Comparing SentinelOne Vs. McAfee

MITRE ATT&CK: See How McAfee Stacks Up

In the 2022 MITRE Engenuity ATT&CK Evaluation—the most trusted 3rd party performance test in the industry—SentinelOne achieved record-breaking results, delivering 100% protection across operating systems with the fastest threat containment and with the most analytic detections 3 years running. The SentinelOne Singularity platform consolidated the 109-step campaign into just 9 console alerts out-of-the-box, providing 99% visibility and automatically providing analysts with the context & correlation they need without extensive setup.

McAfee's performance once more paled in comparison. McAfee paused the evaluation 11 times for configuration changes and still, McAfee missed 24 analytic detections and failed to protect against 3 out of the 9 tests in this year's MITRE ATTACK Evaluation.

Proven EDR Performance & Value

Like many legacy AV vendors, McAfee's protection and detection capabilities were designed decades ago and rely heavily on known signatures and cloud lookups. While this approach may have been effective 10 years ago, it falls apart when tested against the modern adversary. The proof? In the 2022 MITRE ATT&CK® evaluation, McAfee had 13 misses and configuration changes and only detected 84 out of the 109 attack sub-steps.

McAfee also falls short in detecting stealthy trojan attacks like SUNBURST without sophisticated, real-time behavioral AI and adequate EDR data retention, especially when stacked up against SentinelOne's built-in behavioral AI analysis and 2x longer retention.

Legacy vs. The Long Run

On March 8, 2021, McAfee announced the sale of its endpoint security business to STG, leaving tens of thousands of customers behind and adding further uncertainty to the legacy platform's sustainability and adaptability to the future threat landscape.

In contrast, SentinelOne's autonomous platform leads the market not only in preventing, detecting, and remediating modern threats, but also maximizing the efficiency and efficacy of today's SecOps teams—an approach validated by our **97% customer satisfaction rate.**

	SentinelOne	McAfee
PLATFORM CAPABILITIES	✓ **ONE console, ONE agent:** Centralized & intuitive operations through a single platform	✗ **Multiple modules & agents:** Requires frequent navigation between complex interfaces
	✓ **Cloud connectivity optional:** Best-in-class EPP + EDR enabled by robust static & behavioral AI engines, even when offline	✗ **Cloud-dependent:** Detections rely heavily on cloud access (GTI), offline dependencies on legacy signatures (DATs) and immature machine learning
	✓ **Feature parity across cloud SaaS, hybrid, and on-premises deployments**	✗ **Varying feature set between self-hosted vs. SaaS ePO instances**
AUTOMATION & RECOVERY	✓ **Real-time, machine-powered attack reconstruction:** Events are automatically reconstructed into easily navigable Storylines™, focused & contextualized alerts for analysts means faster MTTR	✗ **Tedious correlation & contextualization:** Investigation & hunting requires context-switching between MVISION, ePO, and SIEM integration
	✓ **Fully automated recovery:** Autonomous & 1-click remediation and patented rollback	✗ **Partial automation:** Relies on DAT "repair" feature and can vary across threat types, limited "EDR Rollback"
EDR QUALITY & COVERAGE	✓ **Static & behavioral AI-driven detection:** Equipped to handle unknown threats and modern TTPs, including fileless and in-memory attacks	✗ **Legacy & ineffective, signature-based approach:** Misses fileless, & advanced attack TTPs, rudimentary AI capabilities
	✓ **MITRE ATT&CK mapping:** Integrates with MITRE Framework for easier, more intuitive investigation	✗ **Limited MITRE Framework mapping:** Requires MVISION Cloud add-on/module
	✓ **Fewest misses, richest detections in 2020 MITRE ATT&CK® evaluation:** SentinelOne outperformed McAfee, correlating 8x the telemetry, tactics, and techniques (118 vs. 14) and producing 1/10th as many misses	✗ **Sparse data correlation, 10x as many misses:** McAfee missed 96 detections (among the most misses of the vendors evaluated)
	✓ **14 day standard EDR data retention:** Accessible upgrades up to 365 days	✗ **7 day standard:** Upgrades up to 90 days at an additional cost
VALUE-ADDING SERVICES	✓ **Complete portfolio of security services:** Includes Vigilance Respond MDR & Vigilance Respond Pro MDR+DFIR staffed by in-house experts	✗ **Limited security services:** Outsources MDR activities to partner network