SentinelOne

LinkedIn Link Twitter Link
Facebook Link Email Link

Start Free Trial

- Ransomware Attacks: To Pay or Not To Pay? Let's Discuss — pdf
- Aligning to the NIST Cybersecurity Framework — pdf
- Reducing Dwell Time With Superhuman AI – A CISO's Ammunition Against Ransomware — video
- Stop the Churn, Avoid Burnout | How To Keep Your Cybersecurity Personnel — pdf
- MITRE Engenuity™ ATT&CK® Evaluation – Webinar — video
- Solving The Av Problem — pdf
- SentinelOne vs MBRLocker (Ransomware) — video

The speed, sophistication, and scale of threats have evolved, and legacy AV solutions have failed to keep pace. Organizations lack the global visibility and context needed to combat these threats, creating blind spots that attackers can exploit. Security teams are already overwhelmed with the number of false positives and low detection efficacy of first-generation EDR solutions, which often require manual triage, response, and remediation.

When attackers pierce prevention measures, endpoint detection and response needs to happen autonomously and in real-time. SentinelOne Singularity Endpoint Protection (EPP+EDR) combines next-gen prevention and EDR capabilities in a single platform with a single agent.

Scalable Security Platform

Singularity is architected as a highly available SaaS solution with true multi-tenancy and multi-site hierarchy. Best-in-industry coverage across all major operating systems and a rich integration ecosystem extends the platform to your existing security investments.

Robust Prevention & Control

Replace legacy AV solutions with Static AI models trained to detect threats by looking at various static attributes extracted from executables, eliminating dependencies on signatures, and offering superior detection of file-based threats. Limit your attack surface with native firewall control and granular device control for USB & Bluetooth, Bluetooth Low Energy.

Threat Detection with Storyline™

Behavioral AI evaluates threats — like fileless attacks, lateral movement, and actively executing rootkits — in real-time, delivering high-fidelity detections without human intervention. Individual events are automatically correlated into a context-rich Storyline to reconstruct the attack from start to finish. Threat intelligence is infused from proprietary and 3rd party sources to increase detection efficacy.

Patented 1-Click Remediation

Remediate all affected endpoints with a single click, without the need to write any new scripts, simplifying and reducing mean time to respond. With STAR™ (Storyline Active Response), create automated hunting rules specific t
trigger alerts and responses when rules detect a match.

Next

Deep Visibility™ Threat Hunting

Deep Visibility powers hunting and investigation with zero learning curve, bringing IR and hunting to a broader pool of security talent. Uplevel SOC resources to enable proactive threat hunting with automated hunting rules, intel-driven hunting packs, and support for MITRE ATT&CK techniques. Easy to use search and pivoting lightens analyst load when hunting across large volumes (up to 365 days) of EDR telemetry.