GLOBAL SUBSCRIPTION CATALYST

GS Catalyst for SentinelOne

SentinelOne Singularity Complete

Get SentinelOne Products Here

Phones
Office : +62-21 5088 6328
Email
admin@gscatalyst.com

GS Catalyst - SentinelOne Official Partner in Indonesia

GLOBAL SUBSCRIPTION CATALYST

Planning and Assessment

Strategic planning, alignment of goals - business metrics baseline, deployment of resources with Professional Services Consultant

Training

Provide comprehensive training for IT teams on how to use SentinelOne products and integrate them into their daily operations.

Implementation

Implementation of SentinelOne products with certified Professional Services team

Managed Services

24/7 Managed Services help customers with proactive monitoring, incident response, and ongoing optimization

Why choose GS Catalyst to deliver SentinelOne?

Implementation & Migration Services

Smooth implementation process and migration from existing systems.

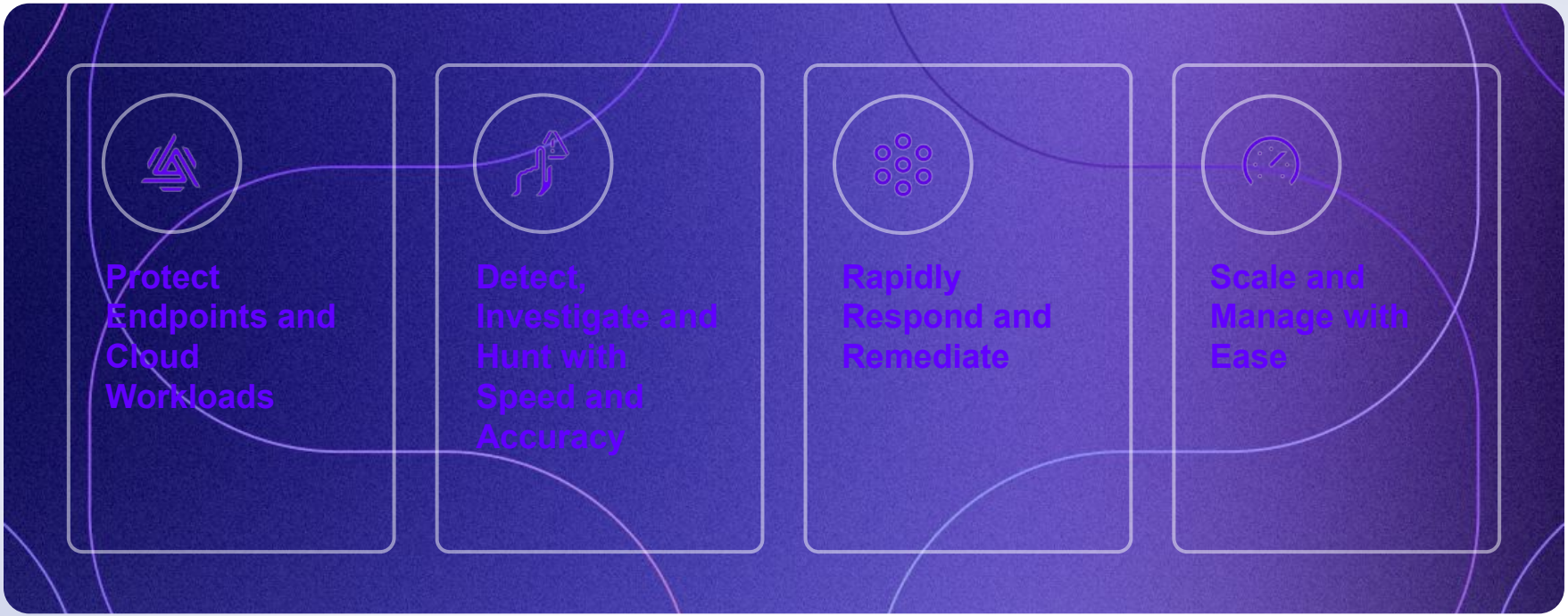
More than 60+ Certified Engineers

Our team of certified engineers brings deep knowledge to manage your directory services

Have Strong Portfolio for Cloud Solution

Designed from the ground up for the cloud, we deliver optimal performance and scalability.

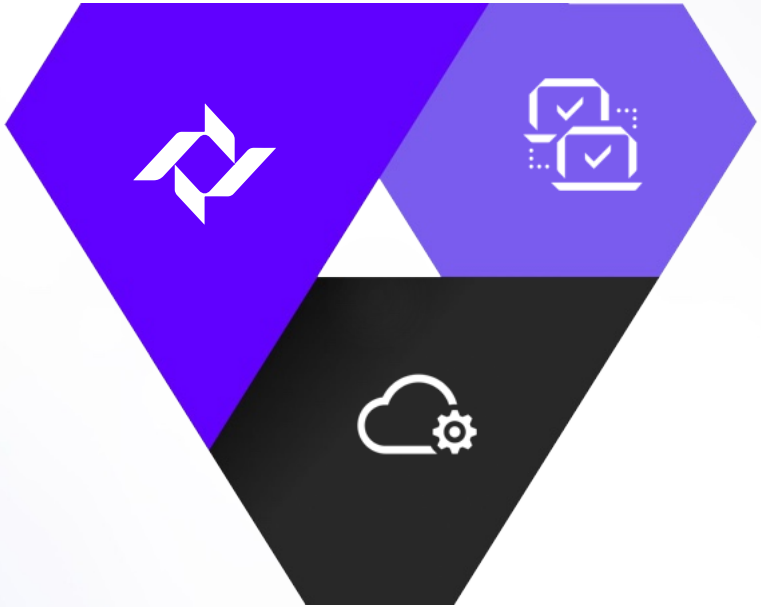
Integrate AI To Empower Security Teams



Singularity Complete

Purple AI

Radically accelerate threat hunting and investigation with an AI security analyst



Endpoint security

Get comprehensive protection and defend against endpoint and identity-based attacks

Cloud workload security

AI-based workload protection against runtime attacks for servers, cloud VMs, and containers across public, private, and hybrid clouds

The Singularity Complete Difference

Unified Agent

Single, resource-efficient agent that incorporates endpoint, identity, and cloud and delivers streamlined capabilities and administration through a shared agent and interface

Behavioral AI Models

Superior behavioral and static AI models that accurately detect suspicious and malicious patterns in real time on servers, workstations and workloads

Purple AI

Purple AI is the industry's most advanced AI security analyst and the only solution built on a single platform, console, and data lake

Storyline Technology

Storyline automatically correlates telemetry data from endpoints, cloud workloads, and identity sources to create a detailed, visual "story" of the events

1-Click Rollback

Remediate all affected endpoints with one-click remediation and rollback

Comprehensive Support

Best-in-industry coverage for Windows, macOS, Linux, and cloud workloads within AWS, GCP, Azure, or private clouds

Singularity Packages

Pricing and Packaging Page	Singularity Core	Singularity Control	Singularity Complete	Singularity Commercial	Singularity Enterprise
Endpoint Protection (EPP)					
Advanced EPP with device control					
Autonomous Prevention, Detection, and Response					
Cloud Workload Protection Platform					
Extended Detection and Response					
Purple AI Foundations					
Purple AI SOC Analyst			Add-On	Add-On	
Data Retention			14 day	90 day	90 day
Managed Threat Hunting					
Identity Threat Detection and Response					
Managed Detection and Response				Add-On	Add-On
Network Discovery					
Forensic Data Collection					
Guided Onboarding and Deployment Advisory					
Training Services					

Licensing

Singularity Complete License Matrix				
Solution	**Meter**	**Product Group**	**Capability**	**Note**
Endpoint Security	Workstation	Complete	EPP/EDR	User device security
Cloud Security	Server	Cloud Server	CWS	OS level security
Cloud Security	Pod or Task	Serverless Container	CWS	Functions and code security
Cloud Security	Container Host	Cloud Container	CWS	K8/Docker security-cloud/on-premises

Singularity Complete Use Cases

Protect Endpoints and Cloud Workloads

Improve Visibility

Unified agent with the industry's best OS and cloud workload coverage, and advanced telemetry collection

Prevent Malware

Autonomous, machine speed prevention powered by on-device AI

Reduce The Attack Surface

Continuous visibility to reduce your attack surface and minimize the risk of compromise

Detect, Investigate and **Hunt** with Speed and Accuracy

Detect Ransomware & Zero Days

Correlate atomic events and map adversary behavior with Behavioral AI

Detect Container Drift

Detect drift within immutable containers and flag malicious actions without false positives

Augment Threat Hunting & Investigation

Threat hunting and investigation at scale with Purple AI natural language hunting and summaries

Rapidly **Respond** and **Remediate**

Automate Incident Response

Automate with policy or use remediation actions including patented 1-click Rollback

Scale and **Manage** with Ease

Optimize Operations

Automate deployment of a resource-efficient user space agent. Get support 24/7 with an always-on interactive AI support agent

Singularity Endpoint

Endpoint Security Has Evolved

Attackers are using AI and moving at machine speed

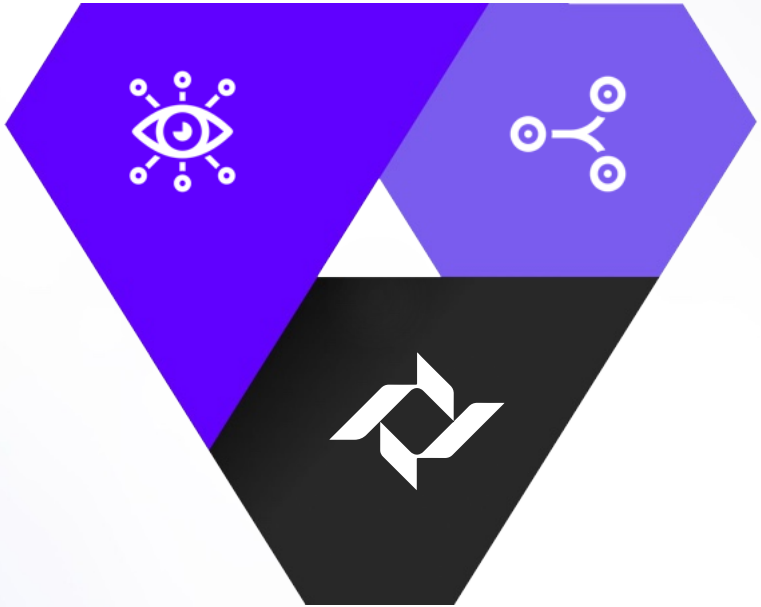
There is a convergence of endpoints and identities

Teams must do more with less despite expanded scope and complexities

SentinelOne Moves Beyond the Endpoint

AI-Powered Detections

Use superior behavioral AI models to accurately detect suspicious and malicious patterns in real time



Unified Agent & Correlation

Get comprehensive protection against endpoint and identity-based attacks with a single platform

AI-Fueled Speed

Radically accelerate triage, investigation, threat hunting and response with Purple AI

Singularity Endpoint:
Your AI-Powered First Line of Defense

Purple AI

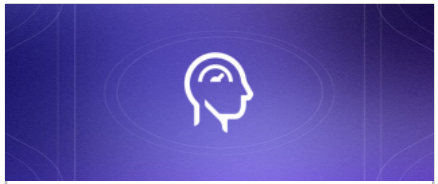
Your AI security analyst that enables autonomous security operations to maximize the power of security teams.
Detect earlier, respond faster, and stay ahead of attacks.

Simplify the Complex

Threat hunt & investigate, in natural language.

Get lightning fast querying on first and third party data.

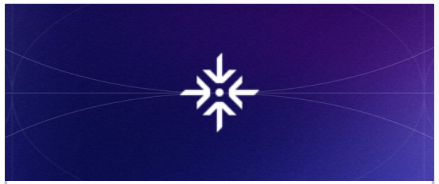
Get interactive support in natural language.



Amplify Every Analyst

Maximize the impact of every analyst with quick starts and auto-summaries.

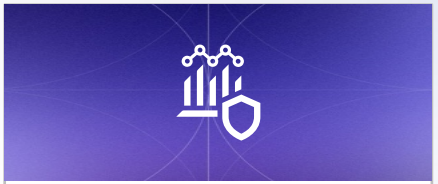
Easily generate reports and emails to accelerate communications.



Accelerate SecOps

Advance hunting and investigations. Get AI analyses, summaries, and next steps.

Use shareable investigation notebooks that seamlessly integrate into your workflows.



Safeguard Your Data

Designed to protect your data and privacy.

Purple AI is architected with the highest level of safeguards that protect against misuse and hallucinations.

Unmatched protection, detection and visibility

Protect against malware

See endpoint and identity alerts

Detect ransomware with AI behavioral models

Customize threat hunting

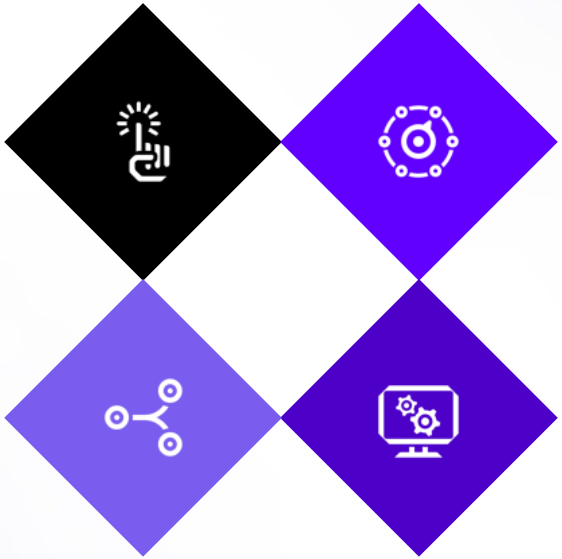
Get deep visibility

Get real-time updates for emerging threats

Lightning-fast response and remediation

Remediate using 1-click rollback

Correlate & prioritize alerts



Visualize attacks with Storyline

Automate response actions

A lightweight, unified agent

Combine endpoint & identity

Unparalleled OS support

Secure by design

Cloud-delivered content

Controlled updates

Anti-tampering measures

The Singularity Endpoint Difference

Unified Agent

Single, resource-efficient agent that incorporates Identity and delivers streamlined capabilities and administration through a shared agent and interface

Behavioral AI Models

Superior behavioral and static AI models that accurately detect suspicious and malicious patterns in real time on servers, workstations and workloads

Purple AI

Purple AI is the industry's most advanced AI security analyst and the only solution built on a single platform, console, and data lake

Storyline Technology

Storyline automatically correlates telemetry data from endpoints, cloud workloads, and identity sources to create a detailed, visual "story" of the events

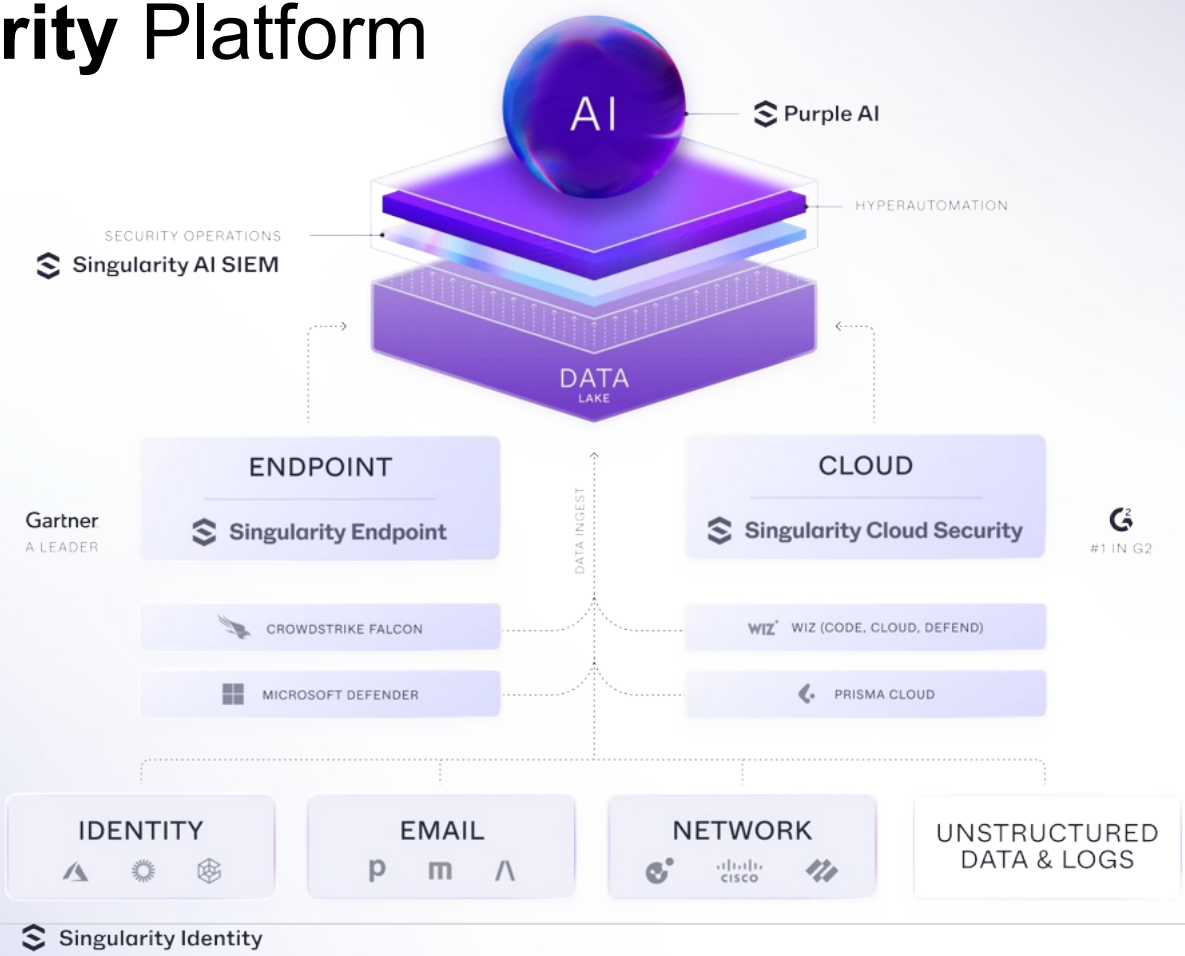
1-Click Rollback

Remediate all affected endpoints with one-click remediation and rollback

OS Coverage

Best-in-industry coverage across Windows, macOS and Linux operating systems

Singularity Platform



Why SentinelOne?

Gartner Peer Insights™

Recognized as a Customers' Choice

4.7 out of 5 stars based on 575 ratings for Endpoint Protection Platforms,

Leader for CNAPP with 98% willingness to recommend

Gartner Magic Quadrant

A Leader. Four Years Running.

A Leader in the 2024 Magic Quadrant™ for Endpoint Protection Programs

MITRE ENGENUITY

Record Breaking ATT&CK Evaluation

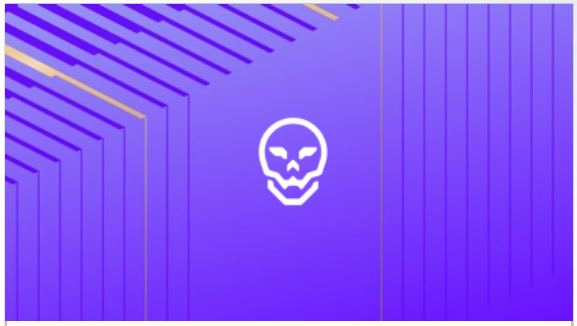
AI-Powered Protection.
100% Detection, 100% Real Time
#1 Ranked on MITRE

Singularity Cloud Security

Security Teams Face Hard Realities Balancing Priorities

Internal

Inefficiencies across people, processes & technology against a drive for innovation



External

Evolving cloud threat landscape and financially motivated threat actors

Cloud Workload Security Overview

AI-powered, real-time threat detection and protection

Generally Available

Servers & VMs

Real-time AI-powered detection and protection for Linux and Windows Servers; public cloud, private cloud, and physical server support.

Containers

Various runtimes; self-managed k8s; managed cloud services like GKE, AKE, ECS, and EKS.

Serverless Containers

Support for AWS Fargate for EKS and more to come.

Cloud Workload Security

Detection and Response

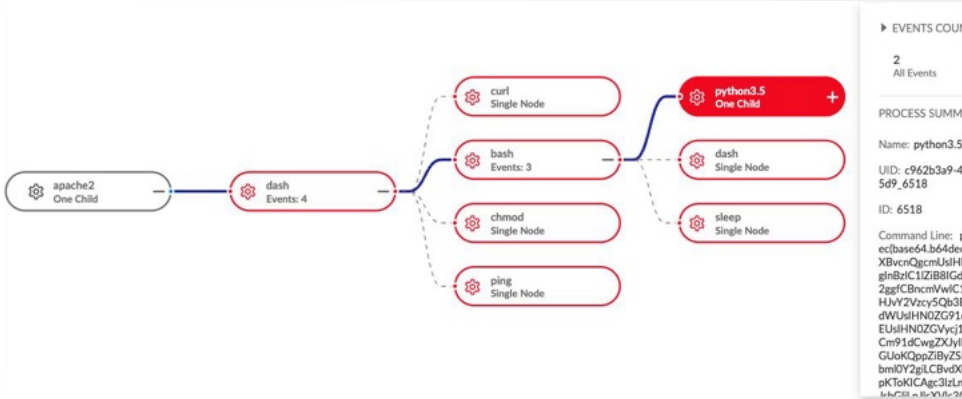
Real-time detection and machine-speed response to runtime threats. Auto remediation. Protect and Detect modes.

Hunting and Forensics

Unified data lake for SentinelOne and partner logs via OCSF. AI-powered insights streamline investigations and IR, fuel threat hunts

Stability and Performance

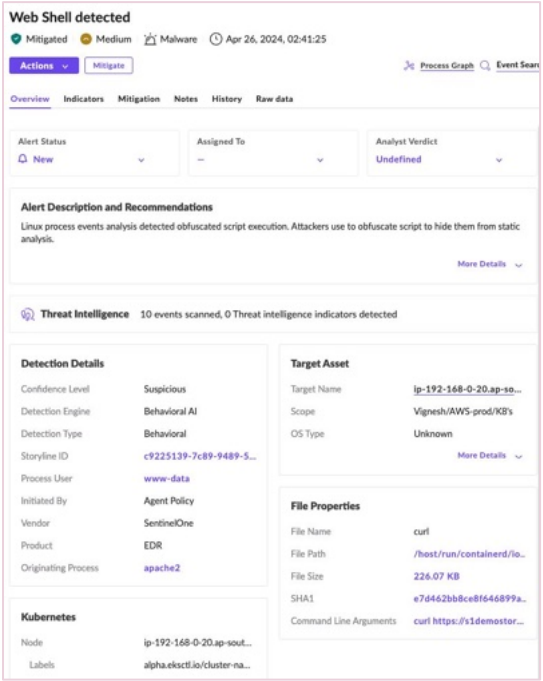
Accelerate innovation with runtime security that does not get in the way. No kernel dependencies. Low CPU and memory usage.



Cloud Workload Security

Unleash AI-powered runtime threat protection

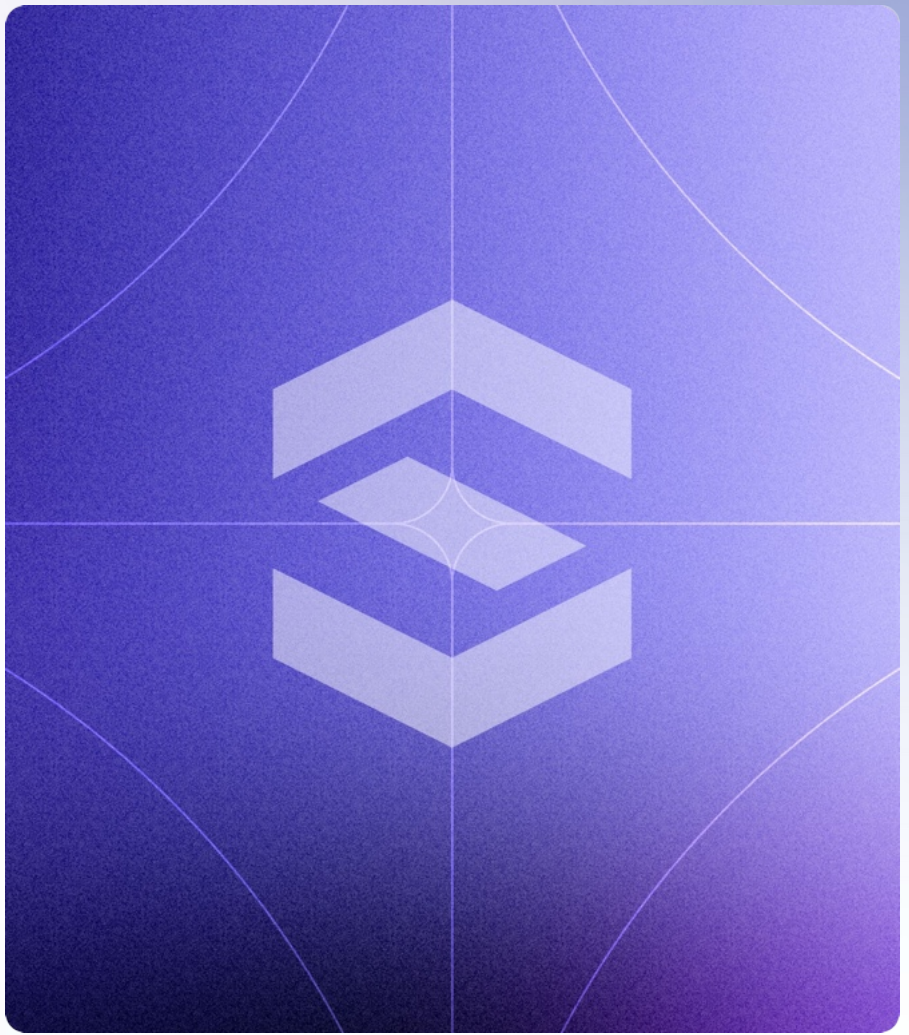
- **High performance, low overhead, stable and scalable agent**
- **Easy to deploy eBPF architecture that runs in user space**
- **No kernel dependency hassles**
- Support for 17 Linux distros and 20 yrs of Windows versions
- Real-time, AI-powered CWPP, to detect and block threats at runtime



Purple AI

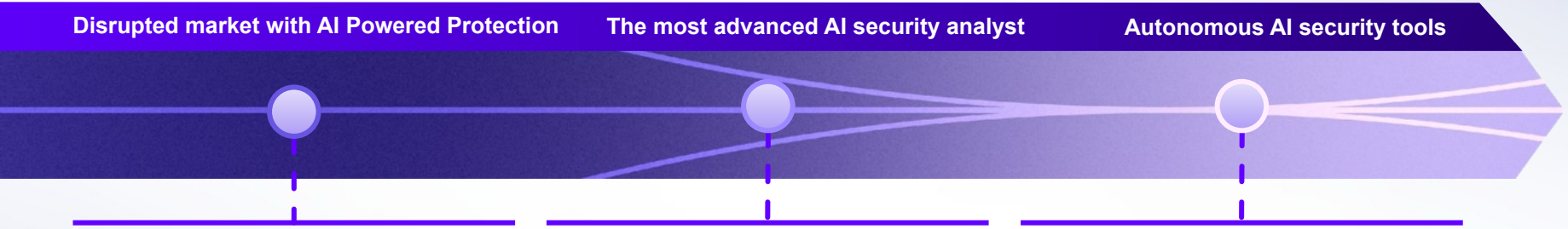
Purple AI

SentinelOne



Built on a history of AI innovation in security

Enabling security teams to work smarter and faster to stay protected



Ransomware Protection with Automated Remediation

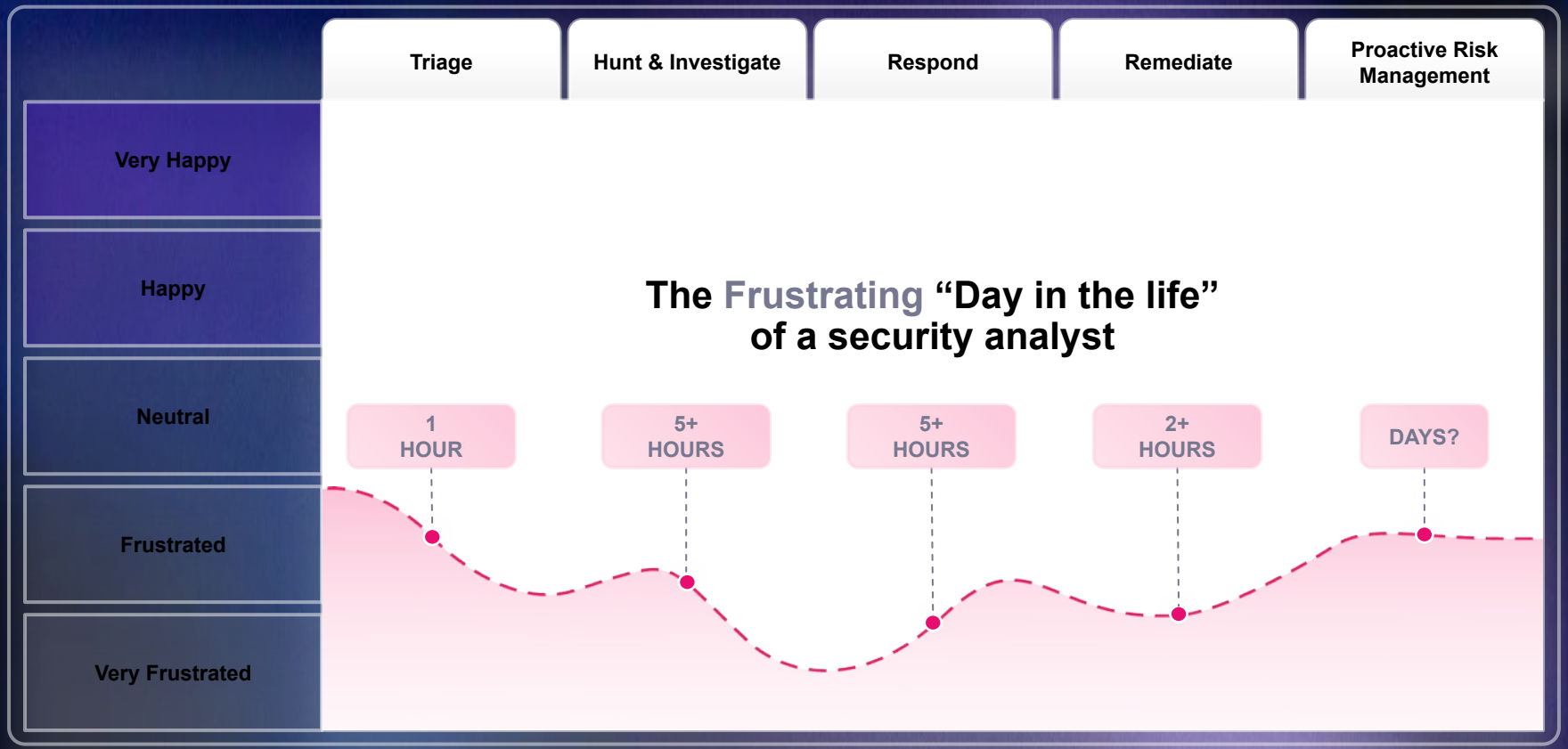
Leveraging AI-powered detections + Storyline technology to automatically kill and quarantine and rollback changes made by malicious actors.

Purple AI: Accelerating SecOps

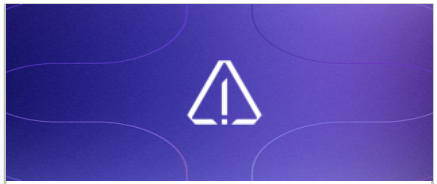
Intelligent hunting, investigation, and support assistance powered by GenAI.

Purple AI: Autonomous Security

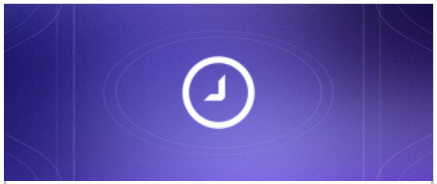
Auto-triage. Auto-investigations. AI Hyper Automation. Automate manual work.


Triage
Hunt & Investigate
Respond
Remediate
Proactive Risk Management
Very Happy
Happy
Neutral
Frustrated
Very Frustrated
The Frustrating “Day in the life” of a security analyst
1 HOUR
5+ HOURS
5+ HOURS
2+ HOURS
DAYS?

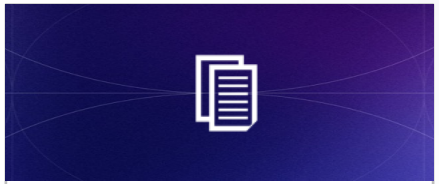
Current Security Operations Challenges



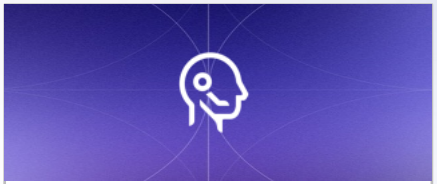
Long alert queues
require thousands of investigation hours and lead to analyst burnout.



Not enough time
for proactive threat hunting to catch risk.



Laborious
evidence documentation, analyses, reporting, and communication.



Talent shortage
and need for advanced hunting skills to proactively secure.

Purple AI

Your AI security analyst that enables autonomous security operations to maximize the power of security teams.

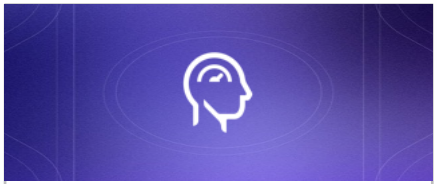
Detect earlier, respond faster, and stay ahead of attacks.

Simplify the Complex

Threat hunt & investigate, in natural language.

Get lightning fast querying on first and third party data.

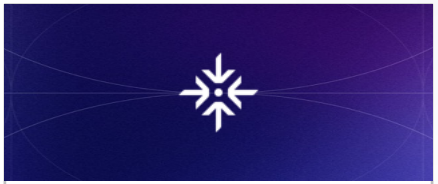
Get interactive support in natural language.



Amplify Every Analyst

Maximize the impact of every analyst with quick starts and auto-summaries.

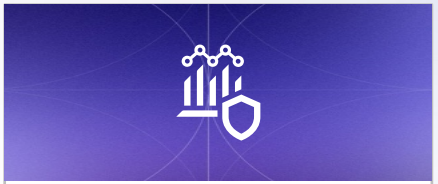
Easily generate reports and emails to accelerate communications.



Accelerate SecOps

Advance hunting and investigations. Get AI analyses, summaries, and next steps.

Use shareable investigation notebooks that seamlessly integrate into your workflows.



Safeguard Your Data

Designed to protect your data and privacy.

Purple AI is architected with the highest level of safeguards that protect against misuse and hallucinations.


NATIVE DATA
AI SIEM
Endpoint & Identity
Cloud
Exposure Management
Services
Singularity™ Platform
SUPERCHARGED BY Purple^ai
Singularity Data Lake
SECURITY & LOG ANALYTICS
INGEST DATA FROM ANY SOURCE
IDENTITY
EMAIL
CASB
SASE
WEB
THREAT INTEL
SANDBOX
FIREWALL
CASE MGMT
LOG INGEST

80%

Faster threat hunting and investigations, as reported by early adopters

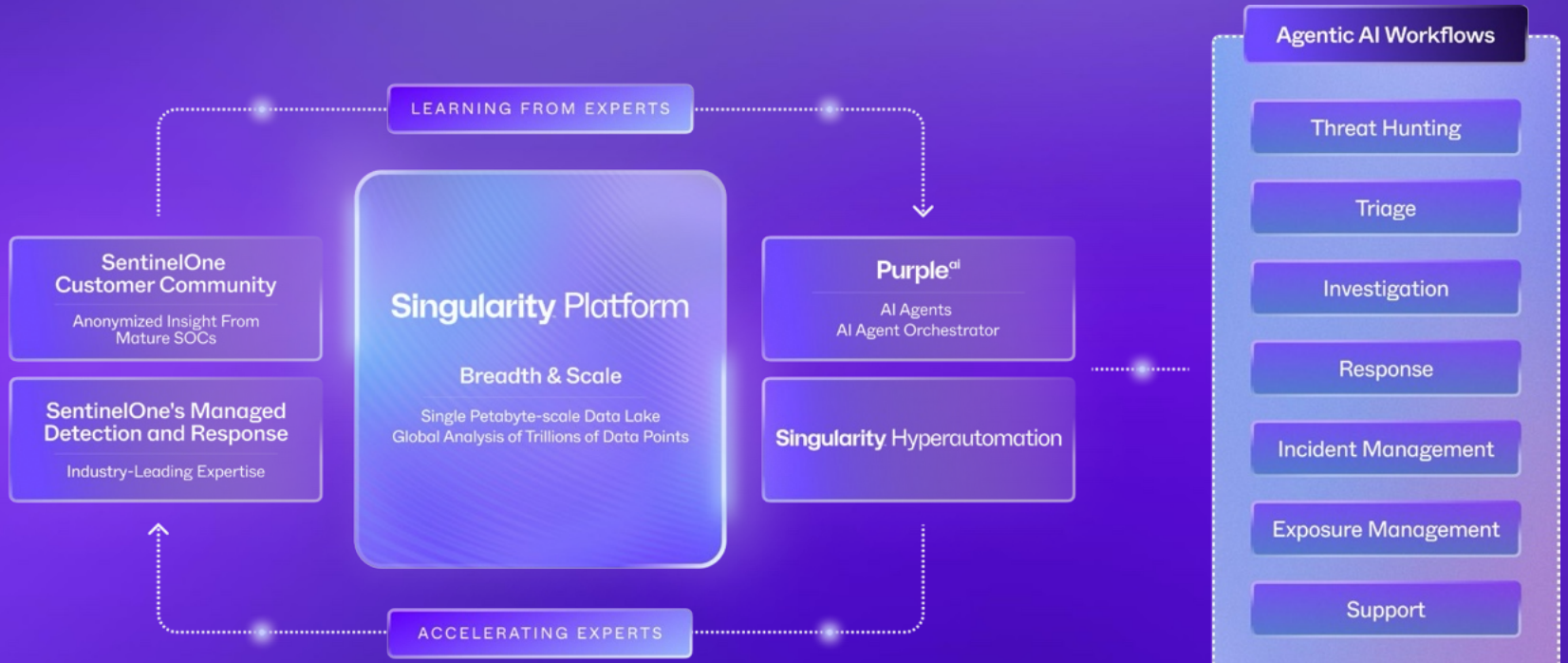
128%

Easier threat hunting, as reported by early adopters

78%

of surveyed early adopters found the notebooks feature either very or extremely helpful

SentinelOne's Agentic AI



The Power of Purple AI's Automation

Mortal vs. Machine Challenge: Our PowerQuery expert vs. Analyst with Purple AI

Place	Player	Score	Flags	Hints	Incorrect Answers	Penalties	% Complete	Last Capture	Time Since Capture
1		10300	33	0	4	0	32.35	3/8/2024 10:50:16 AM	2 days 23 hours 59 mins 12 seconds
2		4780	38	0	6	1	37.25	3/8/2024 10:46:31 AM	3 days 2 mins 57 seconds
3		3700	37	0	2	0	36.27	3/8/2024 10:51:02 AM	
4		3660	37	0	6	2	36.27	3/8/2024 10:49:04 AM	
5		3340	34	0	14	3	33.33	3/8/2024 10:48:47 AM	3 days 41 seconds
6		2660	27	0	5	2	26.47	3/8/2024 10:50:28 AM	2 days 23 hours 59 mins
7		2540	26	0	21	3	25.49	3/8/2024 [illegible] AM	

Analysts *with* Purple AI ranked 1st to 6th

PowerQuery expert *without* Purple AI finished 7th

Purple AI helps every level of analyst to be significantly faster.

"The AI is very fast at finding and knowing what fields to include, versus [my] manual lookups."

Reactions to the ThreatOps challenge

1 of the players had very limited experience with the console and was able to get 2nd place beating their 2 seasoned console users.

Customer feedback was very positive. Including one very experienced Threat Hunter who finished the game then went back in to the console and went "off script". He was blown away that he could actually use some of his typical hunts.

The Purple^ai Difference

Lightning Fast Queries

Built on the most performant data lake in the market to work **5-10x faster.**

Hunting Quick Starts

Help analysts proactively hunt for threats with the latest pre-populated.

Self-documenting Investigation Notebooks

Auditable and shareable with access control to collaborate across the team.

Query Breadth

The only GenAI that supports OCSF data so you can instantly query SentinelOne and partner data in a normalized view.

Accelerate Communication and Reporting

Generate professional emails and summaries.

Contextual Interactions

Go beyond a simple question and answer and interact with Purple with context intact without needing to repeat prompts.

Purple ai

Hunting and Investigation

- Natural language queries
- Hunting Quick Starts
- Automatic natural language summaries of results and events
- Suggested follow-up questions

80%
Easier

128%
Faster

Just ask Purple

Am I being targeted by FIN12?

Find possible Okta MFA fatigue attacks.

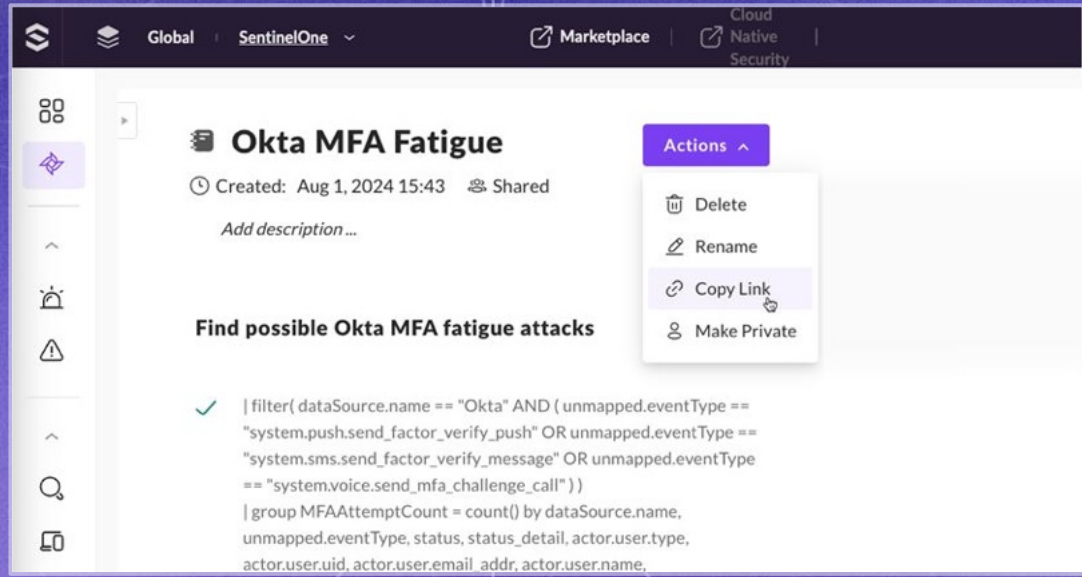
Purple ai

Self-documenting investigation notebooks

- Self-documenting
- Auditable
- Shareable
- Easy to understand with plain language inputs and outputs
- Used by teams for knowledge-amplification

97%
Found notebooks useful

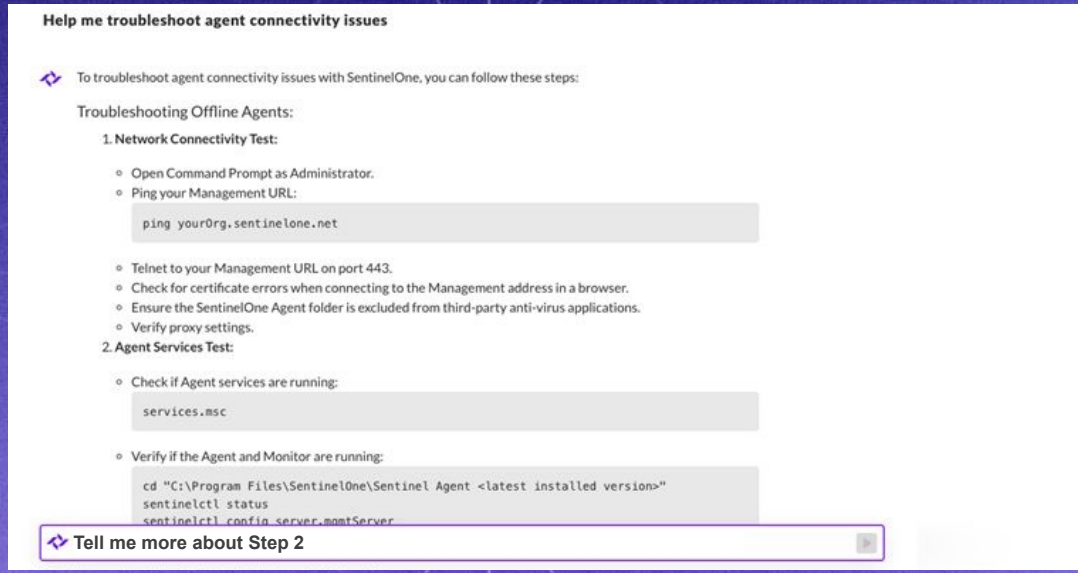
76%
Very or extremely useful



Purple ai

Interactive Support

- Ask support questions interactively
- Ask contextual follow-up questions
- Summarizes responses from multiple help documents



Early Access

Purple ai

Multilingual Questions

- Reduce hunting and investigation time with natural language questions in your native language

Data protection and privacy by design

Our models do not train on your security data. We ensure your data is protected.

Purple AI **does not use your queries to improve its models**, unless you flag a Purple response for review, feedback or support.

Purple interacts with existing SentinelOne Singularity Data Lake technology and stores your data in the same way.

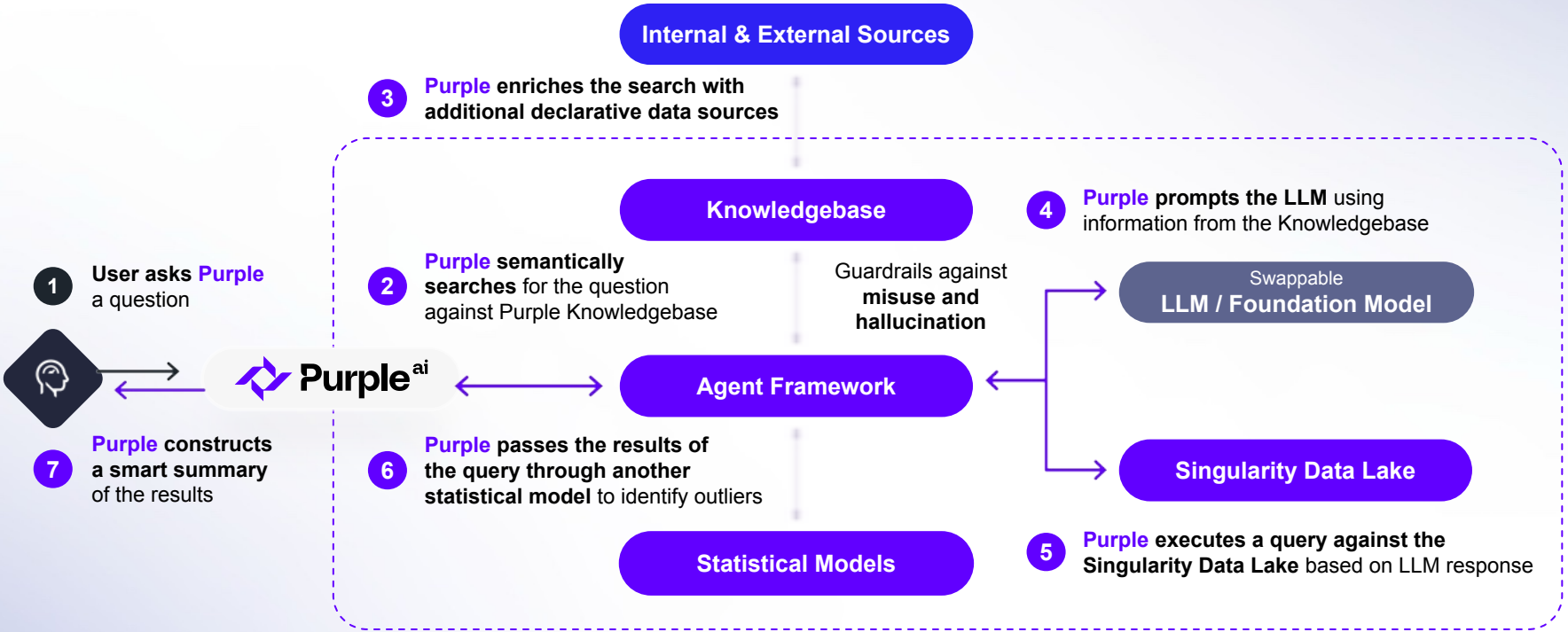
Purple's architecture protects against LLM-related attacks.

This means the scope of data processing activities you and SentinelOne agreed to have not changed.

Purple AI prompts based on your requests and the returned completions will:

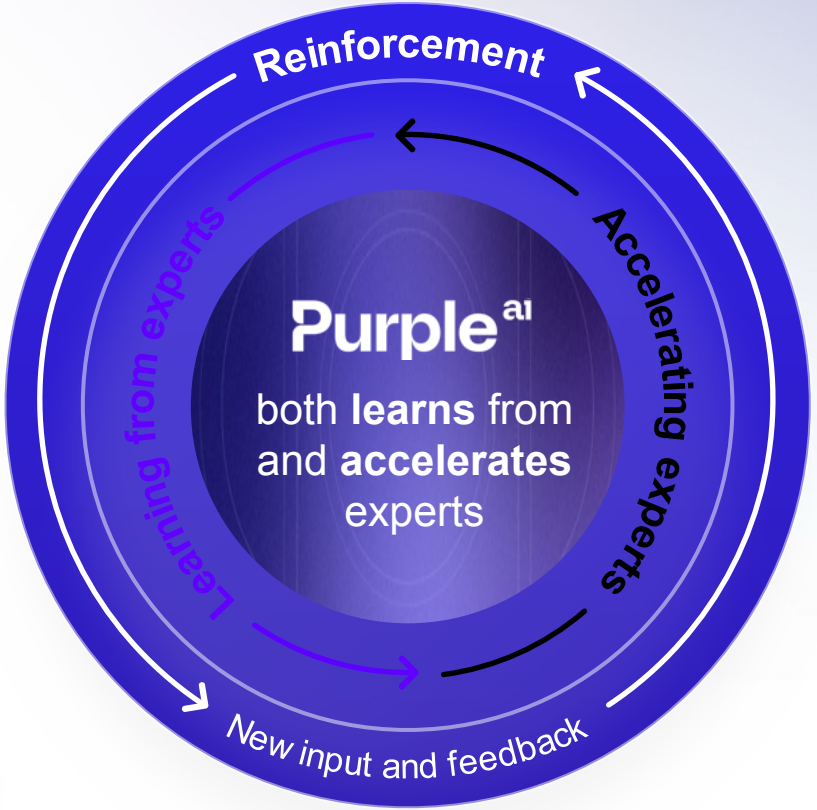
- **NOT** be available to any other customers
- **NOT** be used to improve subprocessor's models
- **NOT** be used to improve any other 3rd party products or services
- **NOT** be permanently retained

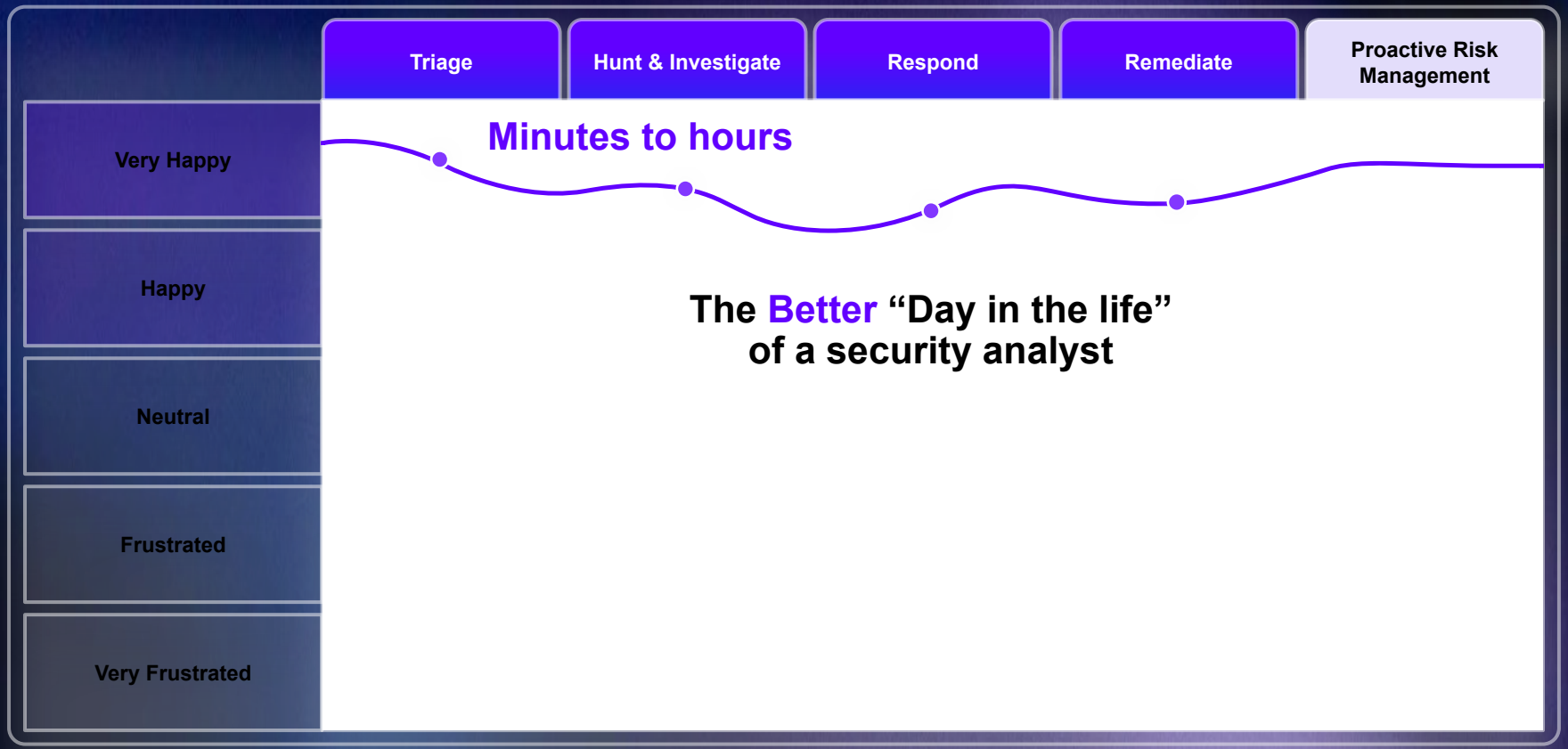
Purple ai Reference Architecture



MDR Expertise and AI in Harmony

Virtuous Cycle: Accelerating detection and response




Triage
Hunt & Investigate
Respond
Remediate
Proactive Risk Management
Very Happy
Happy
Neutral
Frustrated
Very Frustrated
Minutes to hours
The Better “Day in the life” of a security analyst

Autonomous SOC Maturity Model

Purple[ai] Strategy

Empower every analyst to detect earlier, respond faster, and stay ahead of attacks.

SecOps Analyst

Help guide analysts through hunts and investigations

Support and Configuration Assistance

Answer support questions in natural language and help guide sysadmins through common configuration tasks

Auto-Triage

Automate the steps teams go through to determine if an alert needs further investigation

Auto-Investigation

Automate the investigation steps analysts go through for an alert, collecting relevant evidence

Thank You

Get SentinelOne Products Here

Phones
Office : +62-21 5088 6328

Email
admin@gscatalyst.com

Address
Menara Caraka, 7th Floor Jl. Mega Kunigan Barat No.1
Kuningan Timur, Jakarta Selatan, 12950