



Comparing SentinelOne vs. McAfee

	 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 & behavioural 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 & behavioural 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