CISCO Connect

Secure Networking for AI-Ready Data Centers



Vinay Thamatam
AI solutions Engineer

October 13, 2026

Cisco forward-looking statements

This presentation contains or may contain projections and other forward-looking statements regarding future events or the future financial performance of Cisco, including future operating results. These projections and statements are only predictions. Actual events or results may differ materially from those in the projections or other forward-looking statements. Please see Cisco's filings with the SEC, including its most recent filing on Form 10-K, for a discussion of important risk factors that could cause actual events or results to differ materially from those in the projections or other forward-looking statements.

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

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



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

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.

The network is the connective tissue

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

Secure networking: security fused into the network



Resilient infrastructure



Identity



Segmentation & steering



Protection



Visibility & insights

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

Resilient infrastructure

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

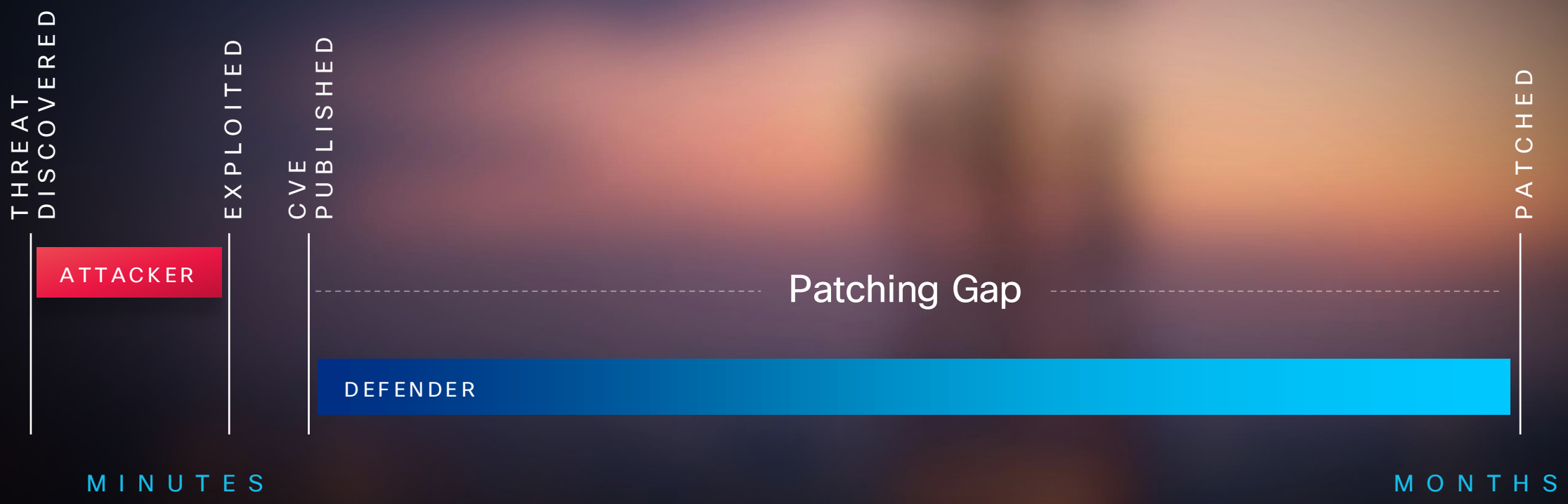
Protecting your infrastructure

From silicon to software – secured at every layer

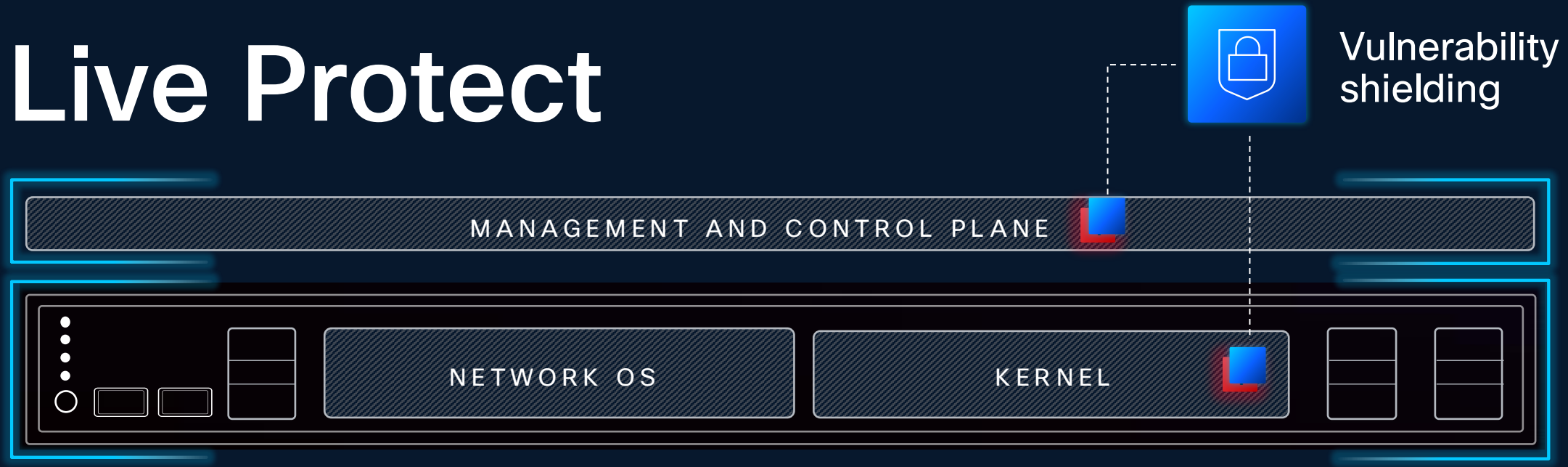


© 2026 Cisco and/or its affiliates. All rights reserved.

AI-speed attacks compress the patching window. Minutes to exploit. Months to patch.



Live Protect



EXTENDING ACROSS CISCO NETWORKING AND SECURITY

Apply policy to live system

Protect now, patch in planned window

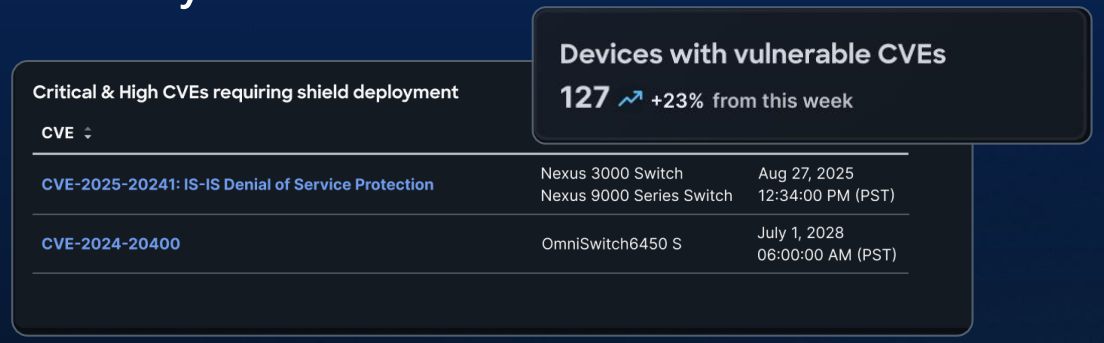
No downtime or switch reboot

Continuous re-validation

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

Live Protect helps teams act before patching is complete

01
Identify affected assets



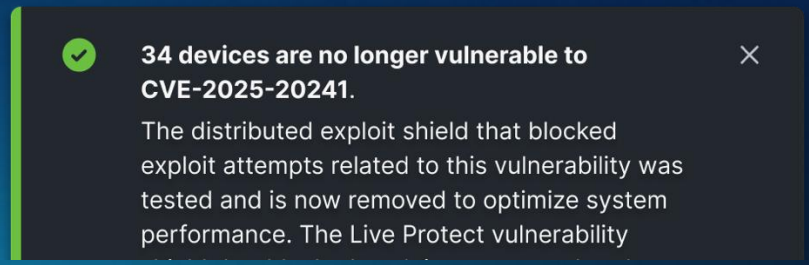
02
Deploy Vulnerability Shields



03
Monitor Shield activity



04
Patch software and auto-retire Shields



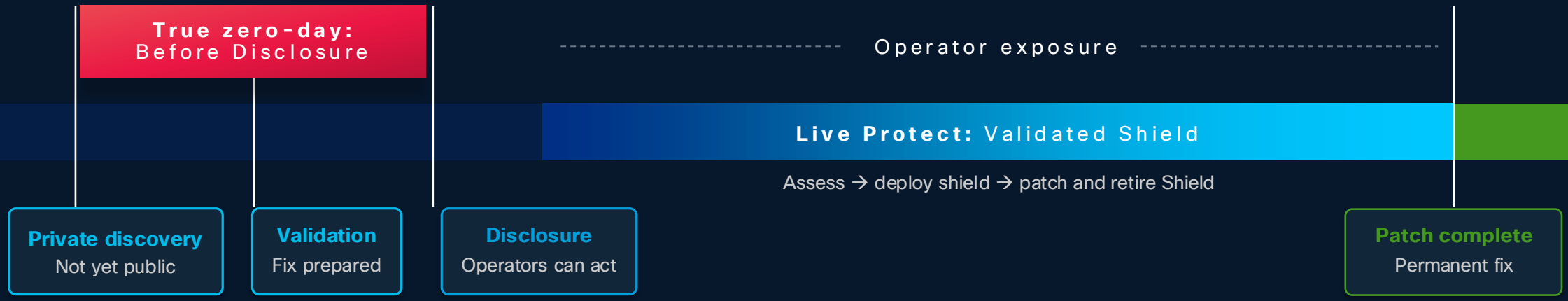
© 2026 Cisco and/or its affiliates. All rights reserved.

Some products and features described are in development and offered on a when-and-if-available basis. Cisco reserves the right to change delivery timelines and will have no liability for any delays or failures to deliver.

Most exploitation risk lives after disclosure

Disclosure starts the operator clock

After disclosure, operators assess affected assets, apply validated Shields where available, and patch to close exposure.



Live Protect helps operators compress post-disclosure exposure
for selected, validated conditions on supported Cisco products.

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

Post-quantum security must protect both communications and product trust

Secure Products

Device and supply chain tampering risk

- **Secure Boot**
  Hardware root-of-trust
- **Secure Storage**
  Protected key & identity store

Quantum resistant trust in HW systems

Secure Communications

Harvest Now, Decrypt Later risks

- **Key Establishment**
  Replace classical KEMs with ML-KEM
- **Identity & Trust**
  Replace classical signatures with ML-DSA

Key Exchange & Authentication

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

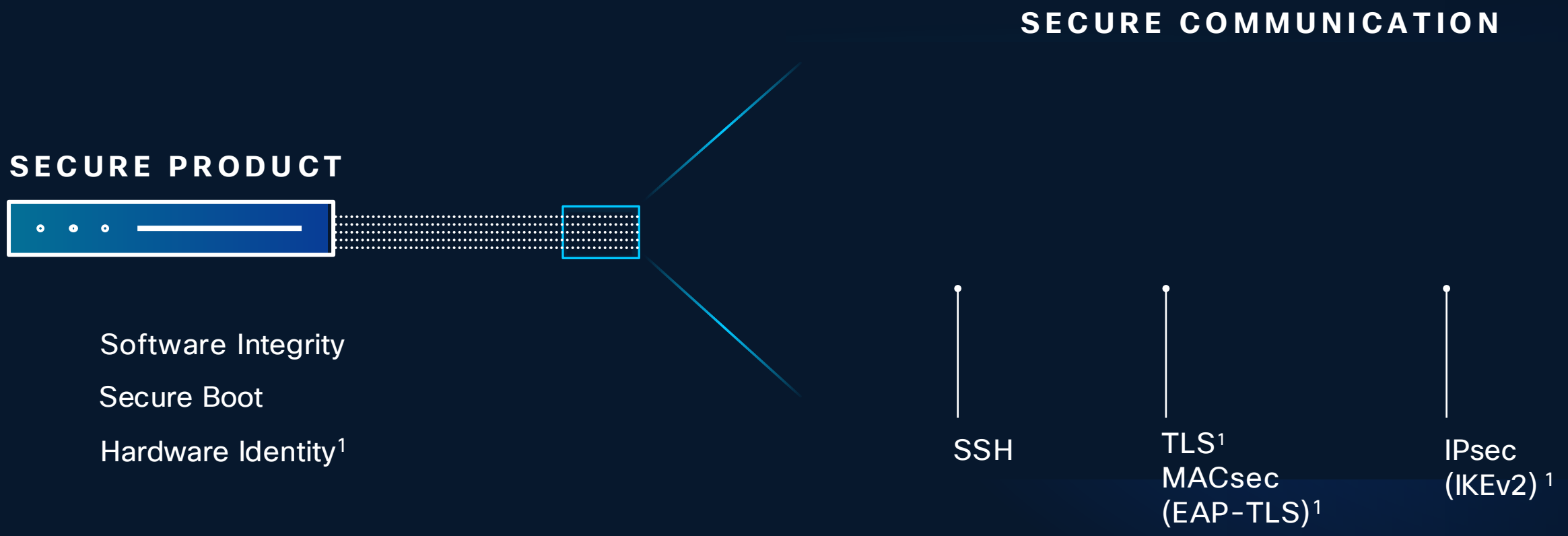
Bringing post-quantum security to Cisco N9000

NEW Q4 CY26

Protect communications and product trust.

Post-Quantum Cryptography (PQC) Resilience in Cisco N9000 Series Switches

Future proof investments | Secure sensitive data



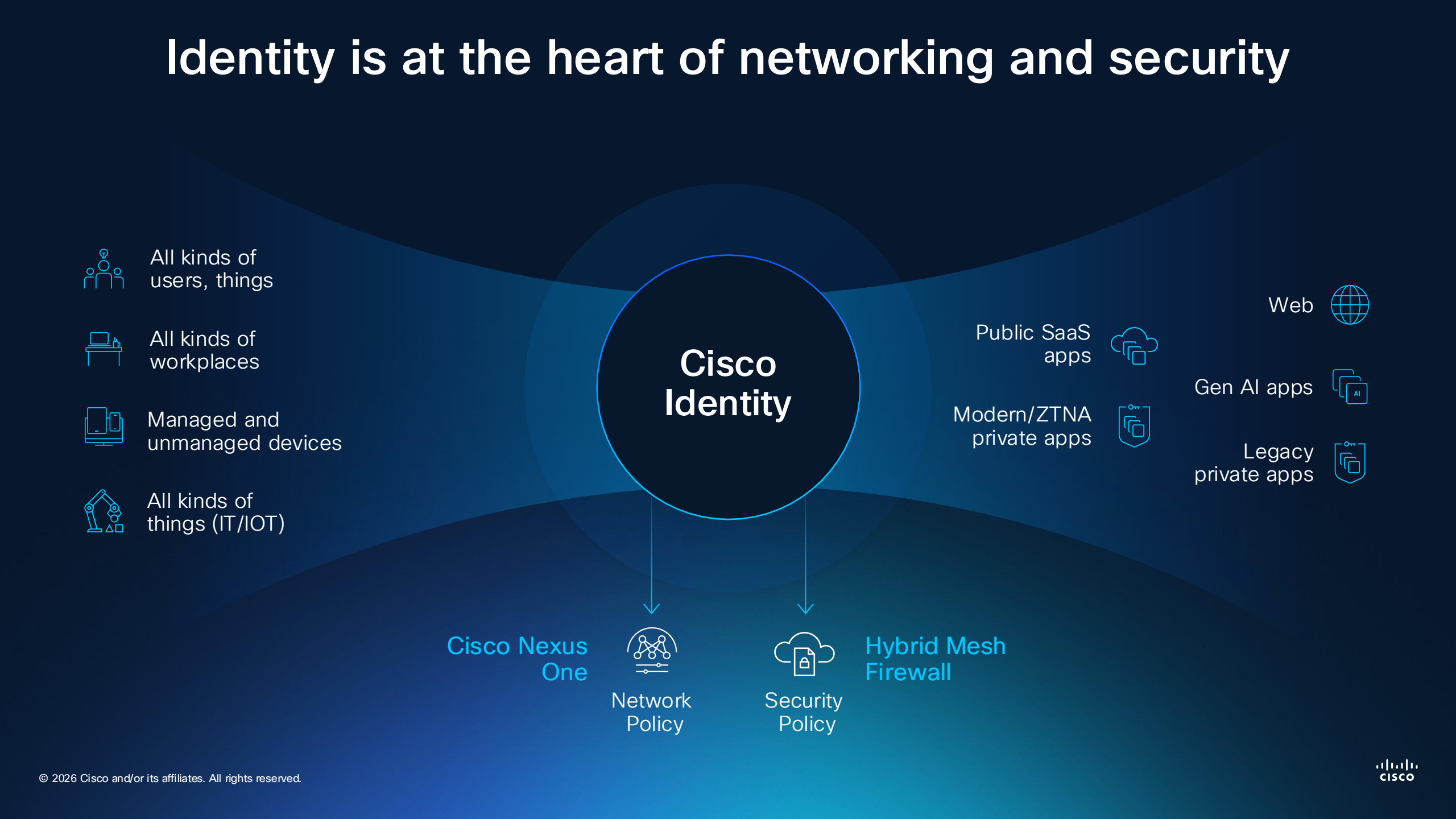
[1] Support planned for NX-OS and ACI CY-2027 releases

© 2025 Cisco and/or its affiliates. All rights reserved.

Identity

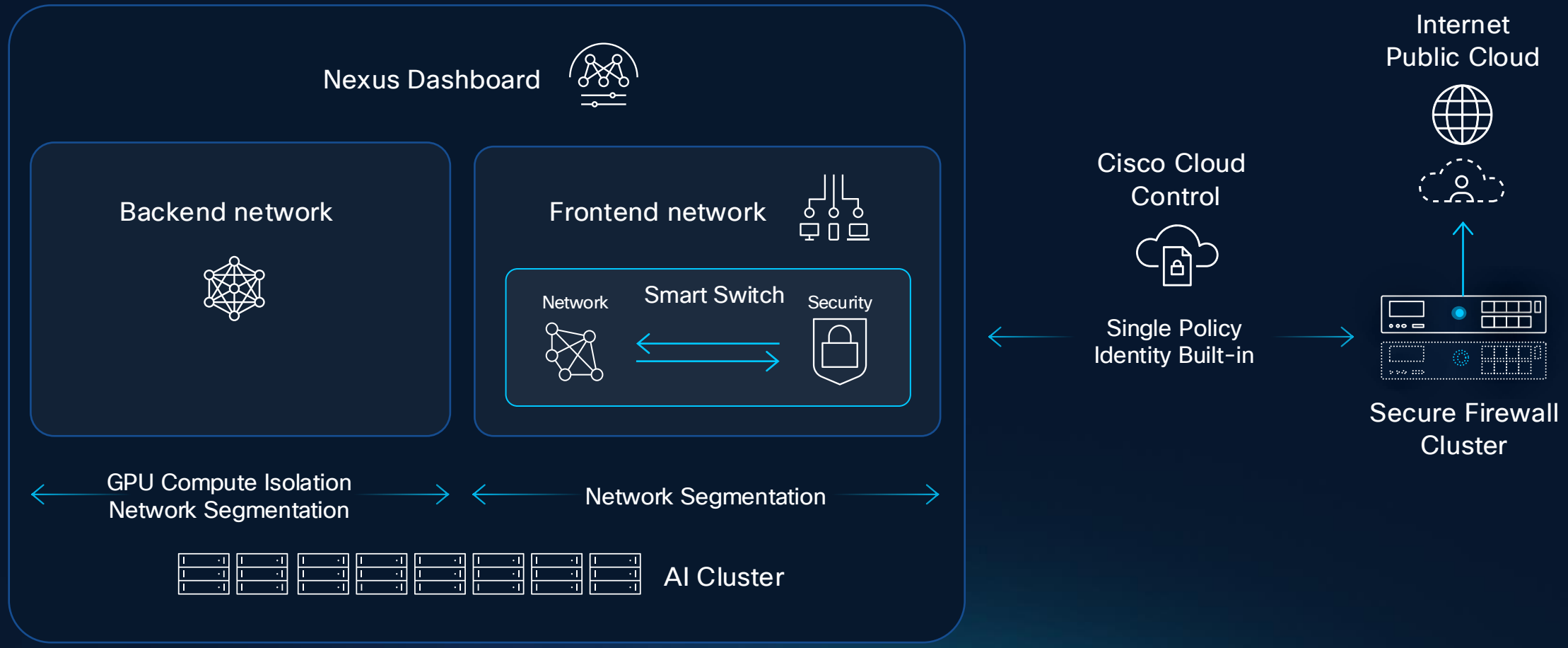
© 2026 Cisco and/or its affiliates. All rights reserved.

Identity is at the heart of networking and security



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

Secure your AI networking fabrics using identity



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

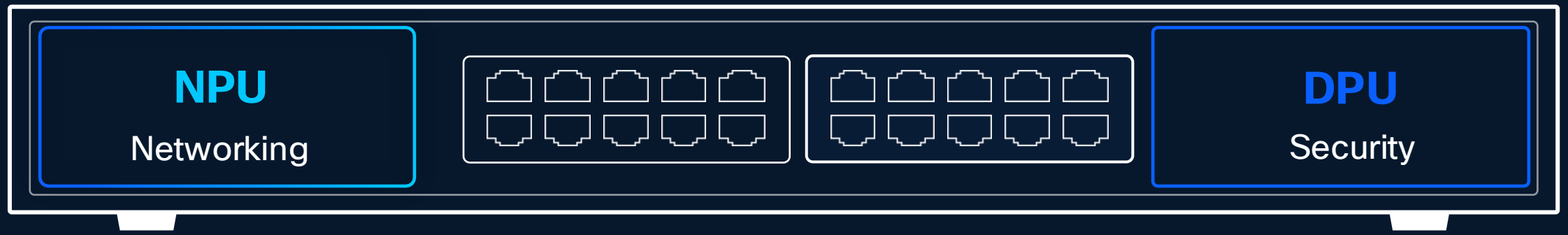
Segmentation

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

Security built into Nexus switching

Networking and hardware-accelerated security in one switch

AVAILABLE NOW



CISCO N9300 SMART SWITCH & HYPERSHIELD

Hardware-accelerated **segmentation** on every port

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

Nexus Smart Switch portfolio

25G connectivity



N9348Y2C6D-SE1U

48×25G
2×100G + 6×400G

100G connectivity



N9324C-SE1U

24×100G

800G DPU services throughput per switch

Cisco NX-OS, Silicon One E100 & AMD DPUs

Leaf | Border Leaf | Border Gateway

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

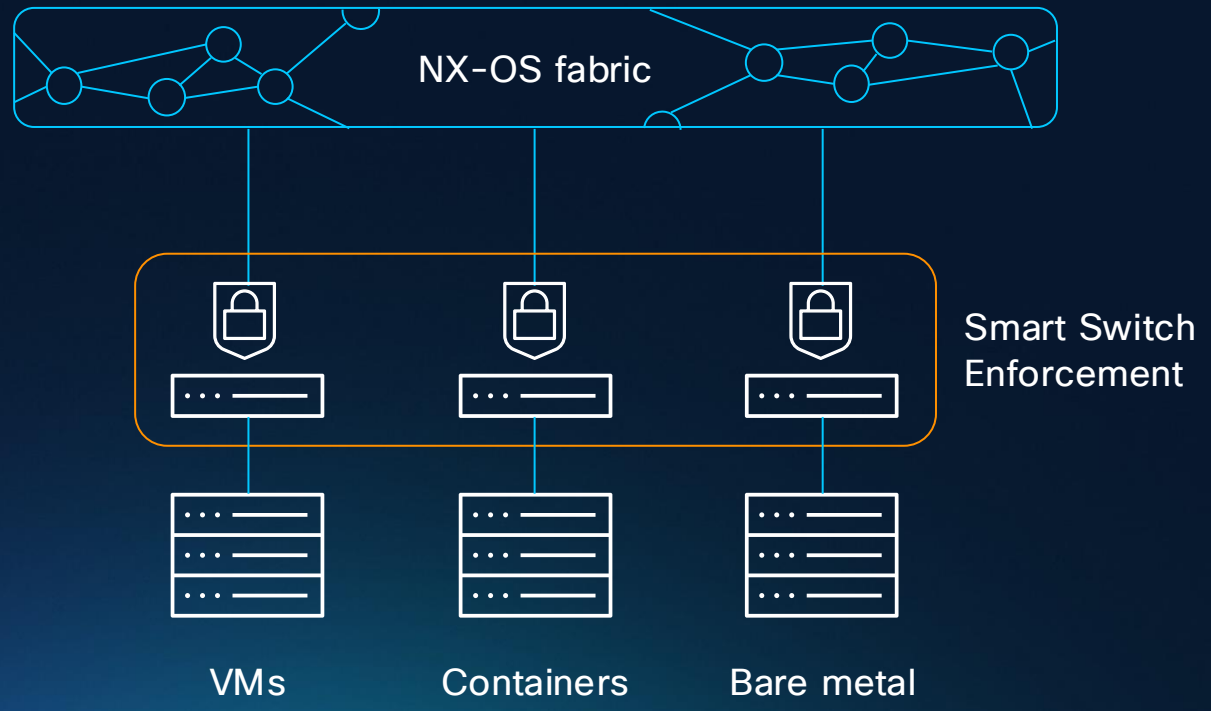
Segmentation close to workloads

Distributed stateful L4 enforcement in NX-OS fabrics

Consistent segmentation across VMs, containers and bare metal

800G

Stateful firewall throughput per Smart Switch

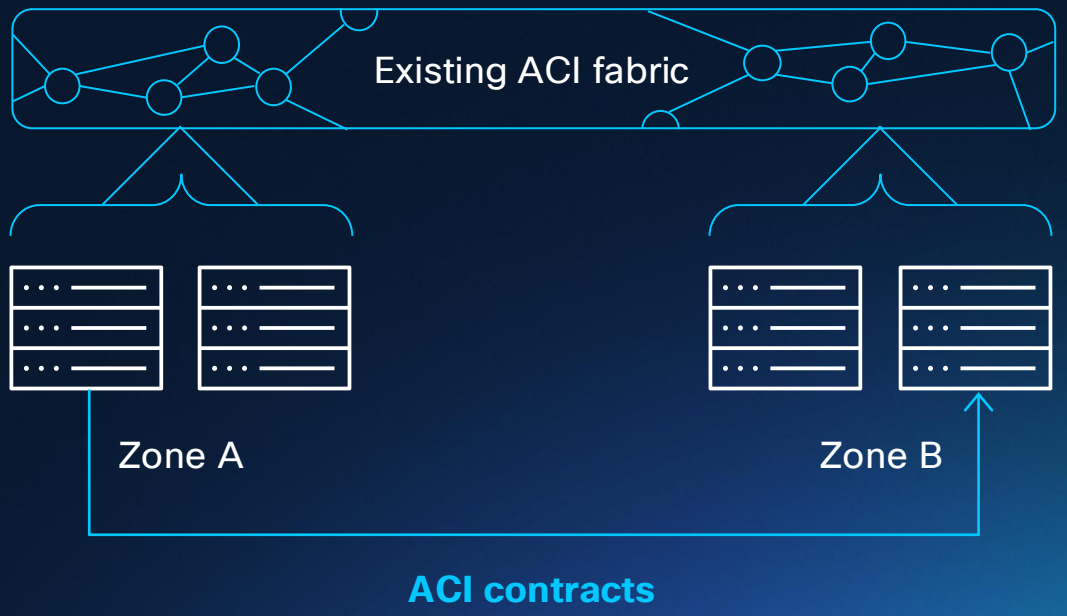


© 2026 Cisco and/or its affiliates. All rights reserved.

Stateful segmentation between ACI zones

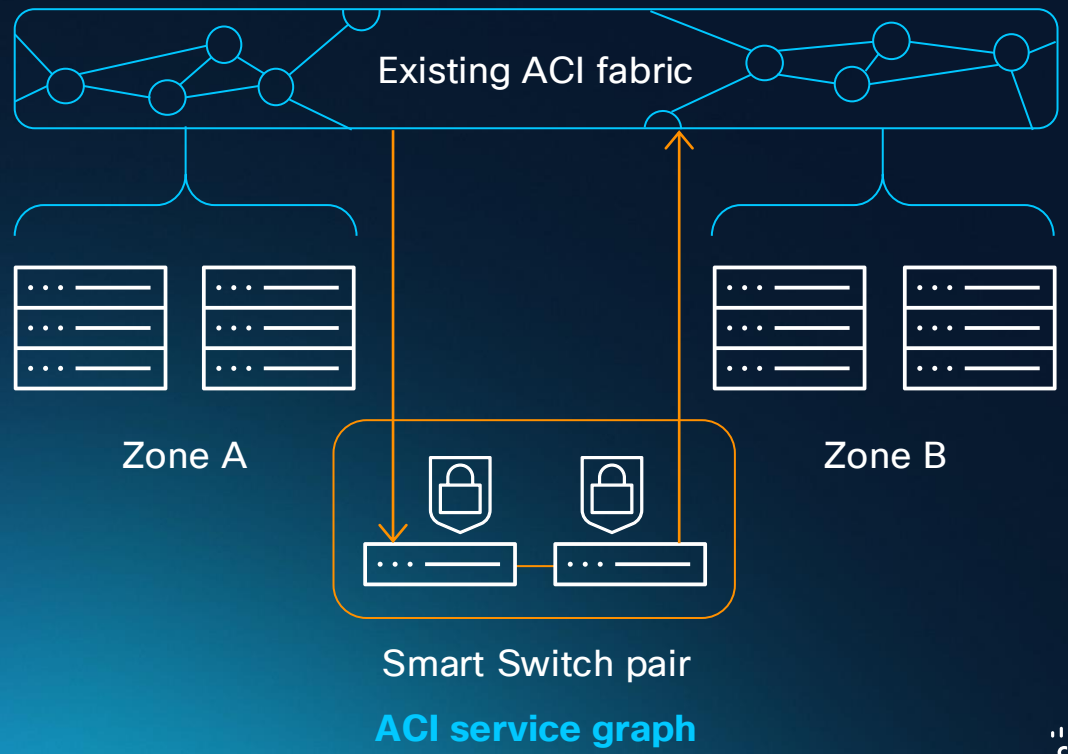
Before
Stateless ACI segmentation

- EPG/ESG contracts
- Limited policy-table capacity
- Costly firewall expansion



After
Cost-effective stateful zone firewalling

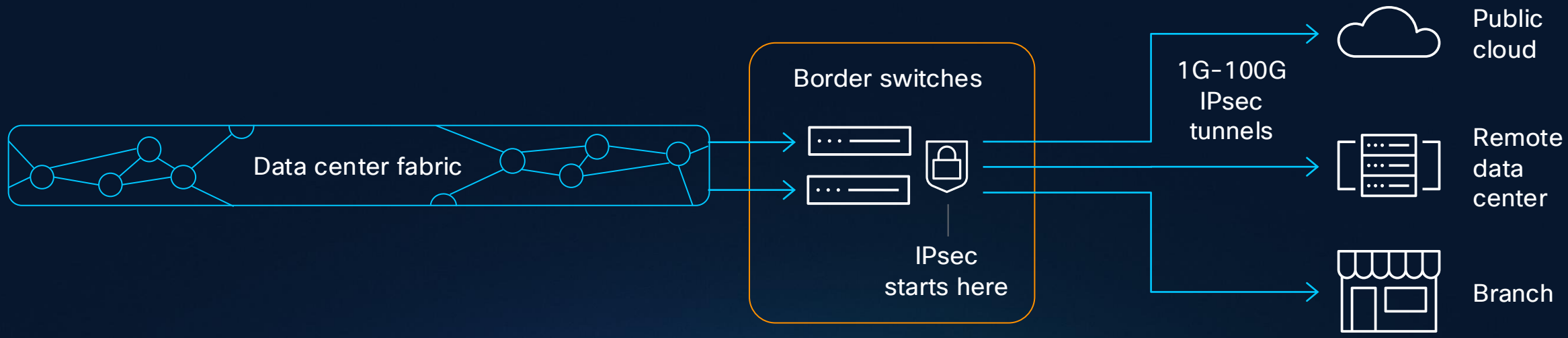
- Stateful L3/L4 inspection
- 1M security rules
- 800G firewall throughput



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

IPsec encryption at the fabric border

Secure connections to clouds, data centers and branches



Built on NX-OS
for Smart Switches
and E100 platforms

800G
IPsec capacity

1k
IPsec tunnels

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

Clear ownership. Shared troubleshooting.

NetOps manages networking. NetSecOps manages security.

NetOps

Switch lifecycle
Network policy
Network telemetry

Nexus Dashboard
NX-API/CLI



NetSecOps

Security policy lifecycle
Stateful segmentation
Security logs and telemetry

Hypershield controller
API

Shared troubleshooting

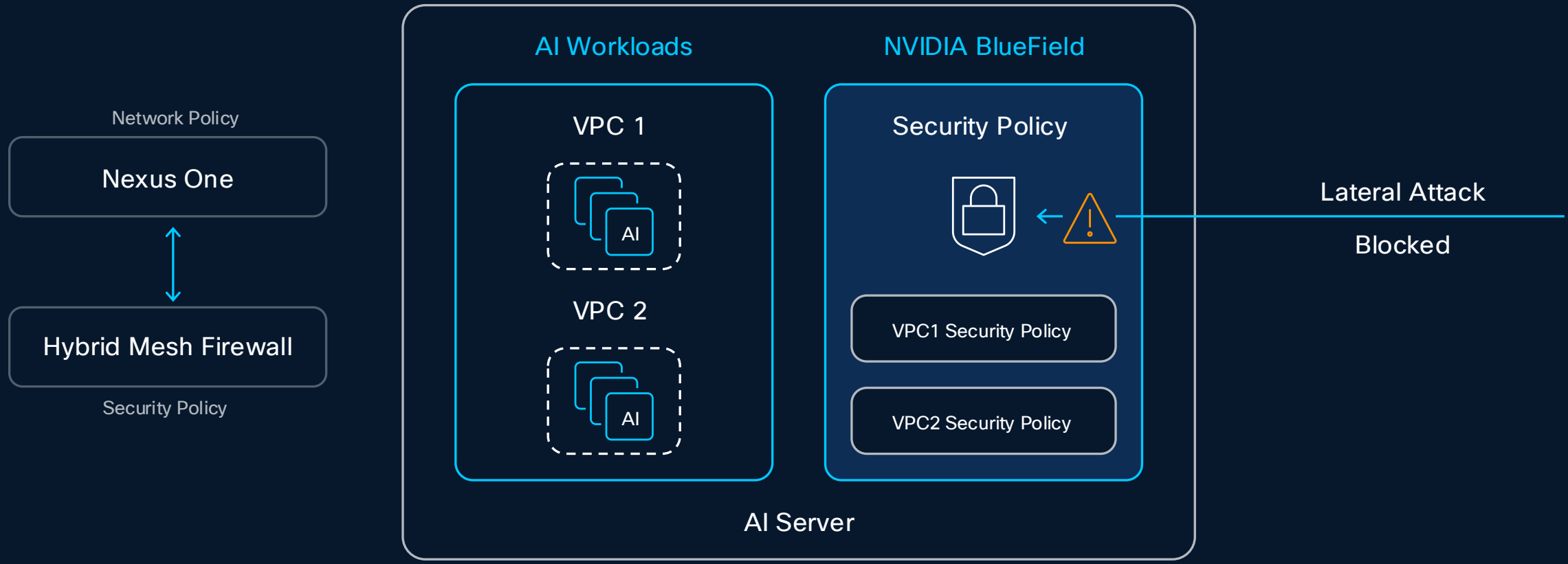
Trace traffic → Share context → Find root cause

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

AI workload protection for frontend fabric servers

NEW

NVIDIA BlueField DPUs with Cisco Hybrid Mesh Firewall to embed security on AI servers



Integrated Inline Security | High-Performance Scalability | Chokepoint-Free Enforcement

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

AI runs on Kubernetes

Process hiding

Credential harvesting

Privilege escalation

Container escape

Kernel exploit

File tampering

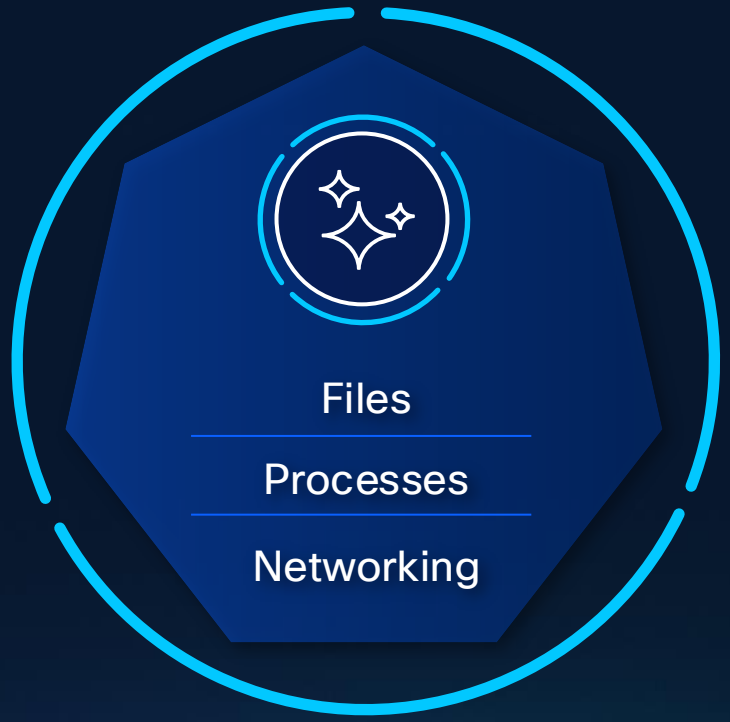
Sidecar injection

Shell injection

Network scanning

Reverse shell

Segmentation



Runtime shields

Host file system access

Service discovery abuse

API server probing

Token theft

Init container abuse

DNS tunneling

Deserialization

Unauthenticated service

Runtime socket exposure

Command injection

Process-level visibility

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

Segmentation is no longer optional

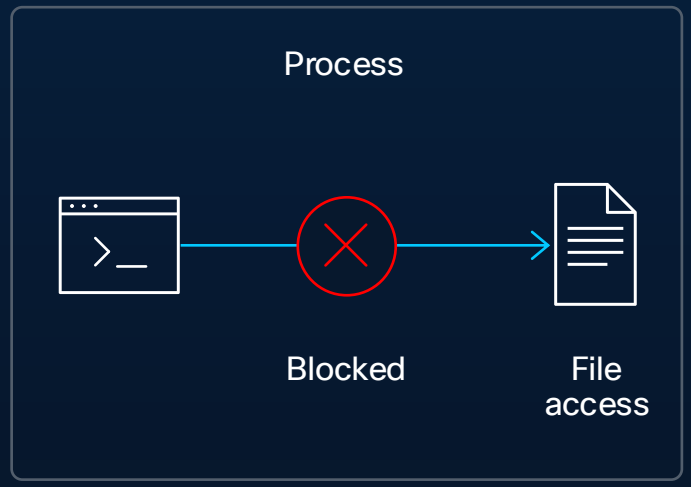


Stop threats from process to network with Cisco Isovalent

Process actions

Control what processes do

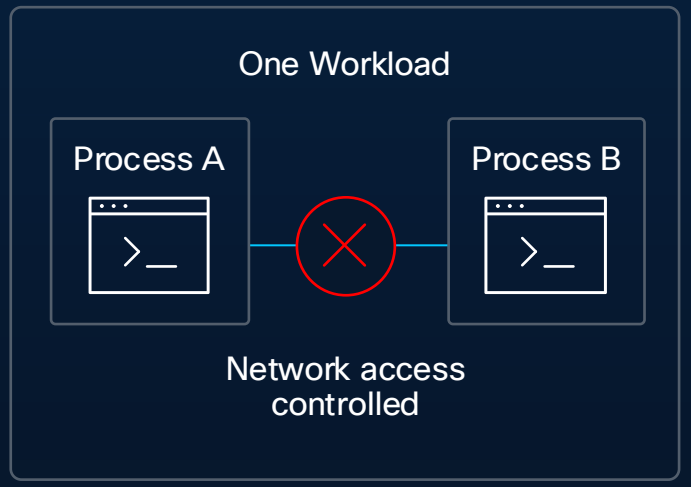
Enforce specific runtime actions



Process connections

Control traffic between processes

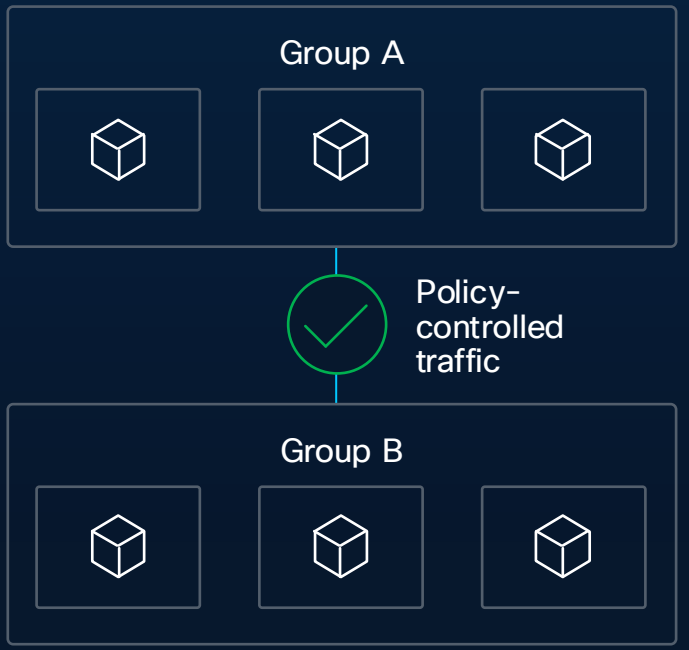
Process-aware network enforcement



Workload groups

Control traffic between groups

Segmentation across groups or zones



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

Protection

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

Cisco Firewall 6100

Near-limitless scale for AI readiness

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

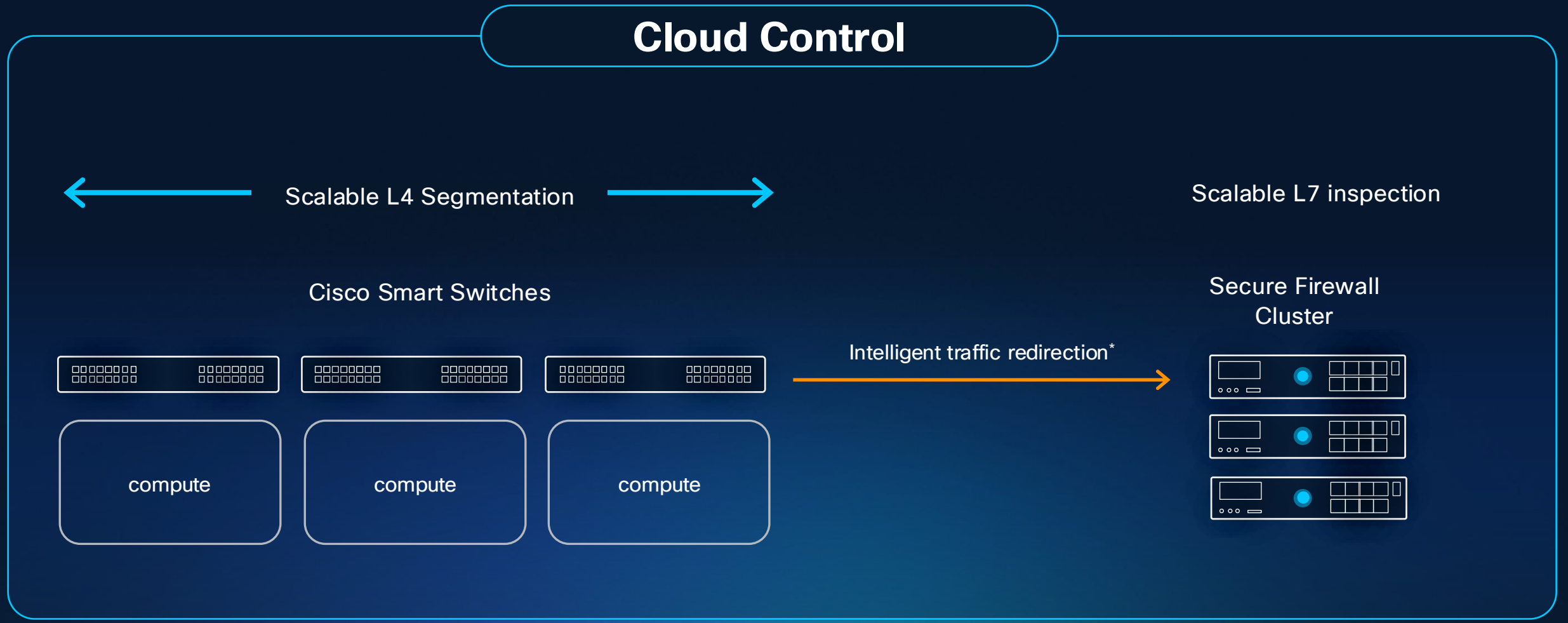
Changes math per protected Gbps: 80% less space, 60% less power, 1/3 the cost

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



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

Scalable security with Smart Switch + Firewall



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

* Roadmap

Cisco AI Defense

SECURING CUSTOM AGENTS AND AI APPS



Discover

New

Adaptive red teaming and guardrails



Detect

New

Protecting the full agent supply chain



Protect

New

Ecosystem to work with any cloud, any GPU

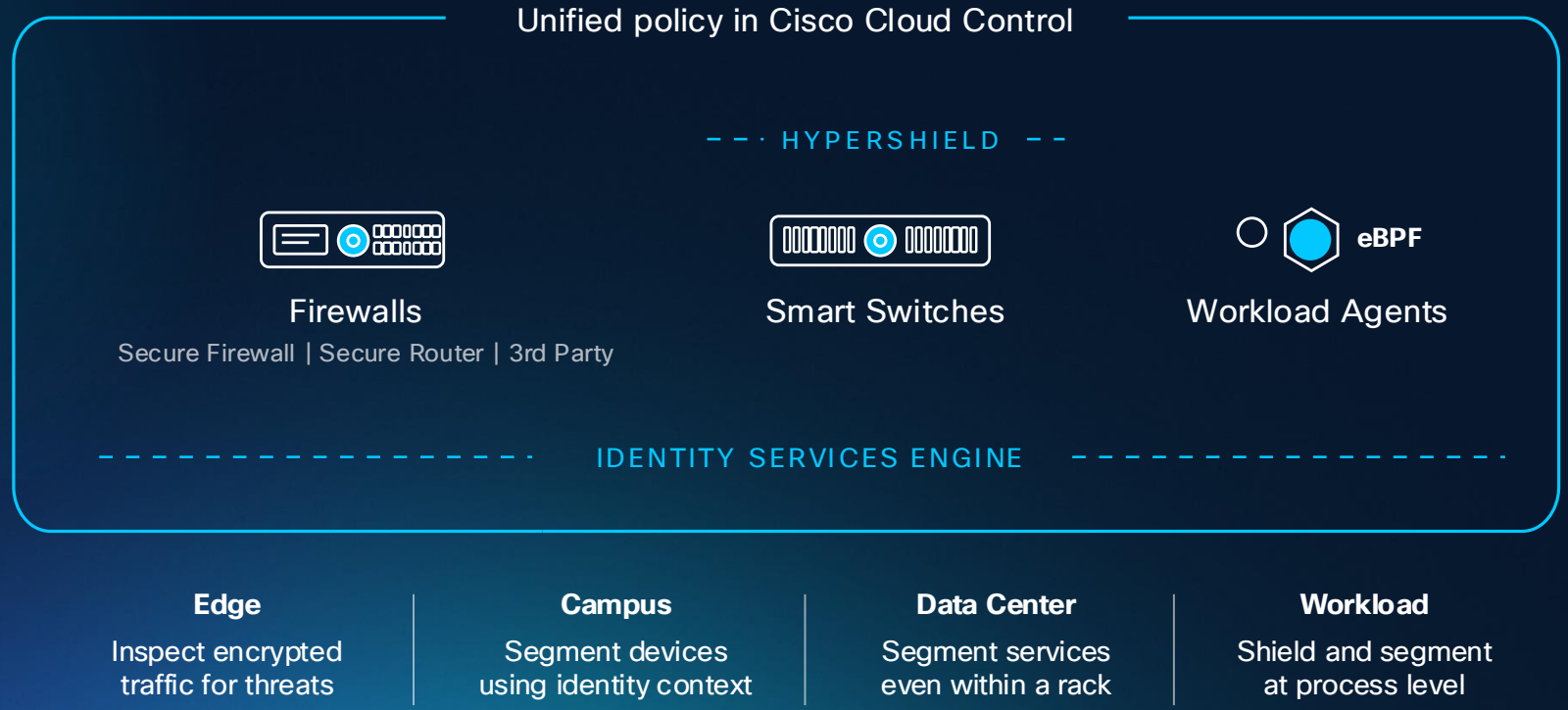
© 2026 Cisco and/or its affiliates. All rights reserved.

cisco

Protecting your apps and infrastructure, including AI

Hybrid Mesh Firewall + ISE

Hyper-distributed east-west traffic protection



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

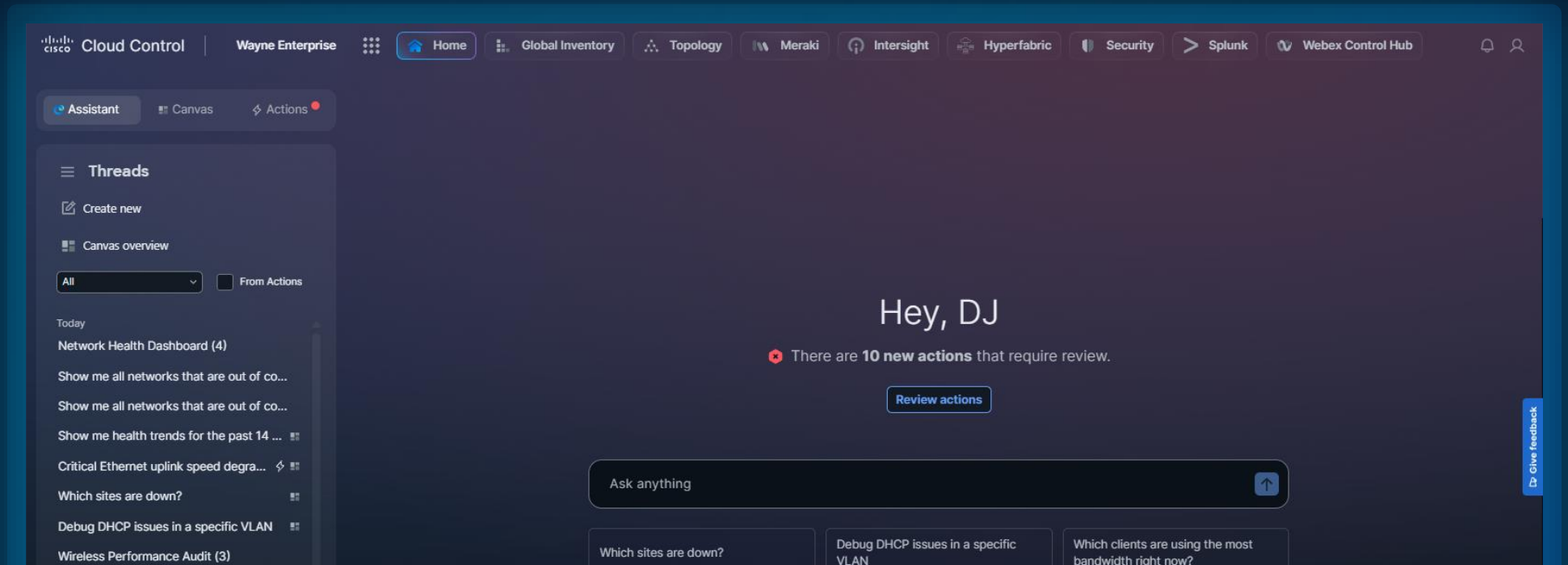
Visibility & insights

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

Cisco Cloud Control

One platform. Every domain. The foundation everything else is built on.

ThousandEyes · Security Cloud Control · Splunk · Nexus Dashboard · Nexus Hyperfabric · Catalyst SD-WAN · Intersight · & more

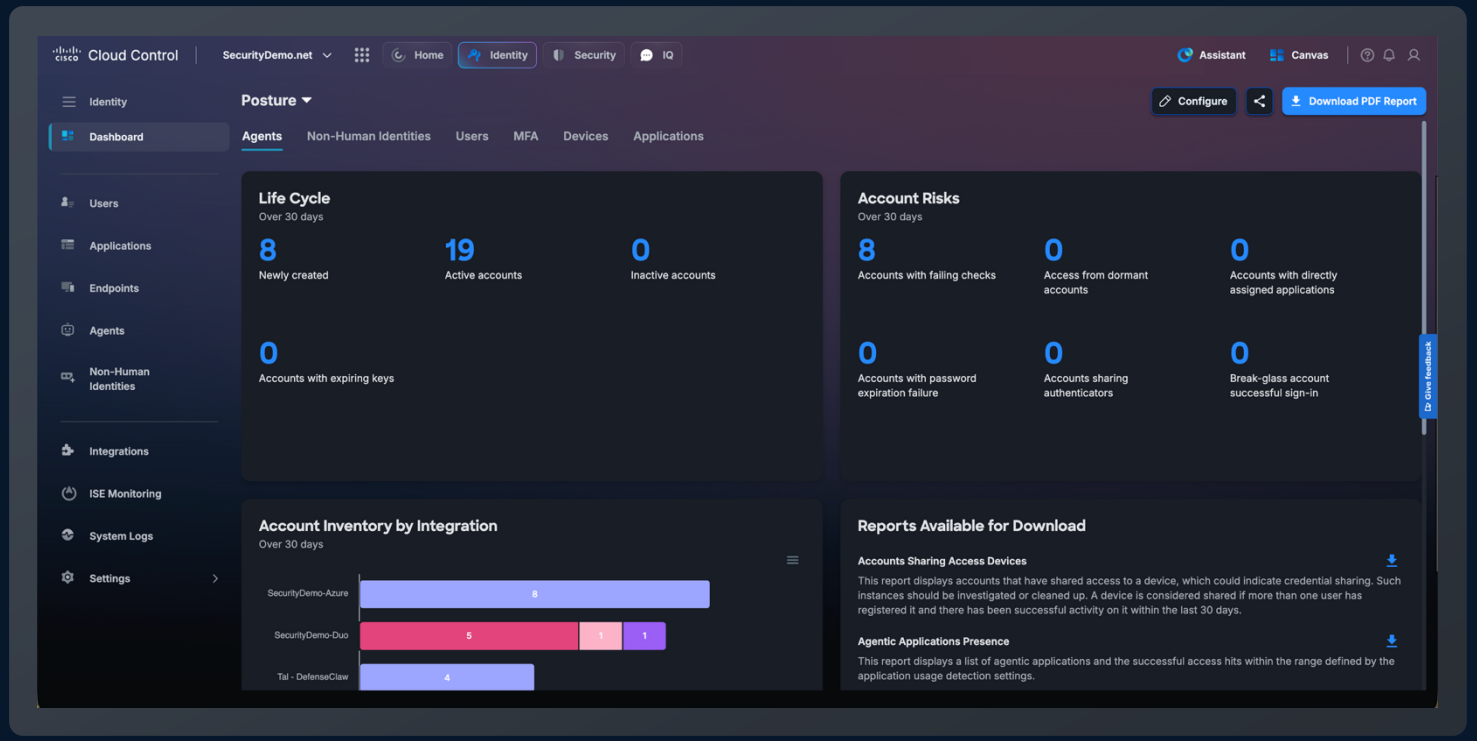


Cisco Cloud Control: Identity built-in

Unified visibility of all identities:
human, device and agent

Enhanced dynamic trust score
single identity signal from
Cisco and vendor systems

Identity powered AgenticOps
across Identity, Security
and Networking domain



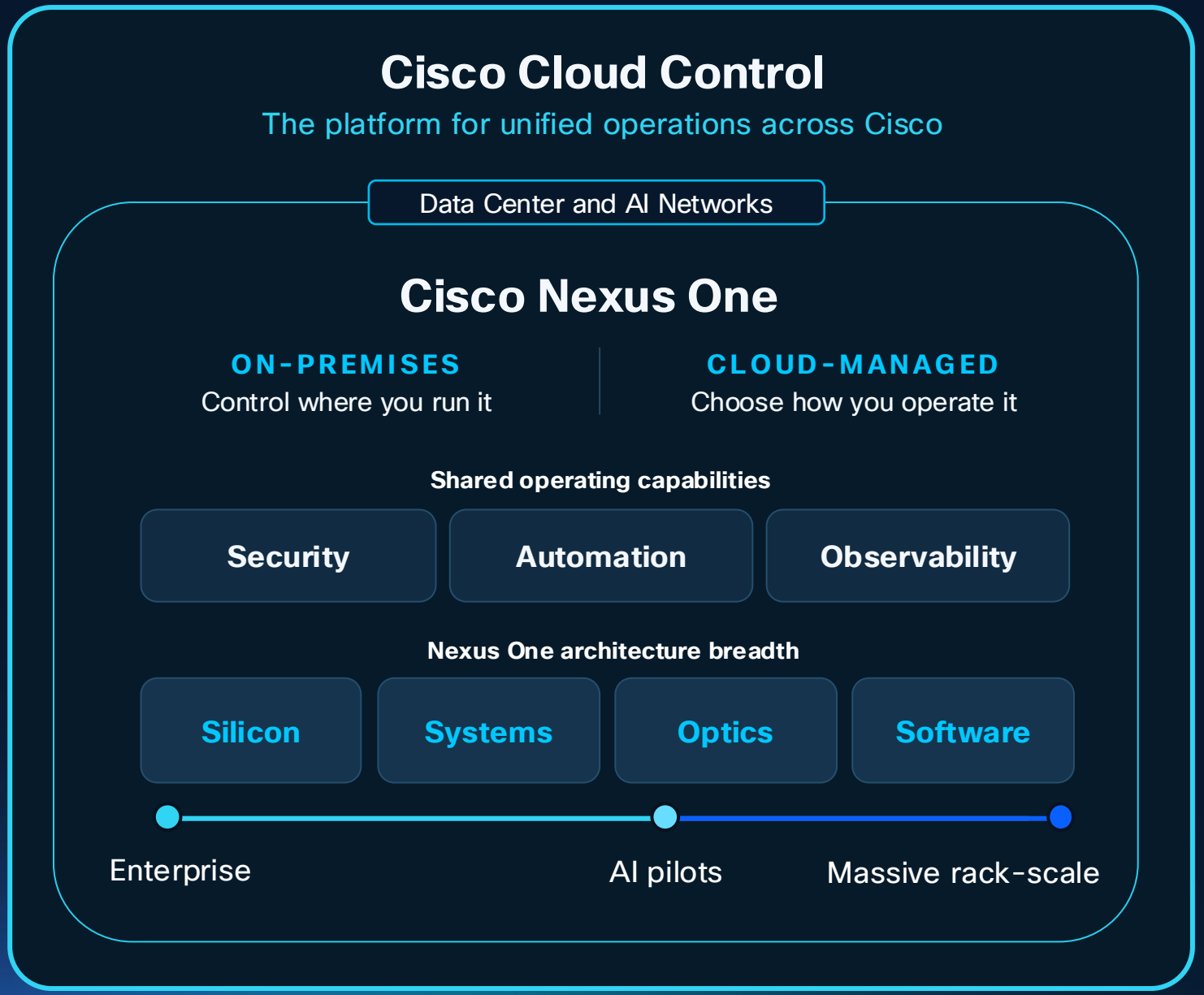
© 2026 Cisco and/or its affiliates. All rights reserved.

CISCO NEXUS ONE

Your data center network evolves

Your investments carry forward

Your choices stay open



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

Why now?

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

Secure your networks today with security fused into the network



Resilient infrastructure



Identity



Segmentation & steering



Protection



Visibility & insights

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

Secure Your AI Data Center. Start Now.

Talk to your Cisco account team to map these capabilities to your fabric.

Learn more about Cisco N9300 Smart Switches

Experience No Downtime with Live Protect

Learn more about Cisco Nexus One

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