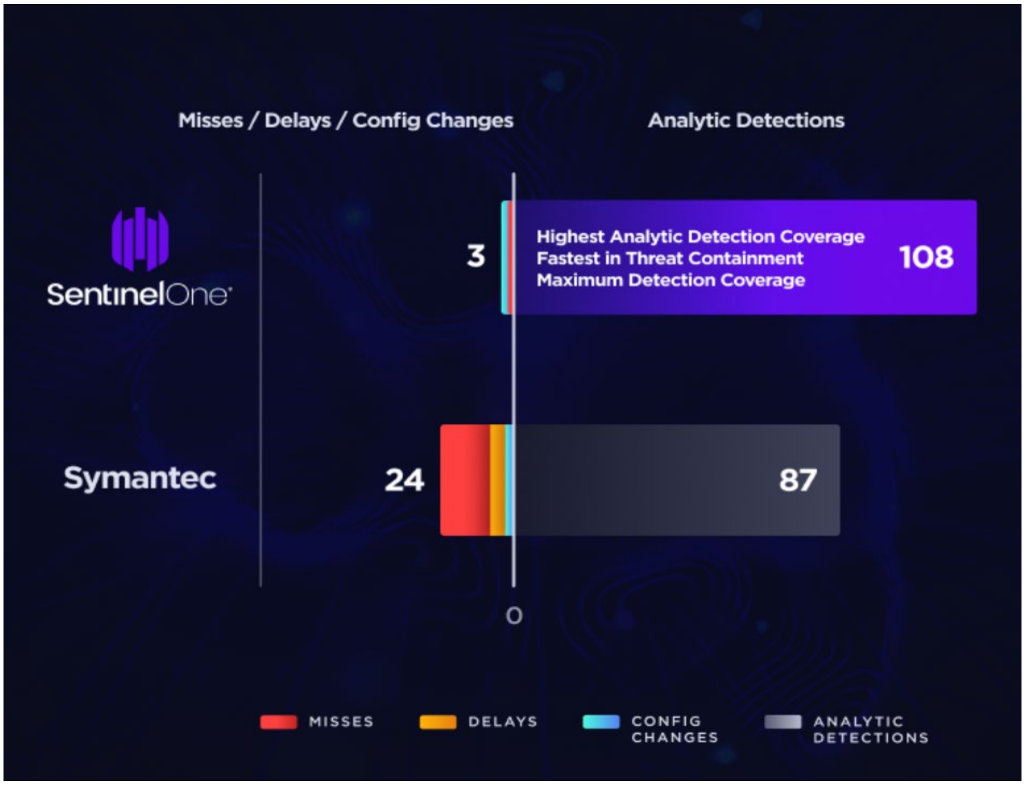
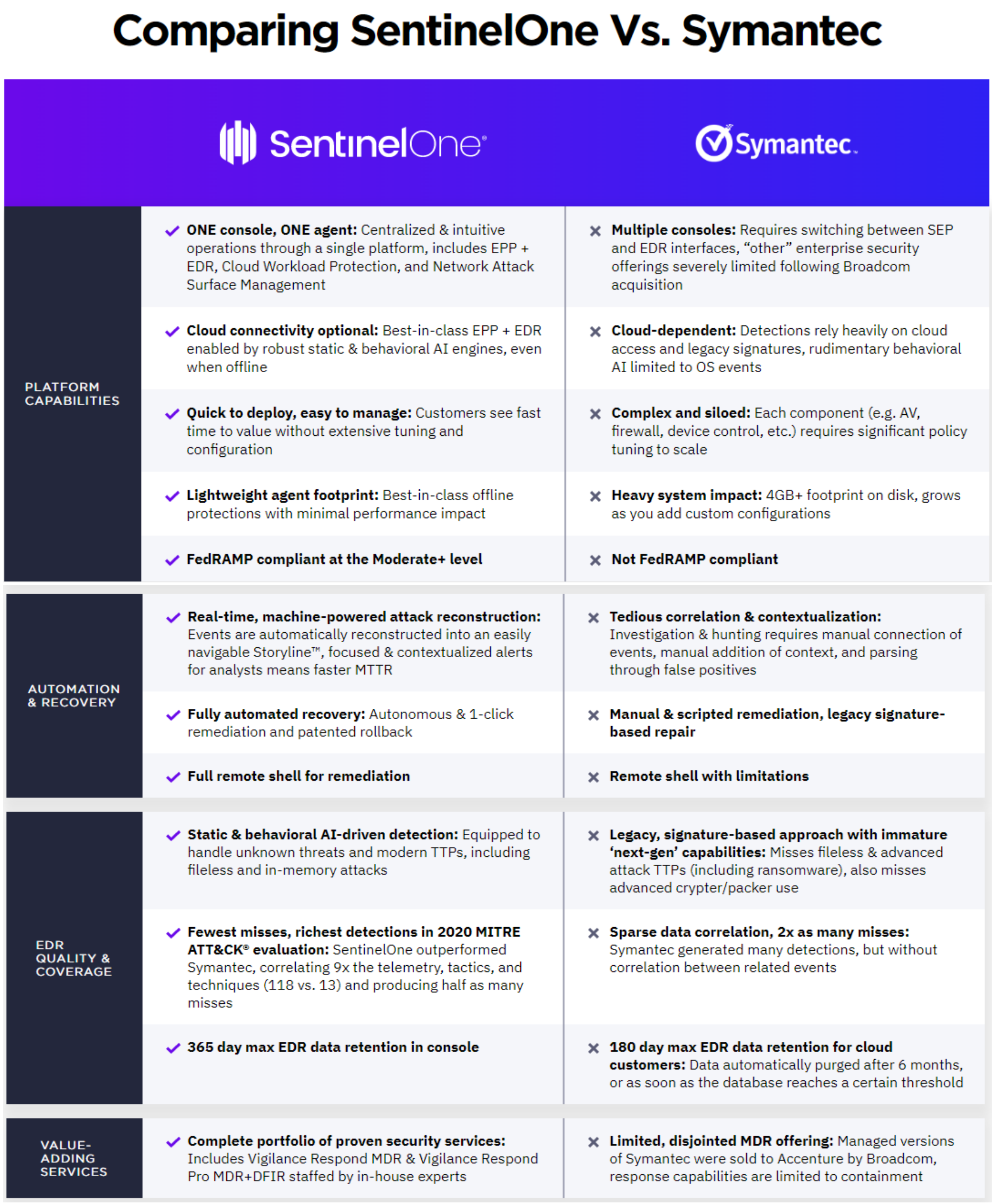
SentinelOne vs Symantec

MITRE ATT&CK:
See How Symantec 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.

Symantec continues to fail against today's real-world attacks. During the evaluation, Symantec missed 17 detections, had 5 delayed detections, required 2 different configuration changes, and could only produce 87 of 109 analytic detections.





Comparing SentinelOne Vs. Symantec

	SentinelOne	Symantec
PLATFORM CAPABILITIES	✓ **ONE console, ONE agent:** Centralized & intuitive operations through a single platform, includes EPP + EDR, Cloud Workload Protection, and Network Attack Surface Management	✗ **Multiple consoles:** Requires switching between SEP and EDR interfaces, "other" enterprise security offerings severely limited following Broadcom acquisition
	✓ **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 and legacy signatures, rudimentary behavioral AI limited to OS events
	✓ **Quick to deploy, easy to manage:** Customers see fast time to value without extensive tuning and configuration	✗ **Complex and siloed:** Each component (e.g. AV, firewall, device control, etc.) requires significant policy tuning to scale
	✓ **Lightweight agent footprint:** Best-in-class offline protections with minimal performance impact	✗ **Heavy system impact:** 4GB+ footprint on disk, grows as you add custom configurations
	✓ **FedRAMP compliant at the Moderate+ level**	✗ **Not FedRAMP compliant**
AUTOMATION & RECOVERY	✓ **Real-time, machine-powered attack reconstruction:** Events are automatically reconstructed into an easily navigable Storyline™, focused & contextualized alerts for analysts means faster MTTR	✗ **Tedious correlation & contextualization:** Investigation & hunting requires manual connection of events, manual addition of context, and parsing through false positives
	✓ **Fully automated recovery:** Autonomous & 1-click remediation and patented rollback	✗ **Manual & scripted remediation, legacy signature-based repair**
	✓ **Full remote shell for remediation**	✗ **Remote shell with limitations**
EDR QUALITY & COVERAGE	✓ **Static & behavioral AI-driven detection:** Equipped to handle unknown threats and modern TTPs, including fileless and in-memory attacks	✗ **Legacy, signature-based approach with immature 'next-gen' capabilities:** Misses fileless & advanced attack TTPs (including ransomware), also misses advanced crypter/packer use
	✓ **Fewest misses, richest detections in 2020 MITRE ATT&CK® evaluation:** SentinelOne outperformed Symantec, correlating 9x the telemetry, tactics, and techniques (118 vs. 13) and producing half as many misses	✗ **Sparse data correlation, 2x as many misses:** Symantec generated many detections, but without correlation between related events
	✓ **365 day max EDR data retention in console**	✗ **180 day max EDR data retention for cloud customers:** Data automatically purged after 6 months, or as soon as the database reaches a certain threshold
VALUE-ADDING SERVICES	✓ **Complete portfolio of proven security services:** Includes Vigilance Respond MDR & Vigilance Respond Pro MDR+DFIR staffed by in-house experts	✗ **Limited, disjointed MDR offering:** Managed versions of Symantec were sold to Accenture by Broadcom, response capabilities are limited to containment

Legacy vs. The Long Run

Since Broadcom's purchase of Symantec in 2019, the legacy platform has fallen further behind in adapting to today's cyber threats, and left thousands of customers scrambling for a new solution. Customers report ongoing pains with console management & updates, missed detections, alert fatigue, and rapidly waning support—without the upside of any significant technological innovations.

In contrast, SentinelOne's autonomous platform leads the market in preventing, detecting, and remediating modern attacks—without the overhead and manual workflows. SentinelOne customers report a 97% satisfaction rate, and see an average of 353% ROI when they switch from legacy AV providers, according to Forrester's Total Economic Impact report.

Proven Protection vs. Unknown & 0-Day Threats

Like many legacy AV vendors, Symantec'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 any modern adversary. The proof? In the 2020 MITRE ATT&CK® evaluation, Symantec **failed to detect twice as many attacker steps as SentinelOne**, and only correlated 13 telemetry points, tactics, and techniques compared to SentinelOne's 118 correlations.

Through a single endpoint agent that leverages robust static & behavioral AI with or without cloud connectivity, SentinelOne ensures you're protected against today *and* tomorrow's threats, 24/7.

One Console, One Agent for Easier EPP+EDR

With most SOC teams overstretched and resource-limited, every second counts. Most Symantec customers still leverage on-prem components, requiring tedious copy & pasting between endpoint protection (SEP) and EDR consoles. Symantec customers also spend valuable time manually correlating & contextualizing informationally sparse detections, pushing updates, and repairing endpoints. Staying responsive to contemporary threats not only requires agent upgrades (including signature versioning), but also changes to underlying infrastructure.

With SentinelOne, you can perform easy, directed investigations with auto-generated attack Storyline™ technology that comes with pre-built context, and trigger automatic or 1-click remediation & rollback of threats—all from a single console. Agent upgrades are easily scheduled on your terms, and no infrastructure changes are needed.