

Endpoint Security powered by SentinelOne



SECURITY AROUND THE CLOCK, CONTROLLED BY YOU



AI-powered endpoint prevention, detection, investigation, response, and remediation with SentinelOne Singularity Complete



24x7 managed detection and response coverage through SentinelOne MDR Essentials



Complete client control over configurations, policies, alerts, exclusions, endpoint groups, workflows, and security decisions



Summit-led environment provisioning, licensing administration, technical support, and vendor escalation

Overview

Summit Endpoint Protection powered by SentinelOne puts Singularity Complete and MDR Essentials in a SentinelOne environment dedicated to your organization. The service combines advanced endpoint protection with continuous managed detection and response coverage, and your team keeps day-to-day platform administration and security decisions under your control.

Modern endpoint attacks use fileless techniques, legitimate administrative tools, stolen credentials, and previously unseen methods. You need greater endpoint visibility, faster containment and remediation, and coverage that runs past normal business hours while your team stays in charge of the environment.

Strengthen endpoint protection and cut response time with autonomous, AI-powered security and 24x7 MDR coverage. Your team retains control of the SentinelOne environment. Summit provides a consistent path for provisioning, licensing, platform support, and vendor escalation.

Why this matters

- ⚠ Traditional antivirus doesn't give you the behavioral detection, endpoint telemetry, or investigation context modern threats call for
- ⚠ Internal teams don't always have the time or resources to review endpoint activity around the clock
- ⚠ Disconnected alerts hide the sequence, scope, and root cause of an attack
- ⚠ Slow containment and remediation widen the operational impact
- ⚠ Fully managed security models don't fit organizations that need direct control over policies, exclusions, alerts, workflows, and risk decisions

Threats run continuously and move fast across endpoints and workloads. Shortening the time between suspicious activity, investigation, containment, and remediation limits disruption, and continuous MDR coverage addresses activity outside normal business hours.

Key capabilities

Detection in real time, response at machine speed

SentinelOne Singularity Complete

- **Behavioral AI protection:** Prevent and detect malicious and suspicious activity at machine speed
- **Investigation context:** Correlate related endpoint activity into visual Storylines for faster investigation
- **Automated response and remediation:** Isolate devices, stop malicious processes, remediate threats, and use rollback where supported
- **Purple AI:** Run natural-language threat hunts and get AI-generated event summaries
- **Broad workload coverage:** Protect supported Windows, macOS, Linux, virtual machine, and cloud workloads

SentinelOne MDR Essentials

- **24x7 managed detection and response:** Continuous coverage across supported attack surfaces
- **Integrated threat hunting:** Hypothesis-driven hunts informed by SentinelOne expertise and threat intelligence
- **Policy-driven containment:** Configure MDR Workflows so escalation and response actions match your environment
- **Real-time visibility:** Track activity through dashboards and detailed reporting

Benefits



Catch what signatures miss: behavioral detection beyond traditional signature-based antivirus, across continuous endpoint telemetry



Investigate faster: correlated Storylines show sequence, scope, and root cause in one view



Contain and recover quickly: autonomous containment, remediation, and rollback capabilities



Cover every hour: 24x7 MDR oversight that builds on your team instead of a new internal security operations center (SOC)



Keep authority: direct authority over platform configuration, policies, alerts, exceptions, groups, workflows, and security decisions



Lean on one support model: Summit provisioning, licensing administration, troubleshooting, and vendor escalation, with client administration and Summit platform support clearly separated

How it works

01

PROVISION

Summit provisions the dedicated SentinelOne environment, contracted licensing, and authorized client administrator access

02

CONFIGURE

Your team deploys and manages agents and configures policies, endpoint groups, alerts, exclusions, allowlists, and MDR Workflows

03

PROTECT

Singularity Complete continuously prevents, detects, investigates, and responds to endpoint threats according to configured policies

04

MONITOR AND RESPOND

SentinelOne MDR Essentials provides continuous monitoring, threat hunting, investigation, and response activities defined by client-controlled automated workflows

05

SUPPORT

Summit assists with platform functionality issues, gathers information for vendor cases, and coordinates escalation to SentinelOne

Summit Provisions



You configure and control



Singularity Complete protects



MDR Essentials monitors and responds



Summit supports and escalates

Differentiators



Complete client control: your organization operates the console and retains ownership of security governance and business decisions



Integrated EDR and MDR: Singularity Complete and MDR Essentials work through the SentinelOne platform to combine autonomous endpoint protection with continuous detection and response coverage



Dedicated environment: provisioned for your organization, not delivered as a shared, opaque service



One support path: Summit handles provisioning, licensing administration, technical support, and vendor coordination, with responsibilities clearly separated between client administration and Summit platform support

Outcomes

- ✓ Improved visibility into endpoint activity and attack progression
- ✓ Continuous detection and response coverage across supported endpoints and workloads
- ✓ Reduced platform administration friction through Summit provisioning and technical support
- ✓ Faster containment and remediation of detected threats
- ✓ Direct client control over policies, exceptions, alerts, workflows, and security decisions
- ✓ A scalable endpoint security foundation for workstations, servers, virtual machines, and supported cloud workloads

100% detection coverage in the MITRE ATT&CK evaluation

88% fewer alerts than the median of all vendors evaluated

96% of Gartner Peer Insights EDR reviewers recommend SentinelOne Singularity

TESTIMONIAL



Now our team can focus on managing applications and business processes.

ActiveCampaign >