SentinelOne

AI-powered endpoint protection that prevents, detects, responds, and rolls back attacks automatically, even when offline.

SentinelOne®

Logically™

EXECUTIVE SNAPSHOT

What It Is

A fully managed SentinelOne Autonomous AI Endpoint Protection Platform delivered by Logically, combining prevention, ActiveEDR, IoT discovery, and cloud workload protection in a single agent.

What It Replaces

Legacy antivirus, passive EDR tools, cloud-dependent detection models, and fragmented endpoint security stacks.

What You Gain

Real-time autonomous protection, rollback remediation, full-context forensics, IoT visibility, and 24/7 SOC-backed monitoring through Logically SecureCare.

THE CHALLENGE

Traditional antivirus, EPP, and EDR solutions do not solve today's cybersecurity problem.

Most tools:

- Rely on cloud connectivity, increasing dwell time
- Generate alert fatigue
- Depend on human operators to respond after damage occurs
- Require multiple products to close protection gaps

It takes only seconds for malicious activity to infect an endpoint, do harm, and remove traces. Cloud latency and manual intervention are too slow.

Security teams face:

- Too few staff
- Too many threats
- Too many products

Passive tools respond after it is already too late.

THE IMPACT IF NOTHING CHANGES

Without autonomous protection:

- Increased ransomware downtime
- Extended dwell time and recovery costs
- Visibility gaps across remote and distributed endpoints
- Manual alert triage consuming IT resources
- Inability to trace root cause quickly
- Ongoing dependency on connectivity

Delayed detection results in operational disruption, financial exposure, and audit risk.

THE SOLUTION:
SENTINELONE AUTONOMOUS AI PLATFORM

One platform to prevent, detect, respond, and hunt in the context of all enterprise assets. All at machine speed.

Delivered through a single agent, single codebase, and single console architecture, SentinelOne ActiveEDR goes beyond traditional antivirus and EDR.

Powered by proprietary TrueContext™ technology, it:

Protects against known and unknown threats in real time

Eliminates dependency on cloud latency

Stops processes, quarantines threats, and remediates automatically

Rolls back events to pre-encrypted states

Provides full-context, real-time forensics

Enables threat hunting with visual execution flow storytelling

Devices self-defend and heal themselves. Security teams focus on the alerts that matter. Logically delivers SentinelOne as a fully managed solution with 24/7 monitoring and response through SecureCare SOC.

One lightweight agent. One unified console. No delays. No gaps.

WHO IT'S FOR

Mid-market and distributed enterprises facing advanced, fast-moving threats

Organizations requiring audit-ready forensics

Healthcare, finance, manufacturing, and government organizations with remote workers

Logically customers bundling SentinelOne into SecureCare for full-stack MDR

Security-conscious firms seeking real-time visibility and autonomous response

WHAT YOU GET

Real-Time Endpoint Protection
- Multiple patented AI algorithms
- On-device prevention of known and unknown threats
- Protection without reliance on connectivity

Active Detection & Response
- Autonomous threat detection
- Policy-based remediation
- Process termination and quarantine
- Rollback to pre-breach state
- Perpetually clean endpoint state

Full-Context Forensics with TrueContext™
- Visual execution flow storytelling
- Root cause tracing
- Deep visibility into every operation on the agent
- Ability to search historic data
- Monitor any file and receive access or change notifications

IoT Discovery & Control

SentinelOne Ranger transforms every device into a sentinel:
- Maps enterprise IoT footprint
- Hunts rogue devices
- Enforces vulnerability hygiene
- Segments devices with dynamic policies

Cloud Workload Protection
- Autonomous CWPP
- Protection across cloud, container, and server workloads
- Visibility, file integrity monitoring, and compliance support

Single, Holistic Agent
- Lightweight, high-performance
- Windows, macOS, Linux, VDI support
- Cloud and on-premise management
- Offline support
- Robust API

Security Integrations

Pre-built integrations including:
- Splunk
- Fortinet
- Okta
- BigFix
- Tanium

Enterprise Proven
- Protects millions of endpoints
- Protects trillions of dollars of enterprise value
- Selected by global industry leaders
- Used by organizations such as JetBlue, McKesson, Flex, and Aston Martin

Certified & Recognized
- MITRE ATT&CK tested and ranked among top performers
- Gartner Magic Quadrant Leader for Endpoint Protection Platforms
- NSS Labs
- AV-Test
- AV-Comparatives
- MRG Effitas
- PCI-DSS
- HIPAA

USE CASE SNAPSHOT

Scenario
A 250-employee retail chain required airtight protection for point-of-sale systems and mobile endpoints.

Challenge
Frequent ransomware attempts, remote store visibility gaps, manual alert triage.

Solution
Logically deployed SentinelOne across all endpoints with rollback enabled and integrated alerts into the SecureCare platform.

Outcome
- Zero ransomware downtime
- Three times faster incident triage
- IT staff reallocated to strategic initiatives

Adoption & Deployment
- Single-agent deployment
- Unified console management
- Cloud, on-premise, and hybrid options
- 24/7 SOC-backed monitoring through Logically SecureCare

Fast time to production. Easy to deploy. Fully autonomous.

Autonomous Endpoint Defense.
Real-Time Remediation.
Always Watching.

hello@logically.com
866-946-9638