Secure, Intelligent Networking for Modern Data Centers

Mika Meritähti
Cloud and AI Solutions Engineer
Cisco Finland and Baltics

Legal Disclaimer

Any information provided in this document regarding future functionalities is for informational purposes only and is subject to change including ceasing any further development of such functionality. Many of these future functionalities remain in varying stages of development and will be offered on a when-and-if-available basis, and Cisco makes no commitment to the final delivery of any of such future functionalities. Cisco will have no liability for Cisco's failure to deliver any or all future functionalities and any such failure would not in any way imply the right to return any previously purchased Cisco products.

The Security Challenge

Customer Challenges

Mounting pressure to rethink DC architecture for the AI era

Complexity

More service-specific devices and multipoint solutions increase complexity

Prone to errors

Modernization

Business growth demands cost-effective scalable network services

Security

Policy management and enforcement challenges

Risks with changes/updates

Point Solutions Hinder Implementing Holistic Zero Trust

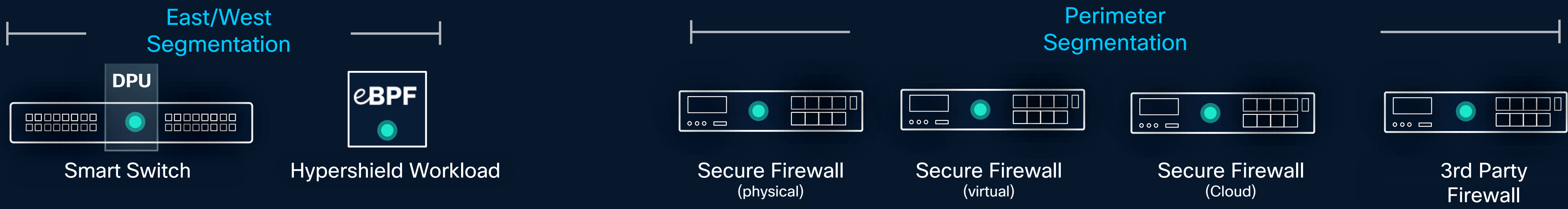
Incomplete Security Posture | Impacting Application Performance | Visibility & Enforcement Blind-Spots

Cisco Hypershield

Cisco Hybrid Mesh Firewall

Broader and deeper

SECURITY CLOUD CONTROL



Only Cisco Fuses Security Into Both the Network & Workload

"Cisco's Boxes managed as one"

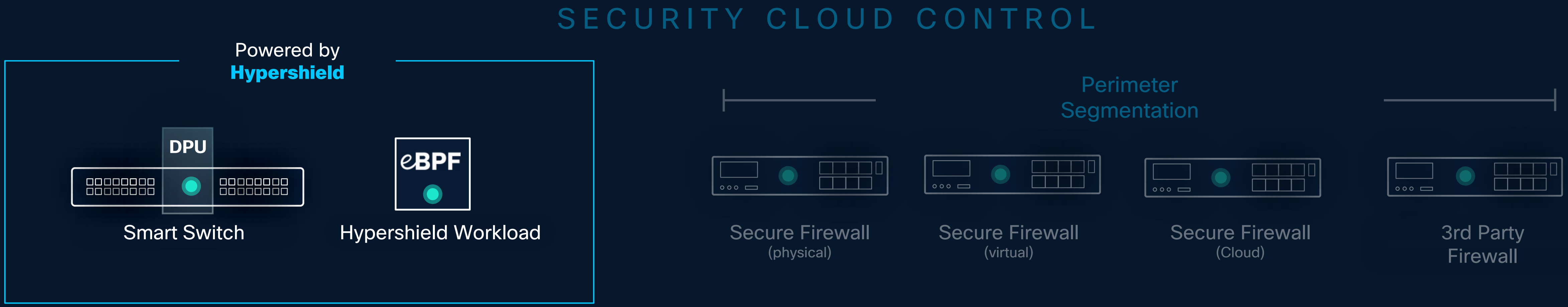
Cisco also manages 3rd-Party Firewalls

Smart Switches work in Cisco's Hybrid Mesh Firewall solution for customers that still want advanced firewall features implemented in the network along with Smart Switches (e.g L7 AppID, IDS/IPS, URL Filtering, SSL Decryption)

Write policy once, enforce across the mesh

Cisco Hybrid Mesh Firewall

Broader and deeper



Only Cisco Fuses Security Into Both the Network & Workload

"Cisco's Boxes managed as one"

Cisco also manages 3rd-Party Firewalls

Smart Switches work in Cisco's Hybrid Mesh Firewall solution for customers that still want advanced firewall features implemented in the network along with Smart Switches (e.g L7 AppID, IDS/IPS, URL Filtering, SSL Decryption)

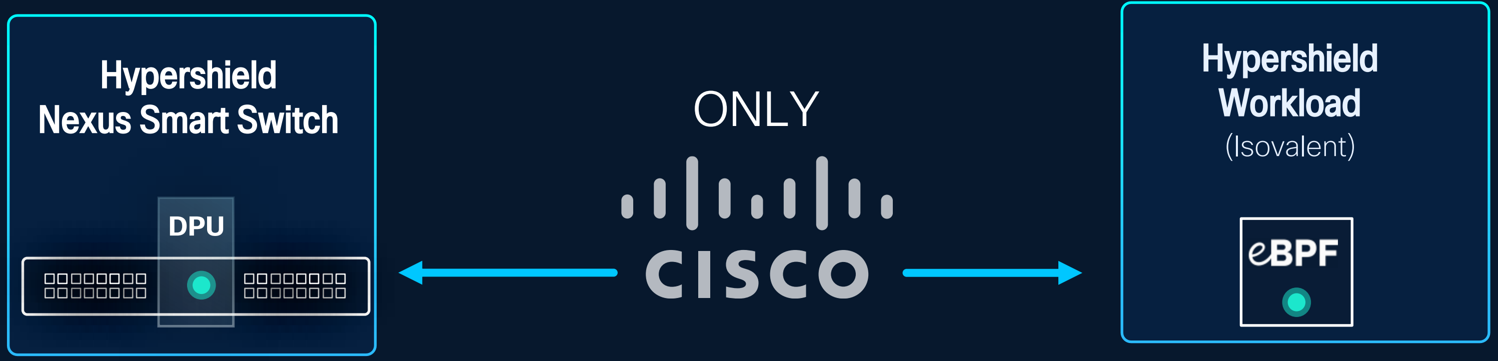
Write policy once, enforce across the mesh

Cisco Hypershield

Cisco's Key Network Security Differentiator

Hypershield fuses security into....

the Network & the Workload



Hypershield Nexus Smart Switch

DPU

ONLY

Hypershield Workload

(Isovalent)

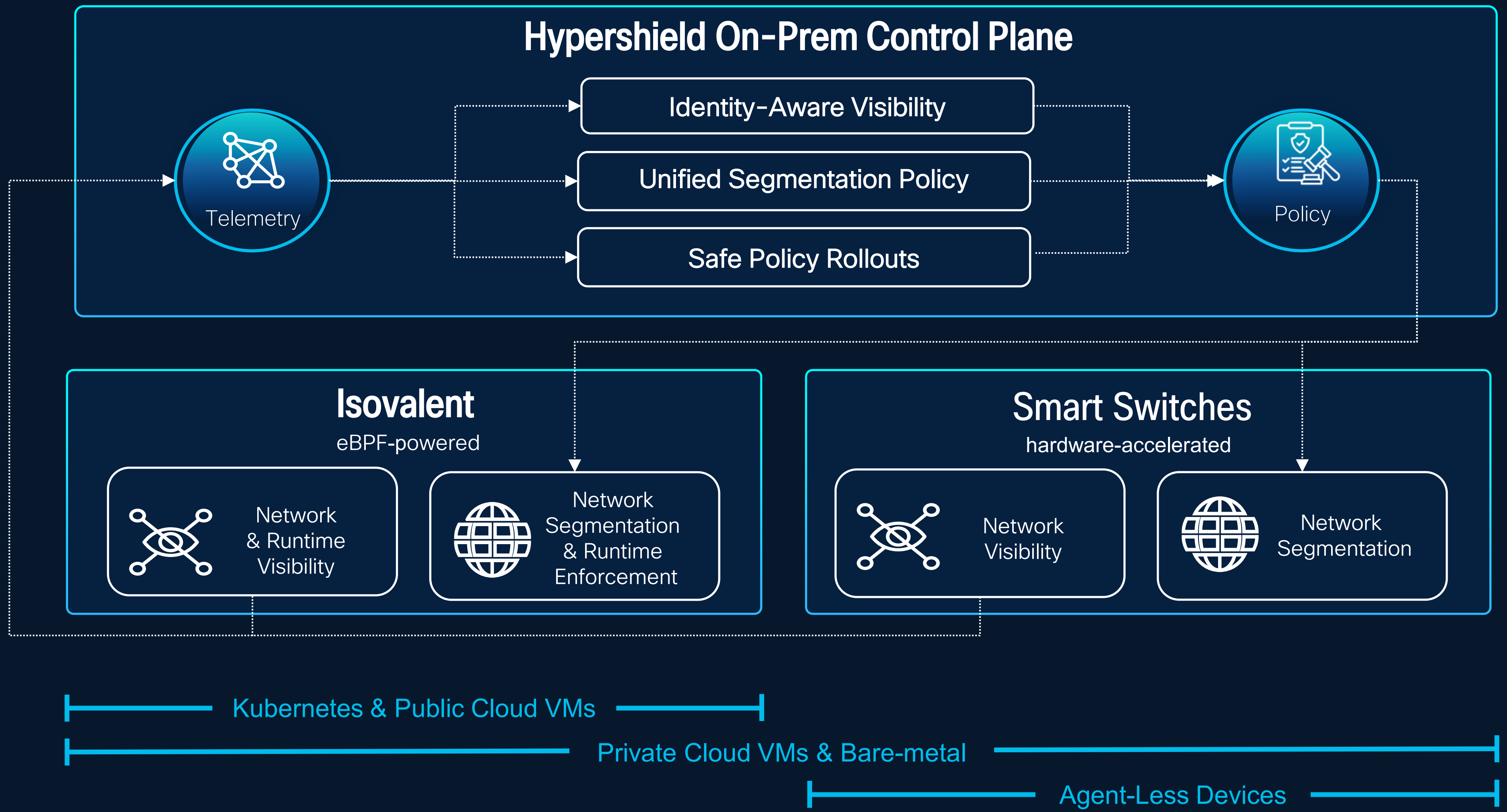
eBPF

Eliminates east/west security blind spots in the datacenter with no changes to application workloads

Adds deep application awareness and extends east/west security to the public cloud and Kubernetes

Hypershield

Architecture Overview



Hypershield On-Prem Control Plane

Telemetry

Identity-Aware Visibility

Unified Segmentation Policy

Safe Policy Rollouts

Policy

Isovalent

eBPF-powered

Network & Runtime Visibility

Network Segmentation & Runtime Enforcement

Smart Switches

hardware-accelerated

Network Visibility

Network Segmentation

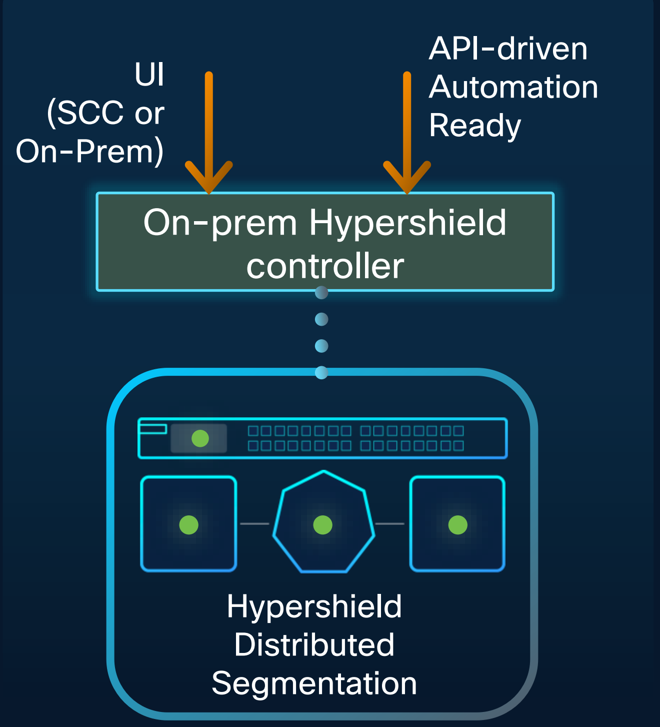
Kubernetes & Public Cloud VMs

Private Cloud VMs & Bare-metal

Agent-Less Devices

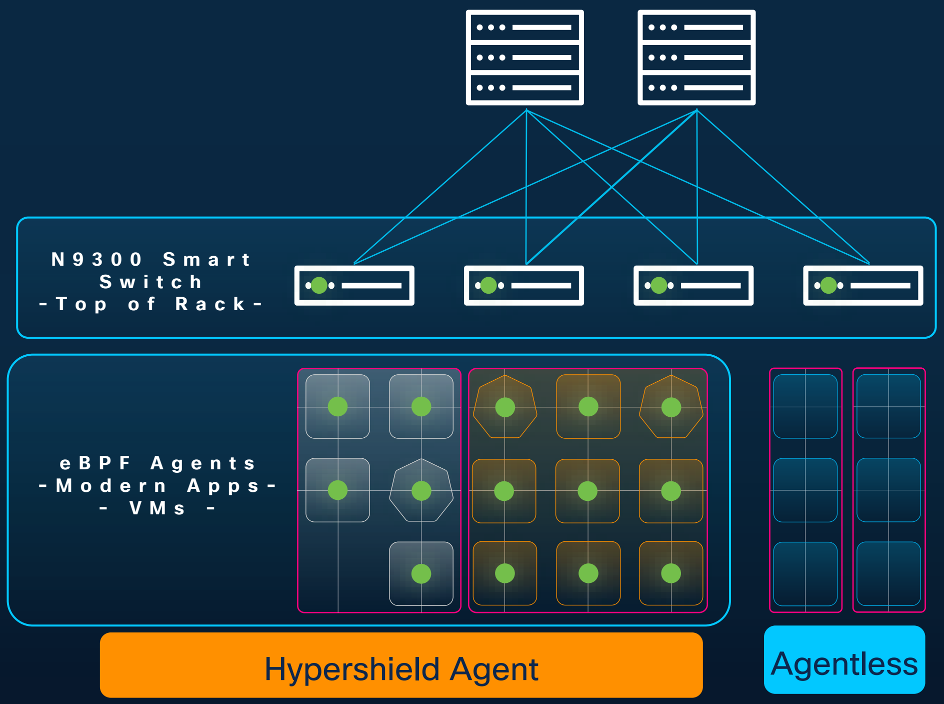
Cisco Hypershield

Distributed Segmentation Architecture



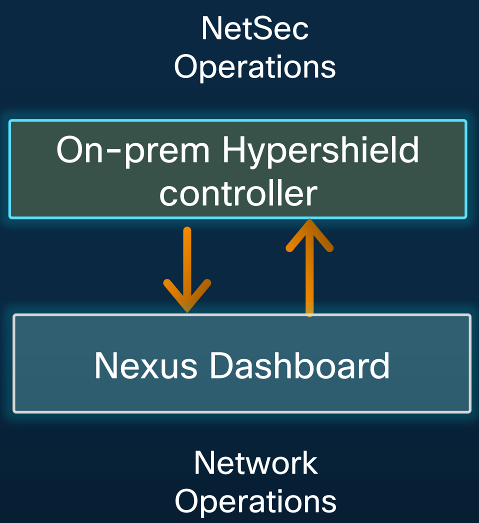
Global Control

Unified visibility and global policy across agents and smart switch



Distributed

Eliminate blind spots with fully distributed enforcement
– Inline everywhere, kernel and network fabric -



Unified operations

Separation of control with combined operations and troubleshooting

Cisco Nexus Smart Switches

Nexus Smart Switch

Unmatched Flexibility, Performance, and Efficiency

Cisco N9300 Smart Switches

Networking

cisco Silicon One

- Rich NX-OS Features and Services
- High-speed connectivity and scalable performance
- Optimized for latency and power efficiency

Routing Switching

EVPN/MPLS/ VXLAN/SR

Rich Telemetry

Line-rate Encryption

Power Efficiency

Hypershield

- Software-defined Stateful Services
- Programmable at all layers: add new services without HW change
- Scale-out services with wire-rate performance
- Power down DPU complex when not used

Distributed Security

IPSEC Encryption

Large-Scale NAT

Event-Based Telemetry

DoS Protection

Future Use Cases

Cisco Smart Switches Integrated with Hypershield Security

UltraEthernet Consortium

Cisco N9300 Series Smart Switches

Shipping

N9324C-SE1U

24-port 100G

800G Services Throughput

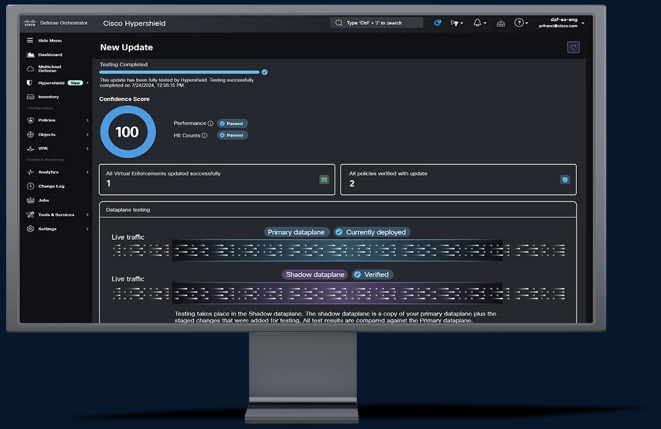
Orderable

N9348Y2C6D-SE1U

48-port 1G/10G/25G, 6-port 400G, 2-port 100G

800G Services Throughput

Cisco Hypershield



New Update

Testing Completed

This update has been fully tested by Hypershield. Testing successfully completed on 7/24/2024, 12:56:15 PM.

Confidence Score

100

Performance: Passed

Hit Counts: Passed

All Virtual Enforcements updated successfully 1

All policies verified with update 2

Dataplane testing

Live traffic — Primary dataplane — Currently deployed

Live traffic — Shadow dataplane — Verified

Testing takes place in the Shadow dataplane. The shadow dataplane is a copy of your primary dataplane plus the staged changes that were added for testing. All test results are compared against the Primary dataplane.

Use Cases

Top of Rack segmentation and enforcement

Nov 2025

Cloud Edge

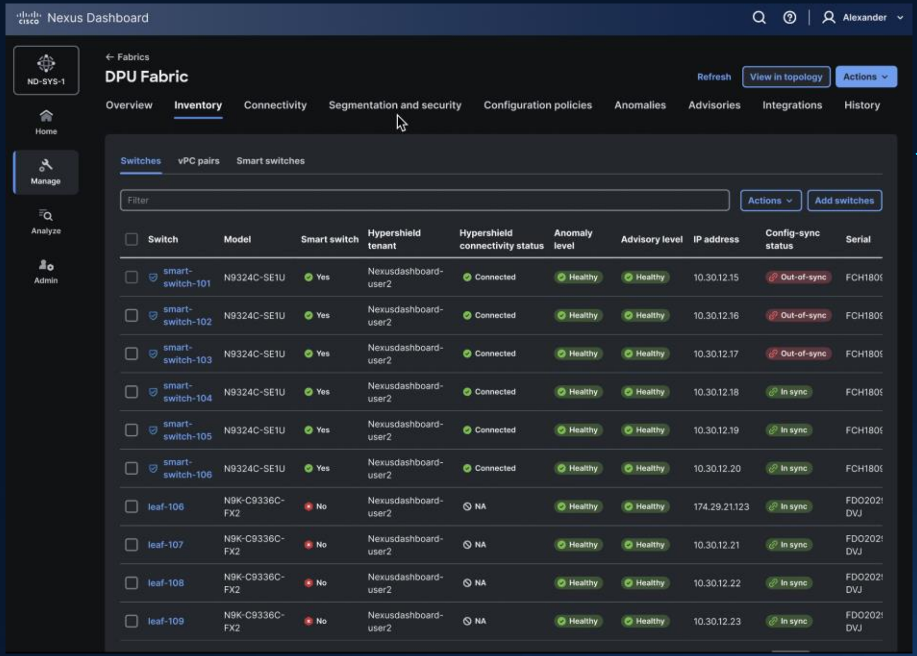
April 2025

Zone-based segmentation

April 2025

Separate Workflows for NetOps and NetSecOps

Nexus Dashboard, NX-API, NX-CLI



Nexus Dashboard — Alexander

ND-SYS-1 · Home · Manage · Analyze · Admin

← Fabrics

DPU Fabric

Refresh · View in topology · Actions

Overview · Inventory · Connectivity · Segmentation and security · Configuration policies · Anomalies · Advisories · Integrations · History

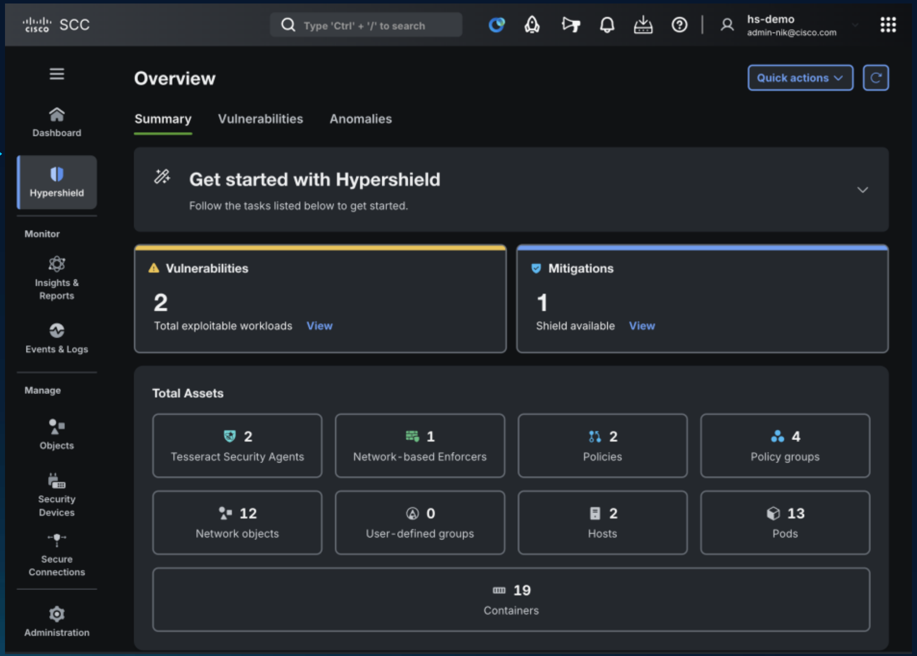
Switches · vPC pairs · Smart switches

Filter · Actions · Add switches

Switch	Model	Smart switch	Hypershield tenant	Hypershield connectivity status	Anomaly level	Advisory level	IP address	Config-sync status	Serial
smart-switch-101	N9324C-SE1U	Yes	Nexusdashboard-user2	Connected	Healthy	Healthy	10.30.12.15	Out-of-sync	FCH180
smart-switch-102	N9324C-SE1U	Yes	Nexusdashboard-user2	Connected	Healthy	Healthy	10.30.12.16	Out-of-sync	FCH180
smart-switch-103	N9324C-SE1U	Yes	Nexusdashboard-user2	Connected	Healthy	Healthy	10.30.12.17	Out-of-sync	FCH180
smart-switch-104	N9324C-SE1U	Yes	Nexusdashboard-user2	Connected	Healthy	Healthy	10.30.12.18	In sync	FCH180
smart-switch-105	N9324C-SE1U	Yes	Nexusdashboard-user2	Connected	Healthy	Healthy	10.30.12.19	In sync	FCH180
smart-switch-106	N9324C-SE1U	Yes	Nexusdashboard-user2	Connected	Healthy	Healthy	10.30.12.20	In sync	FCH180
leaf-106	N9K-C9336C-FX2	No	Nexusdashboard-user2	NA	Healthy	Healthy	174.29.21.123	In sync	FDO202 DVJ
leaf-107	N9K-C9336C-FX2	No	Nexusdashboard-user2	NA	Healthy	Healthy	10.30.12.21	In sync	FDO202 DVJ
leaf-108	N9K-C9336C-FX2	No	Nexusdashboard-user2	NA	Healthy	Healthy	10.30.12.22	In sync	FDO202 DVJ
leaf-109	N9K-C9336C-FX2	No	Nexusdashboard-user2	NA	Healthy	Healthy	10.30.12.23	In sync	FDO202 DVJ

Context sharing for troubleshooting

Hypershield On-Prem Controller



SCC — Type 'Ctrl' + '/' to search — hs-demo admin-nik@cisco.com

Dashboard · Hypershield · Monitor · Insights & Reports · Events & Logs · Manage · Objects · Security Devices · Secure Connections · Administration

Overview

Quick actions

Summary · Vulnerabilities · Anomalies

Get started with Hypershield

Follow the tasks listed below to get started.

Vulnerabilities: 2 — Total exploitable workloads — View

Mitigations: 1 — Shield available — View

Total Assets

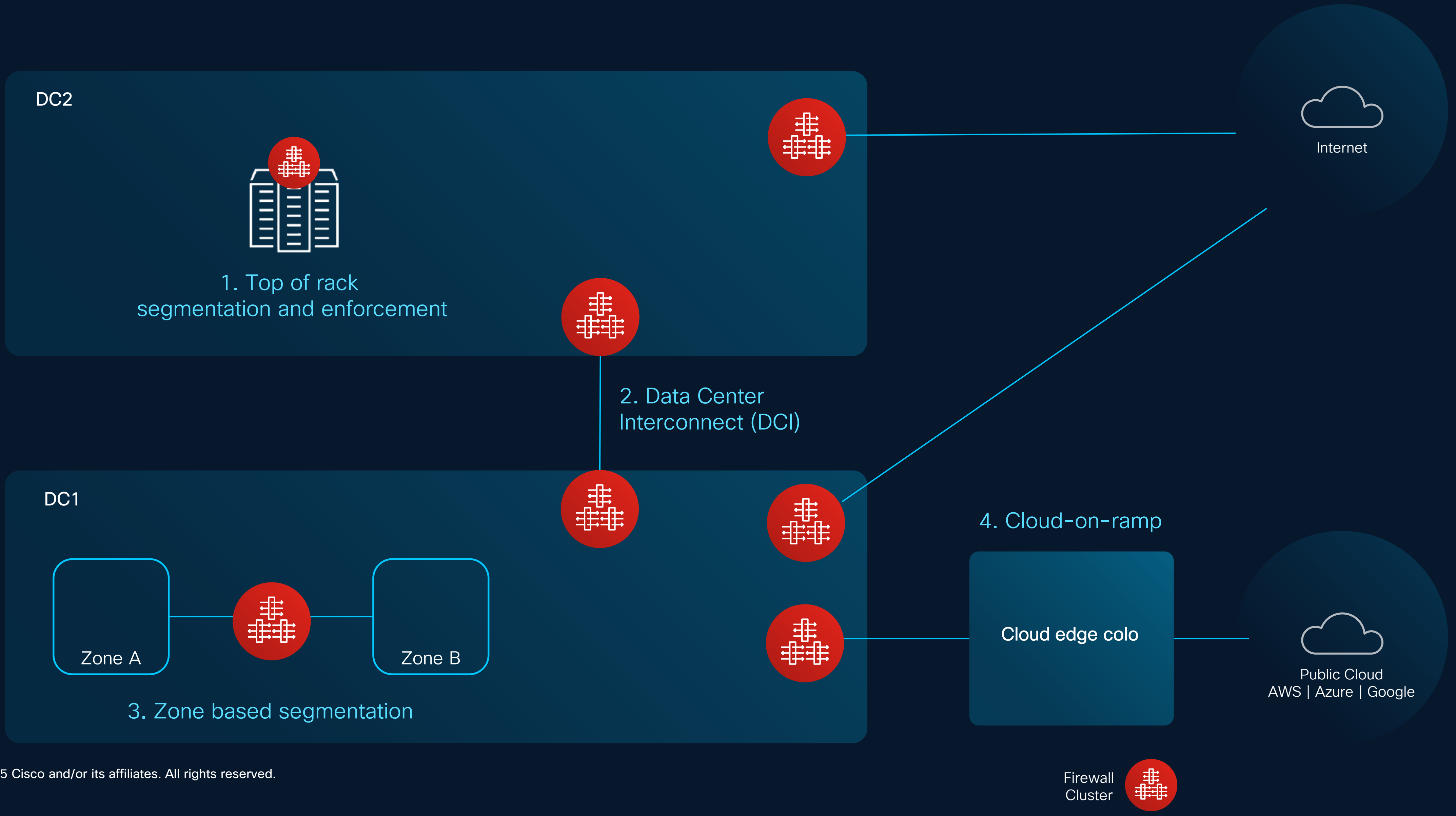
2 Tesseract Security Agents	1 Network-based Enforcers	2 Policies	4 Policy groups
12 Network objects	0 User-defined groups	2 Hosts	13 Pods
19 Containers			

Nexus Smart Switch

Use Cases

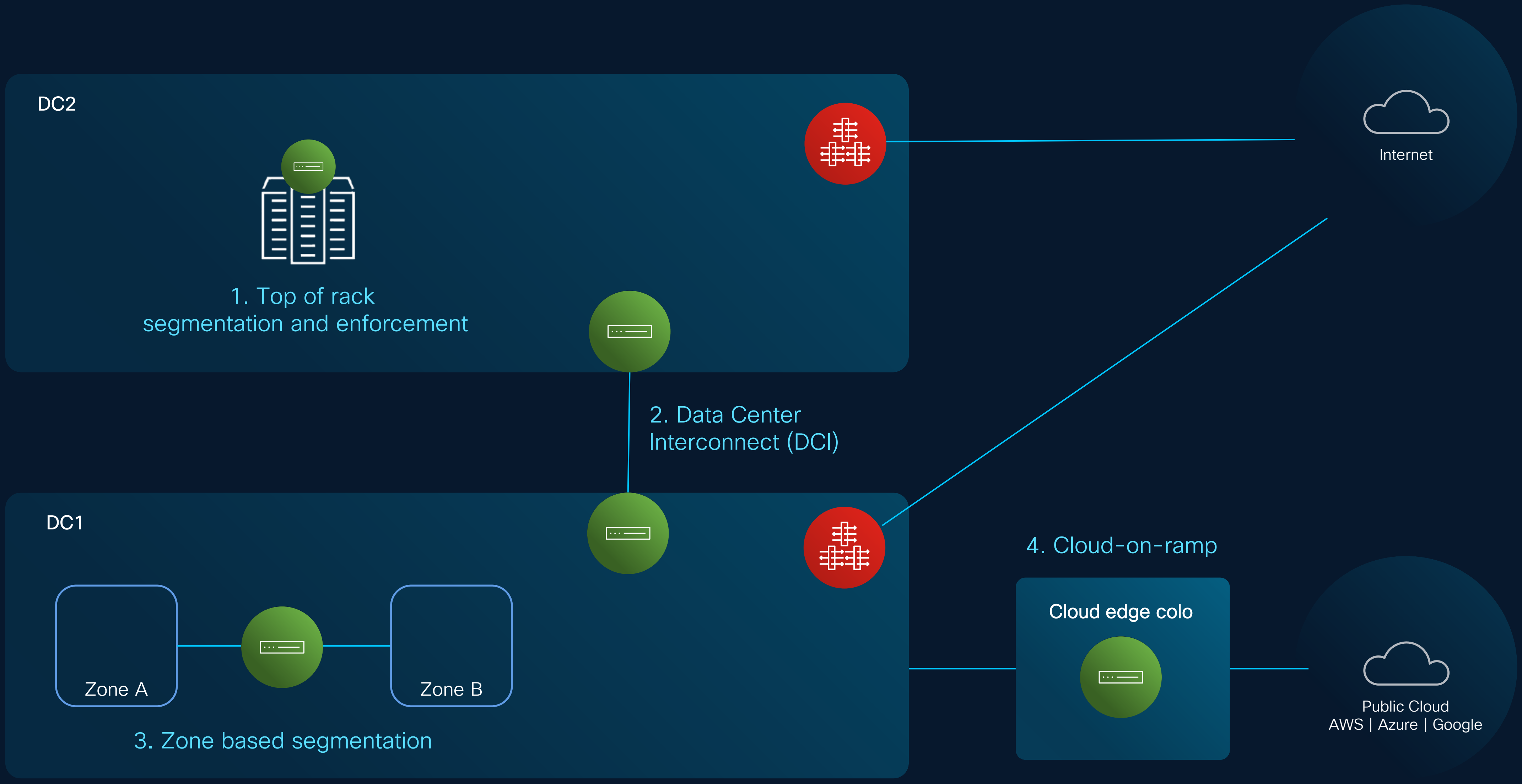
Security infused into the data center fabric

Current implementation is complex and expensive



Security infused into the data center fabric

Use cases with Cisco Smart Switches



DC2

1. Top of rack segmentation and enforcement

2. Data Center Interconnect (DCI)

DC1

Zone A

Zone B

3. Zone based segmentation

4. Cloud-on-ramp

Cloud edge colo

Internet

Public Cloud
AWS | Azure | Google

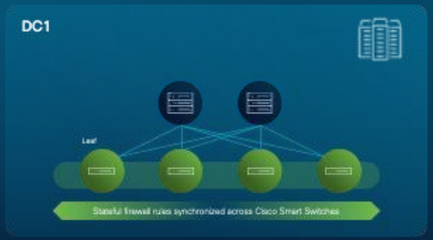
Firewall Cluster

Cisco Smart Switch

Cisco Smart Switches Use Cases

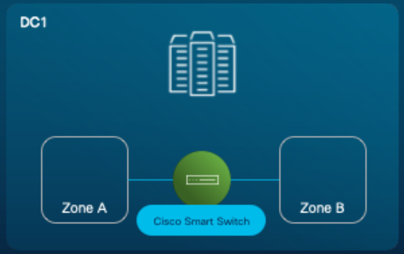
Timelines

Top of Rack Segmentation Enforcement


DC1
Leaf
Stateful firewall rules synchronized across Cisco Smart Switches

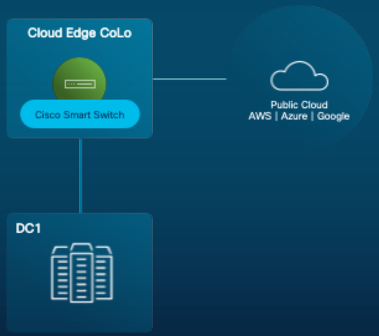
Nov 25

Zone-based Segmentation



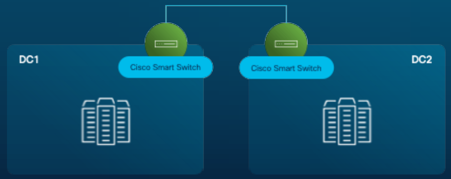
Apr 26

Cloud Edge Cloud On-ramp



Apr 26

Data Center Interconnect (DCI)

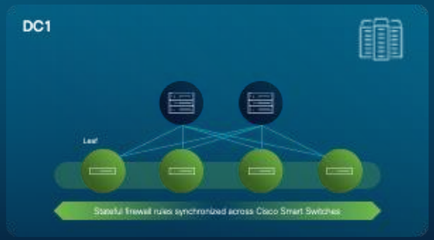


Future

Cisco Smart Switches Use Cases

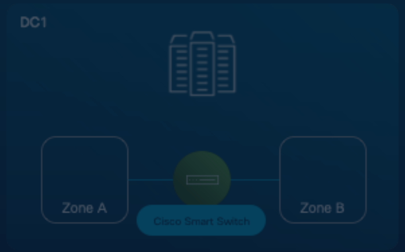
Timelines

Top of Rack Segmentation Enforcement


DC1
Leaf
Stateful firewall rules synchronized across Cisco Smart Switches

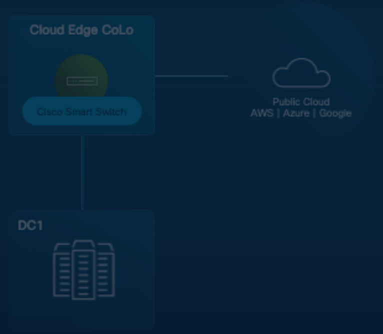
Nov 25

Zone-based Segmentation



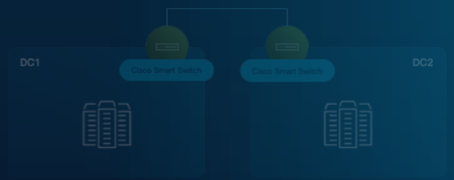
Apr 26

Cloud Edge Cloud On-ramp



Apr 26

Data Center Interconnect (DCI)



Future

Focus

Top-of-Rack Use Case

Nexus Smart Switches in “Network Mode”

Available Now

Shipping

Single Fabric Use Case

Single Fabric
- VXLAN-EVPN
- BGP

ToR Smart Switch
N9348Y2C6D-SE1U, N9324C-SE1U

✓ Role: Leaf, Border Leaf
✓ Comprehensive fabric features (L2, L3, QoS, Multicast, VPC, L2 mobility, L2/L3 stretch, etc ...)

Multi-Fabric Use Case

San Jose
Las Vegas
Denver
Dallas

Multi-Site
VXLAN-EVPN

ToR Smart Switch
N9348Y2C6D-SE1U, N9324C-SE1U

✓ Role: Leaf, Border Gateway
✓ Active-Active & DR continuity
✓ Multi-site features (L2/L3 stretch, anycast border gateway, TRMv4, etc...)

Position Futureproofing:

- Future-ready
- LDOS refresh & competitive refresh
- Brownfield insertion
- Greenfield new builds & RFP

Roadmap:

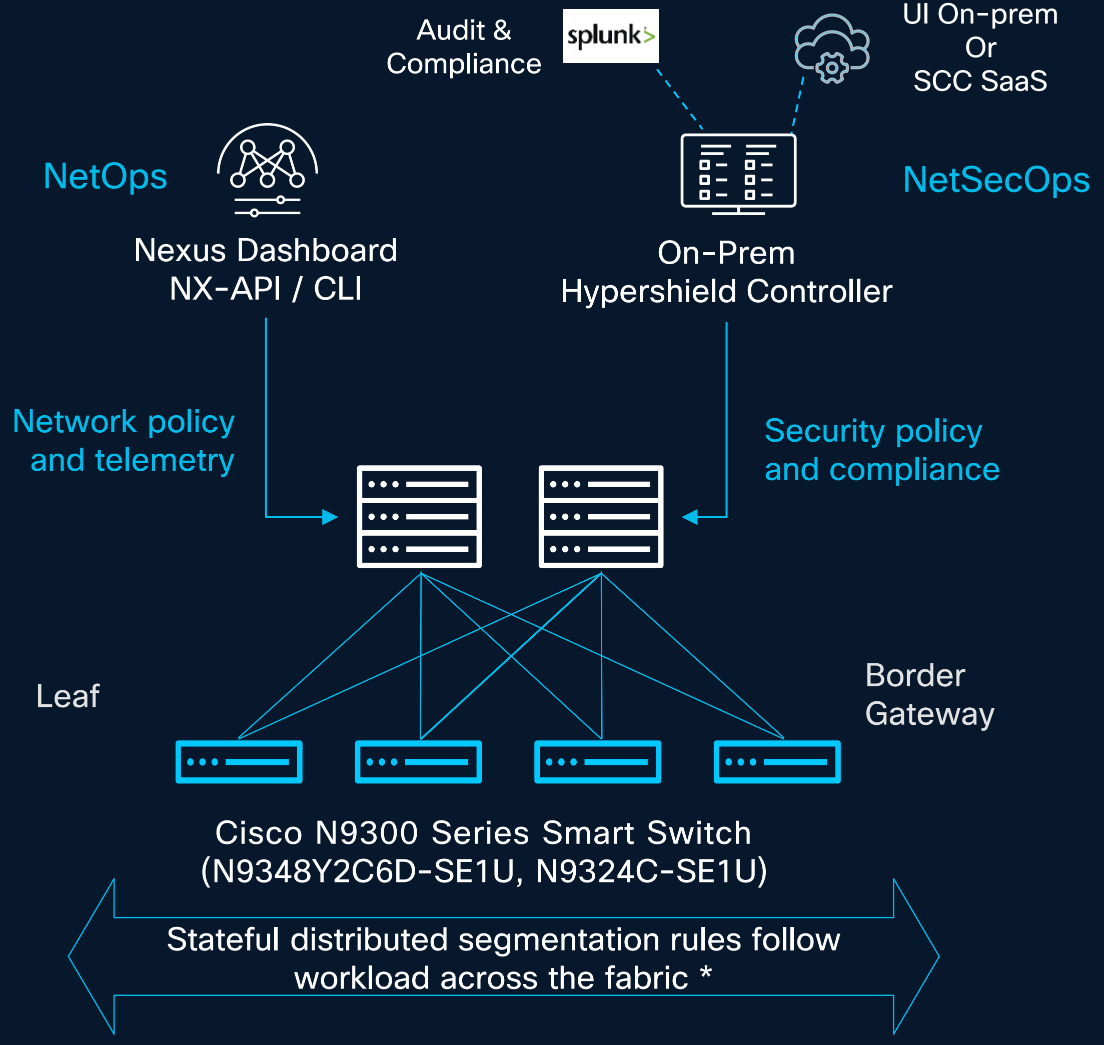
November 2025

- Nexus Dashboard 4.1.x support
- 1G support
- VXLAN vPC BGW
- Netflow

Note: Smart Switch networking mode means DPU powered off

Smart Switch "Networking & Security" Use Case

Top of Rack L4 Segmentation



Audit & Compliance
splunk>
UI On-prem Or SCC SaaS
NetOps
NetSecOps
Nexus Dashboard NX-API / CLI
On-Prem Hypershield Controller
Network policy and telemetry
Security policy and compliance
Leaf
Border Gateway
Cisco N9300 Series Smart Switch (N9348Y2C6D-SE1U, N9324C-SE1U)
Stateful distributed segmentation rules follow workload across the fabric *

Security Infused in Data Center Fabric

Version: NXOS 10.6(2)F, Hypershield 1.2

Fabric: VXLAN-EVPN, VXLAN-multi-site, BGP fabric, brownfield environments

Traffic redirection:

- VLAN or VRF redirection to DPU
- Segmentation across VRFs (route leak) or VLANs

Segmentation Policy:

- Distributed segmentation, order independent
- Stateful or stateless policy
- Per VRF/VLAN, CIDRs, L4 (CRD schema)
- Canary rollout/rollback
- Start with 100K rules, 800G throughput (benchmark pending)

Policy Sync and HA:

- Active-active HA (vPC & HSRP) with state sync

Hypershield On-prem Controller:

- Full on-premises API/UI (air-gap ready*)
- Optional Security Cloud Control SaaS for global policy
- DPU load and agent updates (via NXOS workflows)

Visibility & Observability

- Network: Nexus Dashboard
- Security: Grafana, Prometheus, On-prem controller observability
- Compliance & Audit: Splunk compliance and audit logs

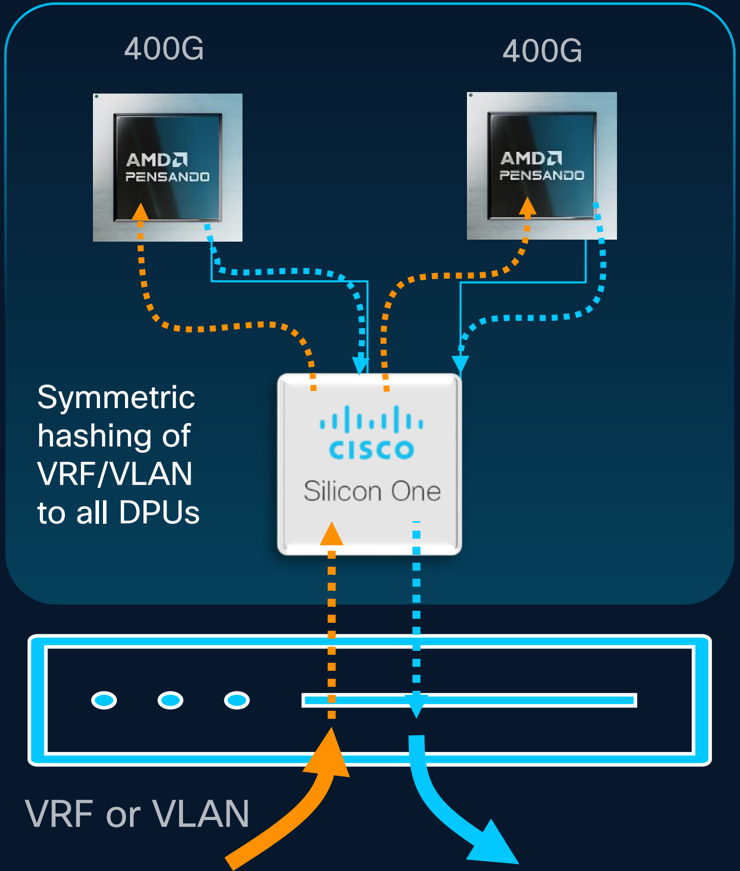
* Future | ** More details coming soon

Segmentation Journey

Traffic Redirection to DPUs

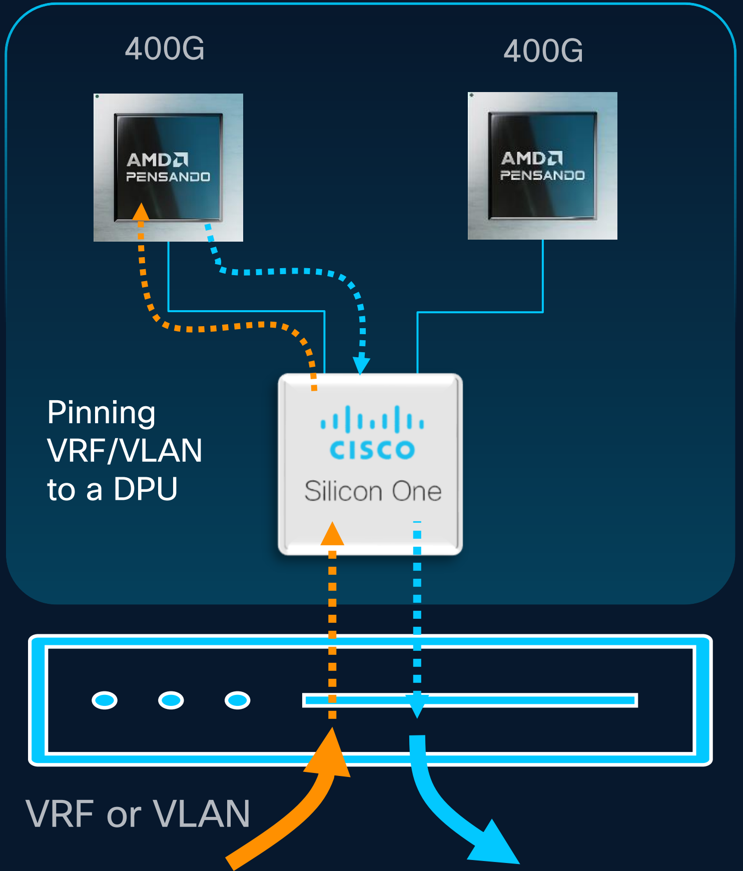
Symmetric hashing or Pinning VRF/VLAN to DPUs

Single policy applied all DPUs



Symmetric hashing of VRF/VLAN to all DPUs

Single policy per DPU

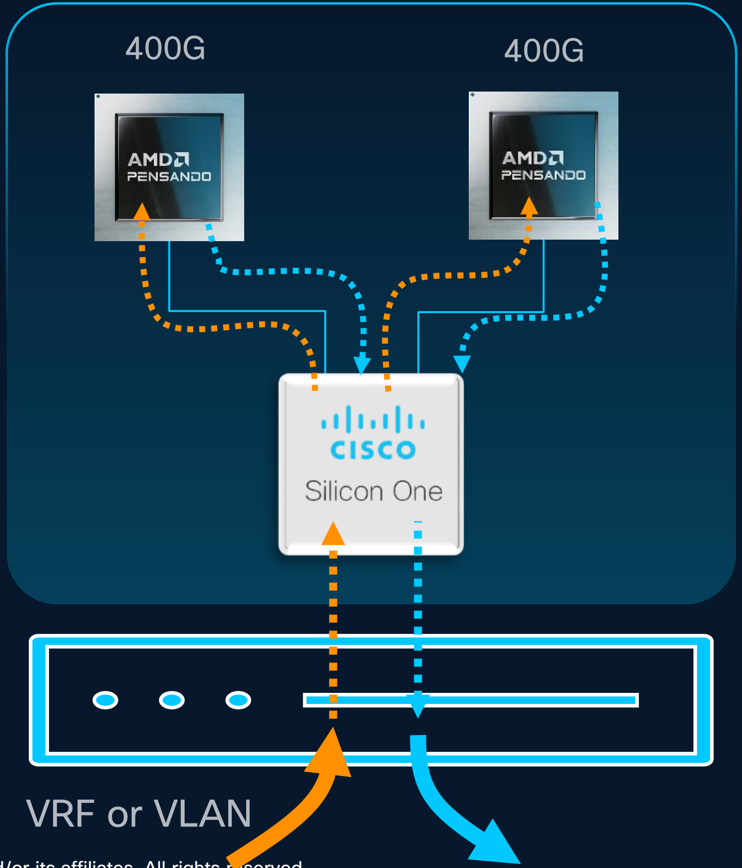


Pinning VRF/VLAN to a DPU

Security Policy Applied to All Smart Switch DPUs

Spray flows between all DPUs

Single policy applied all DPUs



Symmetric Hashing of VRF and VLAN across DPUs

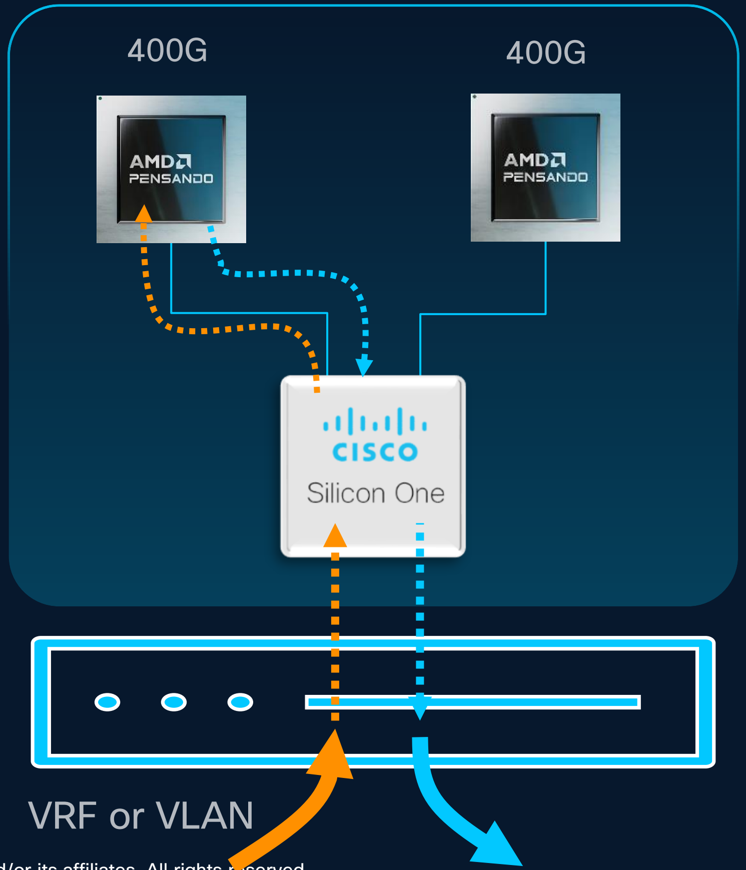
```
service dpu load-balance symmetric-hash

service system hypershield
  service firewall
    vlan 10
    vlan 13
    vrf blue
    vrf green
      in-service
```

Redirect VRF or VLAN to DPU for L4 segmentation

Pinning Security Policy to a DPU

Localize flows to a DPU

Single policy per DPU



Pin VRF or VLAN to a DPU for policy

```
service system hypershield
  service firewall
    vrf green module-affinity 1
    vlan 103 bridged-traffic
    module-affinity 1
      in-service
```

Pin flows to DPU 1

Segmentation Capabilities

A journey that starts with a future-proof hardware

Nexus Smart Switch

Stateful and Stateless L4 Segmentation

VLAN/VRF Redirect to DPU

State Sync within HA pair

Phase 1

Stateless* Macro-Segmentation

+

Proxy ARP / Macvtap**

L2 Isolation

Phase 2

Stateless* Micro-Segmentation

+

State Sync across Fabric

Phase 3

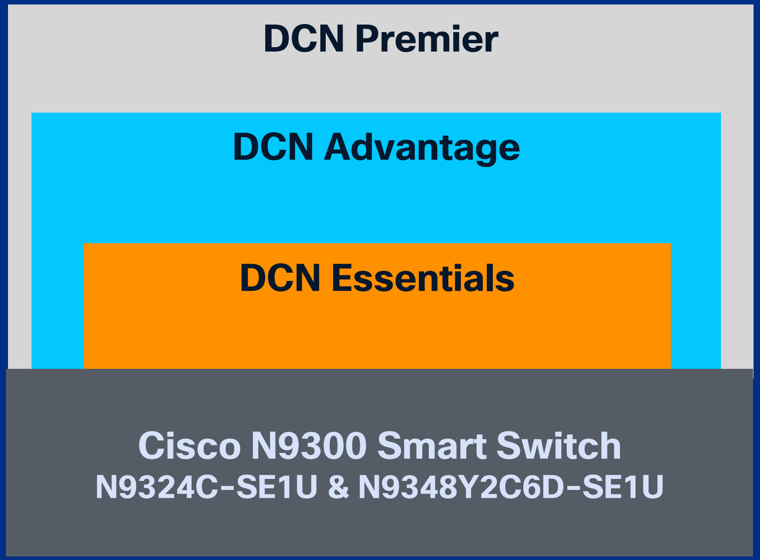
Stateful Micro-Segmentation

Macro = inter-subnet | Micro = intra-subnet

* Could be stateful in scenarios where workloads always remain in the same vPC pair - E.g., Baremetal

** Also known as 802.1Qbg or VEPA – For KVM environments

Licensing



DCN Premier

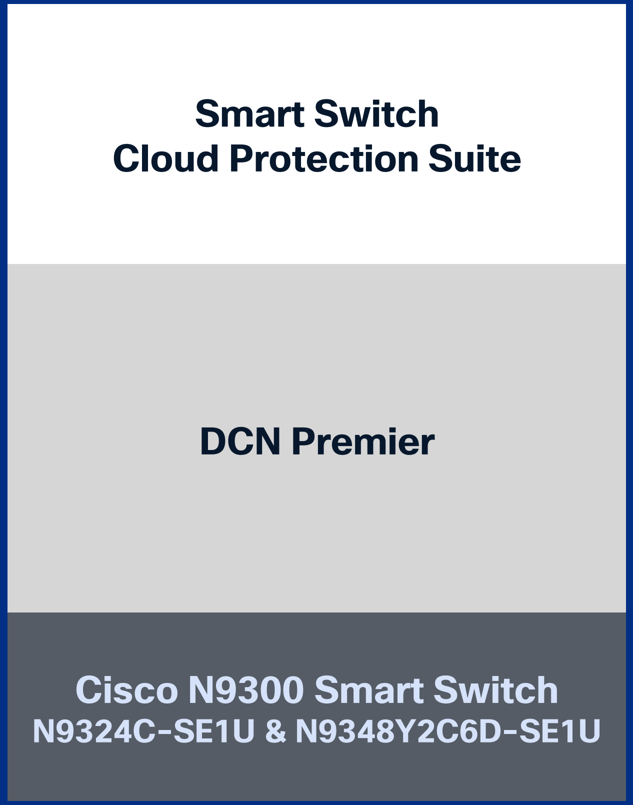
DCN Advantage

DCN Essentials

Cisco N9300 Smart Switch
N9324C-SE1U & N9348Y2C6D-SE1U

Start with Networking mode
today and add Hypershield later

Future-proof your infrastructure



Smart Switch
Cloud Protection Suite

DCN Premier

Cisco N9300 Smart Switch
N9324C-SE1U & N9348Y2C6D-SE1U

Large customer orders, EA, WPAs where
networking and security are transacted separately

Infuse security into every switch port in your network

Value Proposition

Why upgrade your infrastructure today?

Value Proposition

- Architectural Shift: Simplified, scalable networking and security w/ Nexus Dashboard and Hypershield for hyper-distributed data centers
- Cost Efficiency: Consolidates networking, security and other services into a single physical form factor
- High Performance: Real-time, lower-latency processing with DPU acceleration for hybrid cloud AI/ML data centers
- Scalable Security: Enforce microsegmentation and firewall policies at higher (800G) speeds.
- Future-ready Data centers: Future-proof today's data center infra investments to unlock DPU applications (firewalls, segmentation, ADCs, telemetry) over next 5-7 years

Cisco Nexus 9300 Smart Switch vs Firewall

Benefits & Limitations

Benefits

- Consolidates switching and firewalling on the same device
  - Reduced power, cooling and space requirements
  - Lower Total Cost of Ownership (TCO)
- Provides firewall services at a better scale and lower cost
  - Better performance
  - Lower latency

Limitations

- Limited set of NGFW capabilities
  - Stateful inspection, TCP state tracking, ALG but no L7 inspection or other NGFW