

SentinelOne ActiveEDR

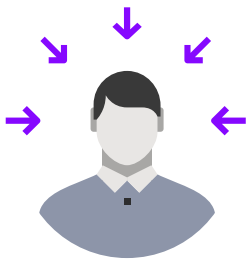
Autonomous Endpoint Protection That Saves You Time

The Problem

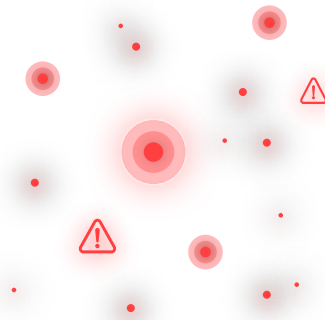
Anti Virus, EPP and EDR as you know them do not solve the cybersecurity problem for the enterprise. To compensate, some rely on additional services to close the gap. But relying on the cloud increases dwell time. Depending on connectivity is too late in the game, as it takes only seconds for malicious 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

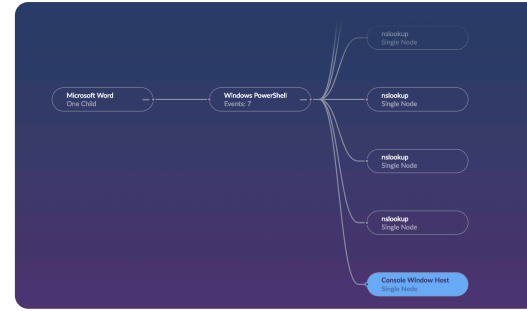


The SentinelOne Endpoint Protection Platform unifies prevention, detection, and response in a single purpose-built agent powered by machine learning and automation. It provides prevention and detection of attacks across all major vectors, rapid elimination of threats with fully automated, policy-driven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

FOR MORE INFORMATION, VISIT WWW.SENTINELONE.COM.

The Solution - Active EDR

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 proprietary TrueContext technology, allows security teams to quickly understand the story and root cause behind threat actors and autonomously respond, without any reliance on cloud resources. With ActiveEDR, everyone from advanced SOC analysts to novice security teams can automatically remediate threats and defend against advanced attacks. 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

Track Everything

Visual diagram representing an execution flow, helping IR teams to quickly evaluate the impact of any threat

Contextualize and Identify Evil in Real Time

Visibility into the encrypted network traffic without pushing certificates or the need for expensive SSL appliances/blades

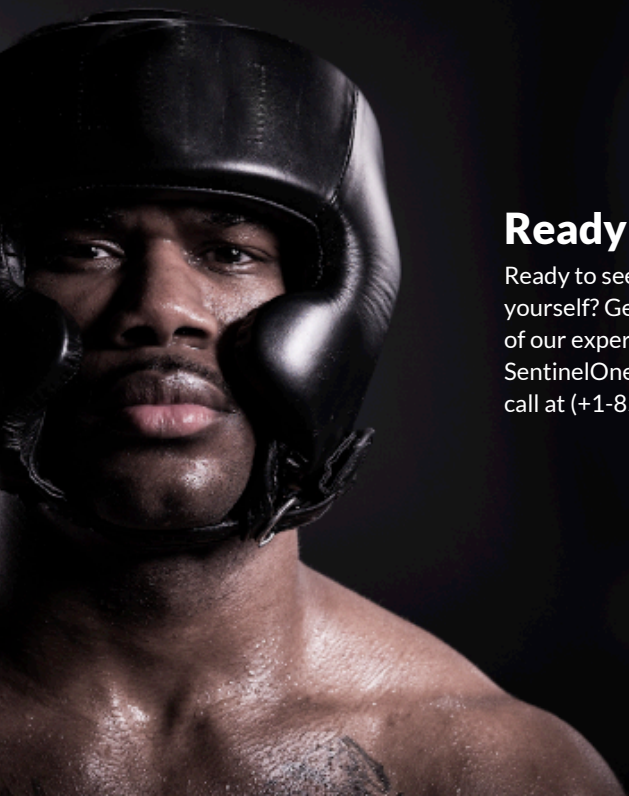
Respond & Rollback

Deep Visibility into every operation on the agent, including the ability to search for historic data

Threat Hunt with TrueContext

Monitor any file and get notified upon access or change

FOR MORE INFORMATION, VISIT WWW.SENTINELONE.COM.



Ready for a Demo?

Ready to see SentinelOne ActiveEDR for yourself? Get your customized demo from one of our experts by completing the form on SentinelOne.com/Demo, or you can give us a call at (+1-855-868-3733)

