Next Gen Security Smart Switches for the AI Data Center

Pin Han Wong

Cisco Security Architect APAC - Hypershield

15 July 2026

Agenda

01 Why Smart Switches

02 Smart Switch Overview

03 Use Cases

04 What is Beyond Smart Switch – Hypershield Security

05 Live Protect

06 Closing

Why Smart Switches?

Attacker's Advantage: A Growing Threat

130+ disclosed vulnerabilities / day

+16% increase YoY

30% weaponized within 24h

Faster than patching can be done

70% attacks use lateral movement

$5M global average breach cost

The Defense Mismatch

Centralized firewall architecture creates blind spots

60-day patch cycle leave persistent exposure

Yesterday's **approach to security** must now **fundamentally** *change*

Sources: Morphisec 2025, Elisity 2025, IBM Cost of Breach 2024, Edgescan 2024, Cisco Talos - July 2025, Safran Security 2026

Top Priorities from Our Customers

Stop lateral movement

Reduce the patching gap

Protect data and workloads

Simplify Operations

SECURE AI DATA CENTERS

Fuse Security Into Networking

1. Traditional Data Center Security Limitations
2. Turn every switch port into an enforcement point
3. Continuous Runtime Defense

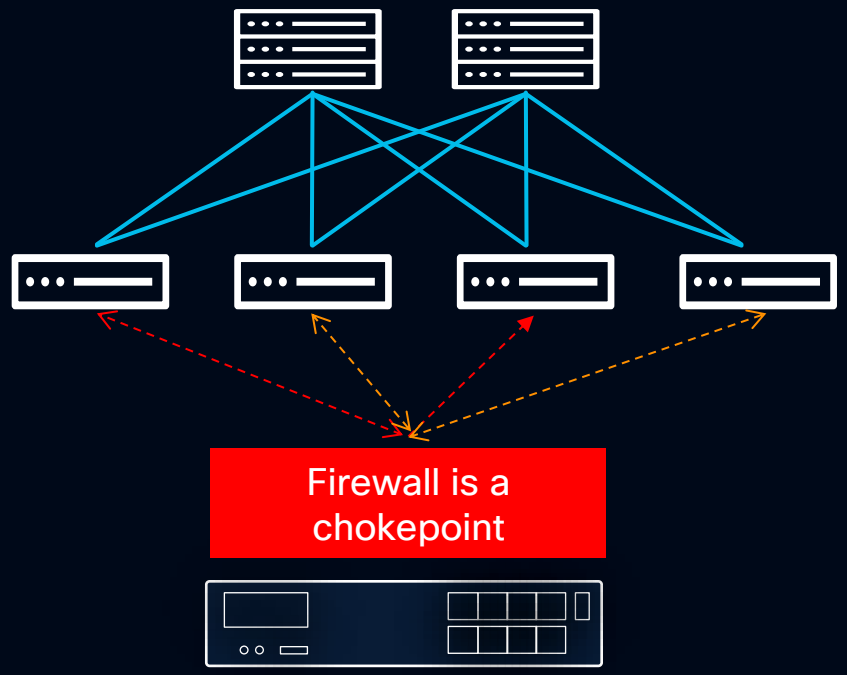
SECURE DATA CENTERS

Fuse Security Into Networking

1 Traditional Data Center Security Limitations

2 Turn every switch port into an enforcement point

3 Continuous Runtime Defense



↑ Latency ↑ Cost ↑ Complexity

Secure Data Center

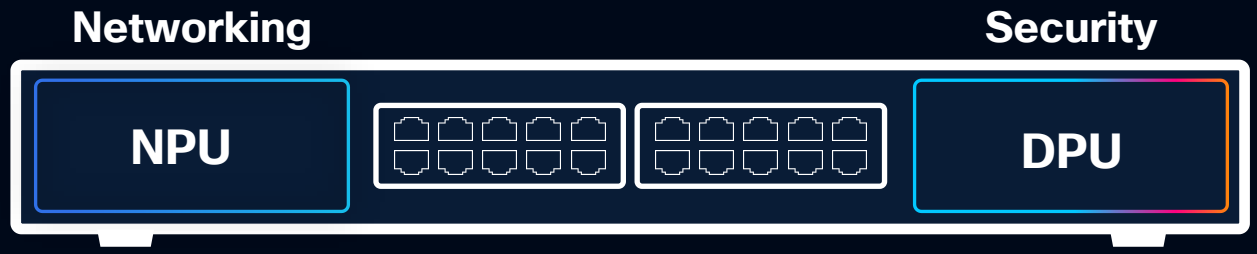
Fuse Security Into Networking

1 Build an AI-Ready Enterprise Fabric

2 Turn every switch port into an enforcement point

3 Continuous Runtime Defense

Cisco Nexus Smart Switches with Hypershield security



Eliminate External Firewall chokepoints

Security & Switching in One

800G Security Services with DPU

Unified network & security visibility

Secure Data Center

Fuse Security Into Networking

1 Build an AI-Ready Enterprise Fabric

2 Turn every switch port into an enforcement point

3 Continuous Runtime Defense

Vulnerability shielding for Cisco Nexus

No PSIRT patching or OS upgrade

No downtime or switch reboot

Continuous re-validation

Smart Switch Overview

Cisco Nexus 9300 Series Smart Switches

N9348Y2C6D-SE1U

48-port 25G, 6-port 400G, 2-port 100G, 800G, 2 DPU services

Shipping

N9324C-SE1U

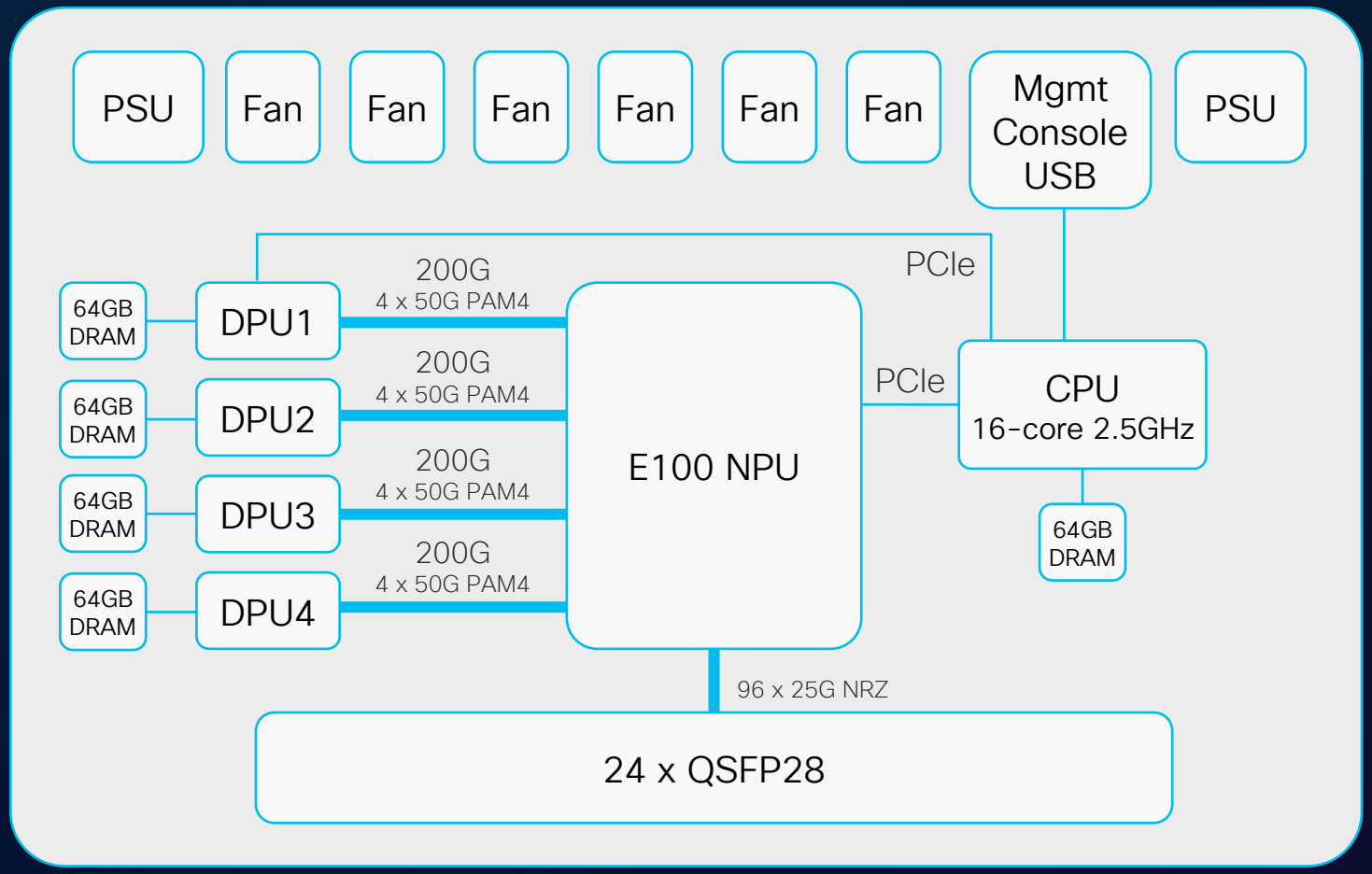
24-port 100G, 800G, 4 DPU services

Shipping

Security Use Cases

- Top of Rack segmentation & enforcement
- Zone-based segmentation
- Cloud Edge

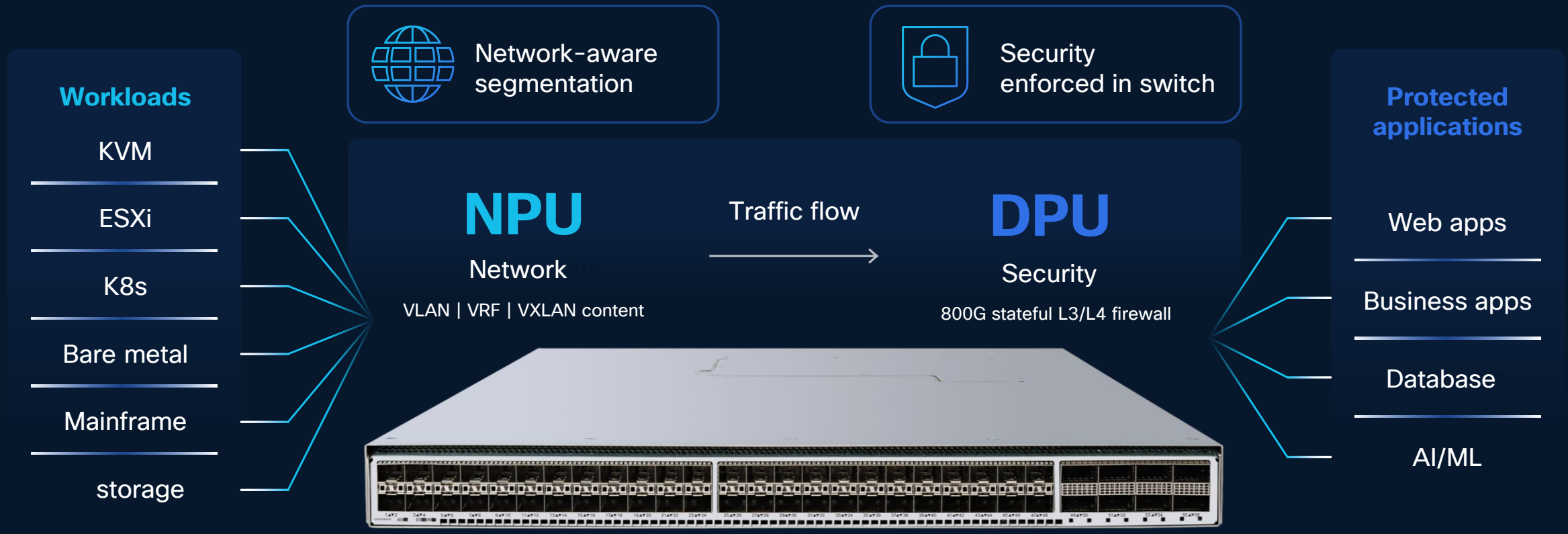
Smart Switch 4 DPU Architecture



N9324C-SE1U
"Dansberg"

Segmentation with Smart Switches

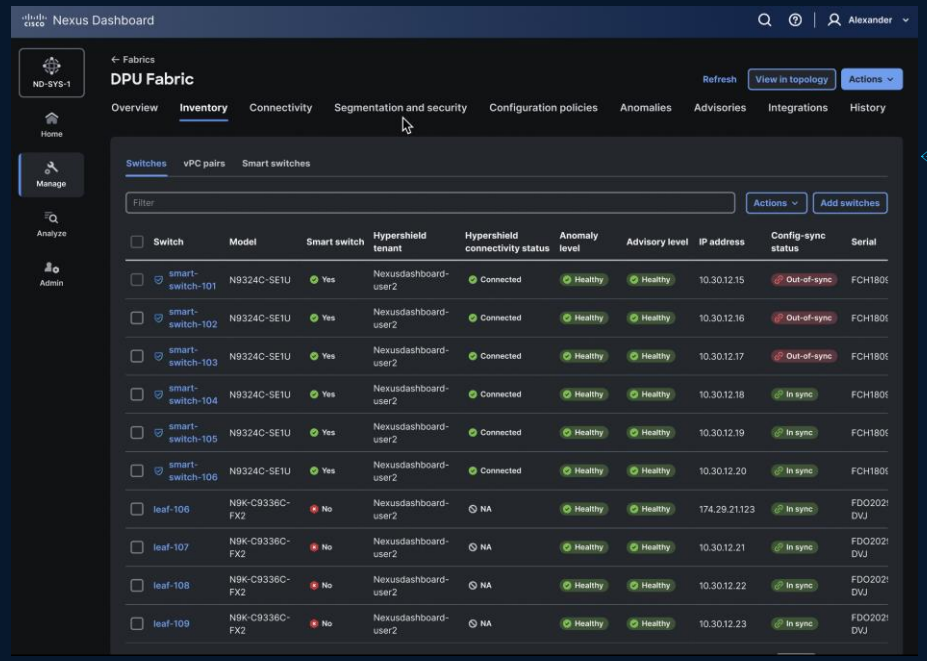
Turn every switch port into an enforcement point for every workload



Consistent segmentation across virtualized, containerized, and bare metal workloads

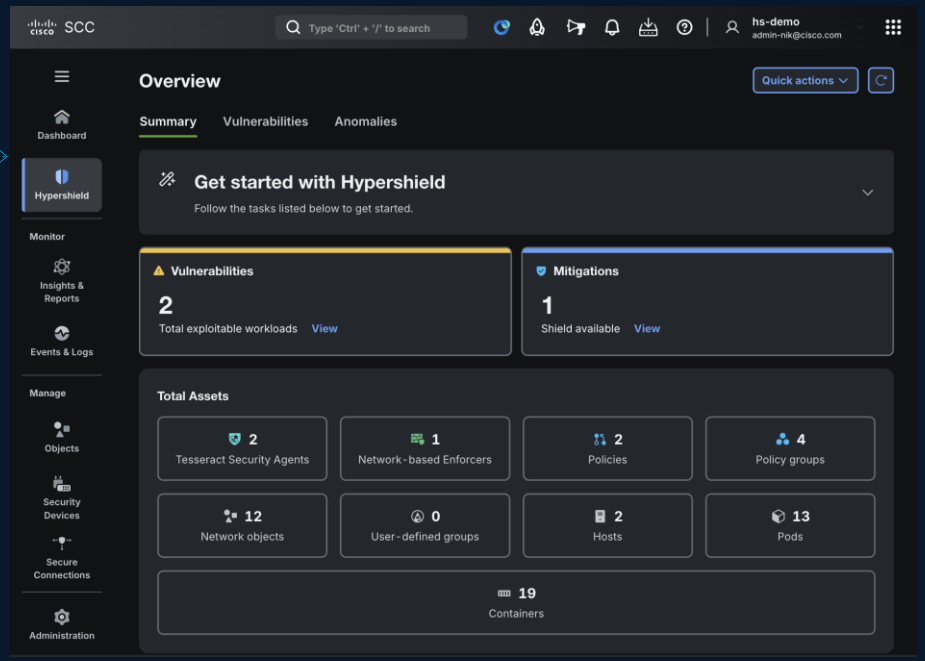
Separate Workflows for NetOps and NetSecOps

Nexus Dashboard, NX-API, NX-CLI



Context sharing for troubleshooting

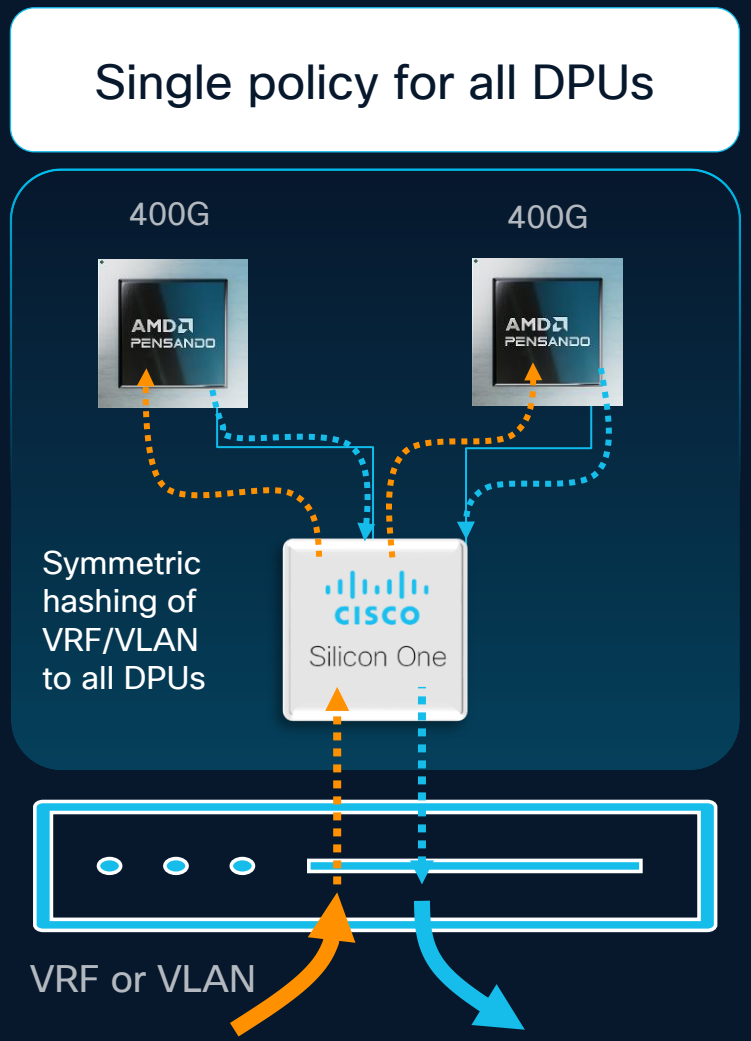
Hypershield On Prem Controller

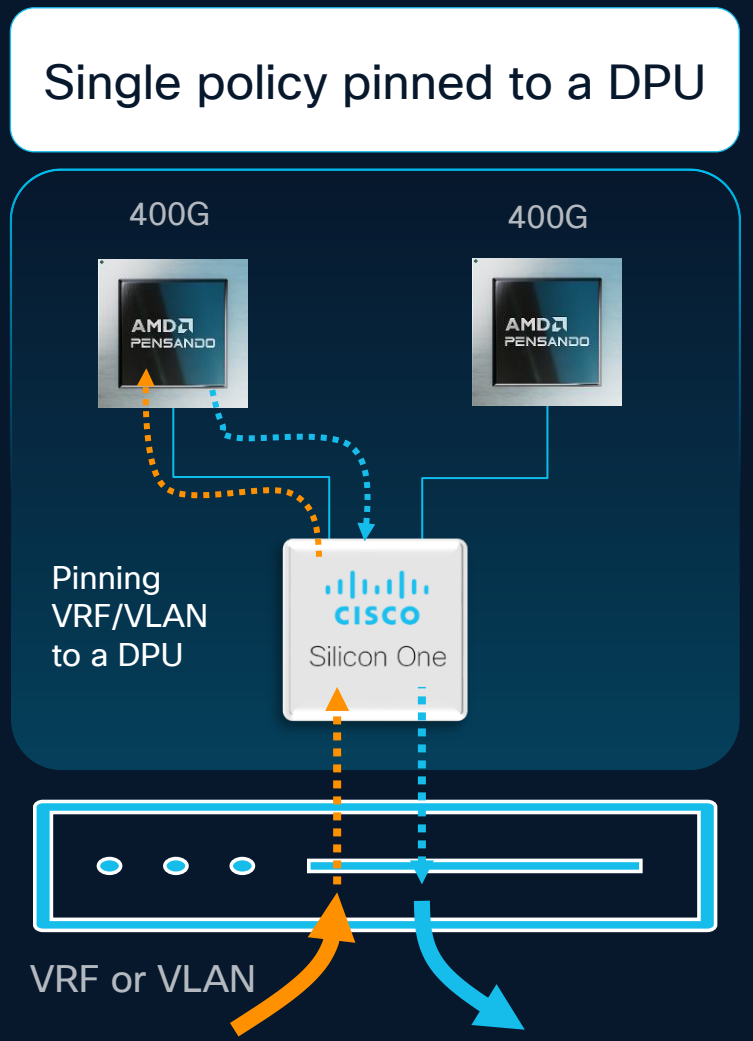


NEXUS SMART SWITCH

Flexible Policy Enforcement

Enforce policy at Smart Switch or DPU level



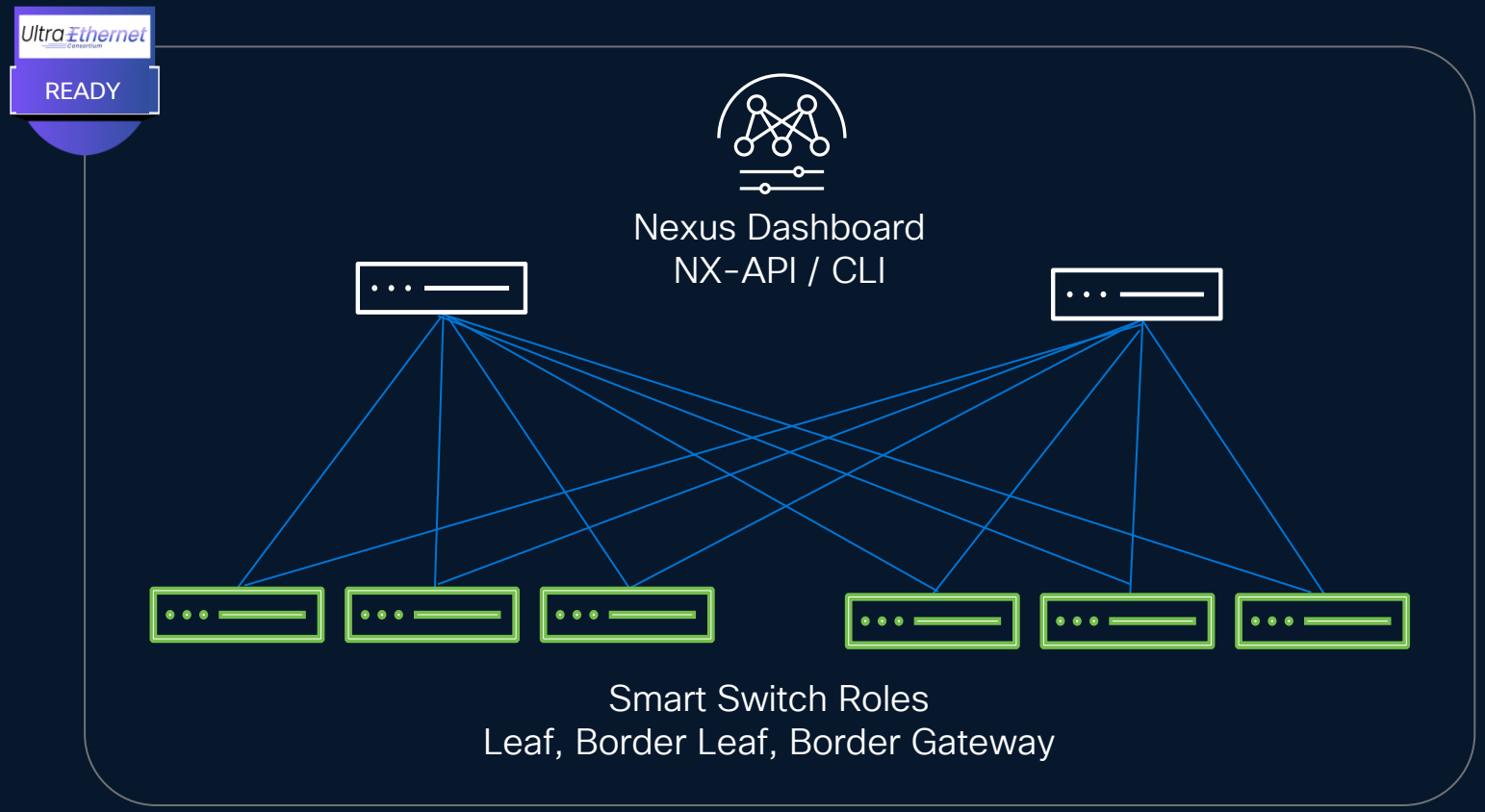


Use Cases

Top of Rack: Network Mode Use Case

Available Now

Ideal for New NXOS Fabrics and NXOS EOL Refresh



Network Use Cases

- VXLAN-EVPN Fabric
- Multi-Site VXLAN-EVPN Fabric
- BGP routed Fabric
- Classic LAN

Note: In Network Mode, DPUs are powered down in Smart Switch.

EOL Refresh

Brownfield Insertion

Future Ready with Security

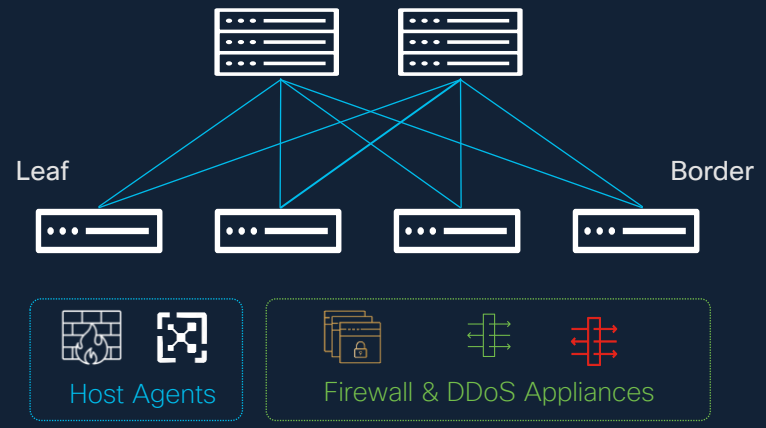
Top of Rack: Stateful L4 Segmentation

NXOS Fabric Use Cases

Currently under Controlled Availability –GA in Aug 2026

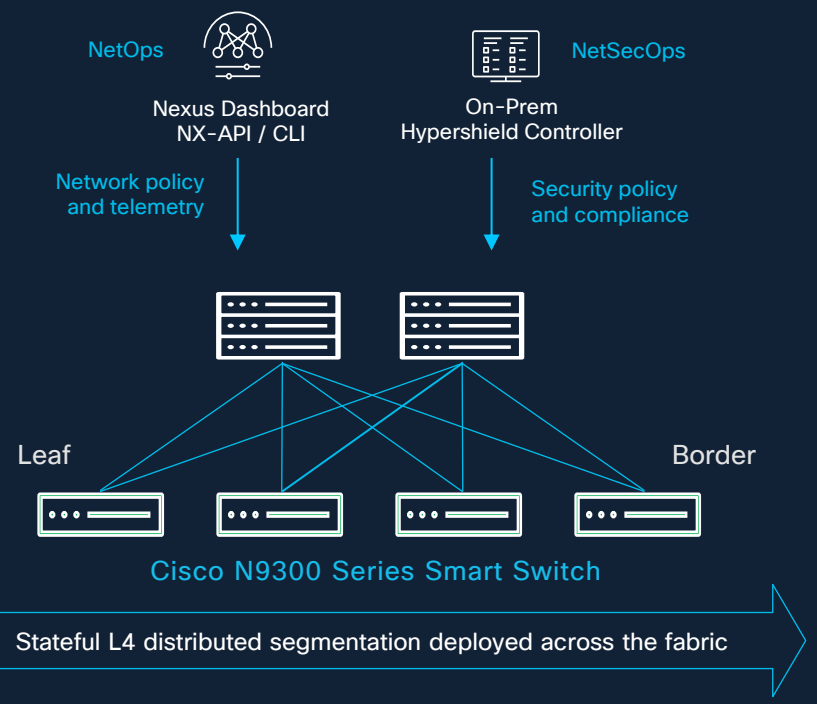
Security "Attached" to Network

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



Smart Switch Stateful L4 Segmentation

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



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

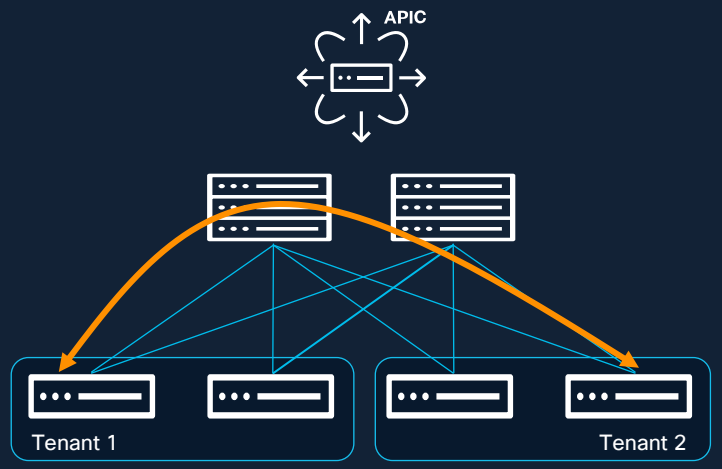
ACI Fabric Use Case

Zone Segmentation

Currently under Controlled Availability

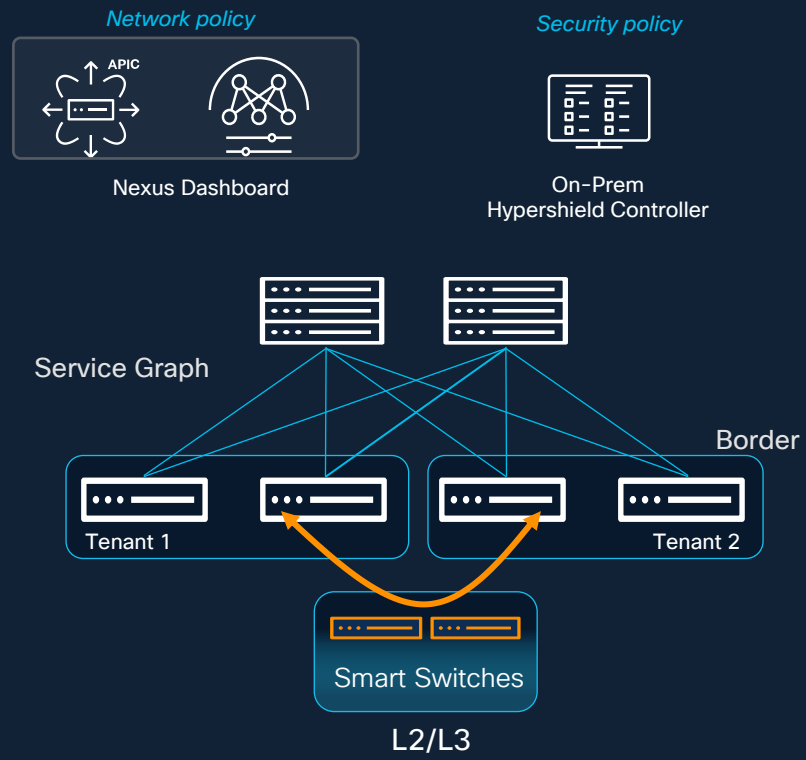
ACI Stateless Network Segmentation

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



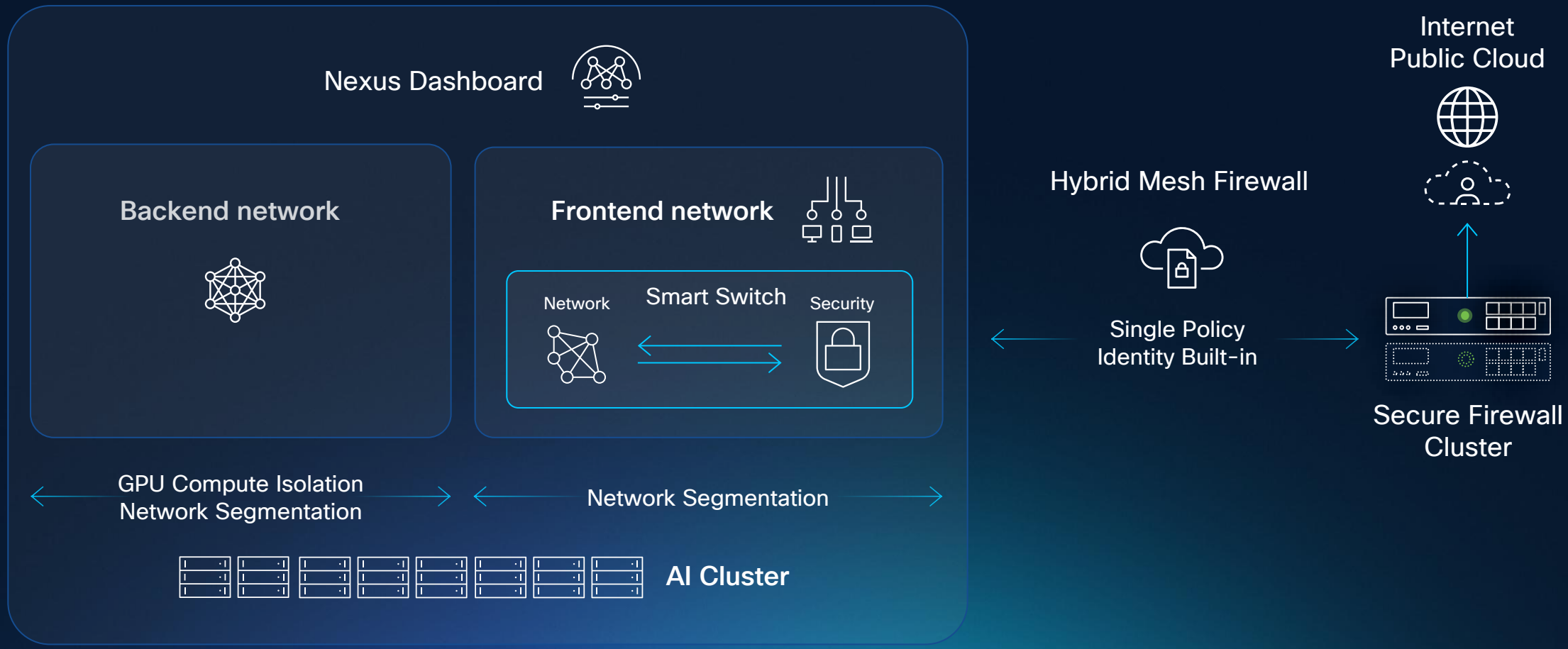
Stateful Zone Firewalling for ACI fabrics

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



Secure Your AI Fabrics

Committed



What is Beyond Smart Switch – Hypershield Security

Hybrid Mesh Firewall

Write Policy Once, Enforce Across the Mesh

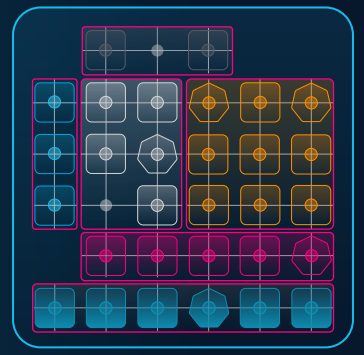
Cisco Cloud Control
(SaaS)

Mesh Policy Engine | Hypershield | Hybrid Mesh Firewall

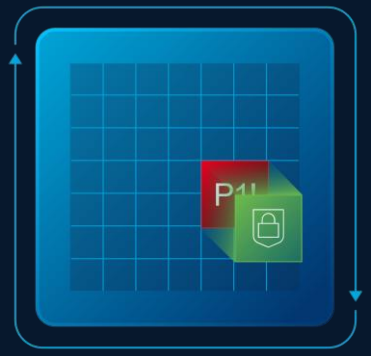
Datacenter | Private Cloud | VMs | Public Cloud | Kubernetes

Cisco Hypershield

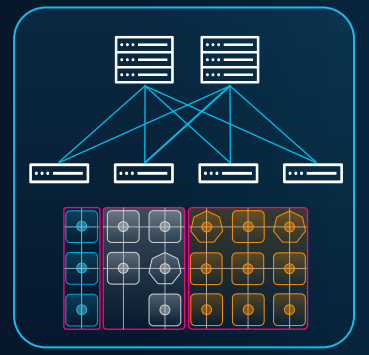
Fusing Security into the Network



End-to-End Visibility



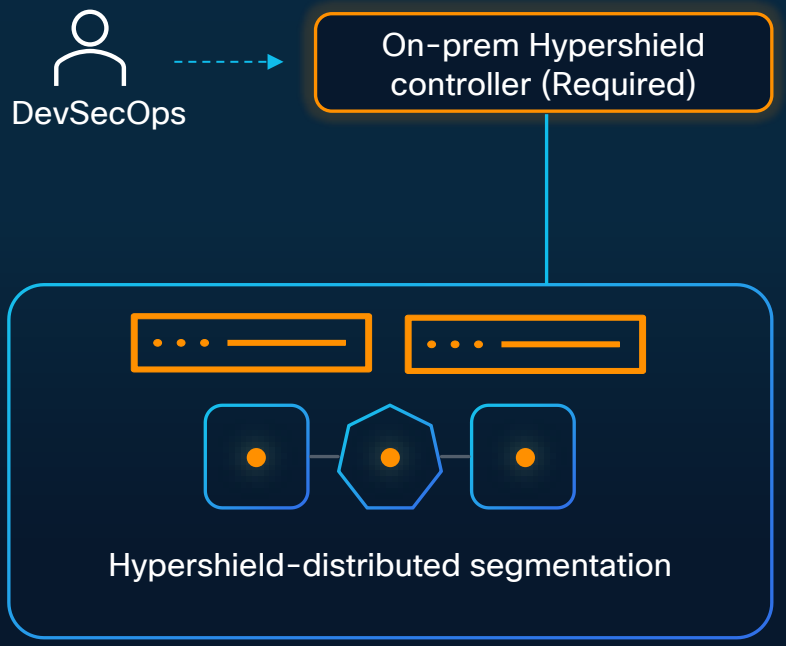
Policy Deployment



Distributed Segmentation

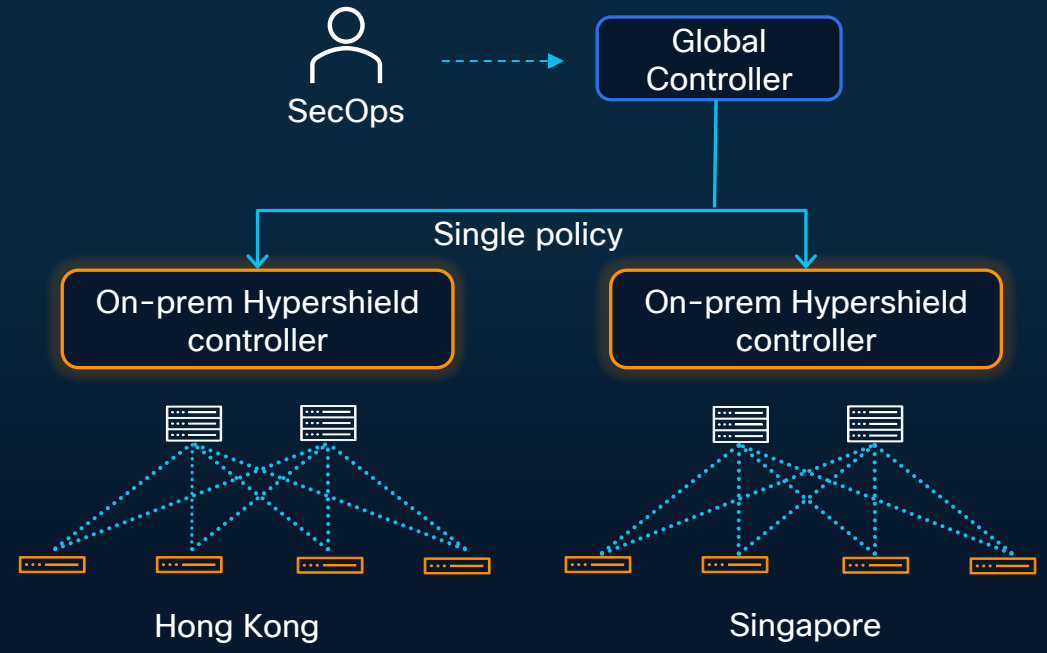
Hypershield Management Smart Switch

On-Prem



Local control

Unified visibility and policy across agents and Smart Switch



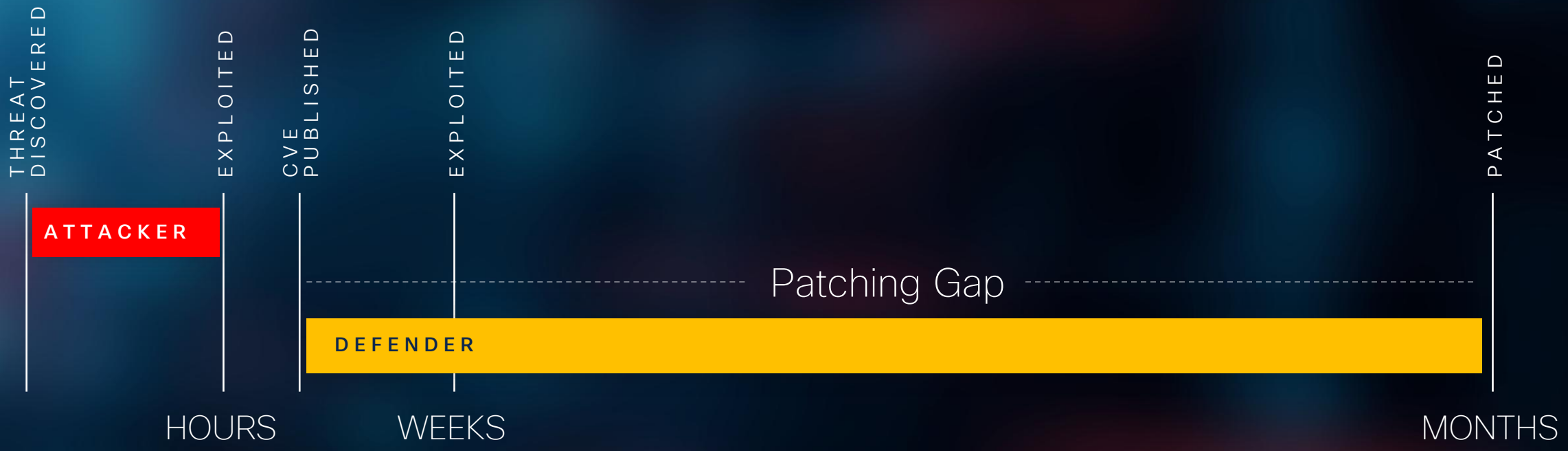
Global control*

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

*Roadmap

Live Protect

Patching Vulnerabilities is Challenging



Live Protect

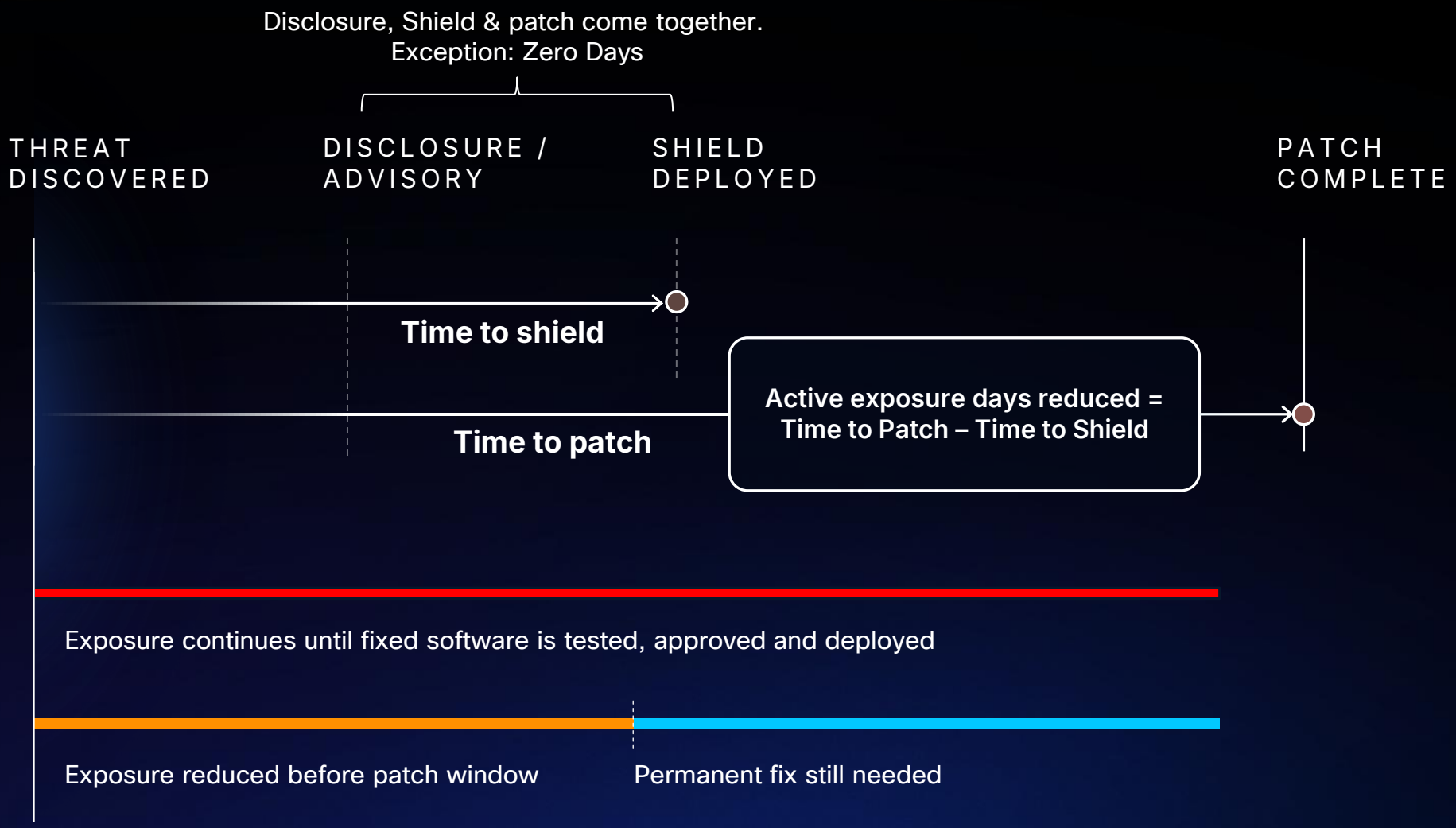
Vulnerability shielding for Cisco networking devices

Stop the attack... but don't stop the network.

Apply policy to live system | No PSIRT patching or upgrade | No downtime or switch reboot | Continuous re-validation

Live Protect closes the exposure gap, not the patching process

Cisco-validated Vulnerability Shields reduce exposure while teams complete the permanent software fix



Cisco validates each Shield before operators deploy it

Live Protect is not a DIY runtime rule. Vulnerability Shields are initiated and validated through Cisco's security and product process.

1	2	3	4	5
PSIRT advisory intake	Talos exploit analysis & shield design	Shield testing (Cisco & 3rd party)	Disclosure, Shield & patch release	Operators stage & deploy (Nexus BD)

What Cisco validates

- Shield feasibility & exploit-relevant targeting
- Normal behavior preserved
- Supported platforms, releases, modes, and limits
- Retirement path after fixed software

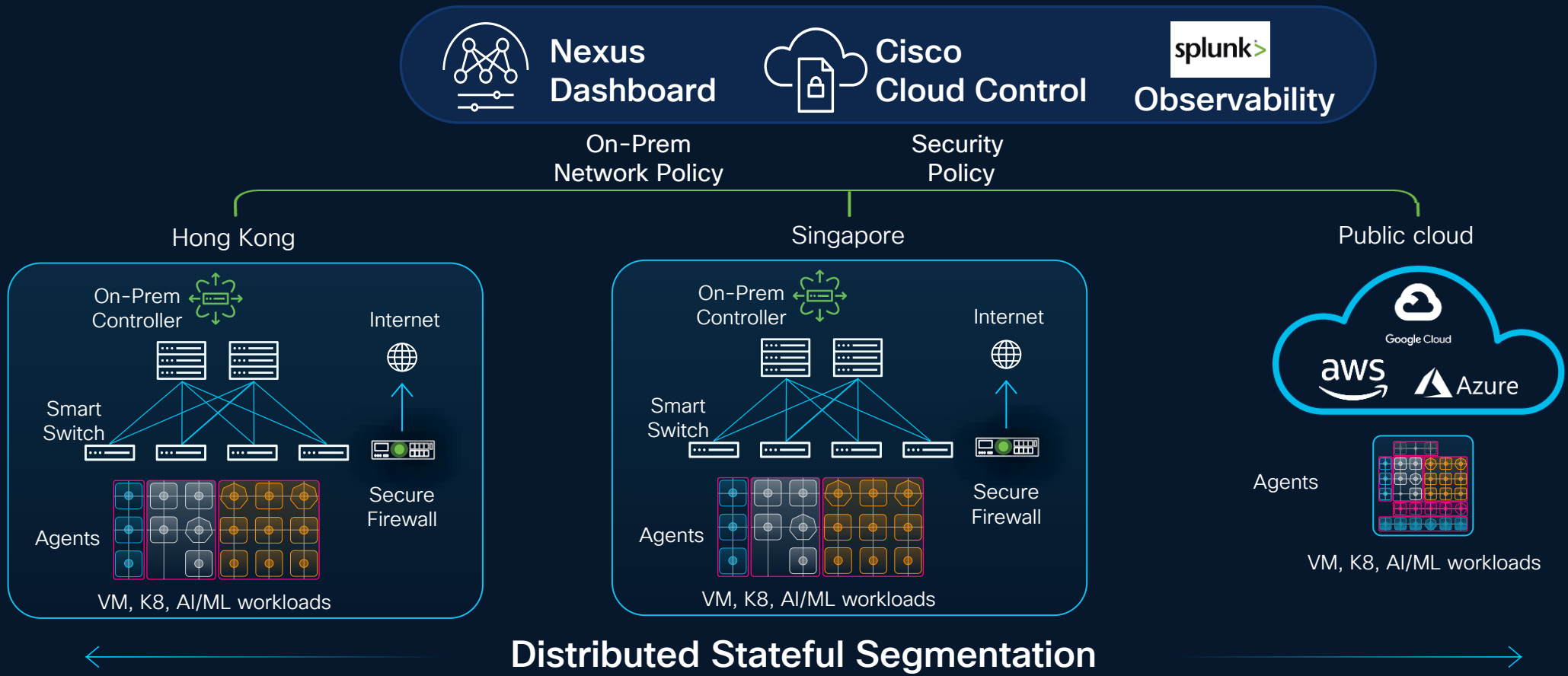
What operators get

- Cisco-provided, Cisco-validated protection
- Less customer burden for custom control design, testing, support, and retirement

Closing

Security infused in Data Center and Cloud

Unified Policy across Smart Switch, Workload & Perimeter



Global or air-gapped management

Unified Policy Enforcement
Smart switch, workload, perimeter

800G security with large scale

Always On high availability

Full visibility from data center to cloud


CISCO