DET –Datacenter Networking Update

Alex Brantsma
Cloud and AI Solutions Engineer

April 2026

Agenda

- Cisco Datacenter Networking Solutions Overview
- Nexus ONE
- Nexus Highlights
- Nexus Dashboard
- Q&A

Nexus Solution overview

Introducing Cisco Nexus Platform

Network Intelligence that propels AI to deliver secure, power-efficient, scale-out & scale-across fabrics with assured performance

One Platform. Open Choice. No Compromises.

The Nexus One advantage

Now with Nexus Hyperfabric

Cisco Nexus 9300 Series

a consistent, unified hardware foundation for all your data center needs

Operate your way, evolve when ready.

Common Hardware: Nexus 9300

N9K-9336C-SE1 (100G Spine/Leaf)
Silicon One E100 • 36x QSFP28

N9K-93180YC-FX3 (SFP28 Leaf)
Cloud Scale FX3 • 48x SFP28 + 6x 100G QSFP28

N9K-93108TC-FX3 (Copper Leaf)
Cloud Scale FX3 • 48x 100M/1G/10G Cu + 6x 100G QSFP28

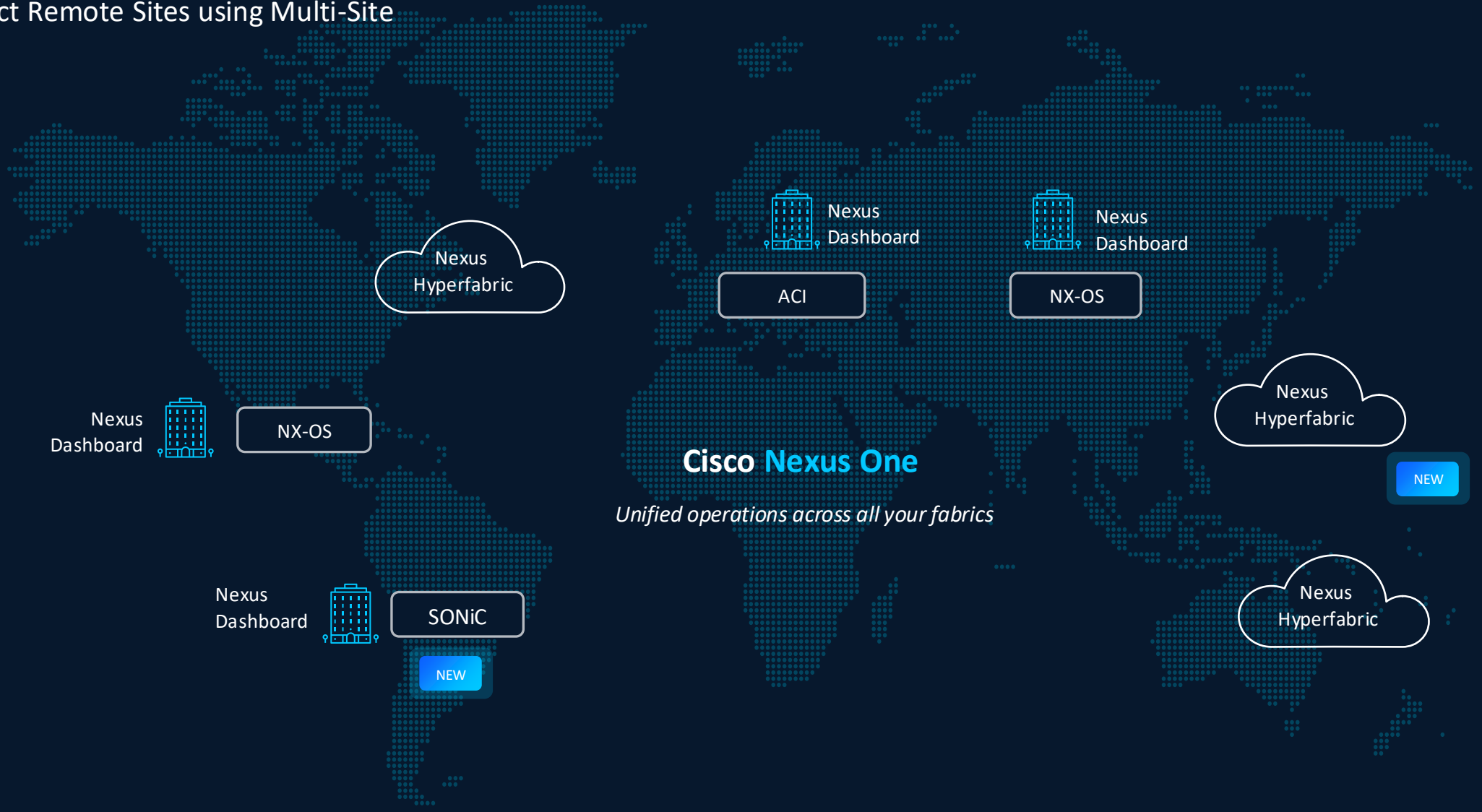
Flexible Operating Models

Nexus Dashboard	Nexus Hyperfabric	DIY Automation
On-Prem	Cloud-Managed	Custom automation with open APIs

*Nexus 9300 support available 2H CY2026

Proven distributed architectures and multisite orchestration

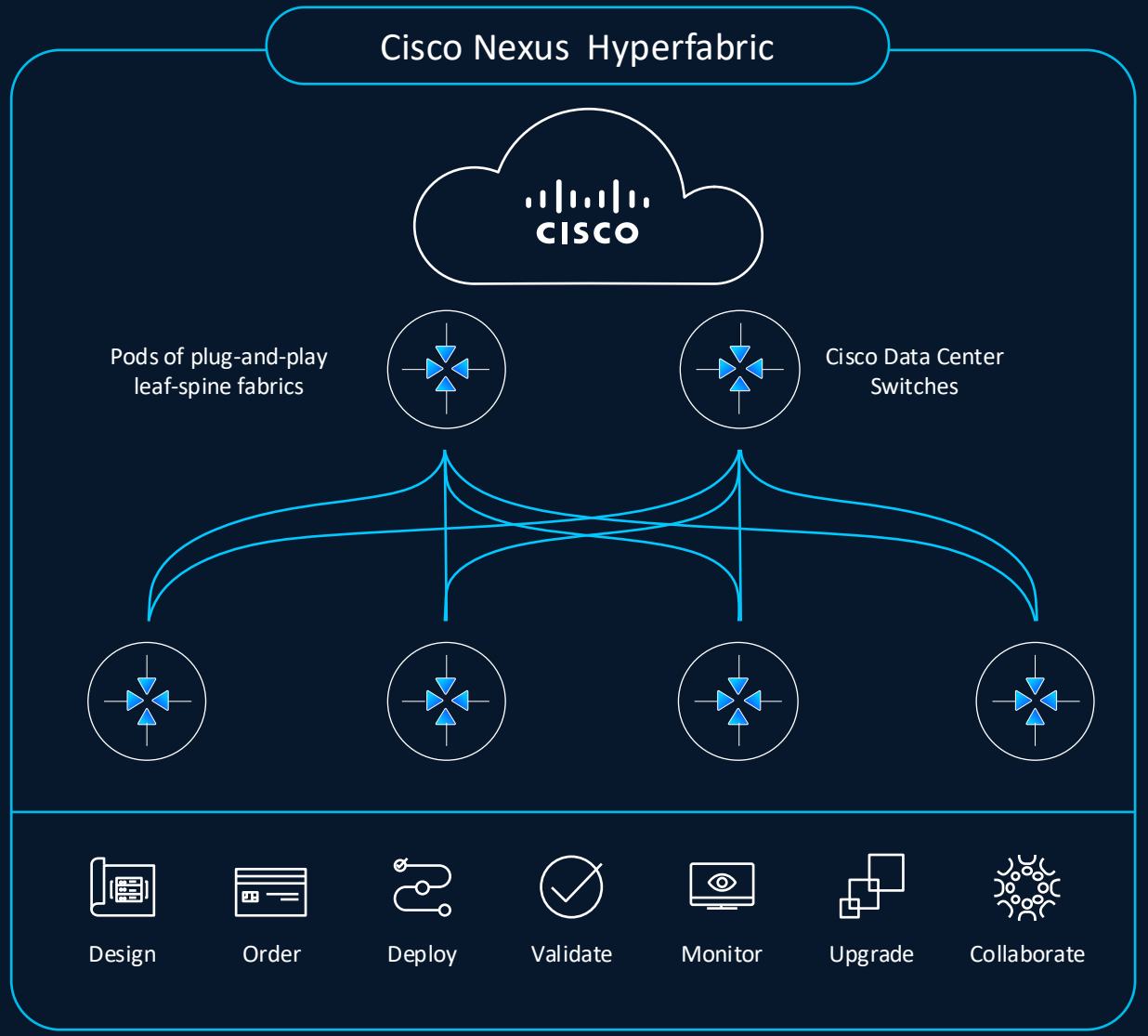
Connect Remote Sites using Multi-Site



Nexus Hyperfabric

Cisco Nexus Hyperfabric

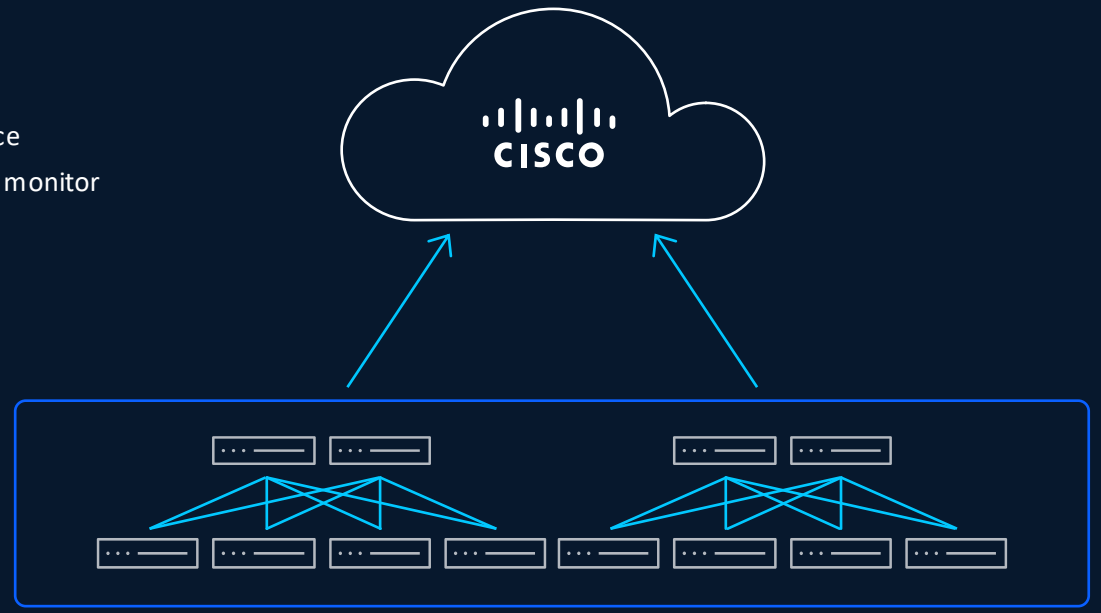
- Design, deploy, and operate on-premises fabrics located anywhere
- Streamlined operations for IT generalists, application, and DevOps teams
- Outcome driven using purpose-built vertical stack



Nexus Hyperfabric components

Cloud controller

- Scalable, distributed multi-tenant cloud service
- Design, plan, configure, deploy, upgrade, and monitor
- Browser, API, and mobile access



Cloud-managed switches

- Boot-strapped from cloud
- Full visibility and control from the cloud
- Silicon One®-based performance and capabilities

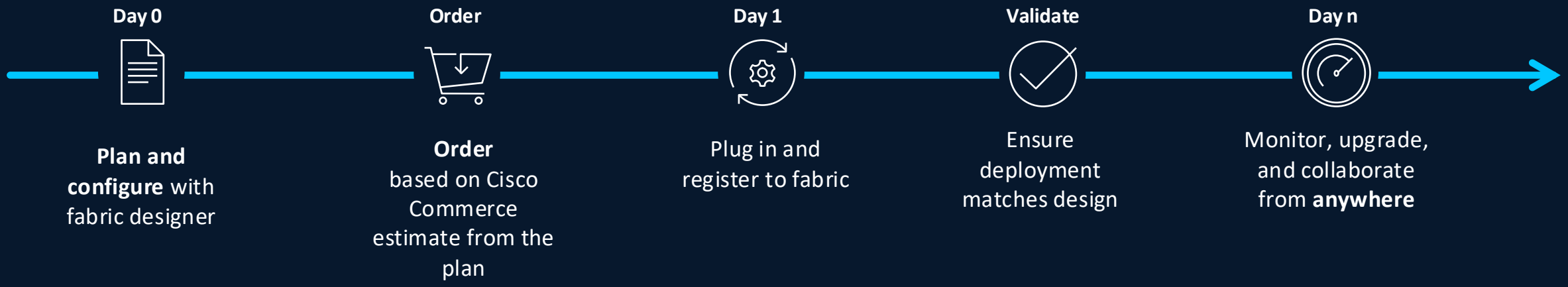
High-performance fabrics

- I0/25/100/400/800 GbE connectivity
- Standards-based EVPN/VXLAN fabric with IPv4/IPv6 routing
- Mesh and/or spine-leaf fabric designs
- Horizontal scale

On-site web portal

- Step-by-step deployment tasks
- Registration and cabling
- Real-time validation

How it works



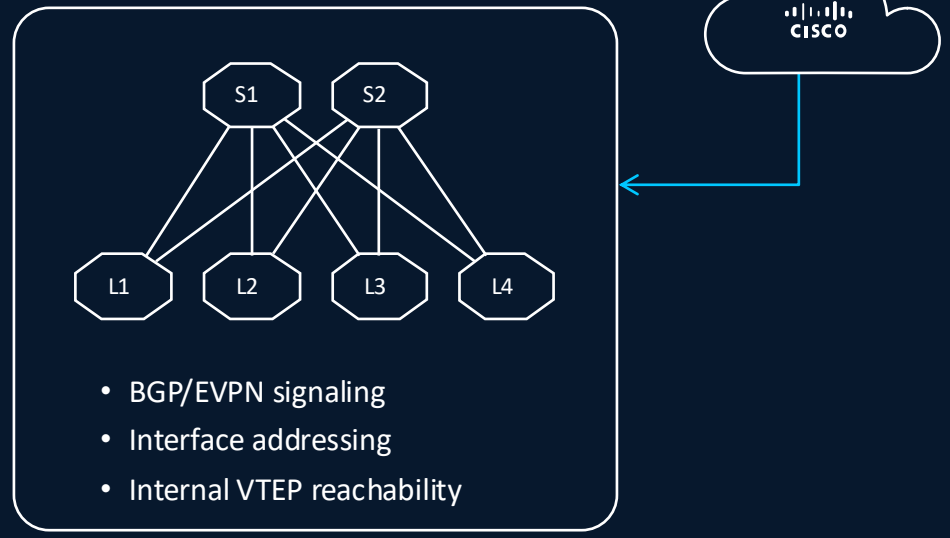
The Hyperfabric Lifecycle

- **Design:** Use the intuitive GUI to create validated fabric blueprints, generating BOMs and cabling plans
- **Deploy:** Switches auto-connect to the cloud controller for provisioning
- **Manage:** Manage fabrics through a single interface
- **Scale:** Manage updates, seamlessly expand or redesign fabrics

Fabric management

Internal network is opaque: no switch configs

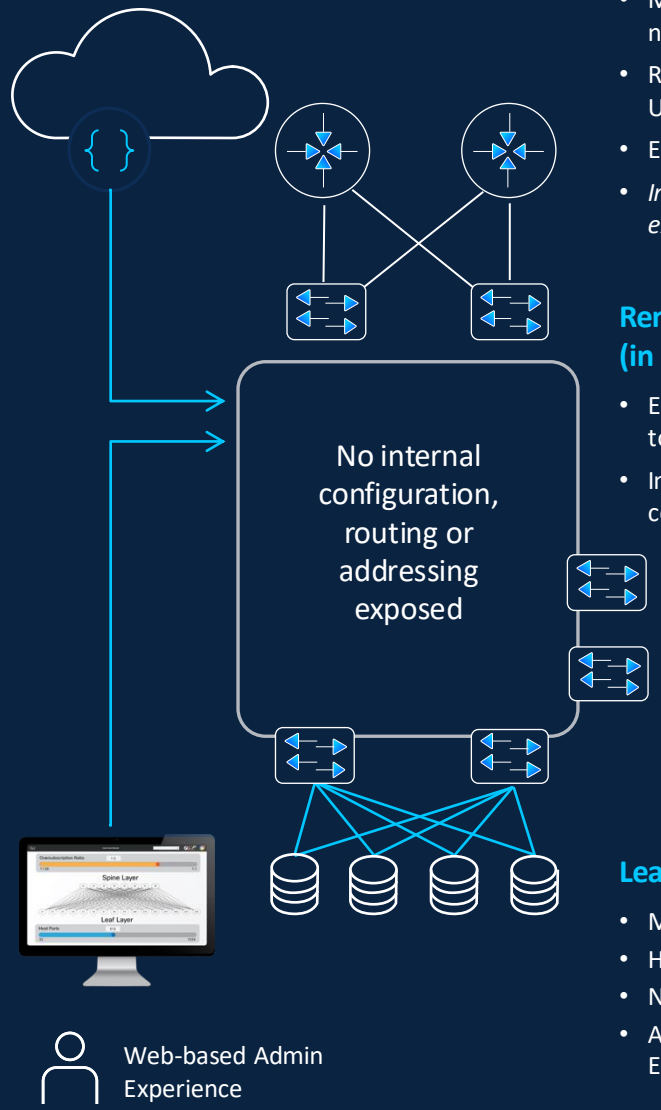
- L2/L3 services described by service data model
- Cloud UI and API used to provision services
- Visibility and assurance are built-in



Cloud SaaS controller manages all internal pod configurations

(internal routing and interface addressing)

Cloud-based provisioning/ telemetryAPI



Gateway peering config

- Multi-VRF peering and dot1q to upstream network
- Routing and peering configuration through Cloud UI
- External routing/peering configuration exposed
- *Internal routing/addressing not exposed to external network*

Remote gateway / pod connect (in development)

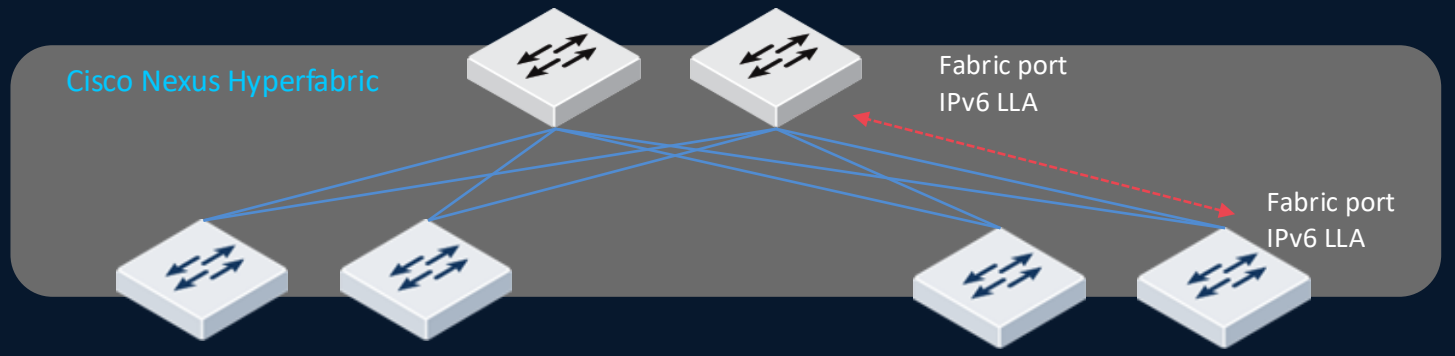
- Encrypted tunnel connectivity to remote Nexus® Hyperfabric™ pods
- Internal signaling managed by cloud SaaS controller

Leaf: host/edge port config

- MLAG and host peering with dot1q VLAN
- Host connectivity services data model
- Network-based service data model
- Automated provisioning though API: Ex: Ansible/Terraform providers

Automating the Underlay

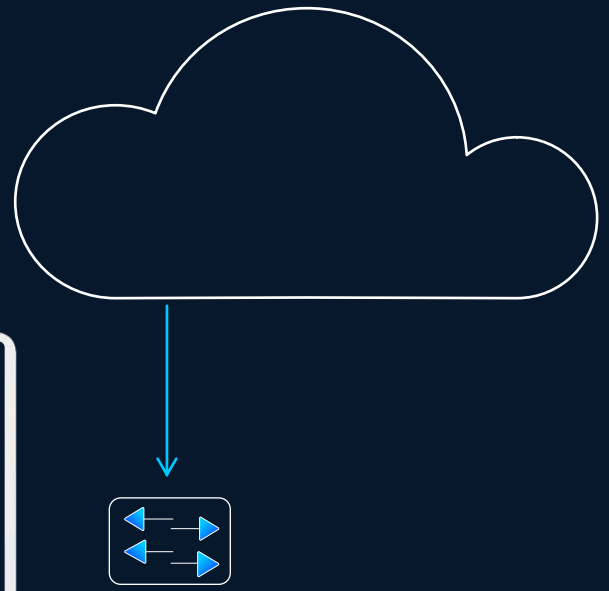
- Hyperfabric switches automatically detect and authenticate each other.
  The communication between switches use Fabric port IPv6 Link Local Addresses (LLA).
- Once it’s hardware authenticated, underlay and overlay configuration is automatically done.



- Neighbor discovery via LLDP
- Authenticate each other
- Automatically configure BGP and VXLAN

Plug-and-Play Fabric Links

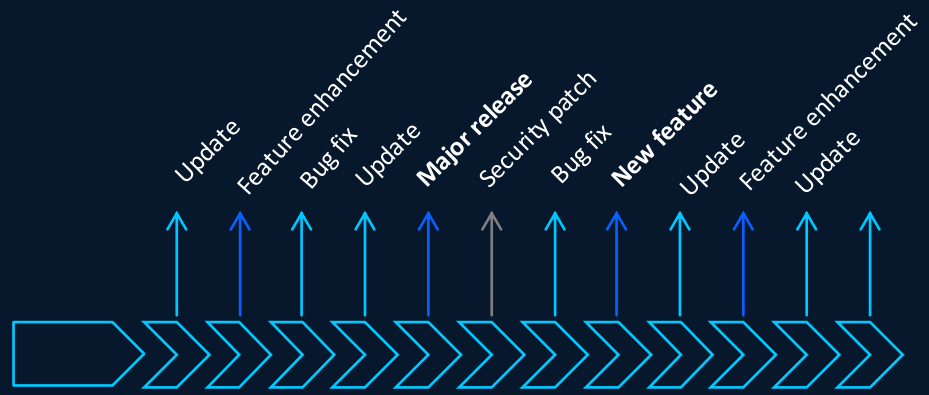
Software lifecycle management



Cloud SaaS controller:

Continuous delivery model: always up-to-date

- Continuous delivery of new features and software updates to the production cloud service
- No user testing or software maintenance required



On-premises switch software

Cloud-delivered software upgrades: user-driven update schedule

- Schedule switch software updates
- Software rollback support
- Intelligent sequencing of fabric upgrades

Flexible architectures

Fabrics anywhere

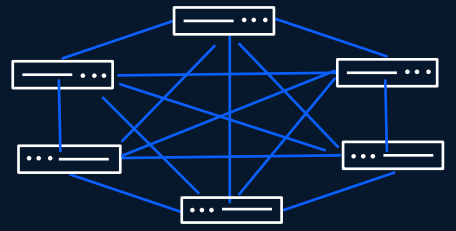
Mesh / spine-less fabrics

A Fabric of One”
Lab and API

2-switch fabric
120 host ports

4-switch fabric
240 host ports

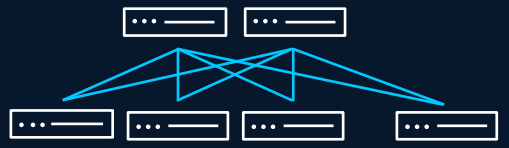
6-switch N9300 fabric
288 host ports



2 spine, 2 leaf

2- or 4-way spine, 2-32 leaf

≈ 2000 host ports



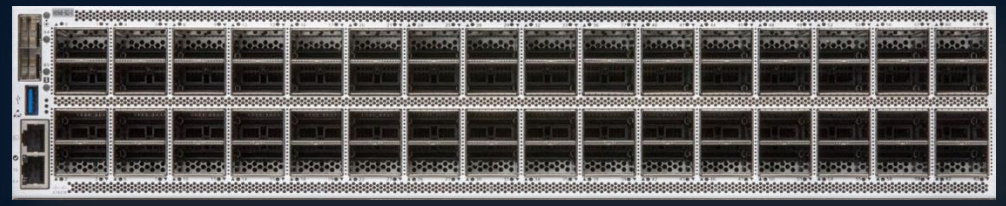
Leaf-spine DC fabrics

3-Tier Super-Spine

Nexus Hyperfabric Hardware

Nexus 6100 Series

AI-Ready 400G/800G Fabric



HF6100-64ED (800G Spine / AI)
Silicon One G200 • 64x 800G OSFP

HF6100-32D (400G Spine)
Silicon One Q200 • 32x 400Gb QDD

HF6100-60L4D (Leaf)
Silicon One Q200 • 60x SFP56 + 4x 400Gb QDD

Nexus 9300 Series*

Enterprise 100 Gb Fabric

N9K-9336C-SE1 (100G Spine/Leaf)
Silicon One E100 • 36x QSFP28

N9K-93180YC-FX3 (SFP28 Leaf)
Cloud Scale FX3 • 48x SFP28 + 6x 100G QSFP28

N9K-93108TC-FX3 (Copper Leaf)
Cloud Scale FX3 • 48x 100M/1G/10G Cu + 6x 100G QSFP28

*Nexus 9300 support available 2H CY2026

Demo

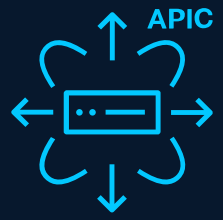
ACI

What is Cisco ACI?

An application-centric networking framework

Software-defined networking that takes a systems approach to deliver best-in-class automation through integration of hardware and software, physical and virtual elements

Policy model (application basic components)



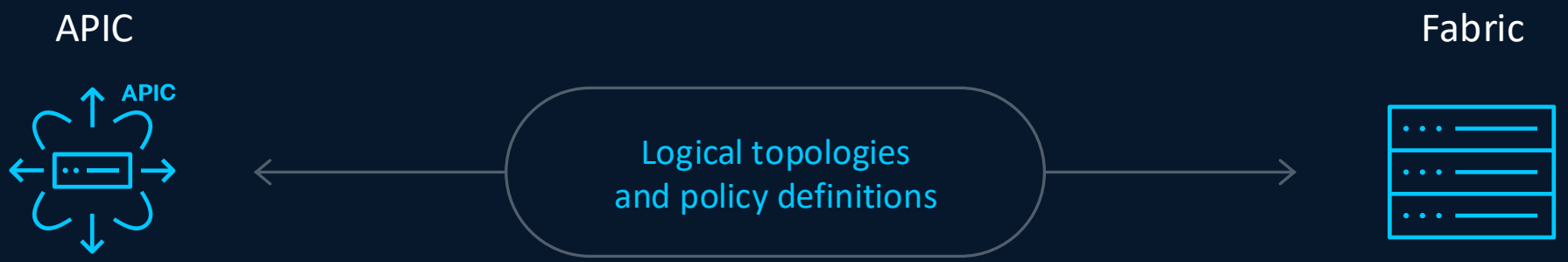
Cisco® Application Policy Infrastructure Controller (APIC)

Fabric (Cisco Nexus® 9000)

The unified point of automation and management for the Cisco ACI® fabric, policy enforcement, and health monitoring for physical, virtual, and cloud infrastructures

Cisco ACI

Application Policy Infrastructure Controller



Cisco® APIC is the main architectural component of Cisco ACI®

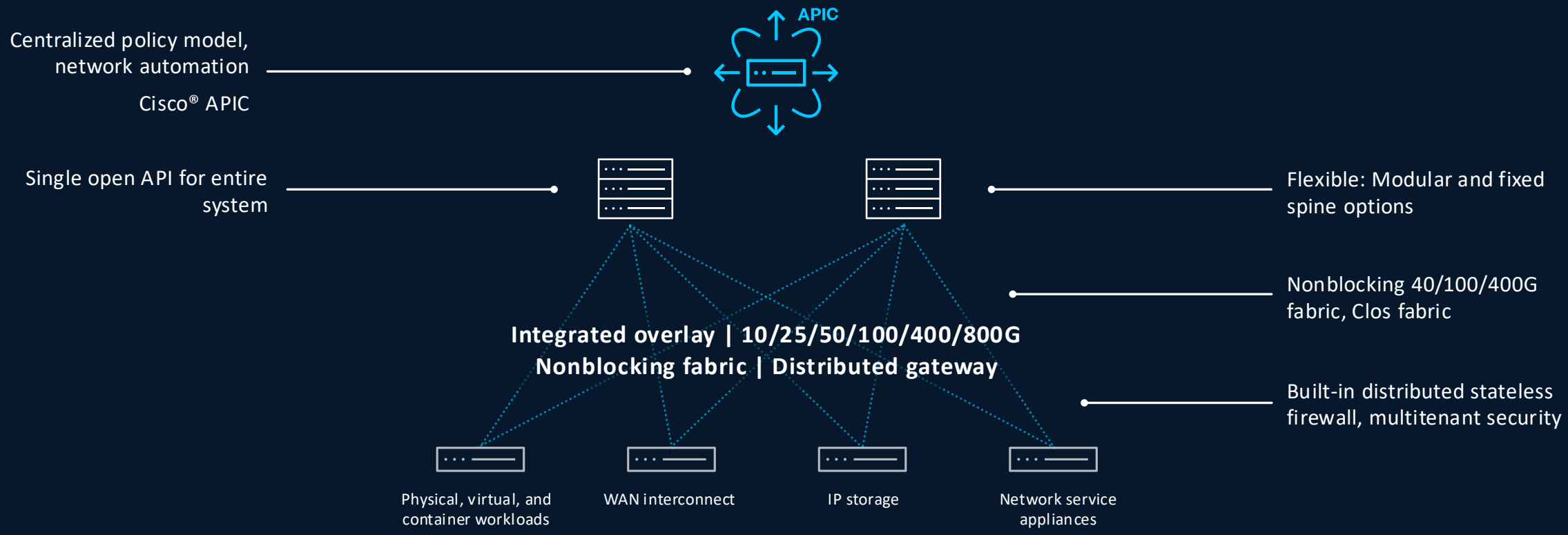
It is the unified point of automation and management for the Cisco ACI fabric,
policy enforcement, and health monitoring for physical, virtual, and cloud infrastructures

Cisco ACI

Core building blocks

Application Centric Infrastructure building blocks

Built on Cisco Nexus 9000 Series



Industry leading

Price | Performance | Port density | Programmability | Power efficiency

Cisco ACI Nexus 9000 portfolio evolution

New 400G and 800G-ready products

Shipping

100G

400G

800G

Nexus 9300
16 ports 400G
28 ports 100G plus 8 ports 400G

CY19

Nexus 9500
16-port 400G line card

CY21

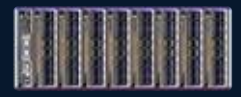
Nexus 9300
32 ports 400G

Nexus 9300
48 ports 400G
64 ports 400G

CY22 Q2

New

Nexus 9400
64 ports 400G
128 ports 200G



CY23 Q1

Nexus 9800
Up to 288 400G ports
800G ready

Nexus 9800
Up to 144 400G ports
800G ready

Future

Cloud service providers

Telco service providers

Enterprise

Media networks

Cisco ACI

Deployment models

Flexible Cisco ACI controller deployments

Remote APIC cluster

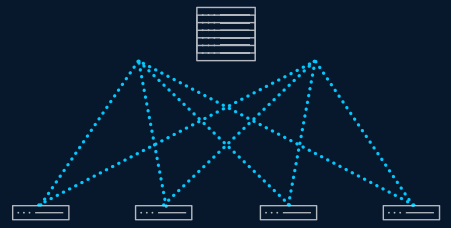
Layer 3 network

Deploy APIC cluster in a remote secure zone

Virtual APIC cluster

Hypervisor

Layer 3 network

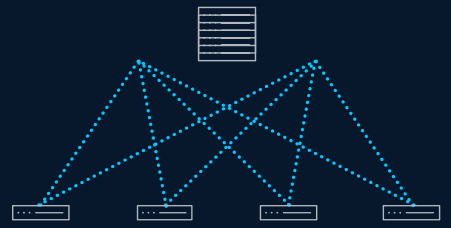


Deploy APIC cluster on hypervisor over Layer 3 network

Cloud-hosted APIC cluster

aws

Layer 3 network

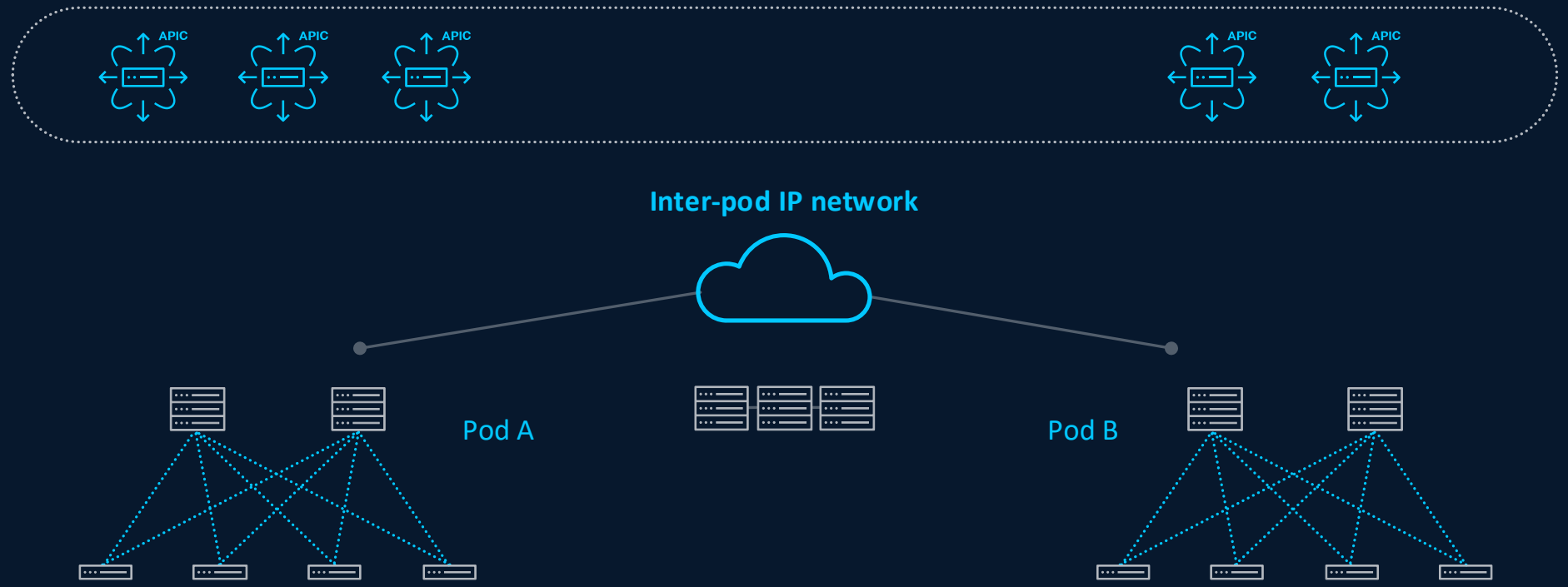


Deploy APIC cluster in the cloud to manage on-premises fabric

*Future release

Cisco ACI Multi-Pod

Create on-premises availability zones with multiple fabrics

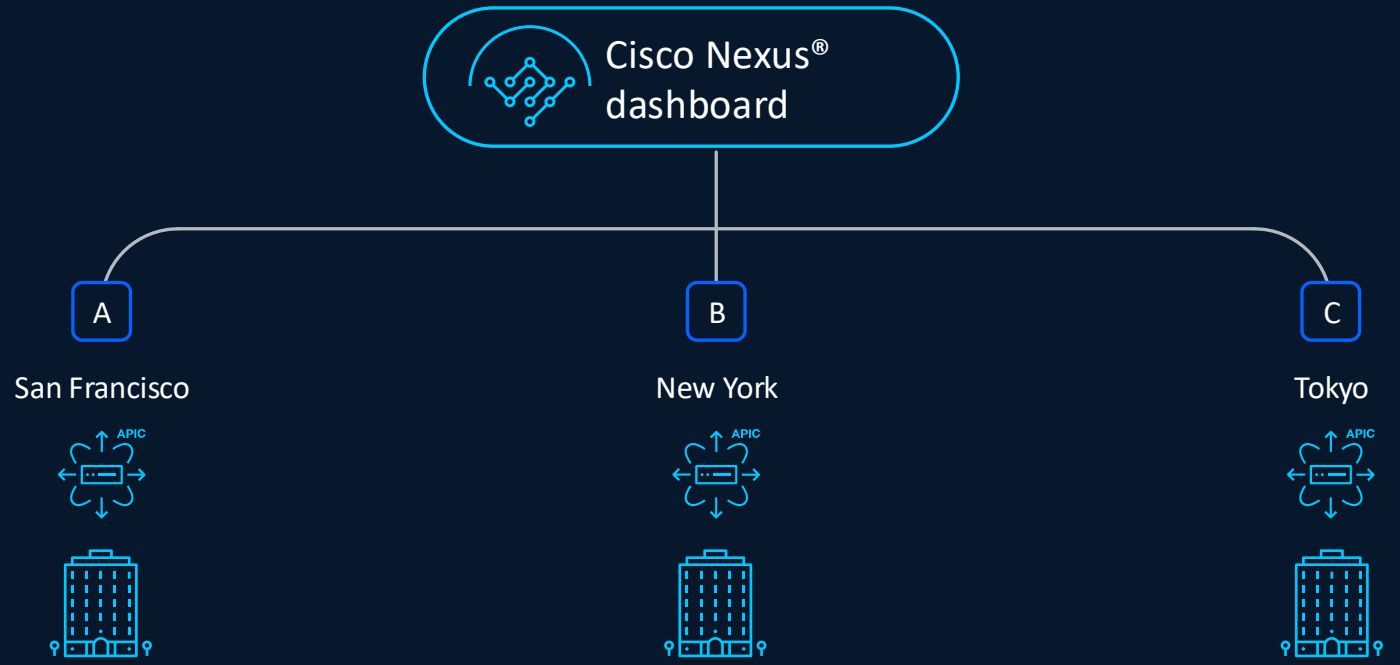


Benefits

- Disaster recovery
- Active-active load balancing
- Deploy highly available applications
- Extend VM and container mobility domains

Cisco ACI Multi-Site

Create fault-tolerant regions in geographically distributed on-premises data centers

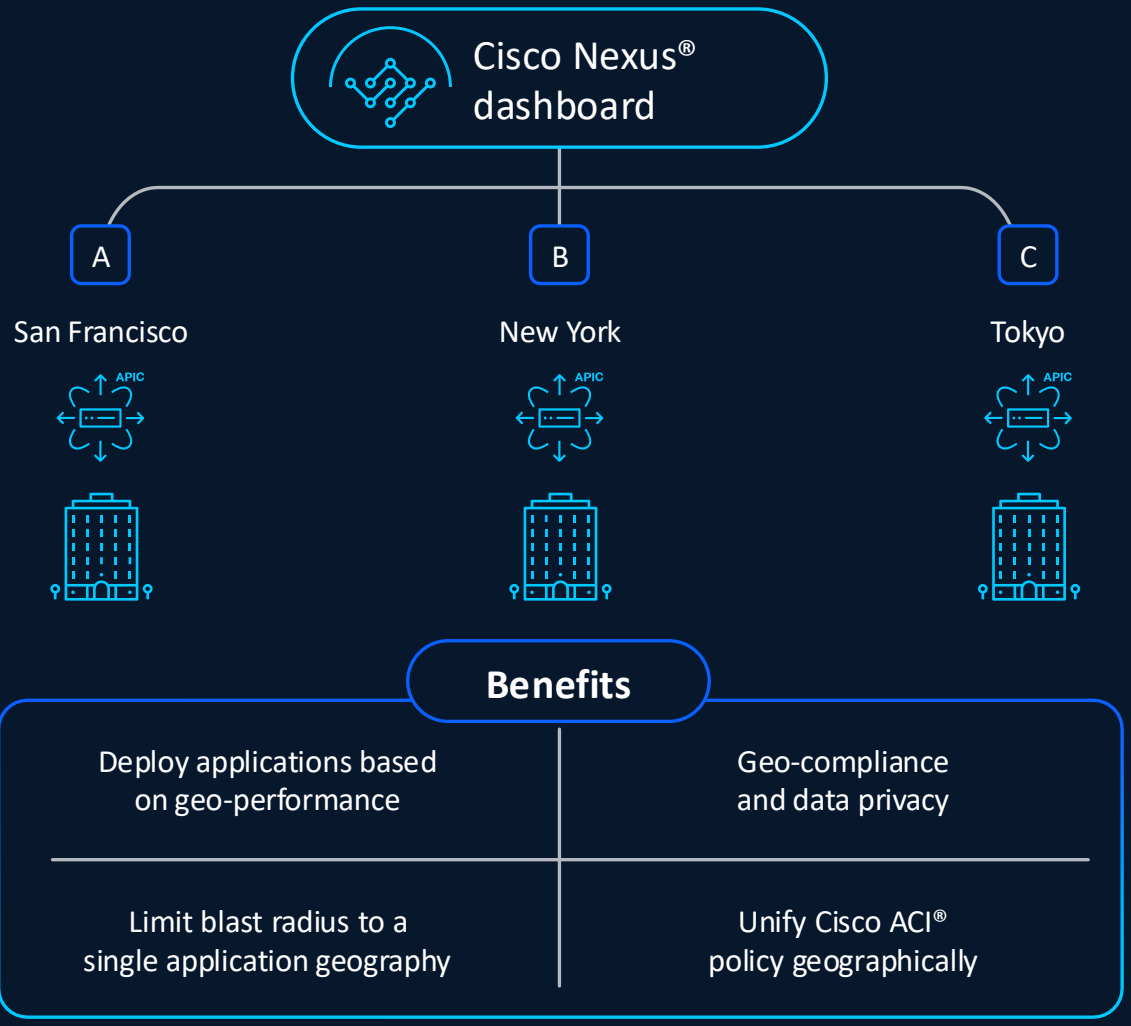


Benefits

- Deploy applications based on geo-performance
- Geo-compliance and data privacy
- Limit blast radius to a single application geography
- Unify Cisco ACI® policy geographically

Cisco ACI Multi-Site

Create fault-tolerant regions in geographically distributed on-premises data centers

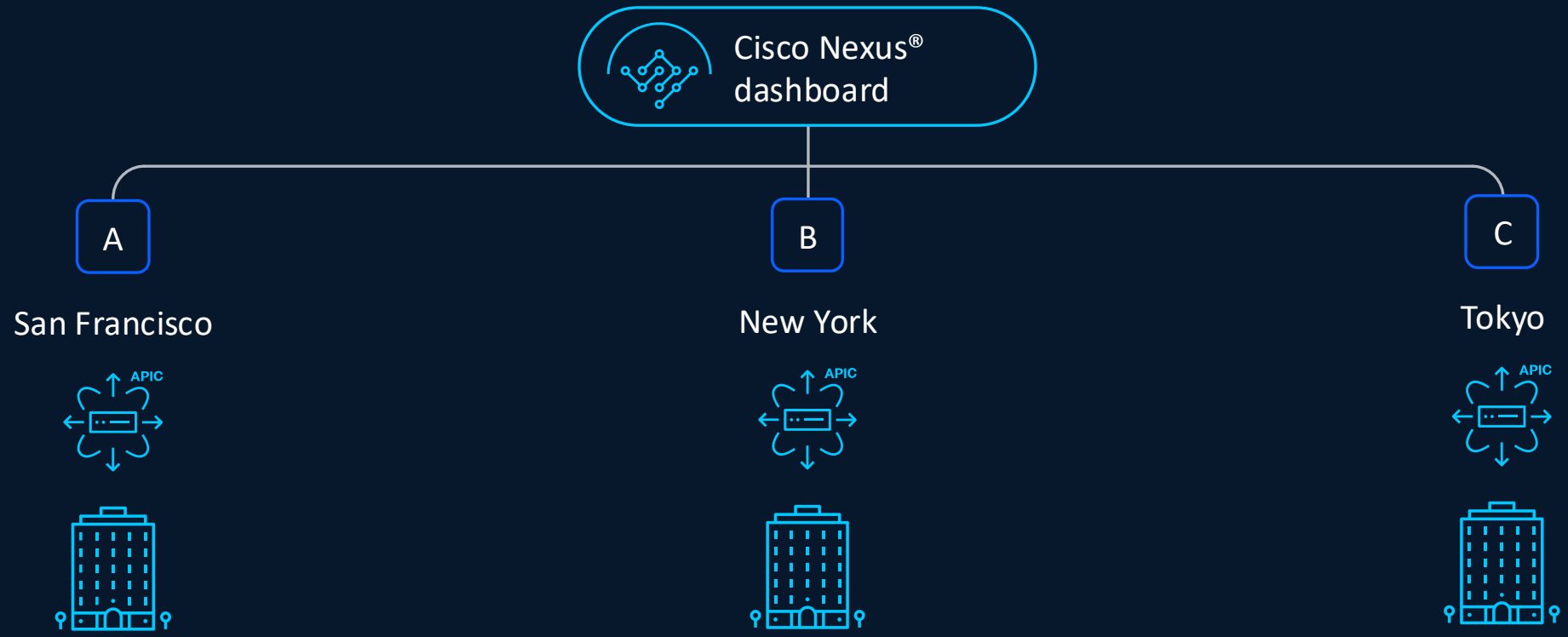


Benefits

- Deploy applications based on geo-performance
- Geo-compliance and data privacy
- Limit blast radius to a single application geography
- Unify Cisco ACI® policy geographically

Cisco ACI Multi-Site

Create fault-tolerant regions in geographically distributed on-premises data centers

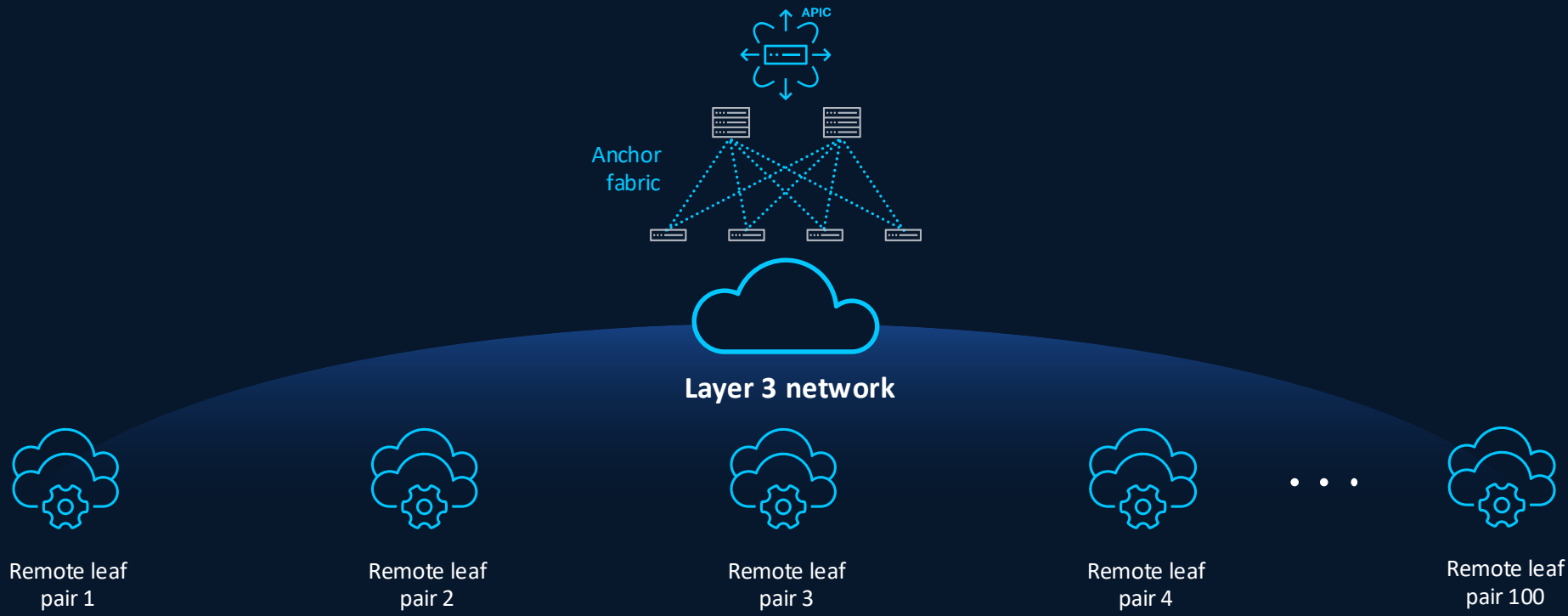


Benefits

Deploy applications based on geo-performance	Geo-compliance and data privacy	Limit blast radius to a single application geography	Unify Cisco ACI® policy geographically

Cisco ACI: Remote leaf

Enable low-touch remote application deployments with the power of Cisco ACI



Benefits

Single management plane for core fabric and remote leaf	Automation of global data center footprint	End-to-end security using Cisco ACI's segmentation model

Cisco ACI

Software constructs

Basic policy constructs of Cisco ACI

Single open API for entire system

A model-driven framework where the software maintains the representation of the administrative and operational state of the system.

The APIC detects a change and applies a modification to the model; this in turn triggers a change to the managed endpoint.

Tenant

Virtual routing and forwarding domain (VRF)

Contract

Endpoint group (EPG)

Endpoint security group (ESG)

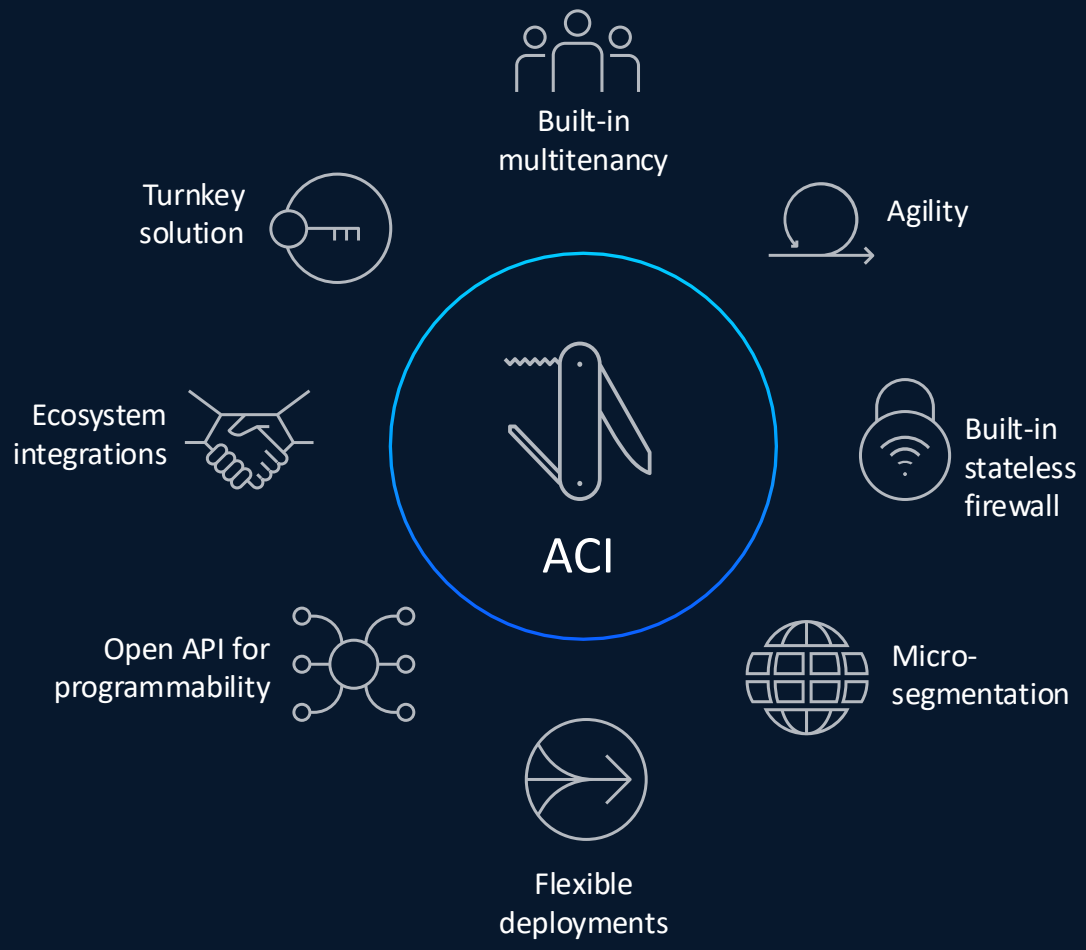
Bridge domain (BD)

Application network profile (ANP)

Single open API for the entire system; the API is a first-class citizen

Cisco ACI

Core capabilities

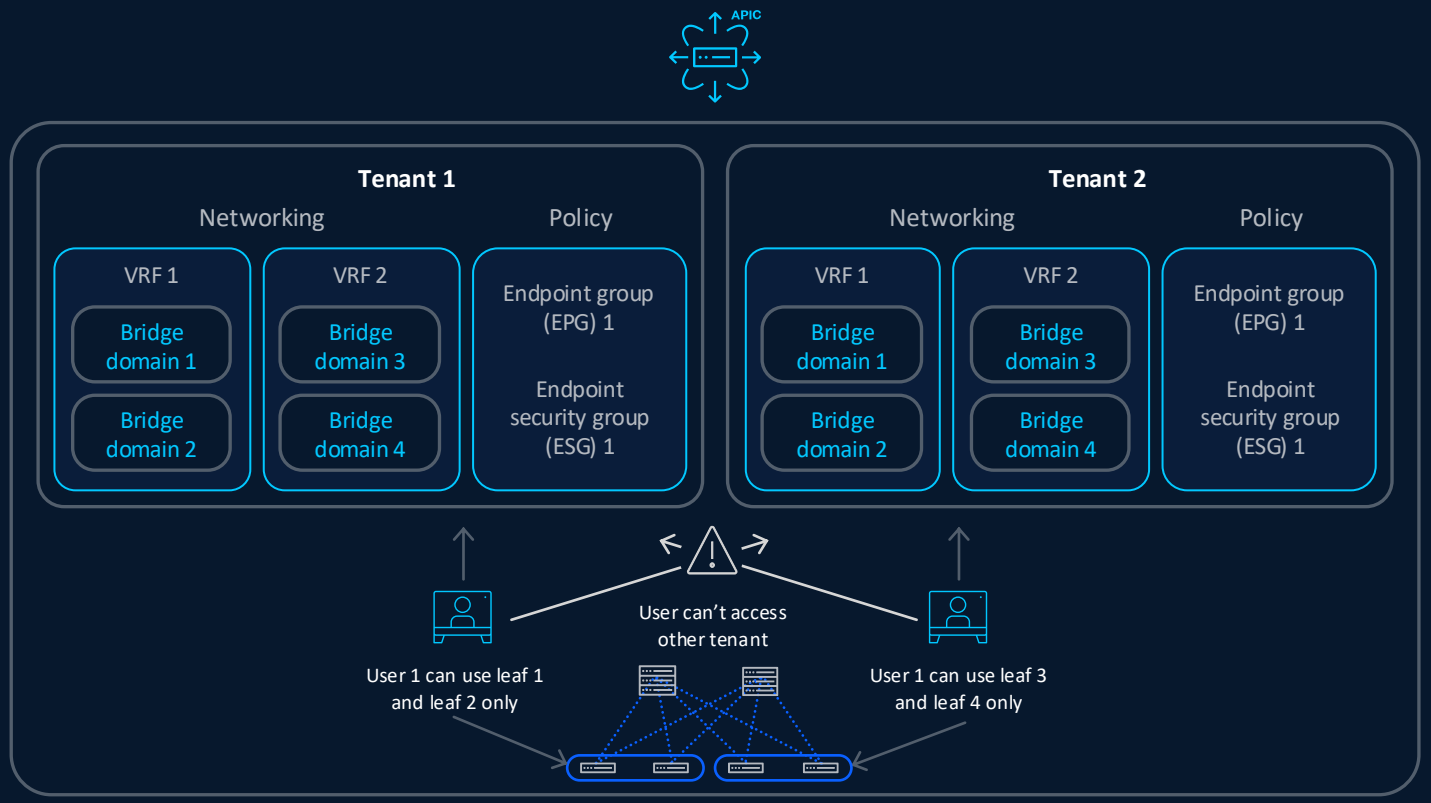


Cisco ACI

Administrative multitenancy and distributed security model

Build a true administrative boundary

Public cloud-like tenancy in an on-premises data center



What are tenants in Cisco ACI?

Tenants create a grouping of network and policy constructs based on an administrative boundary.

Within a tenant, VRFs (private networks) provide traditional routing table (forwarding) isolation.

Why tenants?

To realize enterprise-specific business outcomes associated with administrative separation.

Benefits

Separate virtual network fabrics aligned to organization	Limit impact of human error with smaller failure domains	Administrative separation in addition to traditional VRF isolation

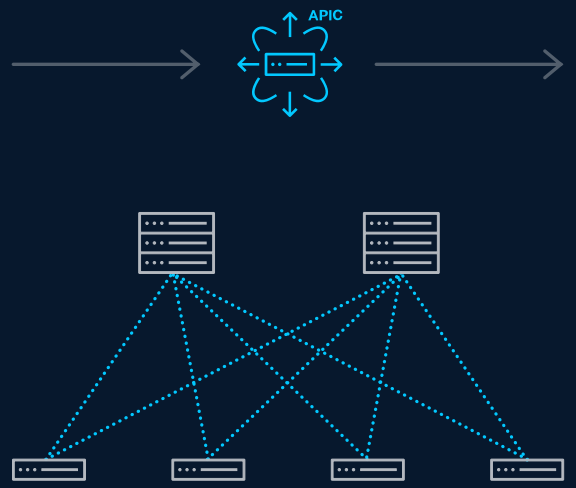
Cisco ACI’s pervasive security model

Microsegmentation across workload and network boundaries

Workloads

- Bare metal
- Virtual machines
- Containers

Cisco ACI® admin



Segmentation

Application components	Application groups	Application zones
App group	Sales apps	Dev zone
DB group		Test zone
Web group	HR apps	Prod zone

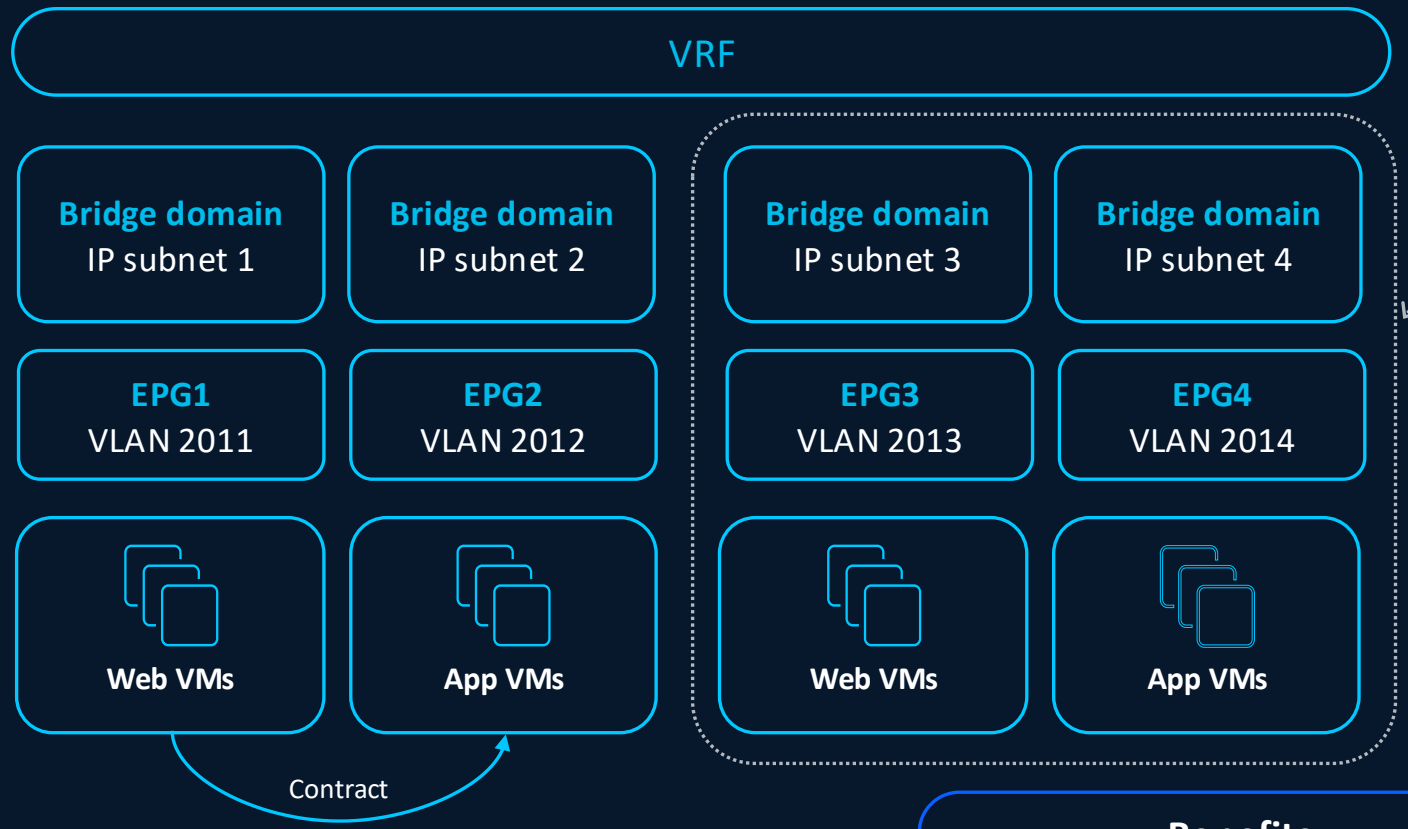
Enforcement

Benefits

- Bare metal, VMs, and containers in a single security grouping
- Build security policy based on application criteria
- Security grouping membership across entire data center

Cisco ACI’s pervasive security model

Creative use cases to match patterns of business activity with endpoint security groups (ESGs)



Business outcome: ESG as a container for all workloads that comprise a single application

ESG 1
All workloads in application A

ESG 2
All workloads in application B

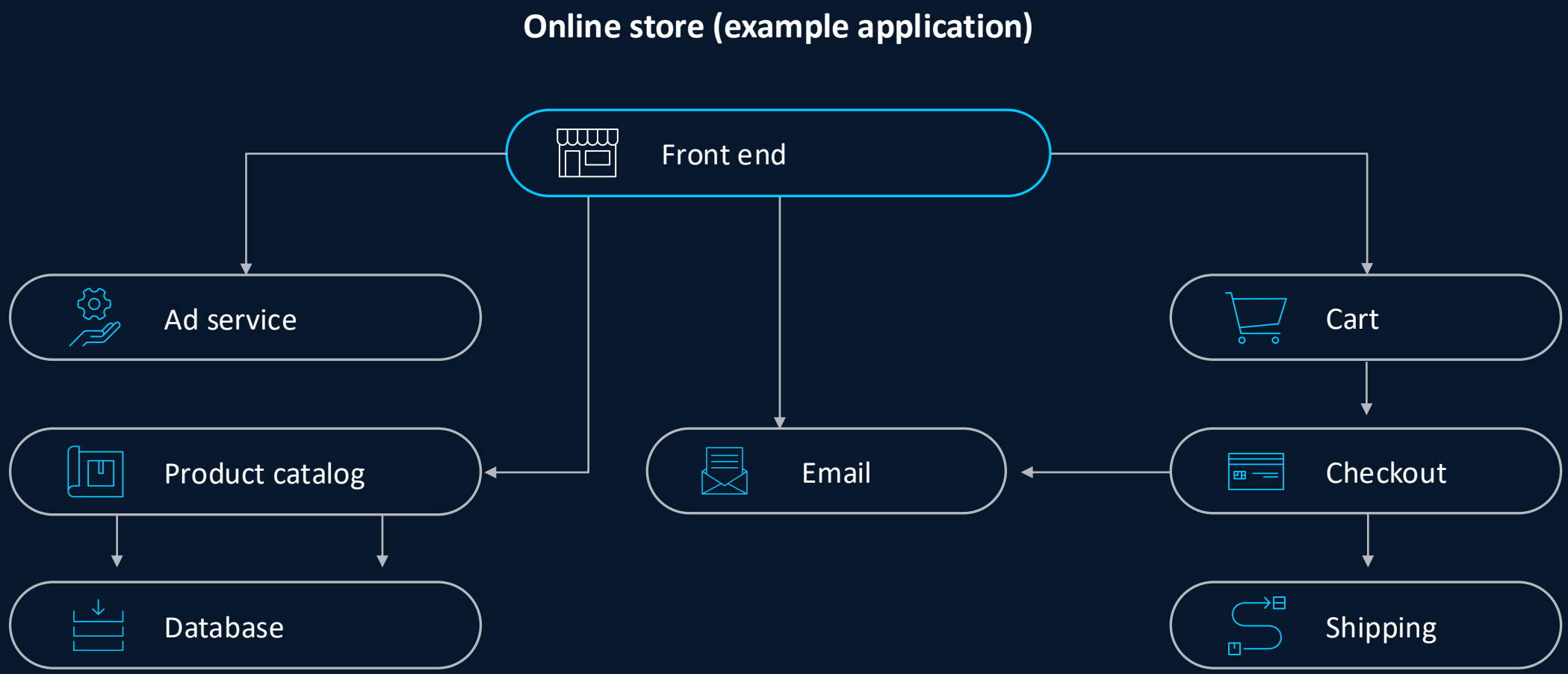
Business outcome: ESG as a container for all malware-infected hosts

ESG 3
All systems infected by malware

Benefits

- VRF-wide security construct, unconstrained by IP subnet or Layer 2 boundary
- Single security construct to hold bare-metal, VM, and container workloads
- TCAM optimization for policy enablement; no contracts required

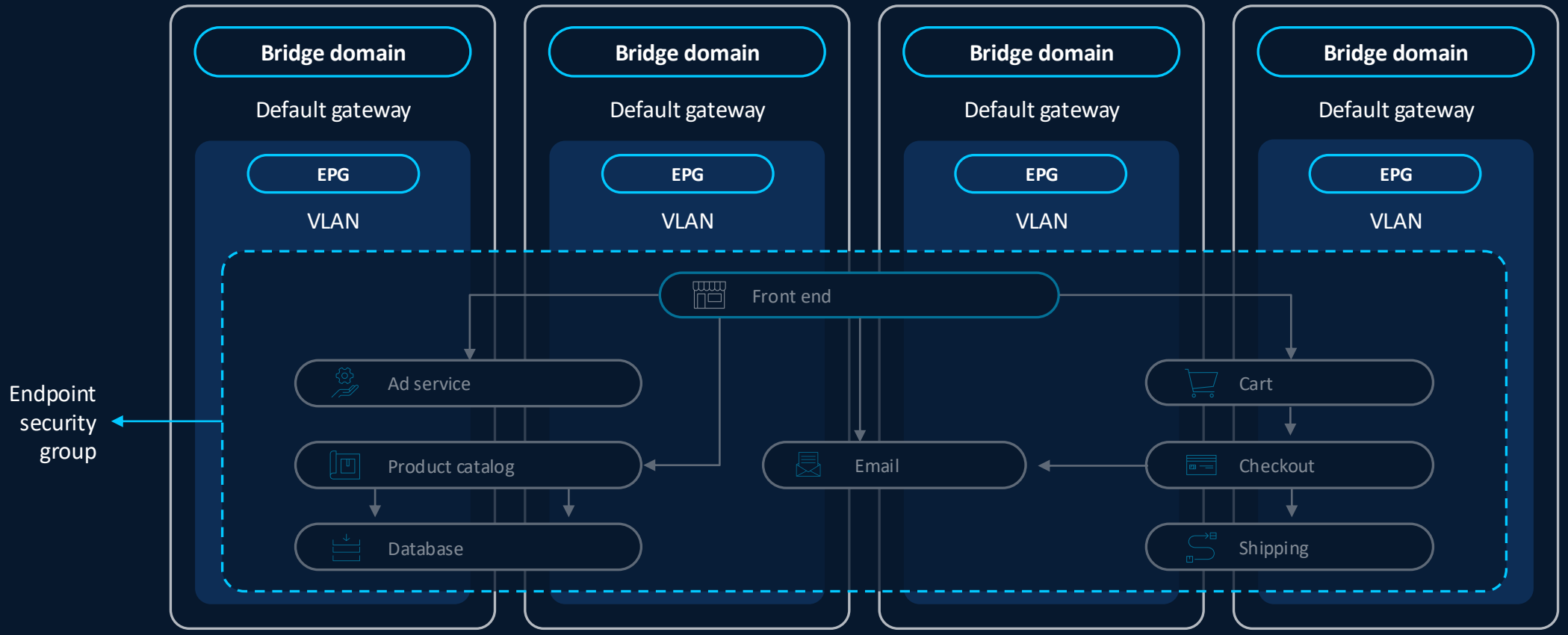
How do developers “see” the application?



How do network engineers “see” the application?

Cisco ACI’s pervasive security model

Network operators finally have a seat at the InfoSec table and the compliance table



Benefits

- One security bucket for containers, VMs, bare metal, and appliances
- Prepare network operators for audit, compliance, and conformance activities
- Optimize day-2 remediation with application layer visibility

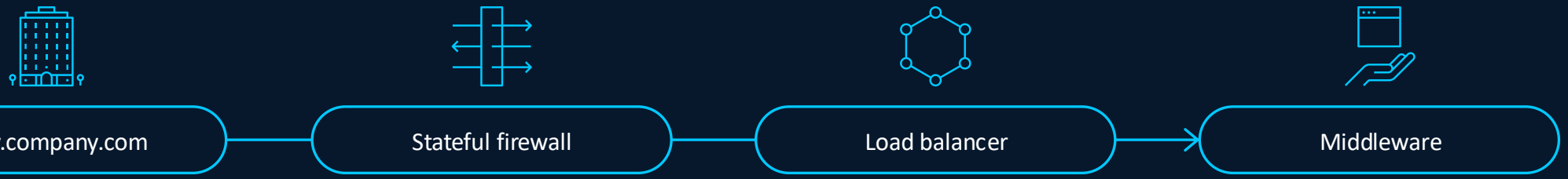
Cisco ACI

Application-aware service chaining

Cisco ACI application-aware service chaining

Different forwarding treatment for different flows in a three-tiered web application

Flow 1: Requires stateful firewalling (compliance) and load balancing (availability)



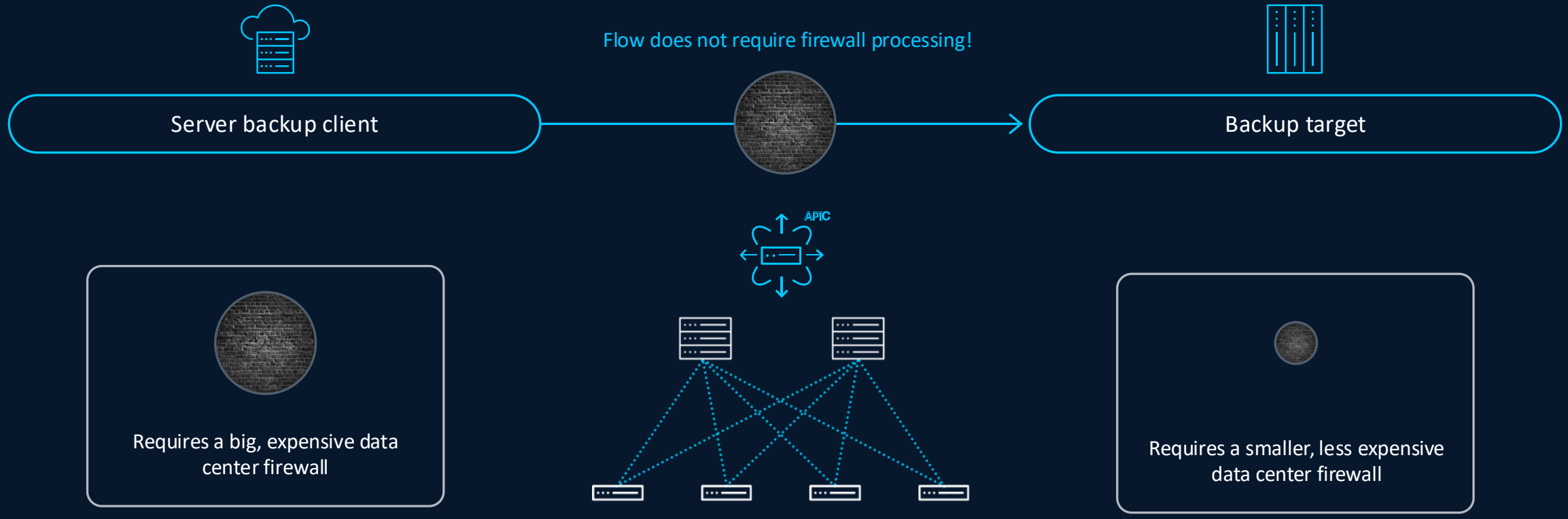
Flow 2: Does not require stateful firewalling or load balancing; requires ultra-low latency (performance)

Benefits

Redirect specific flows based on business requirements	Offload traffic from expensive firewalls and load balancers	Decouple appliance placement from routing table	Forward traffic based on compliance and performance

Cisco ACI application-aware service chaining

Common data center dilemma: Bulky server backup traffic overloads firewall



Benefits

Remove firewalls from flow path using application-aware service chains

Right-size firewall and IP services appliances

Cisco ACI

Virtualization and Virtual Machine Manager (VMM)

Cisco ACI server virtualization integrations

A seat at the compute table for network operators

Cisco ACI®

Orchestration

VM metadata

Visibility

Configuration

Single operator for end-to-end networking constructs

vmware

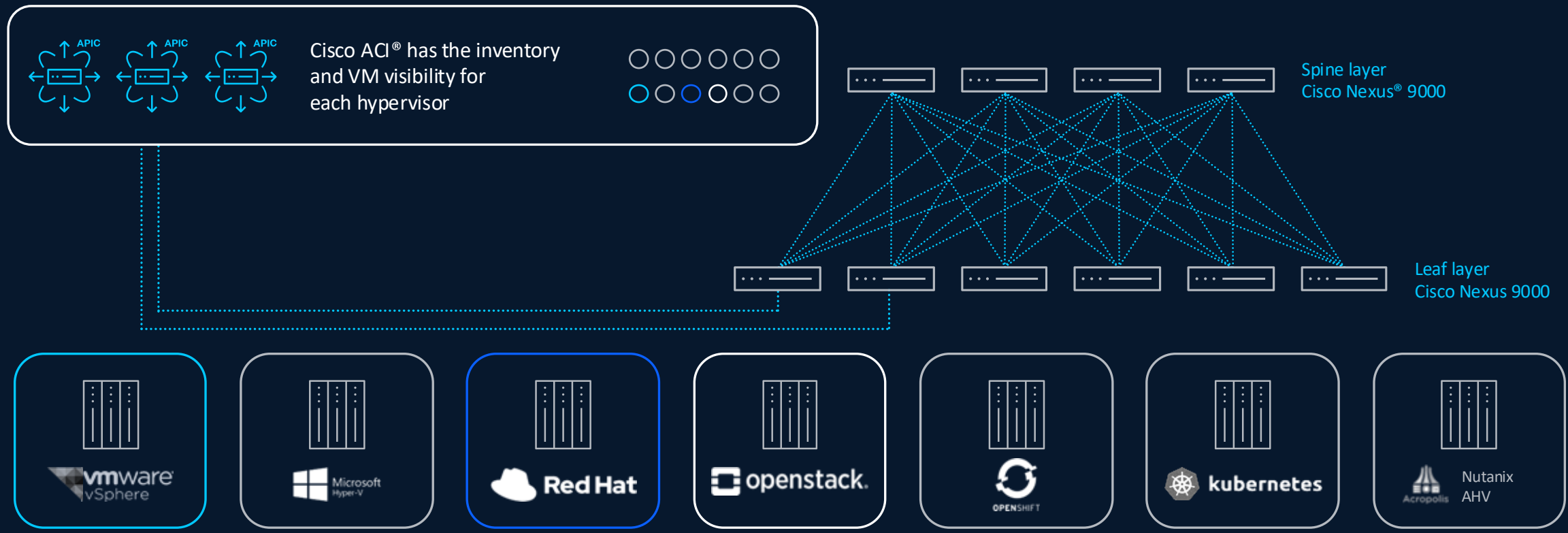
Hypervisor

Benefits

Unifies compute and network teams	Segmentation and ACI policy in the hypervisor	Cisco team does the API integration work for you	Stays current with Cisco ACI and hypervisor software versions

Cisco ACI VMM integration

Cisco ACI: Single SDN for physical and virtual networking



Benefits

Policy-driven integrated network (physical/virtual)	Segmentation and ACI policy in the hypervisor	Dynamic endpoint discovery and policy enforcement	Deep infrastructure visibility and telemetry

Cisco ACI

Automation

Cisco ACI: A platform built for automation

Simplicity and speed: A single API call to deliver a data center-wide construct (like a VRF)

ANSIBLE

HashiCorp Terraform

Day 0

Out-of-the-box automation with zero-touch provisioning

- Hardware
- Fabric
- Underlay
- Parts of overlay

Day 1

Operations ticketing queue

ServiceNow ticket – create VRF

Ansible | Terraform | Python

APIC API

Hundreds of Cisco Nexus® 9000s and thousands of ports

Benefits

Provision, automate, and operate the ITOps lifecycle	Cisco ACI® fabric is automatically deployed based on Cisco best practices	Avoid hundreds of design decisions required with traditional fabrics

RedHat Ansible and HashiCorp Terraform with Cisco ACI

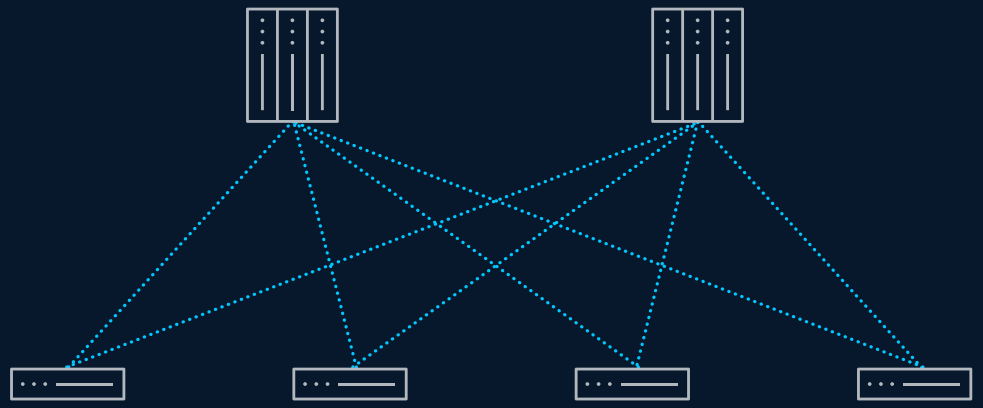
Leverage Cisco ACI's object model and API to distribute networking intent to hundreds of Cisco Nexus 9000s and thousands of ports

ANSIBLE

140+ Ansible modules for Cisco ACI®

HashiCorp Terraform

180+ Terraform resources for Cisco ACI



Benefits

Comprehensive coverage of Cisco ACI's REST API

Certified by RedHat and HashiCorp and supported by Cisco

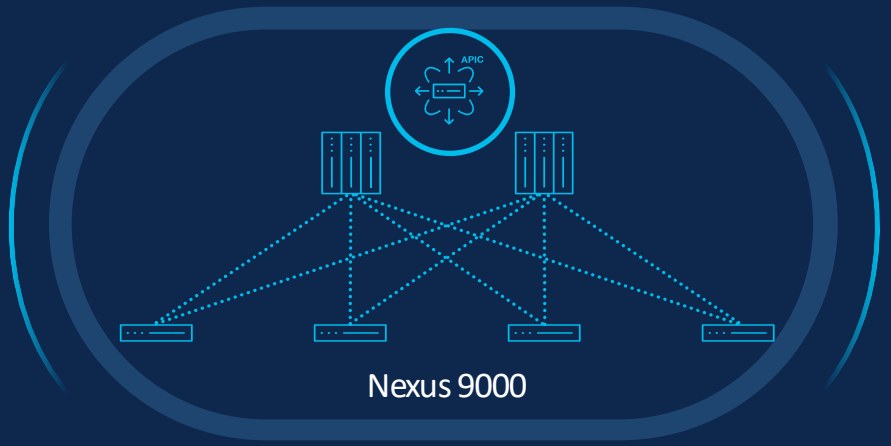
The foundation of an infrastructure-as-code practice

Cisco Nexus One Fabric

SDN Evolution

Cisco’s SDN Journey in the Data Center

Application Centric Infrastructure (ACI) – Industry’s first SDN solution



Launched in 2014

Significant Install Base of Customers

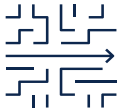
- Zero trust networking
- Turnkey automation
- Network-as-code
- Advanced services insertion

Cisco contributes innovations to the industry via Standardization

ACI innovations are standardized in IETF

Data plane

Control plane



Policy plane

With VXLAN EVPN

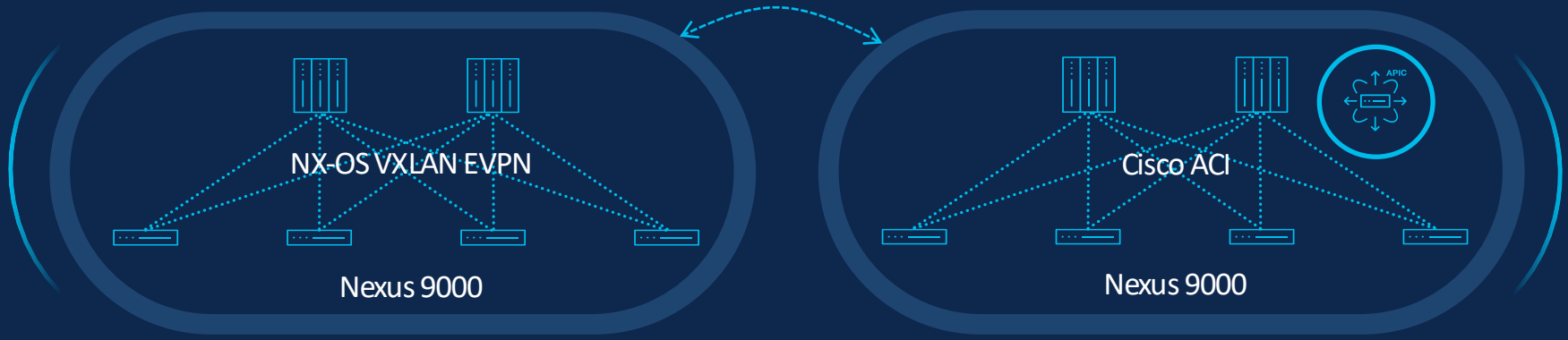
Cisco Nexus One Fabric

Unified management plane

Unified policy plane

Unified control plane

Unified data plane



Unified fabric architecture using Open NEtworking standards

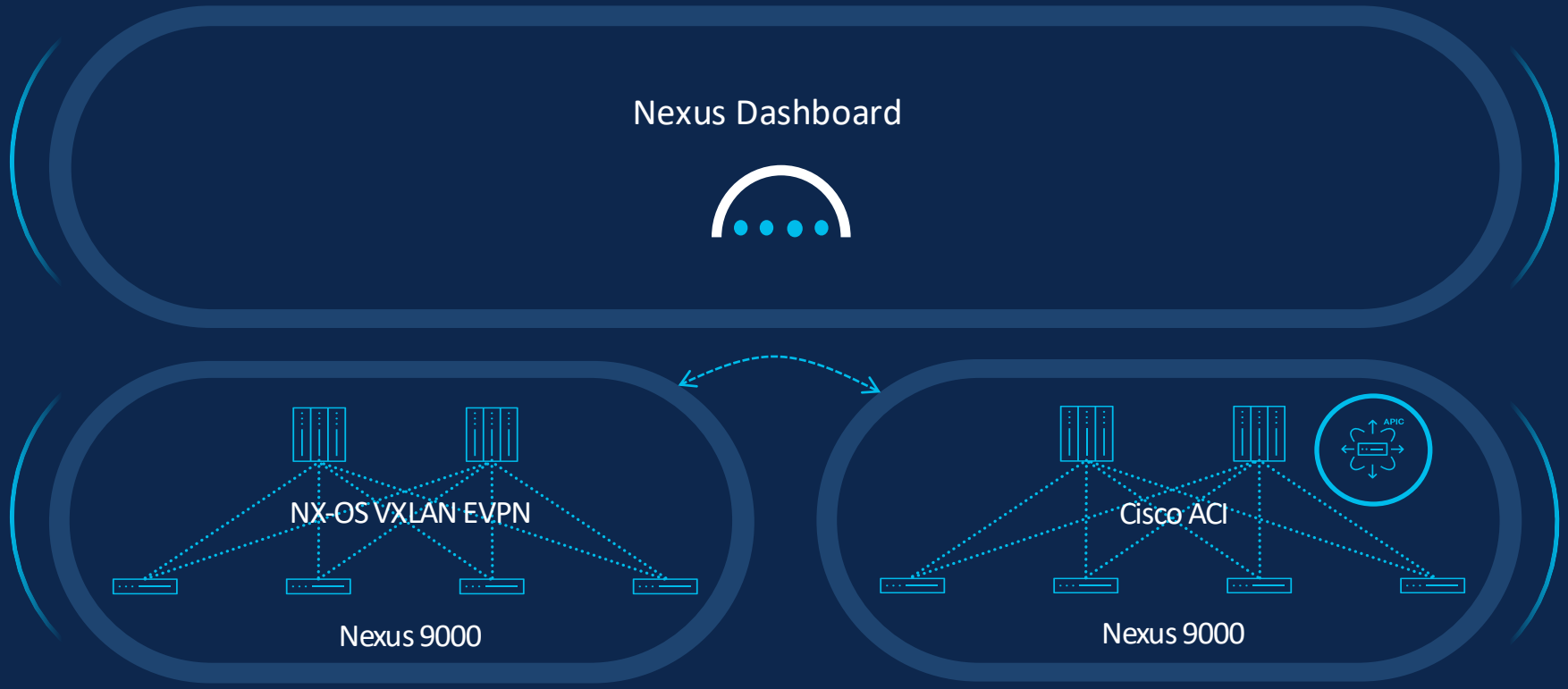
Desired fabric outcomes consistent across fabrics

1. Zero trust networking and microsegmentation
2. Advanced service chaining and service redirection
3. Administrative multitenancy
4. Standards-based interoperability with third-party networks
5. DevOps-ready APIs

Solution Components of Nexus One Fabric

Delivered via Nexus Dashboard

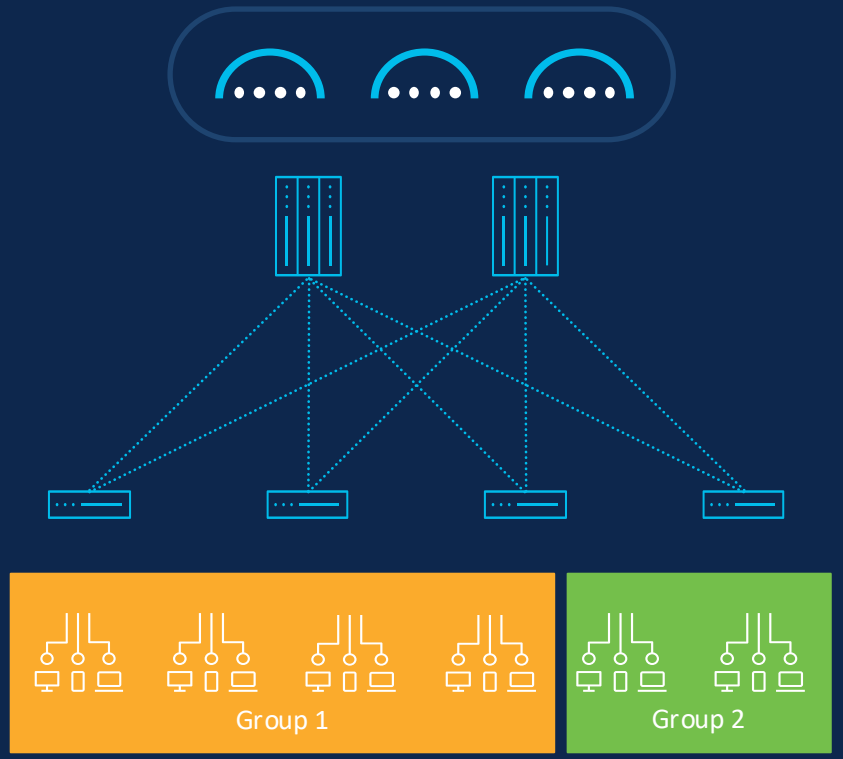
Nexus Dashboard as single point of control and operations



Flexibility of deploying either NX-OS or ACI and drive consistent fabric outcomes

Product Innovations

Microsegmentation for VXLAN fabrics



Grouping

- Classify endpoints to create groups
- Based on IP, VLAN, Port+VLAN
- Based on VM attributes

VXLAN GPO

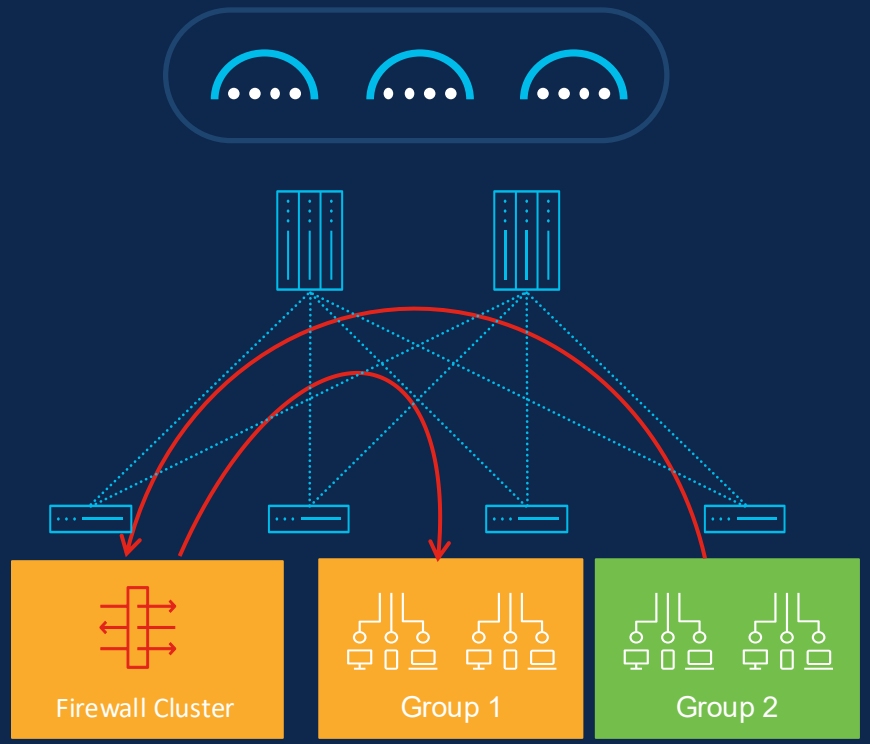
- Group Policy Option carried in standard VXLAN header
- Based on IETF draft-lrss-bess-evpn-group-policy
- Extension to VXLAN that allows policy enforcement
- Backward compatible

Microsegmentation using GPO

- Ability to segment east-west traffic
- Smaller attack surface and better security
- Flexible security isolation

Automate using Nexus Dashboard or Open APIs

Policy-based service chaining



Service chaining based on groups

- Redirect specific traffic based on policy
- Intra-subnet and intra-gr

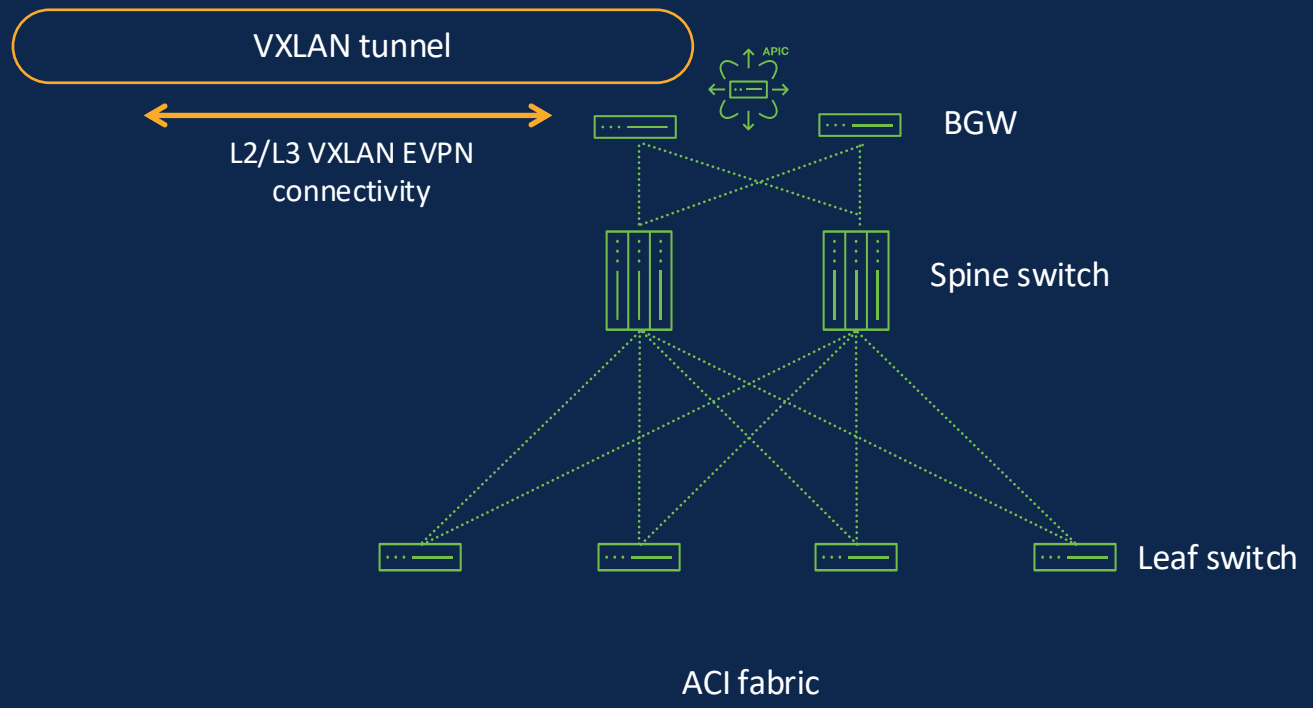
Scale easily

- Symmetric PBR
- Resilient hash PBR

Automate using Nexus Dashboard or Open APIs

Standards-based ACI VXLAN EVPN Gateway

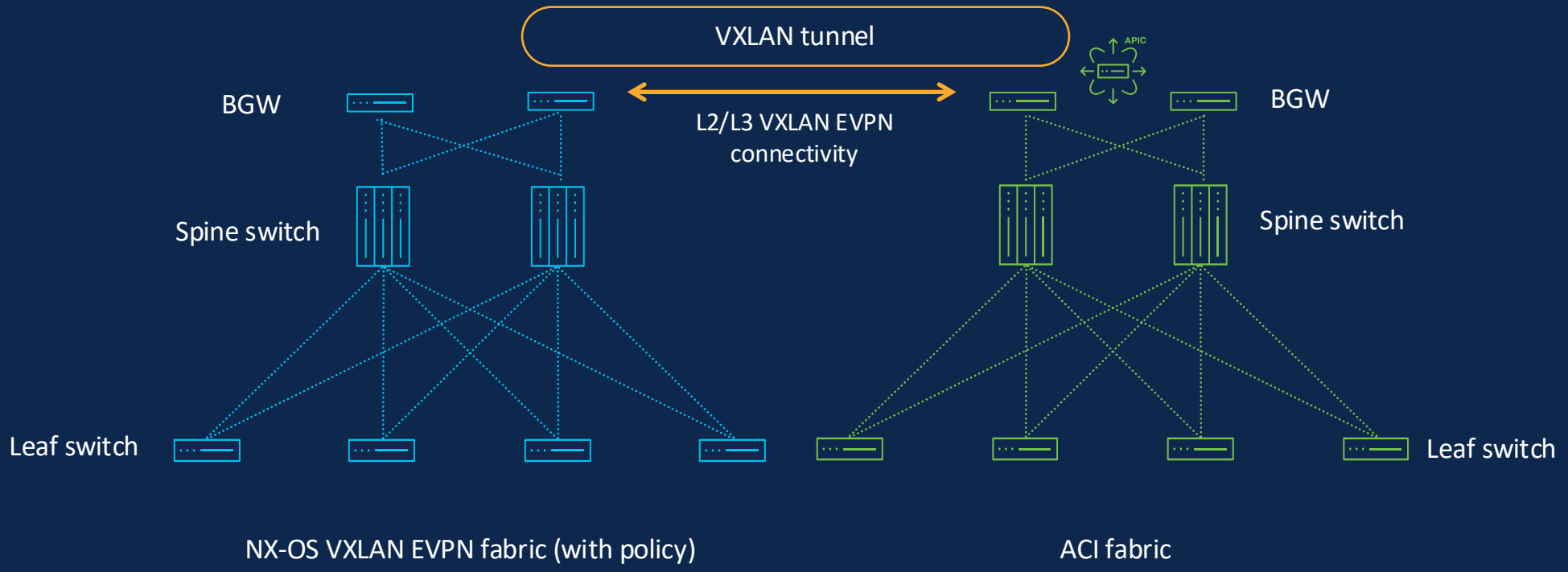
- Dedicated Gateway nodes (BGW)
- Single MP-BGP EVPN session (inter-AS like)
- iVXLAN <> VXLAN translation at Gateway
- Normalized or Translated Namespace (VNID, PCTAG)
- Layer 2 and Layer 3 extension
- Seamless host mobility



Border Gateways for standardized interconnect

Transport of L2/L3 and normalized Group IDs

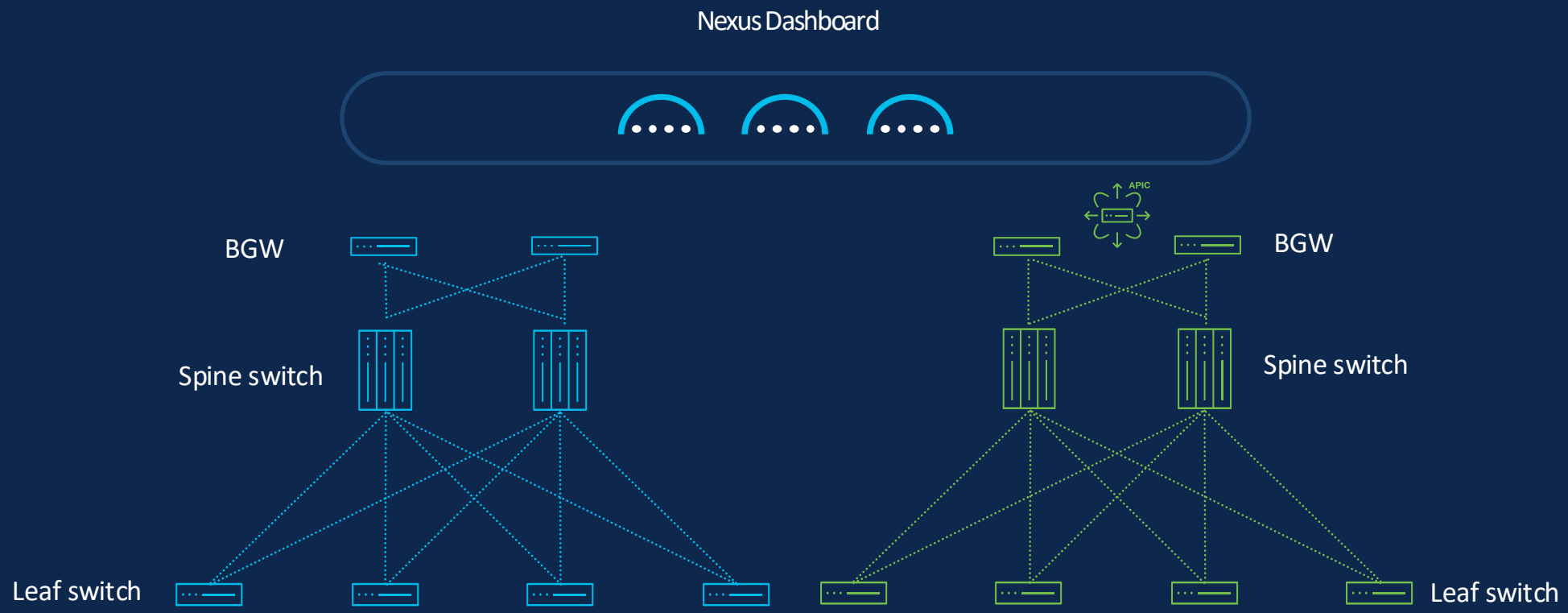
Interconnecting NX-OS VXLAN and ACI



Map EPG/ESG in ACI to Security Groups in GPO

Policy enforcement at Border Gateways

Nexus Dashboard as single point of control and operations



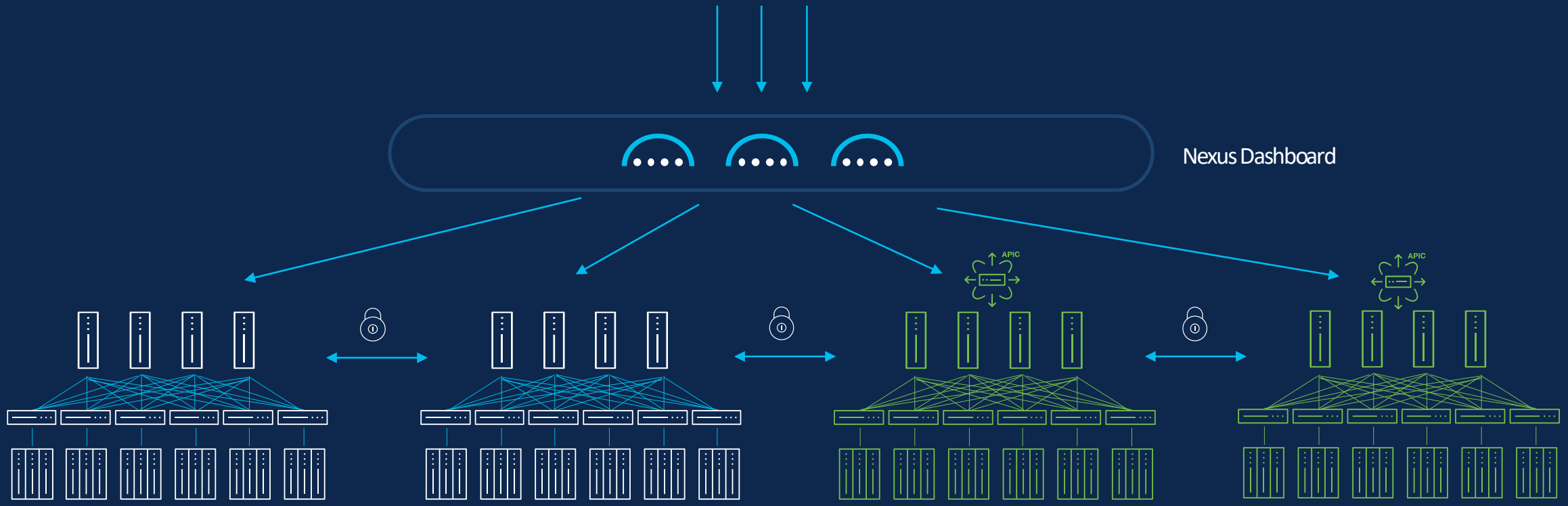
NX-OS VXLAN EVPN fabric (with policy)

ACI fabric

Different fabric architectures

Same outcome with common experience

And as an API gateway



Open Discussion

Securing the Data Center

Smart Switch and Live Protect

Fuse Security Into Networking

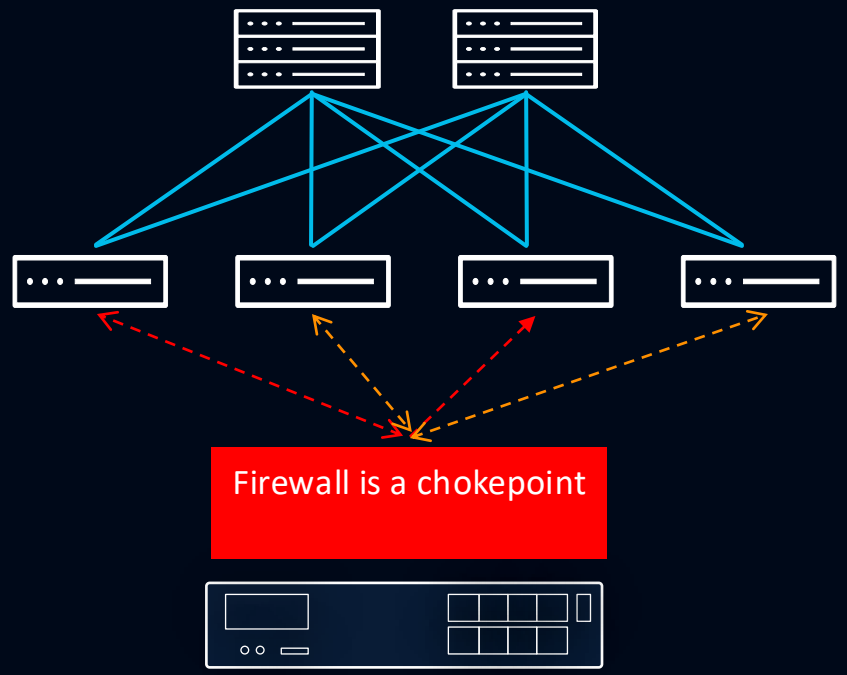
1. Traditional Data Center Security Limitations
2. Turn every switch port into an enforcement point
3. Continuous Runtime Defense

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

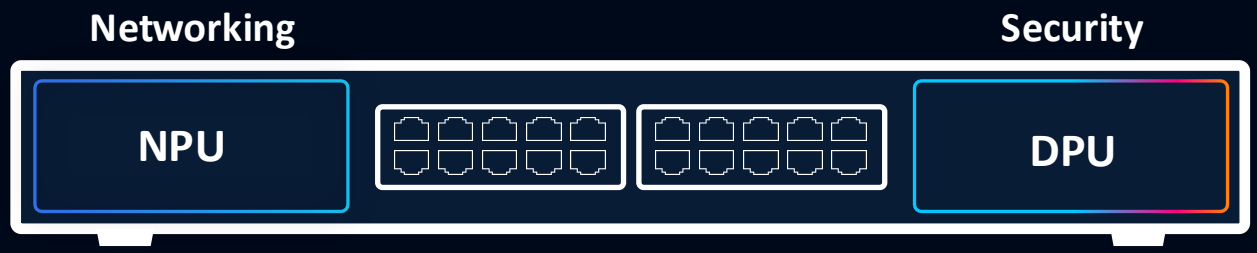
Fuse Security Into Networking

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 services

Shipping

N9324C-SE1U

24-port 100G, and 800G services

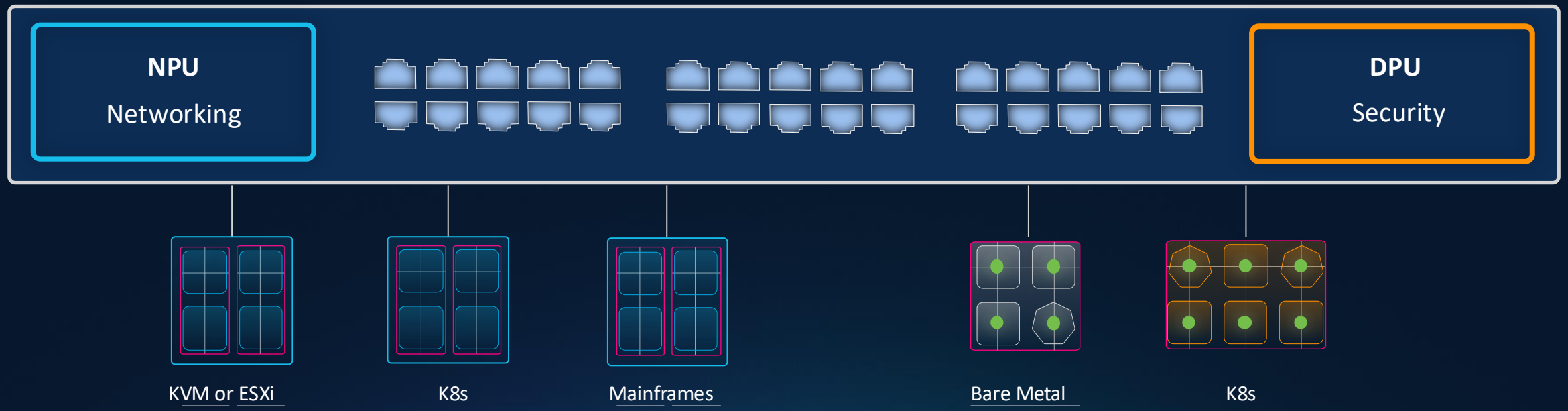
Shipping

Security Use Cases

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

Segmentation with Smart Switches

Turn every switch port into an enforcement point



Nexus Networking

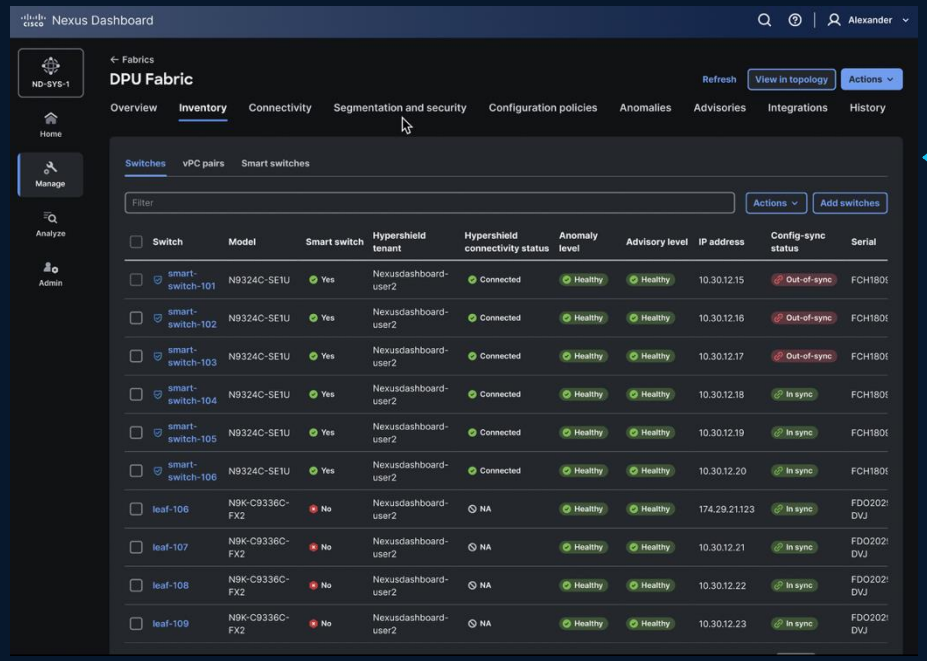
VLAN / VRF / VXLAN
Network context

Hypershield Security

800Gbps of stateful performance
Instant protection for new workloads

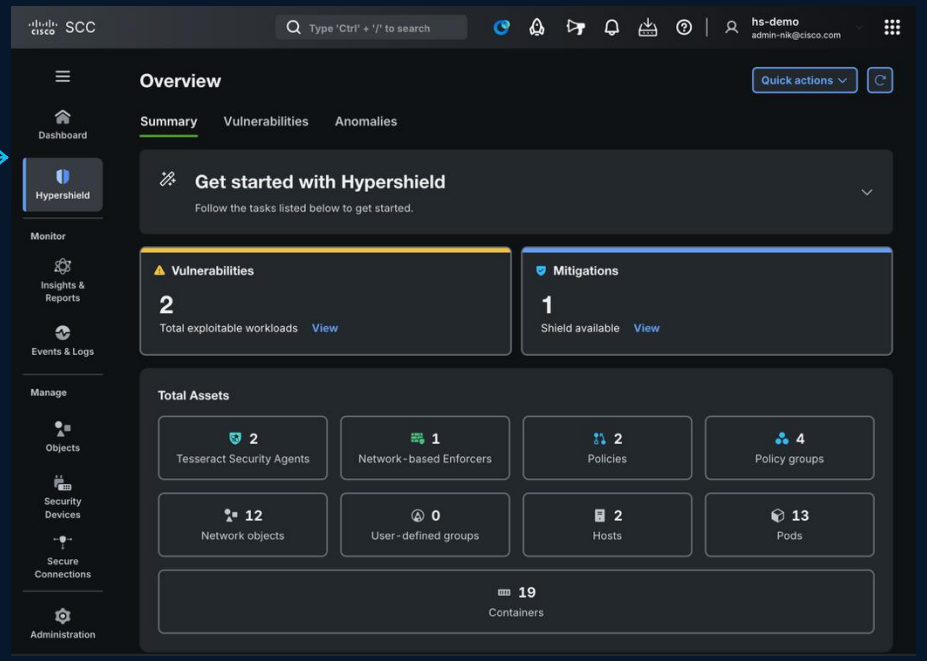
Separate Workflows for NetOps and NetSecOps

Nexus Dashboard, NX-API, NX-CLI



Context sharing for troubleshooting

Hypershield On-Prem Controller



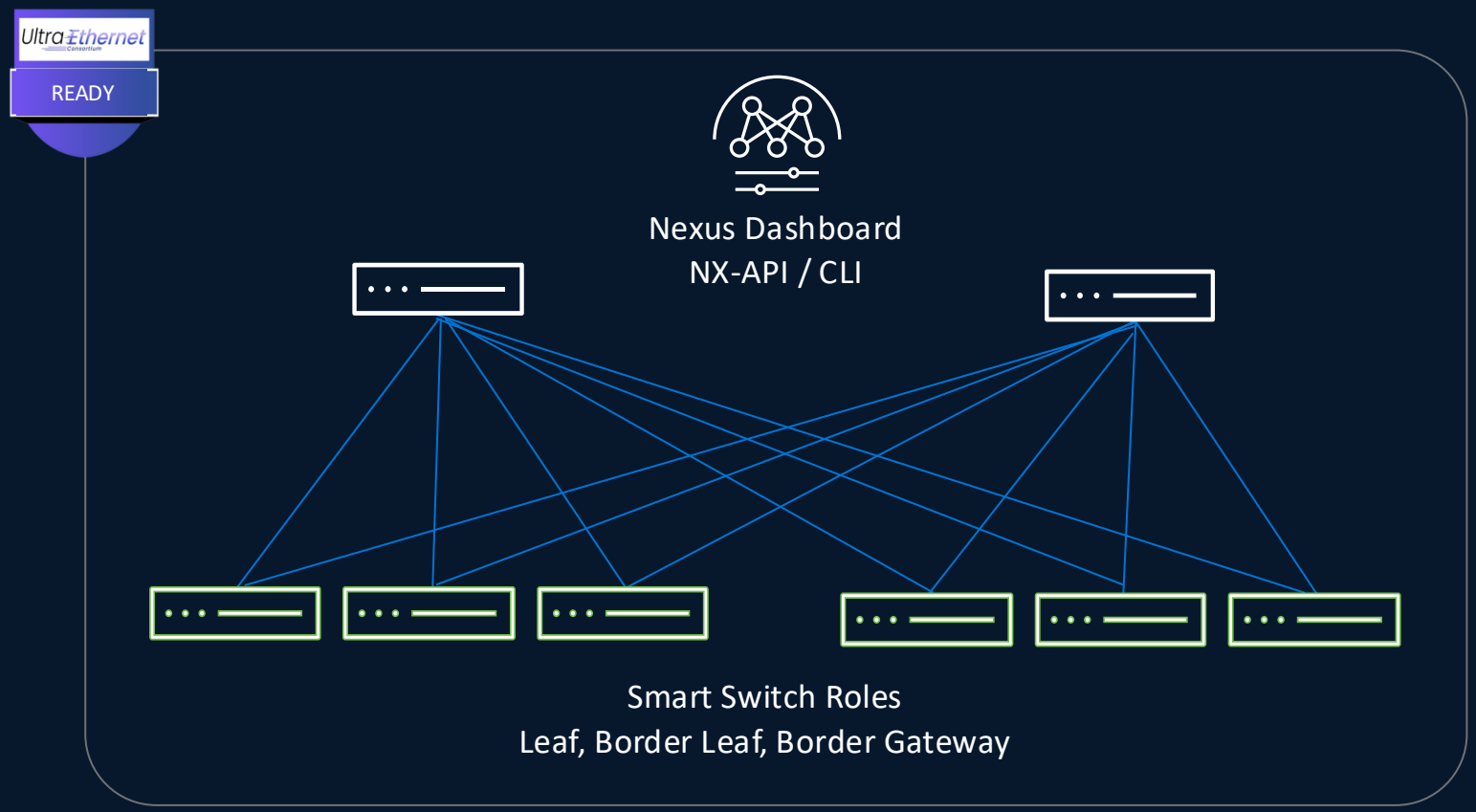
NEXUS SMART SWITCH

Use Cases

Top of Rack: Network Mode Use Case

Ideal for New Fabrics and EOL Refresh

Available Now



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

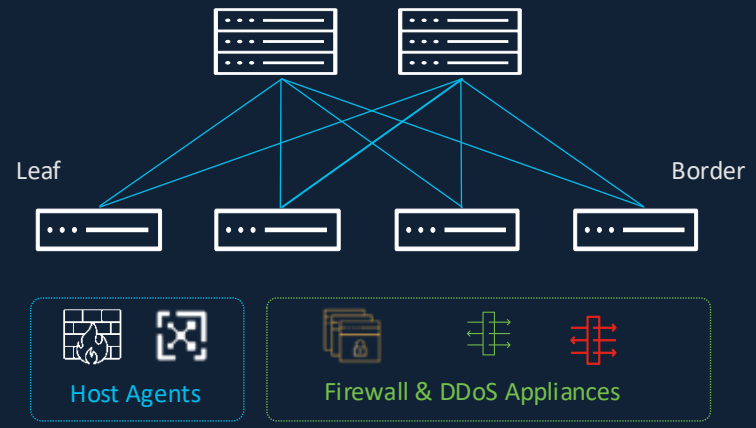
Top of Rack: Stateful L4 Segmentation

NXOS Fabric Use Cases

Currently under Controlled Availability

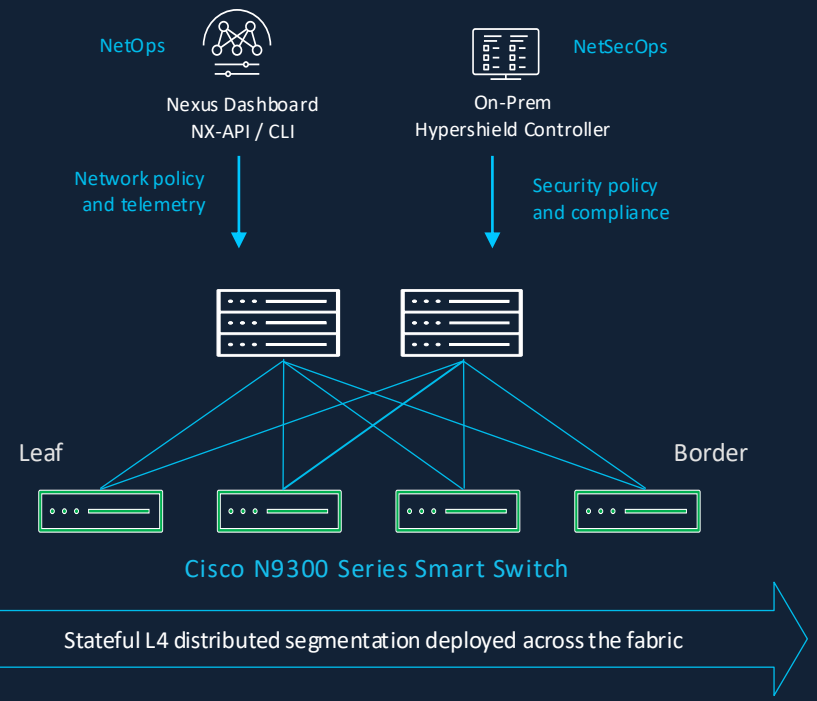
Security "Attached" to Network

- 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

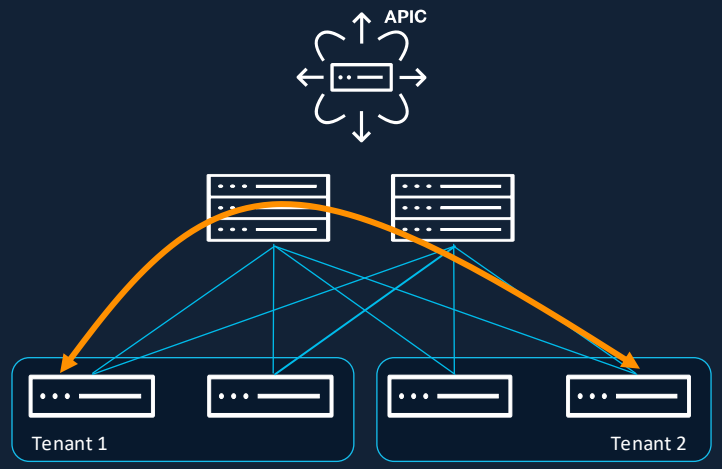
ACI Fabric Use Case

Currently under Controlled Availability

Zone Segmentation

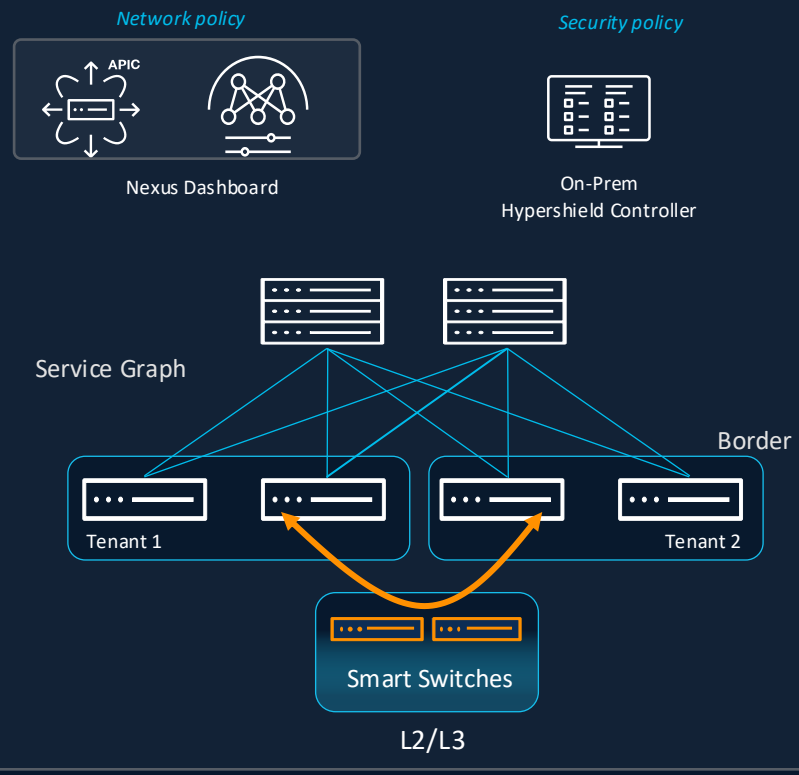
ACI Stateless Network Segmentation

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



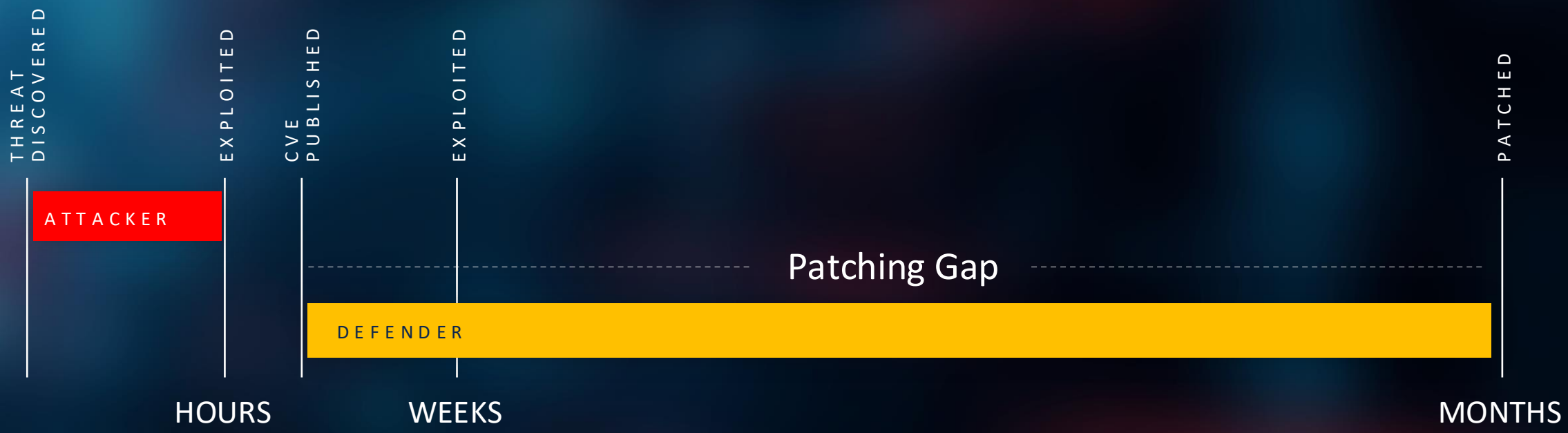
Stateful Zone Firewalling for ACI fabrics

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



Live Protect

Patching Vulnerabilities is Challenging



Is it running in memory?

Is it being exploited in the wild?

Is it a high value asset?

Live Protect

Vulnerability shielding for Cisco networking devices

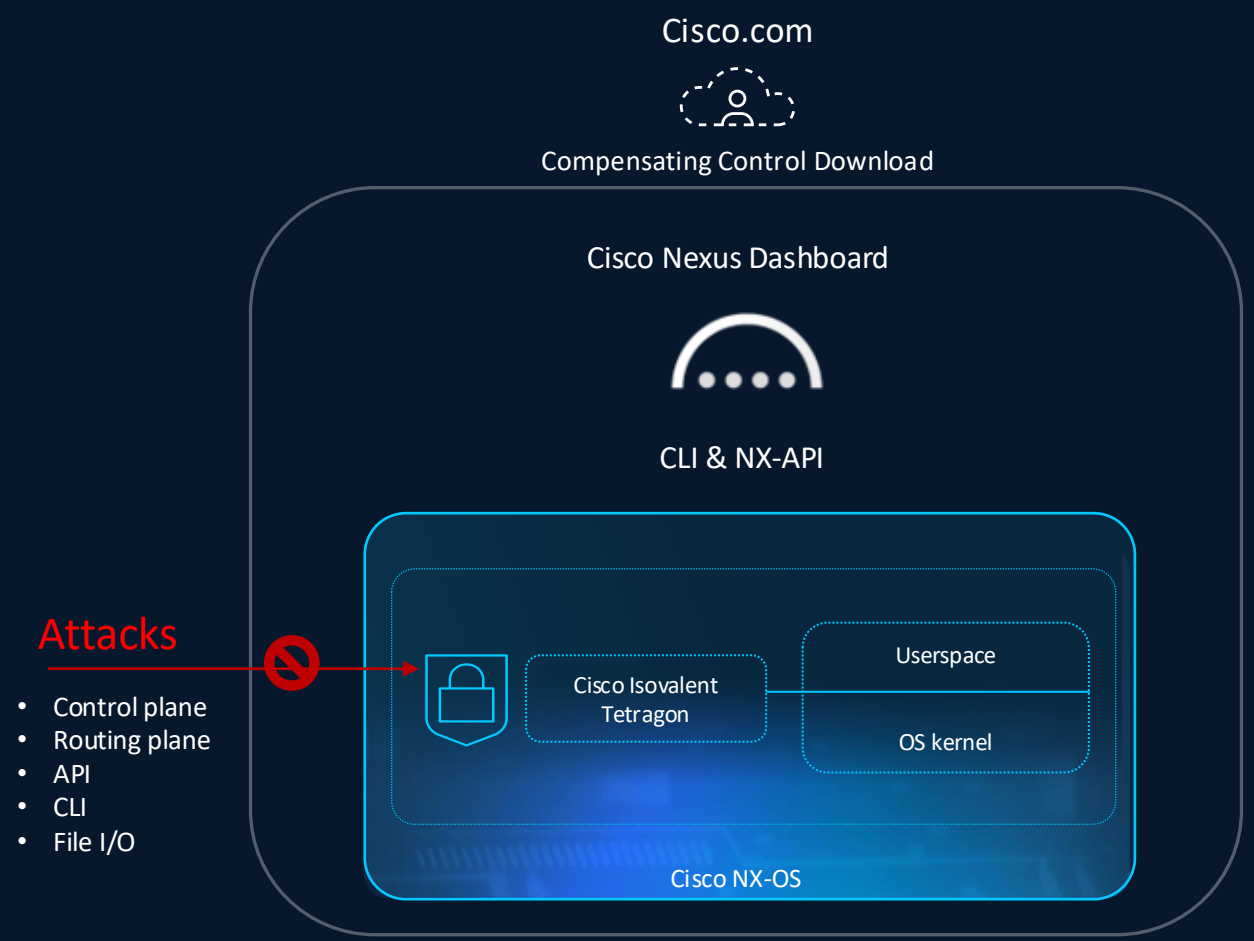
Stop the attack… but don’t stop the network.

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

Vulnerability Mitigation with No Downtime

Available Now

Live Protect for Nexus OS switches



Innovation

- Enterprise-grade Tetragon agent built into NXOS 10.6(1)F
- eBPF-powered security observability and enforcement
- First to market (no equivalent from Arista, Juniper, Aruba, etc.)

Customer workflow

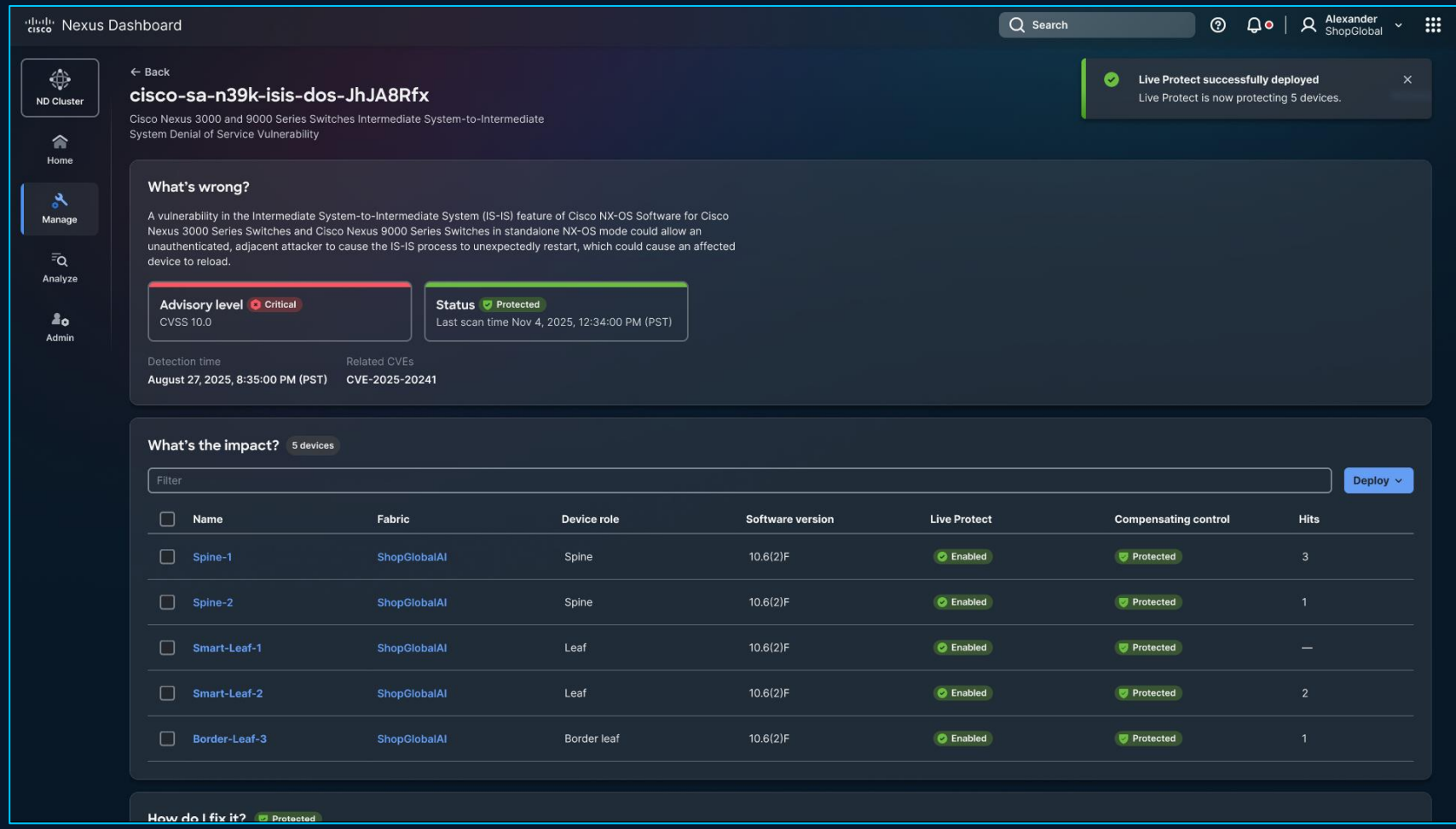
- Policy file (shields) delivered as a signed RPM available on cisco.com
- Download and apply SMU to the switch (Enforce or Monitor mode)
- Collect metrics, events, logs, and traces
- Export Tetragon events to Splunk or other SIEMs
- SMU automatically removed with PSIRT-bundle upgrade

Ease of use

- Available with essentials or higher license
- Integrated Nexus Dashboard workflow
- API and CI/CD support for automation
- PSIRT upgrades during standard maintenance windows

Live Protect for Cisco Nexus switches

- CVE detect/mitigate workflows in Nexus Dashboard
- No software upgrade
- No downtime or reboots
- Export events to Splunk & other SIEMs
- API and CI/CD support



Live Protect Monitoring Mode

- Like ‘EDR’ for infrastructure
- Anomaly detection reported as NX-OS security events
- JSON telemetry export to Splunk/SIEMs
- Traces file access, syscalls, and network events
- Lightweight Isovalent runtime agent embedded in NX-OS

Live Protect supported Nexus platforms

Supported

Nexus Switch models - CloudScale and Silicon 1	Version
N9300 series fixed switches (24G or more RAM)	NXOS 10.6(2)
N9200 series fixed switches (24G or more RAM)	NXOS 10.6(2)
N9300 smart switches in network mode	NXOS 10.6(2)
N9400 series switches	NXOS 10.6(2)
N9100 series switch	NXOS 10.6(3)

Not supported

Nexus Switch Models – CloudScale and Silicon 1
N9000 End of Sale switches
N3000 and N3500 series switches
N9500 series modular switches
N9800 series modular switches
N9300 series switches (< 24G RAM)

Simplify and Unify
Data Center Network Operations

with Cisco Nexus Dashboard

Data Center Admin Reality Check - Expectations

Manage the network
(provision, configure, change)

Innovate and grow

Operate the network
(troubleshoot, fix, analyze)

Reliability, risk control,
brand, user experience

Data Center Admin Reality Check – Operational Challenges

Manual Workflows

Escalating MTTR

Skills Gaps

Compliance & Security Risks

Cross Domain Correlation

The Solution – Unified Nexus Dashboard

Provision
Once, deploy anywhere

Secure
One source of truth

Manage
One logical network

Analyze
Identify, troubleshoot, and fix faster

Physical or Virtual Cluster

Nexus

- Classic Ethernet
- VXLAN
- ACI
- IP Media Fabrics
- AI Fabrics
- Hypershield

Extensible to other networks

- Campus
- WAN/Transport
- Catalyst 8000
- CSR 1000v
- Virtual, Kubernetes & 3rd party Networks

MDS

- SAN

On-Prem, Cloud, Edge, LAN, or SAN— all managed from one place

Nexus Dashboard

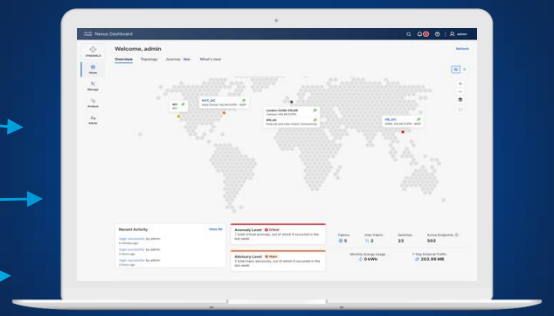
Cisco Nexus Dashboard 4.2

Nexus Dashboard Fabric Controller

Nexus Dashboard Orchestrator

Nexus Data Broker

Nexus Dashboard Insights



Nexus Dashboard 4.2

One stop shop for DC Automation & Visibility

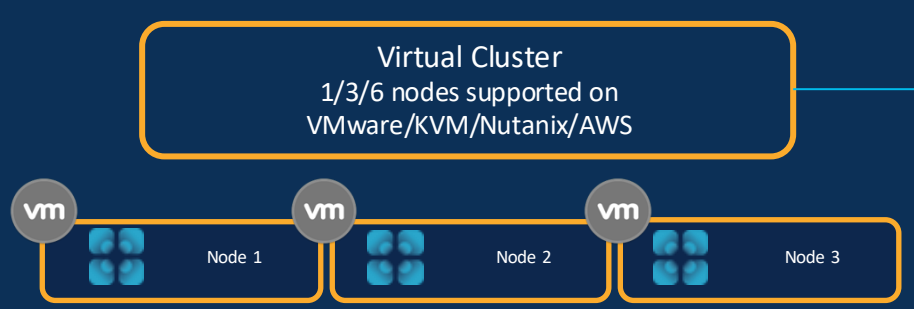
ACI, Nexus, MDS and Catalyst fabrics

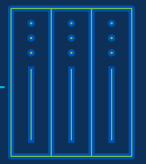
Available as 1/3/6 node clusters in physical or virtual appliance

Scale up & Scale out clusters

Available with all license levels (Essentials/Advantage/Premier

Scale & Flexibility with Cisco Nexus Dashboard



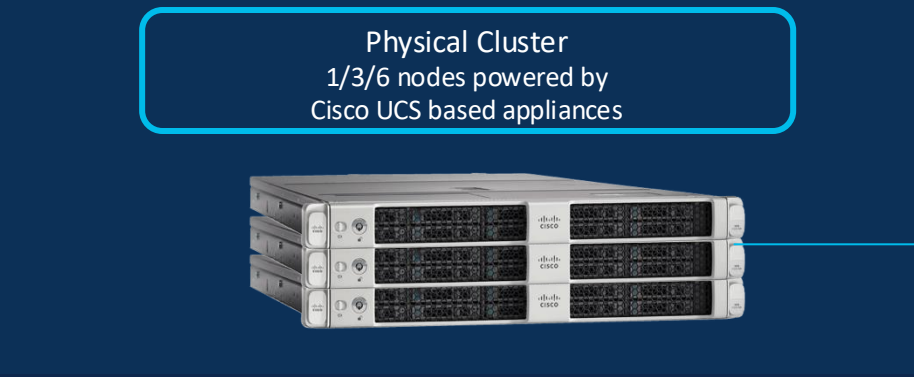


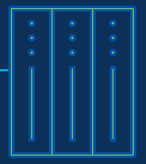
Up to 200 switches

Connect up to 12 ND Clusters

Multi-Cluster scale up to 4000 Switches

Single Pane of Glass for Operation Teams





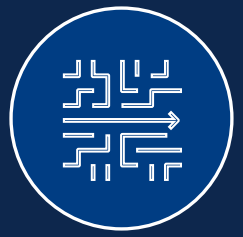
Up to 1000 switches

Provision

Consistent Fabric Provisioning

Build your Fabrics from scratch

Onboard existing fabrics for incremental operations



Consistent fabric builder for all types

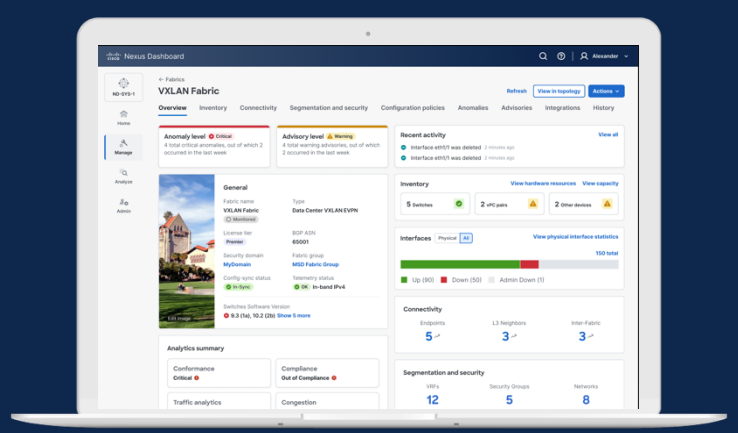
Best practice configurations

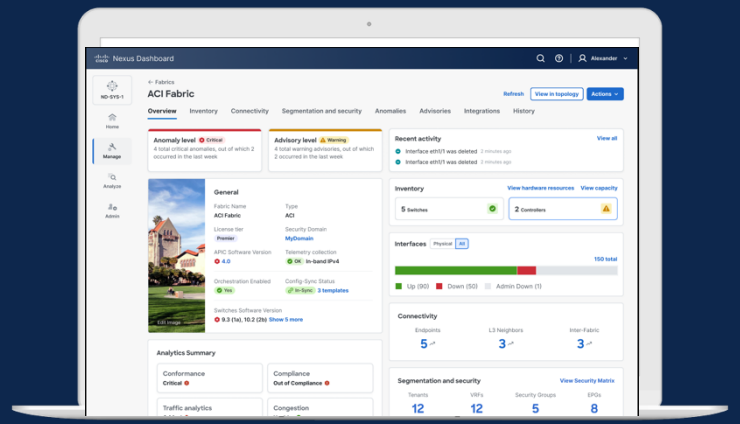
Configuration Compliance

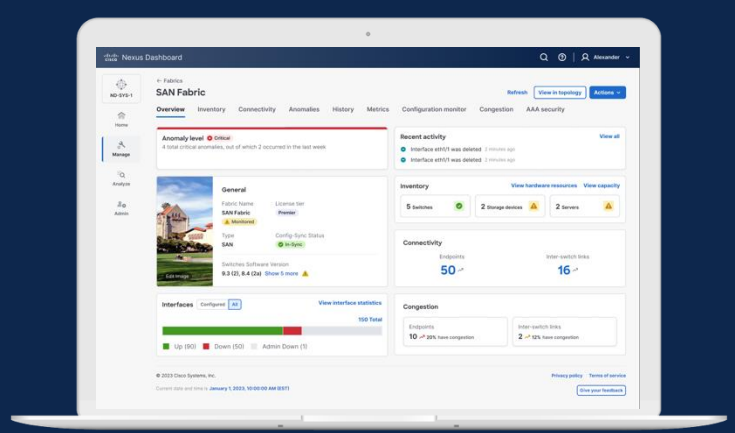
Day-n ongoing incremental & consistent configurations

Fabric Software Upgrades

One Solution to Manage DC Infra







LAN Fabrics

Cisco NX-OS: Zero-Touch Classic, VXLAN, IPFM, Data Broker, AI fabrics & more

Cisco Nexus, Cisco Catalyst and third party

Cisco ACI: Zero-Touch fabric with policy-oriented model[1]

Cisco Nexus 9000

SAN Fabrics

Industry leading SAN Analytics and end-to-end SAN management

Cisco MDS 9000

Consistent operational experience

Open APIs
with Ansible, Terraform

Operate multiple switches as one logical entity

[1] Requires external APIC cluster

Simplified Fabric Management

End-to-end fabric lifecycle automation that drives consistency, scale, and operational excellence

VXLAN
BGP EVPN fabrics for Nexus & Catalyst (IOS XE)

Classic
2- or 3-tier NX-OS architectures

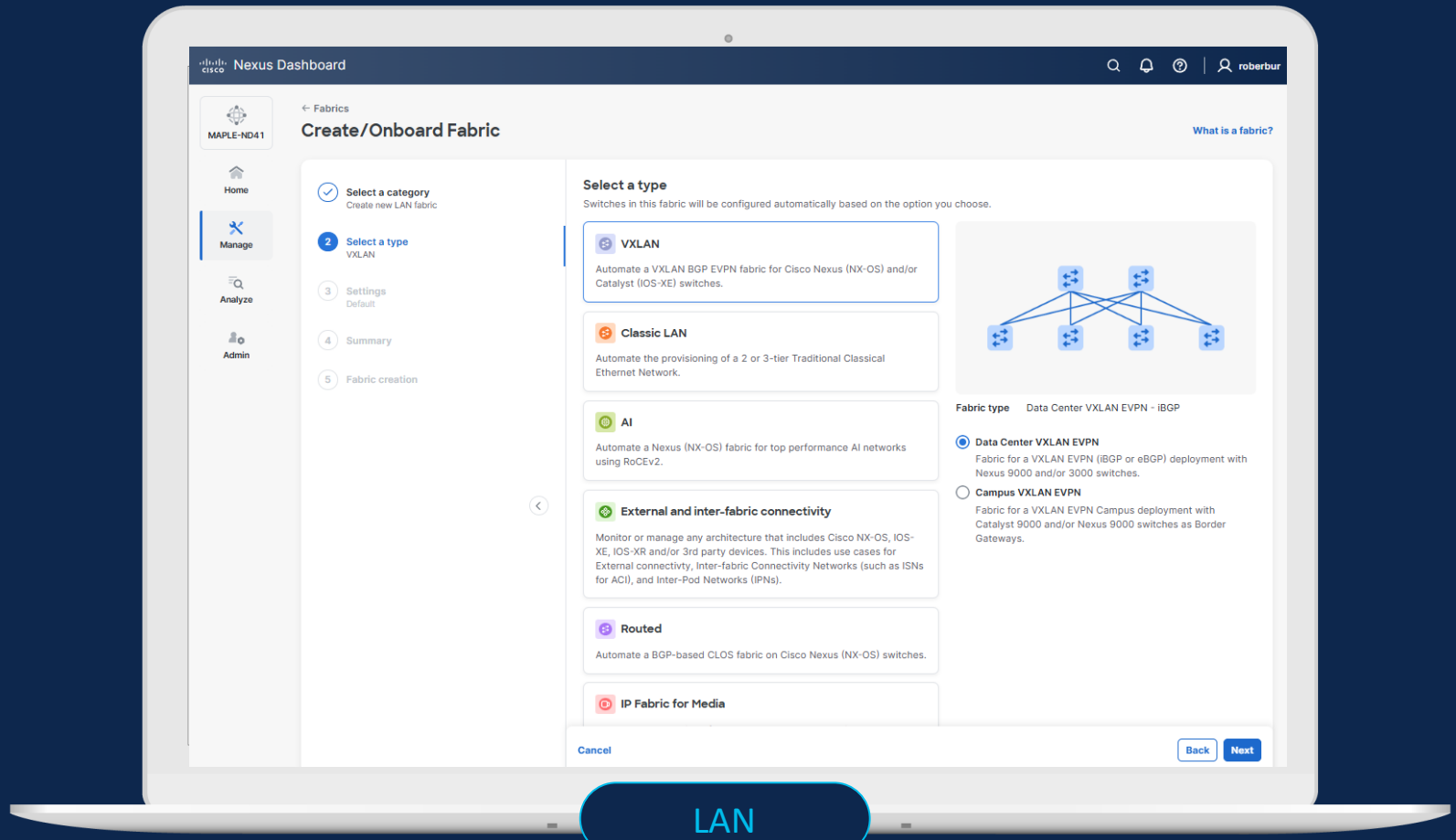
AI
Performance fine-tuned network provisioning to transport AI/ML apps with advanced visibility

External and Inter-Fabric Networks
NX-OS, IOS XE, XR, third-party networks mainly used to interconnect ACI, NX-OS, and Campus

Routed
BGP-based CLOS NX-OS fabrics

IP Fabric for Media
Fine-tuned network provisioning and monitoring for broadcasting and media

Data Broker
Automate the creation of Data Broker Fabric for TAP/SPAN aggregation



LAN

Benefits

Configure Once, Deploy Everywhere

Cisco Nexus Dashboard - Provision

Create or onboard a fabric

LAN

Add a seed switch

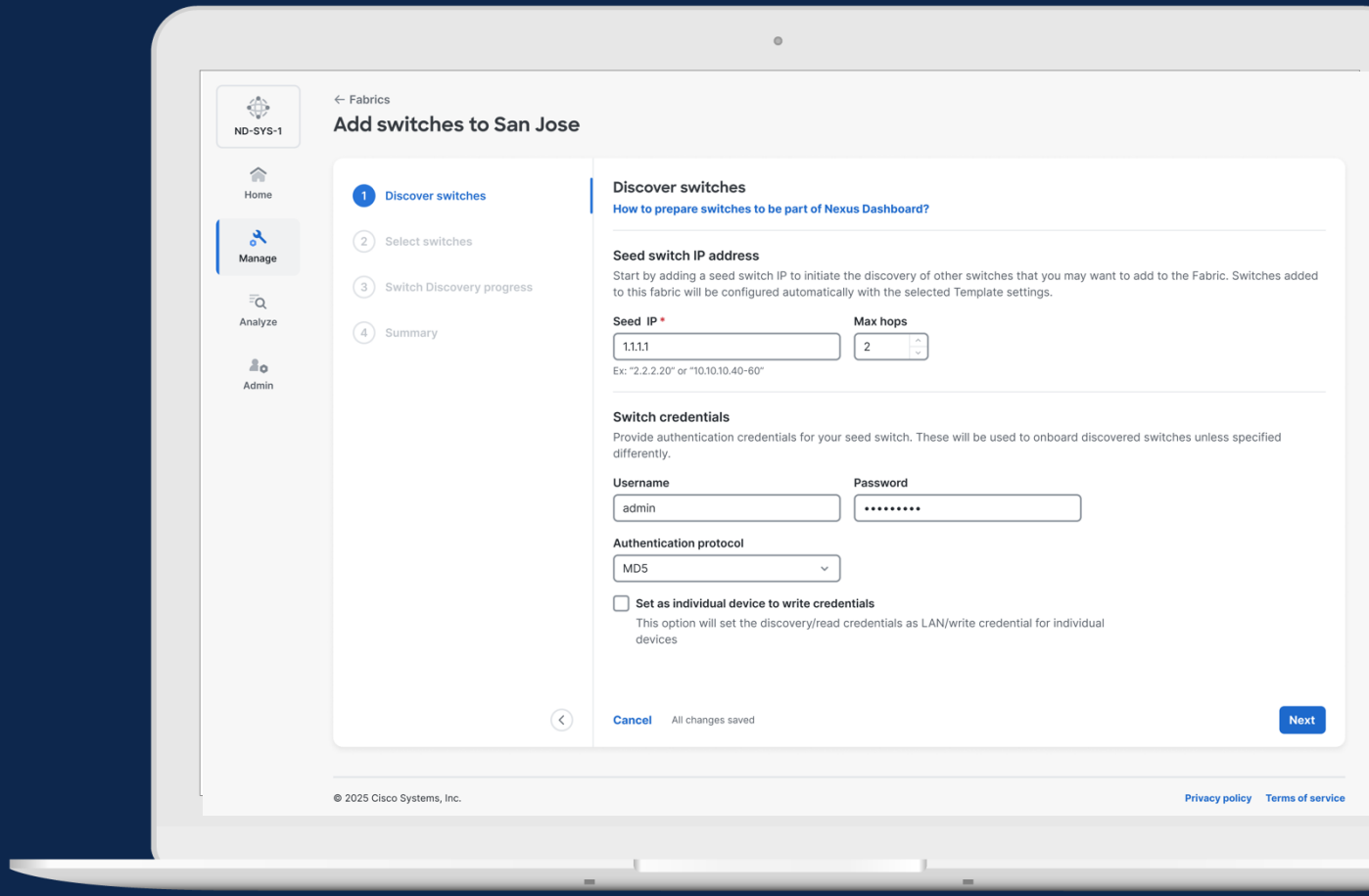
Nexus Dashboard will use it as an anchor point to discover other switches

Auto-discover connected switches

Based on the number of hops selected, making the onboarding process faster

Onboard them all at once

Assign a role to your switches and add them to your fabric in minutes



* Create fabric new UI displayed above scheduled for 4.0 (Q1CY25)

Cisco Nexus Dashboard - Provision

Create or onboard a fabric

AI

Add a seed switch

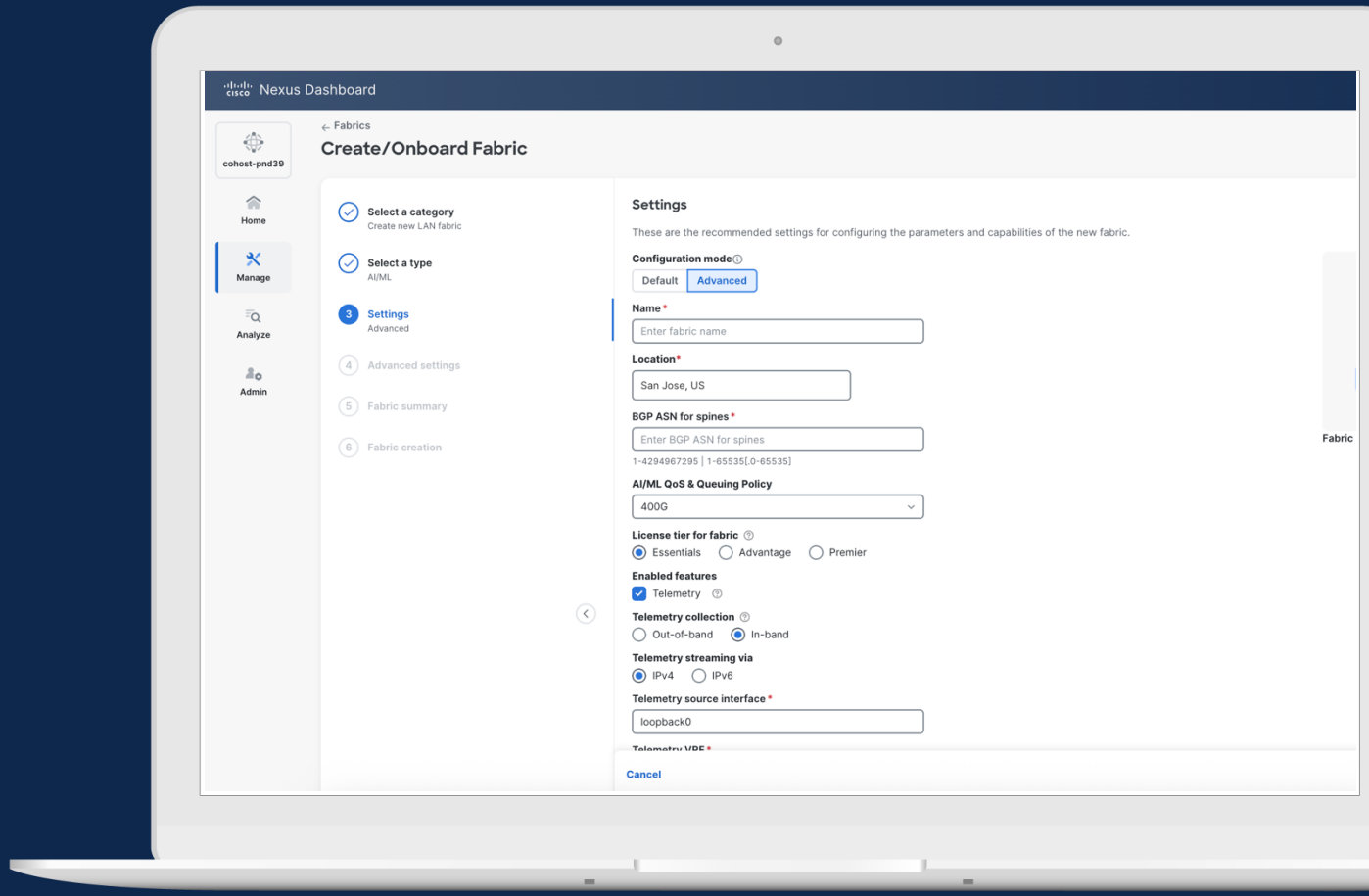
Nexus Dashboard will use it as an anchor point to discover other Nexus switches

Configure metrics

Define your QoS metrics and enable load balancing from your fabric settings

Onboard them all at once

View your AI/ML networks and their elements from a single place



Cisco Nexus Data Broker - Provision

Create or onboard a fabric

Data Broker

Create NDB Fabric

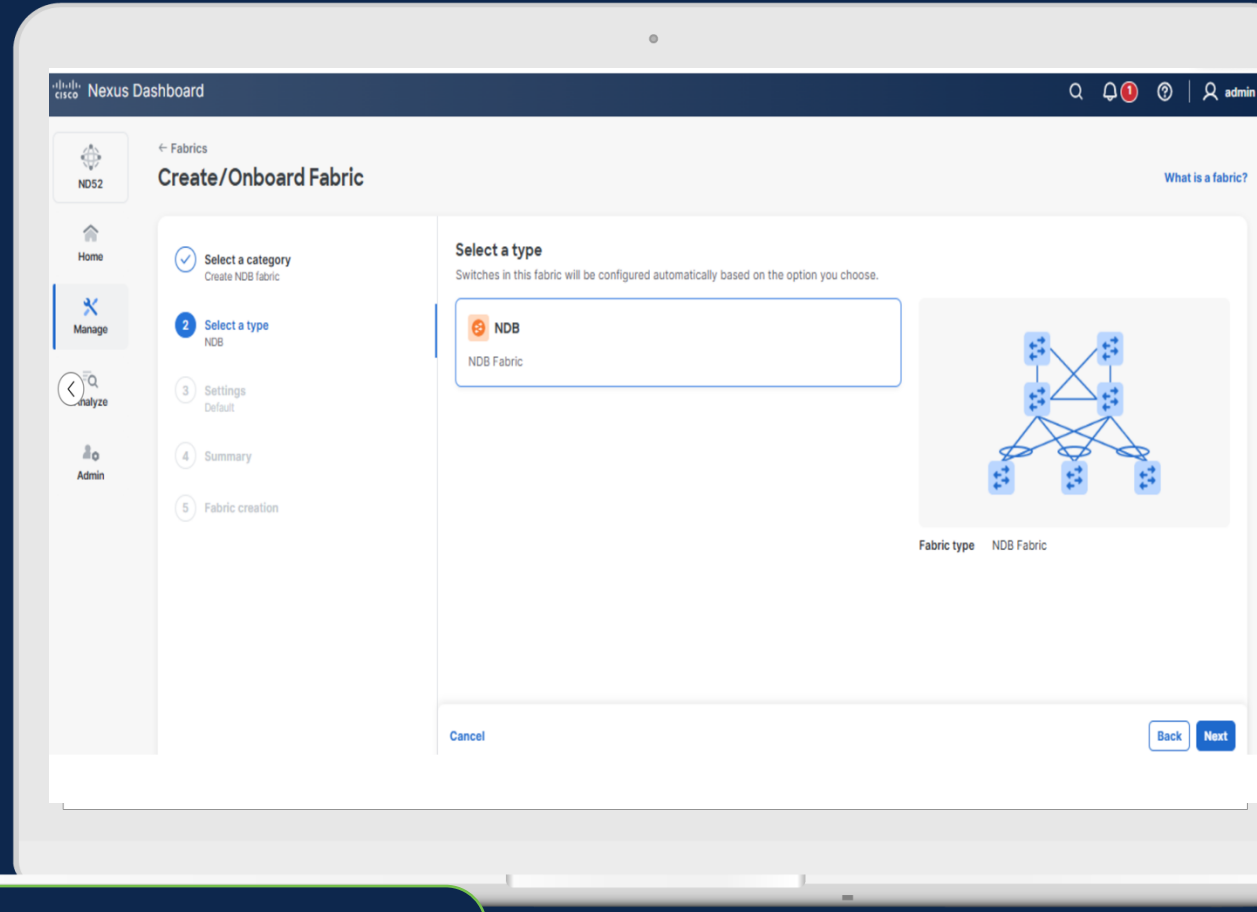
Nexus Dashboard will use login credentials of switches to onboard and create a NDB Fabric

Configure SPAN

Onboard/connect to production fabrics (ACI, NX-OS) and push SPAN config as necessary to copy traffic

Configure policies

Define Filtering policy, Decapsulation, Dedup, redirection and QoS metrics and enable load balancing



Benefits

Extend visibility across data centers and multi-cloud environments

Cisco Nexus Dashboard - Manage

Consistent fabric, switch, and interface configurations

Configure once, deploy anywhere

Define your configuration or network policy and select where you want to apply it, accelerating the time to provision connectivity

Simplified user experience

Future

Set up connectivity to routers, switches, and other devices (incl. VRF-lite, MPLS) in a few clicks

Guided workflows

A step-by-step guide detailing how to build the connection, what is required, and where to implement.

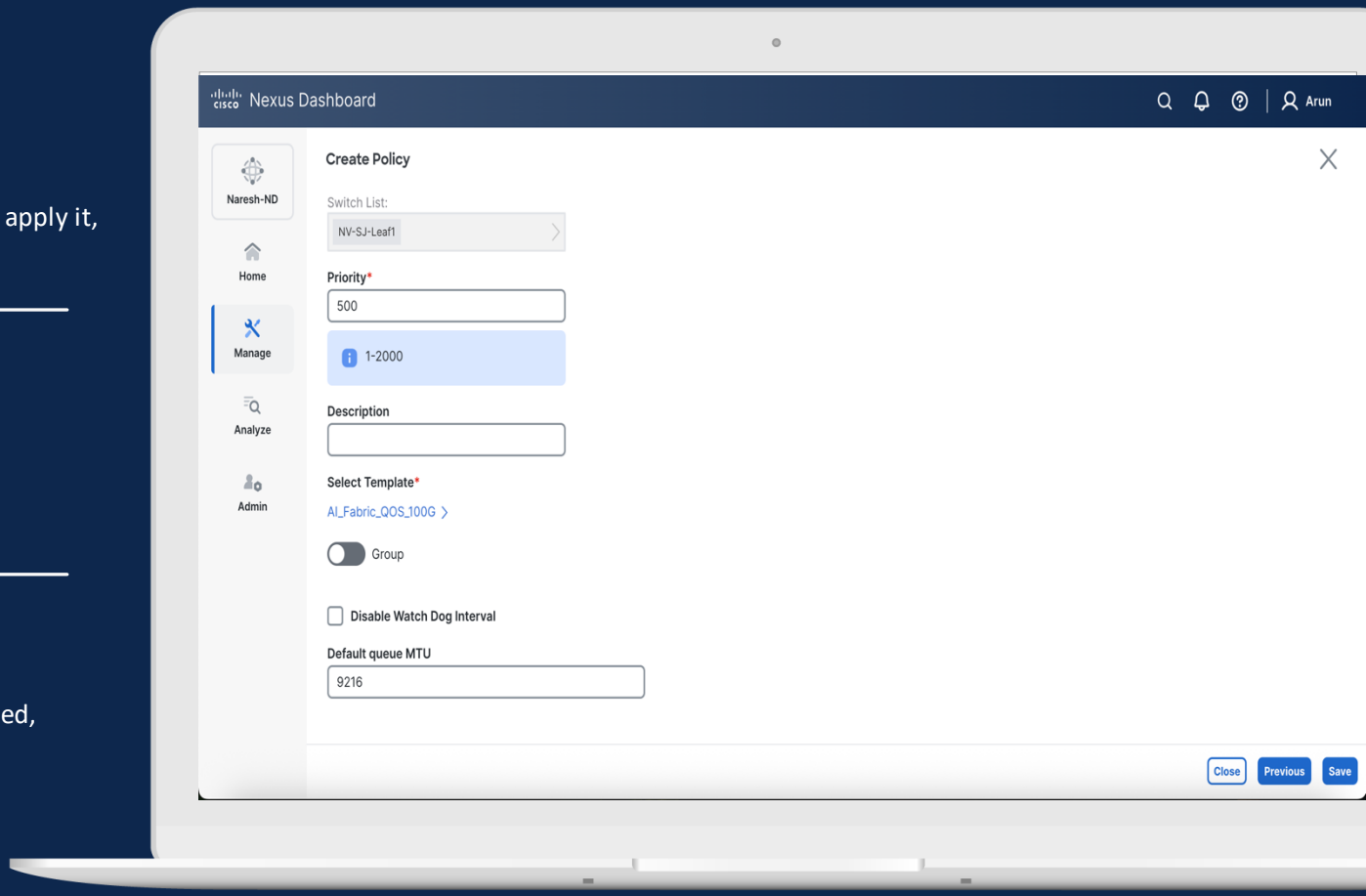


*Image based on Nexus Dashboard 4.1 prototype, subject to change

Benefits

Single workflow for all connectivity configurations

Ease of Use

Cisco Nexus Dashboard - Manage

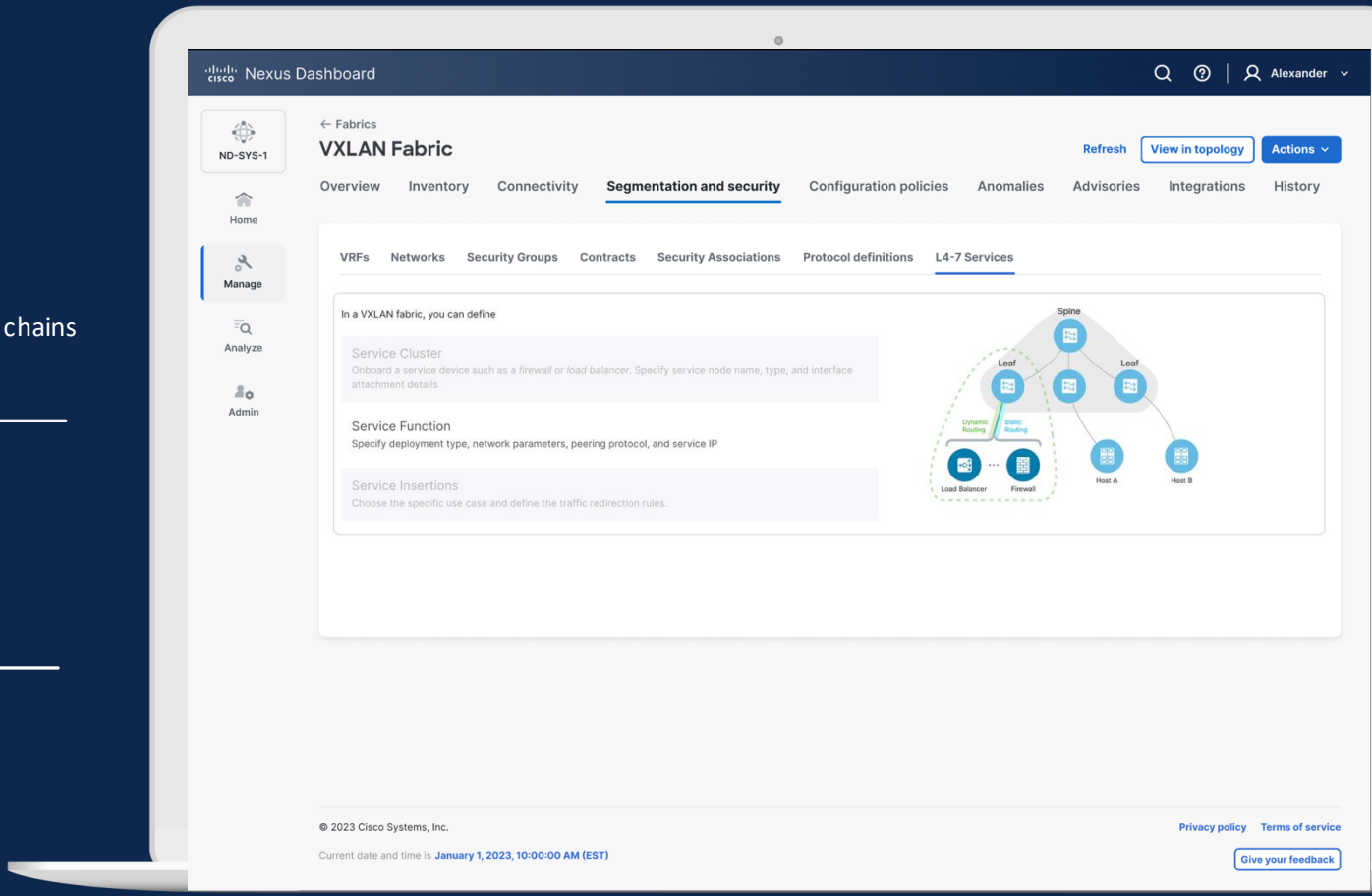
L4-L7 service integration

Traffic steering and redirection

Send traffic to firewalls, load balancers and other L4-L7 services or service chains by using Policy-Based Redirection (PBR)

Monitor and failover L4-L7 services

Detect node health changes and failover as needed, allowing load-share and selective redirection



Benefits

Line-rate, hardware-based L4-L7 insertion

Consistent security and policies

Cisco Nexus Dashboard - Manage

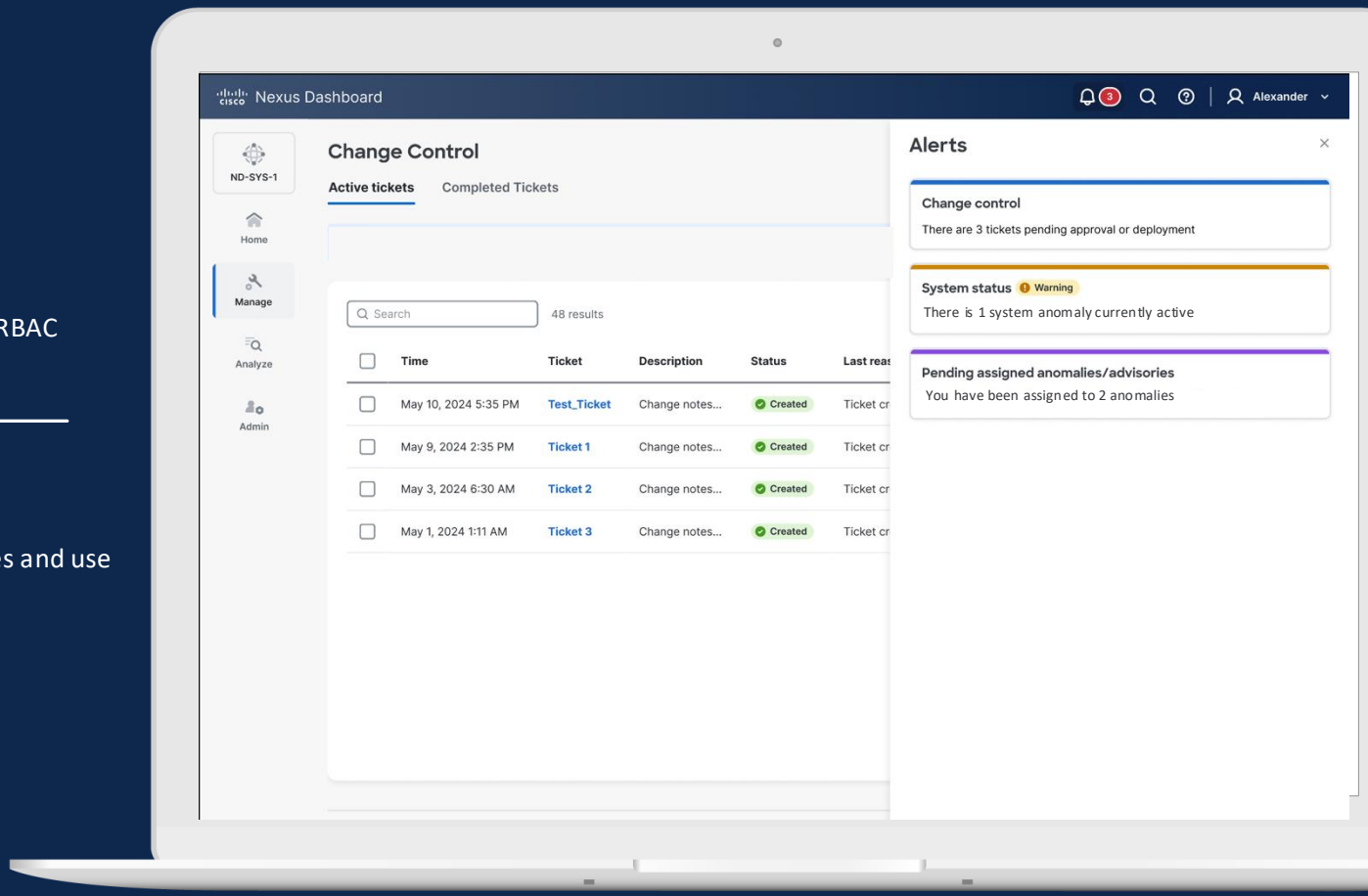
Stage, approve, and deploy changes

Change control

Prevent unwanted changes by creating a line of approval using enhanced RBAC with pre/post-deploy rollback options

Git integration

Integrate Nexus Dashboard with GIT to import or export custom templates and use them across multiple Nexus Dashboard clusters



* New UX based on Nexus Dashboard 4.0 prototype, subject to change

Benefits

Control changes in your environment

Minimize errors and risk

Cisco Nexus Dashboard – Manage

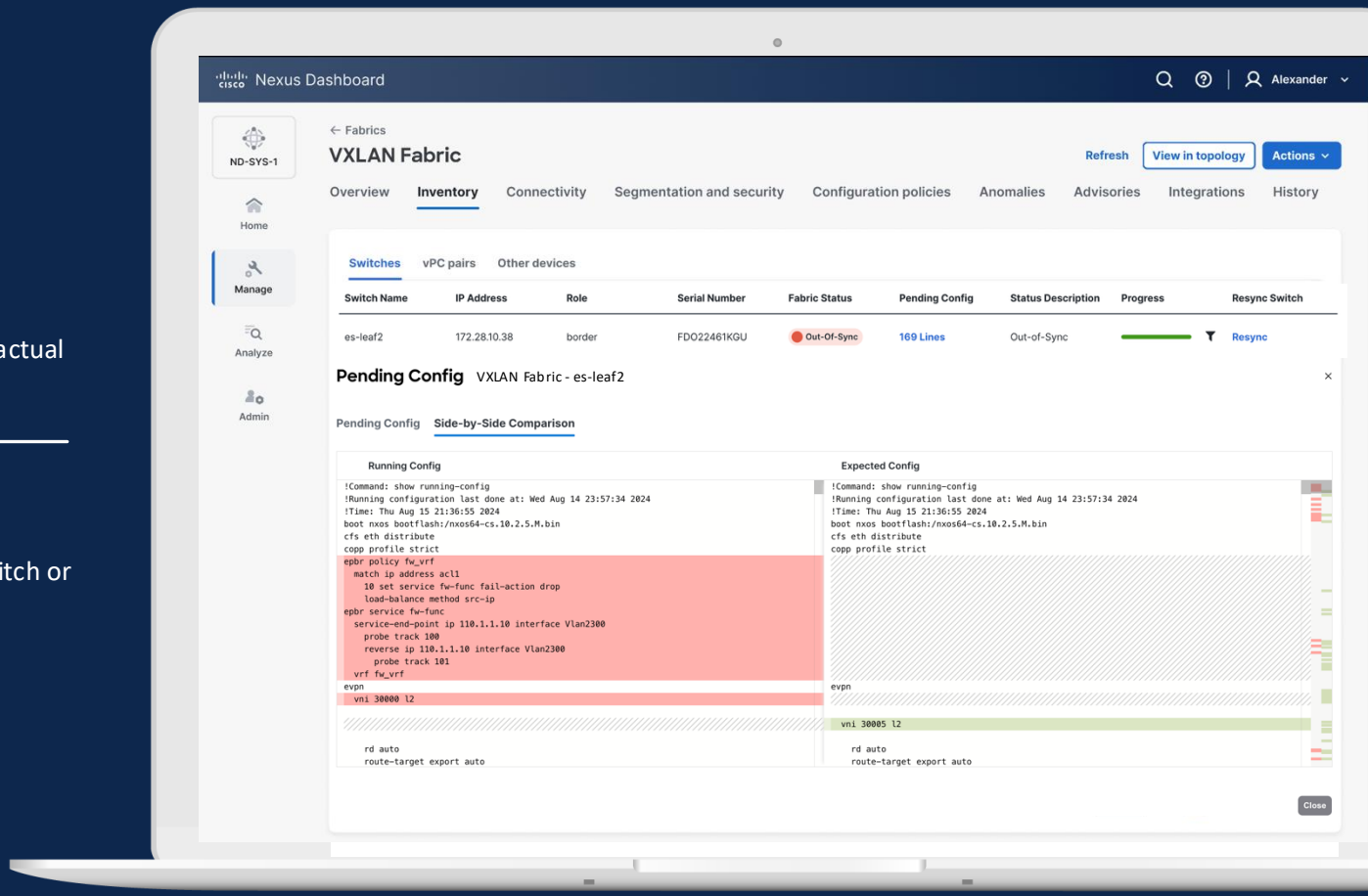
Configuration drifts

Identify inconsistencies

Learn about any differences between the intended configuration and the actual configuration running on a switch or a fabric

Synchronize changes

After you perform a change or if the configuration running locally on a switch or fabric is not what you expect, you can re-sync and deploy to maintain consistency



* NX-OS comparison displayed above. ACI fabric drifts are performed through Orchestration

Benefits

Preserve consistency across switches and interfaces

Reconcile changes with ease

Cisco Nexus Dashboard – Manage

Software Updates – NX-OS, IOS-XE, and ACI

Pre-upgrade analysis

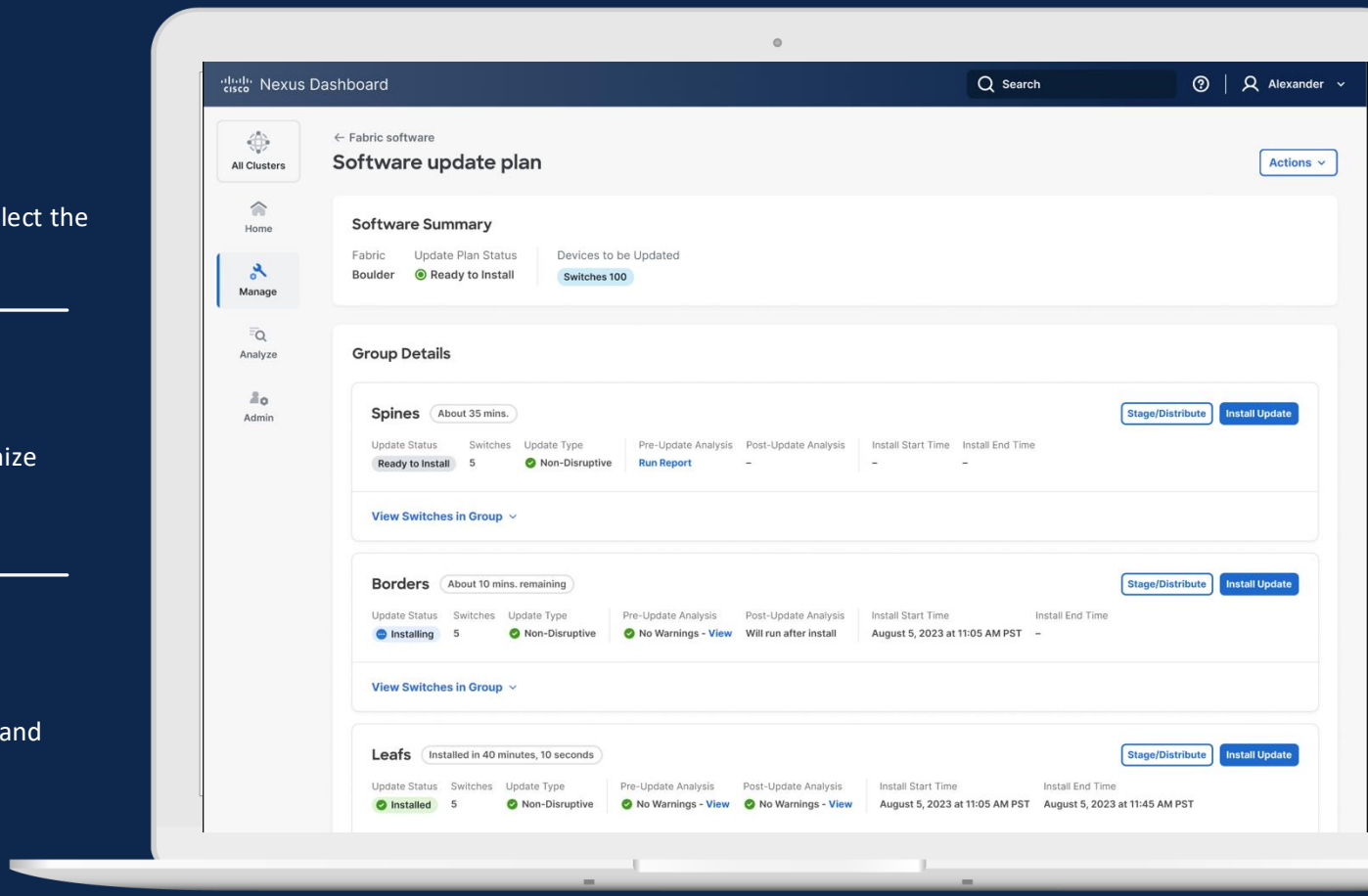
Visualize the potential impact of an upgrade before you perform it. Just select the version you wish to upgrade to and see the results

Automated upgrade plans and recommendations*

Nexus Dashboard will suggest customizable groups and methods to minimize disruption during the upgrade process

Post-upgrade analysis

Once the upgrade is performed, visualize the results, check any changes, and ensure everything came back just as it was before.



* ACI fabrics to support upgrade plans in version 4.1 (not committed)

Benefits

Stay up to date and minimize risk

Ease of Use

Analyze

Identify, troubleshoot and fix faster with Nexus Dashboard

VISIBILITY

- Topology
- IPFM
- IP Packets
- 3rd party integrations

ANALYTICS

- Delta analysis
- Connectivity analysis
- Traffic analysis
- SAN insights

Cisco Nexus Dashboard – Analyze

Topology – Maintain updated visibility across fabrics

Updated topology

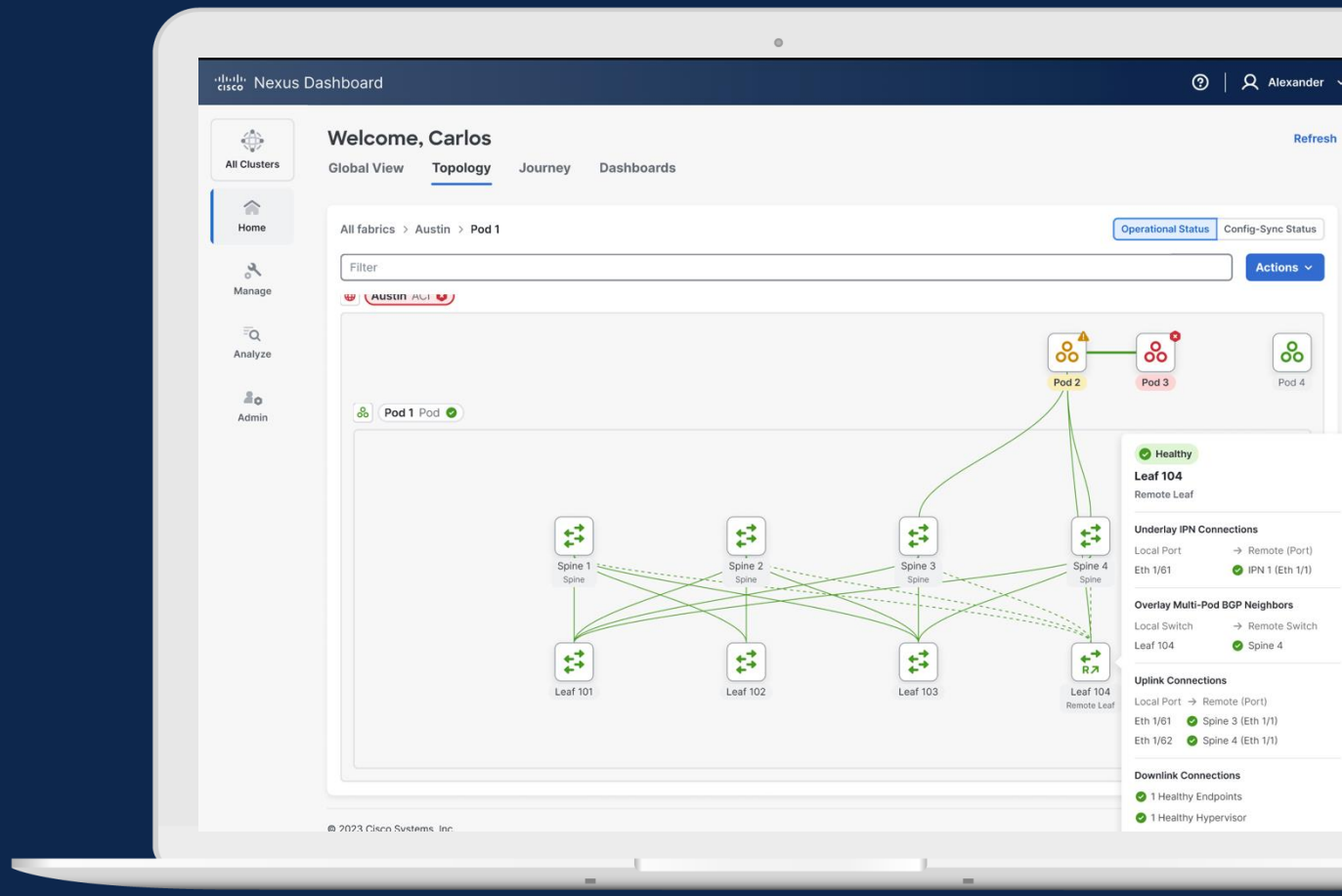
View fabrics, switches, interfaces, and endpoints with their corresponding anomaly scores

Visualize and configure

Verify health and configuration-sync status, configure VPC pairs, assign roles, and more

Single and multi-fabric

Drill down into a fabric or visualize connections across fabrics, including external and inter-fabric networks such as IPN and ISN



Benefits

Visualize all your fabrics in a single place

Cisco Nexus Dashboard – Analyze

Achieve your net-zero goals faster

Cost

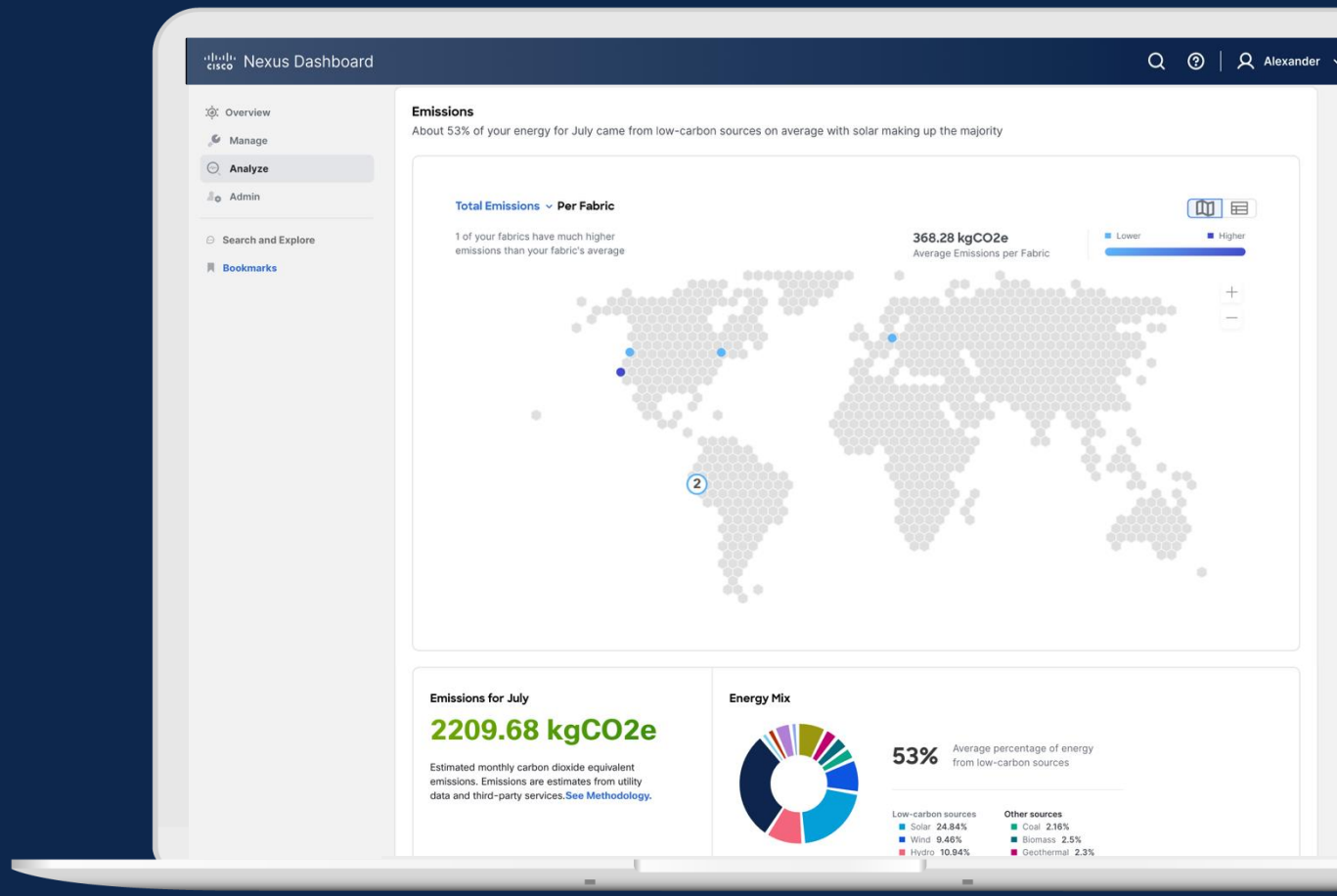
Learn about associated energy costs each month and compare them against previous ones; customize your own negotiated rates

Energy consumption

Switch and PDU (Panduit) power consumption gives you insight into peaks and how efficiently your switches are using electricity

CO2 emissions[1]

Understand the energy sources your data center networks use, visualize the top contributing devices, and compare against previous months



[1] Requires connectivity to Intersight

Benefits

Sustainability | Cost awareness

Cisco Nexus Dashboard – Analyze

Identify latency, congestion, and drops in your network

Automatically identify services in your network

Through well-known L4 ports (e.g., Web - TCP port 80) pre-loaded service categories are learned and monitored; category customization is also allowed based on your own preferences

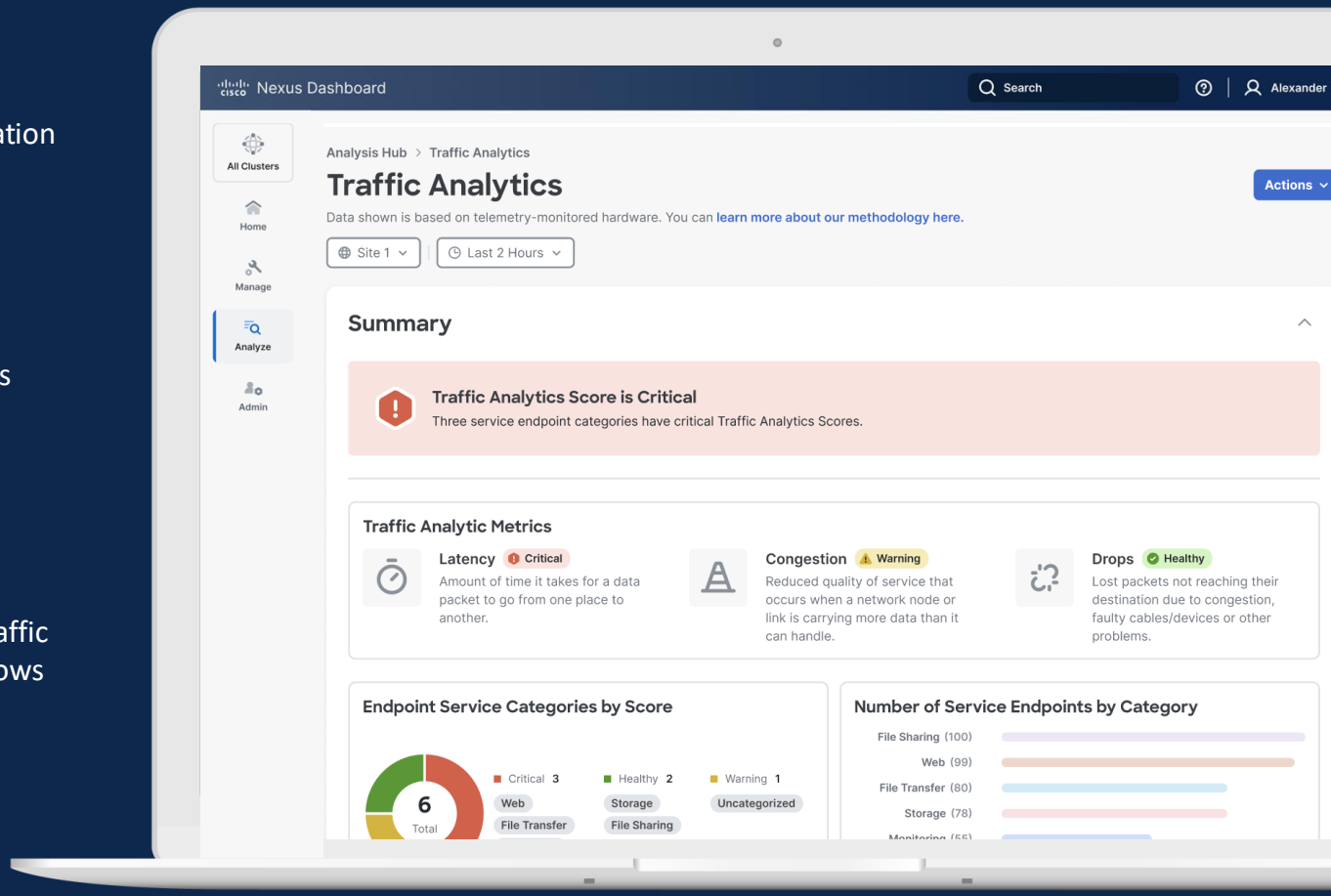
Pervasive across switches and fabrics

Learn about clients and services connecting across multiple fabrics without rules or any additional rule configuration[1]

Granular visibility for every connection

From overall fabric score to category, service, and connection, Traffic Analytics can monitor individual client-to-service sessions and allows you to “tap-in” by capturing flow records on demand

Requires: ACI – 6.1.1 and NX-OS 10.4(2F)



* Fabrics must have PTP configured for timestamping

Benefits

Anticipate performance issues | Customize monitored services

Cisco Nexus Dashboard + Splunk

Observability made simple

Search , Discover , Report and Visualize

Event Monitoring

Anomalies from Nexus Dashboard

Log Security and Threat Detections

Organization Security Events with Advisories from ND

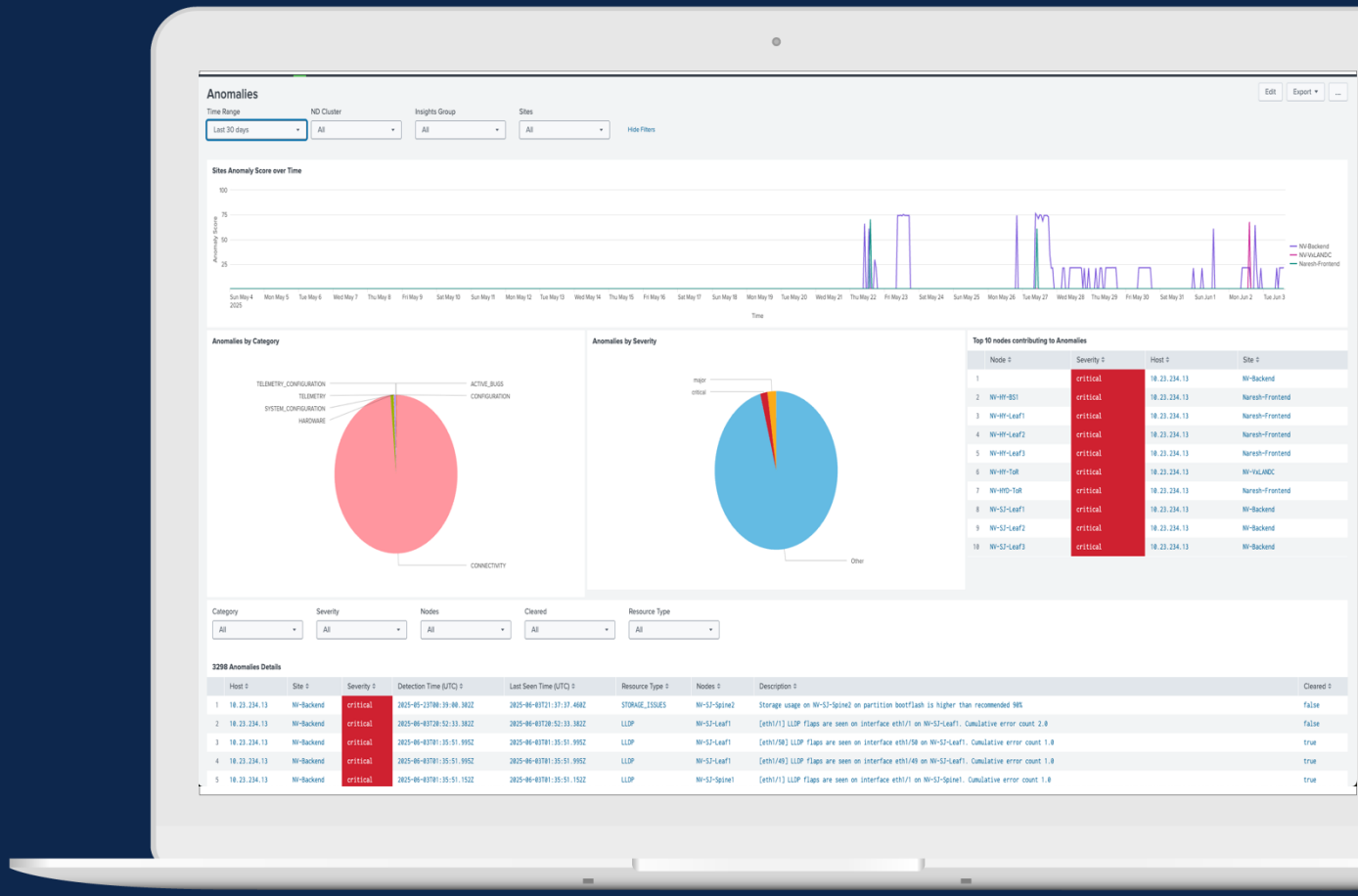
Audit logs from DCN platforms

Log Retention

Retain metric, event and logs for longer duration

Cross correlation

Cross correlation with other network and application data



Benefits

Single pane of glass view

Cisco Nexus Dashboard - Analyze

Search and Explore

Search with Natural Language

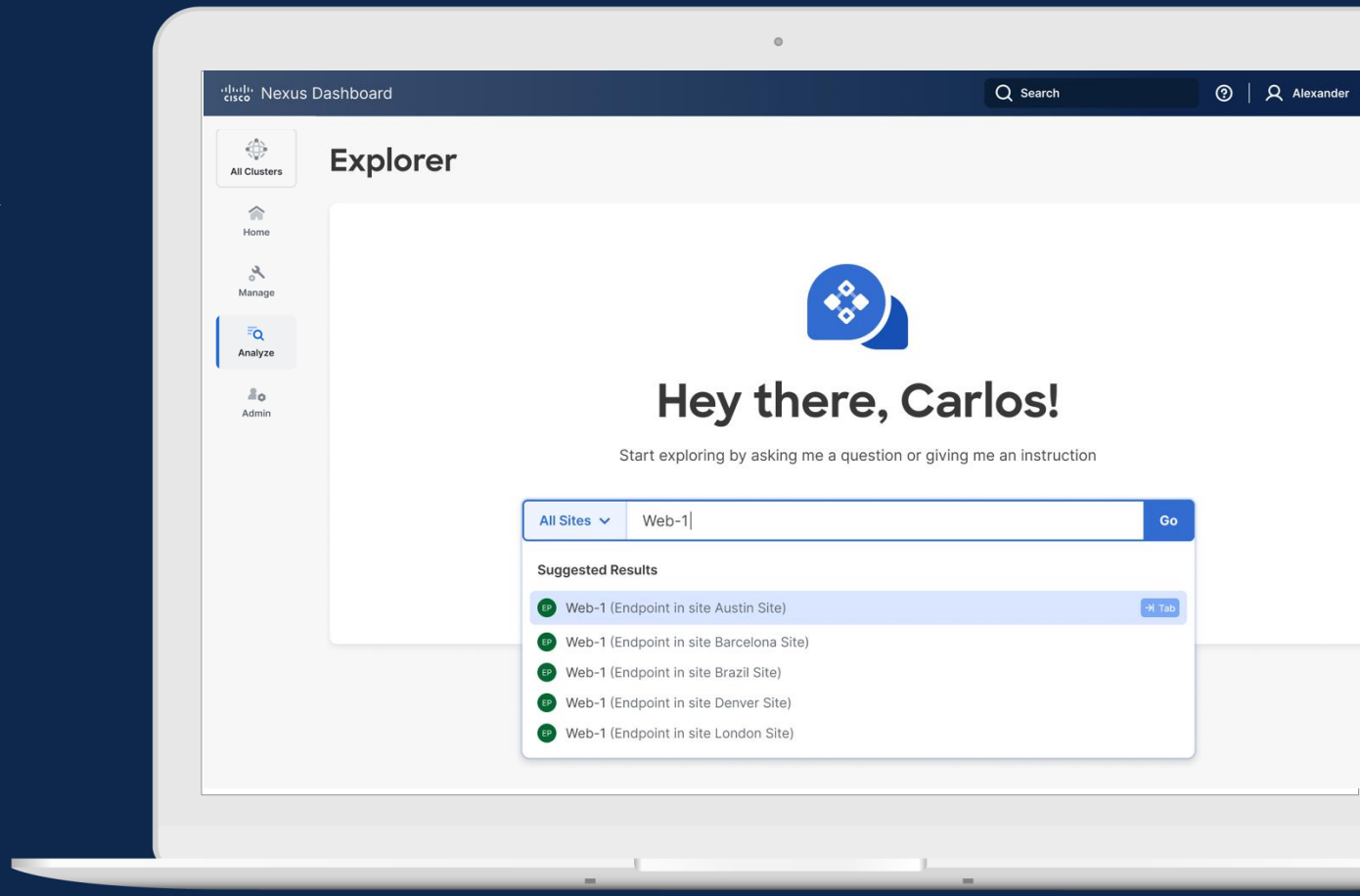
Search and Explore enables quick keyword and show queries across all managed fabrics, allowing users to find IP/MAC addresses, interfaces, switches, anomalies, and more with auto-suggest and detailed results

What and Can queries

Discover associations between network entities and verify communication and connectivity health between entities, with results displayed in tabular or graphical formats

Multi-cluster global search

Search across clusters with enhanced filtering, real-time results, and the ability to view remote resource details, facilitating comprehensive network visibility and troubleshooting



Benefits

Single pane of glass view

Cisco Nexus Dashboard – Analyze

Conformance

Hardware

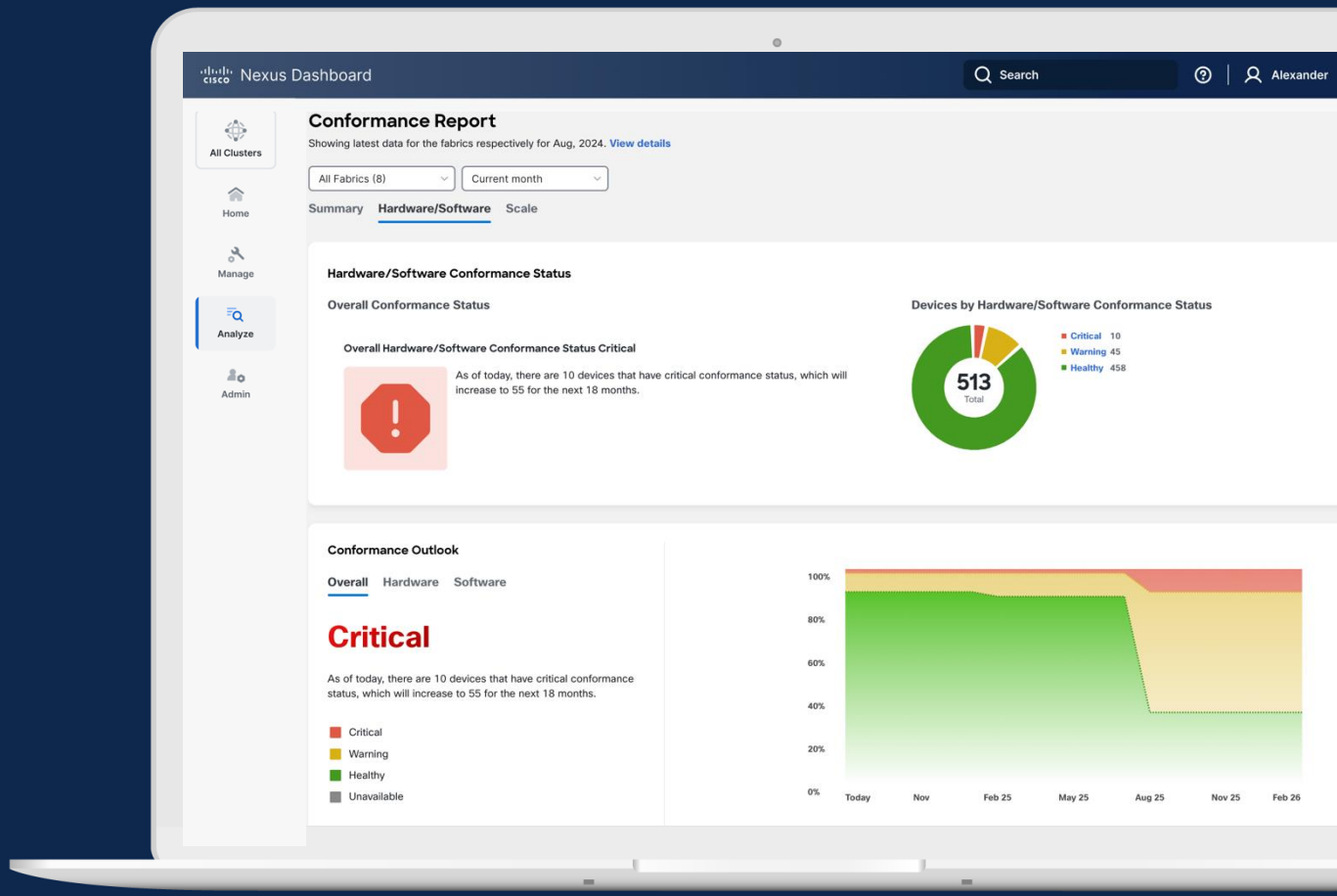
Identify switches, devices, and components running on or approaching End-of-Life (EoL) / End-of-Support conditions

Software

Identify software versions on or approaching End-of-Life (EoL) / End-of-Support conditions

Verified Scalability

Automatically check if your fabric(s) and switches are running under the verified scalability guidelines for each software version



* Image based on prototype, subject to change

Benefits

Single workflow for all connectivity configurations

Ease of use

Cisco Nexus Dashboard – Analyze

Delta Analysis

Anomalies

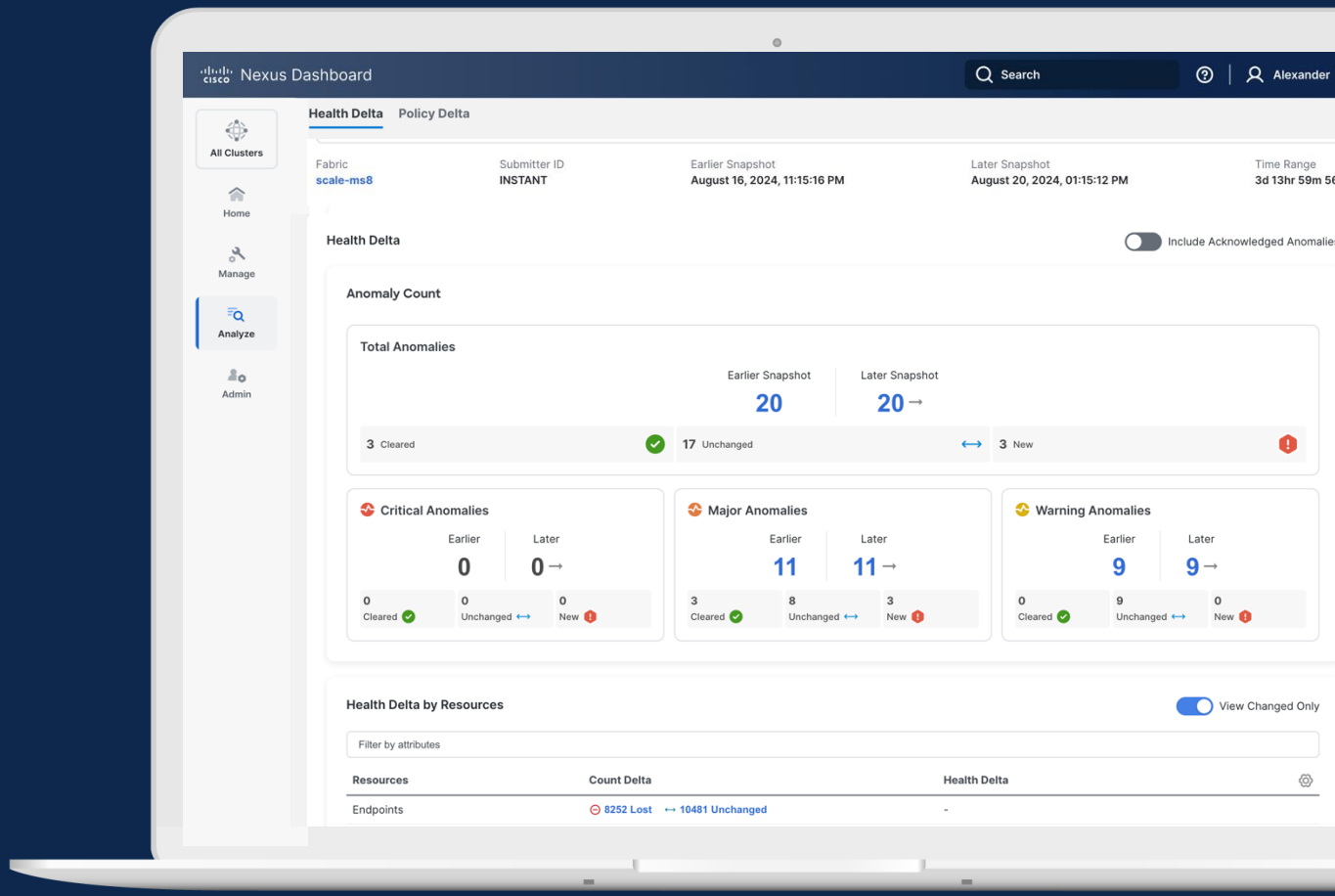
View new, unchanged, and cleared anomalies between two points in time to learn about changes in your network

Resources

Learn about endpoints, interfaces, routes, VRFs, and other objects that may have changed their configuration or health status

Policies and configuration

Get an XML (ACI) or CLI (NX-OS) view of the specific objects that have changed, how they changed, and who changed them



Benefits

Learn about any changes in your network

Troubleshoot faster

Cisco Nexus Dashboard – Analyze

Pre-Change Analysis

Anomalies

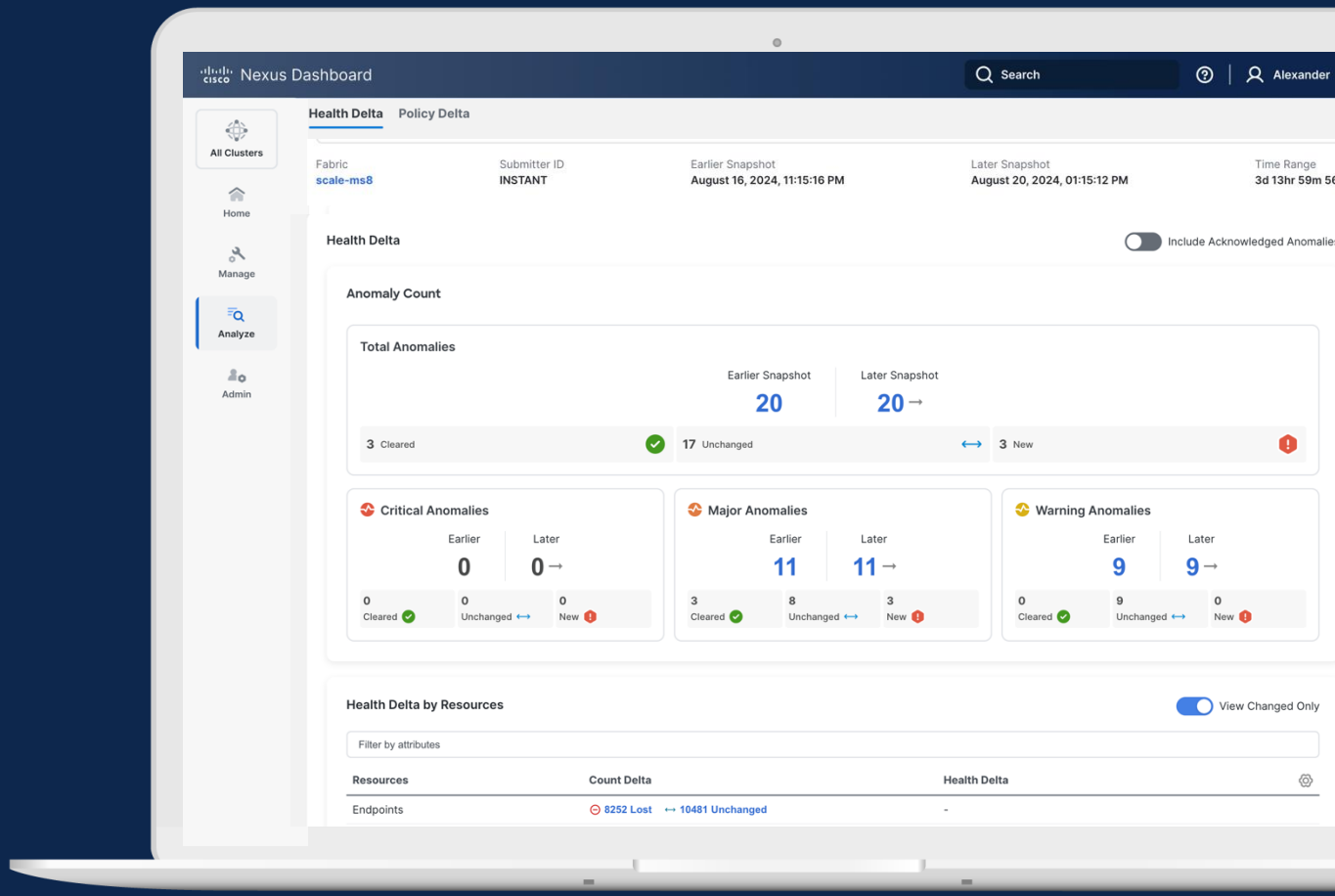
Proactively view new, unchanged, and cleared anomalies of a configuration change before it gets pushed to the network

Resources

Learn about the impact of configuration changes for endpoints, interfaces, routes, VRFs, and other objects

Policies and configuration

Get an XML (ACI) or CLI (NX-OS) view of the specific objects that have changed, how they changed, and who changed them



Benefits

Learn about any changes in your network

Troubleshoot faster

Cisco Nexus Dashboard – Analyze

Connectivity Analysis

Evolve from traceroute

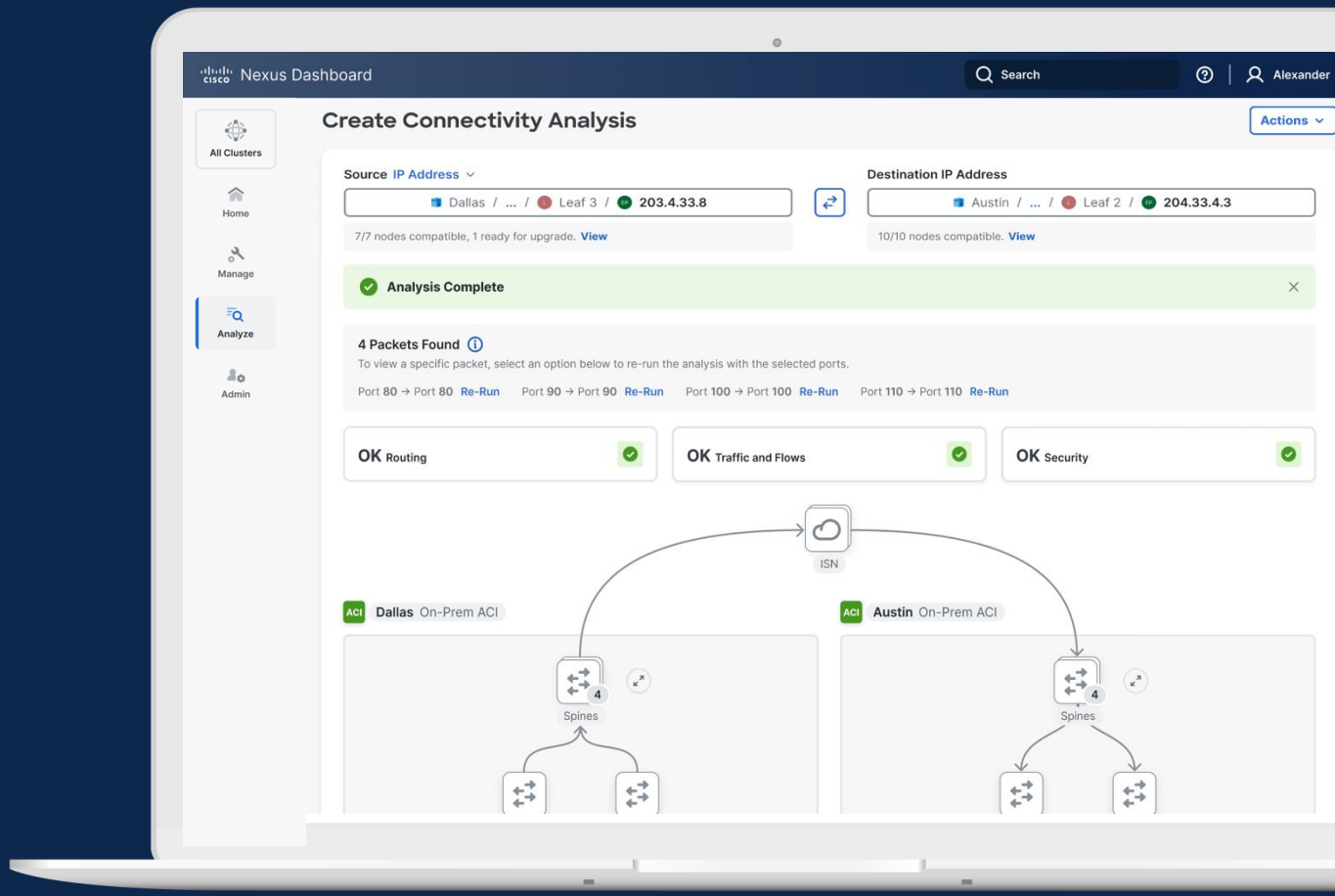
Add a source and destination IP or MAC address and let Nexus Dashboard do the rest; optionally add L4 ports to be more specific

Increased visibility

Add forwarding (ELAM and OAM) and consistency checks, routing verification, traffic analytics, and security[1]

Single and multi-fabric[2]

Visualize the whole path even when endpoints communicate through different Nexus Dashboard–managed fabrics



[1] Security and Traffic Analytics views are expected to be integrated in version 4.1 (not committed)
[2] Must run Nexus Dashboard 4.0 and above

Benefits

Learn about any in-transit issues | Avoid isolated troubleshooting

Cisco Nexus Dashboard – Analyze

Anomalies

Detect potential configuration issues

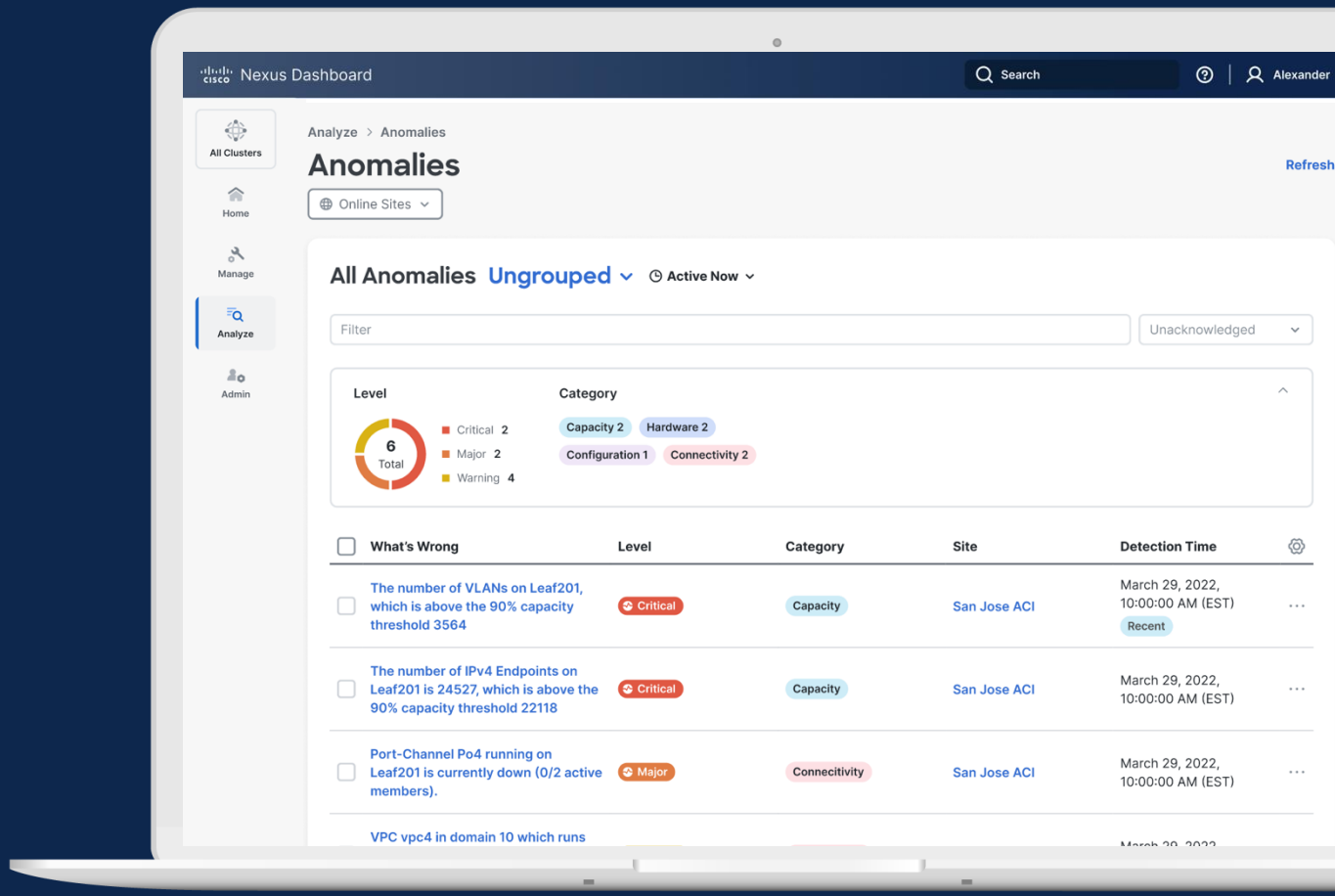
Continuously analyzes network using a mathematical model to detect configuration errors, inconsistencies, and anomalies, enabling proactive troubleshooting and ensuring network compliance and operational health

Capacity planning

Monitor network resource usage against baseline thresholds, detecting deviations that indicate potential capacity issues

Monitor Hardware

Proactively detect deviations in hardware components such as CPU, memory, temperature, fan speed, power, and storage by baselining normal behavior and flagging anomalies when thresholds are exceeded



[1] Security and Traffic Analytics views are expected to be integrated in version 4.1 (not committed)
[2] Must run Nexus Dashboard 4.0 and above

Benefits

Learn about any in-transit issues

Avoid isolated troubleshooting

Cisco Nexus Dashboard

Enrich visibility through integrations and an open ecosystem

LAN

APPDYNAMICS splunk>

App performance / Log collection

vmware* openstack.* OPENSHIFT*

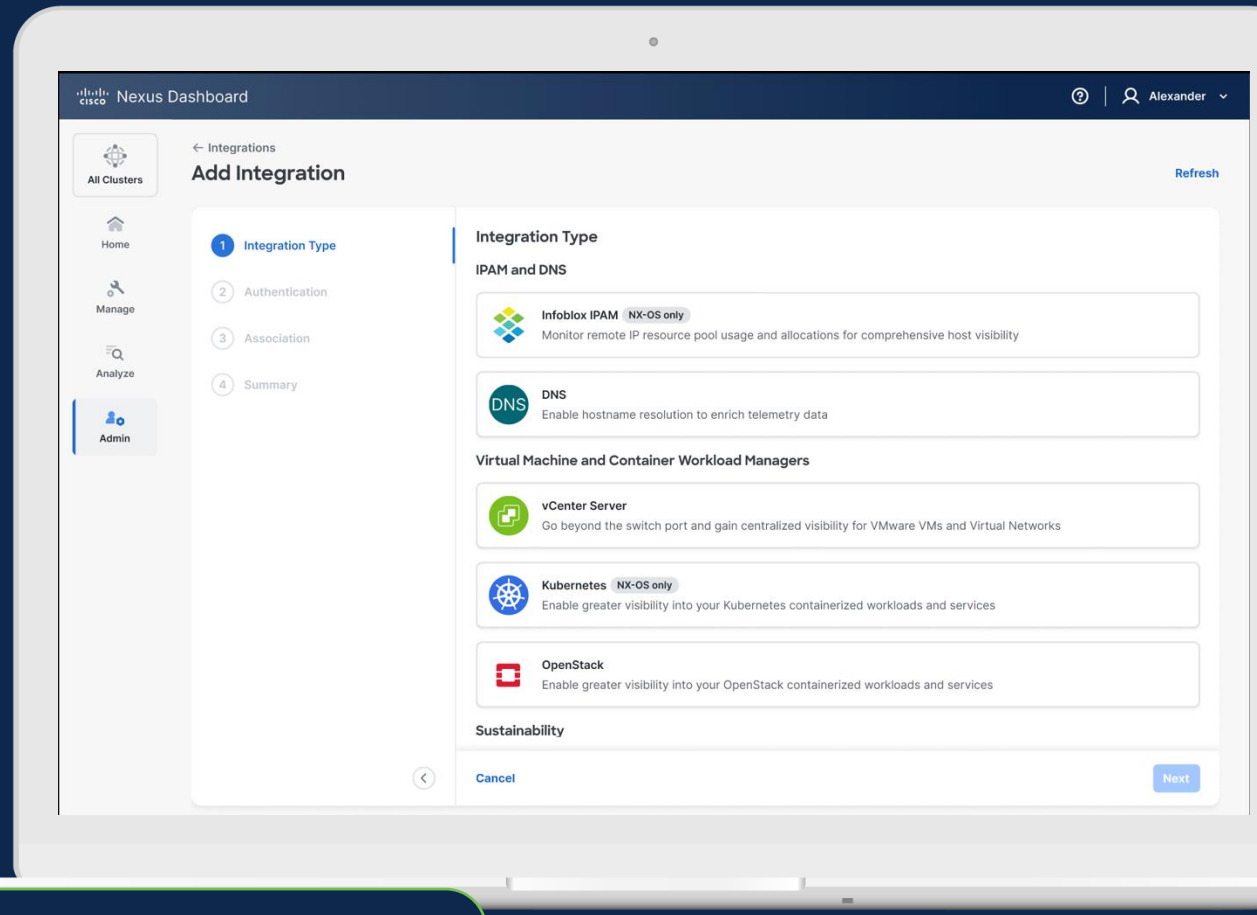
VM and K8s visibility

Infoblox* Generic DNS

DNS and IPAM

PANDUIT

Sustainability



Benefits

Building a rich eco-system of integrations

Minimize congestion, risk and downtime with telemetry and analytics

Turn telemetry into insights

Analyze to minimize downtime

Enhance visibility with integrations

Security

Security as a Design Principle

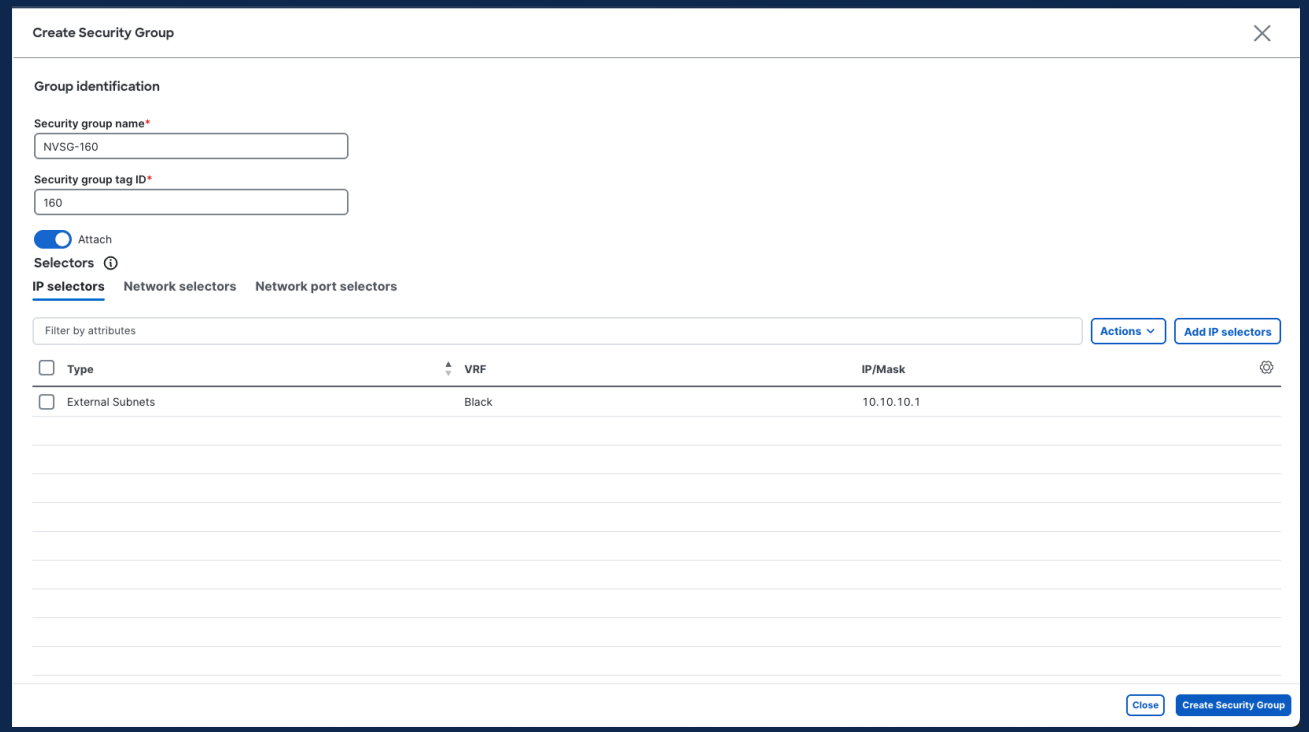
Security cannot be an afterthought; it must be infused into the fabric.

Nexus Dashboard was developed with Security at its core:

- Zero-trust security isolation & micro-segmentation
- Automated configuration drift detection
- Streaming Alerting & Notifications & Rapid remediation
- Hardened RBAC & Remote Authentication & MFA
- Compliance Rules & Pre-Change Validation
- Vulnerability Mitigation with Live Protect
- Smart Switch & Hypershield Integration

Cisco Nexus Dashboard – Security

Micro-segmentation for VXLAN fabrics



Define security groups in a single click (based on IP, VM Attributes and VLAN)

Create and visualize micro-segmentation policies/contracts from a single pane

Intuitive and workflow-based service chaining rules

Scale-out with support for single-site and multi-site architectures

Benefits

Segment East-West traffic

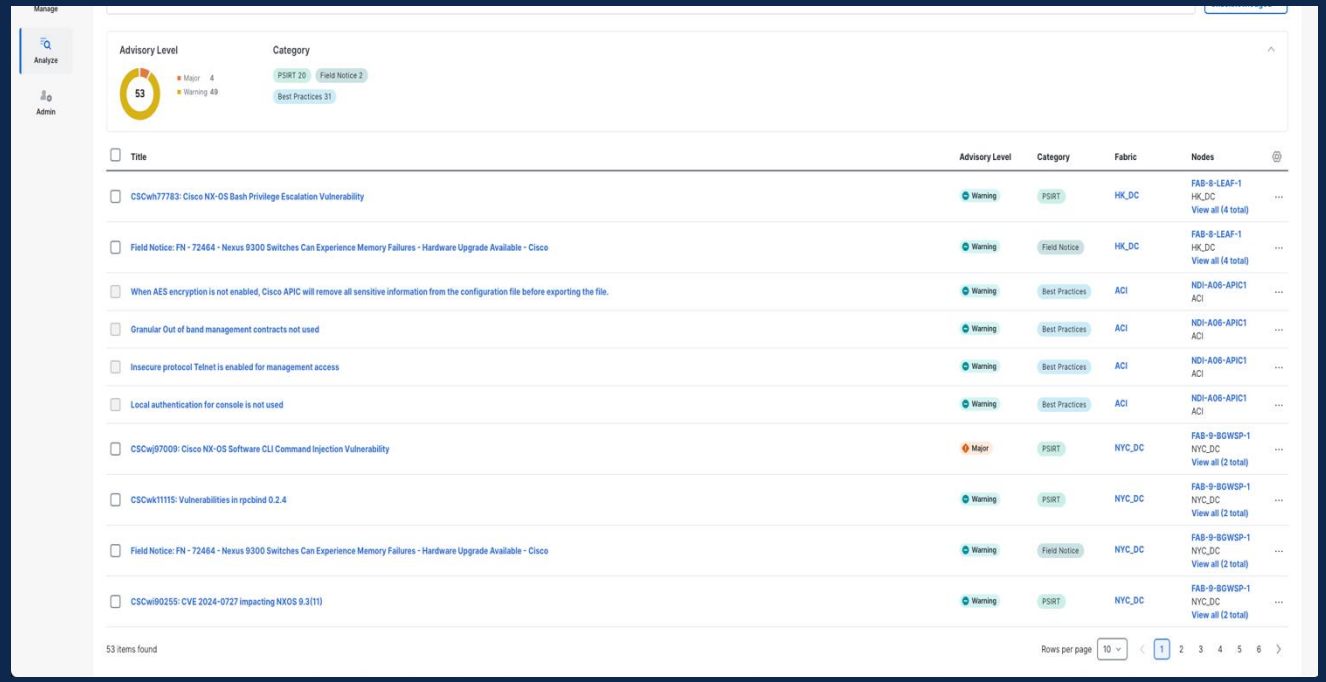
Flexible security isolation

Reduce attack surface

Automate your way

Cisco Nexus Dashboard – Security

Compliance dashboard



- Audit Logs for entire data center networking fabric
- Organization security events with Advisories
- Hardening along with best practices
- Patching using Isovalent

Benefits

Single pane of glass	PSIRT and CDETS	Integration with SIEM	Hardening and best practices

Cisco Nexus Dashboard – Smart Security

Smart Switches & Hypershield Integration

Cisco N9300 Series Smart Switches

N9324C-SE1U

24-port 100G

800G Services Throughput

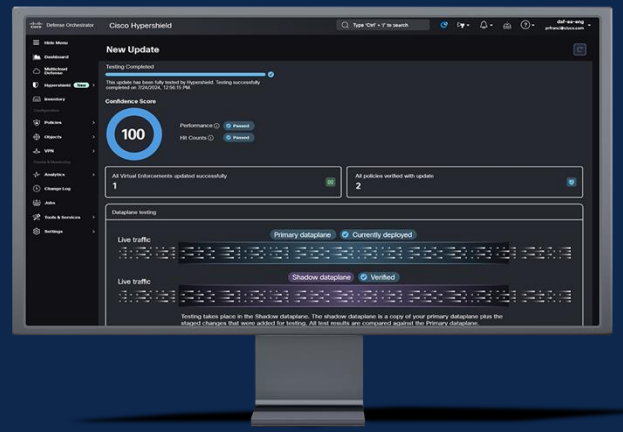
N9348Y2C6D-SE1U

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

800G Services Throughput

Nexus Dashboard

Cisco Hypershield



Use Cases

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

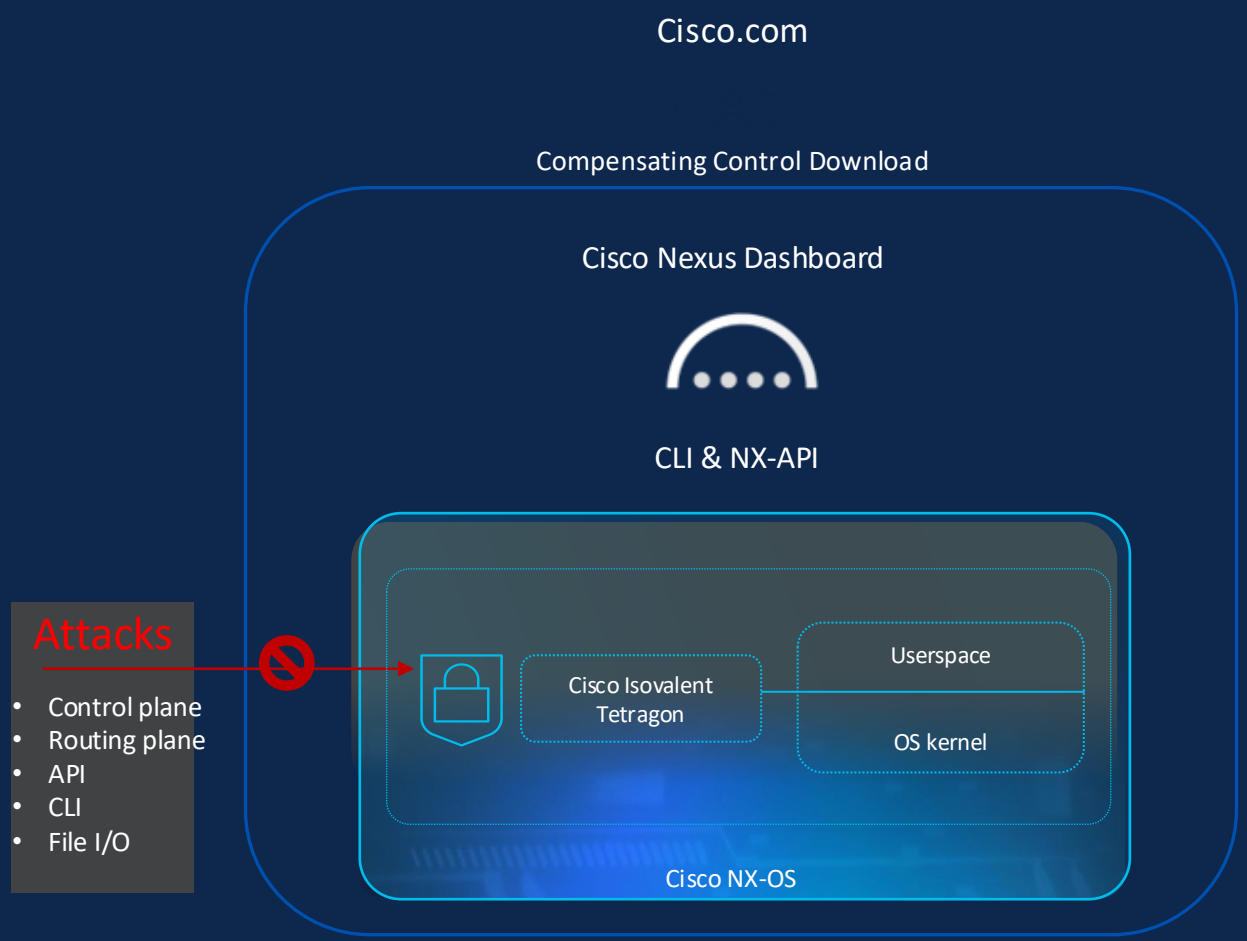
Benefits

Distributed segmentation without sacrificing speed

Vulnerability Mitigation with No Downtime

Available Now

Live Protect for Nexus OS switches



Innovation

- Enterprise-grade Tetragon agent built into NXOS 10.6(1)F
- eBPF-powered security observability and enforcement
- First to market (no equivalent from Arista, Juniper, Aruba, etc.)

Customer workflow

- Policy file (shields) delivered as a signed RPM available on cisco.com
- Download and apply SMU to the switch (Enforce or Monitor mode)
- Collect metrics, events, logs, and traces
- Export Tetragon events to Splunk or other SIEMs
- SMU automatically removed with PSIRT-bundle upgrade

Ease of use

- Available with essentials or higher license
- Integrated Nexus Dashboard workflow
- API and CI/CD support for automation
- PSIRT upgrades during standard maintenance windows

Summary

Nexus Dashboard

Included with every Nexus 9000 switch license

Nexus Dashboard

Consumption choice, single licensing

Cisco Nexus® Dashboard: Automation, management, AI analytics, and troubleshooting tools included with your Cisco switch license

Simple, modern, useful

Cisco Nexus Dashboard 3.2: Available now!

Appliance based (physical or virtual)

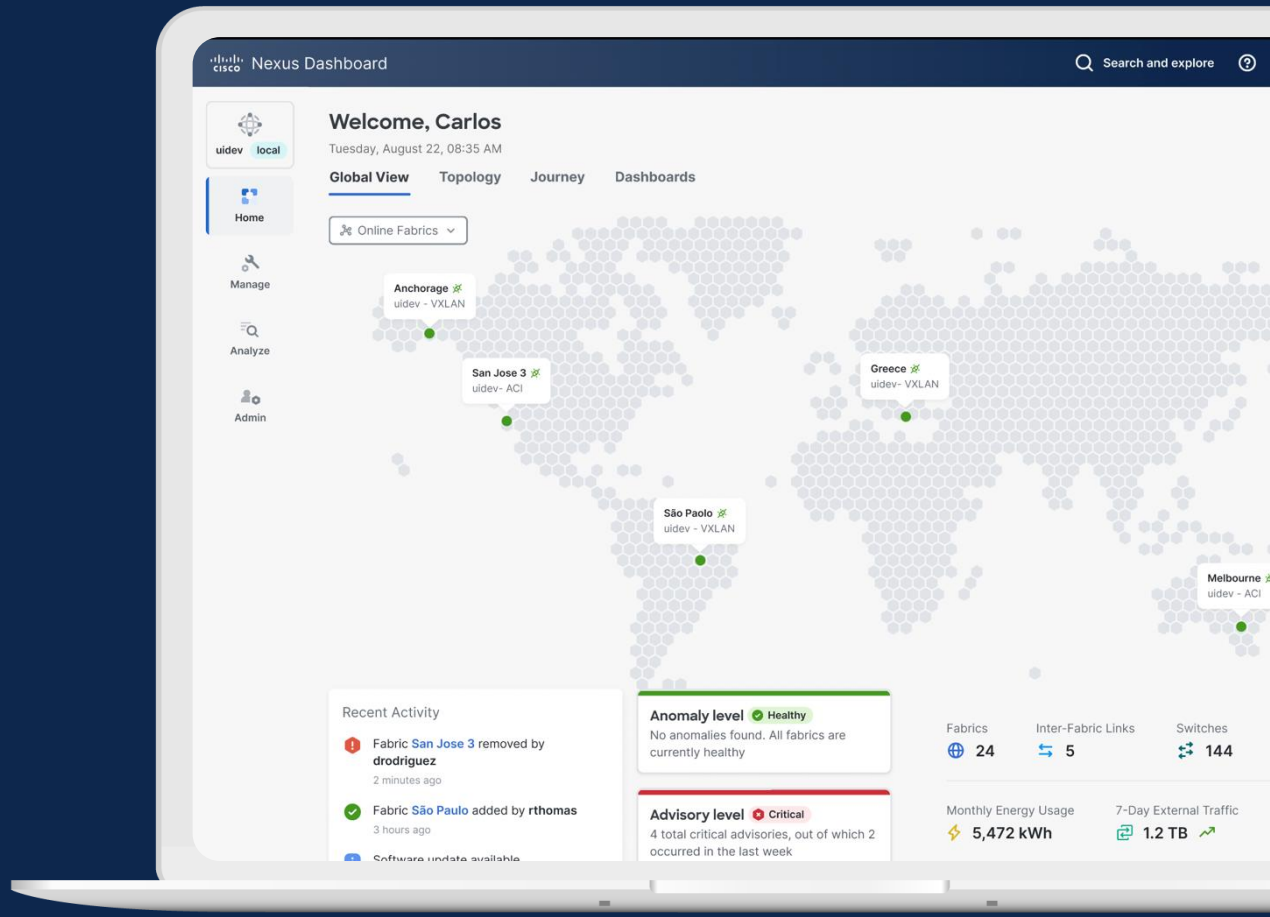
Start with one physical node or three VMs and scale from there

Innovate and minimize risk and downtime

Leverage the power of automation and analytics

Go beyond the switch port

Always connected to Cisco TAC[1]



[1] When connected to Cisco Intersight® and leveraging Cisco TAC Assist

Licensing Tiers

Features	Essentials	Advantage	Premier
Analyze	New	New	All Features
Orchestration		✓	✓
Automation	✓	✓	✓

Included with every Nexus switch license [2]

Entitlements included with Switch Licensing

Nexus Dashboard features included with every Nexus License

Essentials

For Users who would benefit from:

- Streamlined device lifecycle management, including software upgrades with minimal operational overhead
- Essential endpoint visibility
- Proactive hardware monitoring with baseline anomaly detection
- Actionable hardware and software advisories to stay ahead of vulnerabilities and defects

Advantage

For Users who would benefit from:

- Seamless multi-fabric policy extension across ACI sites and domains
- Advanced anomaly detection to surface issues before they impact applications
- End-to-end external and intra-fabric traffic visibility & trending for data-driven capacity planning
- Built-in support for AI/ML-ready fabrics including PFC, ECN, and microburst detection
- Streaming of anomalies to external systems (Kafka) for integrated, real-time operations workflows

Premier

For Users who would benefit from:

- End-to-end endpoint and security intelligence for deep Day-2 operations visibility
- Pre-deployment policy assurance to catch misconfigurations before they deploy to production
- Advanced flow analytics to expose congestion, latency, and hidden blind spots in real time
- Full-stack network troubleshooting arsenal for rapid testing, validation, and verification of policy and routing behavior

Benefits

No additional cost to enable Nexus Dashboard Capabilities


CISCO