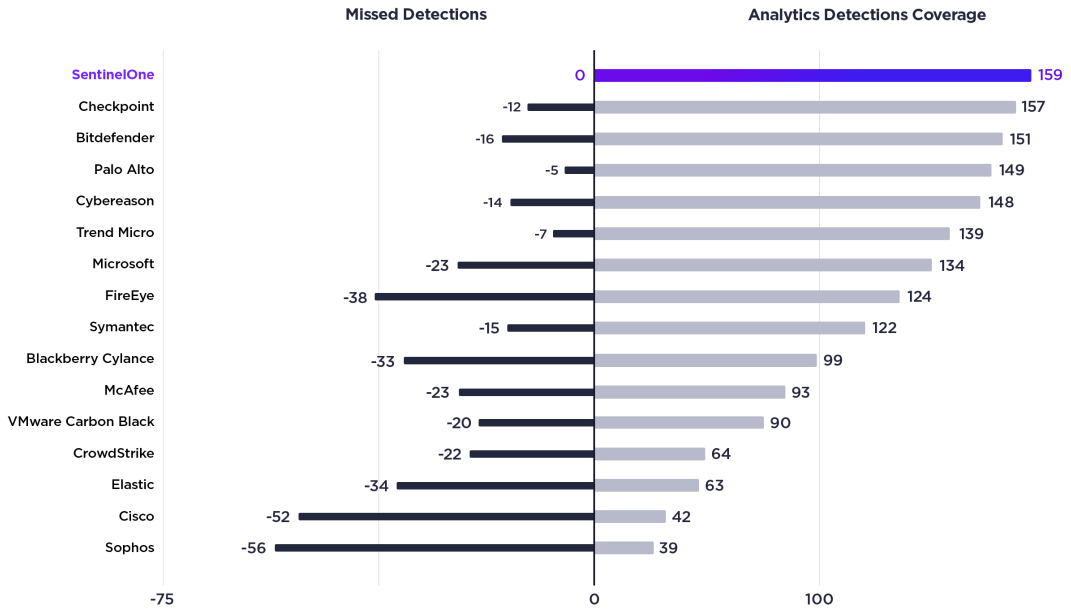
The foundation of a superior EDR solution is its ability to consume pertinent SecOps data at scale across a variety of OSes and cloud workloads while providing 100%, no-miss visibility. With the increased sophistication and frequency of today's attacks, depth and breadth of visibility are fundamental capabilities that an EDR solution should deliver. Having no gaps in

visibility means no blind spots, significantly reducing the attacker's ability to operate undetected. As the ATT&CK evaluation data shows, SentinelOne had ZERO misses in this round. We detected 100% of attacks on Windows devices as well as Linux servers.

Visibility is the Percentage of 174 Evaluation Sub-Steps with Any Detection Type. SentinelOne Leads with 100%.



Missed Detections vs. Analytic Detection Coverage (of 174 Max). SentinelOne Leads in Both Metrics.



EDR should also boost the analyst's efficiency by making context readily available so that they don't have to assemble all the details themselves. Quality over quantity should be a factor when deciding on the best EDR solution. We suggest using Analytics Detection Coverage rather than raw Detection Counts since analytics are a measure of high-fidelity and high-quality. Greater context gives enterprises more time to investigate events rather than searching through a sea of data that may be predominantly false positives.

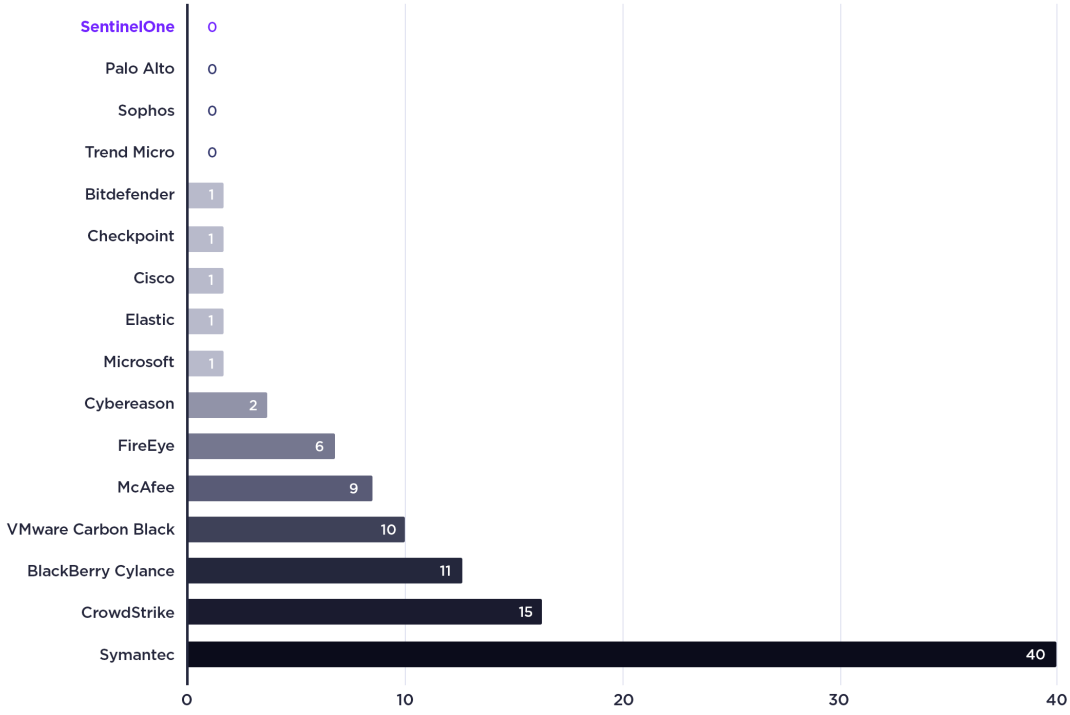
According to MITRE Engenuity's published results, SentinelOne recorded the highest number of analytic detections.

2. SentinelOne experienced zero delayed detections, making EDR real-time.

Time is a critical factor whether you're detecting an attack or neutralizing it. A delayed detection during the evaluation often means that an EDR solution required a human analyst to manually confirm suspicious activity due to the inability of the solution to do so on its own. The solution typically needs to send data to the analyst team or third-party services such as sandboxes, which in turn analyzes the data and alerts the customer, if required. However, many critical parts of this process are done manually, resulting in a window of opportunity for the adversary to do real damage.

As the ATT&CK evaluation data shows, SentinelOne had zero delayed detections.

Number of Delayed Detections During Evaluation. SentinelOne was One of Only a Few Vendors with Zero Delays.

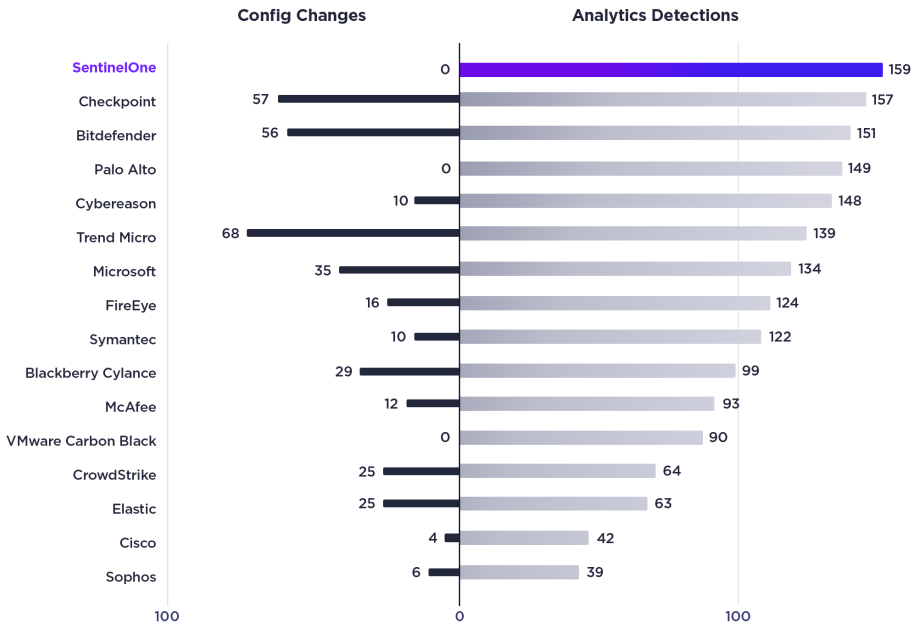


3. SentinelOne required zero configuration changes, making EDR effortless.

In a real-world scenario, SOC operators do not have time to customize settings, especially during an ongoing attack. Constantly tuning, fine-tuning, and adjusting a product means the battle is lost before it starts. In reality, SOC operators wouldn't even know what changes to make. Without an alert, they would not know what to look for to drive the configuration change.

Technology-powered solutions should work at an enterprise-scale right out of the box to realize immediate time-to-value. SentinelOne Enterprise Grade EDR deploys in seconds and works at total capacity instantly, as shown by the MITRE Engenuity evaluation data.

Config Changes vs. Analytic Detection Coverage (of 174 Max). SentinelOne Leads in Both Metrics.

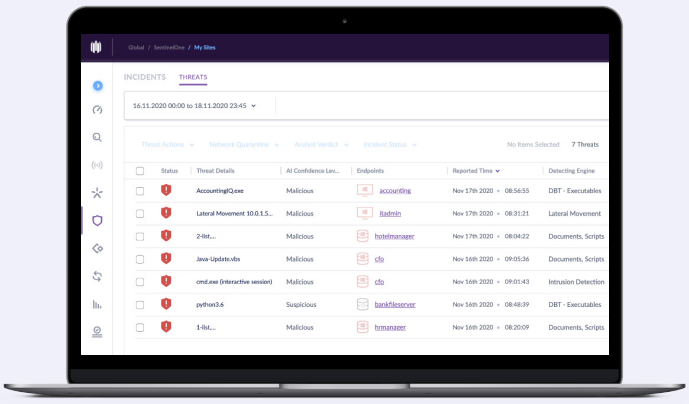


When you look at the data, you'll see some vendors that have high levels of analytic detections but some of them also have high levels of config change modifiers to achieve those detections. This may be an indicator of a product that requires a high level of human intervention to operationalize.

SentinelOne Summarized the Entire 2-day Evaluation into Only 7 Console Alerts

4. SentinelOne excels at the analyst user experience. This 174 step, 2-day evaluation produced 7 total console alerts.

Consolidating hundreds of data points across a 48-hour advanced campaign, SentinelOne correlated and crystallized the attack into one complete story. SentinelOne provides instant insights within seconds rather than having analysts spend hours, days, or weeks correlating logs and linking events manually. SentinelOne reduces the amount of manual effort needed, helps with alert fatigue, and significantly lowers the skillset barrier of benefiting from EDR.



04

What the Results Mean for You

As a security leader, it's important that you look at how you can improve your security posture and reduce risk while reducing the burden on your security team.

SentinelOne's exceptional performance in 2020 ATT&CK evaluations once again prove that purpose-built, future-thinking solutions deliver the in-depth visibility, automation, and speed that the modern SOC needs to combat adversaries. As evidenced by the results data, SentinelOne excels at visibility and detection, and even more importantly, in the autonomous mapping and correlating of data into fully indexed and correlated stories through Storyline™ technology. This technology advantage sets us apart from every other vendor on the market.

Ready for a Demo?

Visit the Great Lakes Computer website for more details, or give us a call at (800) 899-4522

greatlakescomputer.com

Innovative. Trusted. Recognized.

Gartner

A Leader in the 2021 Magic Quadrant for Endpoint Protection Platforms

Highest Ranked in all Critical Capabilities Report Use Cases

MITRE ENGENUITY

Record Breaking ATT&CK Evaluation

- No missed detections. 100% visibility
- Most Analytic Detections 2 years running
- Zero Delays. Zero Config Changes

Gartner peerinsights 4.9

98% of Gartner Peer Insights™

Voice of the Customer Reviewers recommend SentinelOne

FedRAMP

ISO 27001 CERTIFIED by schellman

100 VIRUS virusbtn.com

TEVORA

PCI DSS Attestation
HIPAA Attestation

GREAT LAKES
Computer
Corporation

Contact us

sales@grlakes.com
800-966-4522

About Great Lakes Computer

More than an extra pair of hands, Great Lakes is your partner in IT productivity. Our associates are highly engaged, providing the insight and knowledge to help you navigate the complexities of technology.

greatlakescomputer.com