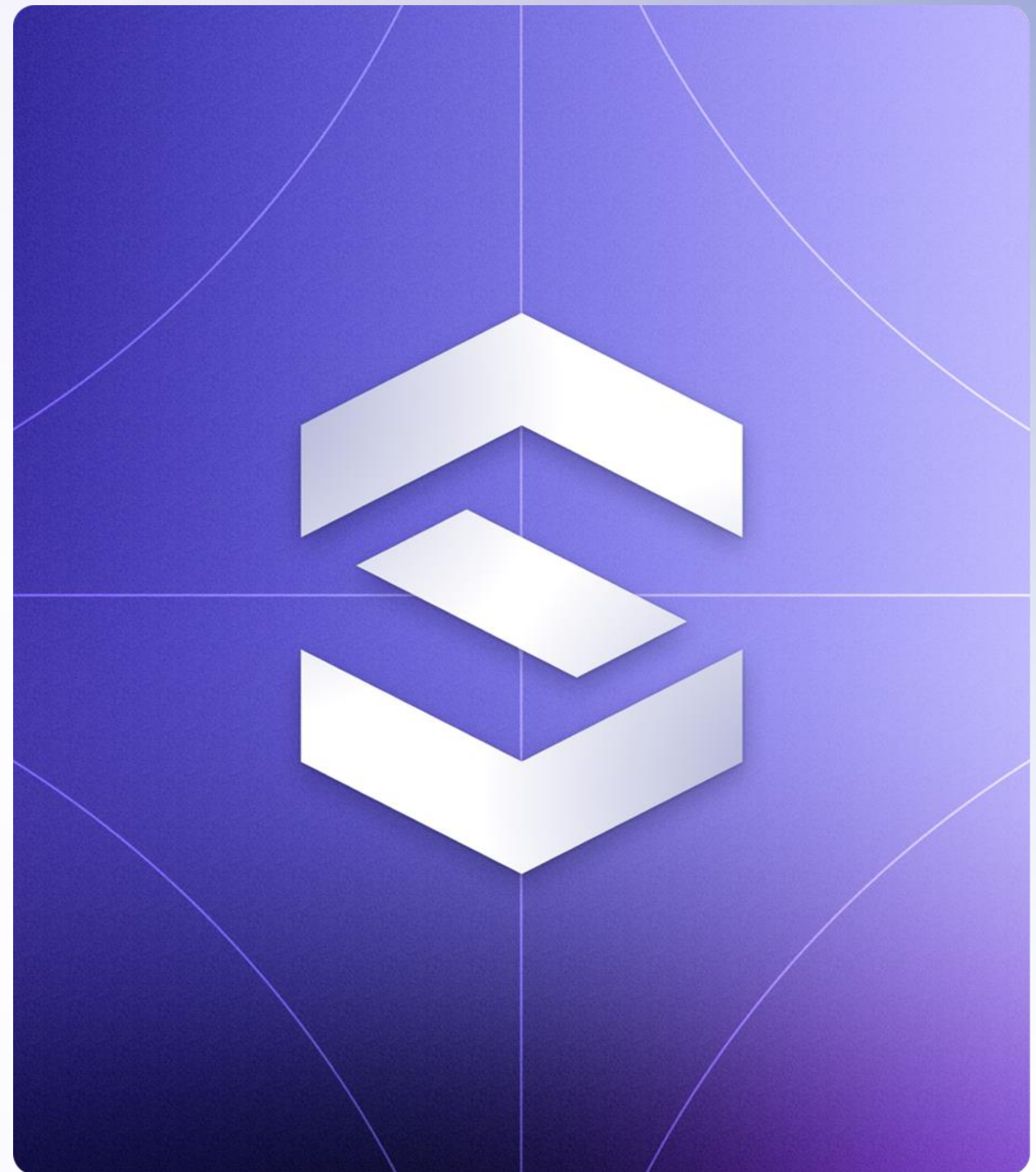


# Singularity™

## AI Cybersecurity Platform

**Lubos Chovan**  
Solutions Engineer



# Singularity Endpoint

## Industry-Leading EPP/EDR

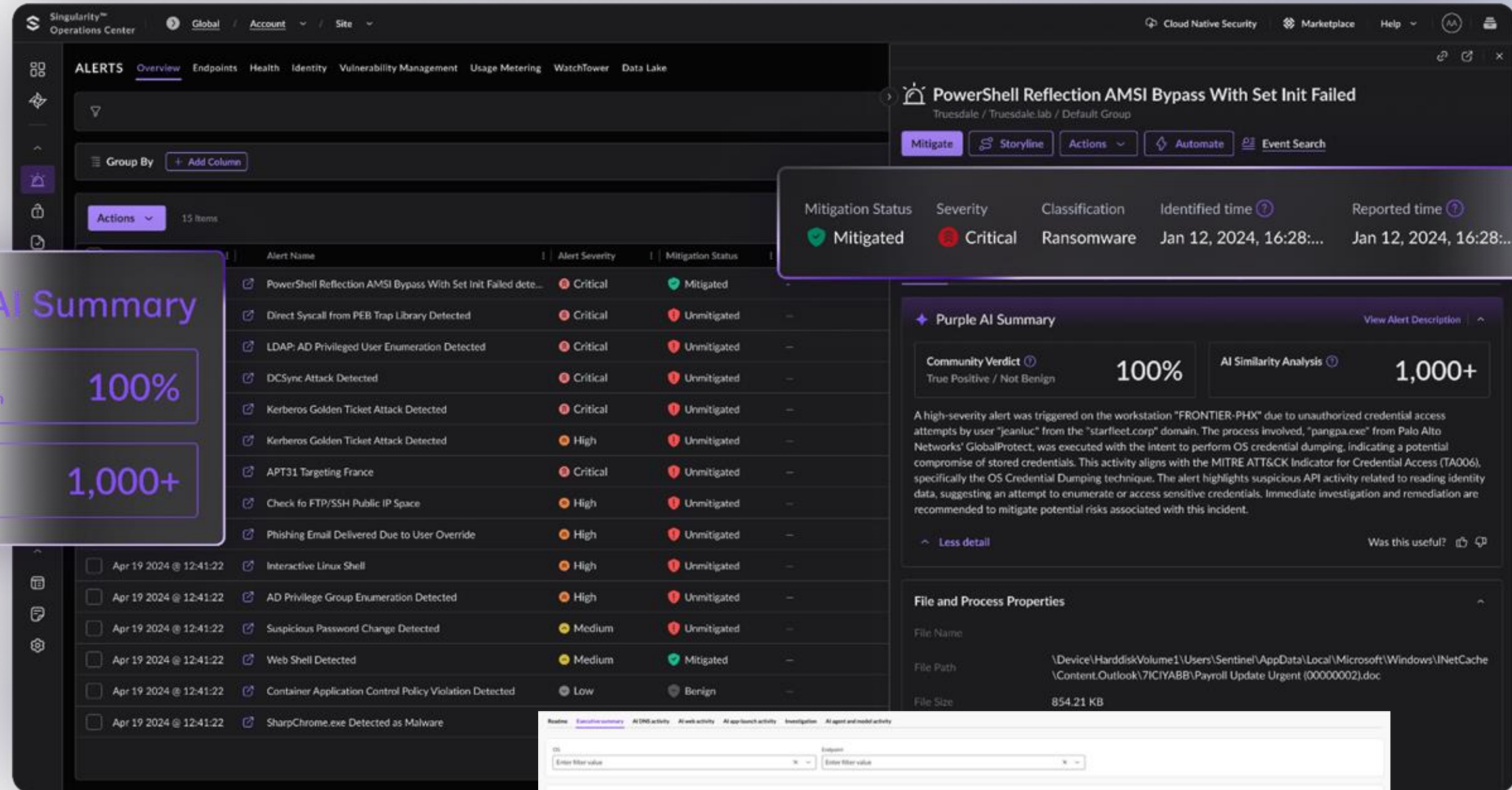
Fastest MTTR with highest accuracy. Free up resources to investigate what really matters.

## Streamlined Security

Single pane of glass. Improved security posture. Increased SOC efficiency driven by automation.

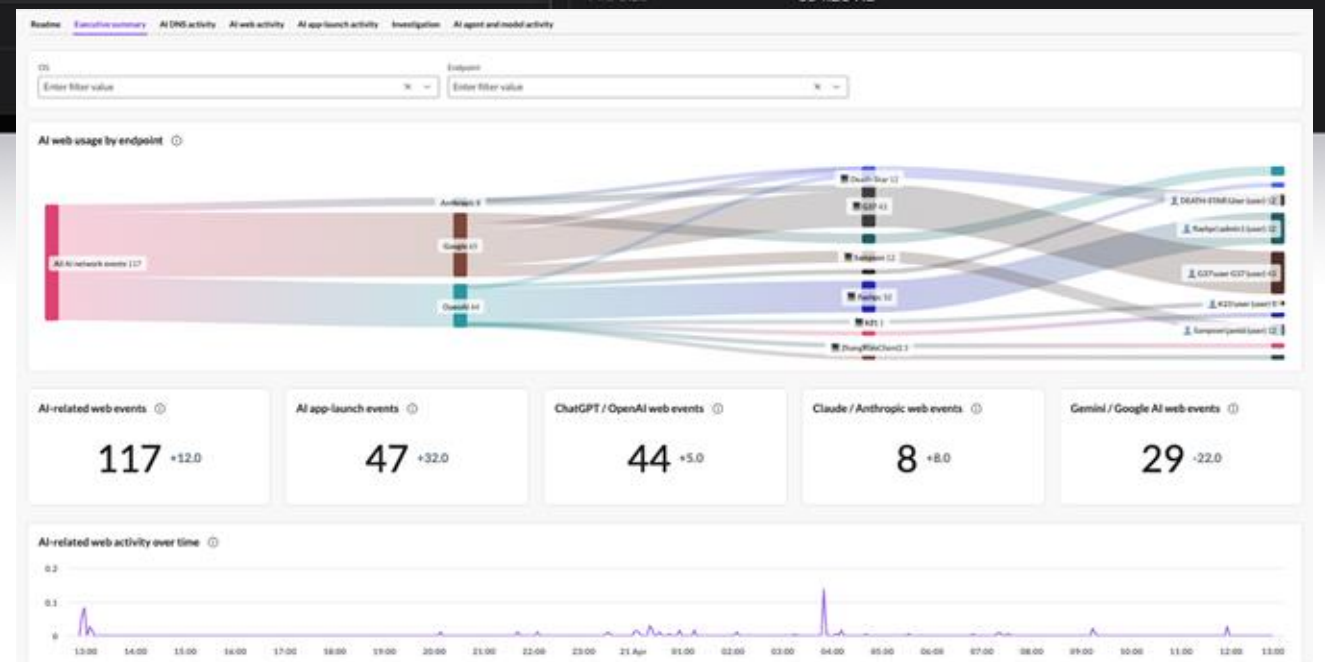
## Increased Analyst Efficiency

Reduce alert fatigue and manual triage for SOC teams. ITSecOps tools provide additional value.



**Gartner**

EPP MQ Leader,  
4 Consecutive Years

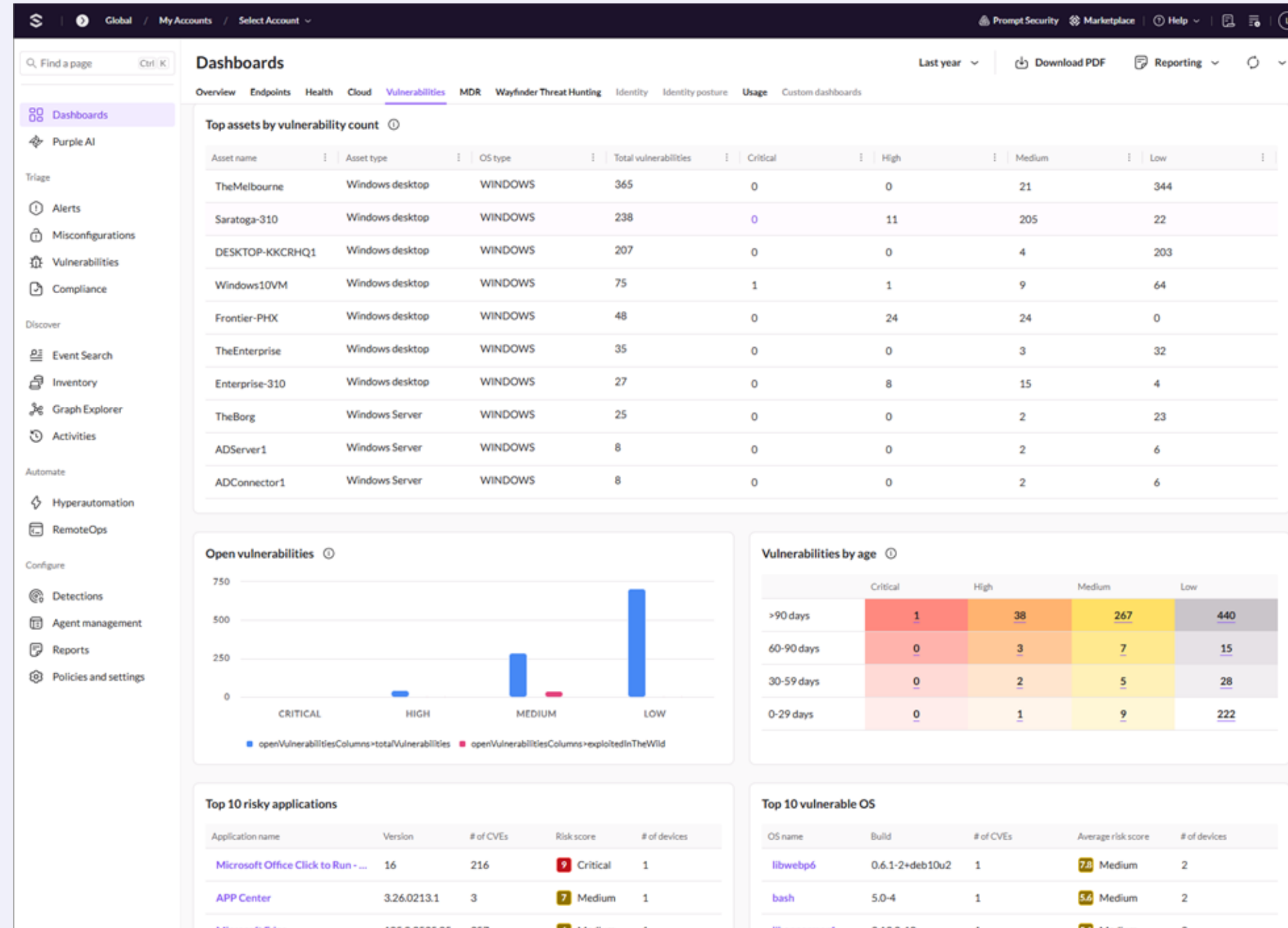


# Vulnerability Management

**Singularity Vulnerability Management** delivers continuous visibility into the vulnerabilities associated with applications and operating systems across Microsoft, Linux, and macOS.

## Outcomes

- Real-time OS and application vulnerability assessment
- Dynamic vulnerability prioritization based on evolving threat landscape and business criticality
- Replace clunky network scanners with a unified agent for EDR, EPP and Vulnerability Management
- Reduced complexity and lowered TCO for VM programs



Application Inventory

Application Vulnerabilities

Operating System Vulnerabilities

Intelligence Driven Prioritization

Transparent Vulnerability Scoring

Mitigation Guidance

Integrated with NVD and MITRE CVSS

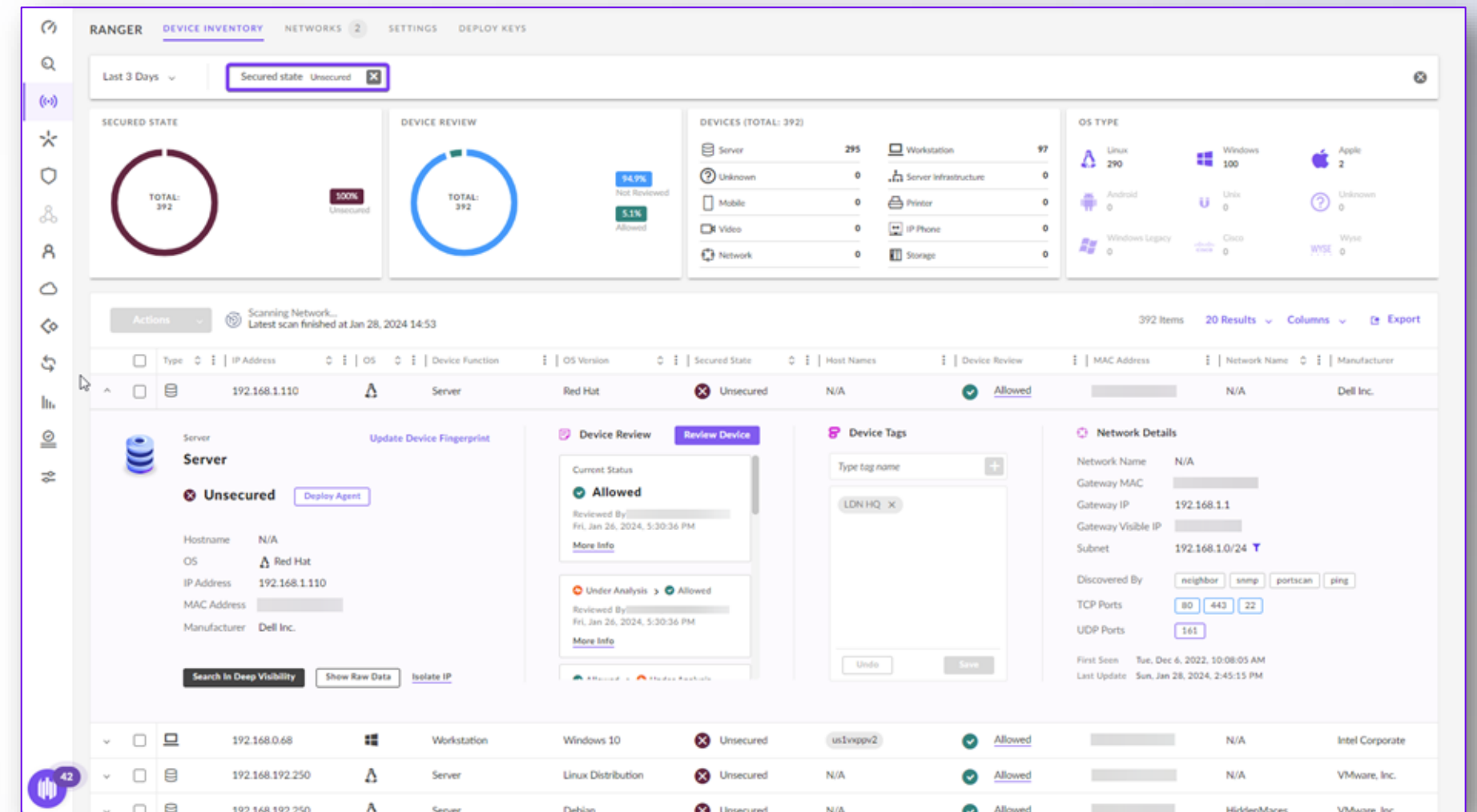
Multitenancy for MSSPs

# Singularity Network Discovery

**Singularity Network Discovery** brings network visibility and attack surface control to the Singularity Platform through intelligent network discovery, peer-to-peer agent deployment, and suspicious device isolation.

## Outcomes

- Know what's connected to all global networks
- Conveniently access actionable network information
- Quickly bring unprotected devices into compliance
- Block suspicious devices with a single click
- Deploy no new software, just turn Network Discovery on.



IP Network  
Discovery



Active & Passive  
Device Learning



AI-Based  
Fingerprinting



Singularity Agent  
Peer-to-Peer  
Deployment



Suspicious Device  
Isolation



Asset Inventory &  
Device Tagging



Secured State  
Classifiers



Multitenancy  
for MSSPs

# Singularity Identity

Real-time defense and end-to-end visibility for every identity



## Gain Complete Visibility

Get end-to-end insight through correlated endpoint & identity activity, accelerating detection & response.



## Reduce the Attack Surface

Continuously uncover and remediate exposures across on-premise and cloud environments.



## Proactively Disrupt Attackers

Use deception techniques and conditional access to stop reconnaissance before it starts.



## Stop Attacks in Real Time

Detect credential-based attacks as they occur and remediate instantly.

The screenshot displays the 'EXTENDED SECURITY POSTURE MANAGEMENT' interface. The main table lists various security issues with columns for Severity, Status, Organization, Environment, Event Source, and Exposure. A detailed view on the right shows the 'Weak SMBv1 Session Allowed' issue, including its status (Critical), affected assets (Active directory), and a description of the risk (SMBv1 is a protocol that does not encrypt data and is vulnerable to man-in-the-middle attacks). It also lists affected assets like 'TerenceMcLaughlin' and provides security policy violation details.

Misconfiguration Name	Severity	Status	Organization	Environment	Event Source	Exposure
Decreased User Accounts	Critical	New	ADlocal.com	Active Directory	SentinelOne	Danger
Weak SMBv1 Session Allowed	Critical	New	Australia.local	Active Directory	SentinelOne	Danger
Decreased User Accounts	Critical	Risk acknowledged	ADlocal.com	Active Directory	SentinelOne	Danger
Weak SMBv1 Session Allowed	Critical	New	ADlocal.com	Active Directory	SentinelOne	Danger
Protected Users Group Not Created/Used	Critical	New	india.local	Active Directory	SentinelOne	User's pr
SecureKey Vulnerability Assessment	Critical	To be patched	ADlocal.com	Active Directory	SentinelOne	Risky Us
Protected Users Group Not Created/Used	Critical	New	ADlocal.com	Active Directory	SentinelOne	User's pr
Decreased User Accounts	Critical	New	india.local	Active Directory	SentinelOne	Danger
Accounts with Risky User Account Contr...	Critical	To be patched	Australia.local	Active Directory	SentinelOne	Risky Us
Weak SMBv1 Session Allowed	Critical	To be patched	Australia.local	Active Directory	SentinelOne	Danger
Decreased User Accounts	Critical	On hold	india.local	Active Directory	SentinelOne	Danger
Payment Spec feature is disabled for In...	Critical	To be patched	india.local	Active Directory	SentinelOne	Danger
Web Devices in Azure AD	Critical	New	india.local	Azure	SentinelOne	App-cre
Unwanted Privilege for Enterprise Key A...	Critical	To be patched	ADlocal.com	Active Directory	SentinelOne	Danger
Azure AD Tenant without User Risk Pol...	Critical	To be patched	ADlocal.com	Azure	SentinelOne	Unwant
Protected Users Group Not Created/Used	Critical	New	ADlocal.com	Active Directory	SentinelOne	Unwant
Enable the AD recycle bin	Critical	On hold	Australia.local	Active Directory	SentinelOne	User's pr
Standard users without Multi Factor Aut...	High	To be patched	Australia.local	Azure	SentinelOne	App-cre
Standard users without Multi Factor Aut...	High	On hold	France	Azure	SentinelOne	Unwant

# Singularity Mobile

## AI-Powered Mobile Threat Protection



### Detect Emerging Threats

Detect zero-day malware and phishing threats in real time with behavioral models.



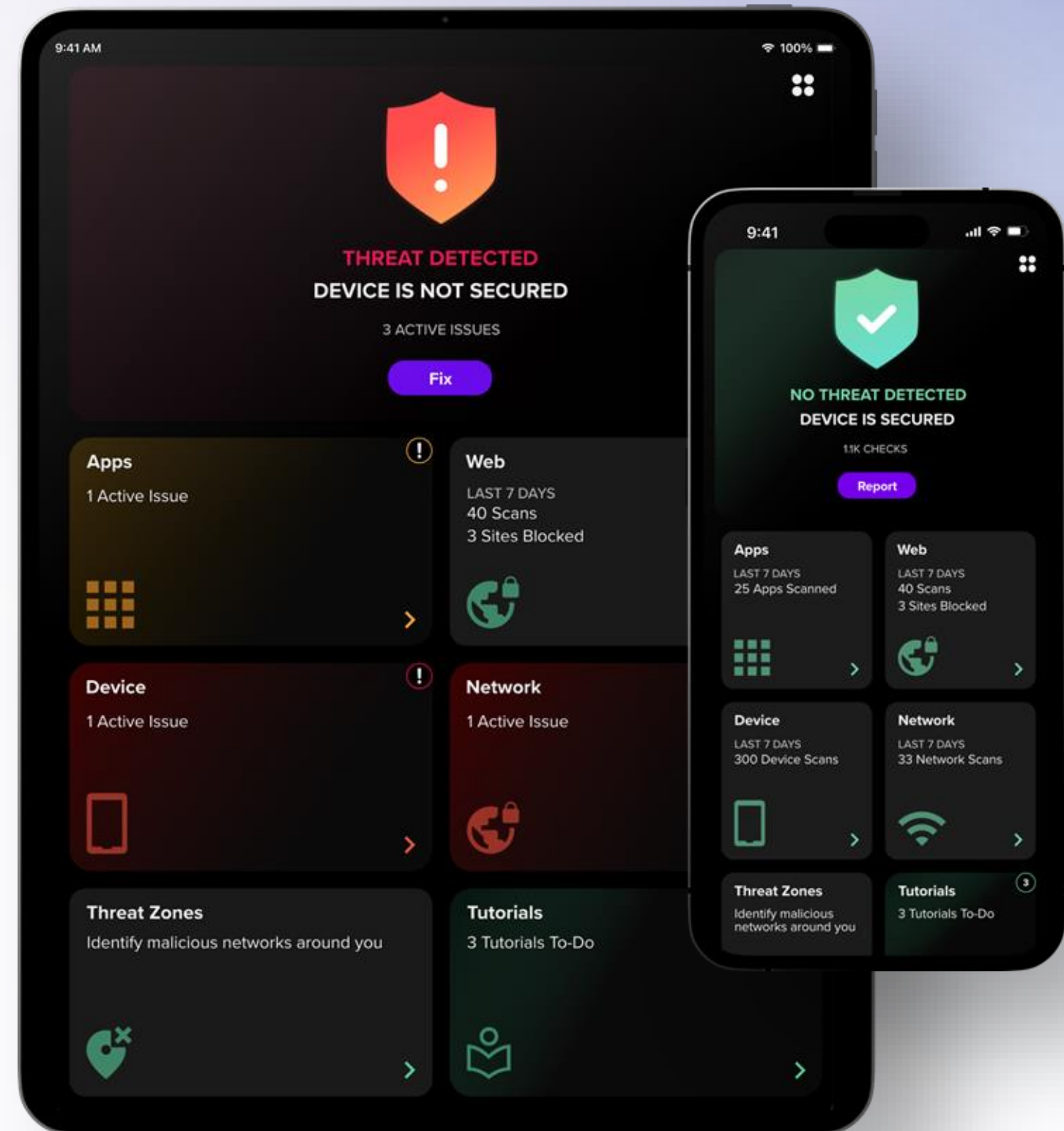
### Stop Active Attacks

Block man in the middle (MITM) attacks and device tampering.



### Adapt to Change

Continuously adapt to evolving risks with always-on protection that keeps pace with the mobile threat landscape.



# Singularity Cloud Security

## Unified and Comprehensive

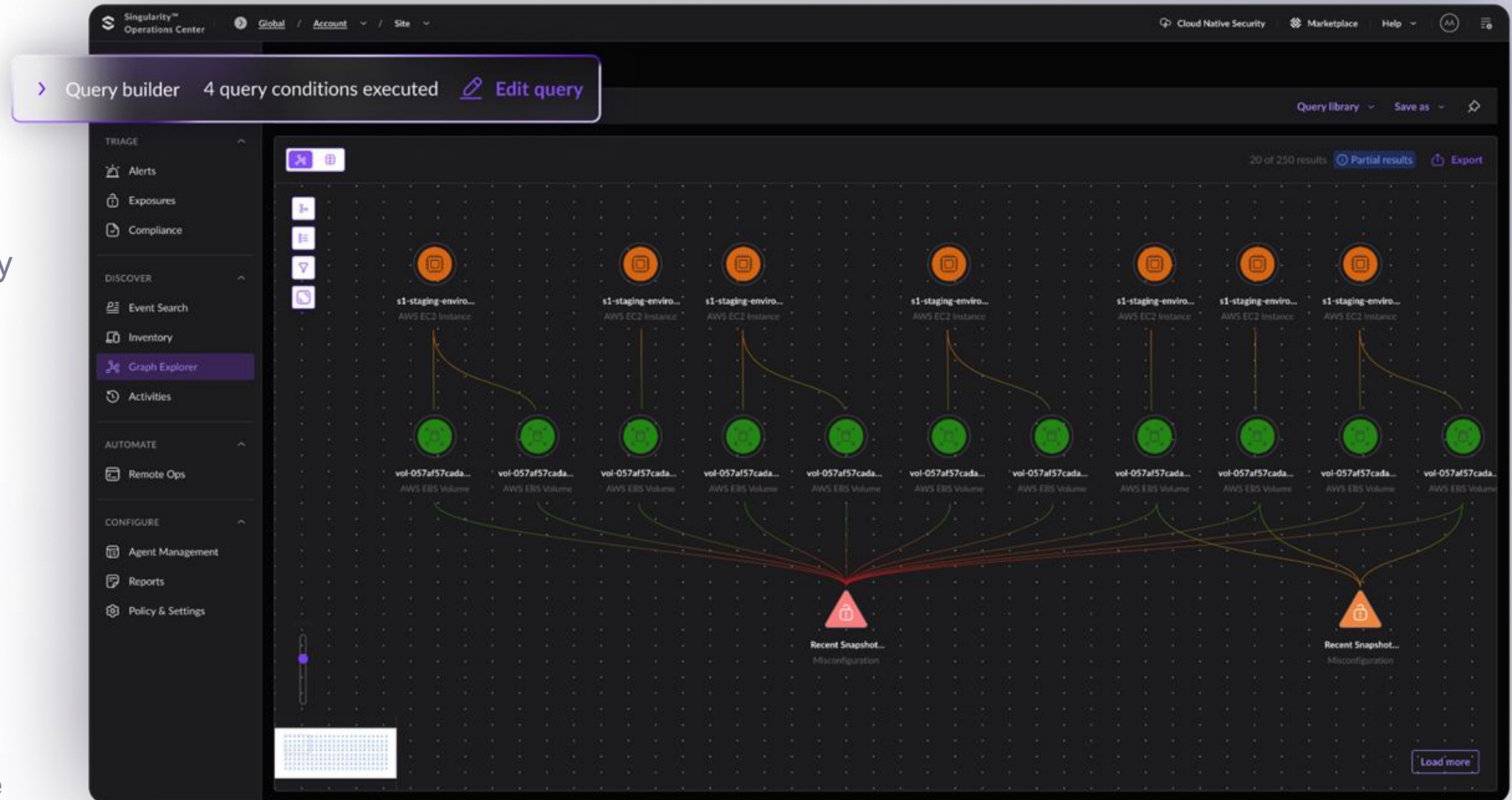
Powered by Singularity Data Lake and Purple AI, customers can have a complete view of their security issues across endpoint, identity, and cloud.

## Focus on Actual Issues

Prioritize cloud health and remediation with evidence-based Verified Exploit Paths™ from code to multi-cloud environments.

## AI-powered Threat Protection and Detection

Secure cloud and container workloads with real-time protection and forensic visibility.



Gartner  
Peer Insights™

Leader for CNAPP



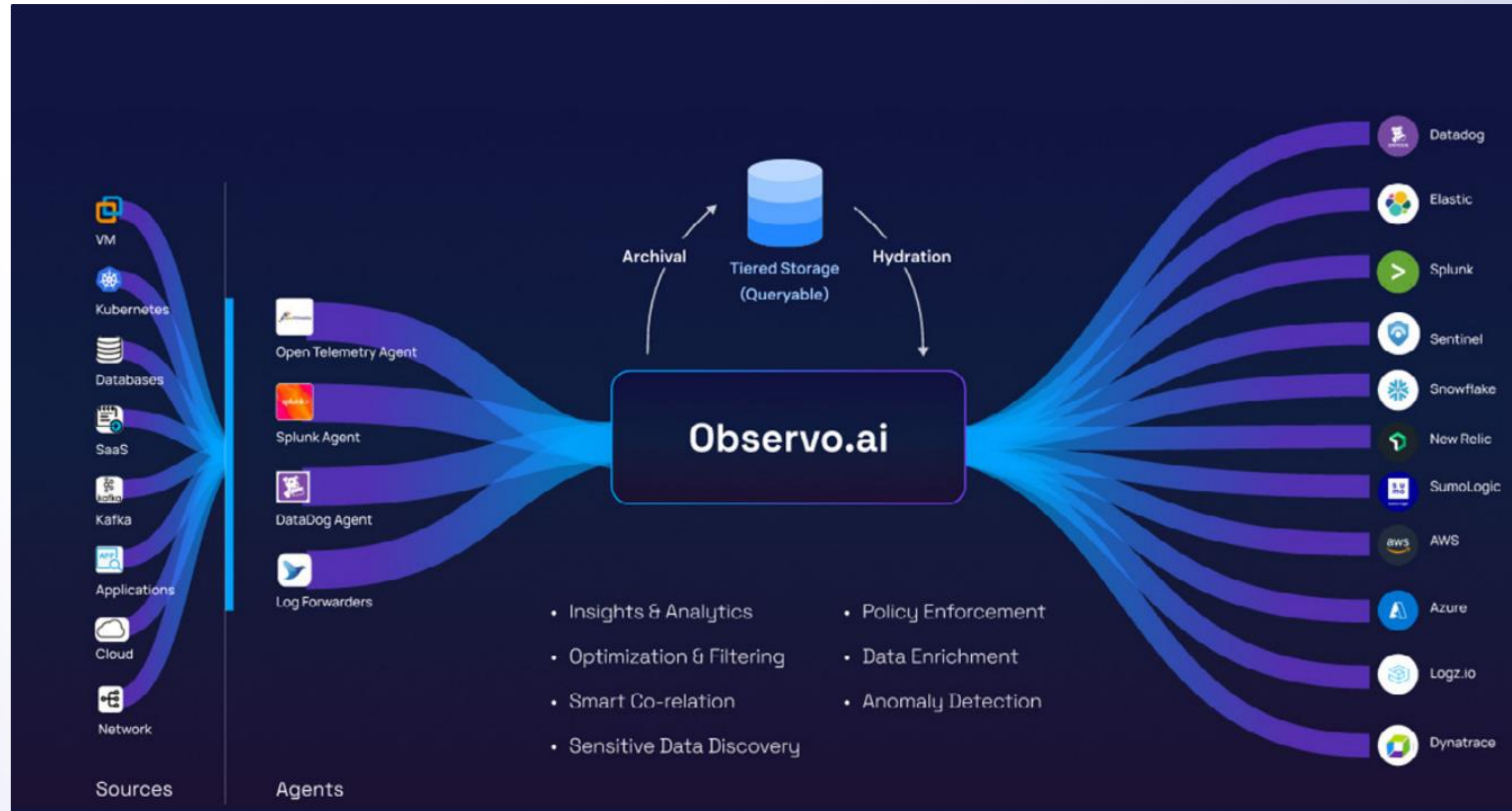
Most awarded  
CNAPP, 4.9/5 rating

240+ Awards

And counting

# Make Your Security Data Work Smarter

- AI-driven data reduction
- Smart routing and transformation
- Real-time data enrichment
- Anomaly detection
- Low-cost searchable data lake
- Sensitive data detection and masking



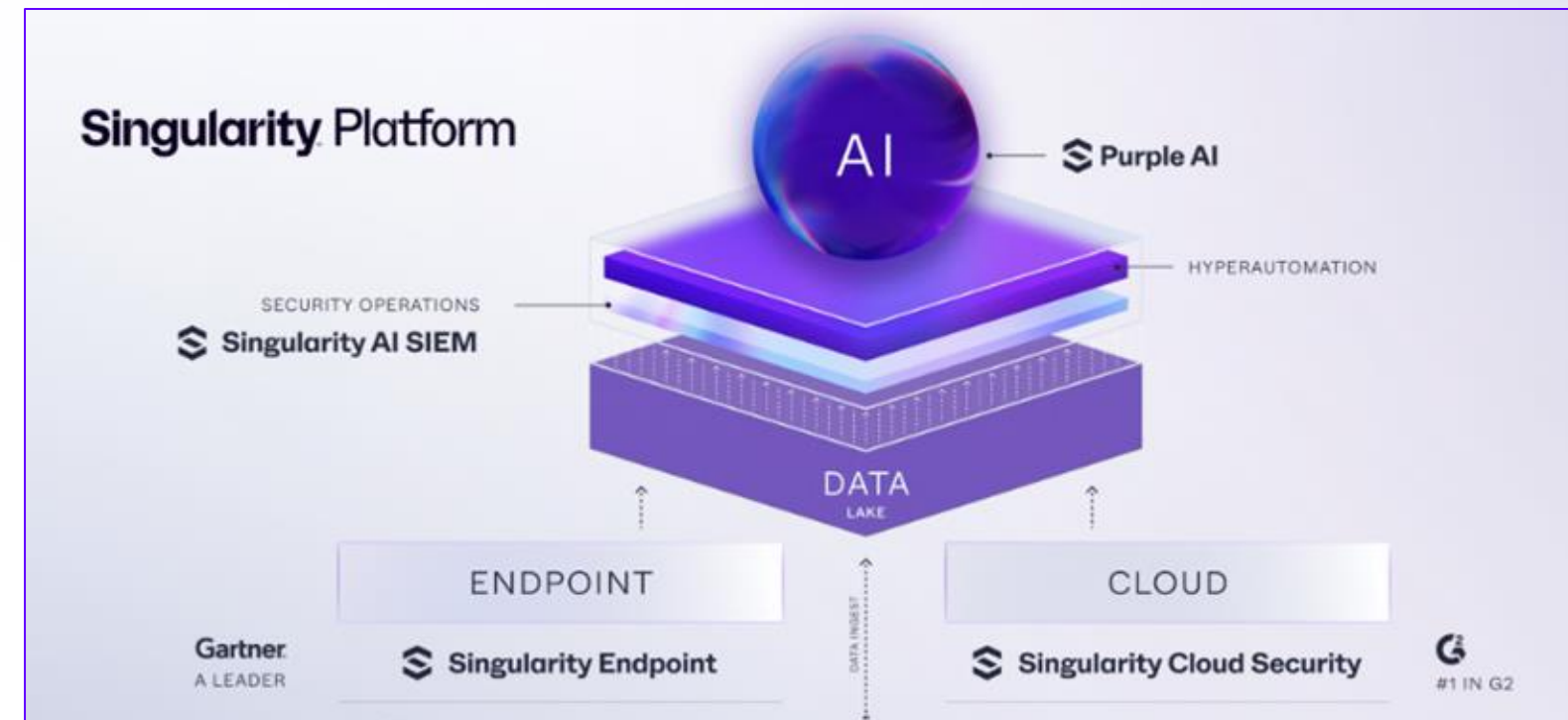


# The HyperAutomated AI SOC Platform

- **Fully integrated** platform for SOC, Endpoint, Cloud & Identity Security
- **10-50x faster query times** than legacy and next gen cloud native SIEM's
- **< 50% of the cost saving of existing SIEM solutions** (with a predictable licensing model)
- **Open standards (OCSF)** interoperability & flexible SOC modernisation paths
- **80% faster** investigations & **128% easier** threat hunting (with Ai assistance)
- Fully integrated HyperAutomation, generativeAi & agenticAi for **Autonomous SOC Operations**

10

## Singularity AI SIEM



**Unmatched & massive multi-tenanted parallel processing engine that scales to PB's**

**Always HOT**, lowest cost storage, with up to **7 years retention** + data encryption as standard

**96% of ALL queries** complete in **< 1 Second**

**500+ detections** & integrated **generativeAi** assistance & **agenticAi** services

# Singularity Hyperautomation

## Connect Everything

Integrate and automate your entire security env by connecting your SaaS apps.

## Accelerate Response

Enhance your workflow with more context and visibility through built-in automation.

## Boost Efficiency

Save time by streamlining processes and automating repetitive tasks without complexity of coding.

## Out of the Box integrations

The screenshot displays the Singularity Hyperautomation interface for a workflow titled "Reactivate User in Okta using Slack". The workflow is a vertical sequence of steps:

- HTTP Trigger** (Slack) with a **Slash Command** action.
- Search Users by Email** (Okta).
- User Exists** (Condition).
- Branching based on the "User Exists" condition:
  - False** path: **Post User Not Found** (Slack).
  - True** path: **User is suspended** (Condition).
- Branching based on the "User is suspended" condition:
  - False** path: **Post User Not Suspended** (Slack).
  - True** path: **Unsuspend a User** (Okta).
- Post User Successfully Unsuspended** (Slack).

The right-hand panel shows the configuration for the "Unsuspend a User" action, which is a POST request to the Slack API. The URL is `https://slack.com/api/chat.postEphemeral`. The body is in JSON format:

```
{
  "channel": "{{slash-command.data.channel_id}}",
  "user": "{{slash-command.data.user_id}}",
  "text": "User {{slash-command.data.text}} successfully unsuspended"
}
```

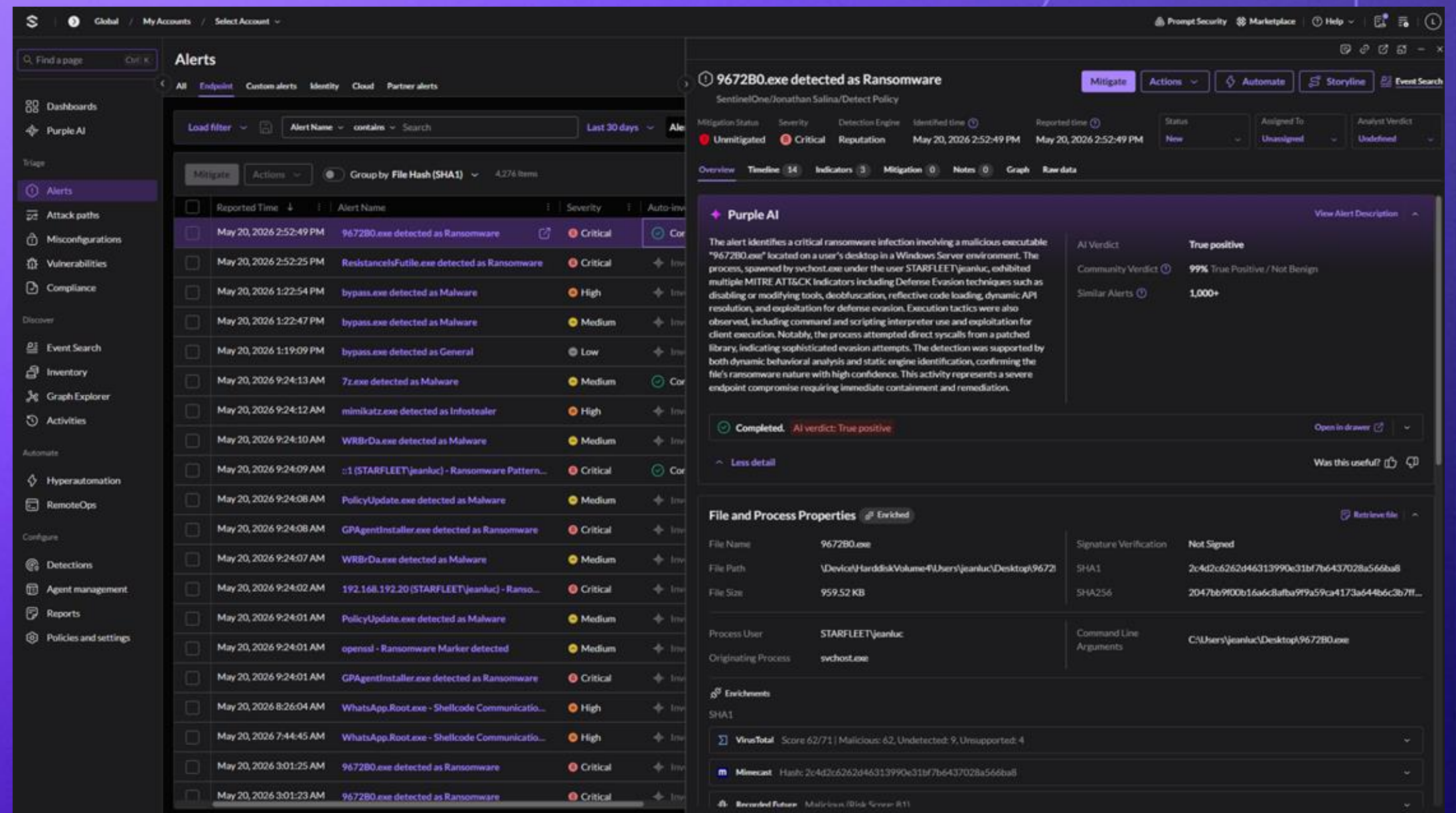
Advanced Configuration options are visible at the bottom of the right panel.



ACCELERATE SECOPS

# Auto-Investigation

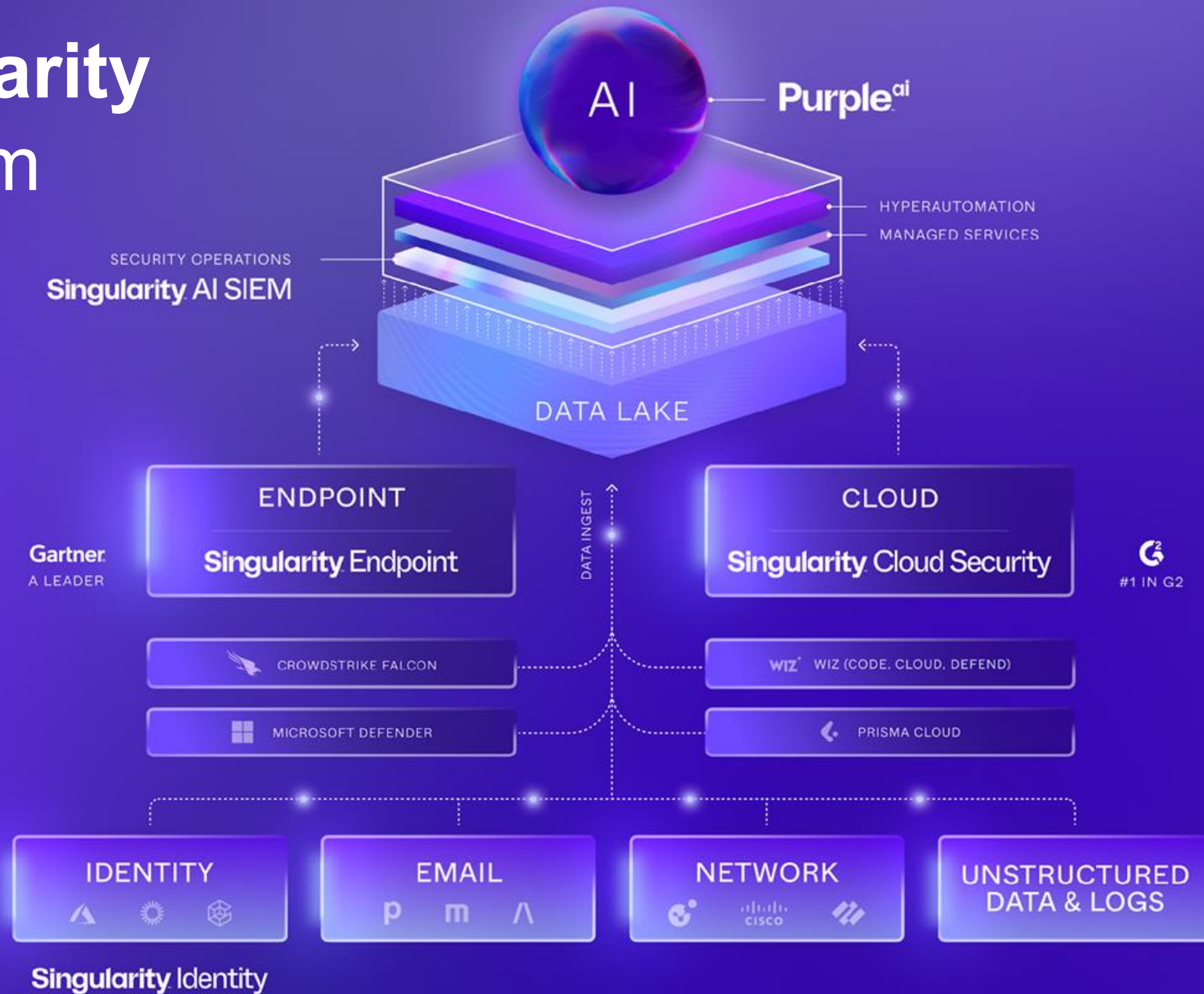
- Dynamic investigations using agentic AI that adapts to real-time evidence.
- Drive confident, rapid decision-making with explainable verdicts that eliminate guesswork.
- Slash mean time to respond and resolve threats faster without sacrificing human control.



**41%** More Efficient Investigation Teams

**55%** Faster to Remediate Security Threats

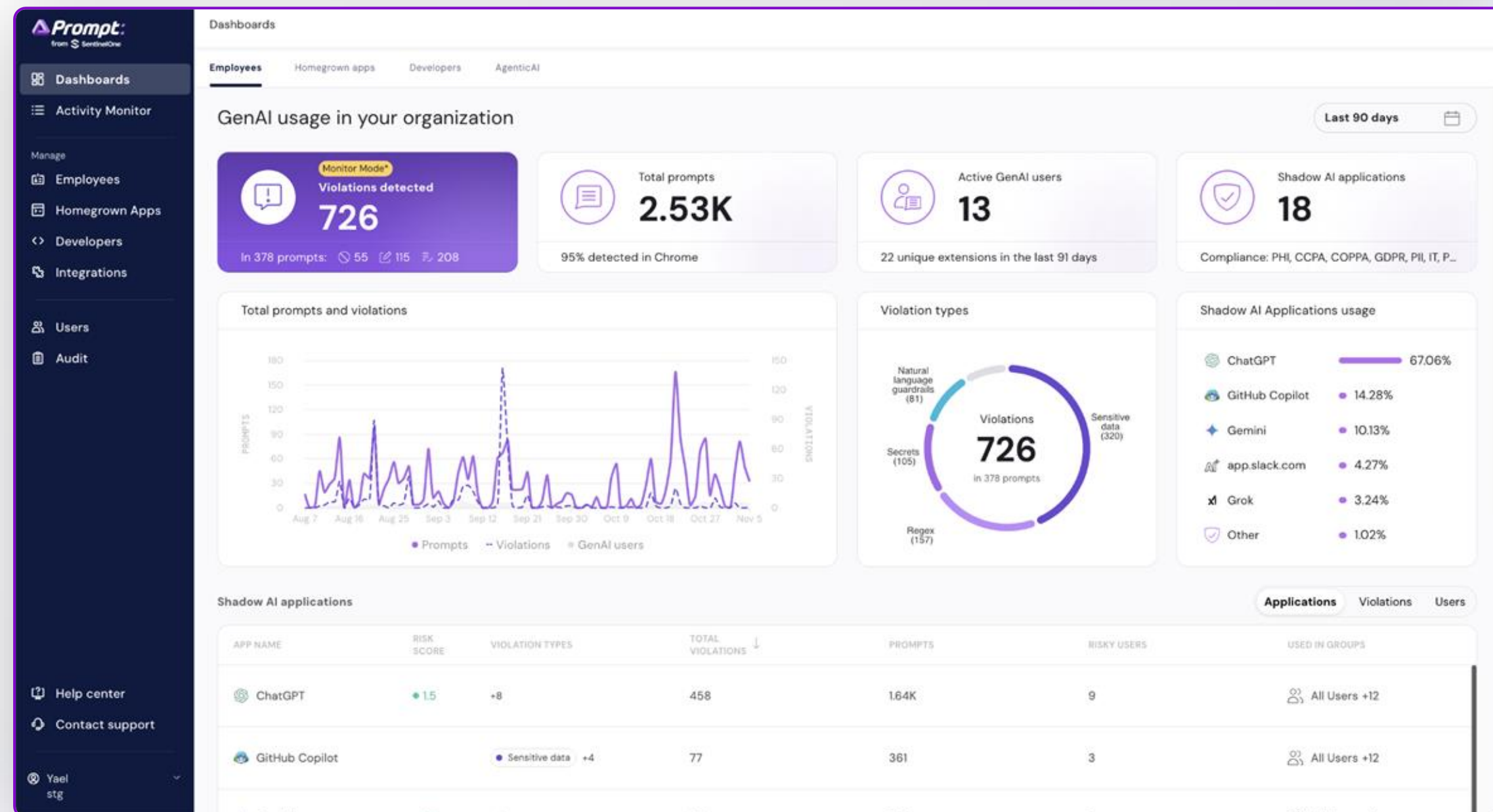
# Singularity Platform



# Prompt Security for AI applications

Enable employees to adopt AI tools without worrying about Shadow AI, Data Privacy and Regulatory risks

- **Observability:** Detect and monitor all AI tools used within the organization and eliminate Shadow AI
- **Data Privacy:** Prevent data leaks through automatic anonymization
- **Risk Management and Compliance:** Enforce granular department and user rules and policies
- **Employee awareness:** Coach your employees on the safe use of AI tools



# Prompt for AI Red Teaming

Find AI vulnerabilities before you ship: Test AI applications for the vulnerabilities that matter most, then use those insights to improve protection before deployment.

### Early Detection

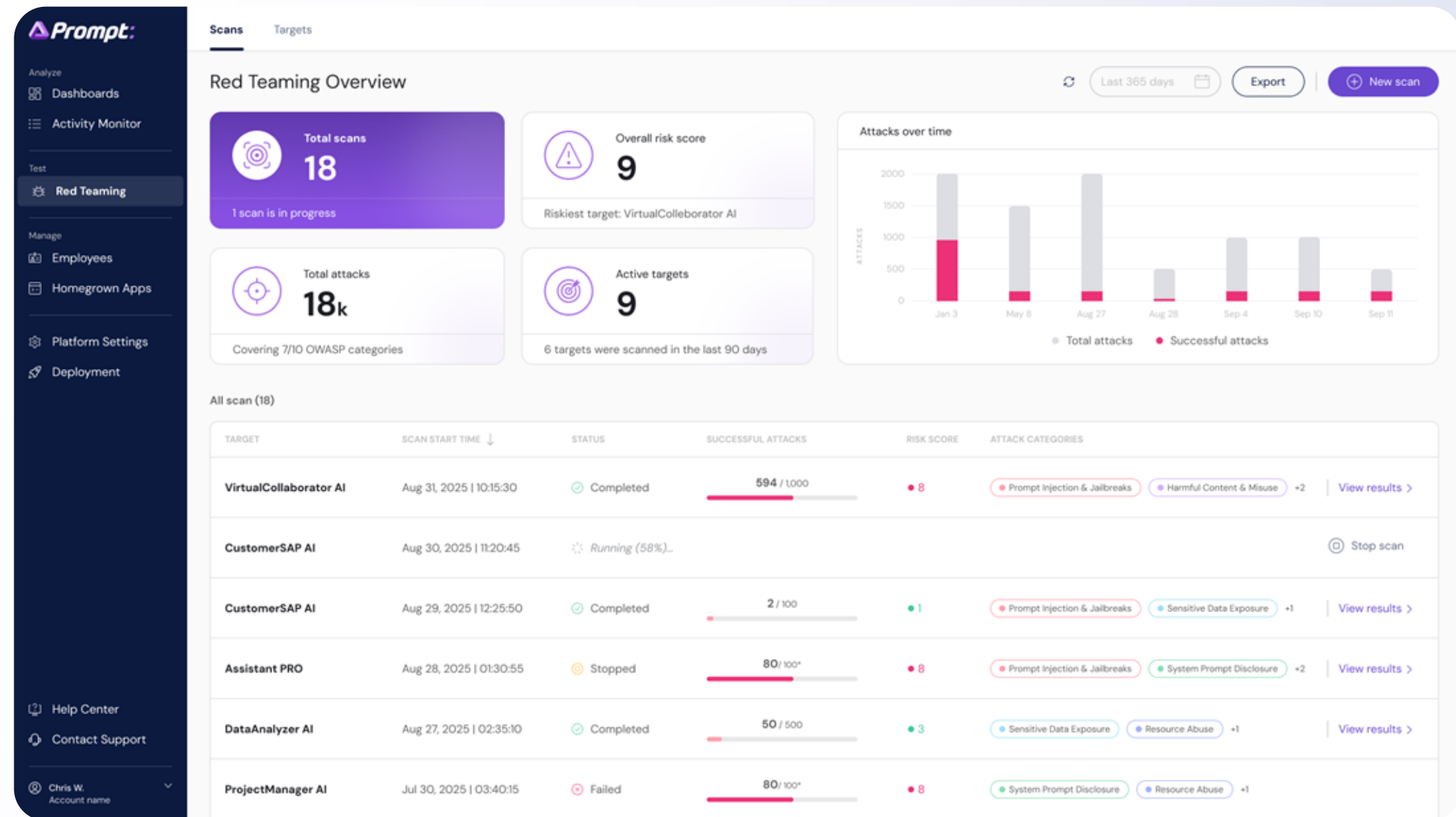
Simulate real AI attacks like prompt injection, jailbreaks, data poisoning, and more, tailored to your app and built for the nondeterministic nature of LLMs

### Guided Remediation

Every finding includes risk scoring, evidence, and remediation guidance, so dev teams can resolve vulnerabilities pre-production

### Continuous Evaluation

Ongoing red teaming cycles automatically detect model drift, emerging vulnerabilities, and new attack vectors as models are updated





# Secure Tomorrow™

See how the world's most advanced cybersecurity platform  
can protect your organization today and beyond.

