Building An AI-ready Data Foundation For The Agentic AI Era
代理式 AI 驅動的次世代資安平台

Turn Data Chaos Into AI Clarity

Lawrence Chiang 蔣佳賓 北亞區售前技術總監
Sr. Leader, Solutions Engineer, Greater China
Splunk, a Cisco Company

7th July 2026

A dual force revolution is happening
一場雙重力量的革命正在發生

Rapid growth in demand for AI & agentic apps

Exponential growth of machine data

But Complexity...
但是事情更加複雜了...

資料孤島與複雜度正在升級

營運效率與安全性受到破壞

解鎖人工智慧下一個前沿的限制

How They Use Splunk to Integrate with the 3rd Party LLM and Maximize the Data Value

指標客戶透過 Splunk 放大資料價值

cisco

AI Toolkit (MLTK)

in Splunk Enterprise

Vendor Agnostic

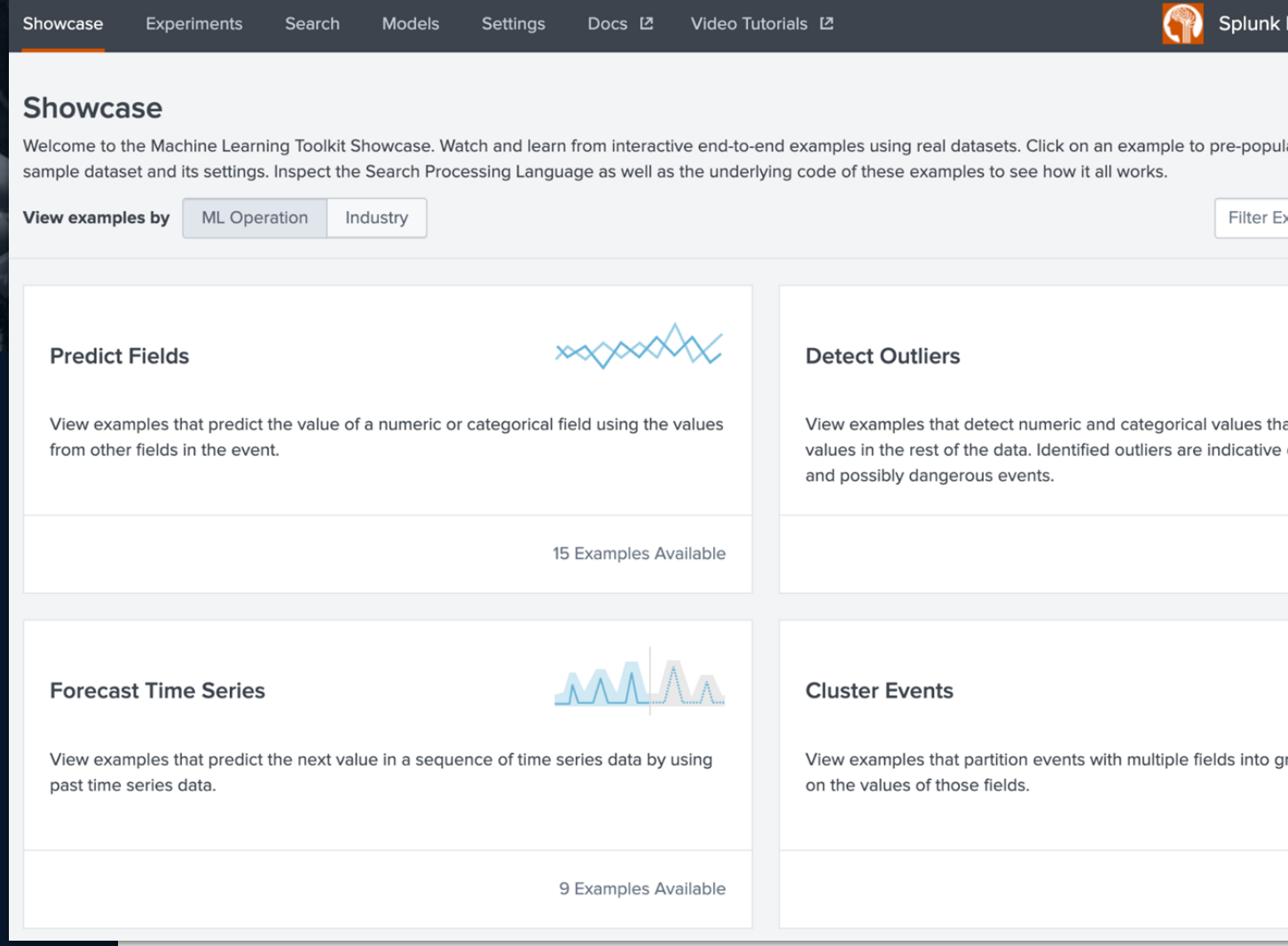
Flexible integration with any LLM no vendor lock-in.

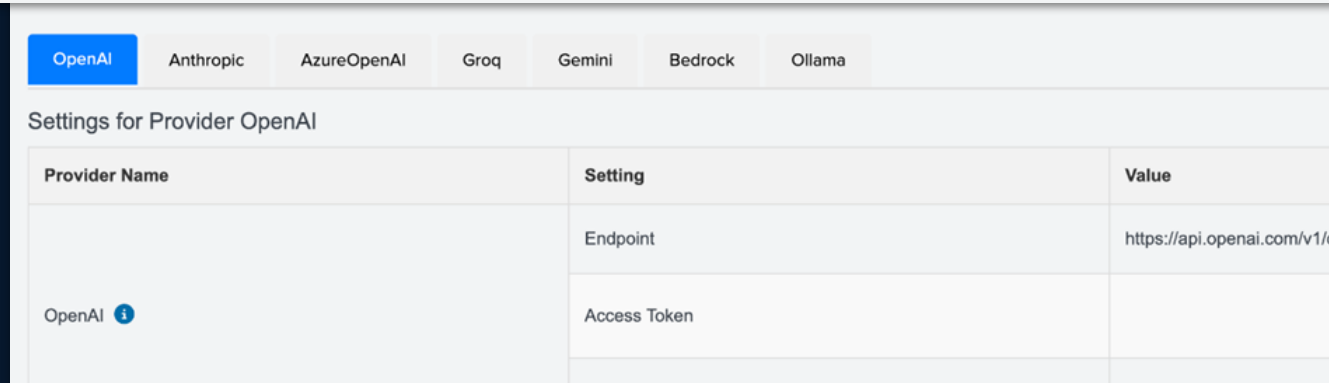
Native Experience

Built-in to Splunk for intuitive, seamless operations.

Knowledge Synergy

Integrates in-house data to optimize RAG performance.



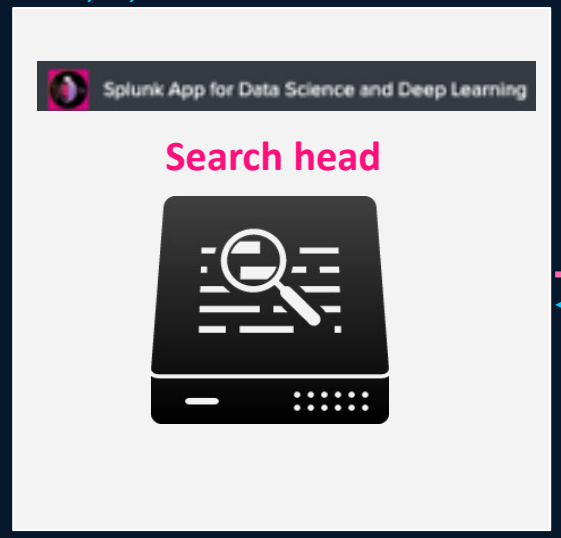


Architecture of LLM Integrations

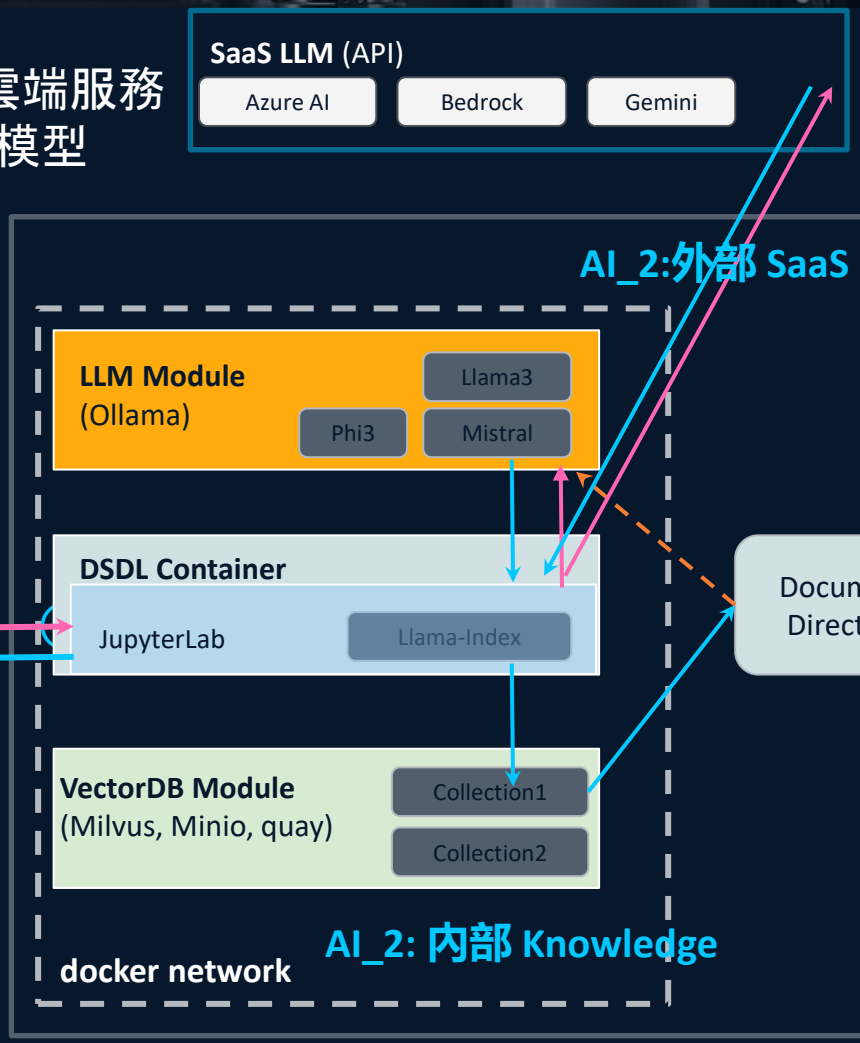
LLM 可以連接至雲端服務
或是地端 Host 的模型

AI_3:根據你過往的 ticket 處理方式, 你應該做 1, 2, 3...

Step1 : 如何解決此錯誤問題?



AI_1: Fit 指令



Maximize the full value of your data

快速部署、提升可視性、發掘洞見、更快解決問題
一同時降低成本

Rapid Deployment to integrated AI/LLM, RAG, Grounding on Splunk.

Rapid deployment

Within **2** weeks

Enhance Specific for Security Threat Intelligence Collection capacity

30x capacity gain in risky intelligence collection

Workforce Efficiency for overall Productivity improved

60%+ improvement productivity and manpower utilization

cisco

Data & AI are unlocking new opportunities
數據與AI帶來了新的挑戰與機會

More Complexity...
事情真的更加複雜了...

數據孤島與資料管理跨雲與地端資料管理者面對更複雜的架構

Agentic AI 的導入使得機器數據呈指數級激增管理成本也激漲

當 Agentic AI 擁有自主決策權使得系統的透明度與安全管理變得棘手

Agentic AI Era Demands New Data Strategy

代理式AI時代 您 需要新的數據策略

cisco

Introducing

Cisco Data Fabric

思科AI世代 數據織物架構

A revolutionary new architecture, powered by Splunk,
to harness the value of machine data with AI
由Splunk驅動的革命性全新架構，利用AI駕馭機器資料的價值

cisco

It is time for a data fabric built for the Agentic AI era

專為人工智慧時代打造的全新一代超級數據架構

Usage and value of data changes overtime
數據的使用與價值會隨著時間而變化

High Performance
Prevention, Detection, Monitoring

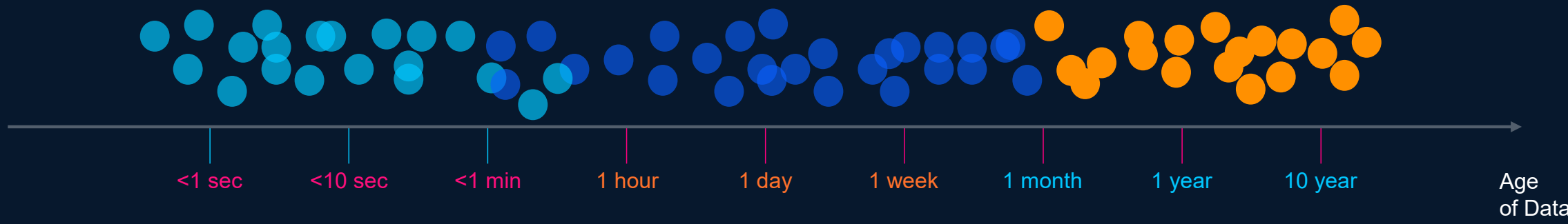
Search & Analytics for highest performance with configurable data retention. Real-time, high frequency

Performance at Cost
Incident Investigation, Threat Hunting

Analytics and ML for performance on data at later stages, subject to data lake latency.

Compliance
Audit, Forensics, Compliance

Search for less performant scanning of archived & long term data, as-needed.



Data still needs to cataloged, governed, prepared, and auditable – more than ever now with AI

Cisco Data Fabric powered by Splunk
由Splunk引動新一代思科數據織網

信任與治理 Trust & Governance

Cisco Data Fabric

AI-powered Data Management
AI驅動數據管理

Federated Search
聯邦搜索與分析

AI-Native Experiences
AI原生體驗

Platform AI Tools
多種AI代理工具

開放與可擴展 Open & Extensible

Machine Data Lake 新一代AI導向 機器數據湖

Strategical Team-up in AI era
通過收購、投資和戰略合作增強 AI 能力

收購

splunk> a CISCO company

Armorblox now part of CISCO

MindMeld

babblelabs

PERSPICA

voicea

ACCOMPANY

Galileo

WideField

投資

ROBUST INTELLIGENCE

DataRobot

cogniac

moogsoft Continuous Assurance

securiti

habana

AISERA

dremio

uniphore

Paxata

10 億美元投資基金
AI 基礎設施和 AI 軟體

戰略合作夥伴關係

NVIDIA

AMD

intel

aws

Microsoft

scale

MISTRAL AI_

cohere

針對經銷商的AI合作夥伴
專業認證教育訓練

CISCO

Splunk AI Journey

AI Assistants

AI Agents

AI Platform & Extensibility

Detection Builder Agent (Alpha Coming)
Goes from detection hypothesis to production in minutes. Imports, tunes, and tags detections

AI Canvas in Splunk (Alpha)
Driving AgenticOps, Cross domain collaboration across Cloud, Network, Security, Apps

Guided Response Agent (Alpha Coming)
Automatically executes response actions based on SOP

Automation Builder Agent (Alpha Coming)
Translate natural language into functional, tested SOAR playbooks

Agent Builder (Private Preview)
Create, test, and deploy an AI agent

SOP Agents (Alpha)
Importing SOPs into response plans using LLM

Malware Threat Reversing Agent (GA)
Give analysts instant insight into malware threats, providing summaries and step-by-step breakdowns of malicious scripts

AI Assistant for Security (GA)
Guided investigation workflow, Event summarization, Remediation suggestions,

Triage Agents (Alpha)
Autonomously enrich, prioritize, and explain alerts, greatly reducing the fatigue put on analysts

Time-Series Foundation Model (Alpha)
Univariate zero-shot forecasting

AI Assistant (GA)
Agent Mode allows for agentic response generation in the assistant

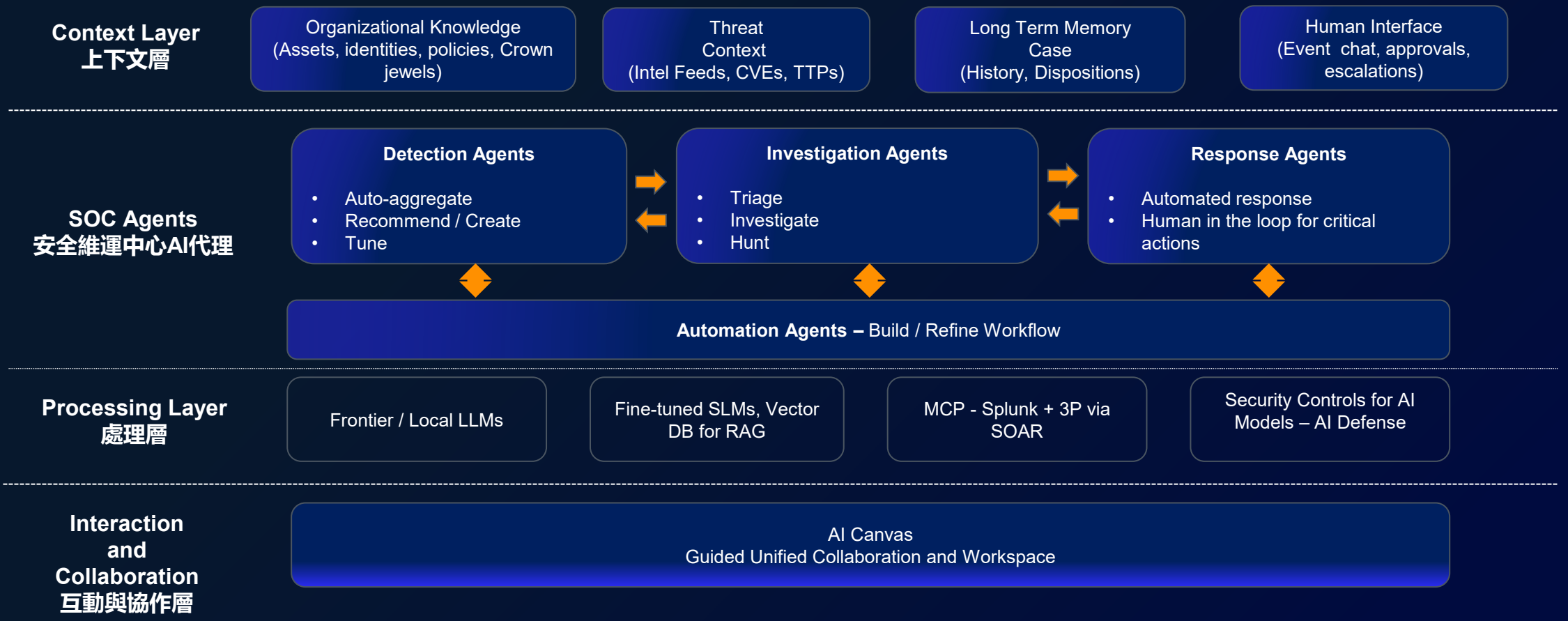
AI Assistant for SPL (GA)
Use Natural Language to create SPL

Foundation-Sec-8b Model (GA)
Open-source Security LLM

AI Toolkit (GA)
External LLM integrationn. Splunk-hosted LLM

Splunk MCP (GA)
Allow External Agent-to-Agent communication with Splunk

Agentic SOC Architecture
代理式AI安全維運中心架構

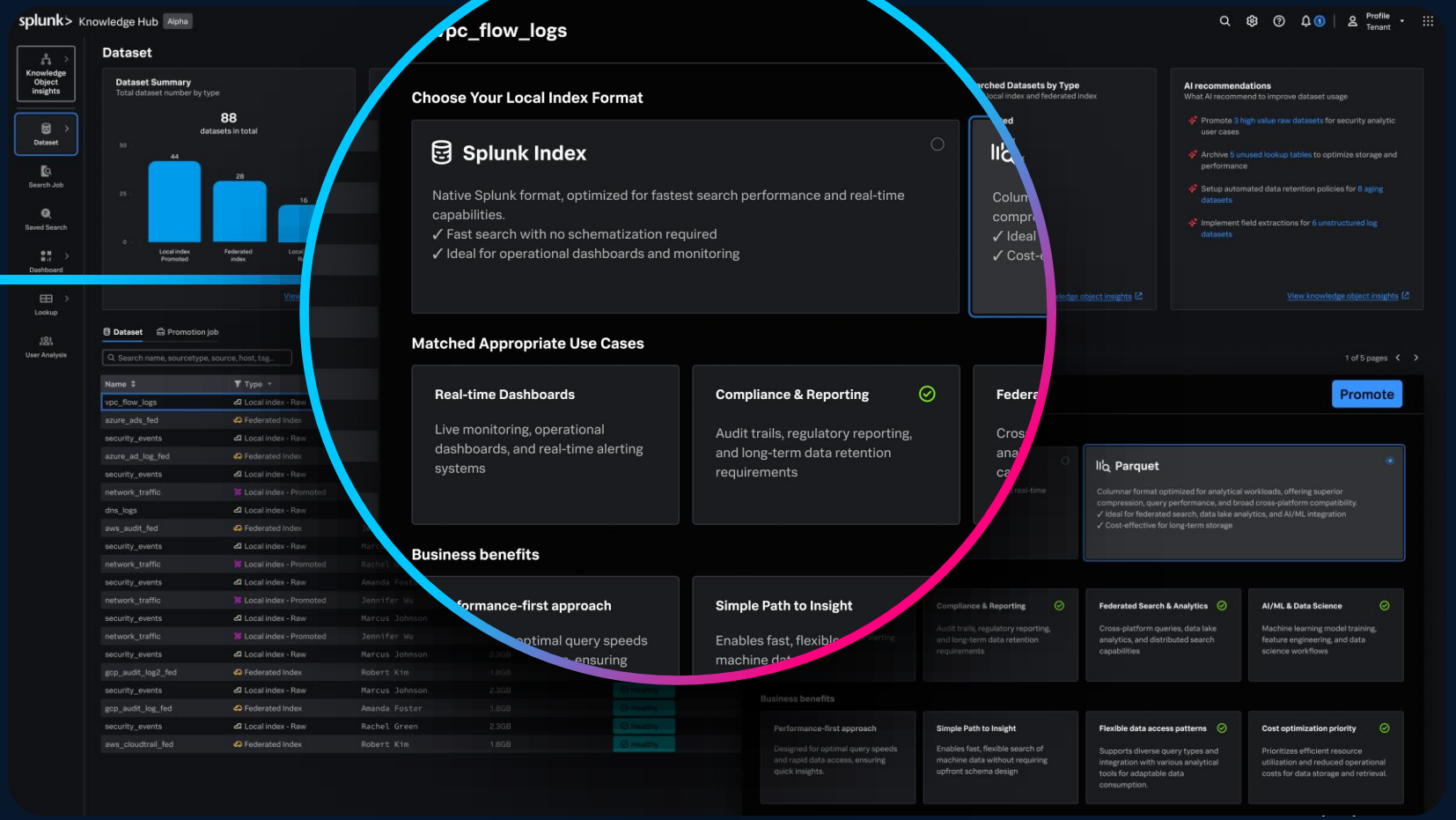


Land your machine data and use as needed
保存機器數據並 按需調用

Machine Data Lake
機器數據湖

Alpha February 2026

- Turn machine data into advantage
- Integrate for AI-ready insights
- Scalable, secured, governed



Maximize your data value with Machine Data Lake
利用機器數據湖最大化資料價值

- Land all your machine data cost effectively, use as-needed

- Central landing zone
- Catalogued & Organized
- Search In Place
- Ready for AI via MCP integration

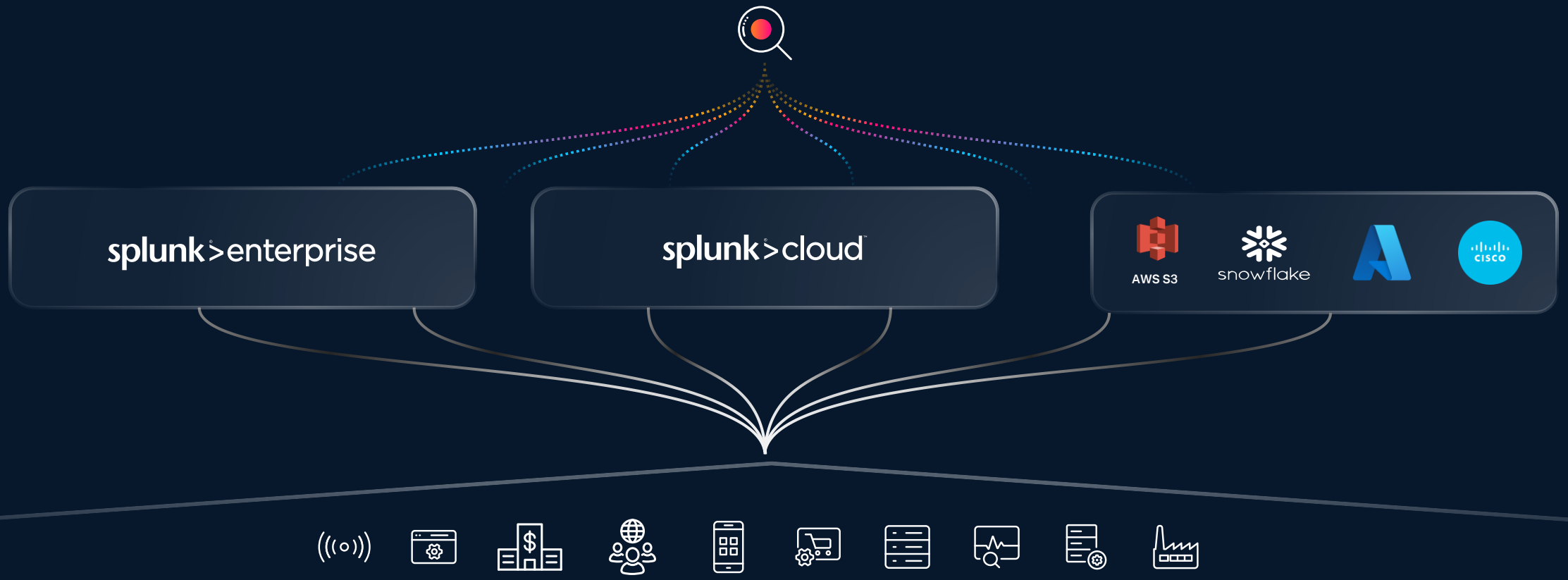
- Browse & Filter Data Slices
- Analyst Experience, Governed

- Right Structure for the Right Job
- Data Window
- Indexing, Parquet

- Query, Investigate
- Train ML model
- API data access for AI and other applications
- Ready for AI Reasoning

Federated search: breaking down data silos

聯邦搜索: 打破數據孤島



Next generation delivering additional destinations with simplified onboarding and querying

How to use Machine Data Lake and Federation

基於效能與成本考量的4種機器數據湖與聯邦搜索使用案例

1

Full Capability Searches

Traditional Index + Search

- Detections (CIM)
- Infra/Service monitoring
- Active investigation (14d)
- Troubleshooting (14d)

Best for heavy usage and frequent searches

2

Enriched Searches

MDL Lakehouse + Search

- Detections (OCSF/SPL2)
- Active investigation
- Troubleshooting
- Scheduled reports
- Future AI/ML

Balanced mix for enriched searches and future AI/ML use cases

3

Limited Capability Search

MDL Ad-hoc + Search

- Audit/compliance
- Threat hunting
- Investigation, troubleshooting
- Historical IOC hunting

Best for data retention over long periods of time

4

Limited Capability Search

3rd Party + Federated Search

- Use case support depends on data shape & format
- Audit, Compliance
- Investigations, Troubleshooting
- Threat hunting

Best when data needs to be external to Splunk, searched in-place with Federation

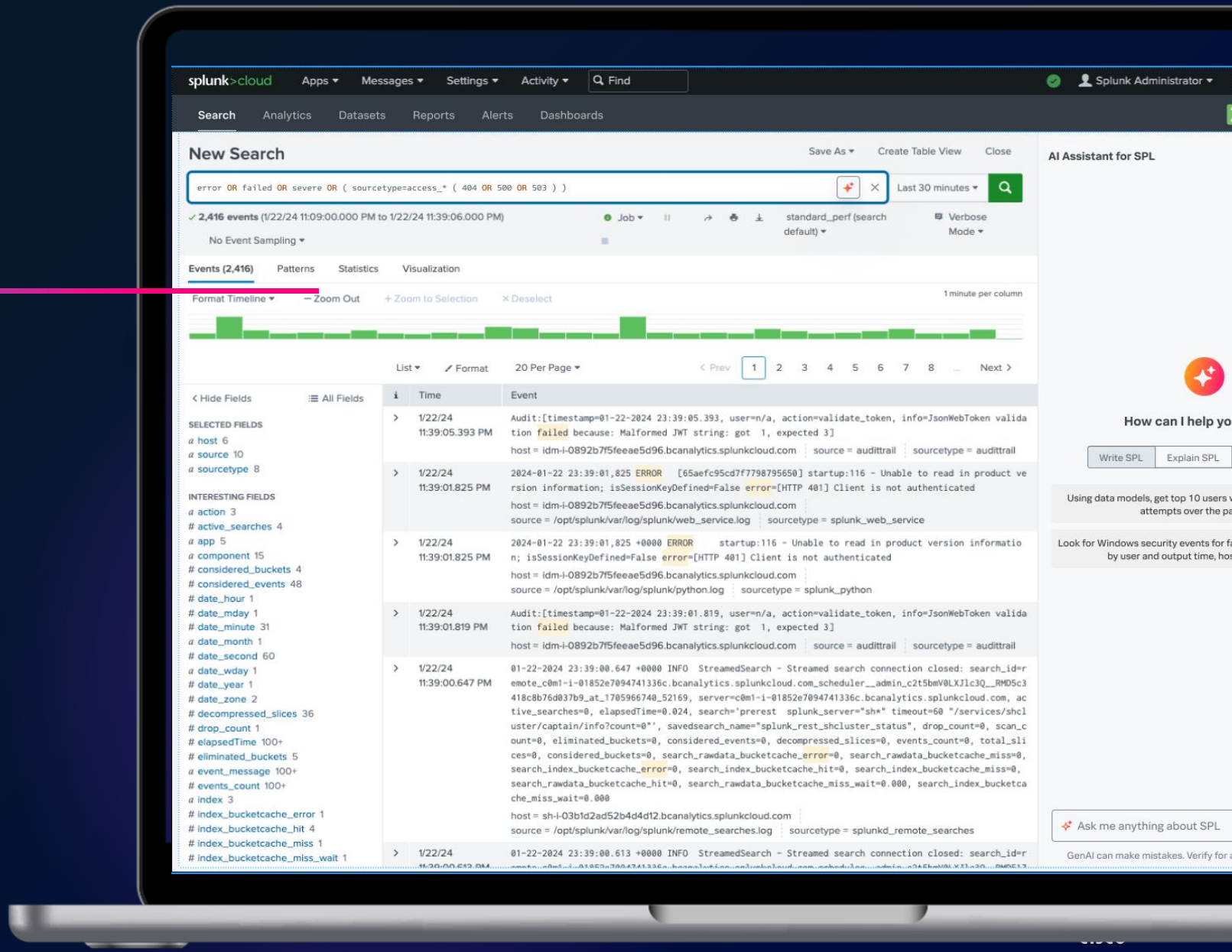
General Availability

AI Assistant AI助理

Generate SPL queries from natural language prompts

Personalized for your unique stack environment

Fully integrated into Search & Reporting in Splunk Enterprise



Alpha (GA in July)

AI-powered Data Management 數據管理

Transforming Data Onboarding, Processing & Monitoring

Guided Onboarding 引導式資料導入 ALPHA Now

Simplifies platform configuration with AI-powered, best-practice architectural guidance

Automated Field Extraction 自動欄位提煉 ALPHA Now

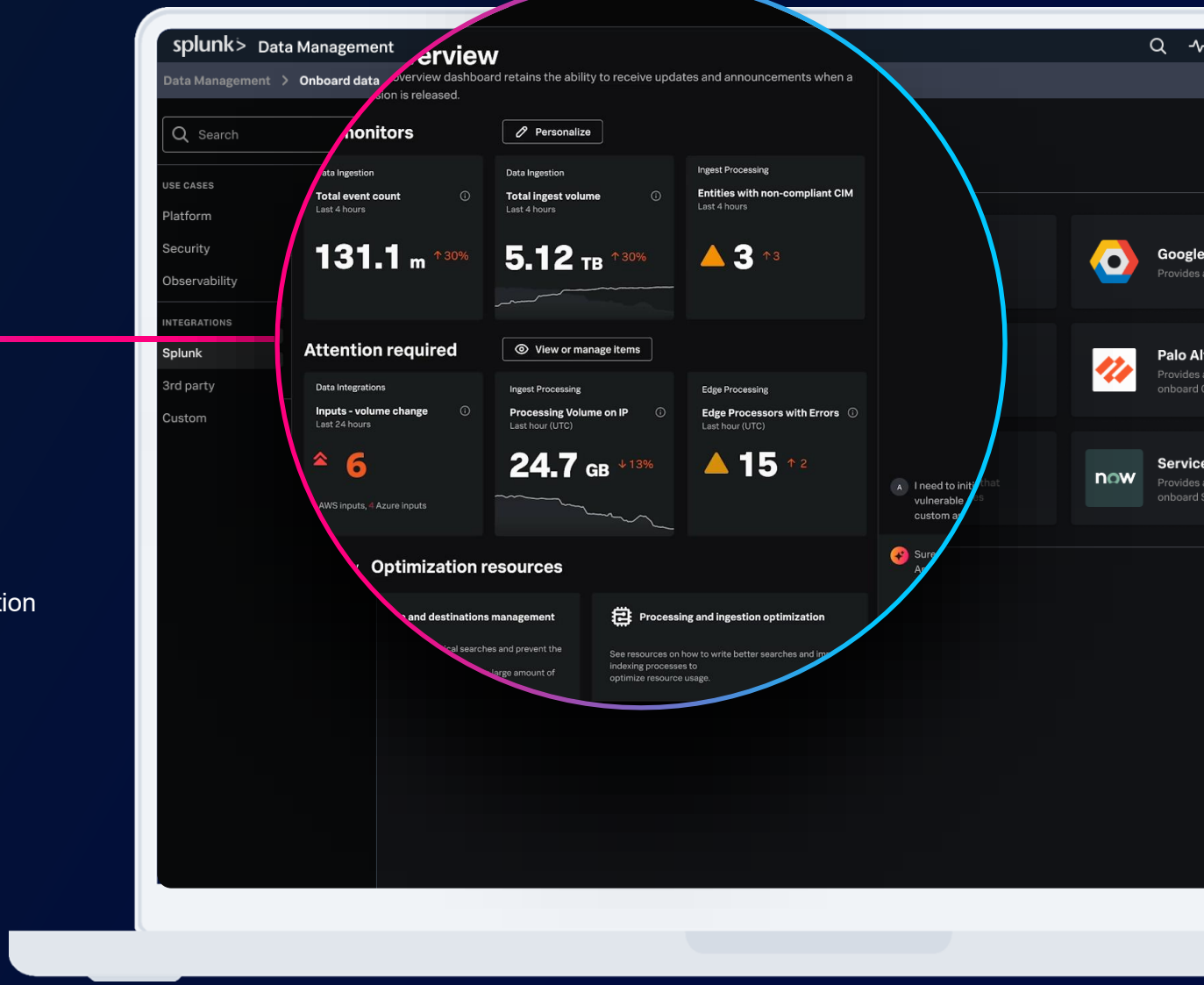
Replaces manual, error-prone regex tasks with AI-driven, intelligent log classification and field extraction

Auto Schematization 自動圖示化 ALPHA Now

Accelerates security operations by leveraging LLMs for automatic CIM-compliant, analytics-ready data normalization

Self-Healing Pipelines 自我修復 ALPHA in April

Ensures continuous data integrity through automated monitoring, diagnosis, and self-repair.



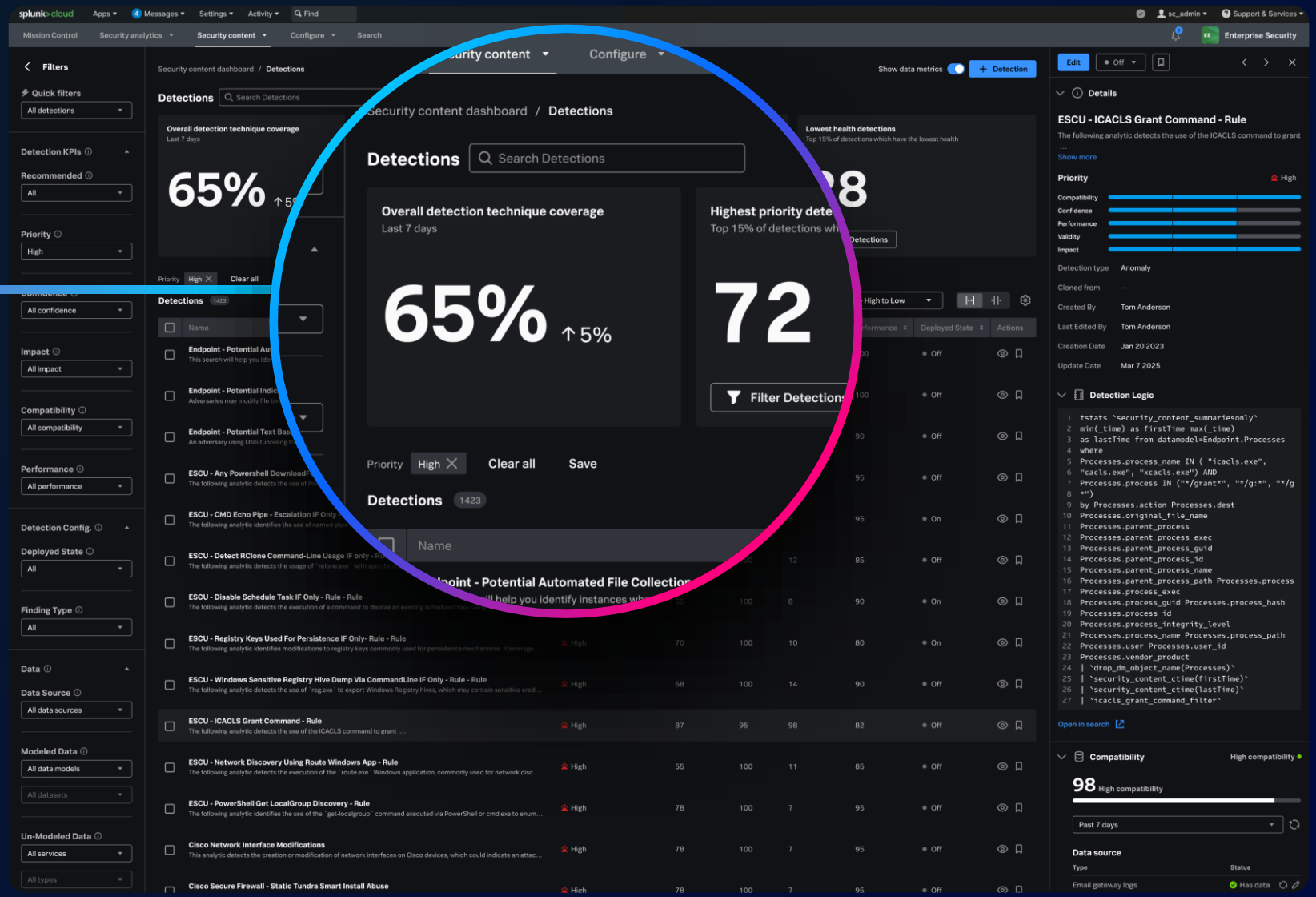
For Splunk Cloud Platform and Splunk Enterprise
Product names in Alpha and Beta subject to change before GA.

General Availability

Detection Studio
偵測工作室

Powered by SnapAttack

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

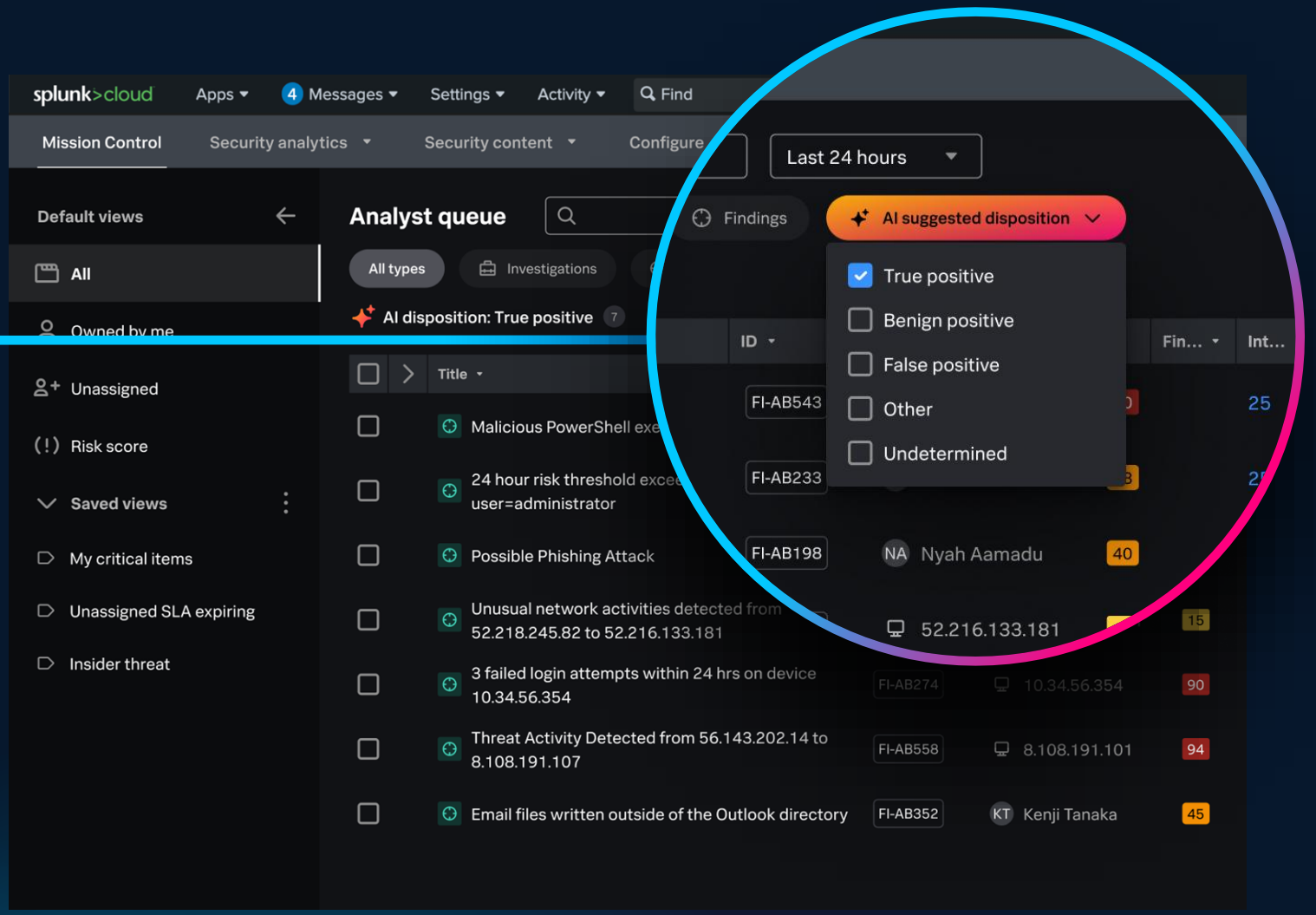


Coming Soon

Triage Agent
診斷代理人

ALPHA APRIL 2026

- Streamline alert prioritization with AI-driven triage
- Rely on agentic AI to plan and execute investigation steps
- Reduce workload and MTTR through automated insights



Cloud-first release

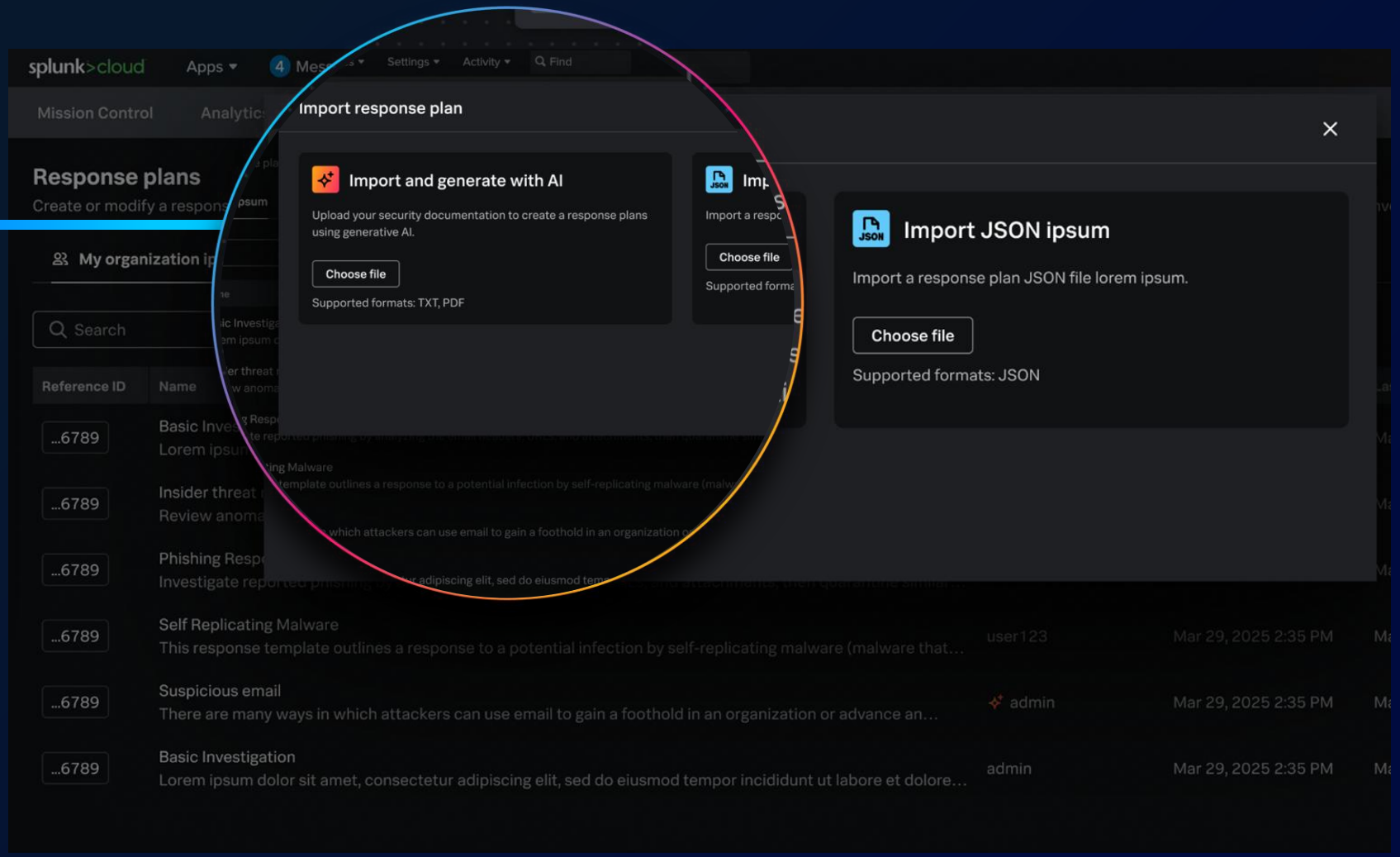
Coming Soon

SOP Agent

標準作業程序代理人

ALPHA APRIL 2026

- Import your SOC's SOPs into ES case management
- Multimodal AI translates the document into a response plan
- Give AI a framework for agentic analysis



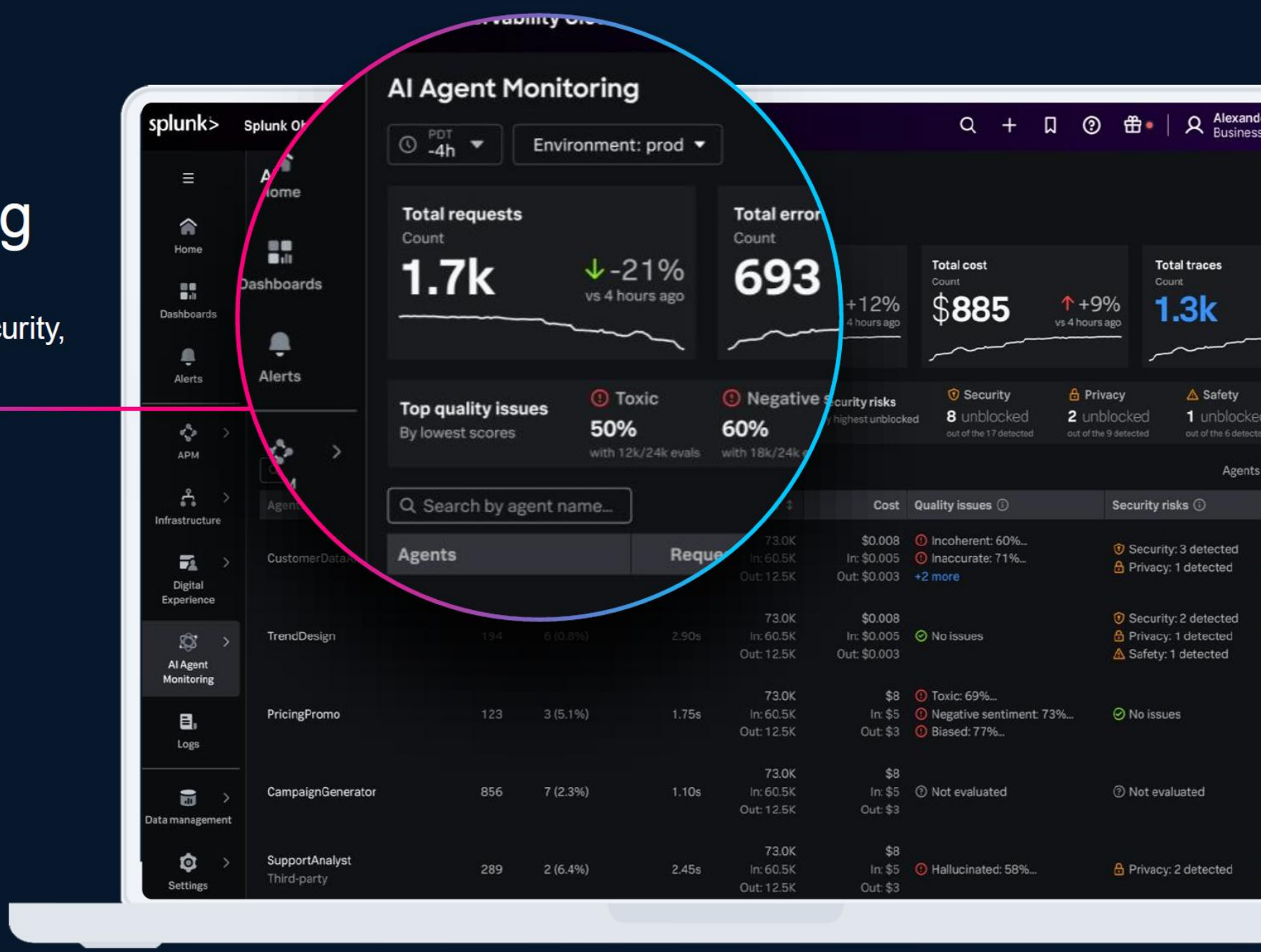
General Availability

AI Agent Monitoring

AI代理人監控

Monitor the performance, quality, security, and cost of your AI application stack

- Pinpoint and correlate the root cause of unreliable or degraded AI performance and agent behavior
- Measure and improve user experiences and increase trust with LLMs
- Mitigate security and compliance risks with Cisco AI Defense

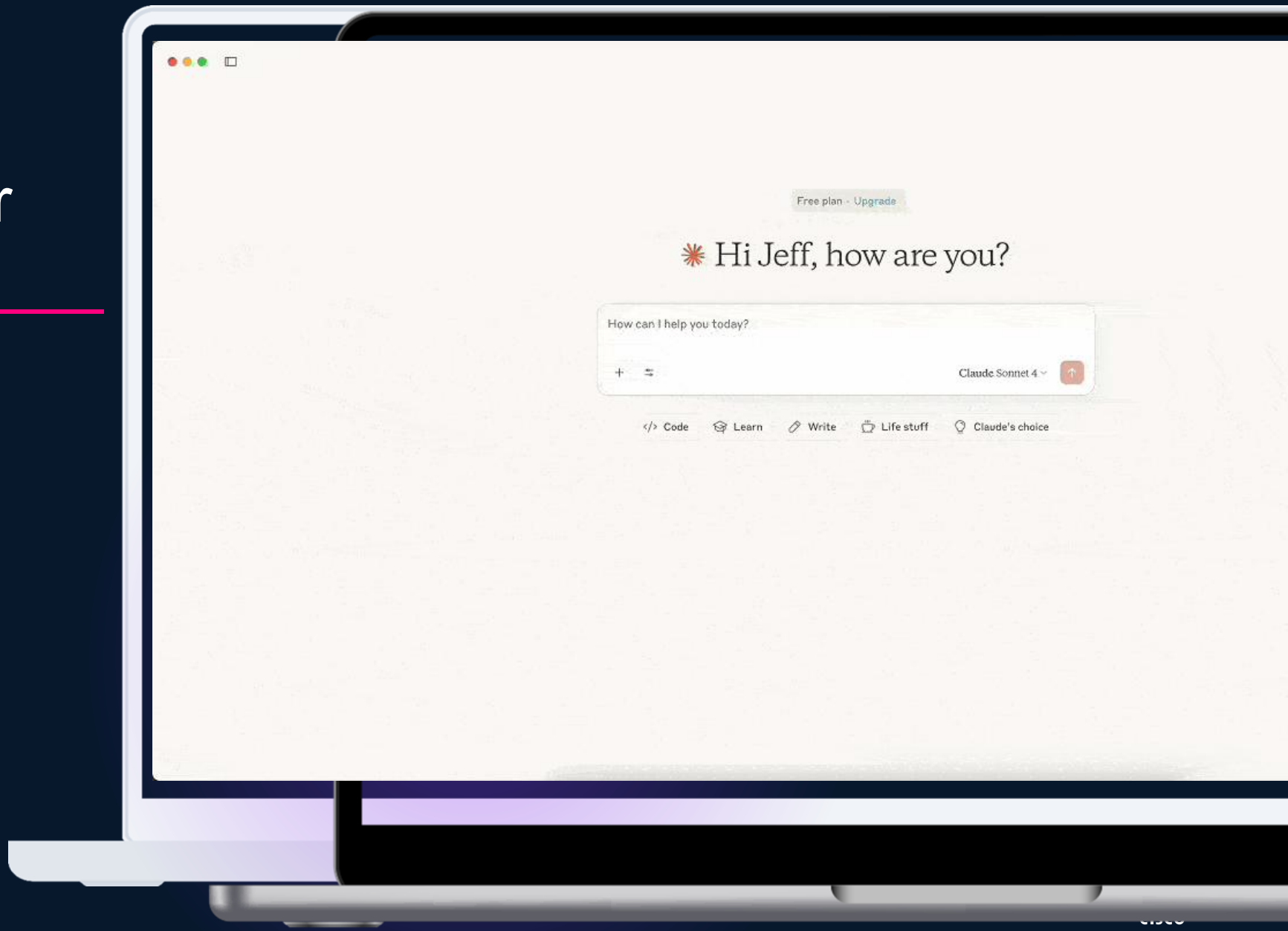


General Availability

Splunk MCP Server

模型上下文協定伺服器

- Secure bridge between Splunk Platform and AI using MCP Protocol
- Easier to use with natural language interaction
- Boosted productivity with automation
- Simpler integration with your own internal tools
- Enterprise-grade security and control

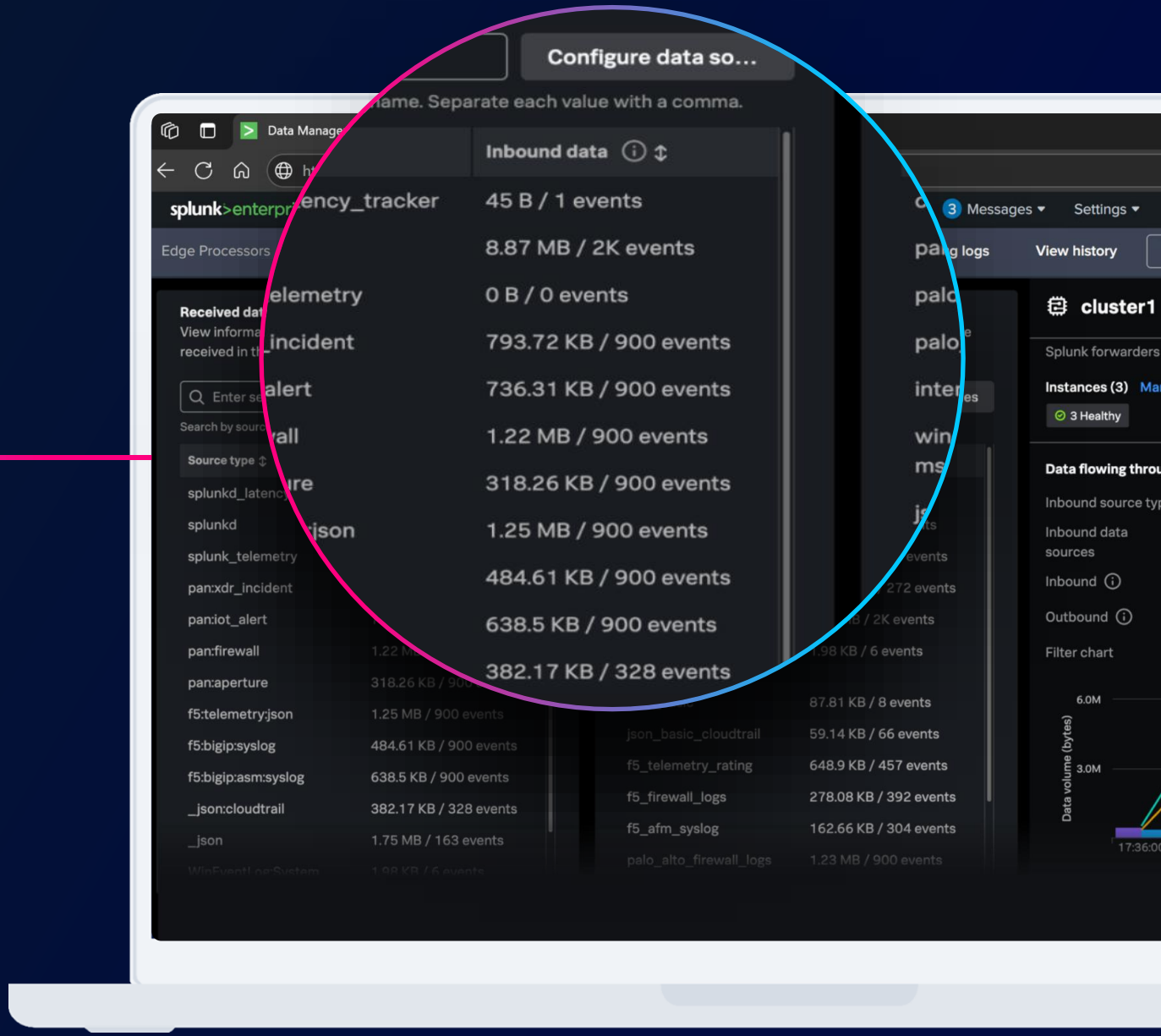


General Availability

Edge Processor for Splunk Enterprise 邊緣處理器

Bringing the power of SPL2 on-prem

- Greater control over data
- Enhance real-time visibility and response
- Strengthen data security and compliance



Available with Splunk Enterprise 10.0

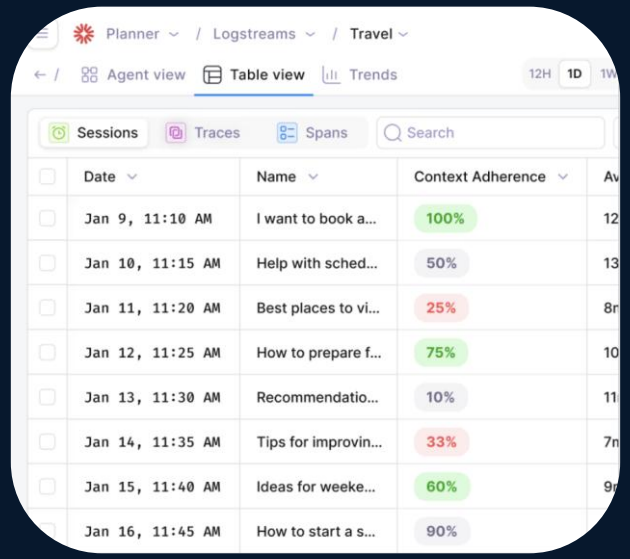
What Galileo can do 伽利略能做什麼

AI observability and evaluation across the agent development lifecycle

AI 可觀察性與評估，涵蓋代理開發生命週期

Testing 測試

Rapid pre-production evaluations
快速pre-生產環境評估

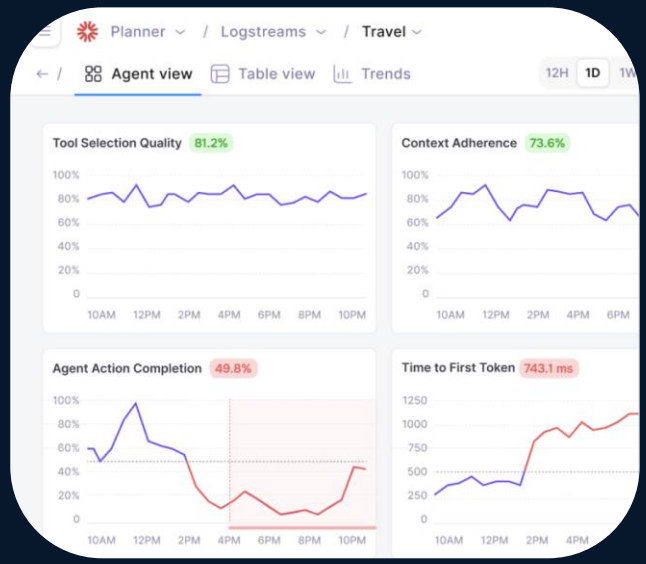


Offline experimentation and testing playground

離線實驗與測試遊樂場

Monitoring 監控

Real-time AI observability
即時AI可觀測性

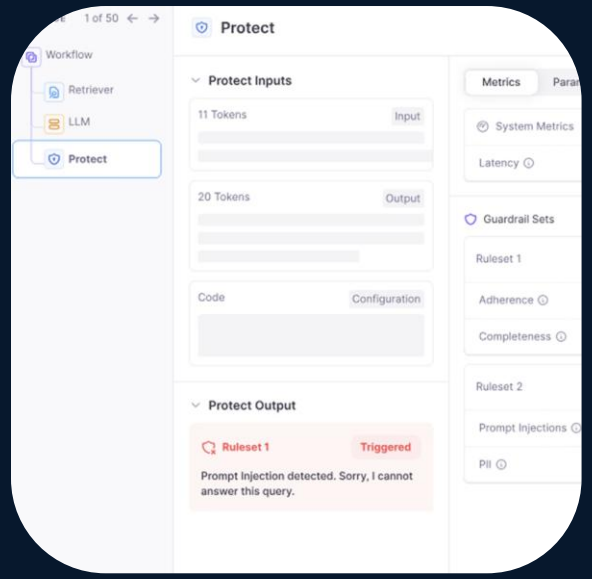


Real-time monitoring and rapid debugging in production

生產環境的即時監控與快速除錯

Protecting 保護

Real-time guardrailing
即時護欄



Real-time interception of prompts and harmful outputs in production

在生產環境即時攔截提示詞與有害輸出

Cisco + Splunk = Complete Digital Resilience
完整的數位韌性

Platform Resilience
大數據平台韌性

- Unified insights across the enterprise with data at massive scale

Preemptive Security
先發制人的資安解決方案

- Mitigate threats with agentic real-time threat monitoring
- Investigate and remediate threats faster with AI-powered automation

End-to-End Observability
端到端的可觀測性

- Observe AI with full stack, silicon to agent monitoring
- End-to-end network, application, and infrastructure monitoring

cisco

CISCO Connect

Thank you