

Powering and Securing the Agentic Enterprise



Timothy Snow

Senior Cybersecurity Advisor, Cisco APJC



AI accelerates
discovery of threats
and vulnerabilities



Quantum Computing
undermines
encryption and
trust systems



Small cracks
can lead into full
architecture
compromise

Zero-minute attacks break your Zero-Trust architecture

Risks are Evolving

Aging
infrastructure
and expanding
attack surface

AI is
compressing
attack window

Detection and
Response
is important,
but its not
enough

Risks are Evolving

Scale

1000s

of critical vulns identified
in weeks, not years

AI is
compressing
attack window

Detection and
Response
is important,
but its not
enough

Risks are Evolving

Scale

1000s

of critical vulns identified
in weeks, not years

Shrinking window

Hours

from patch release to
adversarial reverse
engineering

Detection and
Response
is important,
but its not
enough

Risks are Evolving

Scale

1000s

of critical vulns identified
in weeks, not years

Shrinking window

Hours

from patch release to
adversarial reverse
engineering

Chained exploits

3→1

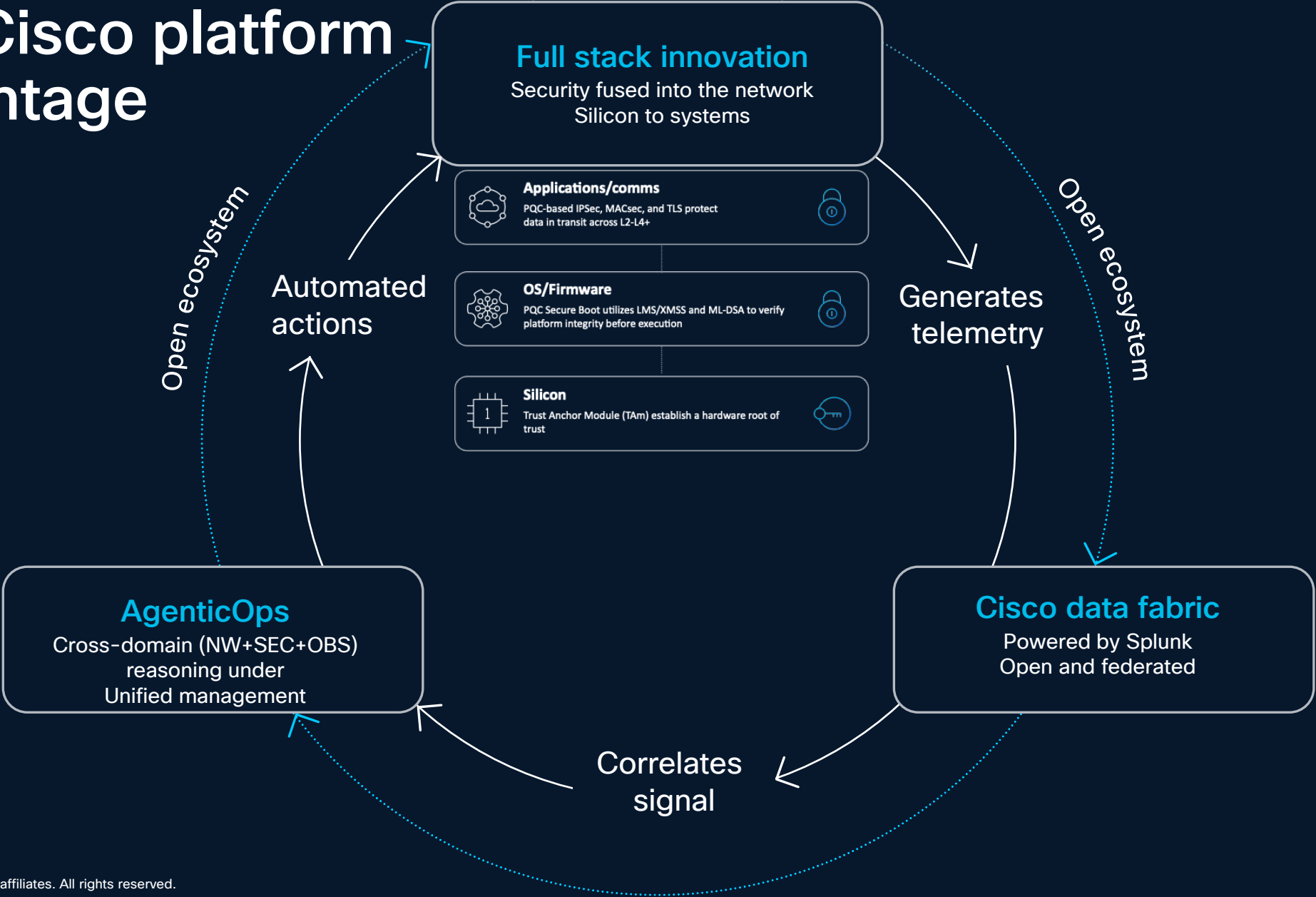
medium CVEs chained into
one critical breach path
Creating pivot paths



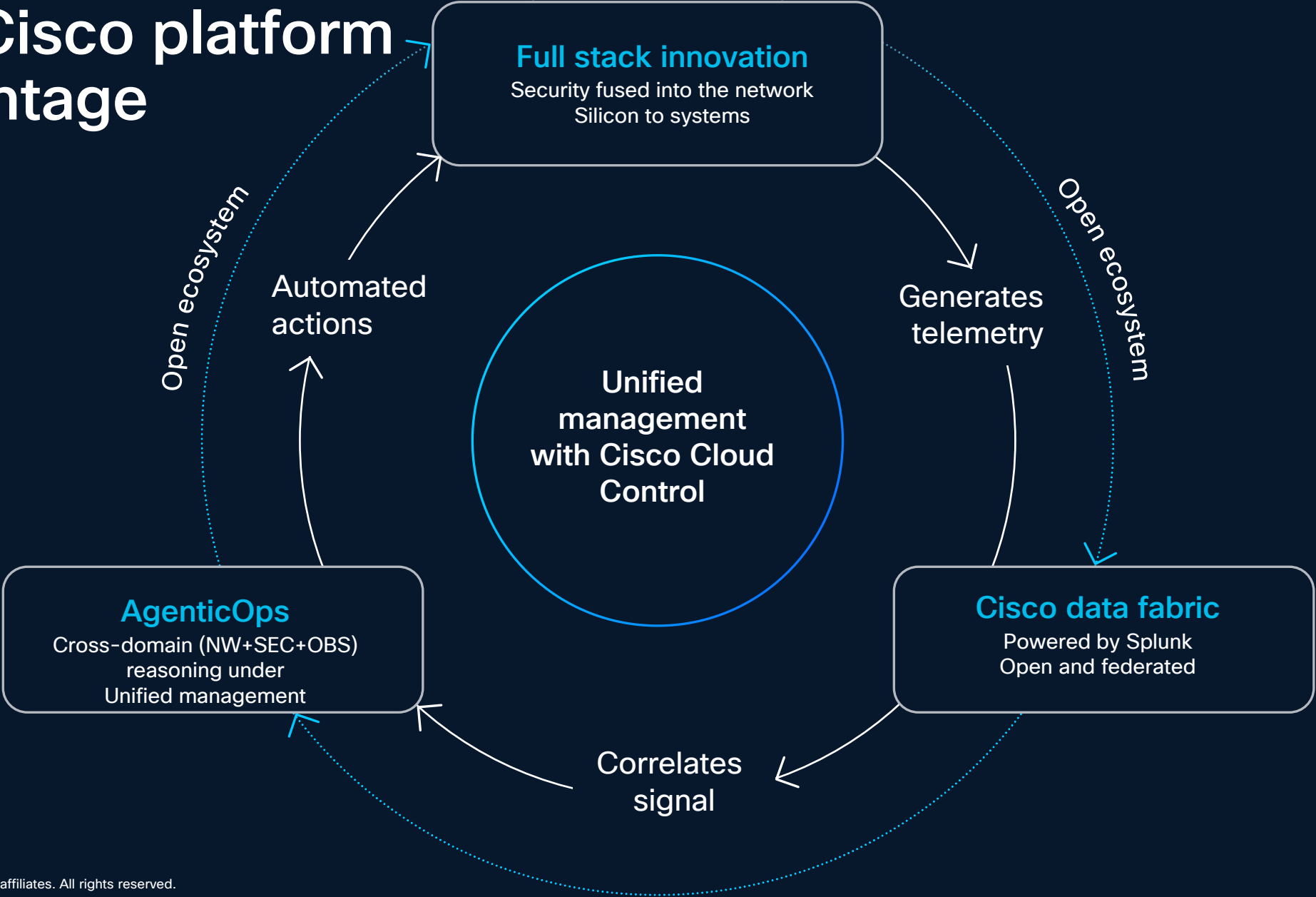
In the era of threats from ever evolving frontier
models,

Security must be fused into the network.

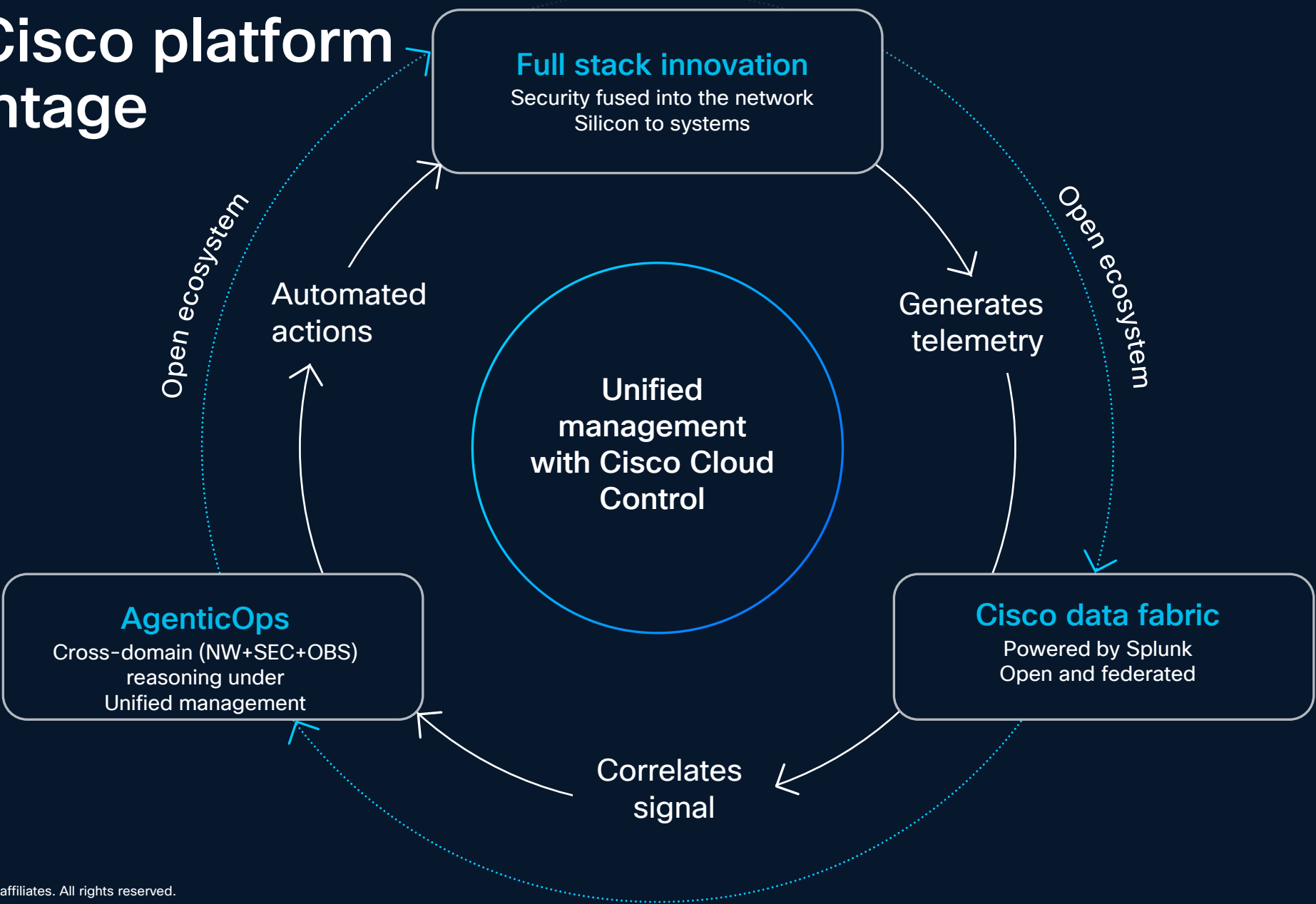
The Cisco platform advantage



The Cisco platform advantage



The Cisco platform advantage



The Cisco platform advantage



Applications/comms
PQC-based IPsec, MACsec, and TLS protect data in transit across L2-L4+

OS/Firmware
PQC Secure Boot utilizes LMS/XMSS and ML-DSA to verify platform integrity before execution

Silicon
Trust Anchor Module (TAM) establish a hardware root of trust

Cloud Control | Wayne Enterprise | Home | Intersight | Meraki | Security | +2

Assistant | Canvas | Actions

Network Health Dashboard | A B +2 | Share

AI Assistant 11:05 am

PseudoCo's network is operating at peak performance with all 15 devices online and perfect health score of 100. The organization spans 6 networks across 6 product types with 16 connected clients, supported by 3 active uplinks and no alerting devices. Licenses are in good standing through February 2031 with adequate coverage for current deployments (10 access managers, 3 VMX appliances, 2 wireless licenses). No immediate action is required.

Title

Product name

Loss rate

16.4% 2.3%

WAN interface latency 87ms (baseline <50ms)

Jitter 15ms (baseline <5ms)

Network Events

Networks Meraki

Name	Device type	Connected AP
losriniv	MacBook Pro	SJC23-22A-AP15
rohanaro	Apple-iPhone	SJC23-22A-AP29
summetha	Intel-Device	SJC23-32A-AP21
antjasi	Apple-Device	SJC23-32A-AP22

Firewall connection

Networks Thousandeyes

QoS policy successfully applied to network.

Revert change

Application / Service	Priority	Bandw
Financial services (ports 443, 8443)	Highest	20%
Voice and video	High	15%

License Overview

Endpoints Meraki

20

60

Network Health

Endpoints Meraki

Packet Loss

Transaction failure ratio

Time (Hours)

Devices by Type

Infrastructure Meraki

00:00

01:00

02:00

03:00

04:00

05:00

06:00

+ Ask anything, / for prompts, # for knowledge

Default



Protect our infrastructure



Protect the world from the agents



Detect and respond at machine speed



Protect our infrastructure



Protect the world from the agents



Detect and respond at machine speed

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



It lowers the threshold for attackers, empowering less-skilled actors to launch complex, high-impact campaigns.

Anthony Grieco

SVP and Chief Security & Trust Officer
Cisco

- **More sophisticated attackers or rather unskilled now upskilled!**
- **More personalized attacks**
- **More outliers to attack**

Fusing security into the network

NEW

Vulnerability shielding

Live Protect* shields infrastructure vulnerabilities with compensating controls to stop exploits before you patch

Exploit containment

Hybrid Mesh Firewall brings together identity services, firewalls, smart switches, and Hypershield agents to stop lateral movement

* Available now in N9000 Switches; support for other devices & services coming soon

Live Protect

Attacks

- Control plane
- Routing plane
- API
- CLI
- File I/O



Vulnerability
shielding



EXTENDING ACROSS CISCO NETWORKING AND SECURITY

Apply policy to
live system

No PSIRT patching
or upgrade

No downtime or
switch reboot

Continuous
re-validation



Protect our infrastructure



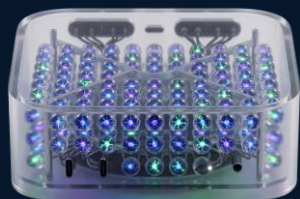
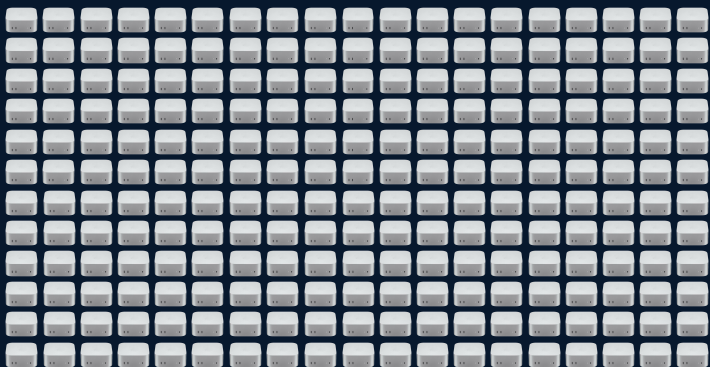
Protect the world from the agents



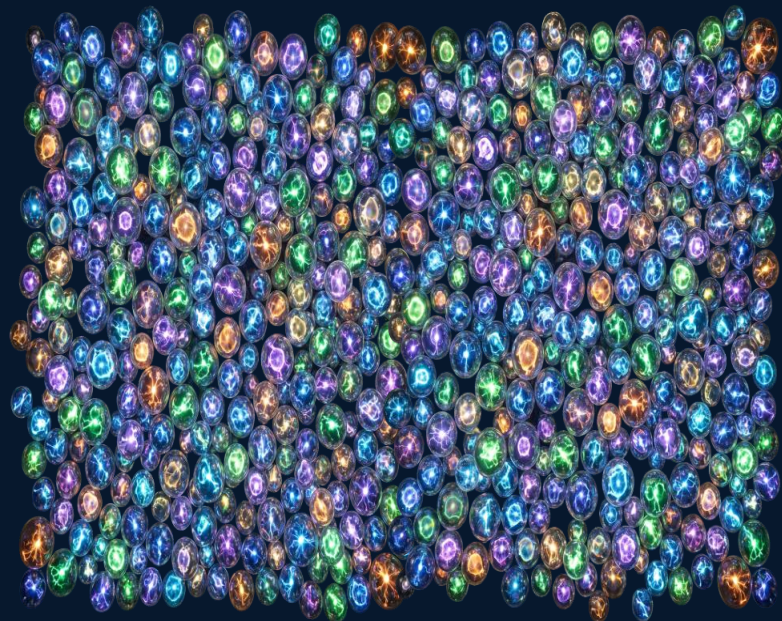
Detect and respond at machine speed

The background is a deep blue gradient. A horizontal band of light blue and white particles, resembling a digital signal or a wave, flows across the middle of the frame. The particles are small, glowing dots and plus signs, creating a sense of motion and data. The text is centered over this band.

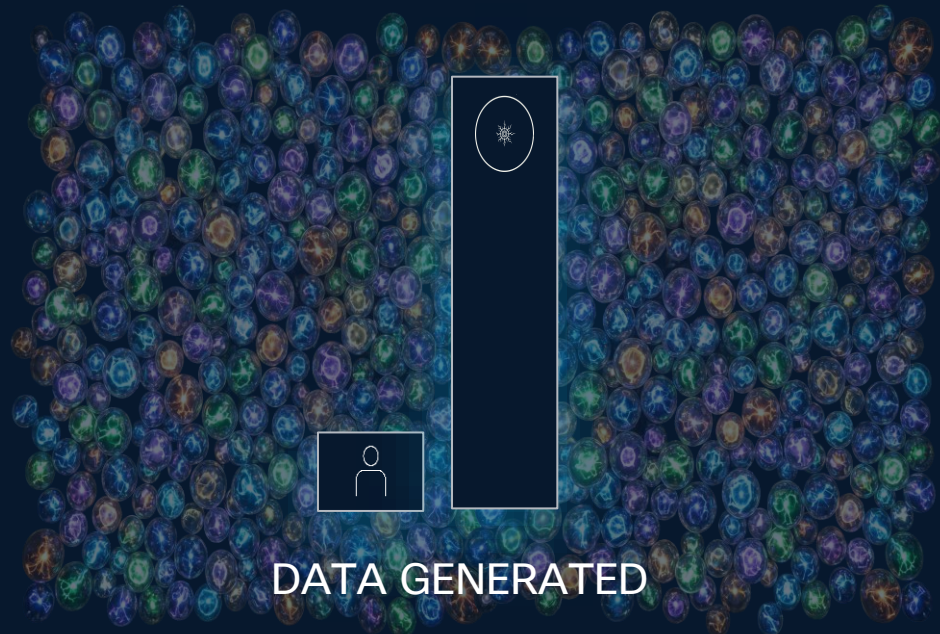
The Pivotal Shift with Agentic Workforce



The demand extends
beyond the cloud



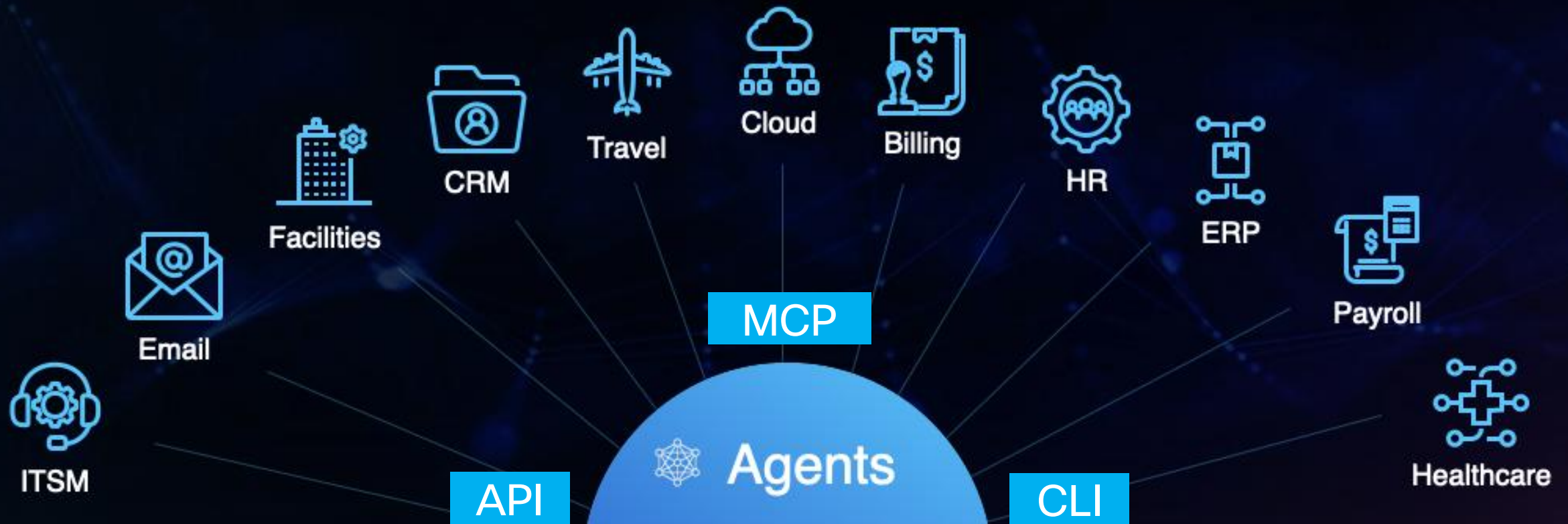
Trillions
of agents



DATA GENERATED

Every agent is generating
450% more traffic than a
human

AI Agents Need Access to Your Systems



Zero Trust must evolve for the agentic workforce



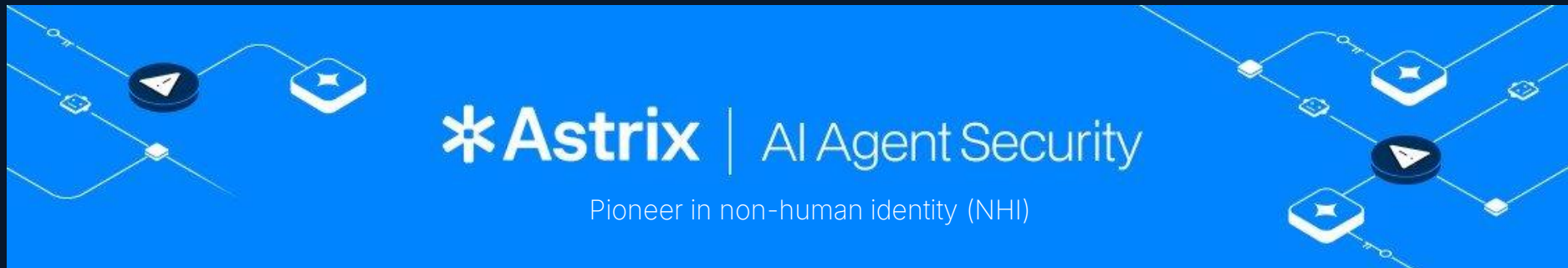
Humans

Prove identity,
Trust the user,
Access Control



Agents

Discover the Agent,
Verify behavior,
Watch the agent



Visibility, identity, and ownership for every AI agent interacting with your environment



Agentic IAM
by Duo

Agent & Tool Discovery

Agent Directory

Agent Access Policy

Human Accountability

Lifecycle Management

KNOW EVERY AGENT

AUTHORIZE EVERY ACTION

ADAPT TO RISK IN REAL TIME

Authenticate, Authorize and Enforce Policy- where agents access enterprise data & tools.



Agentic Workforce



Tools, resources and data

Use intent, threat, and behavioral context to adjust protection decisions.

Runtime protections against
safety and security threats

Threat context

Protecting against and
Detecting abnormal
behavior

Behavioral context

Real-time monitoring
and control

Communication



A three-step framework for developing secure AI applications



Discovery

Uncover AI assets including models, agents, and datasets



Detection

Test for AI risk, vulnerabilities, and susceptibility to attack

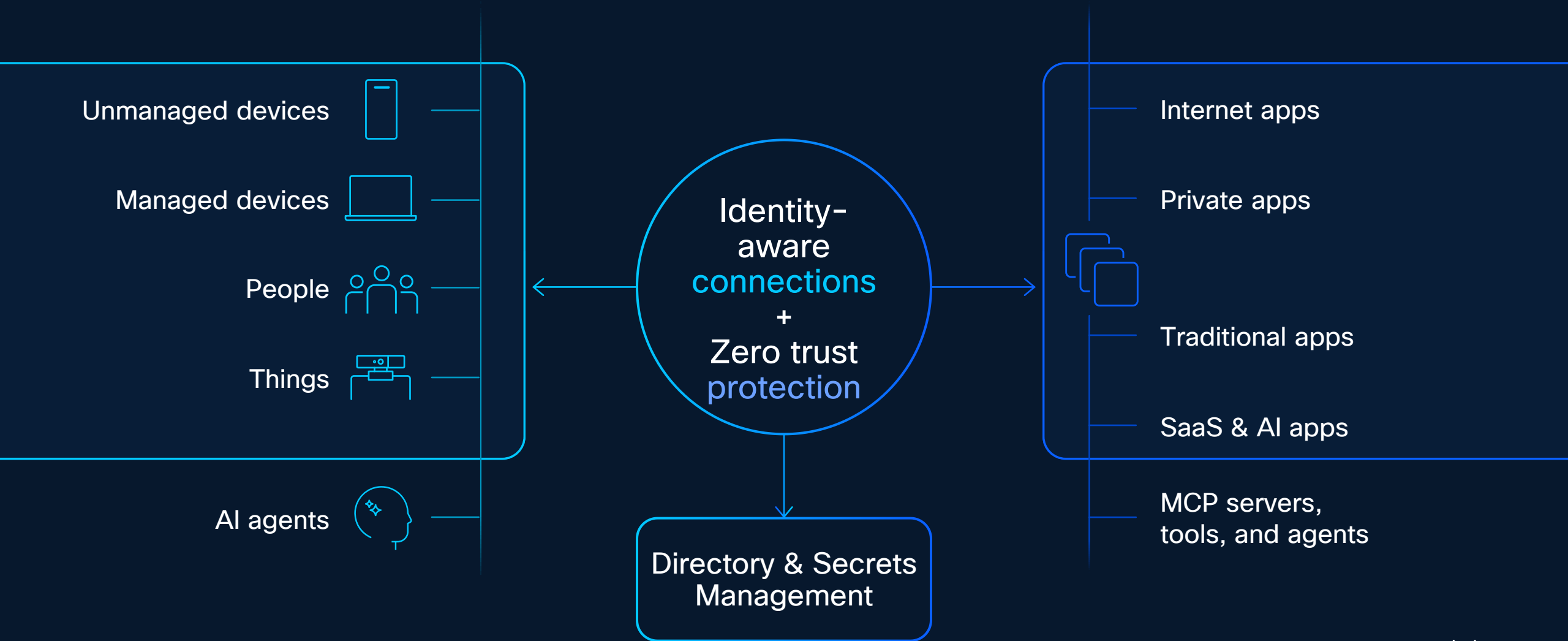


Protection

Define guardrails that secure data and defend against runtime threats

Unified management with Cisco Security Cloud Control

Extending Cisco's Zero Trust Access to secure Agentic AI





Protect our infrastructure



Protect the world from the agents



Detect and respond at machine speed

Cisco Data Fabric powered by the Splunk Platform

Data

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

Context

Catalog your enterprise
Correlate relationships
Surface insights

Action

Deploy agentic operations
Connect your agents
Build proprietary AI

Telemetry

Network

Telemetry

App and Infra

Telemetry

Security

Telemetry

3rd Party

Investigation Canvas

ASK

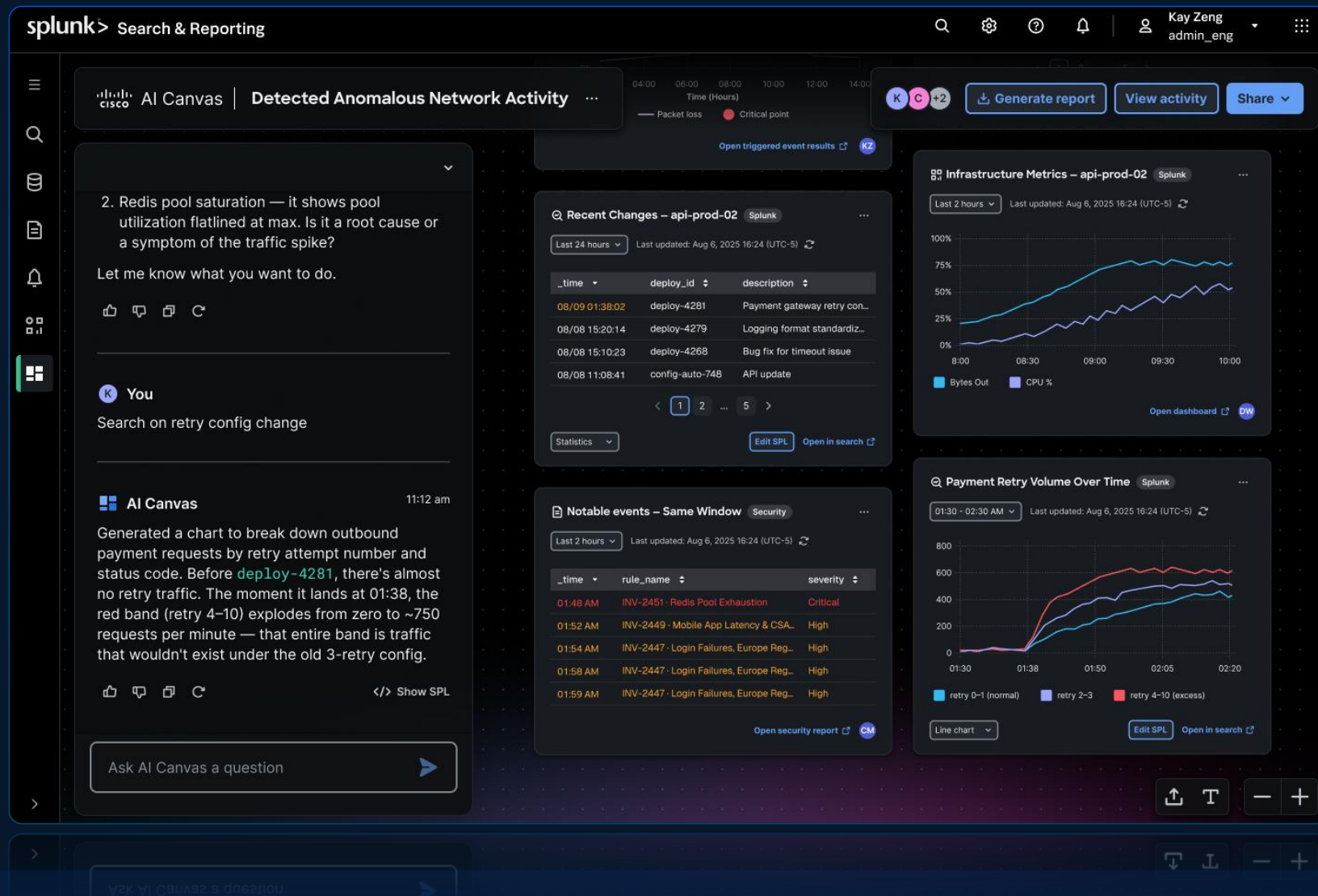
Type what you want to know

SEE

Investigation Canvas builds the visualization for you

ACT

Launch SOAR-powered actions right inside the workspace



Enable analysts to move from question → insight → response in a single generative workspace.

GALILEO ACQUISITION

Supercharging Splunk Agent Observability

- Evaluate behavior
- Observe performance
- Enforce guardrails



Cisco's approach to AI-era cyber defense

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

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

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

Supporting our customers in proactively hardening their network infrastructure

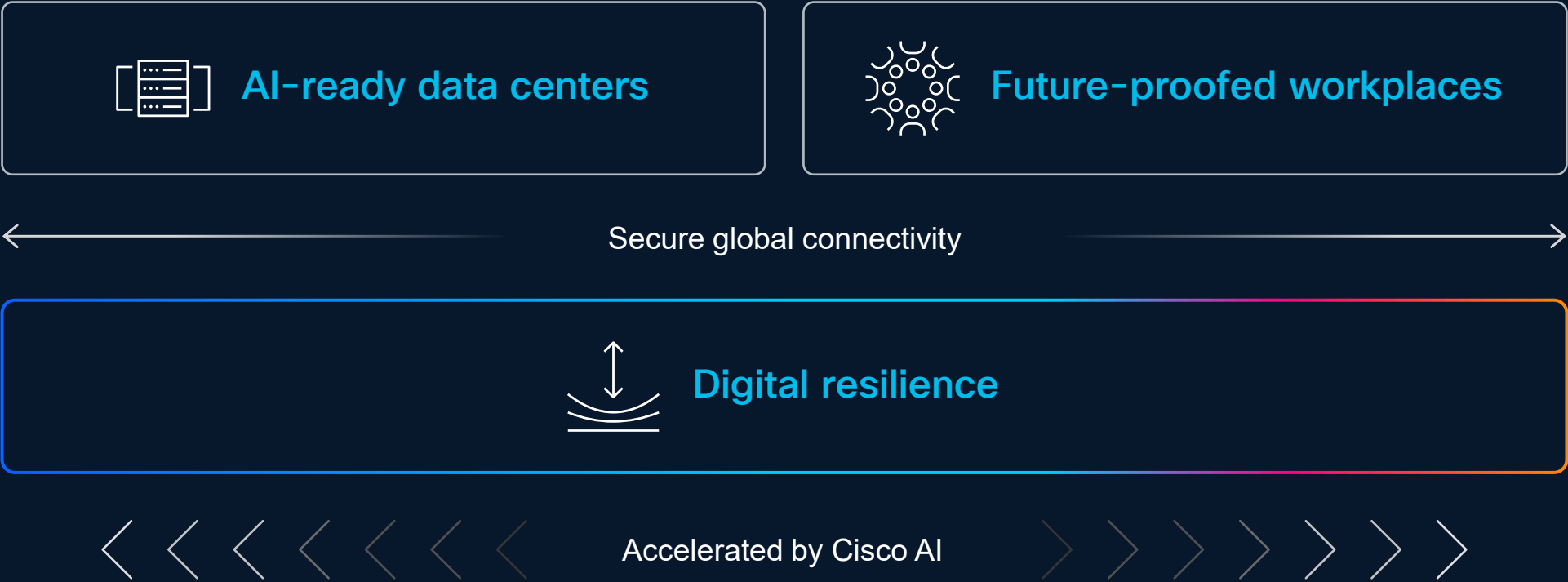
Delivering customer innovation

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.

Cisco powers how people and technology work together across the physical and digital worlds



CISCO Connect

Thank you

