CISCO Connect

Security at Agentic Scale



Greg Holly
Incubation Specialist – AI Defense

Kevin Mast
Incubation SE – AI Defense

October 13, 2026

Agentic AI has changed the game for security



Agents supercharge external attacks

- Find and weaponize faster
- Automate lateral movement



Agents are a new insider threat

- Persistent at machine speed
- No judgement or consequences

Agents are critical for fighting back

© 2026 Cisco and/or its affiliates. All rights reserved.

Every agent action is simultaneously a routing decision, a trust decision, and a telemetry event



Billions of times a day.

© 2026 Cisco and/or its affiliates. All rights reserved.

The agentic era **demands three security outcomes**

01

Protect east-west traffic & workloads

- Stop lateral movement
- Scale beyond traditional perimeters
- Shield workloads

02

Secure the agentic & human workforce

- Know every agent
- Protect every agent
- Authorize every agent action

03

Detect & respond at machine speed & scale

- Leverage machine data at scale
- Detect and respond to threats
- Monitor agent behavior and drift

© 2026 Cisco and/or its affiliates. All rights reserved.

Our platform approach

Unified operating model (Cisco Cloud Control)

Protect east-west traffic & workloads

Secure the agentic & human workforce

Detect & respond at machine speed & scale

Common data platform (Cisco Data Fabric)

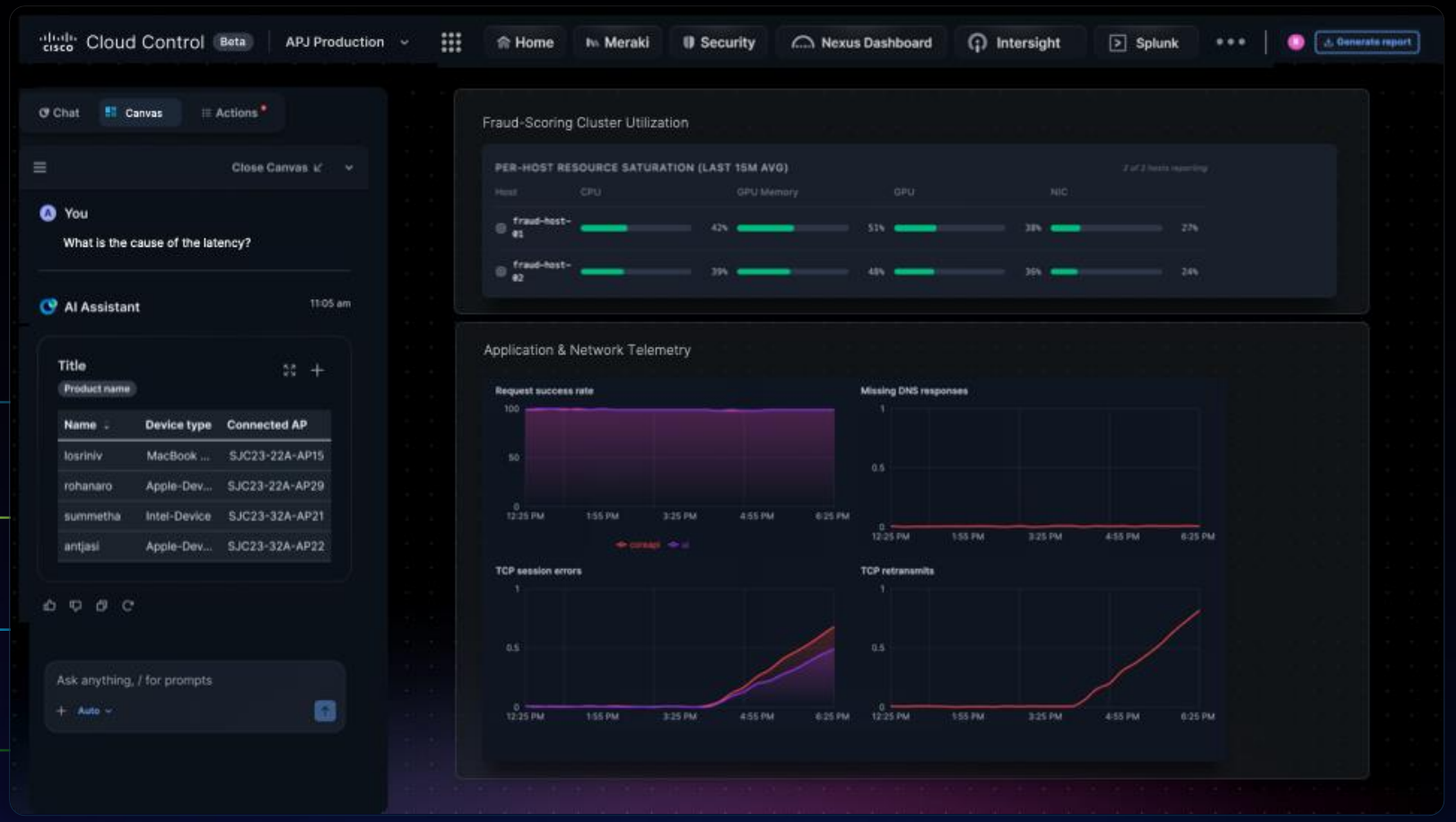
Resilient infrastructure

© 2026 Cisco and/or its affiliates. All rights reserved.

Cisco Cloud Control

One operating model

- Network
- Security
- Identity
- Observability



© 2026 Cisco and/or its affiliates. All rights reserved.

The agentic era **demands three security outcomes**

01

Protect east-west traffic & workloads

- Stop lateral movement
- Scale beyond traditional perimeters
- Shield workloads

02

Secure the agentic & human workforce

- Know every agent
- Protect every agent
- Authorize every agent action

03

Detect & respond at machine speed & scale

- Leverage machine data at scale
- Detect and respond to threats
- Monitor agent behavior and drift

© 2026 Cisco and/or its affiliates. All rights reserved.

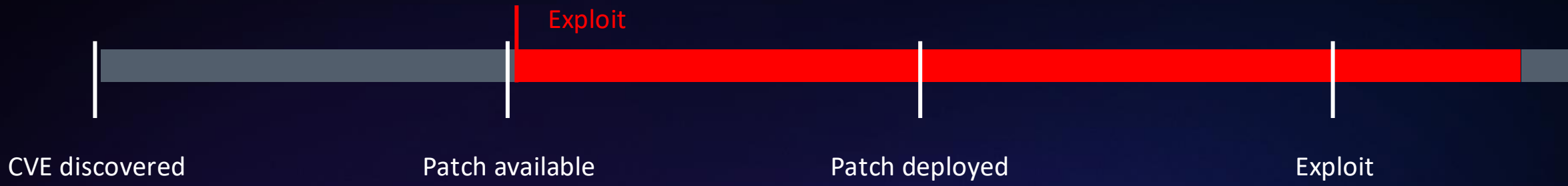
Frontier models are a **step function** change for the security landscape



© 2026 Cisco and/or its affiliates. All rights reserved.

LOG4J patch window should be





© 2026 Cisco and/or its affiliates. All rights reserved.

Live Protect



Apply policy to live system

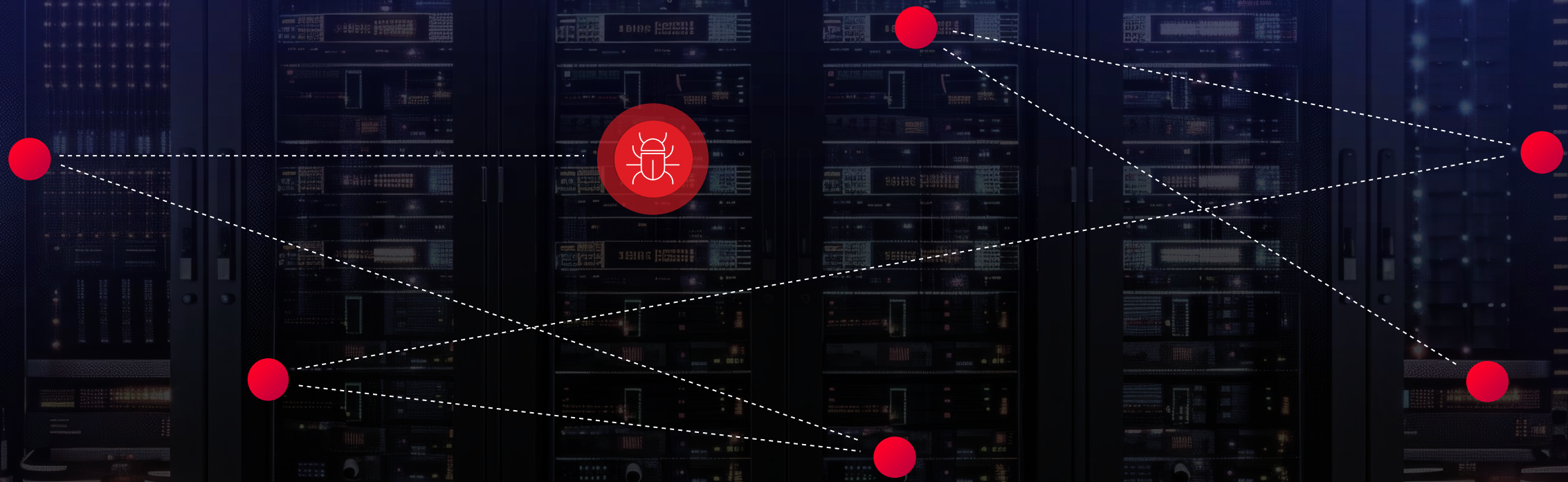
Protect now; patch in planned window

No downtime or switch reboot

Continuous re-validation

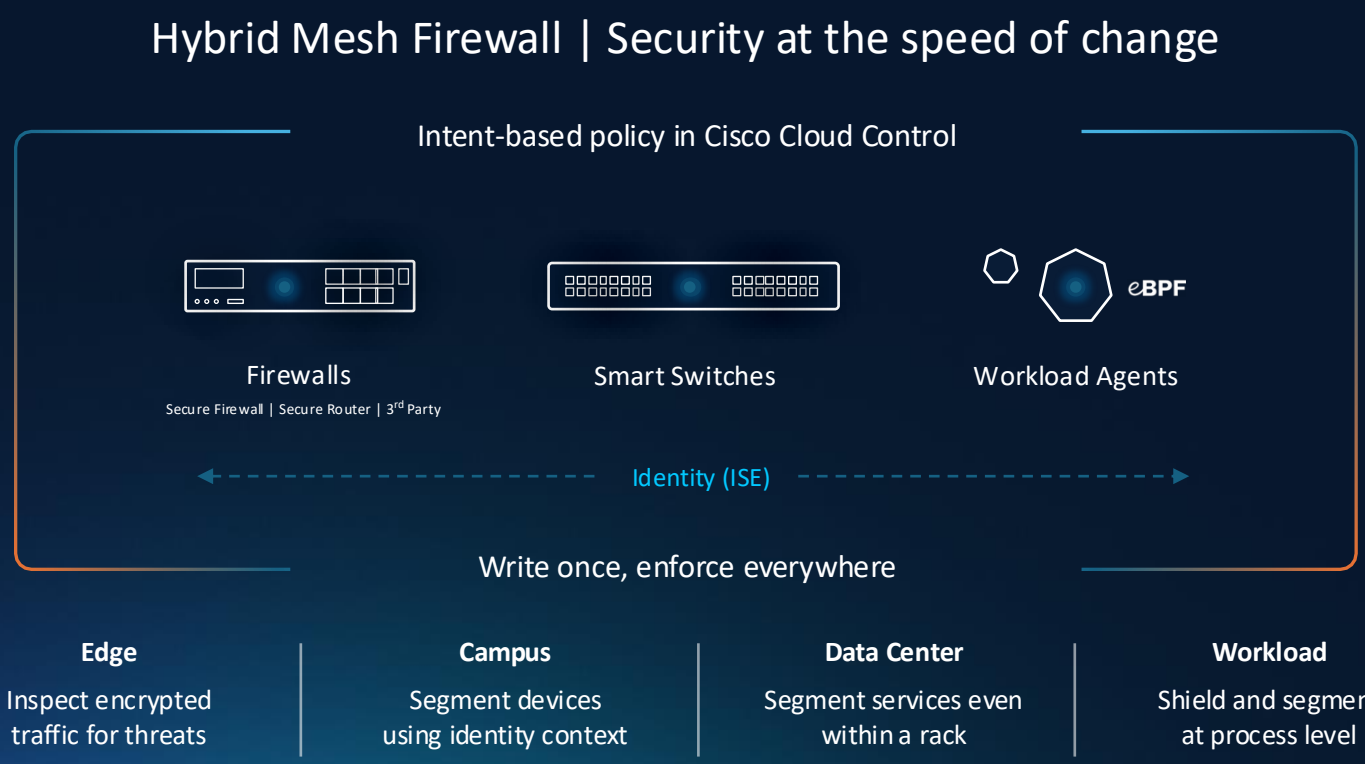
© 2026 Cisco and/or its affiliates. All rights reserved.

It’s not where attackers land, it’s where they go



Protect east/west traffic & workloads

Shield workloads and stop lateral movement at the source



© 2026 Cisco and/or its affiliates. All rights reserved.

Near-limitless scale for AI readiness



Cisco Secure Firewall
6100 Series

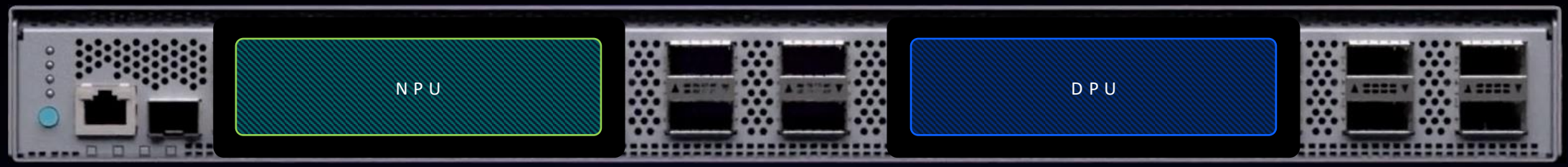
Scales linearly to 8Tbps of L7, appID, threat inspection

Changes math per protected Gbps: 80% less space, 60% less power, 1/3 the cost

No-compromise security: encrypted traffic performance, zero-day protection

Smart Switch

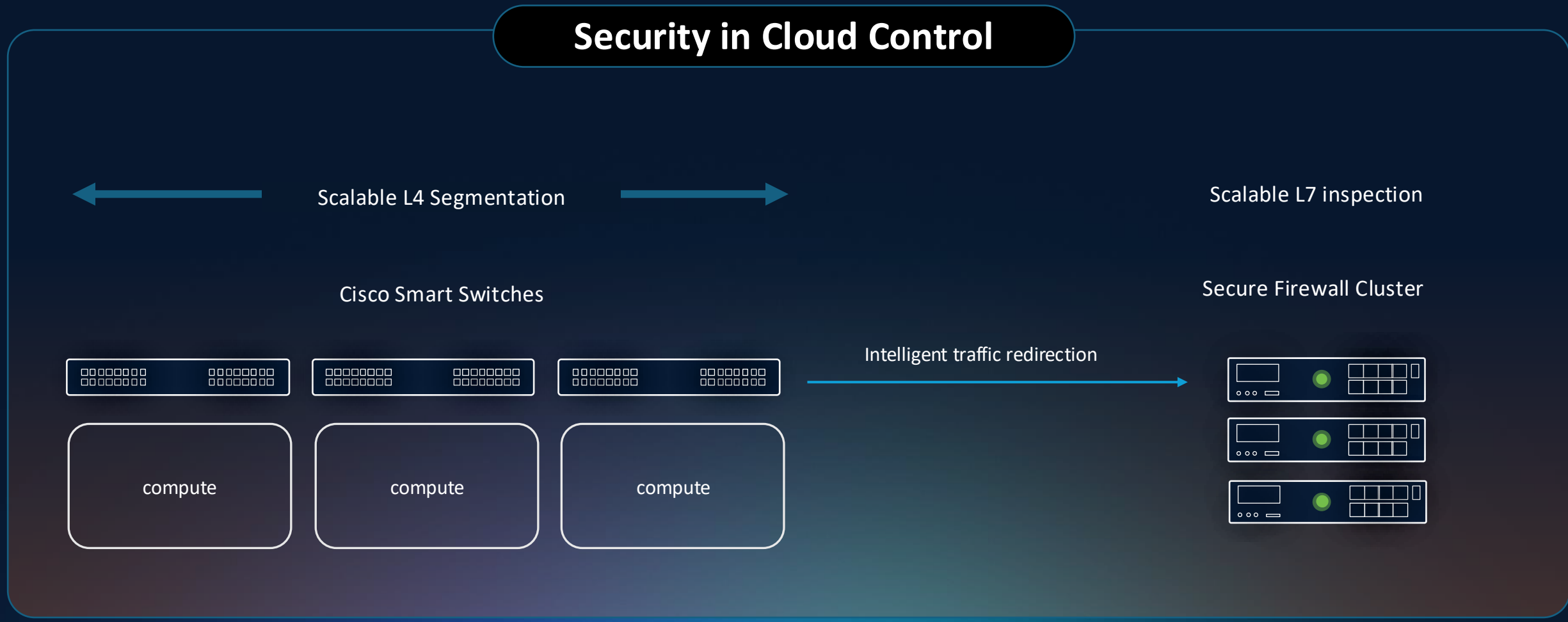
Every switch port becomes a firewall



One device,
two personalities

© 2026 Cisco and/or its affiliates. All rights reserved.

Scalable security with Smart Switch + Secure Firewall



© 2026 Cisco and/or its affiliates. All rights reserved.

Intelligent traffic redirection* is a future capability

The agentic era **demands three security outcomes**

01

Protect east-west traffic & workloads

- Stop lateral movement
- Scale beyond traditional perimeters
- Shield workloads

02

Secure the agentic & human workforce

- Know every agent
- Protect every agent
- Authorize every agent action

03

Detect & respond at machine speed & scale

- Leverage machine data at scale
- Detect and respond to threats
- Monitor agent behavior and drift

© 2026 Cisco and/or its affiliates. All rights reserved.

cisco

Two new critical requirements of security in the agentic era

Protect agents from the world

Prevent attackers from using an organization's agents to attack them from the inside, and stop them if they do

Protect the world from agents

© 2026 Cisco and/or its affiliates. All rights reserved.

cisco

AI agents “lethal trifecta”



Access to private data



Exposure to untrusted content



Ability to communicate externally

Source: simonwillison.net

© 2026 Cisco and/or its affiliates. All rights reserved.

Cisco AI Defense

A three-step framework for developing secure, trusted agents & AI applications



Discovery

Uncover AI assets including models, agents, and datasets



Detection

Test for AI risk, vulnerabilities, and susceptibility to attack with Algorithmic Red Teaming



Protection

Define guardrails that secure data and defend against runtime threats

Unified management with Cisco Security Cloud Control

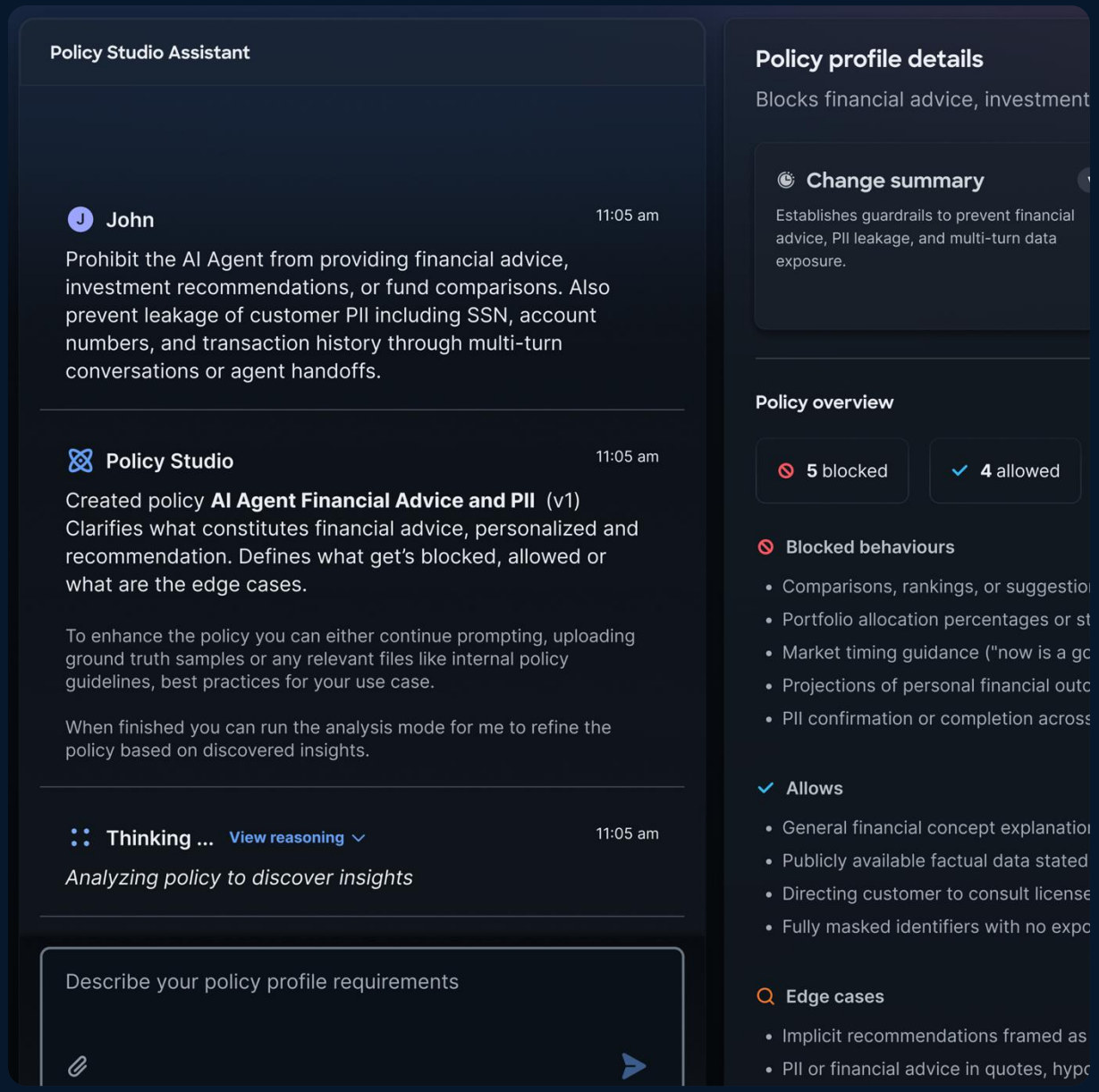
© 2026 Cisco and/or its affiliates. All rights reserved.

cisco

Protect against any risk with Policy Studio

Cisco AI Defense provides out-of-the-box guardrails for common risk categories like prompt injection, data extraction, and unsafe content.

For everything else—risks unique to your application, your organization, or your industry—you can **build adaptive guardrails in Policy Studio.**



© 2026 Cisco and/or its affiliates. All rights reserved.

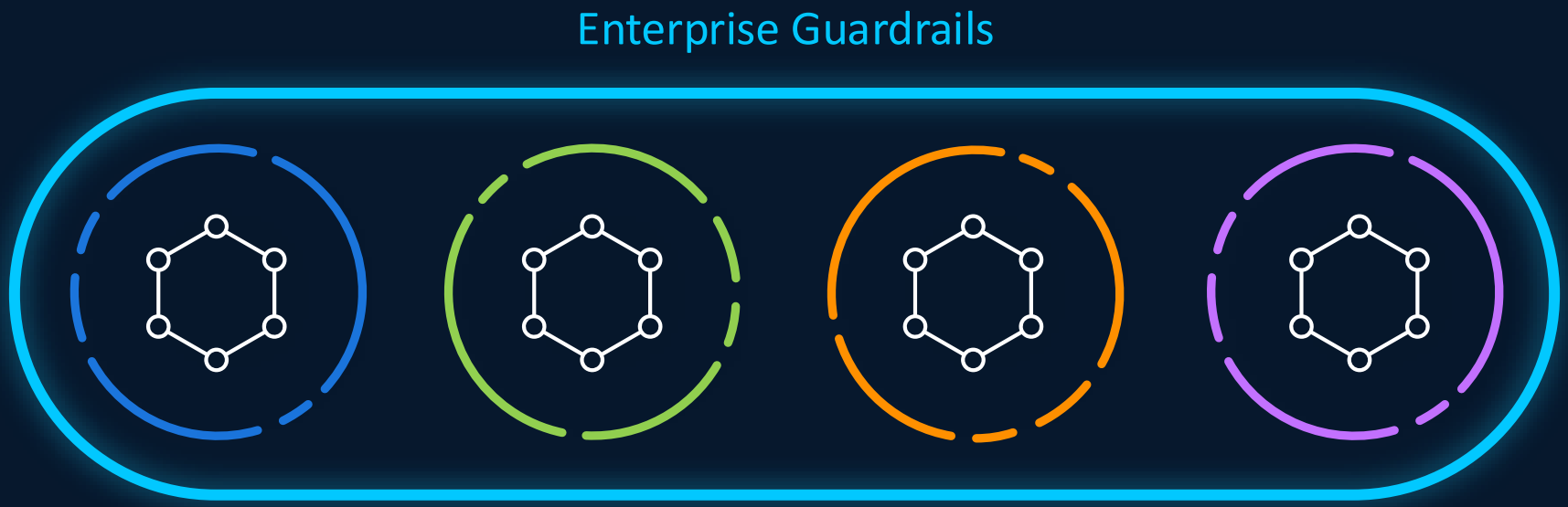
Model security is inconsistent



Built-in guardrails are different for each model, optimized for performance over security, and easily broken when changing the model.

© 2026 Cisco and/or its affiliates. All rights reserved.

Model security is inconsistent



Enterprise guardrails provide a common layer of security across models, allowing AI teams to focus fully on development.

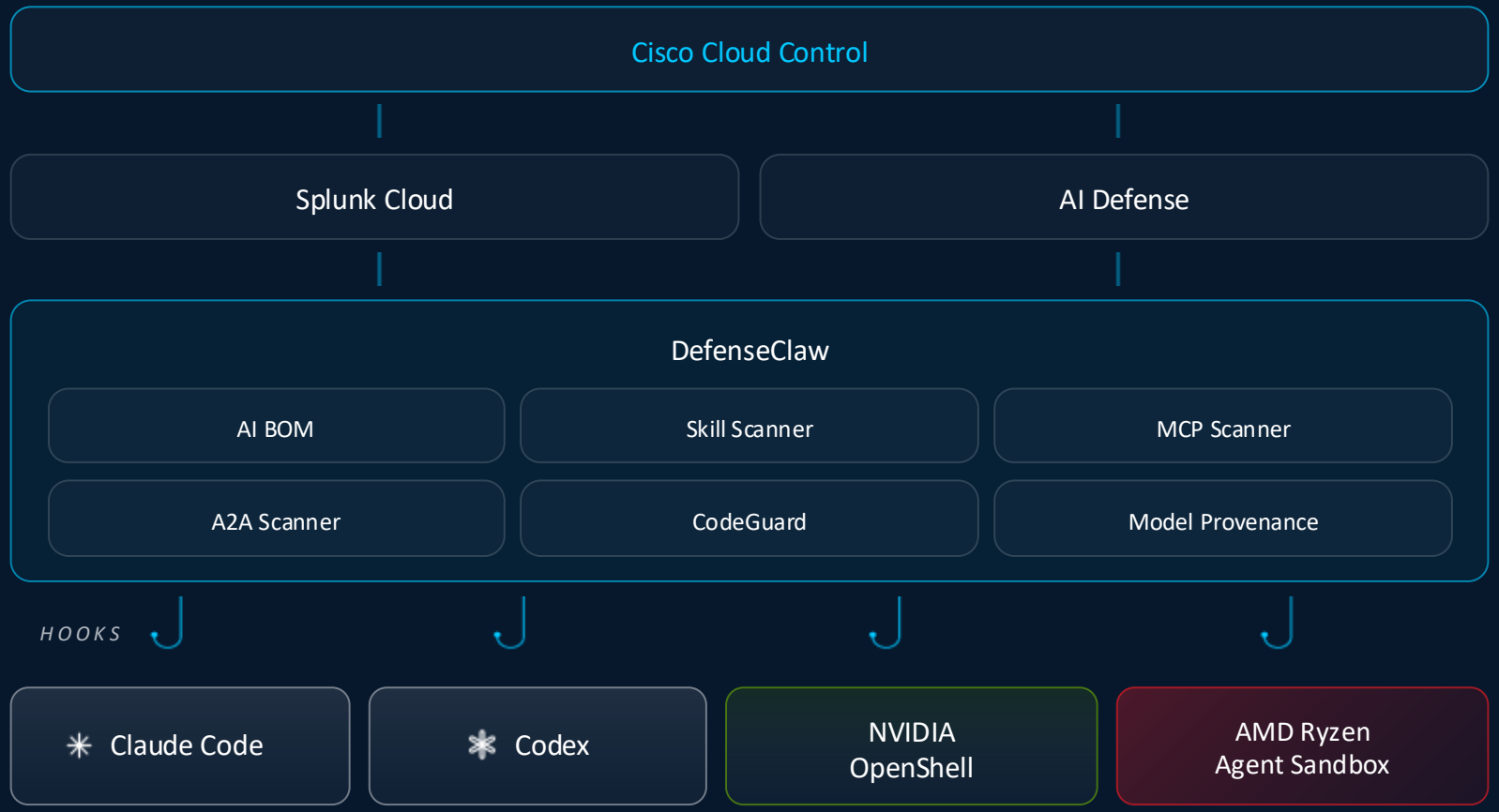
© 2026 Cisco and/or its affiliates. All rights reserved.

DefenseClaw

Works with OpenClaw, Claude Code, Codex, and more

AVAILABLE VIA OPEN SOURCE

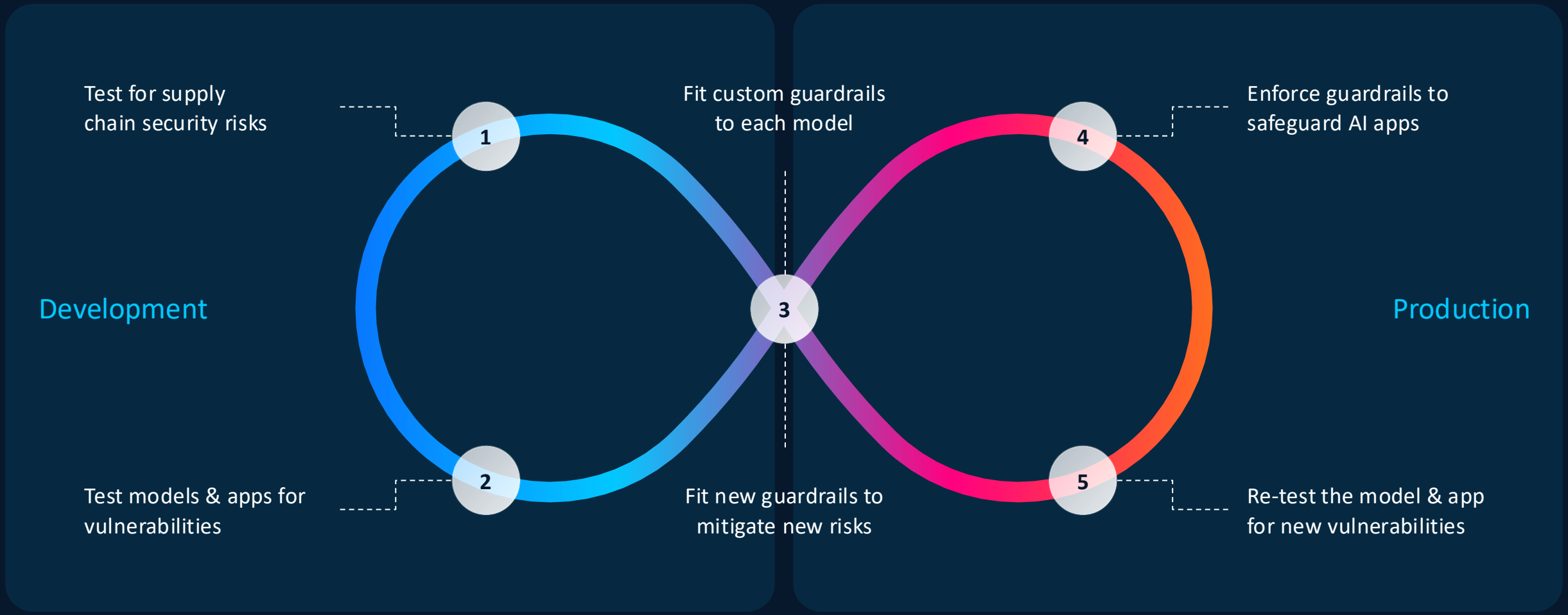
NOW PART OF CISCO SECURE CLIENT



© 2026 Cisco and/or its affiliates. All rights reserved.

Security across the AI development lifecycle

Shift left with Cisco AI Defense



© 2026 Cisco and/or its affiliates. All rights reserved.

Two new critical requirements of security in the agentic era

Protect agents from the world

Protect the world from agents

Prevent an organization's agents from doing internal or external damage by controlling access to tools and systems

© 2026 Cisco and/or its affiliates. All rights reserved.

Agents are being deployed in a variety of ways



Codex

OpenClaw

© 2026 Cisco and/or its affiliates. All rights reserved.

Agents must become part of every organization’s Zero Trust framework

© 2026 Cisco and/or its affiliates. All rights reserved.



© 2026 Cisco and/or its affiliates. All rights reserved.

Zero Trust must evolve for the agentic workforce



© 2026 Cisco and/or its affiliates. All rights reserved.

Zero Trust for agents

Know
every agent

Discover agents

Build directory

Assign human accountability

Authorize
every action

Just in time

Just enough

Just long enough

Adapt
to risk in real time

Threat context

Behavioral context

Runtime protections

© 2026 Cisco and/or its affiliates. All rights reserved.

SASE for the agentic era | Combining the power of security and networking

NETWORKING

Optimize AI traffic

Detect & steer AI flows for low-latency, reliable agentic interactions

SD-WAN

SASE

SECURITY

Secure agent interactions

Native MCP and LLM visibility, policy, and in-path threat inspection

Secure Access

© 2026 Cisco and/or its affiliates. All rights reserved.

The agentic era **demands three security outcomes**

01

Protect east-west traffic & workloads

- Stop lateral movement
- Scale beyond traditional perimeters
- Shield workloads

02

Secure the agentic & human workforce

- Know every agent
- Protect every agent
- Authorize every agent action

03

Detect & respond at machine speed & scale

- Leverage machine data at scale
- Detect and respond to threats
- Monitor agent behavior and drift

© 2026 Cisco and/or its affiliates. All rights reserved.

Example: 10,000 files just disappeared. Was that an attack?

SECURITY KNOWS

The files really were deleted

An identity with valid credentials did it

OBSERVABILITY KNOWS

What the agent was asked to do

The reasoning that led it there

Neither one, alone, can tell you whether this was hostile.

© 2026 Cisco and/or its affiliates. All rights reserved.

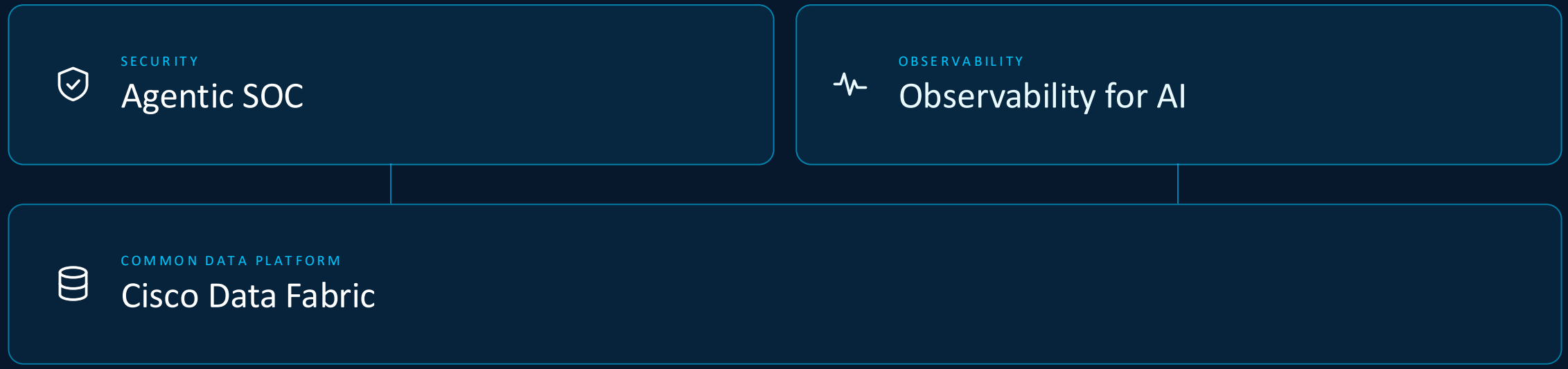
Fuse them to get the right answer





© 2026 Cisco and/or its affiliates. All rights reserved.

End-to-end strategy for detection & response at machine speed and scale



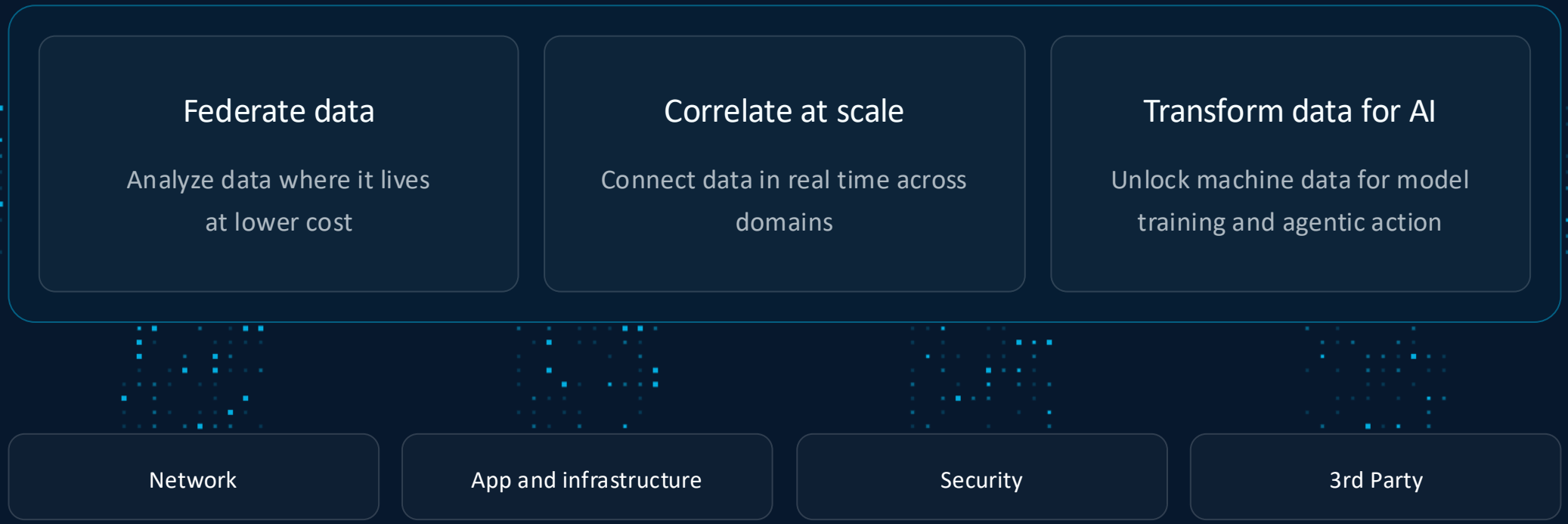
© 2026 Cisco and/or its affiliates. All rights reserved.

Data is the key for defending at machine speed and scale



© 2026 Cisco and/or its affiliates. All rights reserved.

Cisco Data Fabric powered by the Splunk Platform



© 2026 Cisco and/or its affiliates. All rights reserved.

To solve the AI trust deficit, we need
end-to-end observability
across the entire AI stack



WHICH TELLS YOU

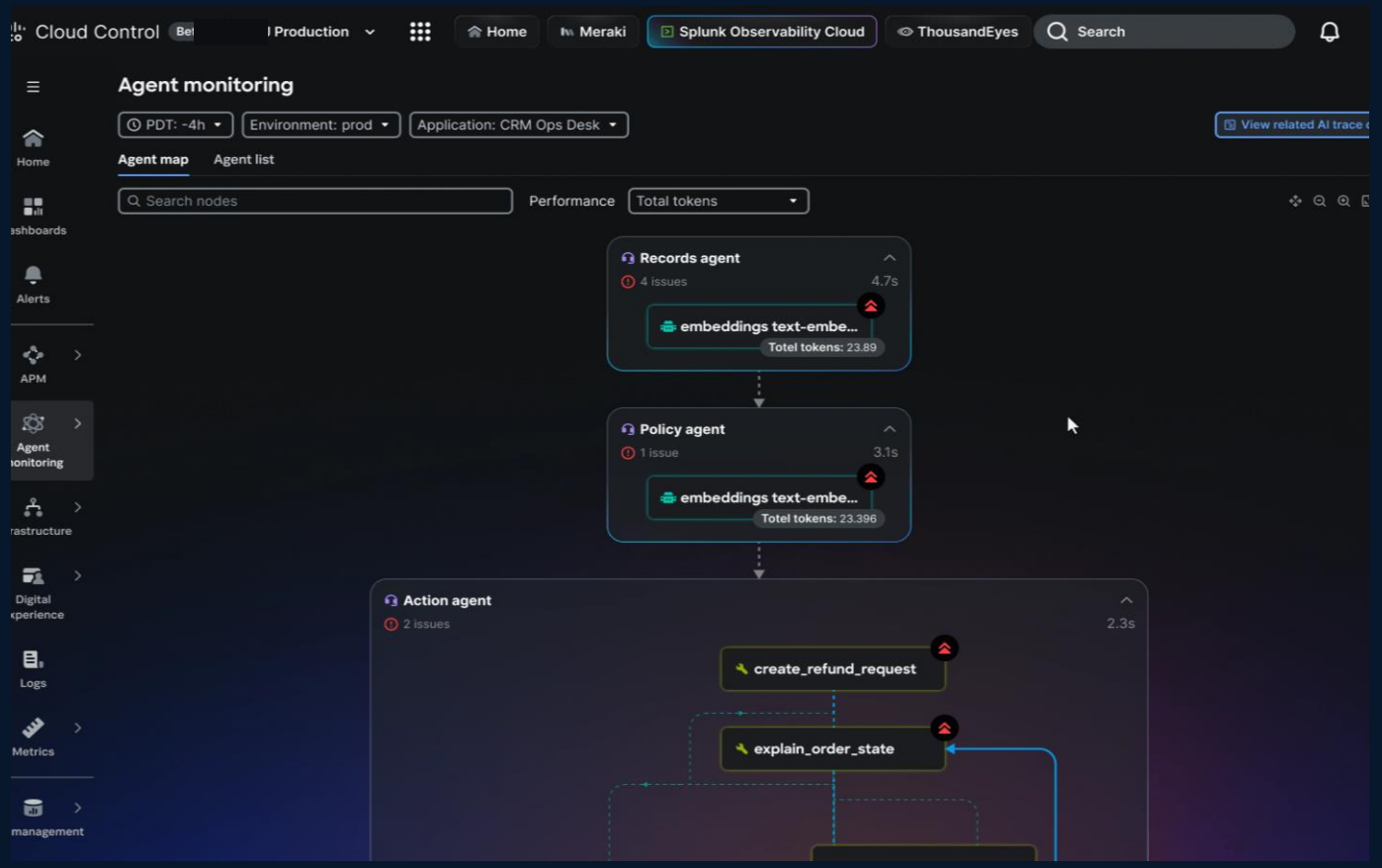
Resilience
Behavior
Tokenomics

© 2026 Cisco and/or its affiliates. All rights reserved.

GALILEO ACQUISITION

Supercharging Splunk Observability for AI

Evaluate reasoning & behavior

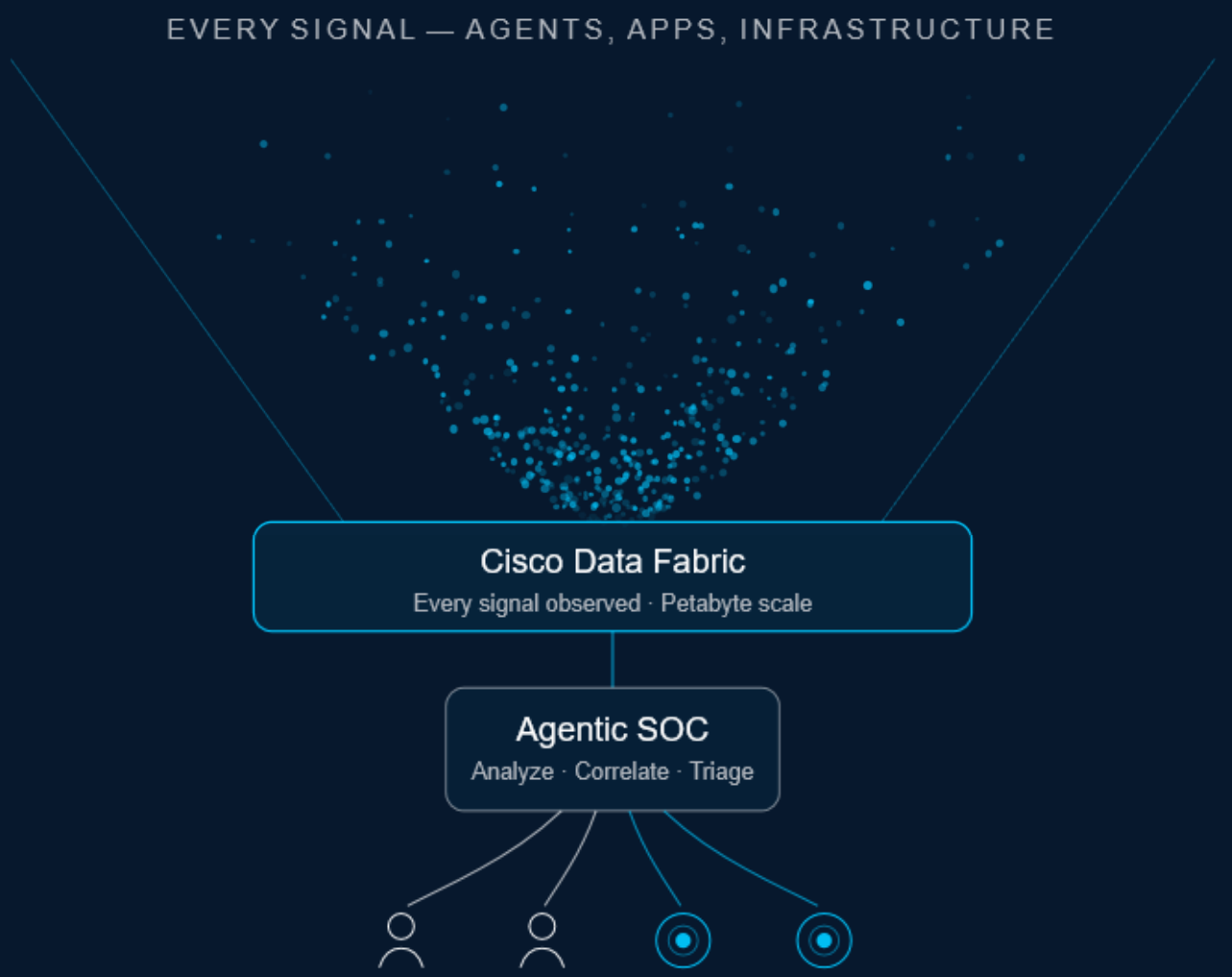


© 2026 Cisco and/or its affiliates. All rights reserved.

We need to help SecOps teams operate at machine speed and scale

© 2026 Cisco and/or its affiliates. All rights reserved.

We believe the ability to analyze every signal is within reach



Humans & agents working together

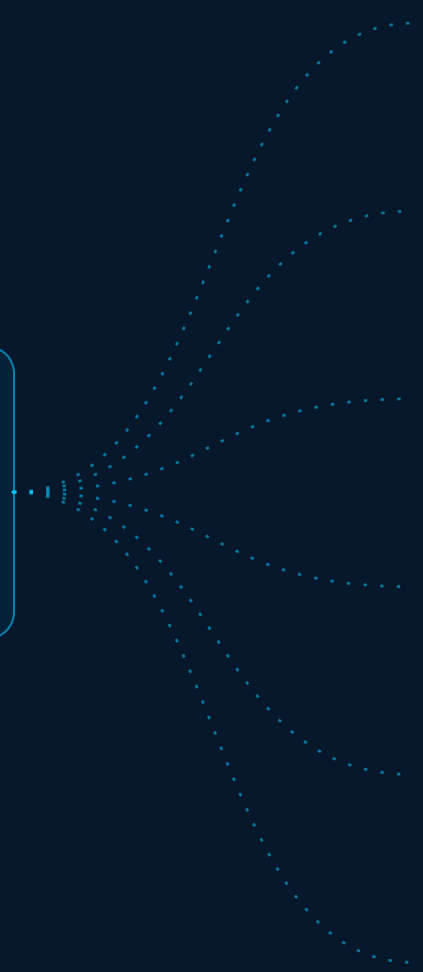
© 2026 Cisco and/or its affiliates. All rights reserved.

The Splunk Agentic SOC

AGENTIC SOC

SOC agents

Working the queue at machine speed



Triage

Evaluates and prioritizes alerts, reducing alert fatigue

Detection builder

Translates threat hypotheses into detection rules

Malware reversal

Extracts indicators of compromise (IOC), flags evasion, groups recurring behaviors

Automation builder

Builds response actions from plain-language descriptions

Standard operating procedure (SOP)

Converts SOPs into executable response plans

Guided response

Executes threat containment actions based on SOPs

© 2026 Cisco and/or its affiliates. All rights reserved.