SentinelOne

Purple AI™

Detect earlier,respond faster, and stay ahead of attacks with the world's most advanced AI security analyst

Modern security operations push defenders beyond human limits. The velocity and scale of today's attacks force teams to operate in environments they simply cannot manage with legacy technology, leading to critical coverage gaps and widespread burnout. Purple AI drives a fundamental shift in the SOC operating model, giving defenders the advantage of speed, skill and scale. Stop fighting the broken workflows and endless tool pivoting. Start fighting the adversary.

Purple AI is the industry's leading agentic AI security analyst. A powerful force multiplier drawing on frontline MDR intelligence, it uses reasoning AI to autonomously hunt, triage, and investigate alerts, delivering clear, explainable verdicts. It offloads manual data collection and reasoning, dramatically increasing analyst bandwidth so your team can clear backlogs and outmaneuver modern adversaries.

Simplify the Complex

Purple AI turns fragmented, high-volume security data into instant insight and action. Secure the broadest visibility across native and third-party data while AI agents analyze threats, prioritize alerts, and surface critical issues. Eliminate advanced query barriers so analysts can focus entirely on defeating the adversary.

Amplify Every Analyst

Maximize your team's impact by offloading manual, repetitive tasks to agentic workflows. Drawing on frontline MDR expertise, Purple AI scales elite human knowledge across your entire team. Elevate your SecOps team to operate beyond human limits.

Accelerate Security Operations

Move beyond rigid playbooks to dynamic, context-aware analysis. Purple AI translates investigations into actionable response recommendations, seamlessly triggering automated workflows to help teams resolve threats 55% faster.

Embrace Autonomy Responsibly

Your security and privacy are protected by design. Purple AI is advanced AI with responsible, secure foundations—architected with the highest level of safeguards. Maintain absolute control over automated responses using strict analyst-in-the-loop governance.

The Purple AI Advantage[1]

63%
Faster to identify security threats

55%
Faster to remediate security threats

338% Return on Investment

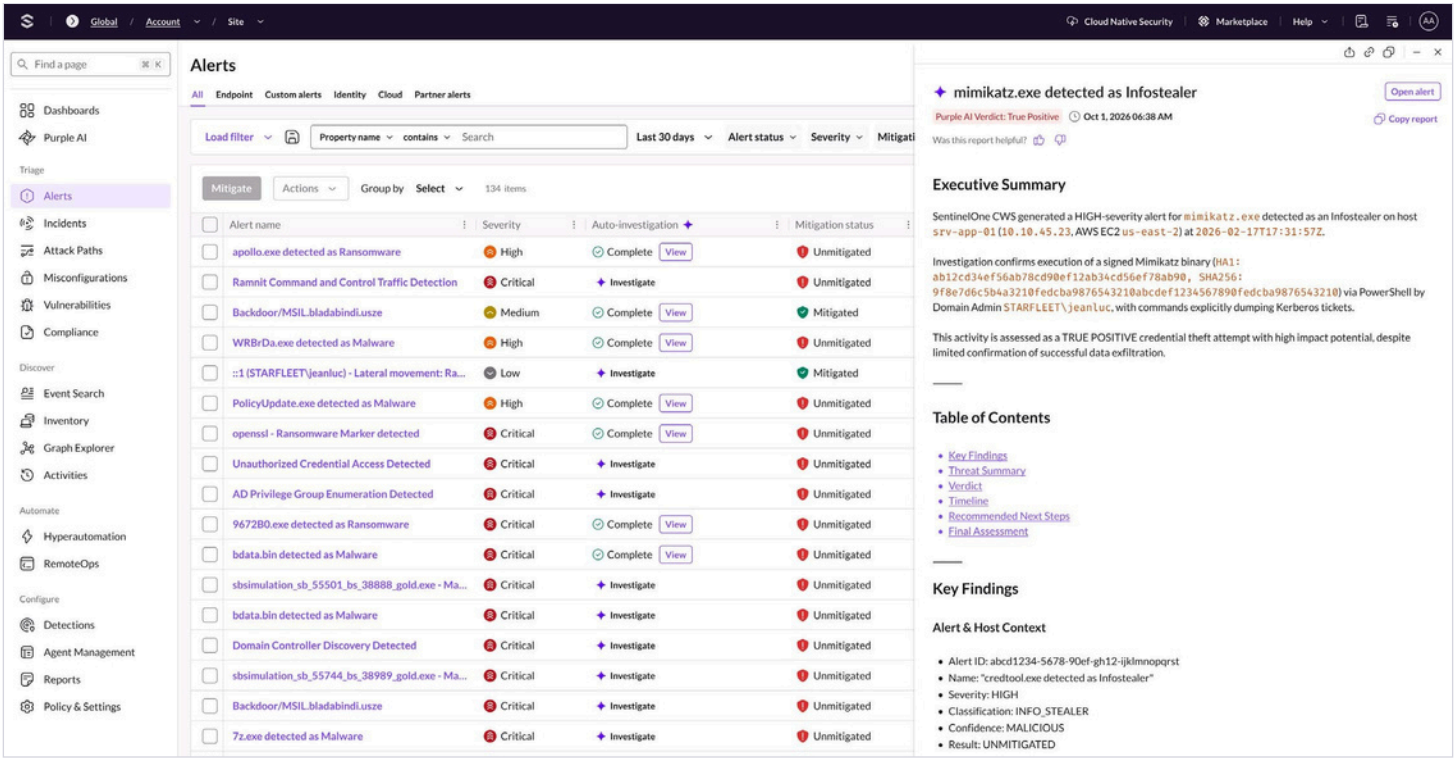
Gartner Peer Insights.

"This product is truly bleeding edge technology that pairs with our security stack to provide the best SOC efficacy and productivity.

★★★★★

IT Security & Risk Management
ENERGY AND UTILITIES

[1] IDC, Business Value of SentinelOne Purple AI (April 2025)



Key Differentiators

Embedded Expertise

Harnessthecollectiveexpertise of SentinelOne's global analyst community to remove triage silos and accelerate MTTR.

Human-Level Reasoning

Advancedagenticreasoningcapabilities that mimic the thought process of a skilled SOC analyst.

Unrivaled Architecture and Speed

Seamless search across nativeand3rd party data, powered by the industry's fastest data lake—5–10x faster than legacy SIEMs.

Security and Privacy by Design

PurpleAIisadvancedAI with responsible, secure foundations—architected with the highest level of safeguards.

Seamless SecOps Workspace

Adedicated AI workbench with shared or private notebooks that auto-save and maintain full investigation context.

Self-Documenting Notebooks

Create auditable,self-documentinginvestigation reports with multi-lingual support.

Open Framework for Agentic Security

Purple AIMCP Serverempowers youto buildand deploy custom AI agents with any LLM, powered by the Singularity Platform.

Human-in-the-Loop Governance

Responses execute onlywithinyourpre-approved policies or explicit authorization. Every action is predictable and auditable.

About SentinelOne

SentinelOne is the world's most advanced cybersecurity platform. The SentinelOne Singularity™ Platform detects, prevents, and responds to cyber-attacks at machine speed, empowering organizations to secure endpoints, cloud workloads, containers, identities, and mobile and network-connected devices with intelligence, speed, accuracy, and simplicity. Over 11,500 customers—including Fortune 10, Fortune 500, and Global 2000 companies, as well as prominent governments—all trust SentinelOne to Secure Tomorrow.