CISCO Connect

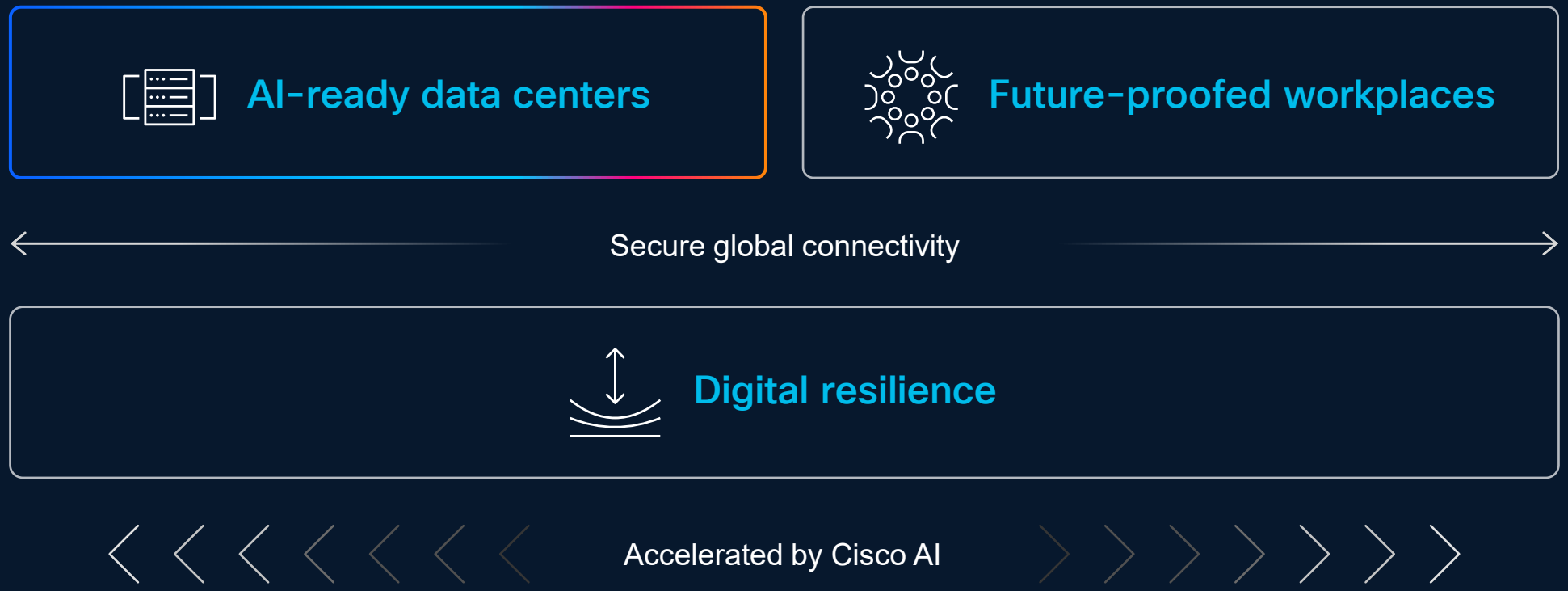
Secure Networking for AI-Ready Data Centers



Chris Barrett
Global DCN Specialist,
www.linkedin.com/in/ciscochris

October 2026

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



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

The three forces re-shaping security

The Mythos moment

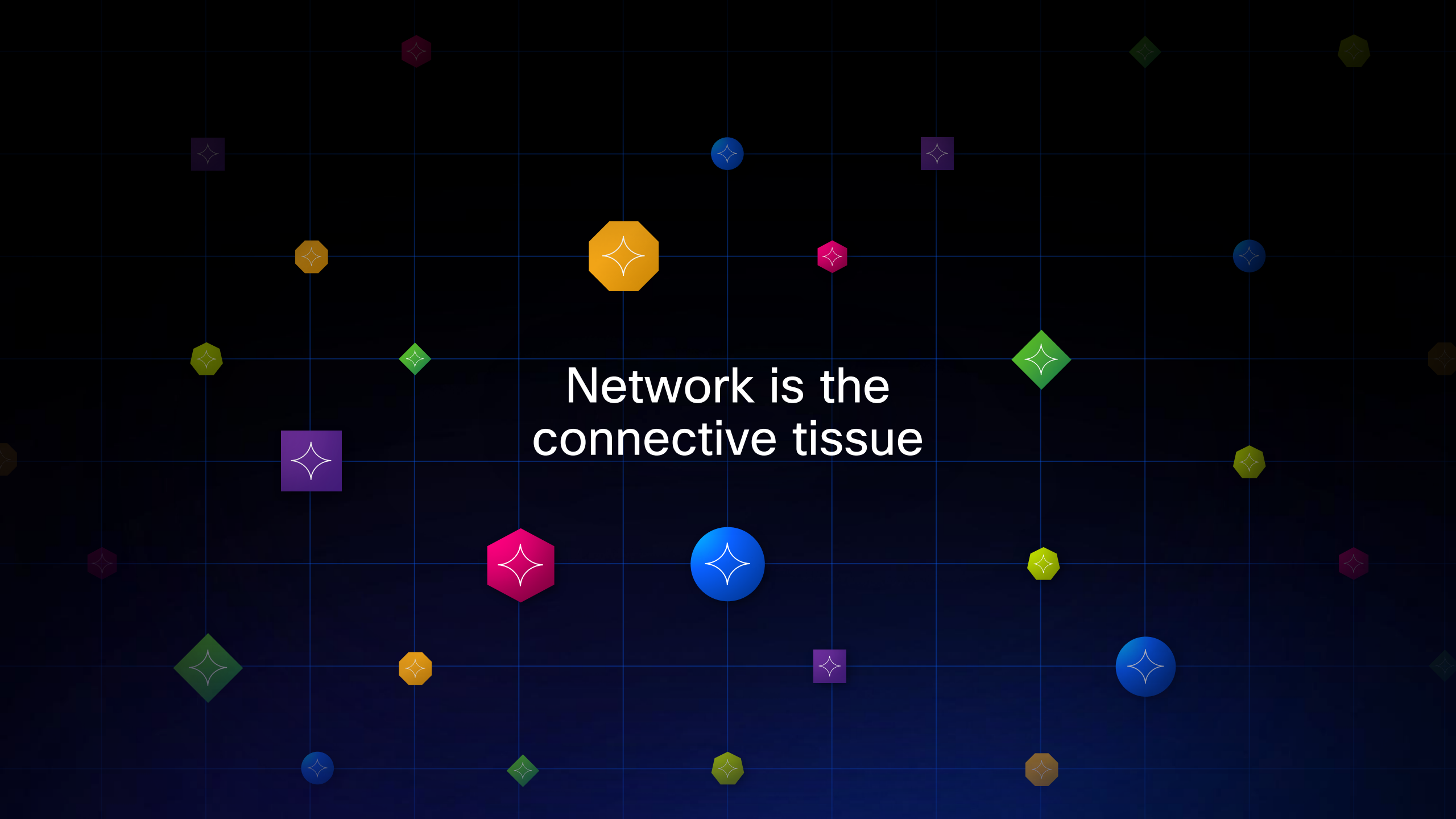
Shields Up

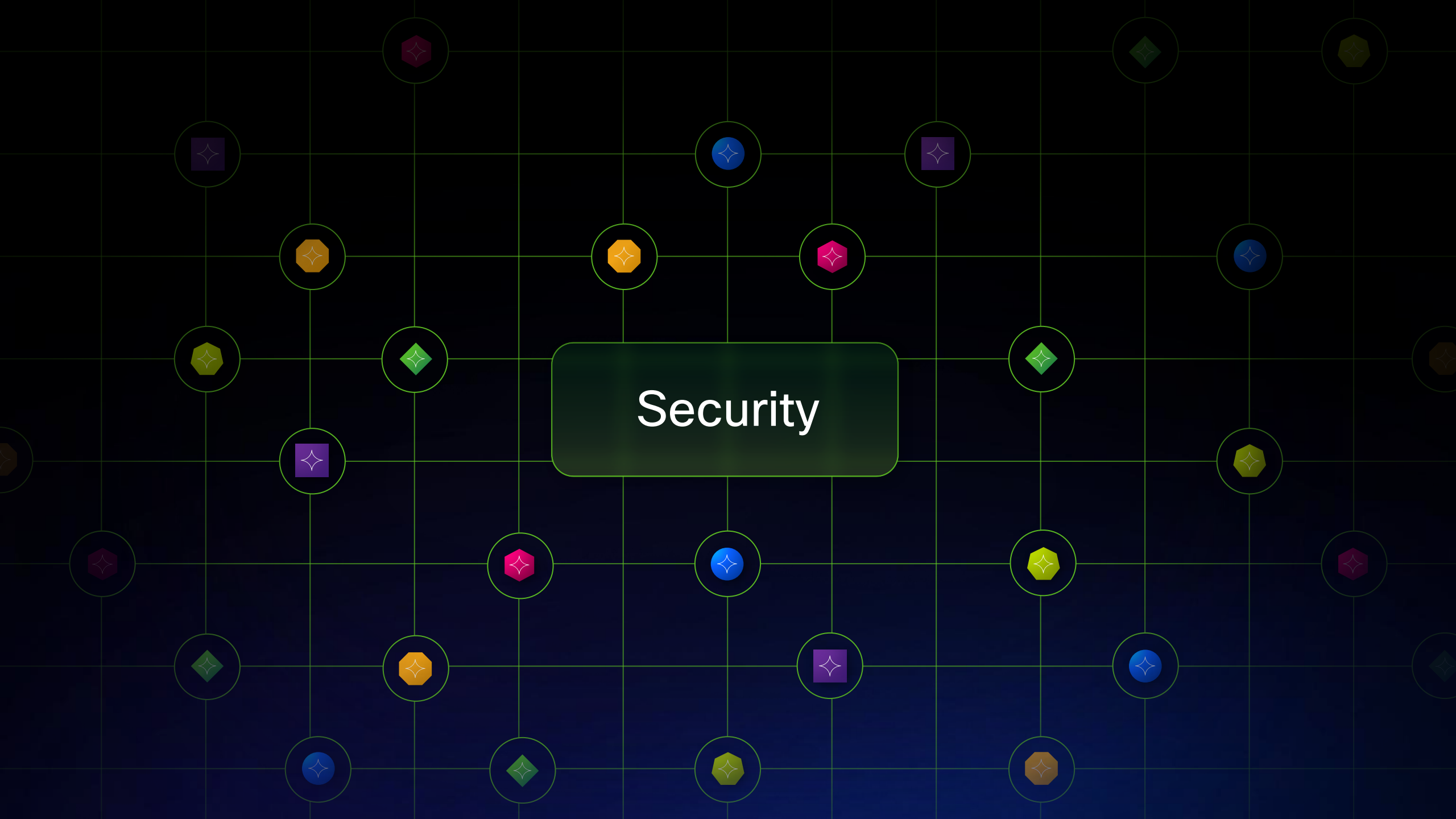
The OpenClaw moment

Security for Agents

The need for speed

Security using Agents


Network is the
connective tissue


Security

Secure Networking: security fused into the network



Resilient infrastructure



Identity



Segmentation & steering



Protection

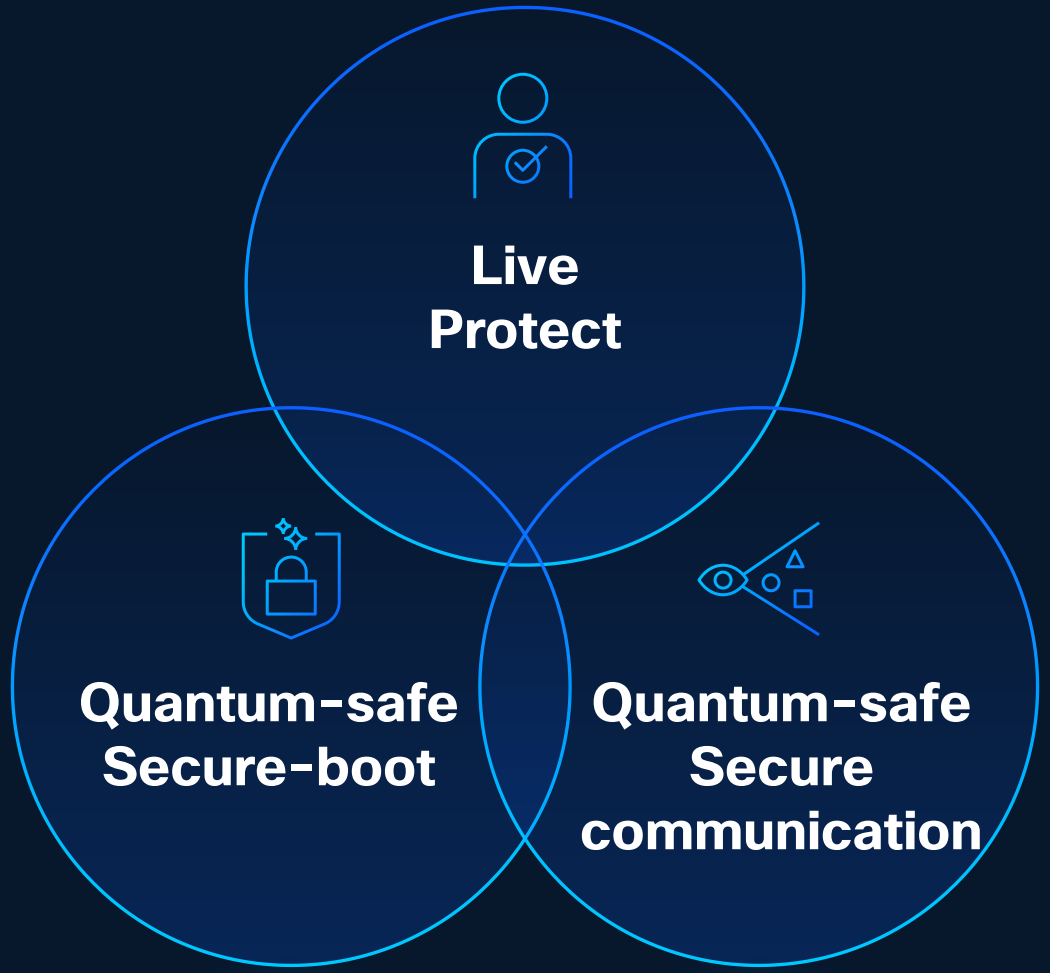


Visibility & insights

Resilient infrastructure

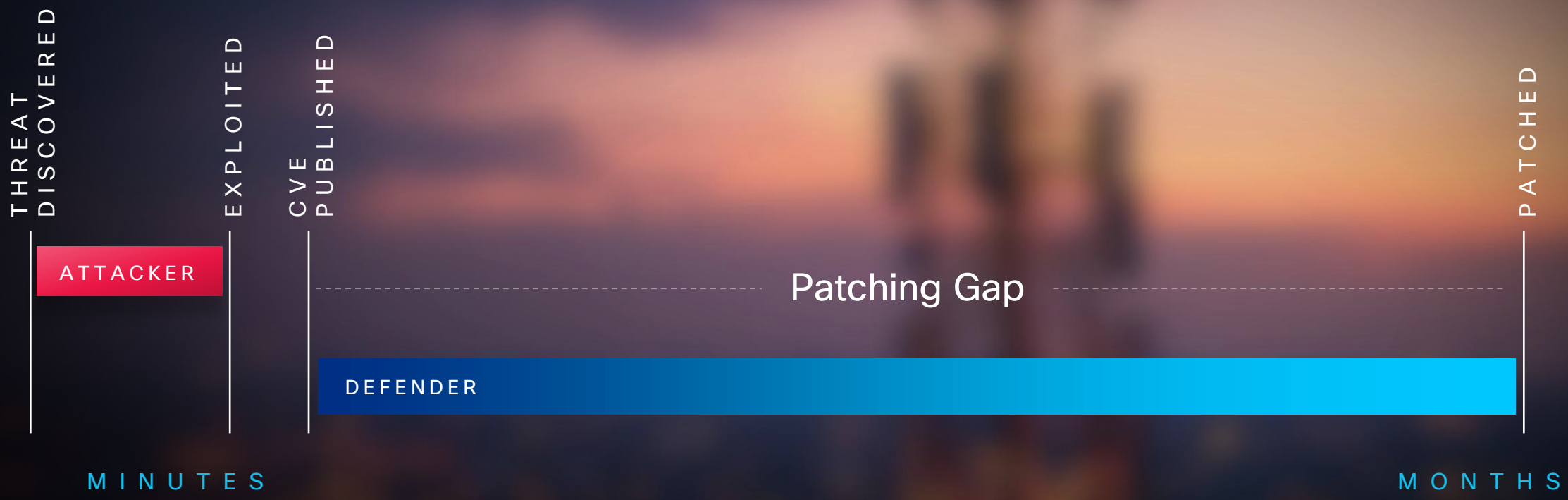
Protecting your infrastructure

From silicon to software – secured at every layer

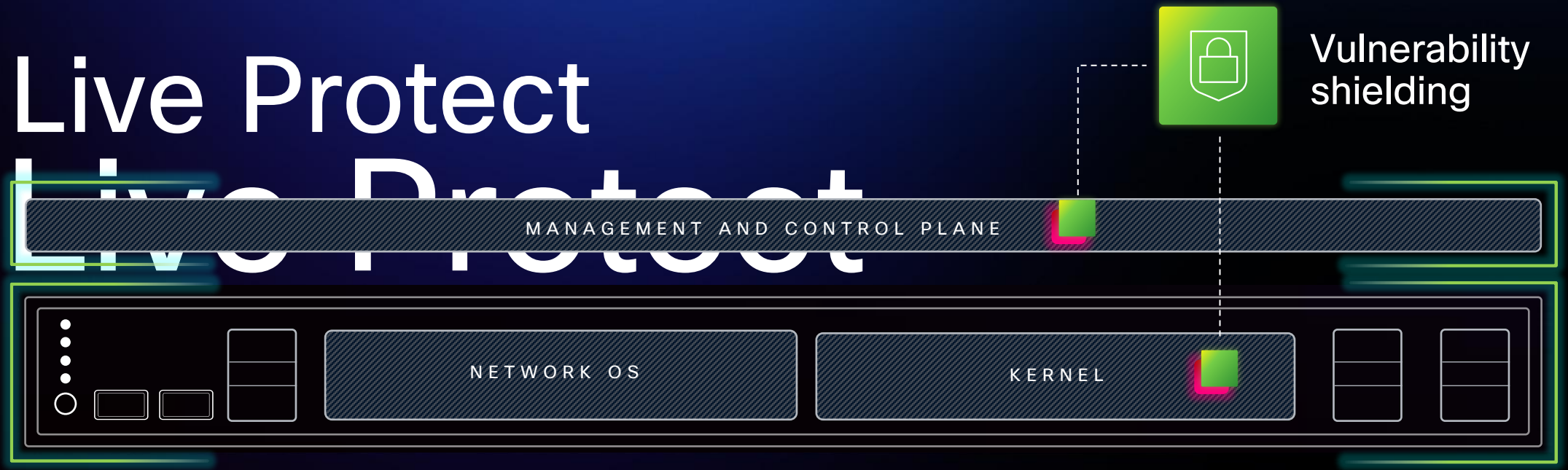


© 2026 Cisco and/or its affiliates. All rights reserved.

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



Live Protect



EXTENDING ACROSS CISCO NETWORKING AND SECURITY

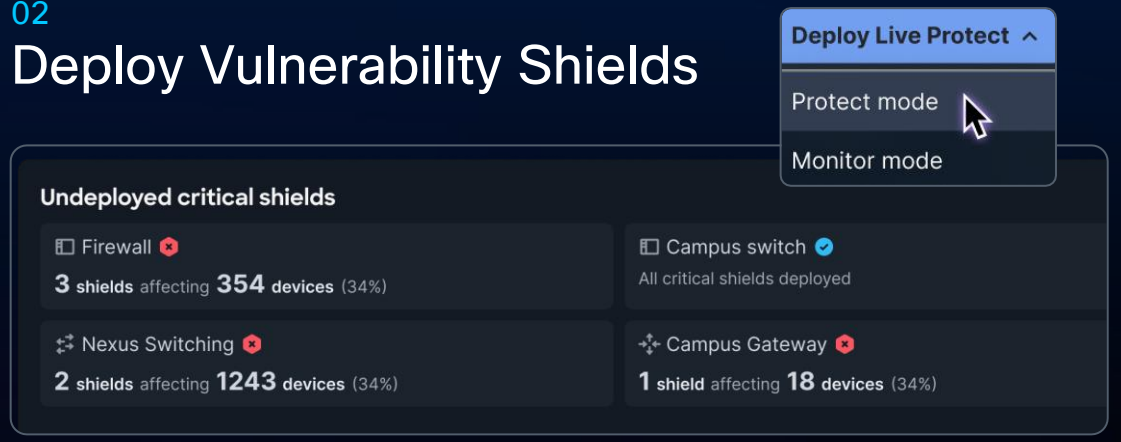
Apply policy to live system	Protect now, patch in planned window	No downtime or switch reboot	Continuous re-validation

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 retire Shields

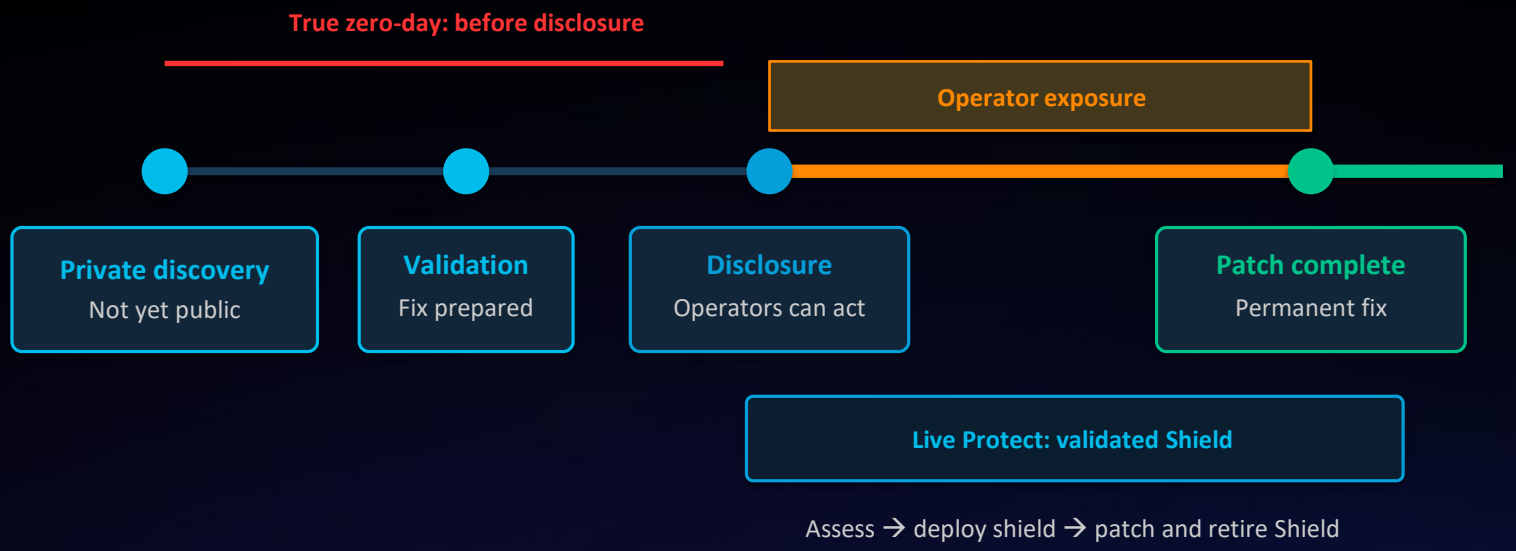


Some products and features described are in development and offered on a when-and-if-available basis. Cisco reserves the right to change delivery timelines and will have no liability for any delays or failures to deliver.

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.

Post-quantum security must protect both communications and product trust

Harvest Now, Decrypt Later risks

Secure Communications

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

Key Exchange & Authentication

Device and supply chain tampering risk

Secure Products

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

Quantum resistant trust in HW systems

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

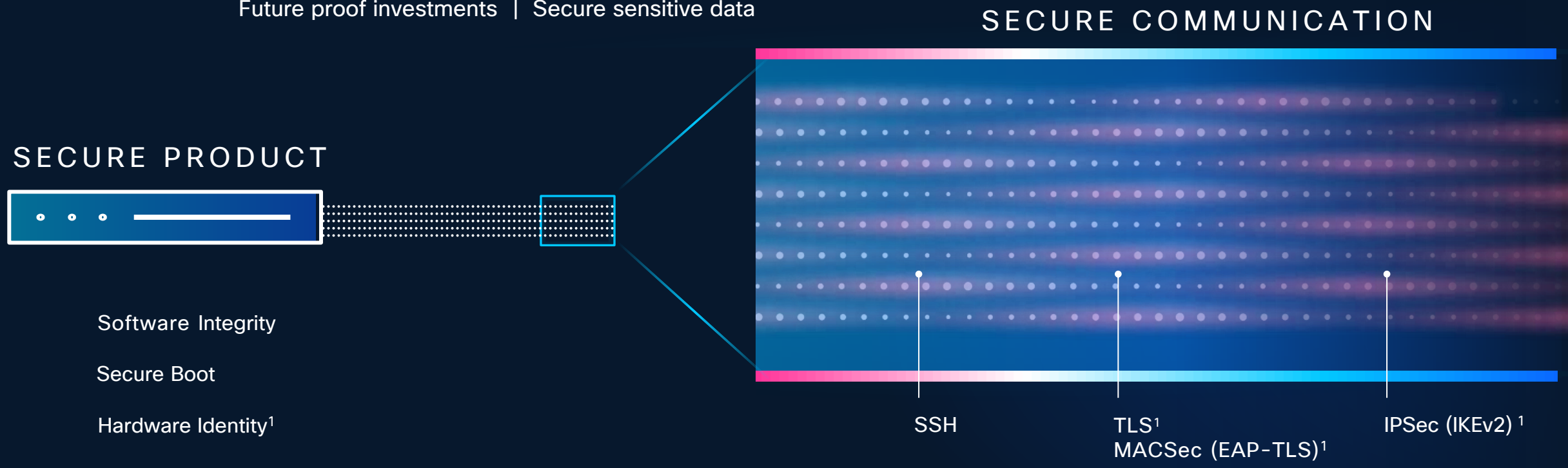
NEW Q4 CY26

Quantum-safe data center networks

Protect your data from Harvest Now, Decrypt Later

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

Identity is at the heart of networking & security



All kinds of users, things



All kinds of workplaces



Managed and unmanaged devices



All kinds of things (IT/IOT)

Cisco Identity



Public SaaS apps



Web



Modern/ZTNA private apps



Gen AI apps



Legacy private apps

Cisco Nexus One



Network Policy



Security Policy

Hybrid Mesh Firewall

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

cisco

GA in Oct 2026

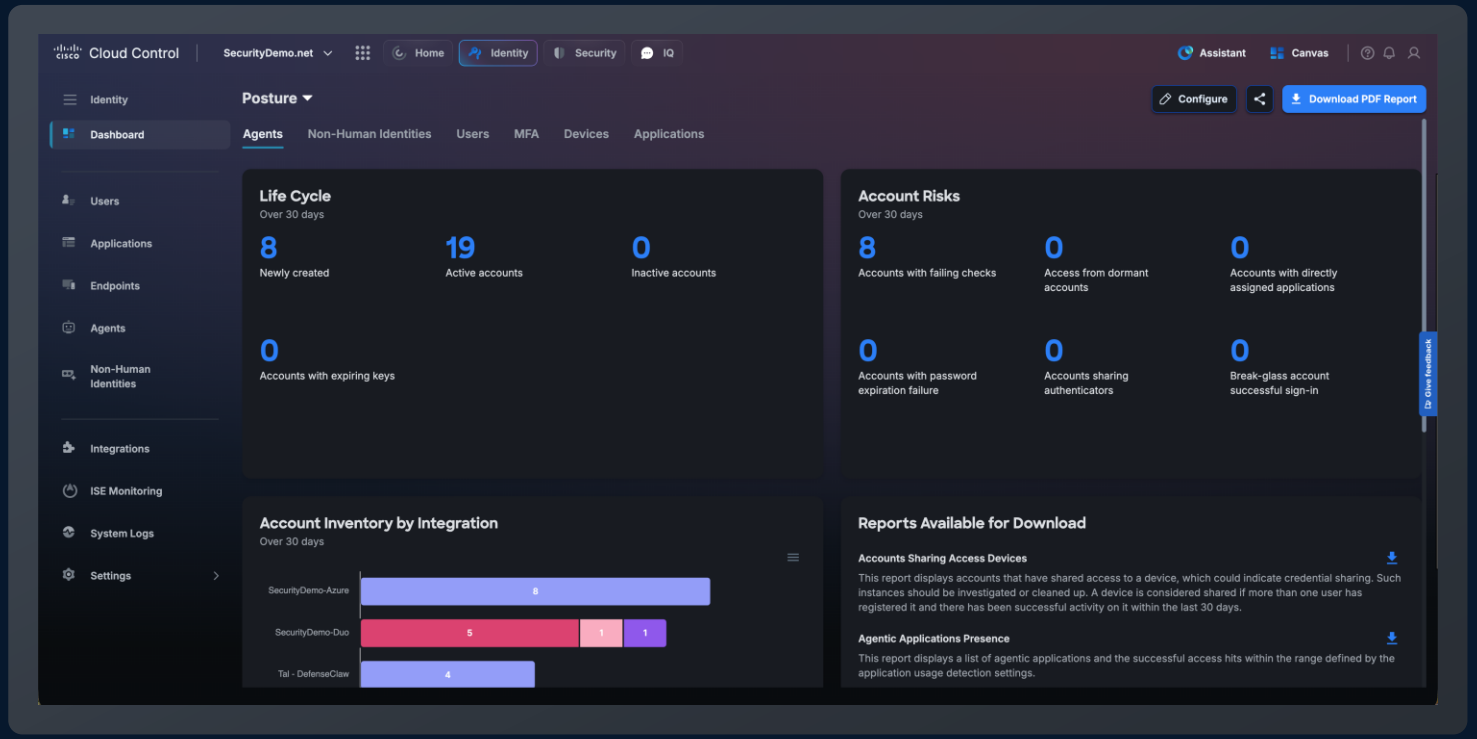
New

Cisco Cloud Control: identity built-in

Unified visibility of all identities
human, device and agent

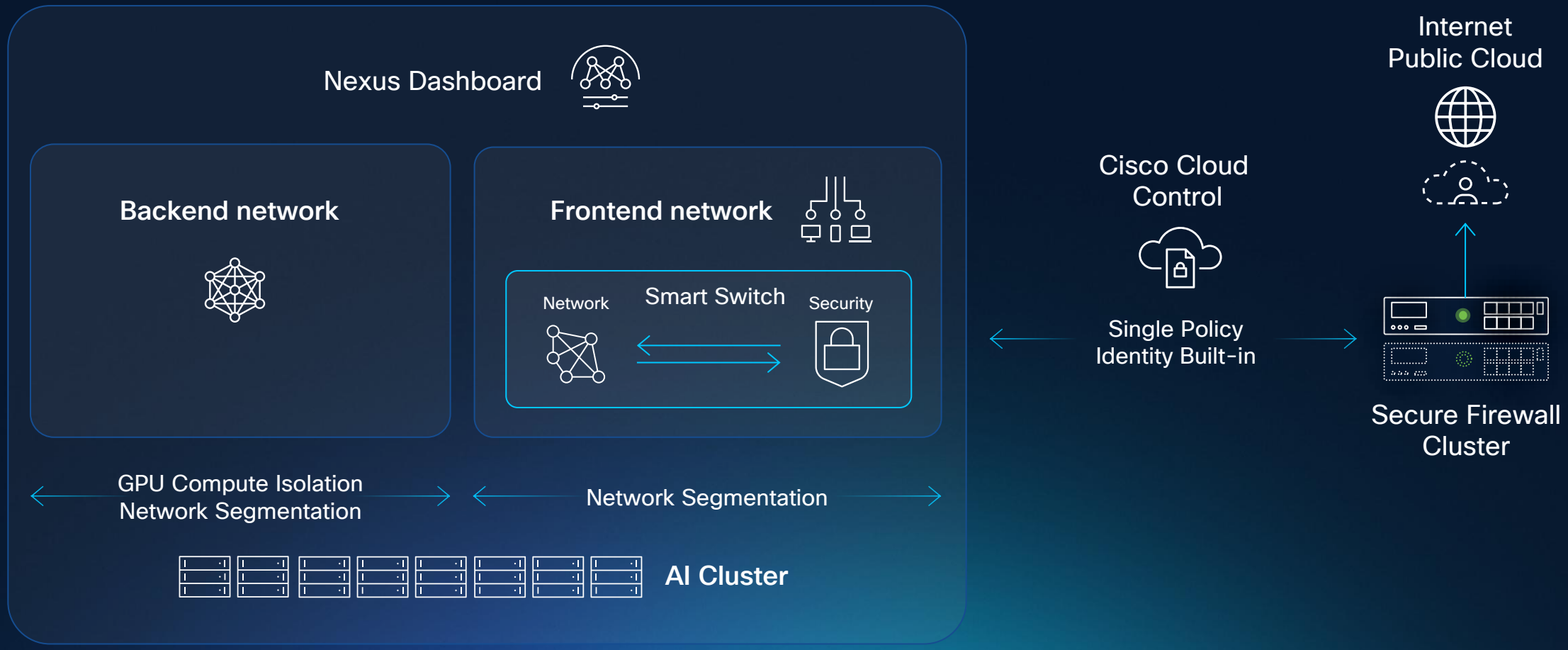
Enhanced dynamic trust score single
identity signal from
Cisco and vendor systems

Identity powered AgenticOps
across Identity, Security
and Networking domain



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

Secure your AI networking fabrics using identity



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

Segmentation

Threat containment at massive scale built into your network



Hardware-accelerated segmentation on every port

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

Nexus Smart Switches

The new standard for top of rack switching

Accelerate DC modernization

Runs on feature-rich NX-OS



N9348Y2C6D-SE1U

Front panel ports: 48x25G, 2x100G, 6x400G | 800G L3/L4 stateful firewall



Nexus 9324C-SE1U

Front panel ports: 24x100G | 800G L3/L4 stateful firewall

Silicon One E100 NPU

AMD DPU

Primary roles

- Leaf
- Border Leaf
- Border Gateway

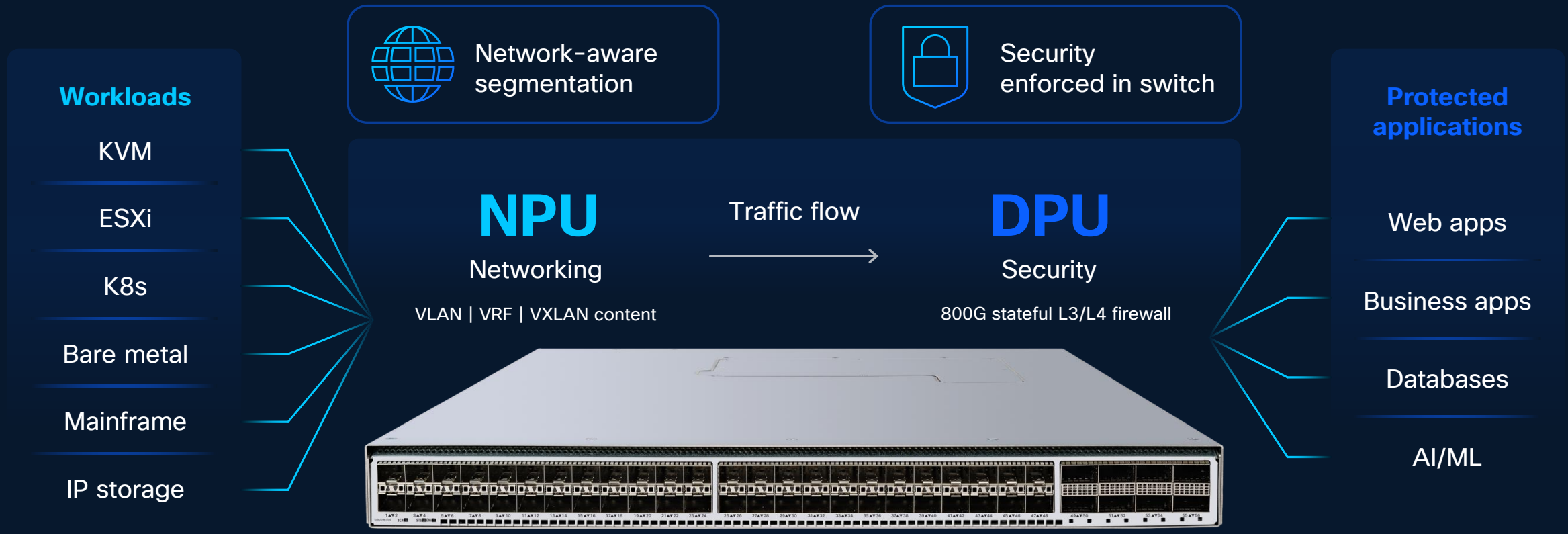
Built for DC verticals

- Enterprise
- Service provider
- AI data center
- Cloud/ managed services
- Financial services
- Public sector

Future-proof new builds and LDOS refresh for the future

Segmentation with Smart Switches

Turn every switch port into an enforcement point for every workload



Consistent segmentation across virtualized, containerized, and bare metal workloads

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

Persona-based workflow for NetOps and NetSecOps

Separate operational ownership with a shared troubleshooting workflow

NetOps

- Switch lifecycle
- Deploy network policy
- NPU telemetry

Nexus Dashboard

NX-API

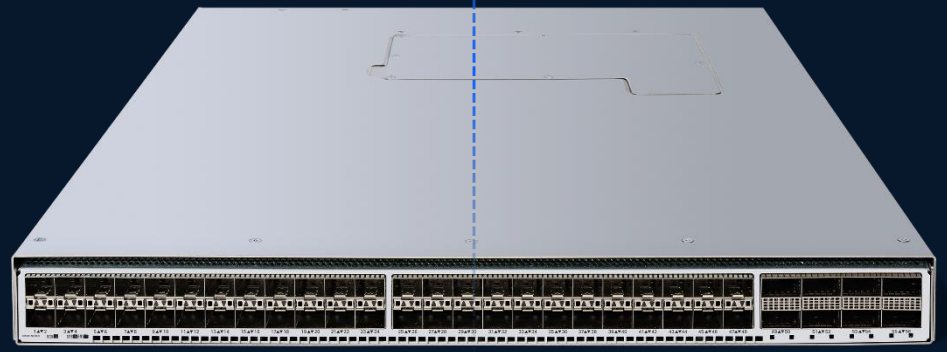
NX-CLI

NPU
Networking

Policy + telemetry
VLAN/VRF/VXLAN

DPU
Security

Security policy +
logs/telemetry



NetSecOps

- DPU security policy lifecycle
- Controller UI or API
- Security logs + telemetry

Hypershield On-prem controller

API

Shared troubleshooting workflow

1 Packet tracer

2 Context sharing

3 Root cause analysis

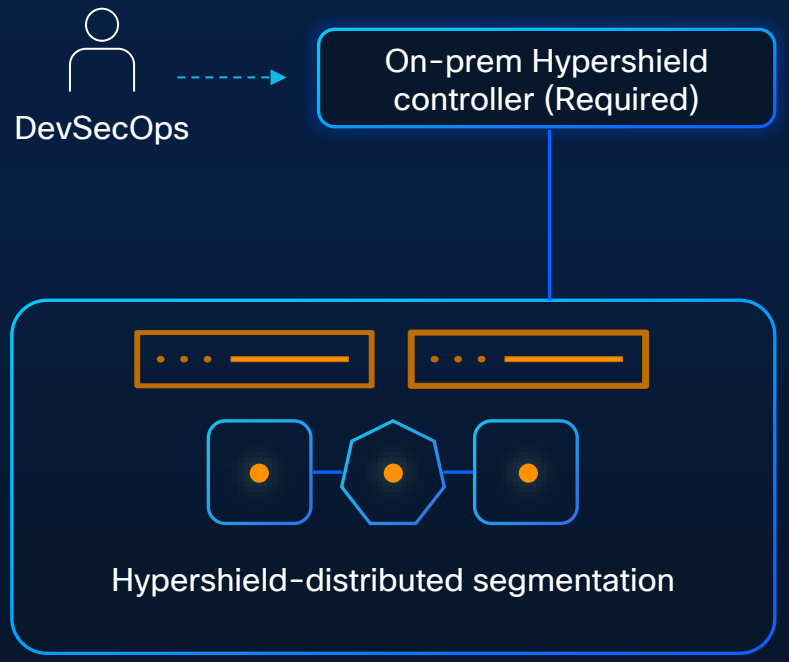
Common workflow used by NetOps and NetSecOps

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

cisco

Management flexibility

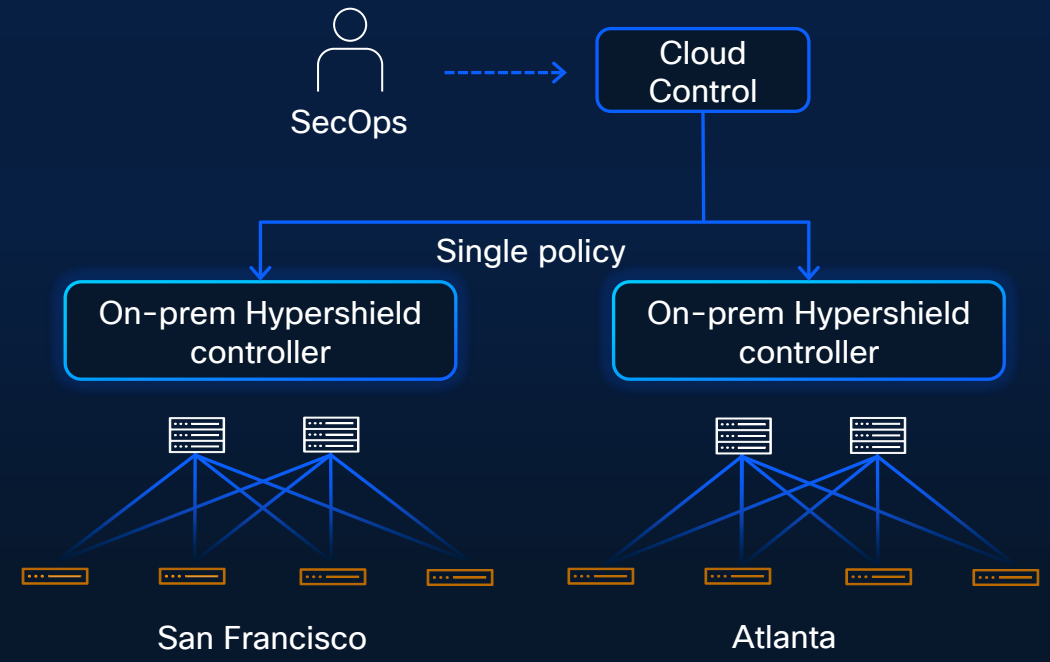
On-prem



Local control

Unified visibility and policy
across agents and Smart Switch

SaaS



Global control

Single policy across on-prem and cloud
in smart switch and workload agents

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

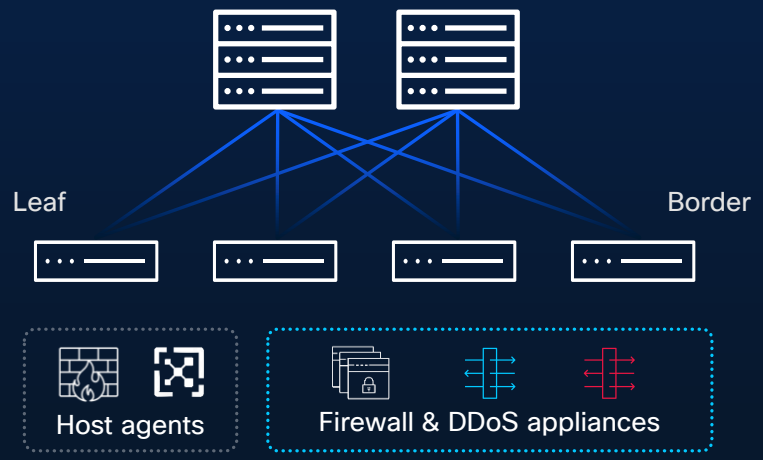
Top of rack: Distributed stateful L4 segmentation

NXOS Fabric use cases

Before

Security “attached” to network

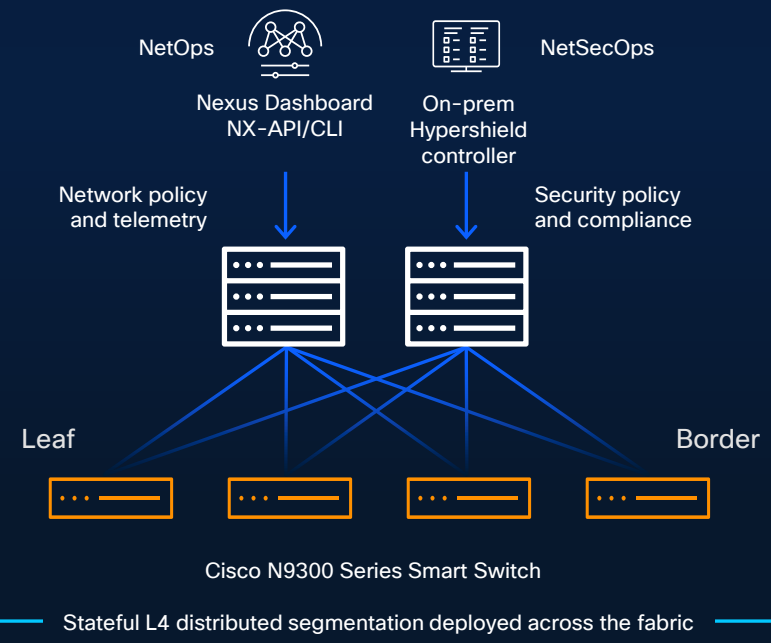
- Many security tools and dashboards
- Fragmented security policy domains
- Higher renewal cost
- Complexity -> Higher Risk



After

Smart Switch Stateful L4 Segmentation

- Lower cost and higher ROI
- 800G services throughput
- High policy scale



N9348Y2C6D-SE1U: 25G ToR
N9324C-SE1U: 100G ToR

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

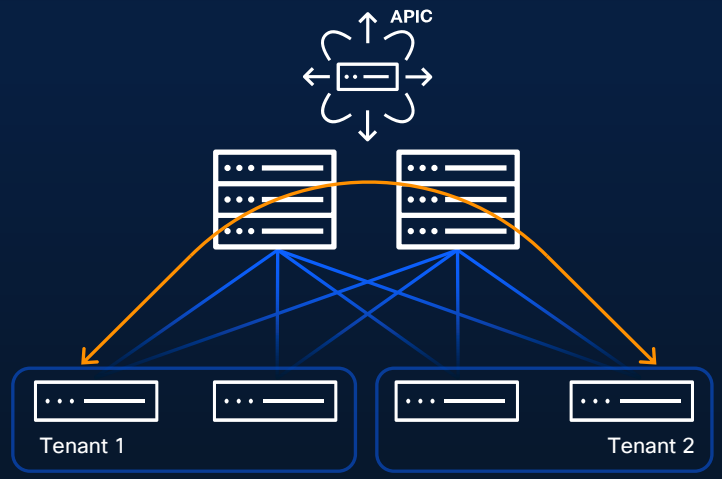
Nexus One Fabric use case

Zone segmentation with Cisco ACI

Before

ACI stateless network segmentation

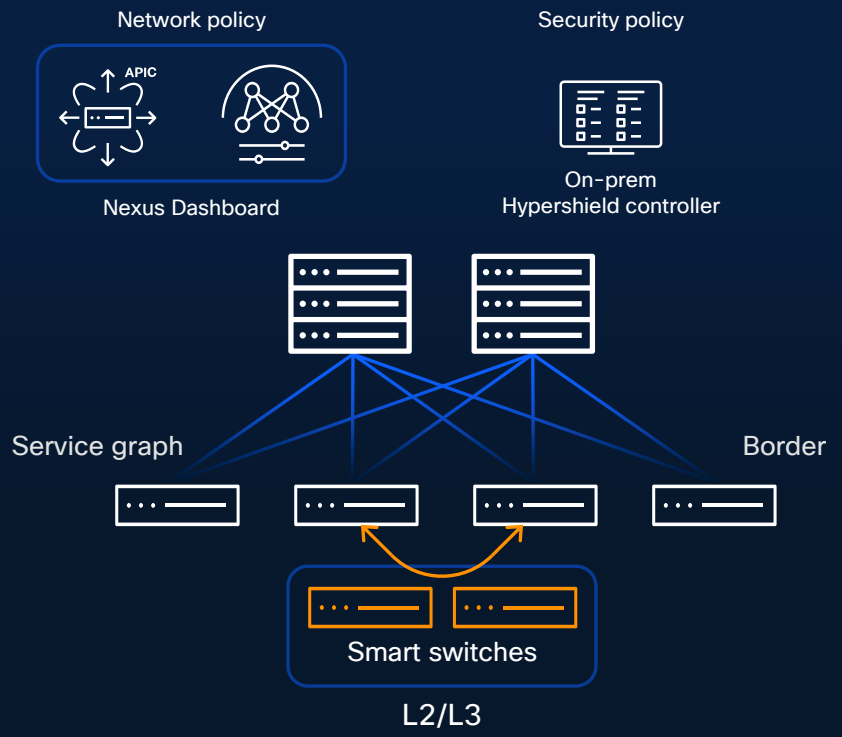
- ESG or EPG network segmentation
- Inter-tenant stateless contracts
- Limited ACL (TCAM) Resources
- Cost prohibitive firewalls at scale



After

Stateful zone firewalling for ACI fabrics

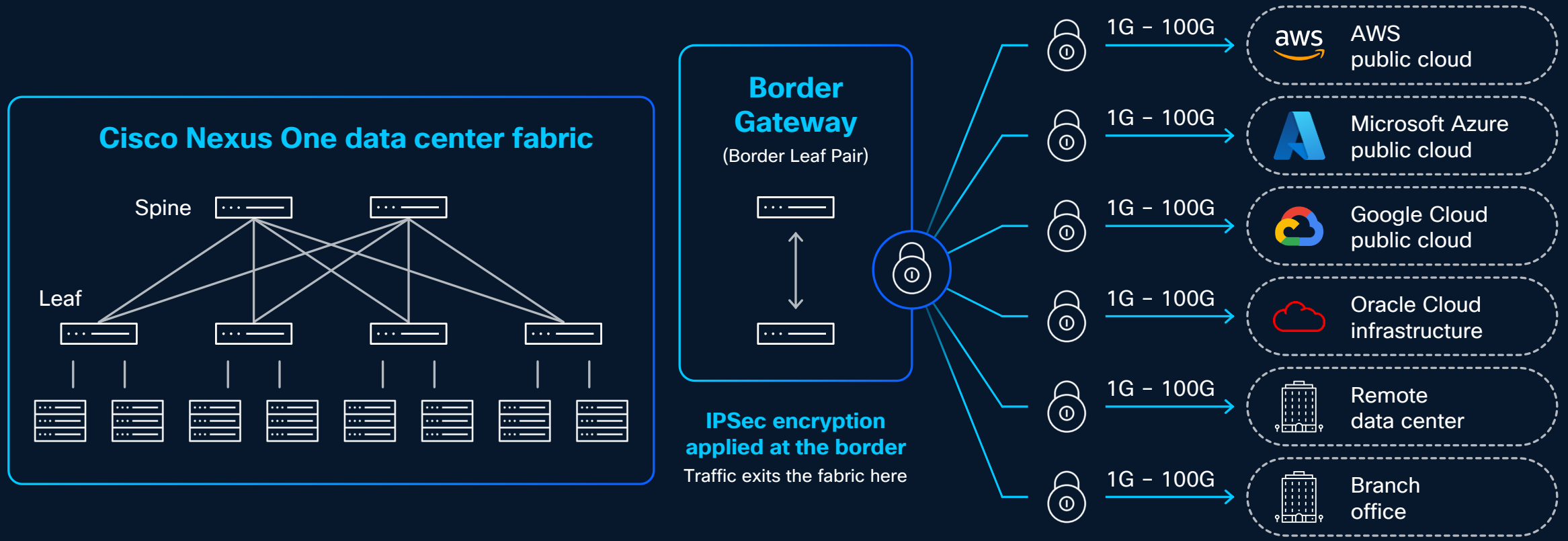
- Smart Switch as external L3/L4 firewall
- Cost effective, 800G firewalling, high scale
- Supported with ACI service graphs



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

Native IPSec encryption use case

Secure, scalable, high-performance connectivity



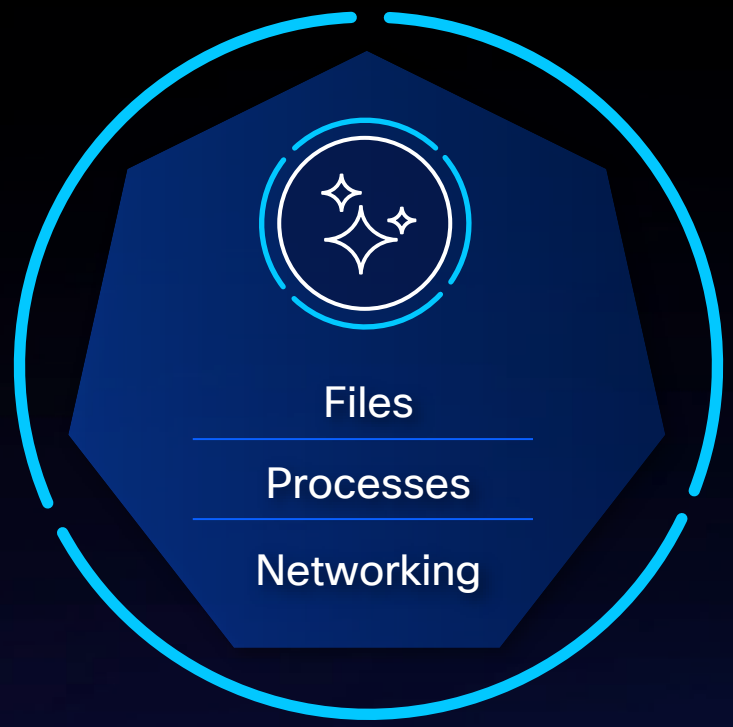
Native IPSec encryption | IKEv2 for key exchange | 1G – 100G IPSec tunnels | 1K tunnel scale | 800G IPSec capacity

Built on NX-OS | Smart Switches and E100 platforms

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

cisco

AI runs on Kubernetes



Segmentation

- Process hiding
- Credential harvesting
- Privilege escalation
- Container escape
- Kernel exploit
- File tampering
- Sidecar injection
- Shell injection
- Network scanning
- Reverse shell

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

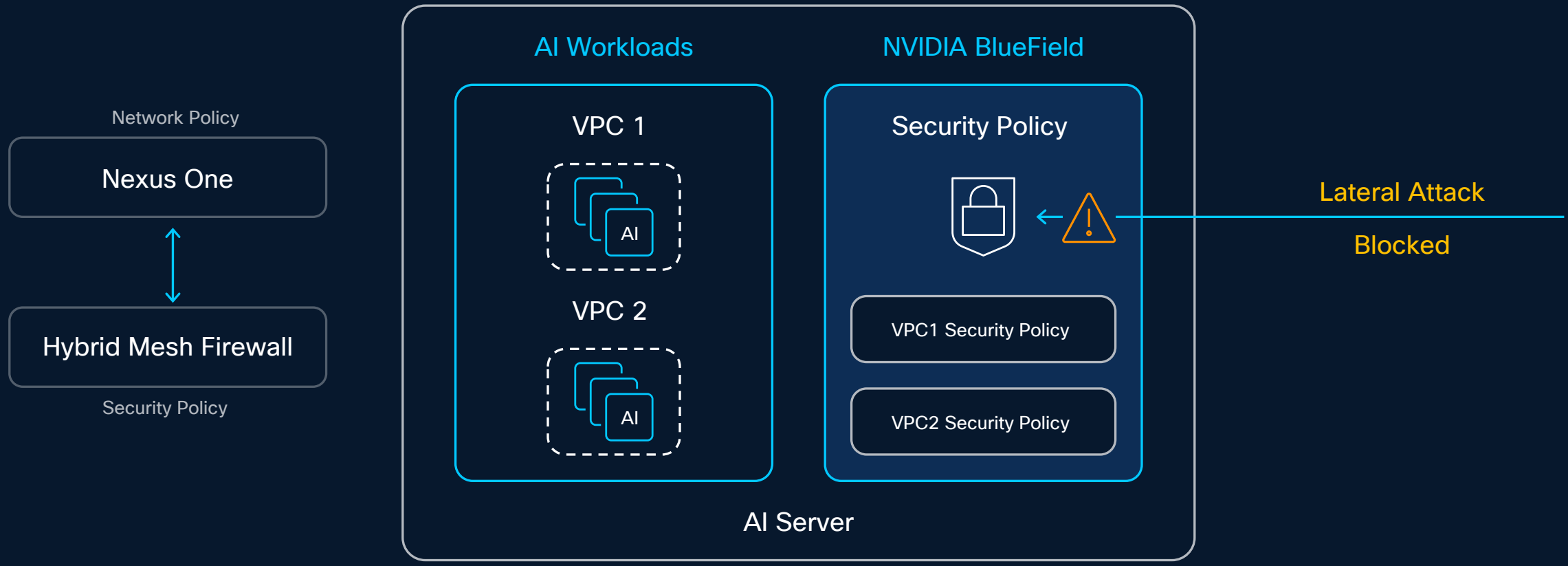
Segmentation is no longer optional



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.

cisco

Protection

Secure Firewall 6100: near-limitless scale for AI readiness



Cisco Secure Firewall 6100 series

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

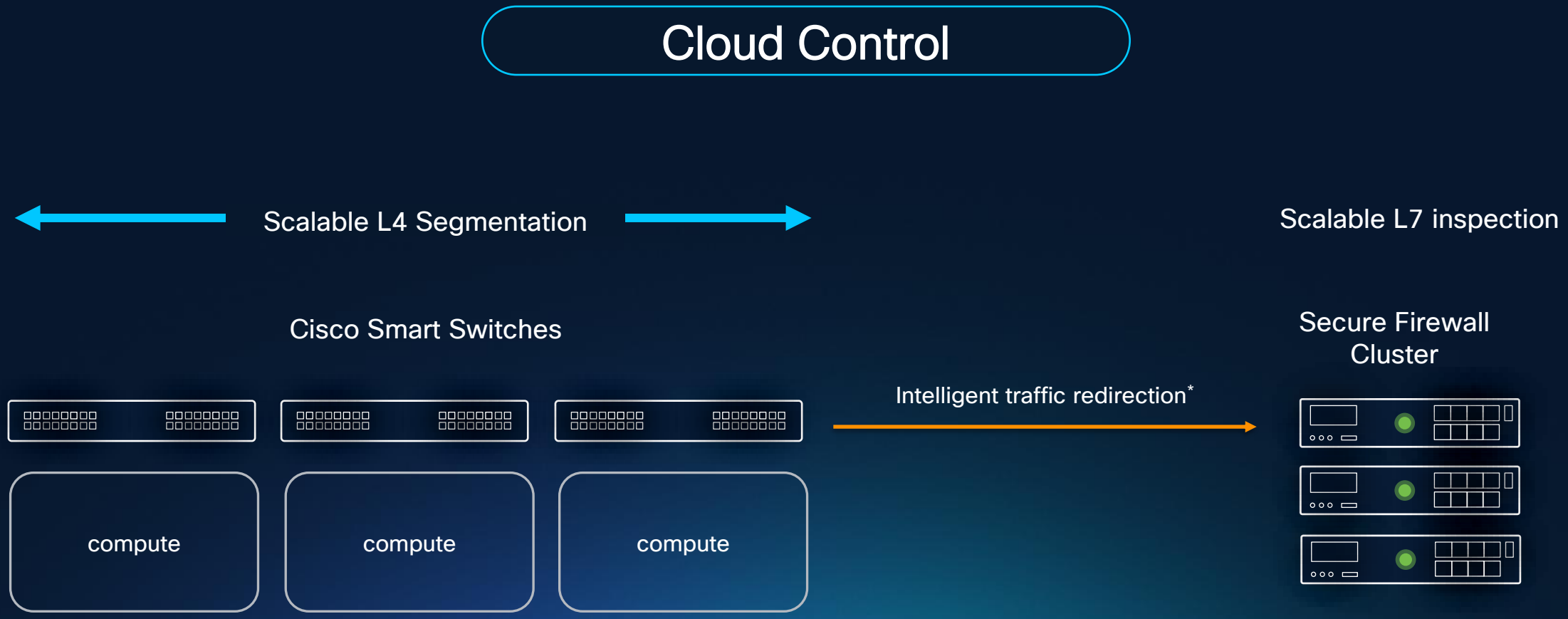
Changes math per protected Gbps: 80% less space, 60% less power, 1/3 the cost

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

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

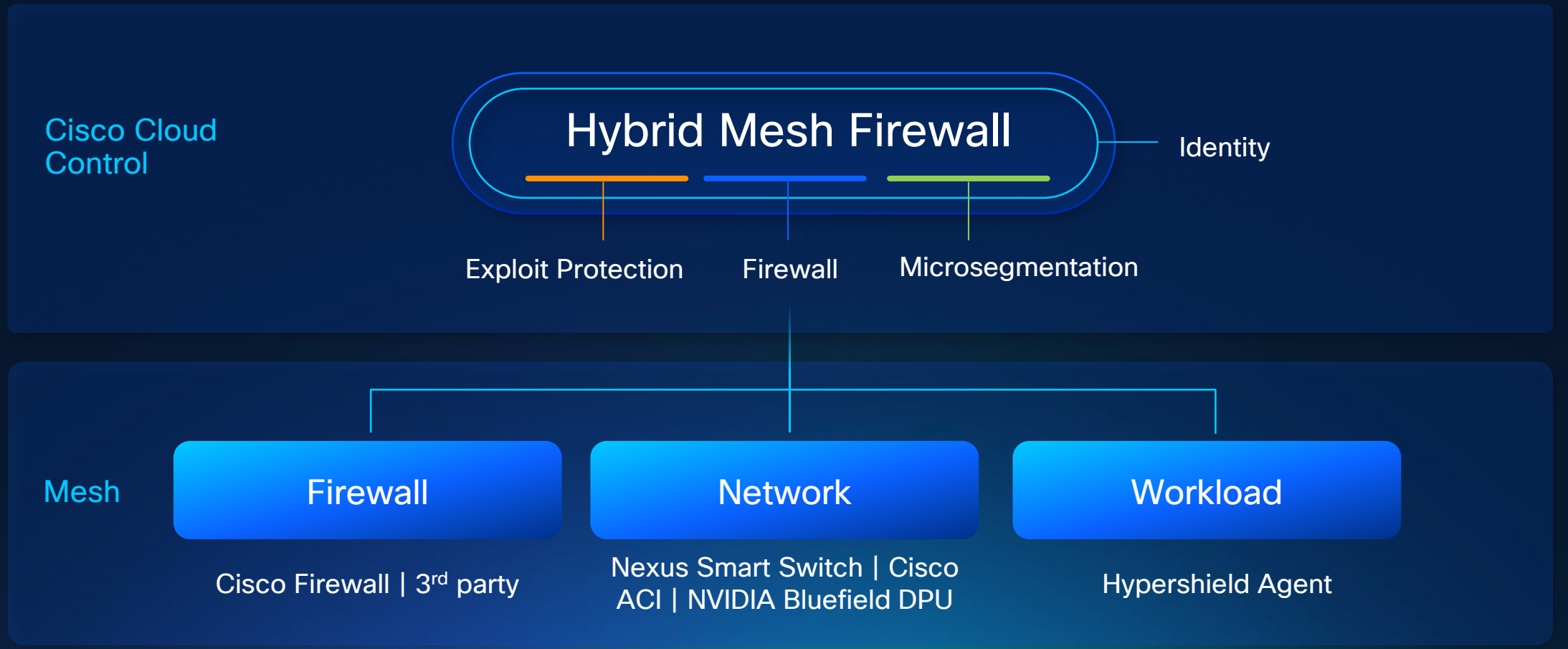
cisco

Scalable security with Smart Switch + Secure Firewall



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

Protecting your apps and infrastructure, including AI



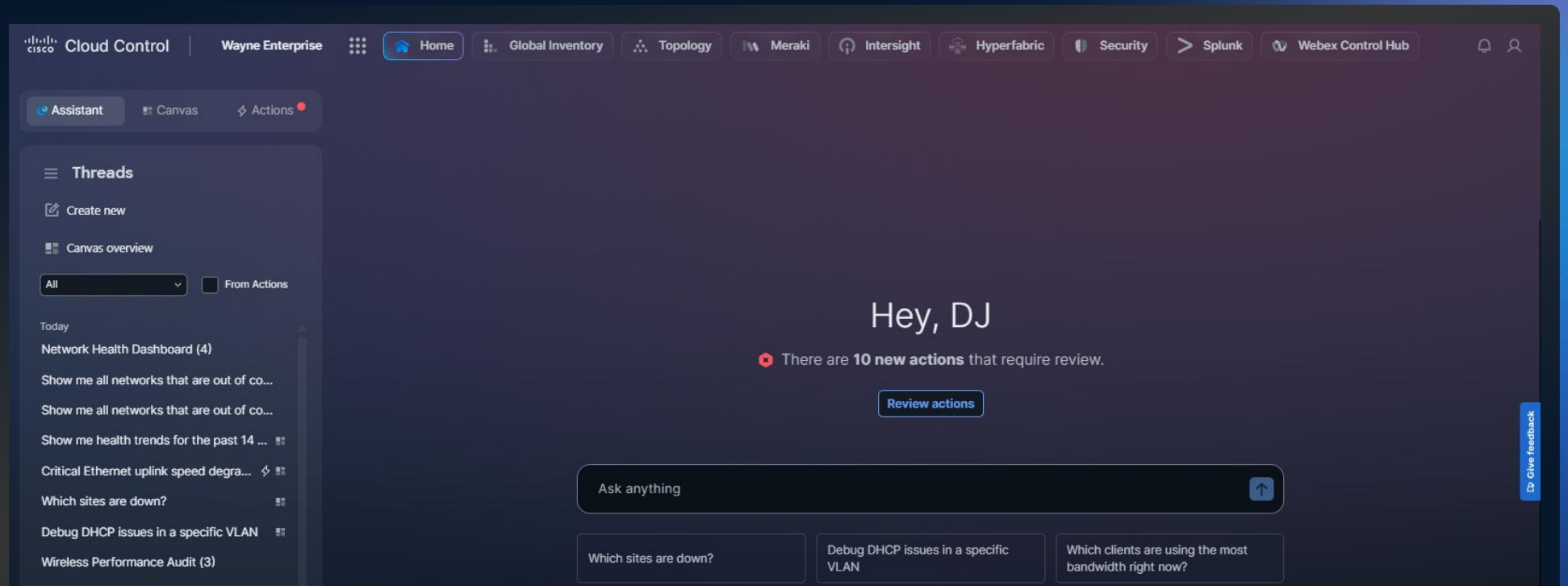
© 2026 Cisco and/or its affiliates. All rights reserved.

Visibility and Insights

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

Unified operations with Cisco Nexus One

FULLY INTEGRATED STACK

Nexus Dashboard

On premises

Nexus Hyperfabric

Cloud management

SILICON	SYSTEMS	OPTICS	SOFTWARE
Cisco Silicon One Cisco Cloud Scale NVIDIA Spectrum-X Ethernet	Cisco N9000 Systems	Cisco Optics	Cisco NX-OS Cisco ACI, SONiC

SECURITY AND OBSERVABILITY

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

Why now?

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.

cisco

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



Nexus One: unified management plane

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

cisco

CISCO Connect

Thank you




CISCO