SentinelOne™

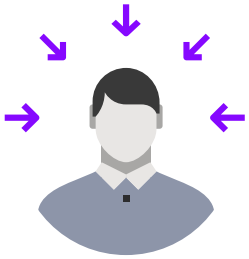
SentinelOne ActiveEDR

Autonomous Endpoint Protection That Saves You Time

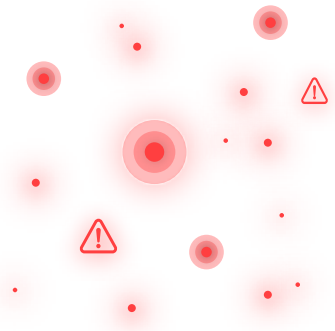
The Problem

AntiVirus, EPP and EDR as you know them do not solve the cybersecurity problem for the enterprise. To compensate, some rely on additional services to close the gap. But relying on the cloud increases dwell time. Depending on connectivity is too late in the game, as it takes only seconds for malicious activity to infect an endpoint, do harm, and remove traces of itself. This dependency is what makes the EDR tools of today passive as they rely on operators and services to respond after it's already too late.

Too Few Staff



Too Many Threats



Too Many Products

The SentinelOne Endpoint Protection Platform unifies prevention, detection, and response in a single purpose-built agent powered by machine learning and automation. It provides prevention and detection of attacks across all major vectors, rapid elimination of threats with fully automated, policy-driven response capabilities, and complete visibility into the endpoint environment with full-context, real-time forensics.

FOR MORE INFORMATION, VISIT WWW.SENTINELONE.COM

SentinelOne™

www. sentinelone.com • sales@sentinelone.com

+1-855-868-3733 605 Fairchild Dr, Mountain View, CA 94043

The Solution - ActiveEDR™

ActiveEDR™ is delivered via SentinelOne's single agent, single codebase, single console architecture. Going beyond traditional antivirus and EDR solutions, ActiveEDR, powered by SentinelOne's patented Storyline™ technology, allows security teams to quickly understand the story and root cause behind threat actors and autonomously respond, without any reliance on cloud resources. Storyline™ correlates and serves as a unique identifier for all events belonging to a group of processes.

With ActiveEDR™, everyone from advanced SOC analysts to novice security teams can visualize and understand the attack storyline without spending hours recreating the storyline by hand. The SentinelOne agent is also able to automatically remediate and rollback the actions of the threats with a single button click. This technology empowers security teams to focus on the alerts that matter and leverage technology to assist in what before was limited to human mandated tasks.

Differentiated in Every Aspect

Rich forensic data and can action threats automatically, including mitigation and even a complete rollback to pre-encrypted states

Extended Storage

Deep Visibility data is streamed to the cloud and stored for 14 days by default. Customers may purchase extended retention to meet compliance requirements for multiple years.

Respond & Rollback

Deep Visibility into every operation on the agent, including the ability to search for historic data and rollback files/ registry keys surgically to a safe known state.

Integrations

SentinelOne provides RESTful APIs and pre-built integrations to various Enterprise applications and services like Splunk, QRadar, Slack, ServiceNow, Joe Sandbox, Reversing Labs Threat Intel, Netskope, and PagerDuty.

Contextualize and Identify Evil in Real Time

Storyline™ technology reduces manual effort and automatically strings together related events in an attack storyline.

Threat Hunt with TrueContext

Monitor files, Indicators of compromise, Network activity and get notified upon access or change

Import/Export

For customers migrating from other EDR solutions, SentinelOne imports your existing queries into the SentinelOne Query Language (S1QL). SentinelOne also provides a Kafka based export stream for customers who wish to store/analyze their EDR data in their own data lakes.

FOR MORE INFORMATION, VISIT WWW.SENTINELONE.COM

SentinelOne

www. sentinelone.com • sales@sentinelone.com

+1-855-868-3733 605 Fairchild Dr, Mountain View, CA 94043