CISCO Connect

Powering Digital Resilience in the Agentic AI Era
代理式 AI 時代的數位韌性

Hao Yang 仰顥
Vice President, AI, Splunk/Cisco
Splunk/Cisco AI部門 副總裁

Frontier AI models are creating an entirely new level of risk for every organization

前沿 AI 模型正為所有企業組織帶來全新層級的風險

> It lowers the threshold for attackers, empowering less-skilled actors to launch complex, high-impact campaigns.
>
> AI大幅降低了駭客的技術門檻，讓菜鳥攻擊者也能發動複雜且具高破壞力的攻擊行動.

Anthony Grieco
SVP and Chief Security & Trust Officer
Cisco

- More sophisticated attackers
  更高明的駭客組織
- More personalized attacks
  更具針對性的攻擊
- More places to attack
  更多可遭攻擊的節點

Source: Cisco Blog, “Rising to the Era of AI-Powered Cyber Defense, ” Anthony Grieco, April 7, 2026

And we all have significantly less time to respond
而我們能應對的時間卻大幅減少

THE AVERAGE TIME TO EXPLOIT VULNERABILITIES

駭客利用漏洞的平均時間

2018	2023	2025	2026
2.3 years	4.2 months	21.5 days	38 hours

Source: zerodayclock.com, May 28, 2026

Cisco’s approach to AI-era cyber defense

思科對於 AI 時代的網路防禦策略

Industry collaboration & leadership
行業合作與領導力

Working with frontier AI labs like Anthropic and OpenAI to proactively identify, triage, and remediate vulnerabilities at AI speed

Existing code remediation
既有程式碼修復

Using early access to these frontier AI models to identify and remediate issues in our existing codebase

Development integration
開發生命週期整合

Enhancing our software development lifecycle to utilize these models to identify potential issues in newly developed code

Resilient infrastructure

Supporting our customers in proactively hardening their network infrastructure

Delivering customer innovation

Providing capabilities to help our customers leverage AI to prevent, detect, and respond to threats at machine speed and scale.

Expertise & partnership

Partnering with our customers on exposure reduction and continuous defense, bringing trusted expertise when it matters most.

Helping You Stay Ahead of AI-era Risks

助您領先一步，全面防範 AI 時代的新興風險

Industry collaboration & leadership

Working with frontier AI labs like Anthropic and OpenAI to proactively identify, triage, and remediate vulnerabilities at AI speed

Existing code remediation

Using early access to these frontier AI models to identify and remediate issues in our existing codebase

Development integration

Enhancing our software development lifecycle to utilize these models to identify potential issues in newly developed code

Resilient infrastructure
韌性基礎設施

Supporting our customers in proactively hardening their network infrastructure

Delivering customer innovation
推動客戶創新

Providing capabilities to help our customers leverage AI to prevent, detect, and respond to threats at machine speed and scale.

Expertise & partnership
專業知識與合作夥伴關係

Partnering with our customers on exposure reduction and continuous defense, bringing trusted expertise when it matters most.

cisco

Digital Resilience Must Evolve
數位韌性必須持續演進

Threats moving at machine speed
威脅正以機器速度來襲

Data volumes and costs exploding
資料量與成本激增

AI visibility and trust deficit
AI 缺乏透明度與信任危機

Splunk is the intelligence layer that powers agentic operations

Splunk 作為核心智慧層 驅動代理式 AI 營運

Predict and prevent at machine speed 以機器速度進行預測與防護

Unlock cross-domain insights at massive scale 解鎖大規模跨領域深度洞察

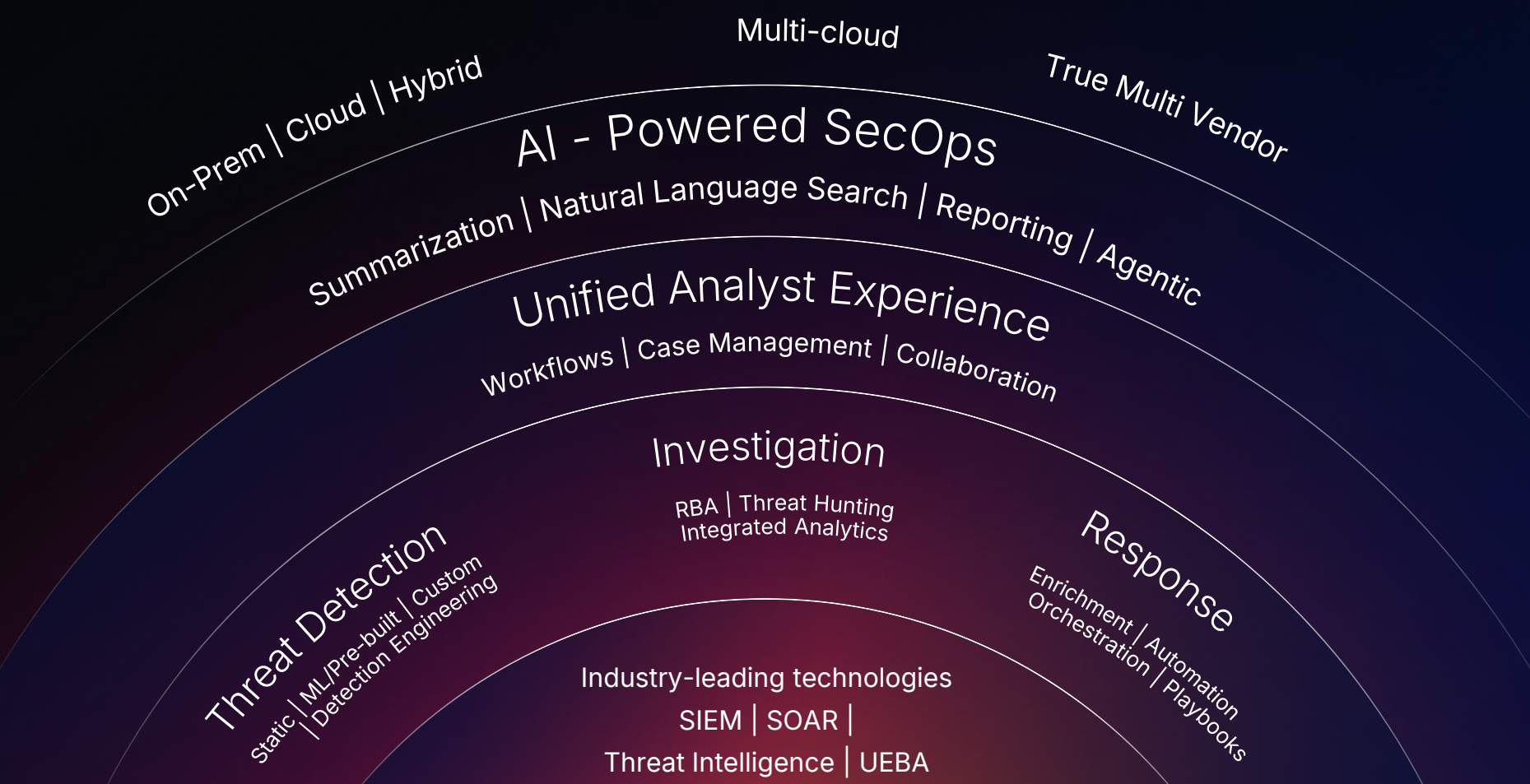
Build trust in AI with end-to-end visibility 透過端到端的全面可視性 化解 AI 信任危機

cisco

Powering the Agentic SOC

Splunk Security

Splunk Enterprise



Data Management & Federation SIEM | SOAR

Data Onboarding | Data Tiering | Scalable Index & Search | Pipeline Management | Federated Search | Federated Analytics

Security AI Agents

Built to detect and respond at machine speed

專為機器速度的偵測與回應而生

SPEED

Detection Builder Agent

SOP Agent

Malware Reversing Agent

Triage Agent

Guided Response/ Automation Builder Agents

cisco

Splunk is the intelligence layer that powers agentic operations

Splunk 作為核心智慧層 驅動代理式 AI 營運

Predict and prevent at machine speed 以機器速度進行預測與防護

Unlock cross-domain insights at massive scale 解鎖大規模跨領域深度洞察

Build trust in AI with end-to-end visibility 透過端到端的全面可視性 化解AI信任危機

cisco

Cisco Data Fabric powered by the Splunk

The System of Record and Intelligence Layer of the Agentic Enterprise

自主代理型企業的數據基石與智慧大腦

Data 資料

Unify Data at Scale for Faster, Safer AI

大規模整合資料 加速並安全推進AI應用

- Manage data at petabyte scale
- Land all data economically
- Tier data by use case

Context 上下文

Fuel Intelligence with Contextualized Machine Data

利用脈絡化的機器資料 全面驅動AI智慧防禦

- Catalog your enterprise
- Correlate relationships
- Surface insights

Action 行動

Activate the Agentic Enterprise to Move From Reactive to Predictive

賦能代理式企業 從被動因應到主動預測

- Deploy agentic operations
- Connect your agents
- Build proprietary AI

Network | Security | Application | Third Party

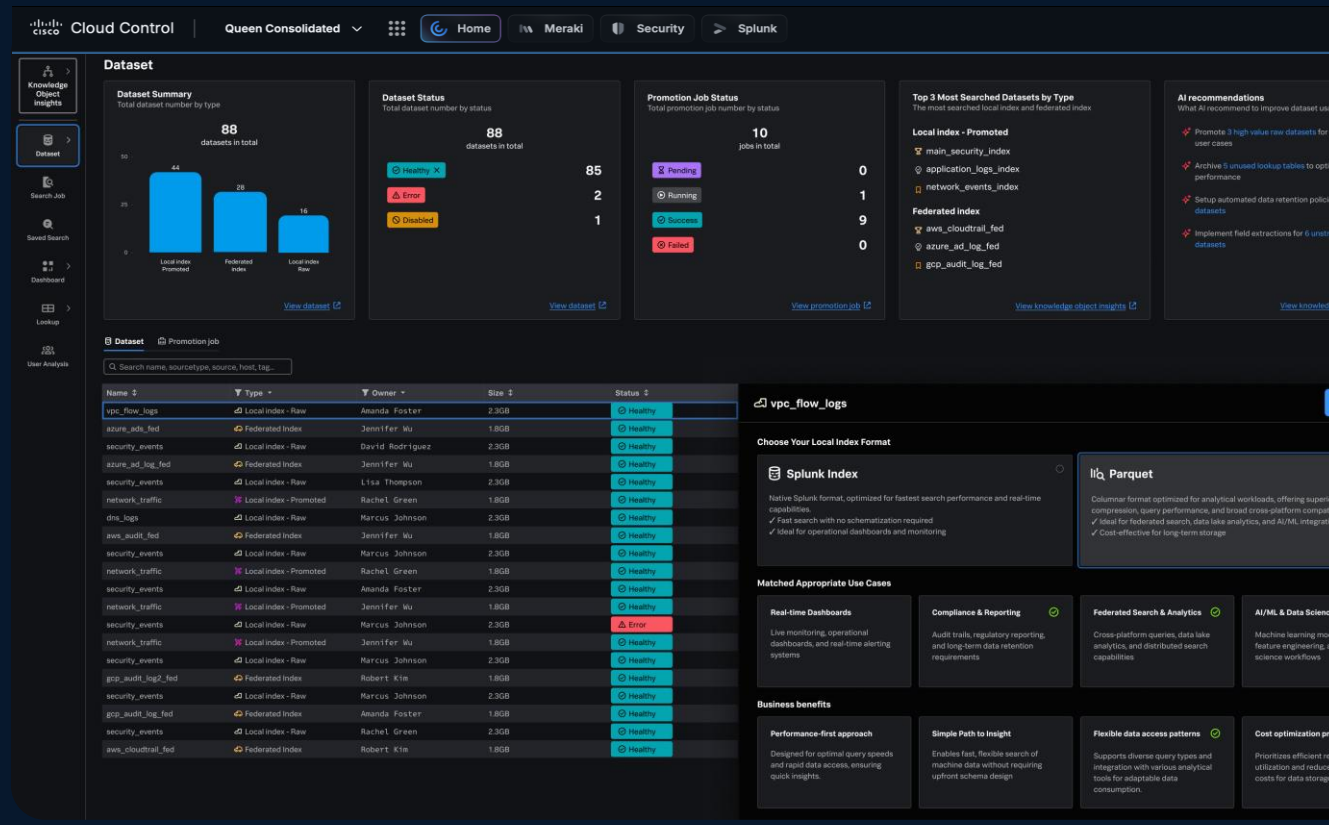
cisco

Not just another lake

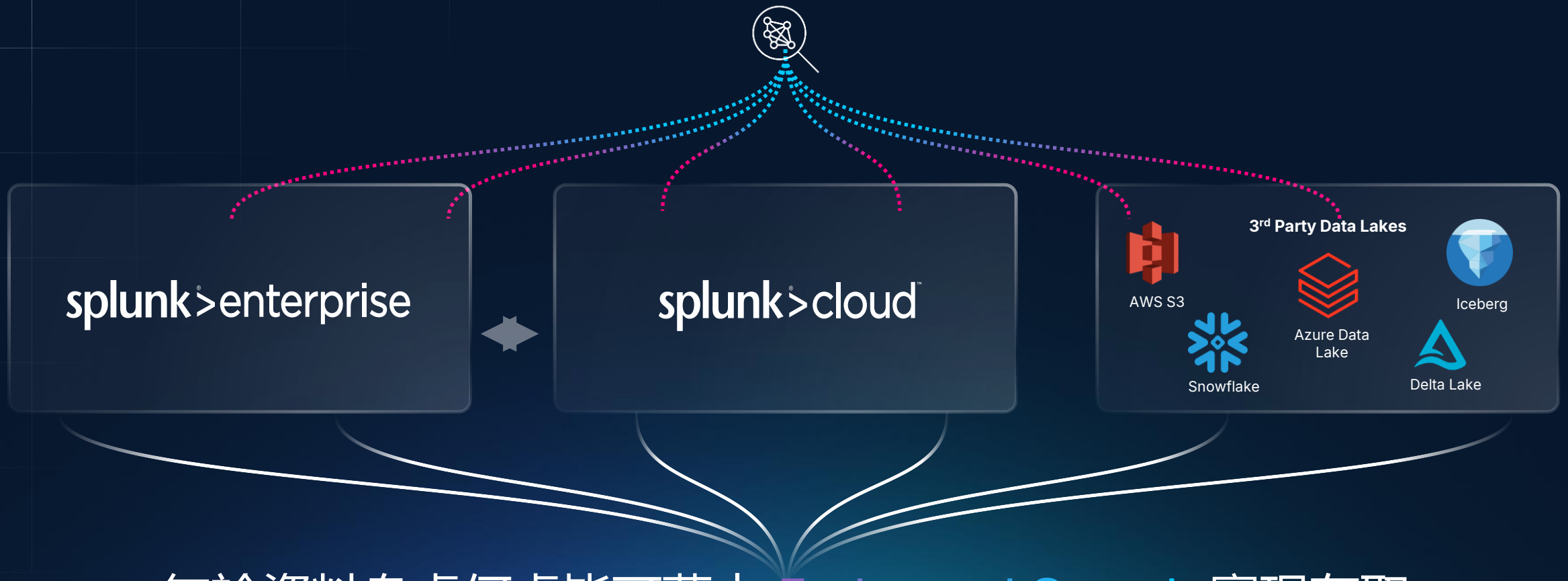
Splunk Machine Data Lake 機器數據湖

GA JULY 2026

- Deliver cost-effective turnkey access to machine data at scale
  以極具成本效益的方式，大規模提供「按需調用」的機器數據存取能力
- Accelerate search and analytics with selective data indexing
  透過「選擇性數據索引」技術，全面提升搜尋與分析效能
- Power agent-ready intelligence with trusted telemetry
  透過可信賴的遙測資料，為 Agentic AI 提供核心智慧



Access your data wherever it lives with Federated Search

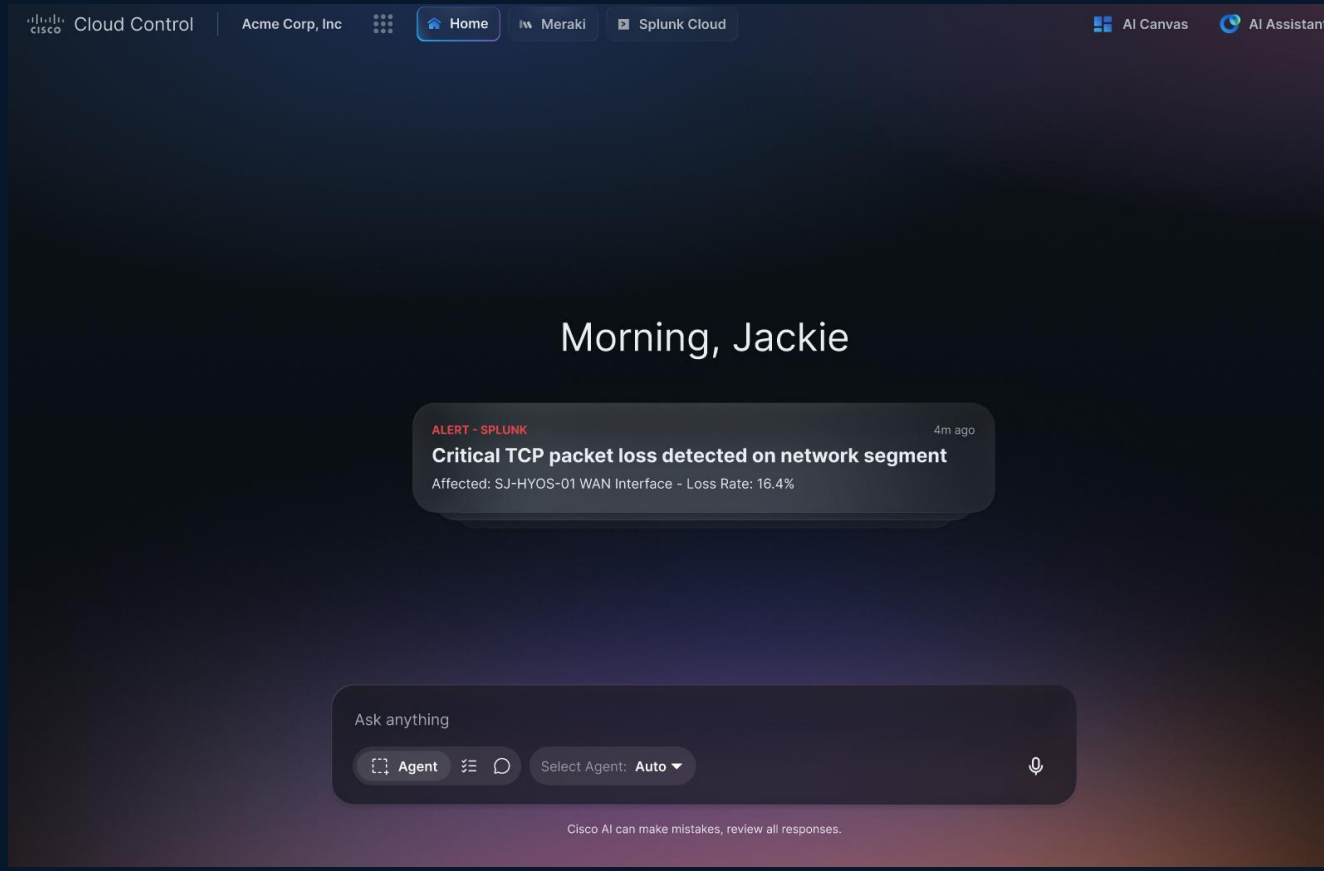


無論資料身處何處皆可藉由 Federated Search 實現存取

Bringing it all together with Cisco Cloud Control Integration
與 Cisco Cloud Control 整合 實現全面完美串聯

CA JUNE 2026

- Access all operations from single point of entry
  透過「單一進入點」全面掌控所有營運作業
- Detect issues, correlate across domains, and get recommended actions
  偵測異常，跨域關聯分析，即時獲取最佳處置建議
- Unify data, identity, and governance for operators and AI agents
  全面整合數據、身分與治理，維運團隊與 Agents



Splunk is the intelligence layer that powers agentic operations

Splunk 作為核心智慧層 驅動代理式 AI 營運

Predict and prevent at machine speed 以機器速度進行預測與防護

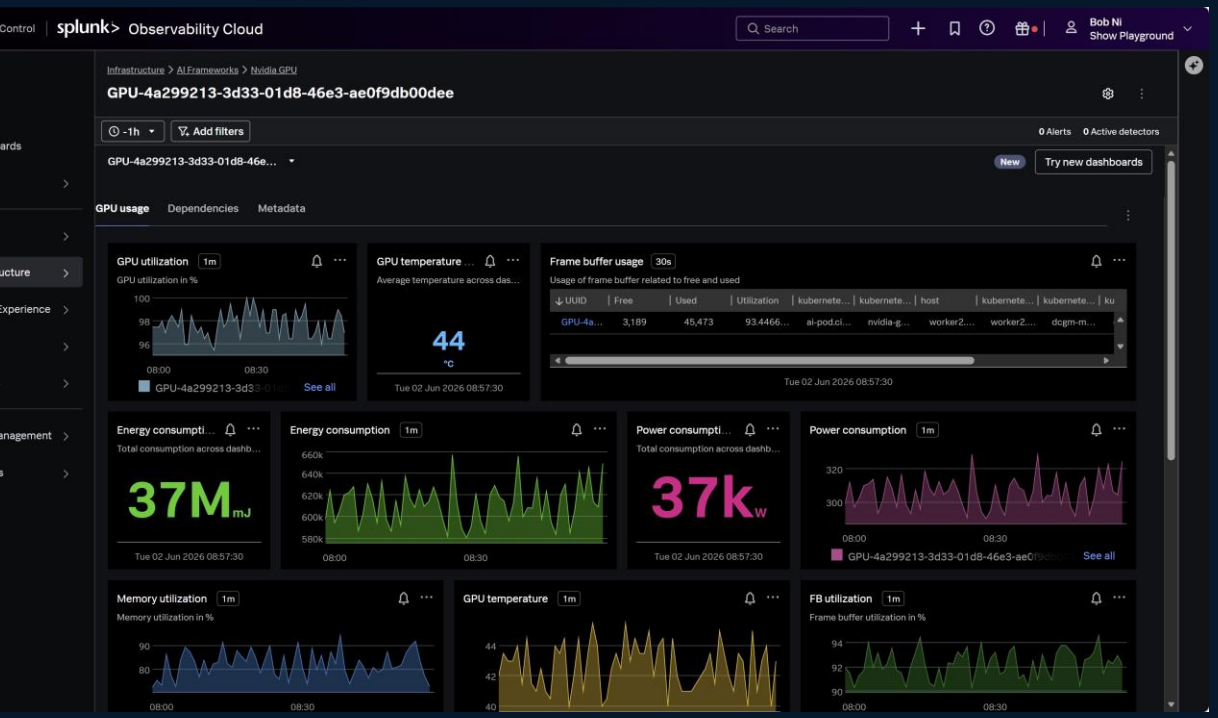
Unlock cross-domain insights at massive scale 大規模解鎖跨領域深度洞察

Build trust in AI with end-to-end visibility 透過端到端的全面可視性 化解AI信任危機

cisco

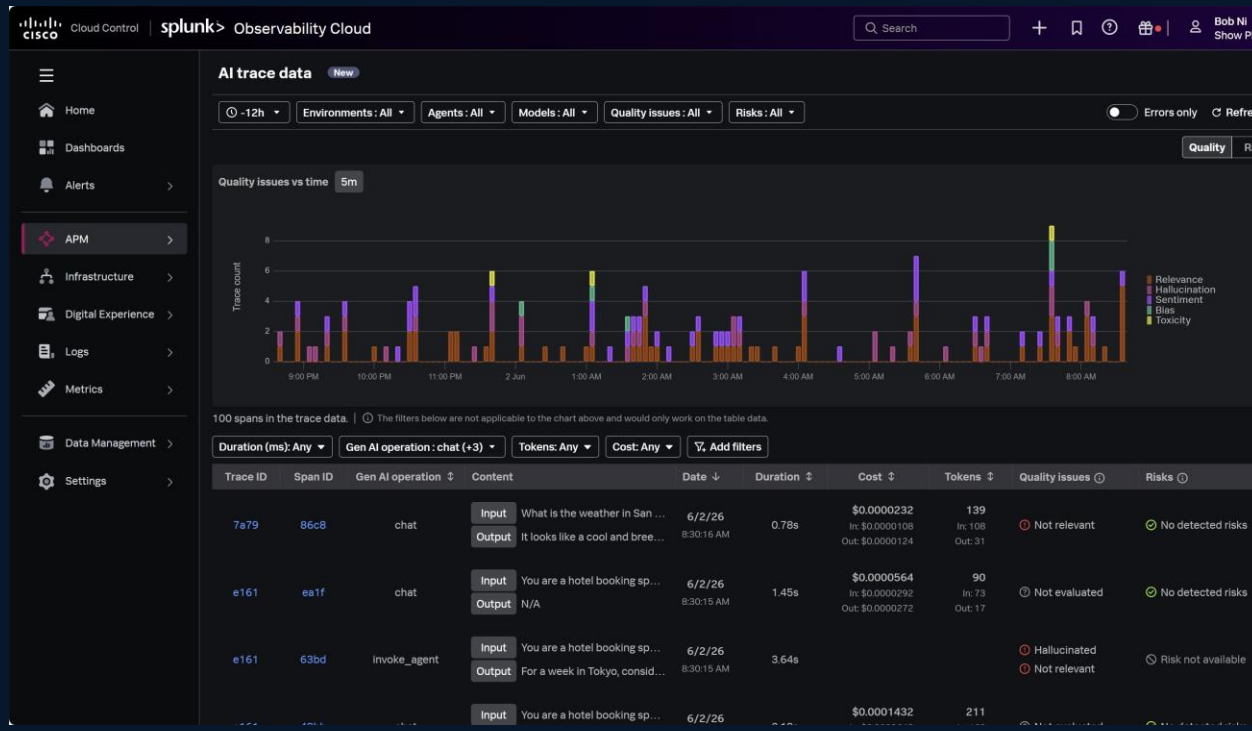
Monitor AI performance, quality, security, and cost with Splunk AI Observability

全面監控技術堆疊的效能、品質、資安與成本



AI Infrastructure
AI 基礎建設

Monitor the health, availability, and consumption (or usage) of AI infrastructure



LLM and Agentic Applications
大語言模型與代理式應用程式

Monitor the performance, quality, security, and cost of LLM and agentic applications

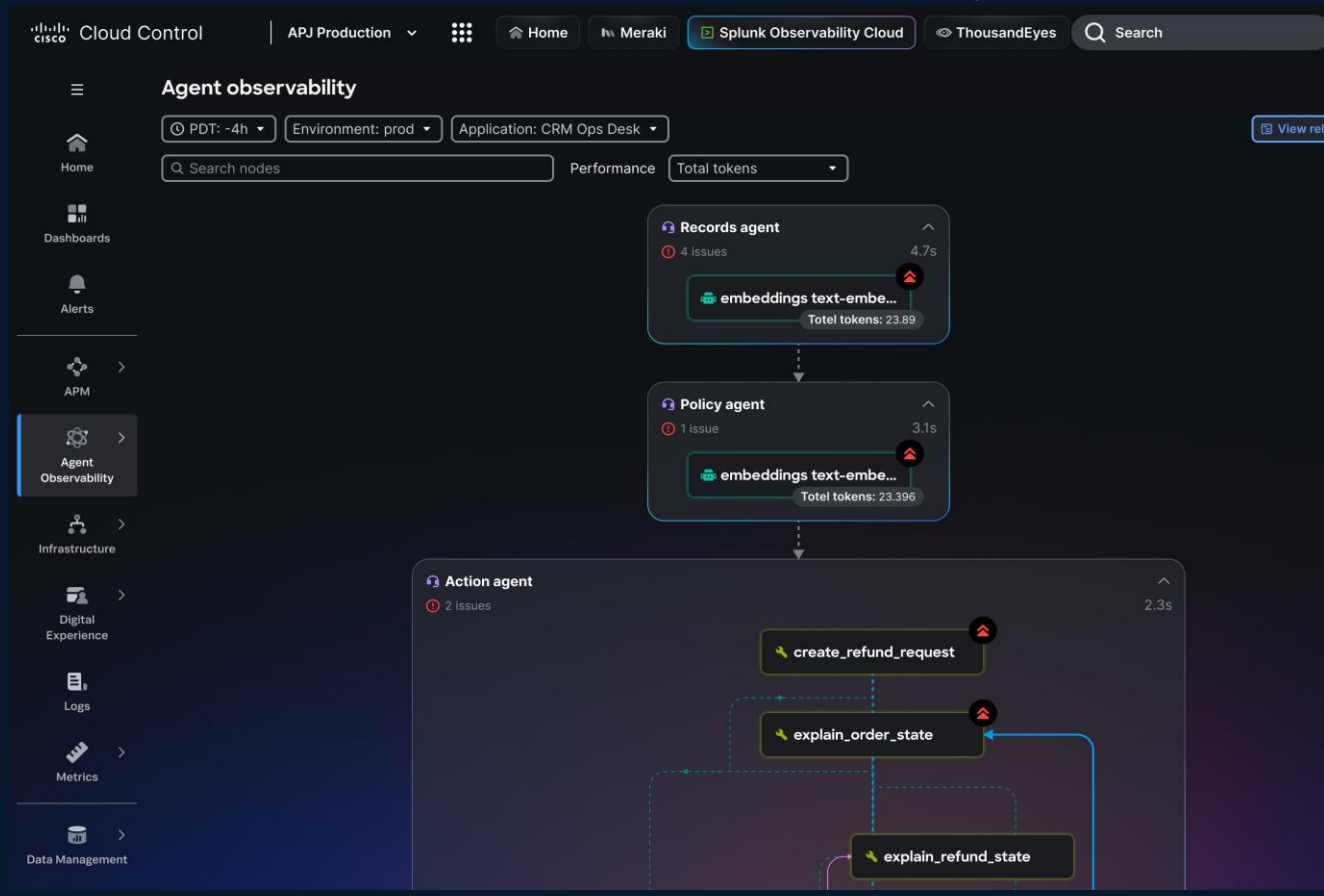
Observability for the agent lifecycle

Agents 生命週期的可觀測性

GA AUGUST 2026

- Evaluate agent, output, and RAG quality with high-accuracy evals and out-of-the-box and custom metrics
- See the root cause of errors in complex multi-agent workflows
- Leverage Luna SLMs for real-time guardrails, block hallucinations, prompt injections and safety violations

Splunk Agent Observability powered by Galileo



Digital Resilience in the Agentic AI Era
代理式 AI 時代下的數位韌性構建

Unify data and teams

One foundation and shared context across complex environment

Secure and monitor the entire stack

Security and observability teams working on one data plane

Accelerate towards self healing

Automate investigations and remediation to reduce MTTR

Build agentic operations

Deepen AI-driven innovation across the organization

cisco

CISCO Connect

THANK YOU!