SentinelOne

Purple AI

Your agentic AI security analyst to detect earlier, respond faster, and stay ahead of attacks

Today's security teams face a sophisticated threat landscape and endless alert queues that grow far faster than analysts can hope to resolve. SOC processes are labor-intensive and lead to burnout, missed alerts, and insufficient time for proactive threat hunting. Progressing along the journey toward the Autonomous SOC is the future of cybersecurity, where AI and automation reduce workloads, enhance detection accuracy, and improve response times.

Purple AI, the industry's leading AI security analyst, is designed to support this journey by providing agentic AI that combines reasoning and decision-making to act as a force multiplier for analysts—not just answering questions, but taking informed action to complement human expertise.

Simplify the Complex

Purple AI turns high-volume, fragmented data into actionable insight. Get the broadest visibility across native and third-party data in OCSF, while AI agents analyze threats, prioritize alerts, and surface the most critical issues. Analysts focus on what matters, helping reduce breach risk by 60%.

Amplify Every Analyst

Offload repetitive tasks to AI agents and agentic systems backed by SentinelOne's intelligence and frontline MDR expertise. Analysts can scale investigations with AI-enriched summaries, threat hunting quick starts, guided investigations, and contextual support. Every analyst becomes a force multiplier.

Accelerate Security Operations

From triage to response, Purple AI delivers speed at every step. Auto-triaged alerts, self-documenting notebooks, auto-generated reports, and intelligent next steps help teams resolve threats 55% faster.

Safeguard Your Data

Your security and privacy are protected by design. Purple AI is advanced AI with responsible, secure foundations—architected with the highest level of safeguards. Breathe easy knowing that your data is yours and yours alone.

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

Experience Purple Firsthand

Request a Demo →

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

Key Differentiators

Unmatched Data Visibility

Powered by the industry's fastest data lake—5–10x faster than legacy SIEMs. The only AI security analyst trained on normalized OCSF data for instant querying of telemetry.

Human-Level Reasoning

Advanced agentic reasoning capabilities that mimic the thought process of a skilled SOC analyst to help assess and triage alerts.

Threat Hunting Quickstarts and Guided Investigations

Reduce MTTD with expert-curated hunting workflows and intelligent, contextual next-step suggestions in natural language.

Seamless SecOps Workspace

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

Contextual Interactions

Go beyond Q&A. Engage with Purple AI with context intact, seamlessly integrating intelligence, collaboration, and agentic workflows to accelerate work.

Self-Documenting Notebooks

Create auditable, self-documenting investigation reports with multi-lingual support and fine-grained access controls.

Capabilities

	Purple AI Foundations	Purple AI SOC Analyst
	Included in Complete, Commercial, Enterprise, AI SIEM	Included in Enterprise. Add-On to Complete and Commercial
Natural Language Queries	✓	✓
Threat Hunting Quick Starts	✓	✓
Third Party Data Support with OCSF	✓	✓
Alert Summaries	✓	✓
Event Summaries	✓	✓
Result Summaries	✓	✓
Suggested Follow-Up Questions	✓	✓
Investigation Notebooks	✓	✓
Purple AI for Support	✓	✓
Multilingual Support	✓	✓
AI Similarity Analysis		✓
Community Verdict		✓

Innovative. Trusted. Recognized.

Gartner

A Leader in the 2024 Magic Quadrant for Endpoint Protection Platforms

MITRE ENGENUITY

Industry-leading ATT&CK Evaluation

+ 100% Detections. 88% Less Noise
+ 100% Real-time with Zero Delays
+ Outstanding Analytic Coverage, 5 Years in a Row

Gartner Peer Insights

96% of Gartner Peer Insights™

EDR Reviewers Recommend SentinelOne Singularity

FedRAMP · TEVORA PCI DSS Attestation HIPAA Attestation · AICPA SOC · STAR Level One · VB100 VIRUS · SE Labs Best Innovator Winner 2021 · AAA · Trusted Cloud Provider CSA

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.

sentinelone.com

sales@sentinelone.com
+1 855 868 3733