SINGULARITY ENDPOINT

Autonomus, Next-Gen EPP and EDR

As digital landscapes transform, the speed, sophistication, and scale of threats against endpoints have also evolved. User endpoints remain a key attack vector for malicious actors seeking deeper access to your network. Simultaneously, security analysts are overwhelmed with the sheer number of false positives and alerts, which requires time-consuming manual investigation. Security teams need a more efficient and robust solution to secure every endpoint in their environment.

Singularity Endpoint combines next-gen prevention with real-time detection and response in a single platform with a single agent, empowering security teams to easily identify and secure every user endpoint on their network.

Industry-Leading Endpoint Protection

Deliver unparalleled endpoint protection and detection with broad visibility, rapid response times, and minimal incident dwell time. As evidenced in the 2022 MITRE Engenuity™ ATT&CK® Evaluation, SentinelOne delivered 100% protection and detection with zerodelays and the highest analytic coverage in real-time.

Quickly Contain Attacks With Built-in Automation

Patented Storyline™ technology provides analysts with real-time actionable correlation and context. Analysts can understand the full story of what happened in the environment with automatic linking of all related events and activities together with a unique identifier. Automate response to affected endpoints to reduce the mean time to respond. Autonomously resolve threats with our patented one-click remediation to reverse all unauthorized changes.

Streamlined Security

Investigate, triage, and hunt with zero learning curve to bring IR and hunting to a broader pool of security talent. Uplevel SOC resources for proactive threat hunting with automated hunting rules, intel-driven hunting packs, and support for MITRE ATT&CK techniques. Easy-to- use search and pivot lighten analyst load to hunt across large volumes (up to 3+ years) of EDR telemetry.

Key Benefits

Protect

Protect endpoints in real-time

Detect

Detect threats without human intervention

Respond

Remediate threats with 1-click or automated or response actions

+ AI-based malware and ransomware protection
+ Patented 1-click remediation and rollback
+ Industry-leading coverage for Windows, Mac, and Linux, including legacy OSes
+ Mobile endpoint support for iOS, Android, and ChromeOS
+ Autonomous operation. Works on- and off-network
+ Hunt by MITRE ATT&CK" Technique
+ Flexible EDR data retention up to 3+ years
+ Rapid deployment interoper-ability features ensure a fast, smooth rollout.
+ Single cloud-delivered platform with true multi-tenant capabilities to address the needs of global enterprises and MSSPs

PURPLE

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

Today's security teams are dealing with a sophisticated threat landscape and endless alert queues that grow far faster than what teams can even hope to resolve. It's labor-intensive, precludes any proactive threat hunting, and leads to burnout and missed alerts.

Purple AI is the industry's most advanced AI security analyst that translates natural language into structured queries, summarizes event logs and indicators, guides analysts of all levels through complex investigations with recommended next questions and auto-generated summary emails, and scales collaboration with shared investigation notebooks—ensuring rapid detection, investigation, and response.

Unlike other solutions that act as a console chat bot, Purple AI is a force multiplier that helps analysts conduct faster, better investigations with:

+ One-click threat hunting quick starts based on the latest threat intelligence
+ Intelligent suggested next queries to continue your hunt
+ Lightning fast queries and visibility of native and third party data in a single view
+ Shared investigation notebooks to collaborate across teams
+ Direct answers to Sentinel One support questions so you don't have to search online documentation

Unlock Your Security Team's Full Potential

Simplify the Complex

Streamline investigations by intelligently combining common tools, synthesizing threat intelligence and contextual insights into a single conversational user experience.

Uplevel Every Analyst

Find hidden risk, conduct deeper investigations, and respond faster—all in natural language. Train analysts with power query translations from natural language prompts.

Take Hunts from Hours to Minutes

Accelerate SecOps with our patent-pending hunting quick starts, AI-powered analyses, auto-summaries, and suggested queries. Save time by seamlessly collaborating on investigations in saved and shareable notebooks.

Safeguard Your Data

Leverage a solution designed for data protection and privacy by design. Purple AI is never trained with customer data and is architected with the highest level of safeguards.

The Purple AI Difference

+80%

Faster threat hunting & investigations
as reported by early adopters

Speed & Visibility with One Console, Platform, & Data Lake

Accelerate operations and see the full picture more clearly with one console, one platform, and the industry's most performant data lake. Purple AI is the only AI analyst that understands OCSF logs—so you can instantly query native and partner data in a single normalized view.

Threat Hunting Quickstarts & Guided Investigations

Help every analyst reduce MTTD and proactively find risk with our patent-pending hunting quick starts library. Leverage intelligent, contextually-suggested next queries to continue investigations in natural language.

Accelerate Collaboration Across the Board

Auto-generate threat summaries, reports, and communications that can be shared across teams and cut down on unnecessary back
and forth by collaborating in saved, shared, and editable notebooks.

Open & Reliable AI

AI shouldn't be a black box.
With Purple AI, you can easily view query translations for verification and analyst training. Purple AI is also carefully architected with guardrails that protect against misuse and hallucinations.

Key Features

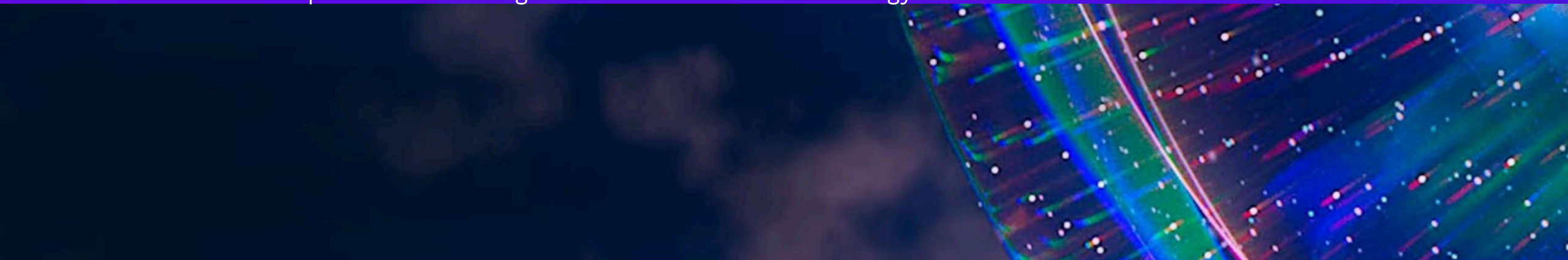
- Translate natural language into structured PowerQueries to search for hidden risk. Get outcomes you can trust with full views of queries and summarized results in natural language.
- Patent-Pending Threat Hunting Quickstarts enable analysts to proactively hunt for threats with a single click, using pre-populated queries based on our leading threat intelligence.
- Lightning fast queries and greater visibility. Built on top of the Singularity Data Lake, Purple AI is the only GenAI analyst that supports the Open CyberSecurity Schema Framework (OCSF) to provide native and third party data in a single normalized view.
- Conduct deeper investigations with suggested, contextual follow-on queries.
- Surface actionable insights faster with AI-powered threat analyses and summaries.
- Refer back to auto-saved private investigations notebooks or boost collaboration on hunts across teams in shared notebooks.

SINGULARITY XDR

Extend Protection, Detection, and Remediation to Endpoint and Beyond

The cybersecurity threat landscape is evolving exponentially in both speed and scope. Meanwhile, most security teams struggle to keep pace with emerging threats with the resources they have at hand. These organizations often lack global visibility and context across their technology stacks, creating gaps in what they can see and detect. Simultaneously, analysts juggle point tools for each vector, forcing them to analyze data in isolation and manually investigate. Today's security teams need a more proactive solution to identify, contain, and remediate emerging threats.

SentinelOne Singularity XDR unifies and extends detection and response capabilities across multiple security layers, including endpoint, cloud, identity, network, and mobile, providing security teams with centralized end-to-end enterprise visibility, powerful analytics, and automated response across a large cross-section of the technology stack.



Comprehensive Coverage Across Your Enterprise Stack With Operational Simplicity

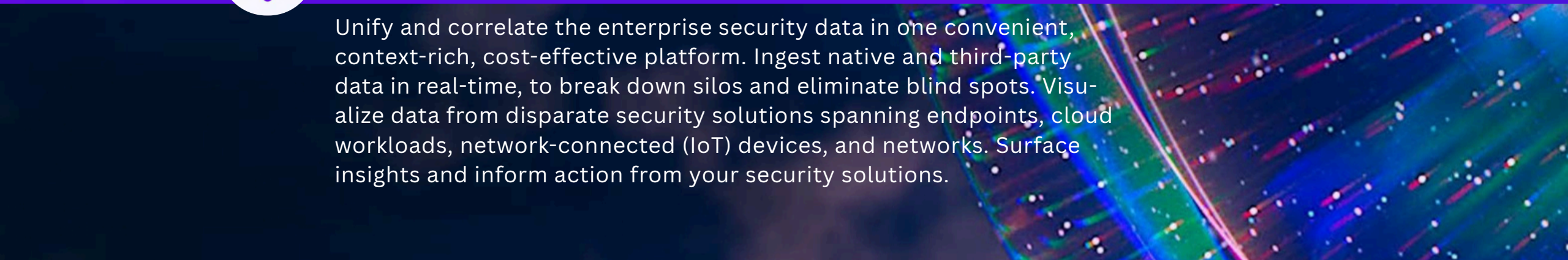
Deliver native protection across multiple solutions, including endpoint, cloud, identity, mobile, and devices. It enables frictionless third-party integrations, including threat intelligence, SIEM, SOAR, email, SASE, sandbox, and more, enabling you to leverage your existing investments.

Increased Security Team Efficiency

Auto-correlate individual events into an attack sequence, to streamline investigation and response. Analysts can automatically resolve threats with one click, without scripting across the estate. Execute orchestrated remediation actions in a single step, including network quarantine, auto-deploy agents on unprotected workstations, or automate policy enforcement across cloud environments.

Streamline Security Workflows Powered by a Unified Data Store

Unify and correlate the enterprise security data in one convenient, context-rich, cost-effective platform. Ingest native and third-party data in real-time, to break down silos and eliminate blind spots. Visualize data from disparate security solutions spanning endpoints, cloud workloads, network-connected (IoT) devices, and networks. Surface insights and inform action from your security solutions.



Key Benefits

See

Maximize visibility across every corner of the enterprise

Protect

Protection coverage with unrivaled speed, efficiency, and simplicity

Resolve

Automate response across the entire connected security ecosystem with a single click

+ Streamline operations andsecurity workflows
+ Reduce mean time to respond with simple, fast, and relevant automation
+ Up-level analyst productivity
+ Accelerate time to value for security analysts
+ Combine native and open XDR to offer customers the flexibility they need without limiting them to one solution multi-tenant capabilities to address the needs of global enterprises and MSSPs