

Building Digital Resilience in the Agentic AI Era

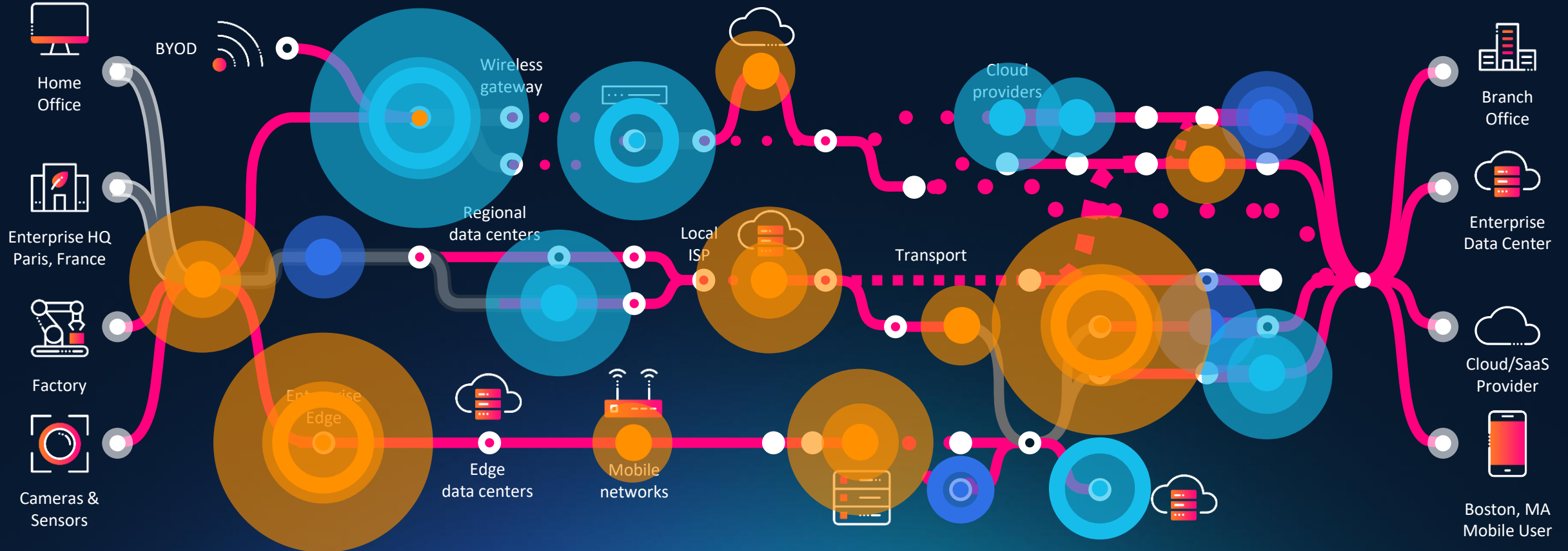
Get ahead of issues and minimize business impact

Patrick Lin (PCL)
SVP & General Manager
Splunk Observability @ Cisco

Anton Eksteen
Head of Networks and Reliability Engineering
HCF

CISCO Live !
IT Leadership Program

Digital Complexity is Exploding



AI is Raising the Stakes

Yesterday

Deterministic apps

Predictable behavior

Manual troubleshooting

Golden signals (latency, errors)

Today

Agentic AI apps

Unpredictable, probabilistic outputs

AI-assisted, autonomous response

New signals (quality, cost, alignment)

The New Mandate: Digital Resilience **for AI, with AI**

For AI

Assure trust and predictability for agentic systems

Digital Resilience

With AI

Use agentic AI to optimize operations and adapt faster

Cisco Data Fabric

A revolutionary new architecture to harness
the value of machine data with AI

Cisco Data Fabric



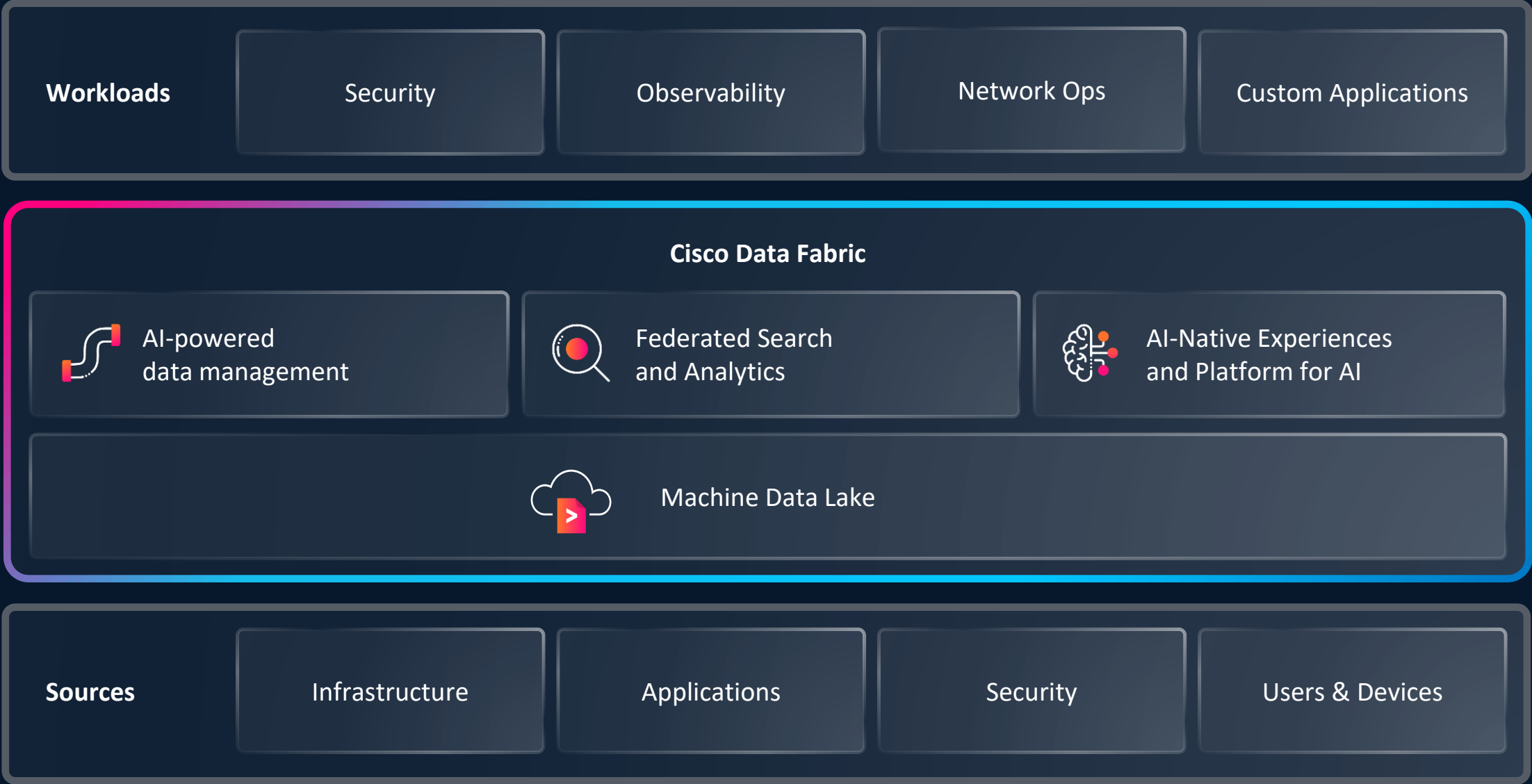
Operate
on machine data
at ludicrous scale

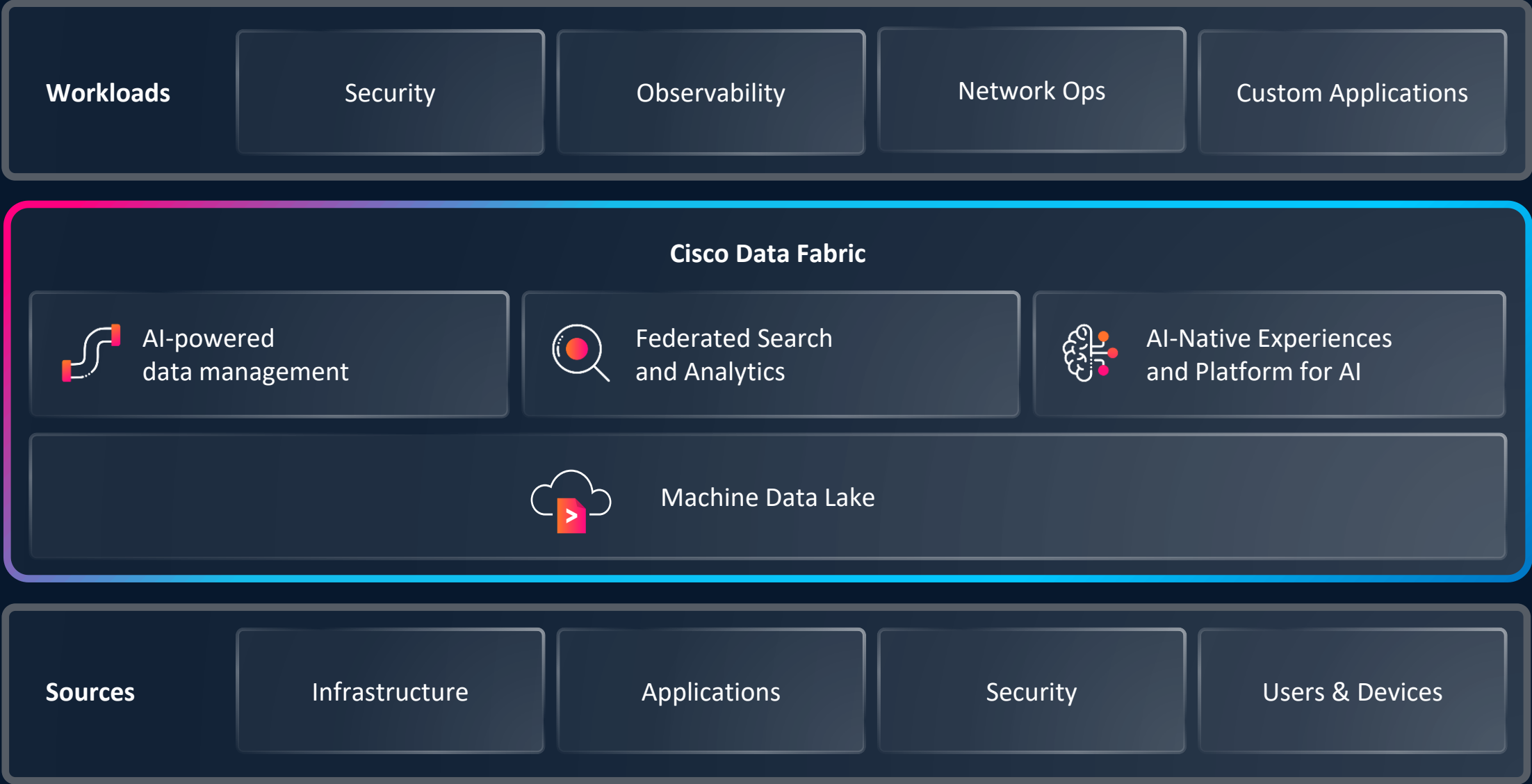


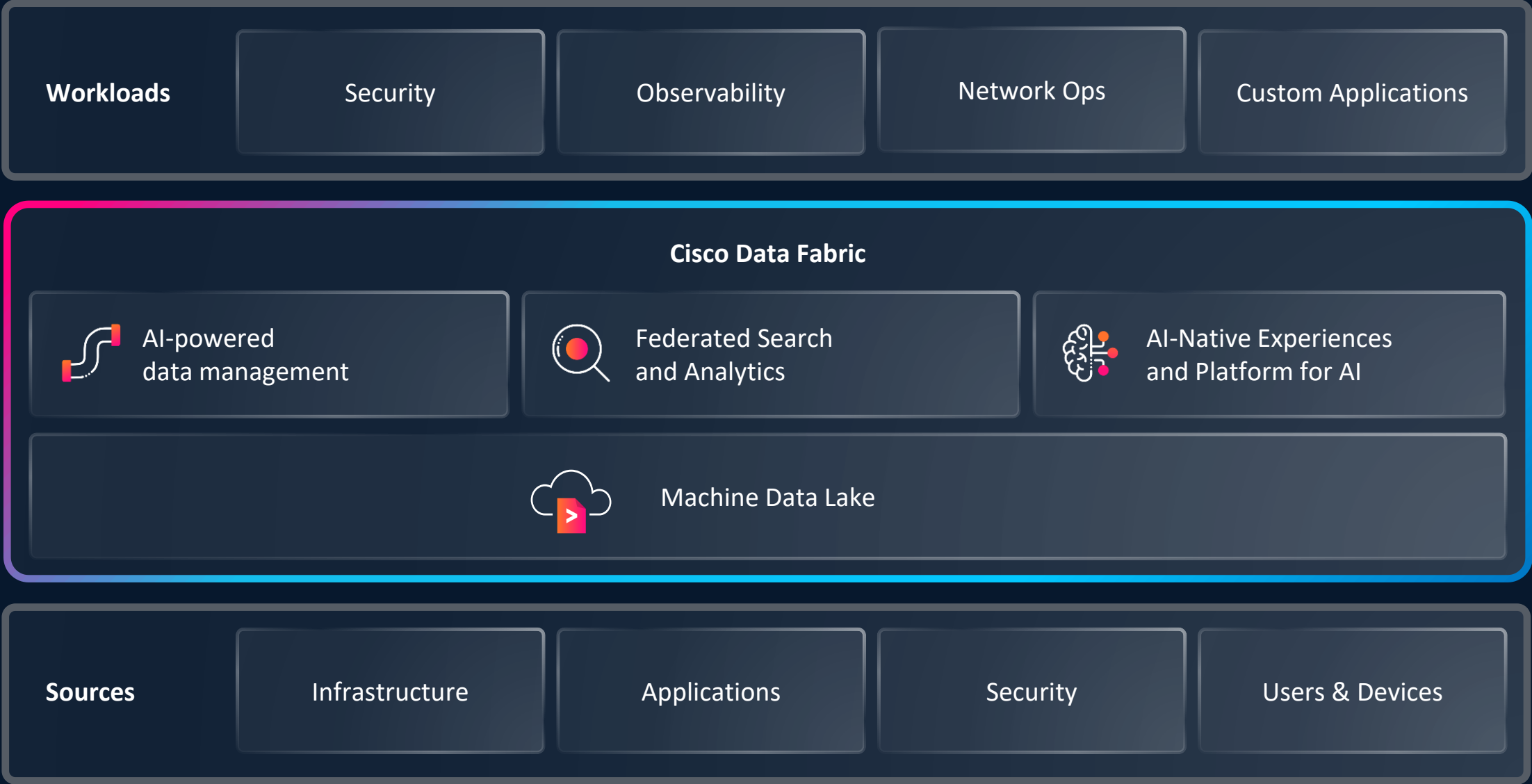
Unlock
your proprietary data
for AI



Unify
experiences for
humans and agents

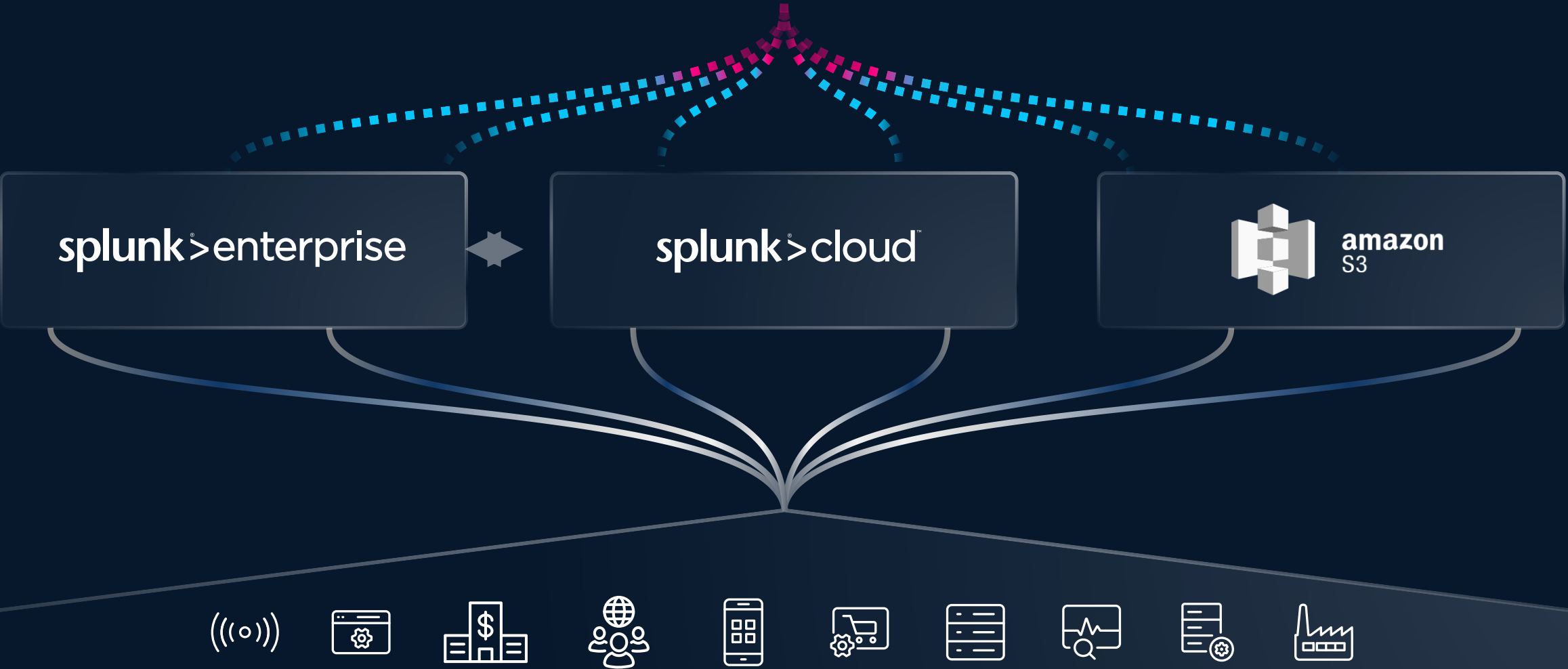






Bringing **Splunk** to **your data**

Federated Search



ANNOUNCING

Federated search for Snowflake

ALPHA FEBRUARY 2026





ANNOUNCING

Cisco Time Series Model

OPEN-SOURCE | ON HUGGING FACE NOVEMBER 2025

Optimized for machine data

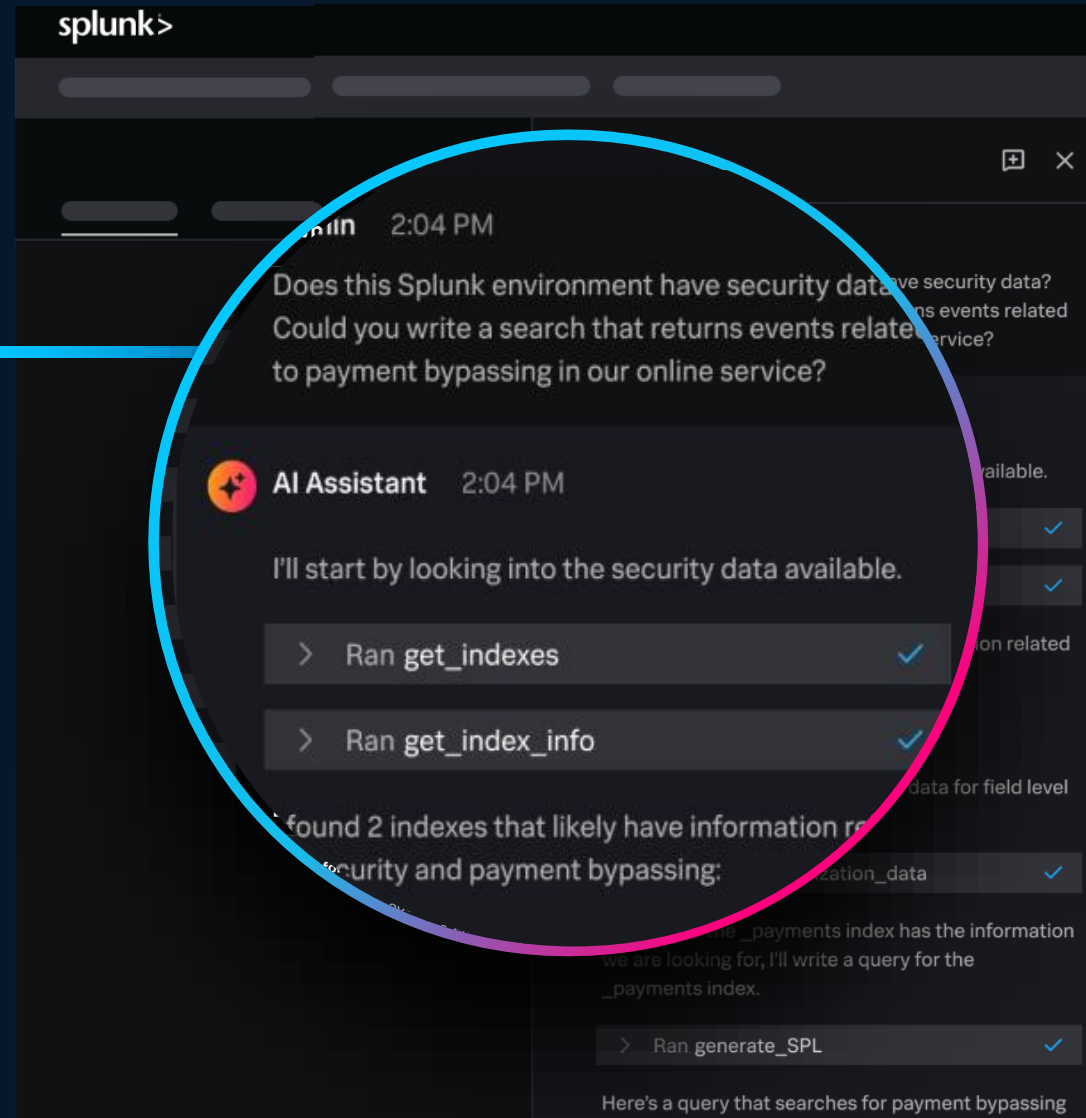
Accurate and scalable

Adaptable to your domain

AI Powered Search and Faster Data Insights

- **Unprecedented Simplicity & Power:** Search Processing Language V2
- **Improved Accuracy with Agentic AI:** Splunk AI Assistant for 1.4

GA November 2025





Agentic Observability

23  8

Incidents (24h)

32 Auto-resolved

 Critical: 12  Warning: 20

Breakdown

17 Auto-detected

15 Manual rules

[View](#)

Agentic Observability

Key Requirements

**Fix and prevent
with AI agents**

**Observe AI agents and
infrastructure**

**Unify observability and
show business impact**



Agentic Observability

Key Requirements

**Fix and prevent
with AI agents**

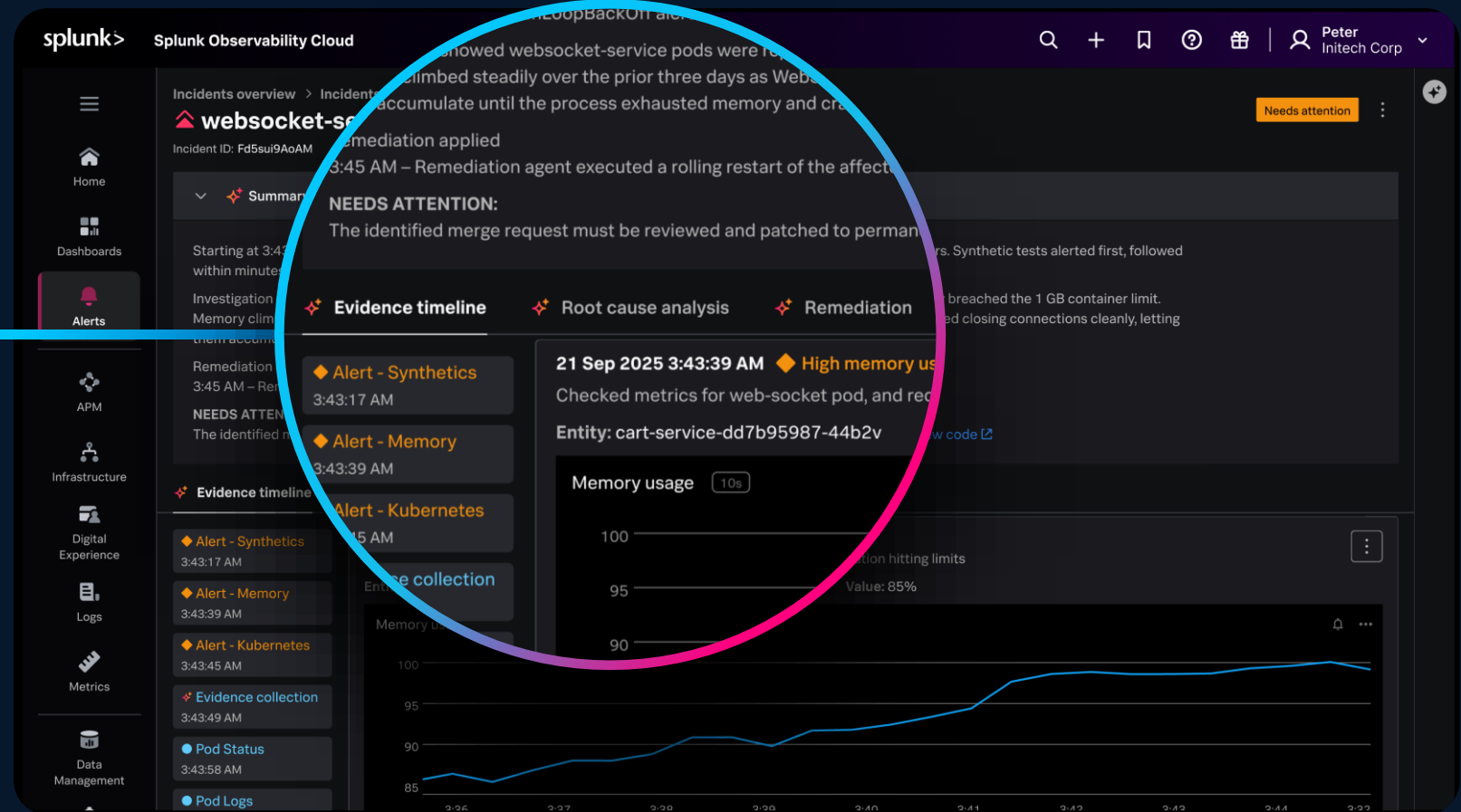
Observe AI agents and
infrastructure

Unify observability and
show business impact



AI Troubleshooting Agents

- Fix issues faster with automated Root Cause Analysis
- Makes everyone an expert



Agentic Observability

Key Requirements

Fix and prevent
with AI agents

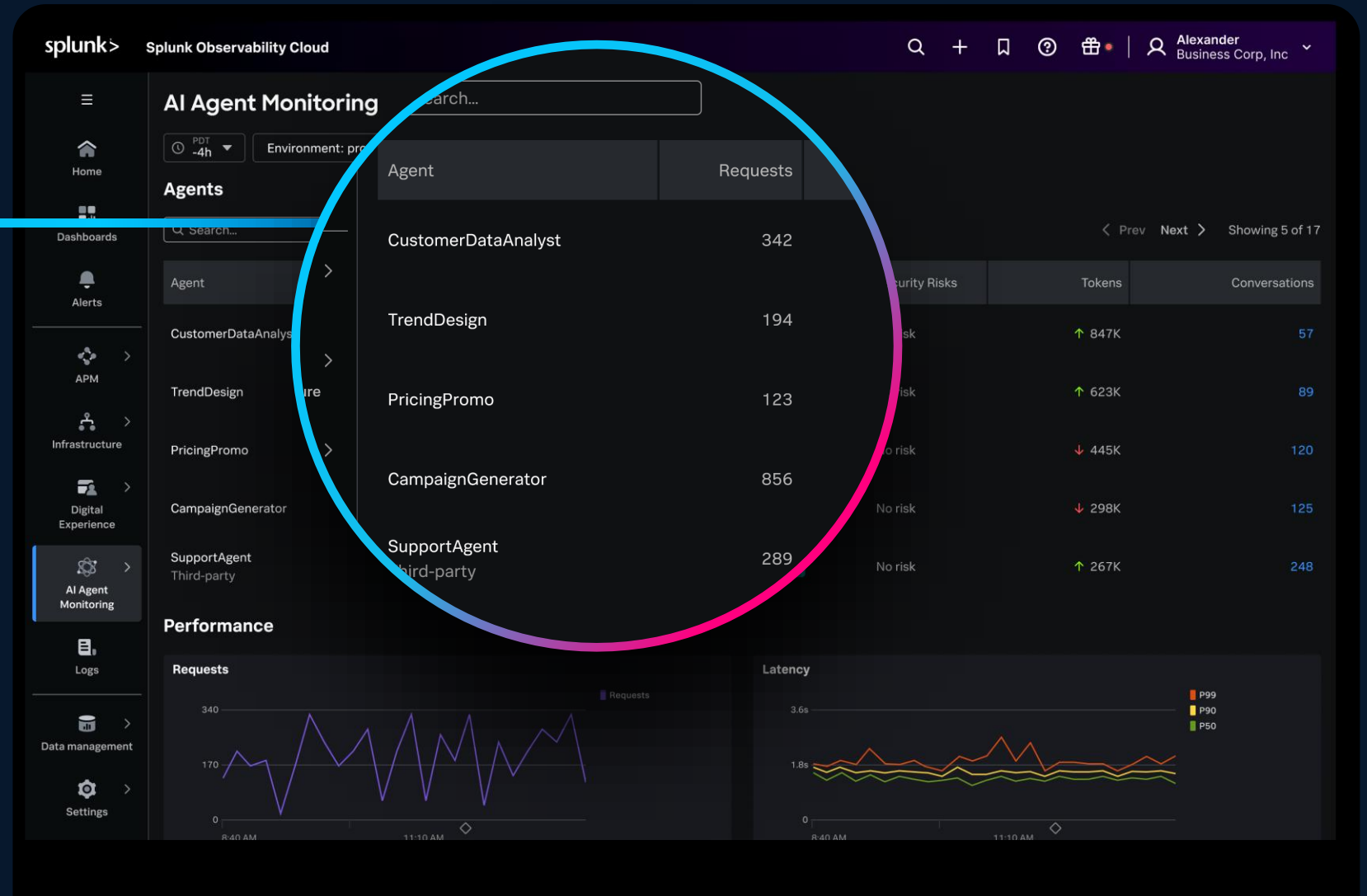
Observe AI agents and
infrastructure

Unify observability and
show business impact



AI Agent Monitoring

- Pinpoint root causes
- Visualize AI components and services
- Measure and secure LLM experiences



Agentic Observability

Key Requirements

Fix and prevent
with AI agents

Observe AI agents and
infrastructure

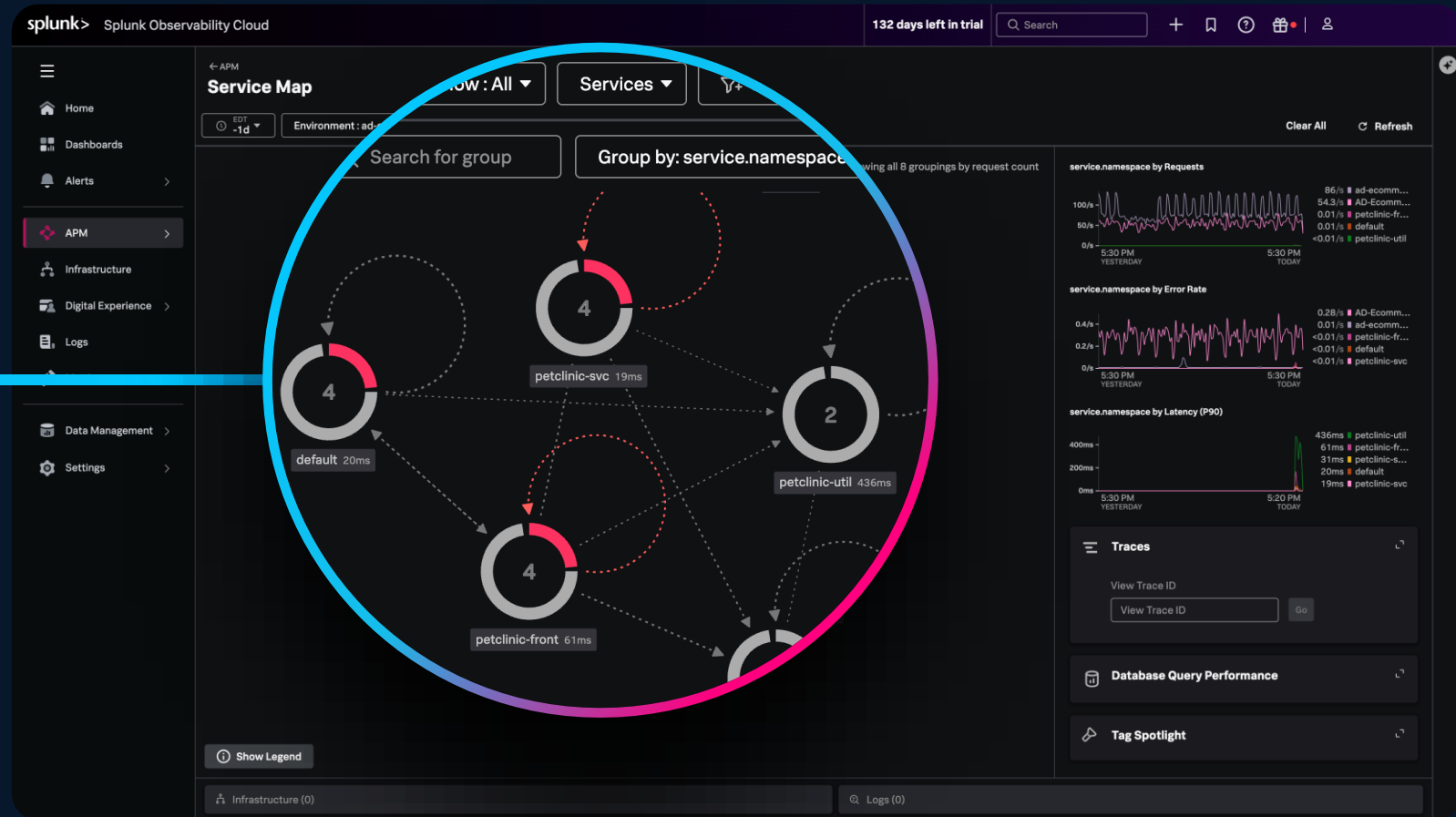
Unify observability and
show business impact



APM support for hybrid apps & business transactions

IN OBSERVABILITY CLOUD

- Monitor business transactions
- Gain code-level insights with Call Graphs
- Organize complex architectures to teams
- Correlate app and infrastructure data

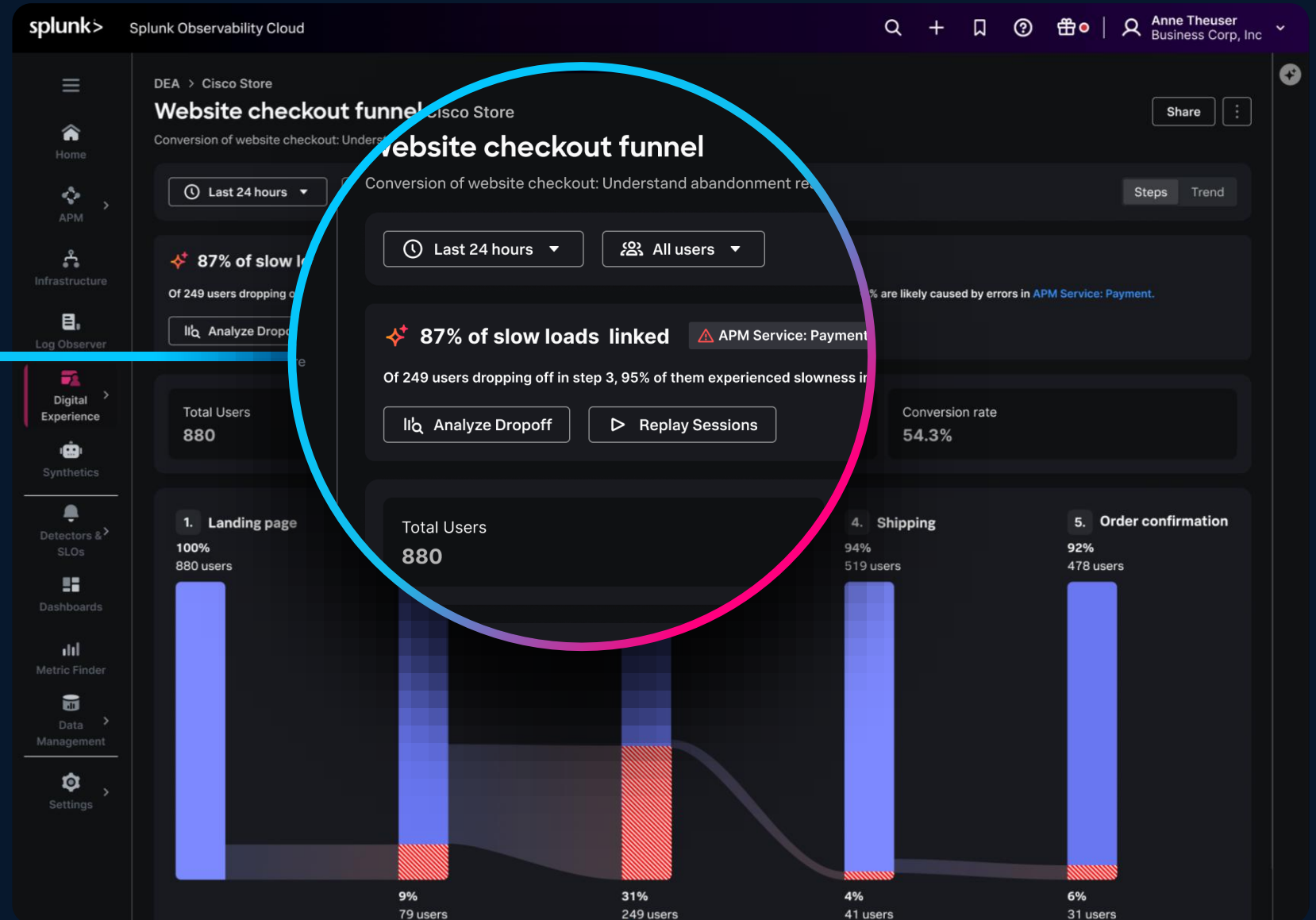


Alpha
Now

Digital Experience Analytics

IN OBSERVABILITY CLOUD

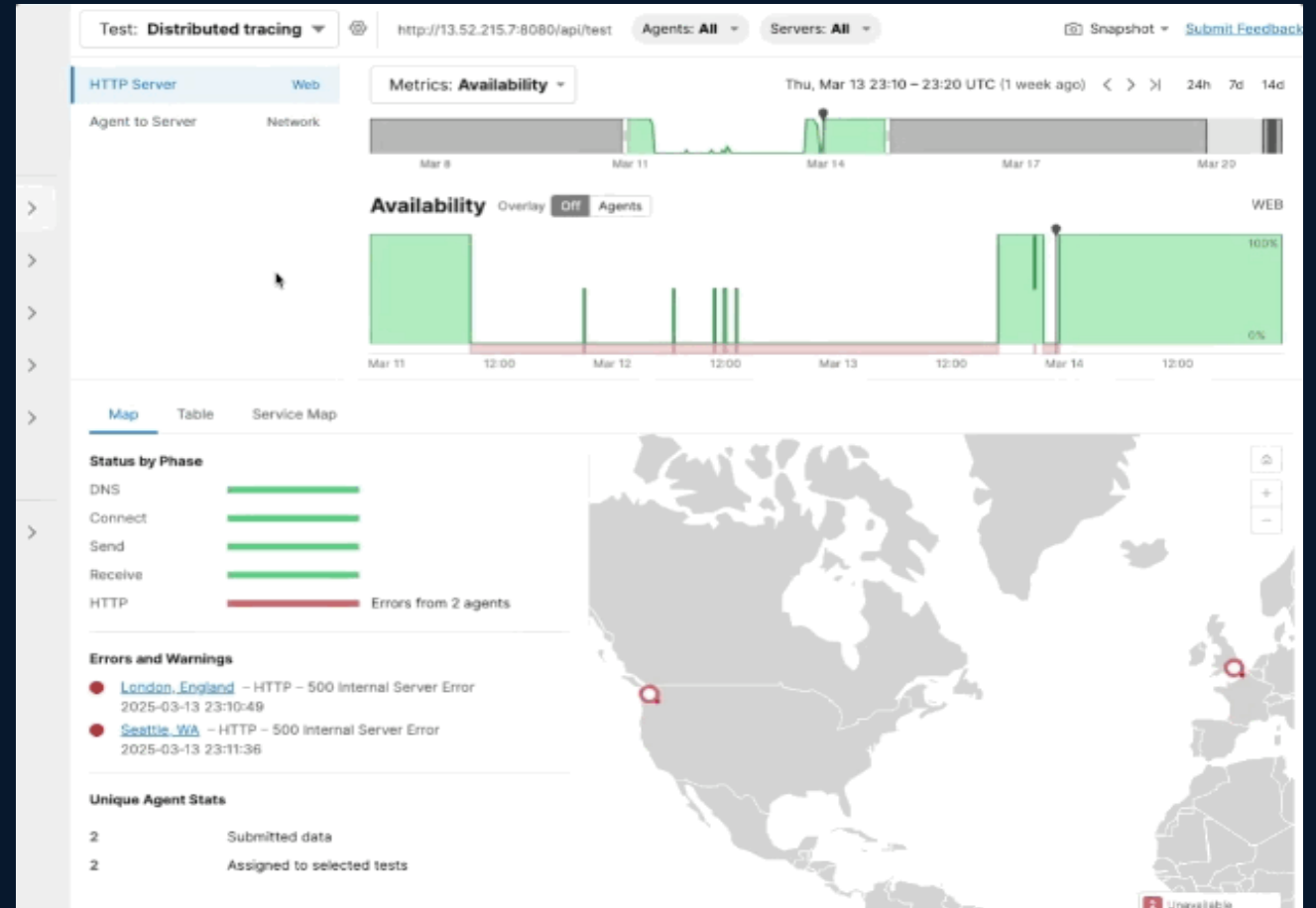
- Gain insights into customer behavior
- See how app performance impacts user experience
- Reduce engineering overhead



Thousand Eyes + Splunk Observability

Unified observability and assurance to drive digital resilience across teams

- Correlate Network & App Health
- Pinpoint Root Cause Faster
- Visualize Global Impact Instantly





Powering the Agentic SOC

Splunk Security

AI Suggested Disposition



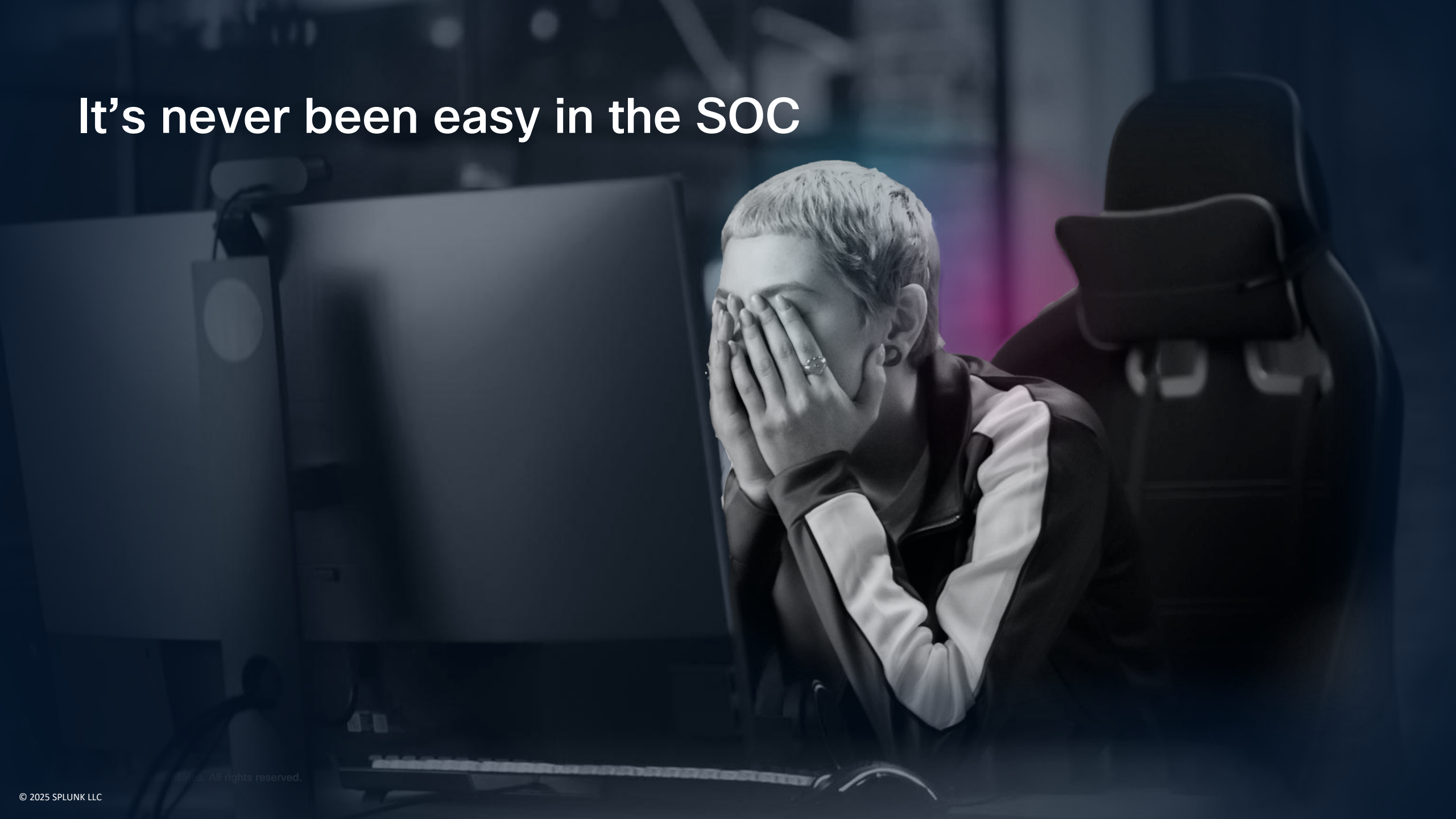
True Positive
Benign Positive
False Positive



Build a playbook to isolate a host with EDR.

To do this we will first need to get additional context of the suspicious host with a custom code block and then isolate the host with an action block.

It's never been easy in the SOC



Security Operations must evolve

Simplify the
analyst
experience

Accelerate the
SOC with AI &
automation

Expand detection
and visibility

Security Operations must evolve

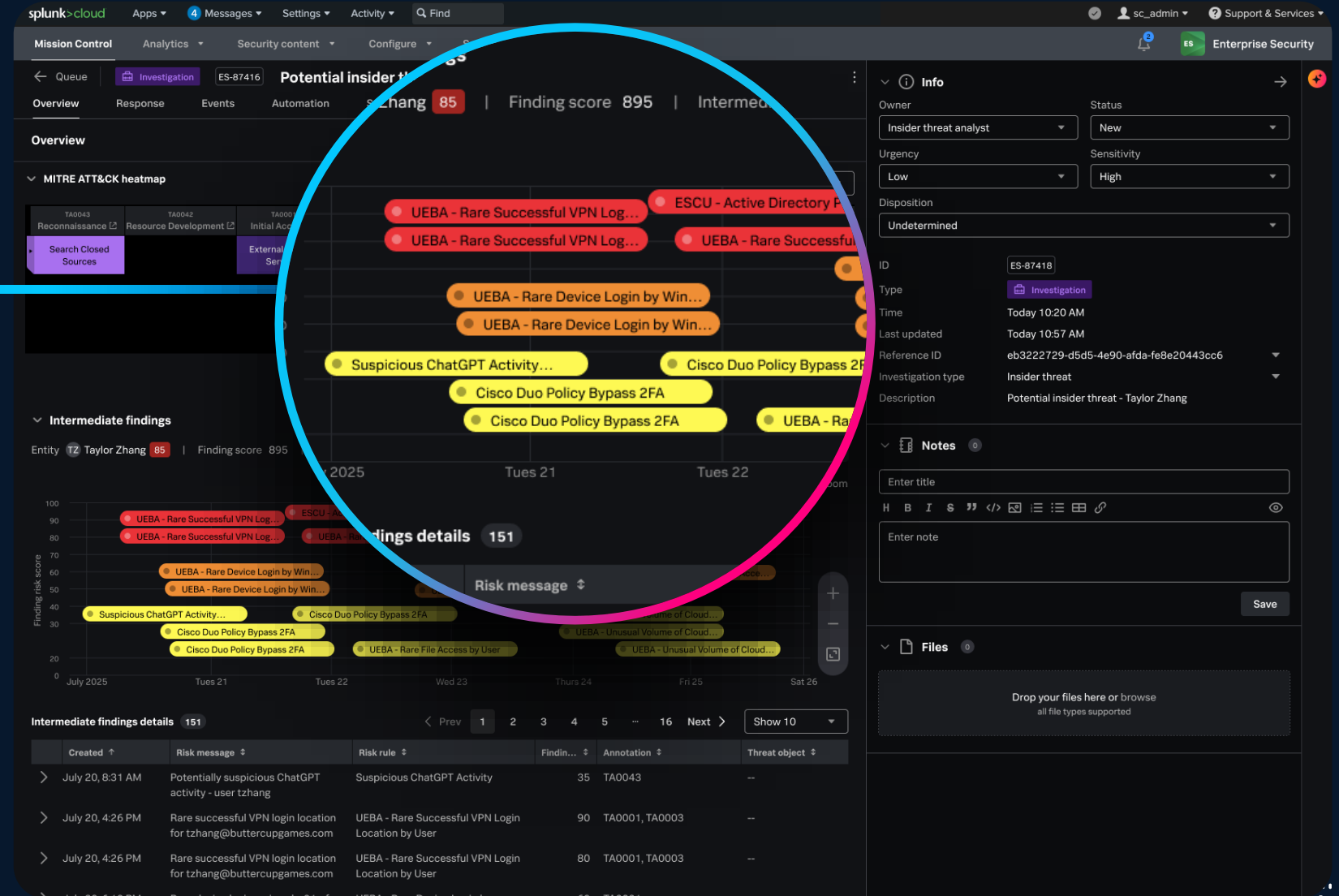
Simplify the
analyst
experience

Accelerate the
SOC with AI &
automation

Expand detection
and visibility

Enterprise Security Premier Edition

- Includes UEBA, SOAR and AI Assistant
- Simplify your analyst experience
- Gain full visibility and control



Security Operations must evolve

Simplify the
analyst
experience

Accelerate the
SOC with AI &
automation

Expand detection
and visibility

AI Assistant in Enterprise Security

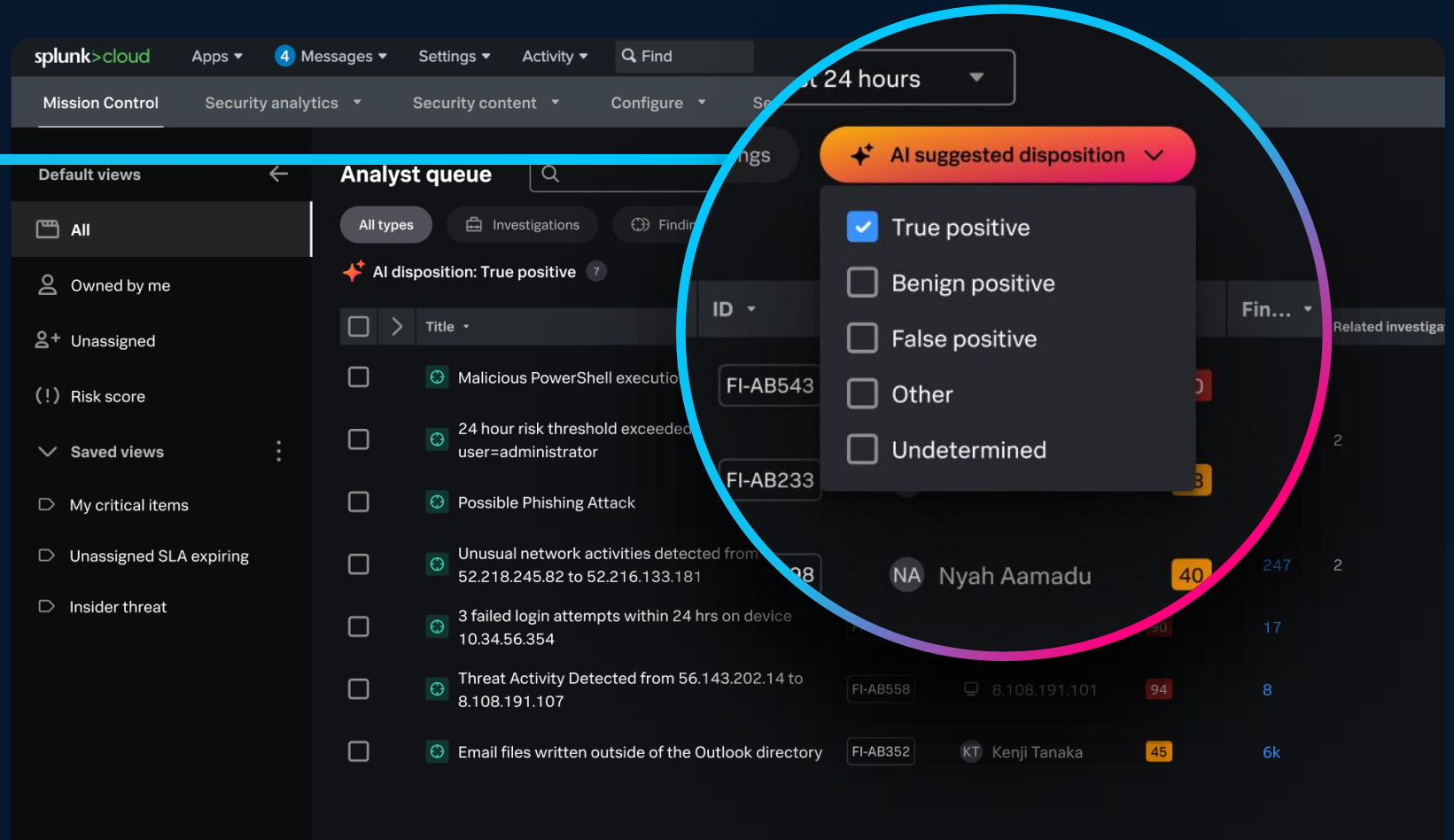
- Embedded across all analyst workflows
- Guide investigations with AI-powered query generation and summarization
- Accelerate workflows with embedded, context-aware AI insights
- Empower decisions with AI-driven next step and remediation guidance

Currently available for Cloud users

The screenshot displays the Splunk Enterprise Security interface with the AI Assistant for Security panel. The panel shows a finding titled "Malicious PowerShell execution" with a finding summarization and a sandbox analysis. The finding summarization states: "On July 25, 2025, an obfuscated PowerShell command was executed using the EncodedCommand flag by a low-privilege user during off-hours. The script contacted a known C2 domain (185.99.132[.]22) linked to the MuddyWater APT group, as confirmed by Cisco Talos threat intel." The sandbox analysis states: "Sandbox analysis showed the script downloaded a second-stage payload, created a scheduled task, and attempted credential theft. Shortly afterward, the host initiated SMB-based lateral movement, indicating early-stage compromise activity. Given the behavioral indicators and threat intel correlation, this is assessed as a True Positive requiring immediate response." The interface also shows a table of findings and a sidebar with related investigations and history.

Triage Agent

- Streamline alert prioritization
- Plan and execute investigations
- Automate insights to reduce MTTR



Security Operations must evolve

Simplify the
analyst
experience

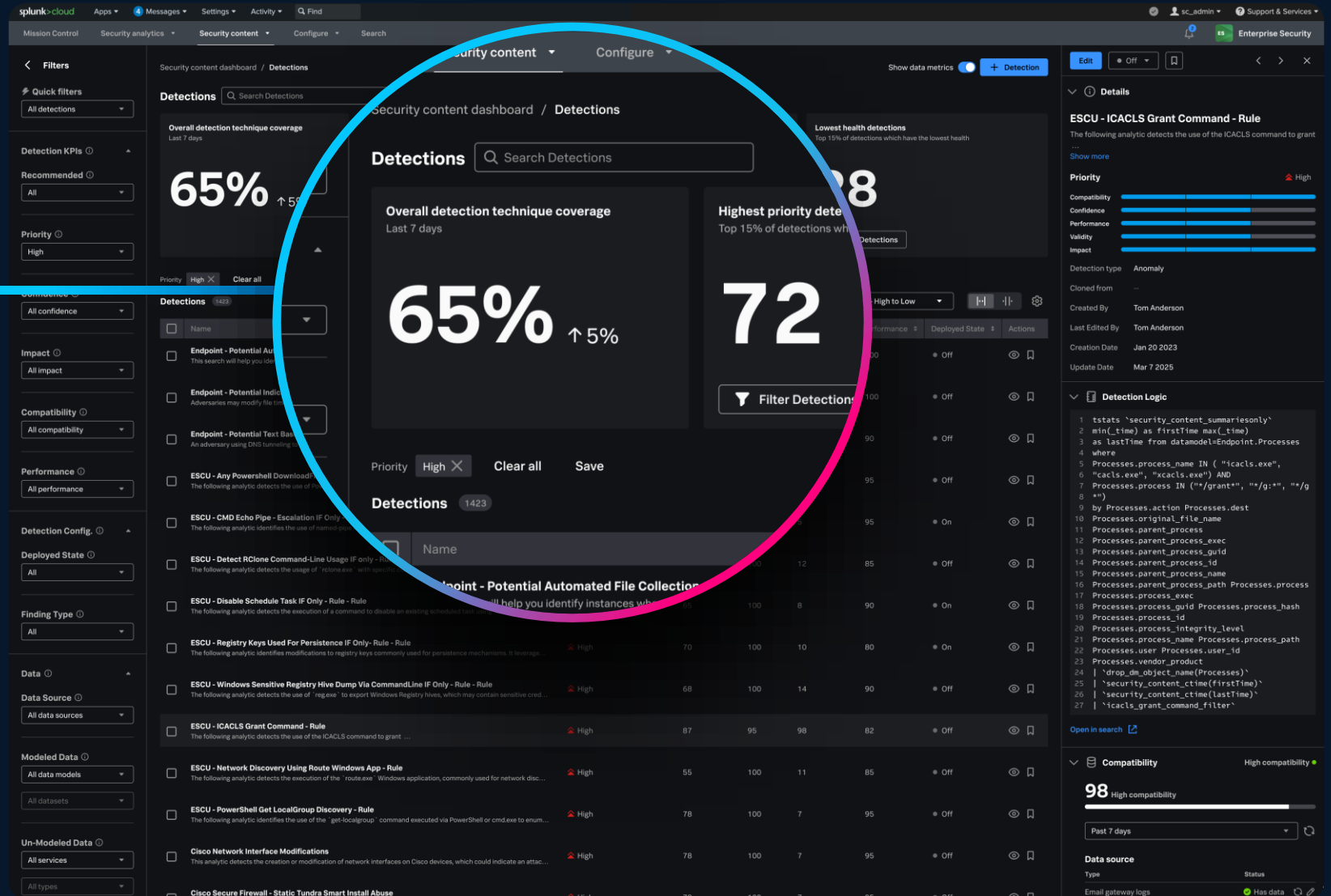
Accelerate the
SOC with AI &
automation

Expand detection
and visibility

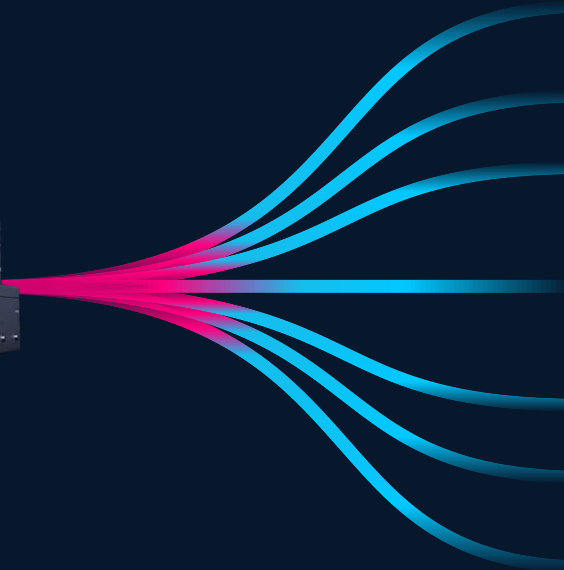
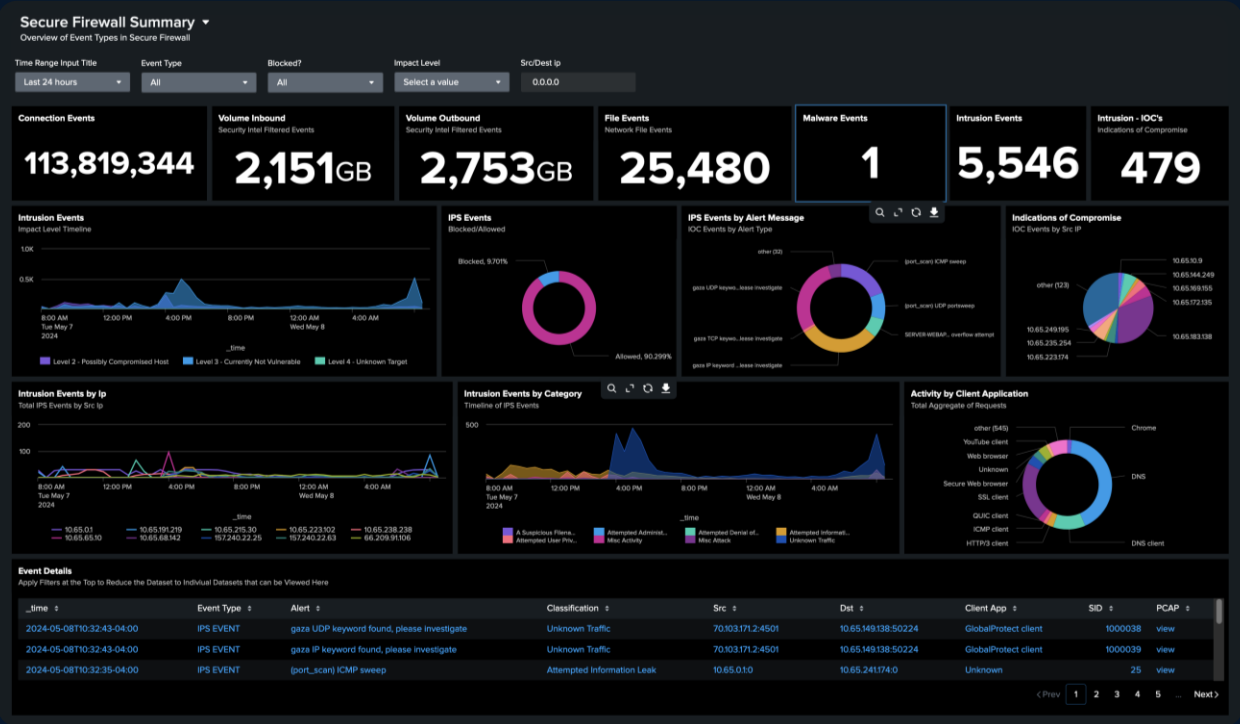
Detection Studio

Author and tune detections

- Streamline detection creation workflows
- Evaluate detection health
- Expand versioning and detection-as-code



Free ingest of Cisco Firewall logs in Splunk



*Ingest up to 5GB/device/day requires Firewall Threat Defense subscription and Splunk license

Splunk and Isovalent

Tackle new threats with expanded visibility

- Monitor and detect emerging risks to open source LLMs like Ollama
- Utilize Splunk Data Management to ensure visibility
- Activate investigations and automation within Splunk Enterprise Security

The screenshot displays the Splunk Enterprise Security (ES) interface. The main panel shows a list of findings under the 'Analyst queue' (547). The findings are sorted by risk score, with 'Ollama Path Traversal' (FI-AB543) at the top, having a risk score of 80. Other findings include 'Malicious powershell execution' (FI-AB233), 'User access from unknown location' (ES-AB416), and 'Geographically Improbable Access Detected' (FI-AB410).

The right-hand panel provides a detailed view of the 'Ollama Path Traversal' finding. It includes fields for Owner (Unassigned), Status (New), Sensitivity (Unknown), and Urgency (Medium). The Disposition is set to 'Undetermined'. The 'Fields' section shows the following details:

- Pinned:** Yes
- Last updated:** Today, 5:57 AM
- Entity:** Ollama pod (80)
- Time:** Aug 10, 2025 7:21 AM
- Detection:** Ollama Path Traversal
- Entity priority:** high
- Entity type:** system
- MITRE:** T1083
- Original Splunk source:** Isovalent Runtime Security
- Security domain:** CVE

The 'Cisco Talos threat intelligence' section shows the finding is 'Untrusted' and categorized as 'Spyware and Adware'. The 'Drilldown search' section shows 'Federated search - Network data'. The 'Related investigations' section shows 1 related investigation, and the 'History' section shows 0 history items.

Splunk Integrations with Cisco

Drive Digital Resilience in the AI Era



Anton Eksteen

Head of Networks and
Reliability Engineering

splunk>
a **CISCO** company

Patrick Lin (PCL)

SVP and GM, Splunk
Observability



About Hospital Contributions Fund (HCF)

- **Australia's largest** not-for-profit health fund
- Provides **2 million+ members** health, life, travel, pet, home and car insurance
- **89¢** of every dollar returned in benefits
- **Cisco & Splunk customer** (Catalyst Center, ThousandEyes, Splunk Cloud, Observability Cloud, AppDynamics) + partner with **AC3**
- **2 Data Centers**, AWS & Azure for Cloud
- **54 branches** + dental, eyecare and call centers
- Mix of in-house developed + some common SaaS products.



Anton Eksteen

Head of Networks and
Reliability Engineering

splunk>
a **CISCO** company

Patrick Lin (PCL)

SVP and GM, Splunk
Observability



Anton Eksteen

Head of Networks and
Reliability Engineering

splunk>
a **CISCO** company

Patrick Lin (PCL)

SVP and GM, Splunk
Observability



Anton Eksteen

Head of Networks and
Reliability Engineering

splunk>
a **CISCO** company

Patrick Lin (PCL)

SVP and GM, Splunk
Observability



Anton Eksteen

Head of Networks and
Reliability Engineering



Patrick Lin (PCL)

SVP and GM, Splunk
Observability



Anton Eksteen

Head of Networks and
Reliability Engineering



Patrick Lin (PCL)

SVP and GM, Splunk
Observability



Anton Eksteen

Head of Networks and
Reliability Engineering



Patrick Lin (PCL)

SVP and GM, Splunk
Observability

Next Steps to Learn More

**Attend our Splunk
breakout sessions**

**See a live demo in the
World of Solutions**

**Sign up for a hands-on
Splunk Workshop**

