The bridge to possible

Introduction to ACI

Chris Merkel, DC TSA

Cisco Webex App

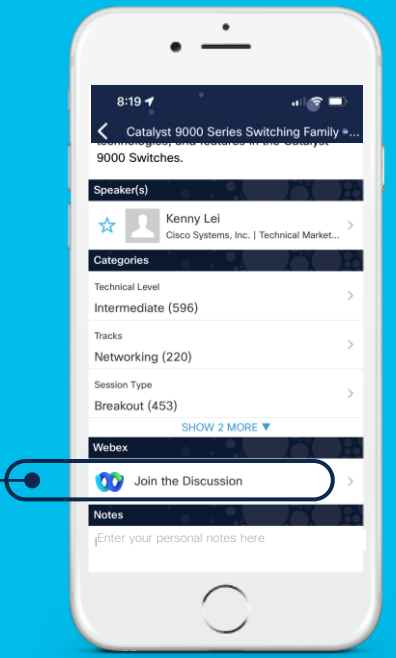
Questions?

Use Cisco Webex App to chat
with the speaker after the session

How

1. Find this session in the Cisco Live Mobile App
2. Click “Join the Discussion”
3. Install the Webex App or go directly to the Webex space
4. Enter messages/questions in the Webex space

Webex spaces will be moderated until February 24, 2023.



Agenda

- Introduction
- Fabric Basics
- Policy Model
- Architectural Deployments
- Day 2 and beyond
- Conclusion

Fabric Basics

ACI: One Network, any location

ACI Anywhere

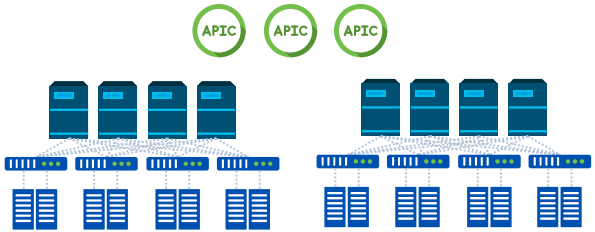
Edge / Remote

Core Data Centers

Hybrid Cloud & Multicloud

IP WAN

IP WAN



ACI
Remote Leaf

ACI
Single-POD

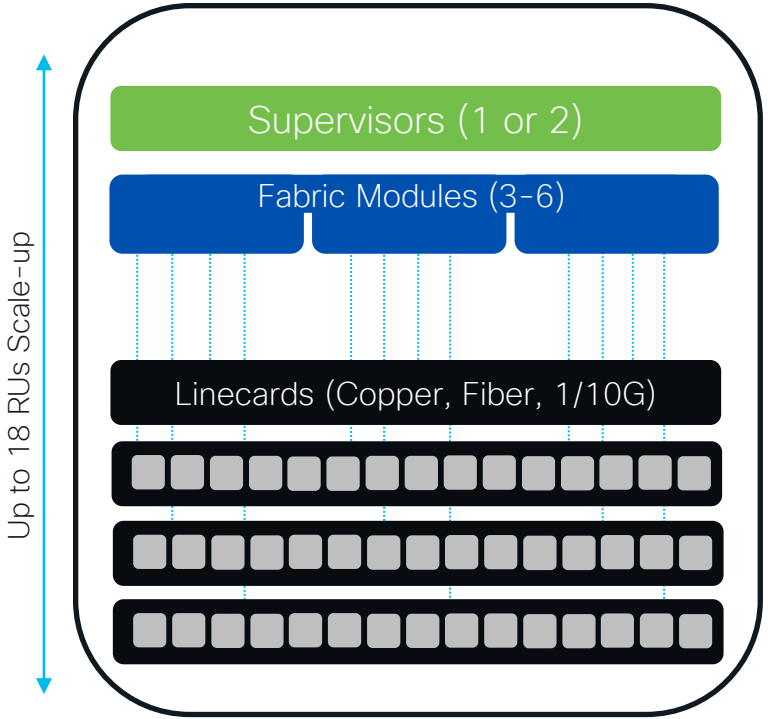
ACI
Multi-POD

ACI
Multisite

Cloud
ACI

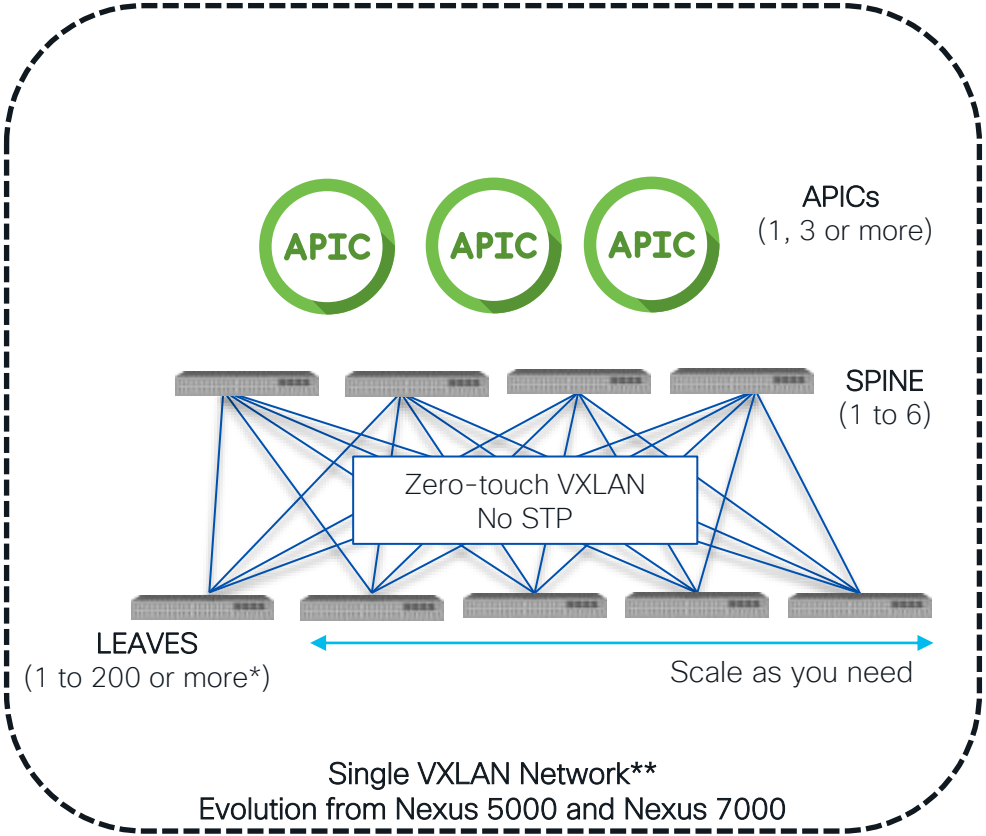
The easiest Data Center and Cloud Interconnect Solution in the Market **Try it today!**

The DC network before
Classic modular switching



Single chassis (e.g. Nexus 7000)

The DC network NOW
ACI



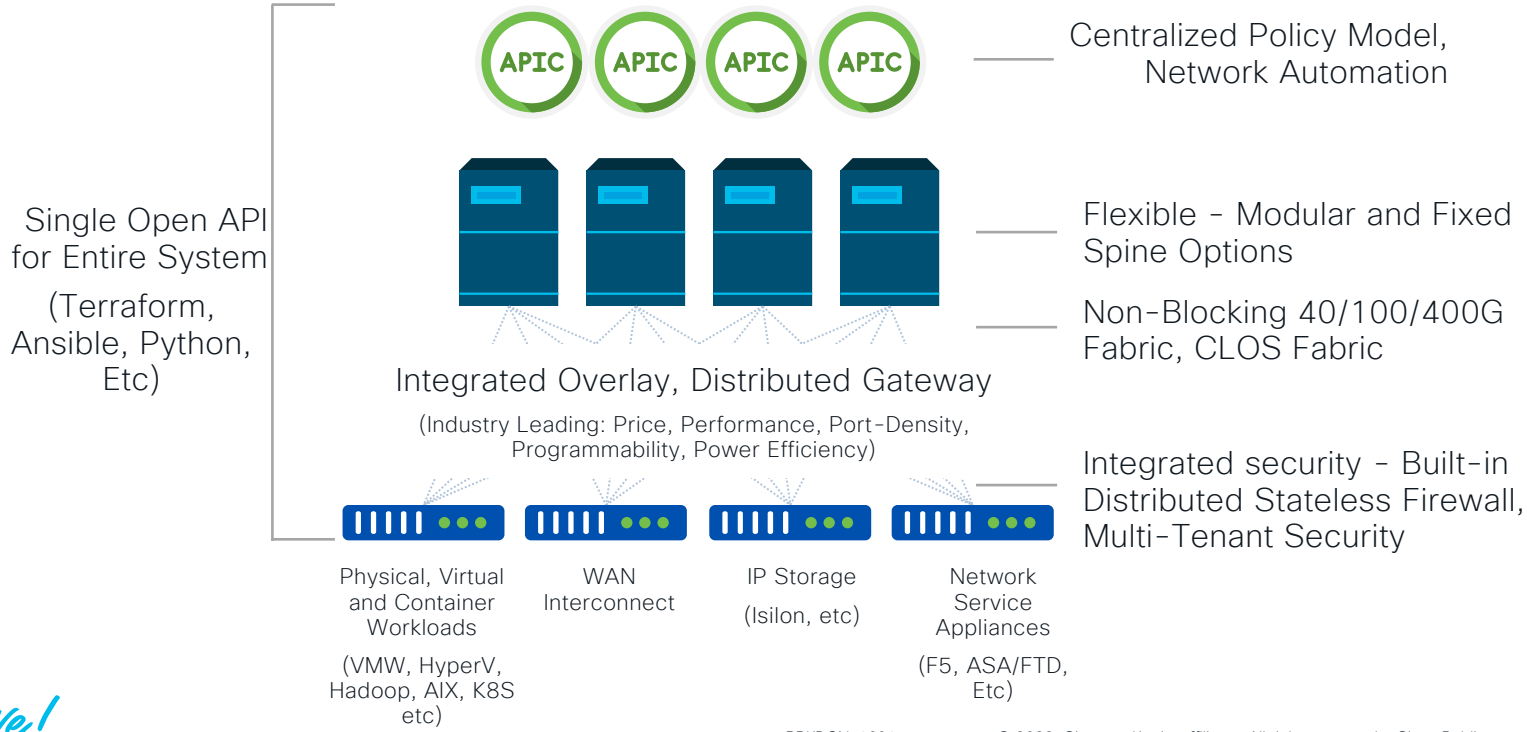
Single VXLAN Network**
Evolution from Nexus 5000 and Nexus 7000

cisco Live!

* > 500 Leaves with MultiPod/Multi-Site
** Other topologies available (e.g. 3-tier, etc)

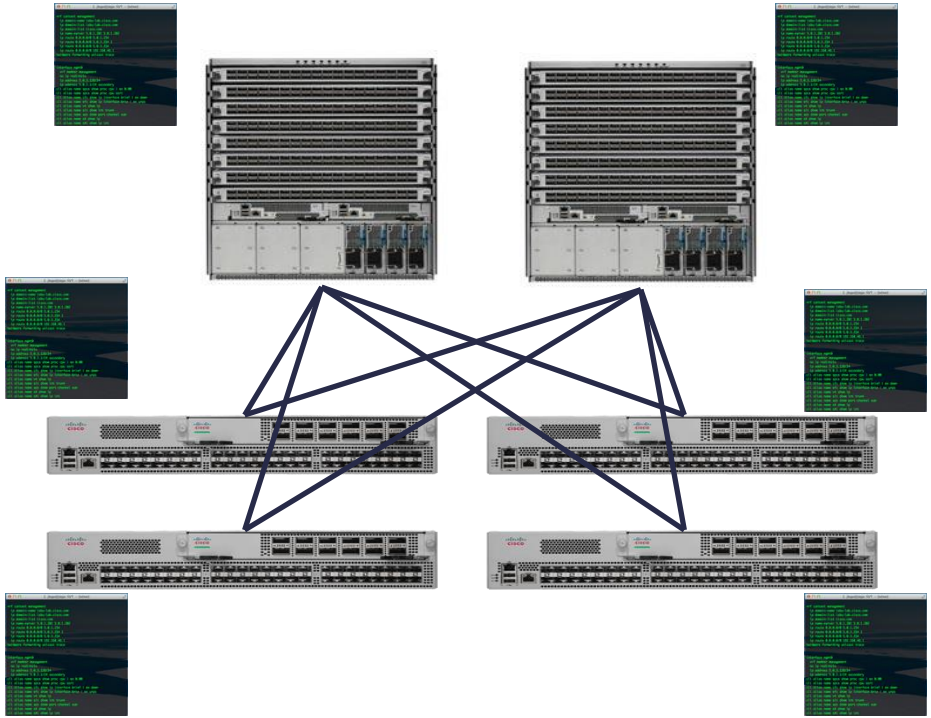
Application Centric Infrastructure Building Blocks

Built on the Nexus 9000



All nodes are managed and operated independently, and the actual topology dictates a lot of configuration

- **Device basics**: AAA, syslog, SNMP, PoAP, hash seed, default routing protocol bandwidth …
- **Interface and/or Interface Pairs**: UDLD, BFD, MTU, interface route metric, channel hashing, Queuing, LACP, …
- **Fabric and hardware specific design**: HW Tables, …
- **Switch Pair/Group**: HSRP/VRRP, VLANs, vPC, STP, HSRP sync with vPC, Routing peering, Routing Policies, …
- **Application specific**: ACL, PBR, static routes, QoS, …
- **Fabric wide**: MST, VRF, VLAN, queuing, CAM/MAC & ARP timers, COPP, route protocol defaults



ACI: How difficult was it to bring up?

What tasks & configuration did ACI just saved me from doing manually on every switch

BEFORE

SSH to every switch, Assign IP Address, Enable Telnet/SSH, Add users on every switch/Create ACLs (optional)

ACI: How difficult was it to bring up?

What tasks & configuration did ACI just saved me from doing manually on every switch

BEFORE

- Nexus 9000 VTEP-1 configuration:

```
switch-vtep-1(config)# feature nv overlay
switch-vtep-1(config)# feature vn-segment-vlan-based

switch-vtep-1(config)# feature ospf
switch-vtep-1(config)# feature pim
switch-vtep-1(config)# router ospf 1
switch-vtep-1(config-router)# router-id 200.200.200.1
switch-vtep-1(config)# ip pim rp-address 10.1.1.1 group-list
switch-vtep-1(config)# interface loopback0
switch-vtep-1(config-if)# ip address 200.200.200.1/32
switch-vtep-1(config-if)# ip address 100.100.100.1/32 second
switch-vtep-1(config-if)# ip router ospf 1 area 0.0.0.0
switch-vtep-1(config-if)# ip pim sparse-mode
switch-vtep-1(config)# interface e2/1
switch-vtep-1(config-if)# ip address 20.1.1.1/30
switch-vtep-1(config-if)# ip router ospf 1 area 0.0.0.0
switch-vtep-1(config-if)# ip pim sparse-mode

switch-vtep-1(config)# interface port-channel 10
switch-vtep-1(config-if)# vpc 10
switch-vtep-1(config-if)# switchport
switch-vtep-1(config-if)# switchport mode access
switch-vtep-1(config-if)# switchport access vlan 10
switch-vtep-1(config-if)# no shutdown
switch-vtep-1(config)# interface e1/1
switch-vtep-1(config-if)# channel-group 10 mode active
switch-vtep-1(config-if)# no shutdown

switch-vtep-1(config)# interface nve1
switch-vtep-1(config-if)# no shutdown
switch-vtep-1(config-if)# source-interface loopback0

switch-vtep-1(config-if)# member vni 10000 mcast-group 230.1
switch-vtep-1(config)# vlan 10
switch-vtep-1(config-vlan)# vn-segment 10000
switch-vtep-1(config-vlan)# exit
```

```
switch-vtep-1(config)# feature nv overlay
switch-vtep-1(config)# feature vn-segment-vlan-based

switch-vtep-1(config)# feature ospf
switch-vtep-1(config)# feature pim
switch-vtep-1(config)# router ospf 1
switch-vtep-1(config-router)# router-id 200.200.200.1
switch-vtep-1(config)# ip pim rp-address 10.1.1.1 group-list 224.0.0.0/4
switch-vtep-1(config)# interface loopback0
switch-vtep-1(config-if)# ip address 200.200.200.1/32
switch-vtep-1(config-if)# ip address 100.100.100.1/32 secondary
switch-vtep-1(config-if)# ip router ospf 1 area 0.0.0.0
switch-vtep-1(config-if)# ip pim sparse-mode
switch-vtep-1(config)# interface e2/1
switch-vtep-1(config-if)# ip address 20.1.1.1/30
switch-vtep-1(config-if)# ip router ospf 1 area 0.0.0.0
switch-vtep-1(config-if)# ip pim sparse-mode

switch-vtep-1(config)# interface port-channel 10
switch-vtep-1(config-if)# vpc 10
switch-vtep-1(config-if)# switchport
switch-vtep-1(config-if)# switchport mode access
switch-vtep-1(config-if)# switchport access vlan 10
switch-vtep-1(config-if)# no shutdown
switch-vtep-1(config)# interface e1/1
switch-vtep-1(config-if)# channel-group 10 mode active
switch-vtep-1(config-if)# no shutdown

switch-vtep-1(config)# interface nve1
switch-vtep-1(config-if)# no shutdown
switch-vtep-1(config-if)# source-interface loopback0

switch-vtep-1(config-if)# member vni 10000 mcast-group 230.1.1.1
switch-vtep-1(config)# vlan 10
switch-vtep-1(config-vlan)# vn-segment 10000
switch-vtep-1(config-vlan)# exit
```

SSH to every switch, Assign IP Address, Enable Telnet/SSH, Add users on every switch/Create ACLs (optional)

(Times X Switches & Y VNIs)

ACI: How difficult was it to bring up?

What tasks & configuration did ACI just saved me from doing manually on every switch

BEFORE

- Nexus 9000 VTEP-1 configuration:

```
switch-vtep-1(config)# feature nv overlay
switch-vtep-1(config)# feature vn-segment-vlan-based

switch-vtep-1(config)# feature ospf
switch-vtep-1(config)# feature pim
switch-vtep-1(config)# router ospf 1
switch-vtep-1(config-router)# router-id 200.200.200.1
switch-vtep-1(config)# ip pim rp-address 10.1.1.1 group-list
switch-vtep-1(config)# interface loopback0
switch-vtep-1(config-if)# ip address 200.200.200.1/32
switch-vtep-1(config-if)# ip address 100.100.100.1/32 second
switch-vtep-1(config-if)# ip router ospf 1 area 0.0.0.0
switch-vtep-1(config-if)# ip pim sparse-mode
switch-vtep-1(config)# interface e2/1
switch-vtep-1(config-if)# ip address 20.1.1.1/30
switch-vtep-1(config-if)# ip router ospf 1 area 0.0.0.0
switch-vtep-1(config-if)# ip pim sparse-mode

switch-vtep-1(config)# interface port-channel 10
switch-vtep-1(config-if)# vpc 10
switch-vtep-1(config-if)# switchport
switch-vtep-1(config-if)# switchport mode access
switch-vtep-1(config-if)# switchport access vlan 10
switch-vtep-1(config-if)# no shutdown
switch-vtep-1(config)# interface e1/1
switch-vtep-1(config-if)# channel-group 10 mode active
switch-vtep-1(config-if)# no shutdown

switch-vtep-1(config)# interface nve1
switch-vtep-1(config-if)# no shutdown
switch-vtep-1(config-if)# source-interface loopback0

switch-vtep-1(config-if)# member vni 10000 mcast-group 230.1
switch-vtep-1(config)# vlan 10
switch-vtep-1(config-vlan)# vn-segment 10000
switch-vtep-1(config-vlan)# exit
```

```
switch-vtep-1(config)# feature nv overlay
switch-vtep-1(config)# feature vn-segment-vlan-based

switch-vtep-1(config)# feature ospf
switch-vtep-1(config)# feature pim
switch-vtep-1(config)# router ospf 1
switch-vtep-1(config-router)# router-id 200.200.200.1
switch-vtep-1(config)# ip pim rp-address 10.1.1.1 group-list 224.0.0.0/4
switch-vtep-1(config)# interface loopback0
switch-vtep-1(config-if)# ip address 200.200.200.1/32
switch-vtep-1(config-if)# ip address 100.100.100.1/32 secondary
switch-vtep-1(config-if)# ip router ospf 1 area 0.0.0.0
switch-vtep-1(config-if)# ip pim sparse-mode
switch-vtep-1(config)# interface e2/1
switch-vtep-1(config-if)# ip address 20.1.1.1/30
switch-vtep-1(config-if)# ip router ospf 1 area 0.0.0.0
switch-vtep-1(config-if)# ip pim sparse-mode

switch-vtep-1(config)# interface port-channel 10
switch-vtep-1(config-if)# vpc 10
switch-vtep-1(config-if)# switchport
switch-vtep-1(config-if)# switchport mode access
switch-vtep-1(config-if)# switchport access vlan 10
switch-vtep-1(config-if)# no shutdown
switch-vtep-1(config)# interface e1/1
switch-vtep-1(config-if)# channel-group 10 mode active
switch-vtep-1(config-if)# no shutdown

switch-vtep-1(config)# interface nve1
switch-vtep-1(config-if)# no shutdown
switch-vtep-1(config-if)# source-interface loopback0

switch-vtep-1(config-if)# member vni 10000 mcast-group 230.1.1.1
switch-vtep-1(config)# vlan 10
switch-vtep-1(config-vlan)# vn-segment 10000
switch-vtep-1(config-vlan)# exit
```

SSH to every switch, Assign IP Address, Enable Telnet/SSH, Add users on every switch/Create ACLs (optional)

(Times X Switches & Y VNIs)

NOW

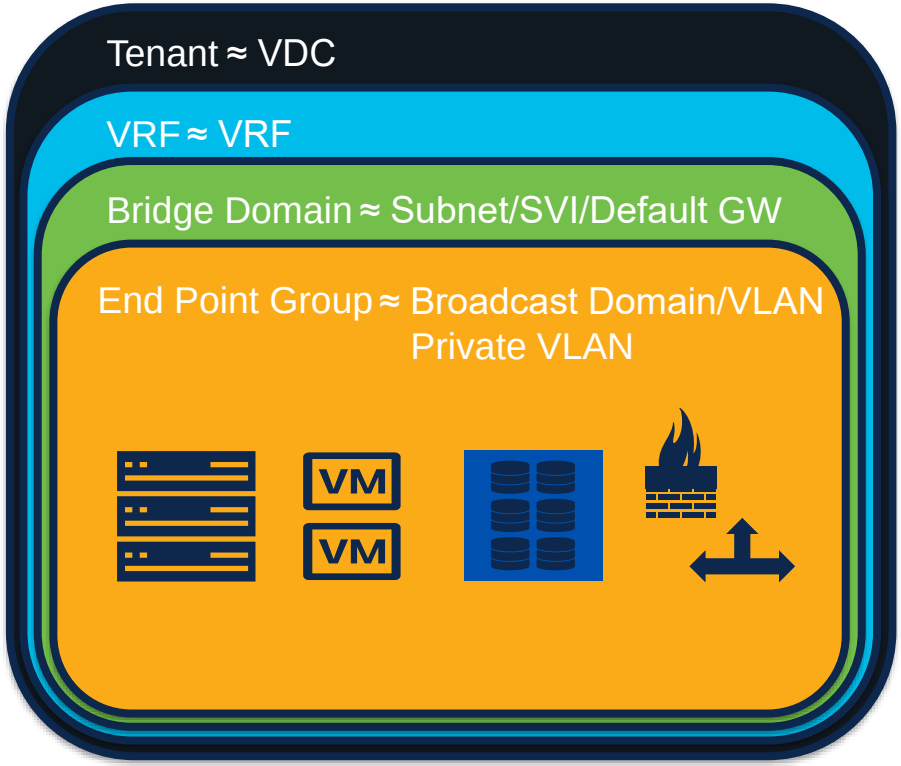
- External to Internal Route redistribution & Control Plane (MP-BGP, QoS, etc)
- Multicast (BD GIPo Addressing)
- Overlay Network (VXLAN)
- Underlay Routed Network (IS-IS)
- Switch management & Best Practices

ACI Automated tasks
From HOURS to seconds!

ACI Policy Model Simplified

cisco Live!

The ACI Policy Model



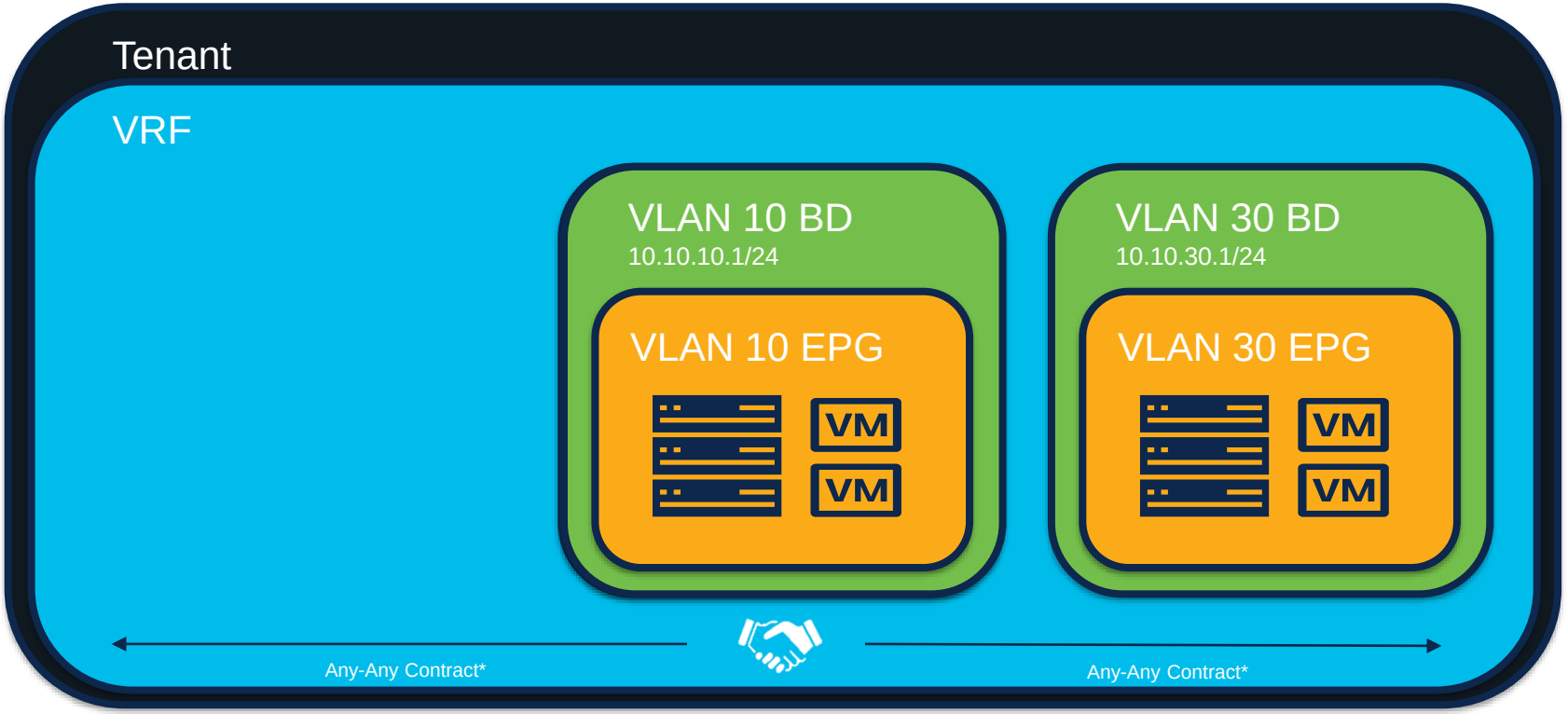
Contracts ≈ Access Lists

L2 External EPG ≈ 802.1q Trunk

L3 External EPG ≈ L3 Routed Link

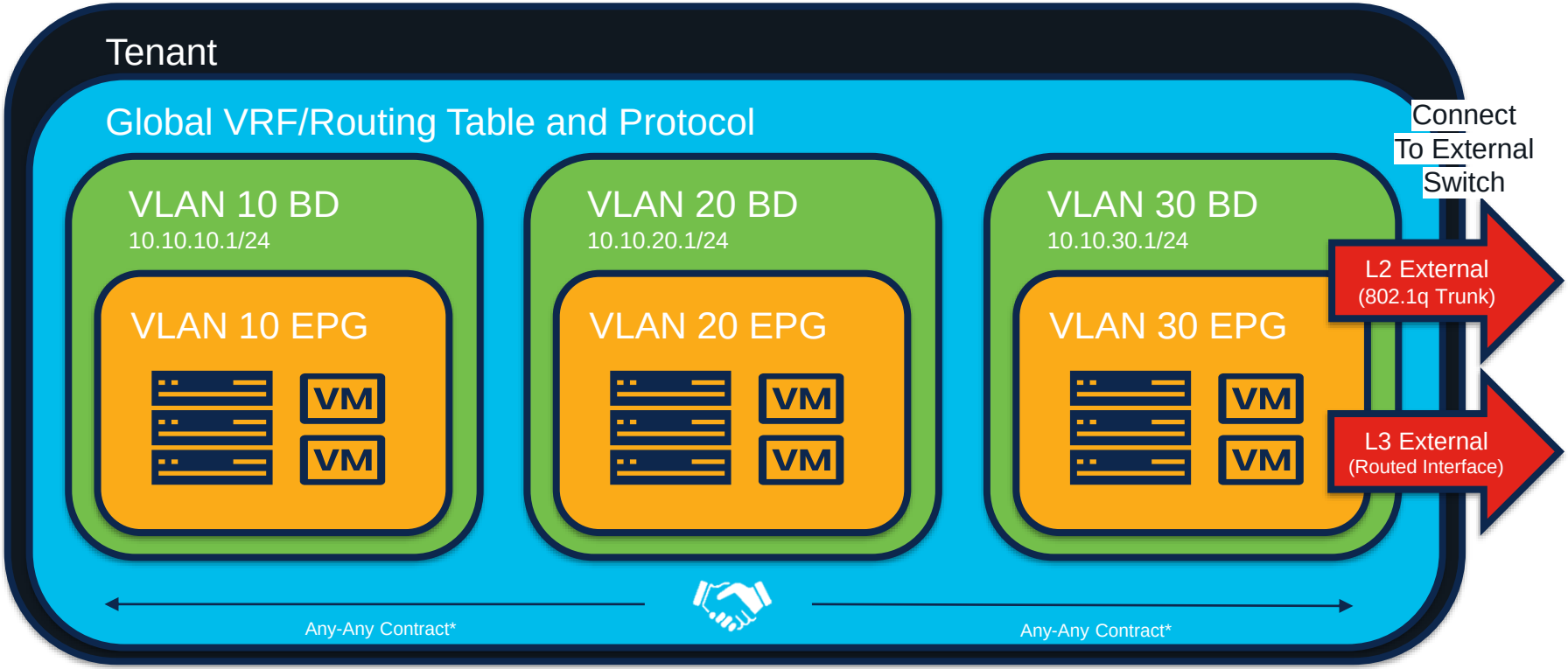
* Preferred group or vzAny achieve the same outcome

The ACI Policy Model – Migrating into ACI



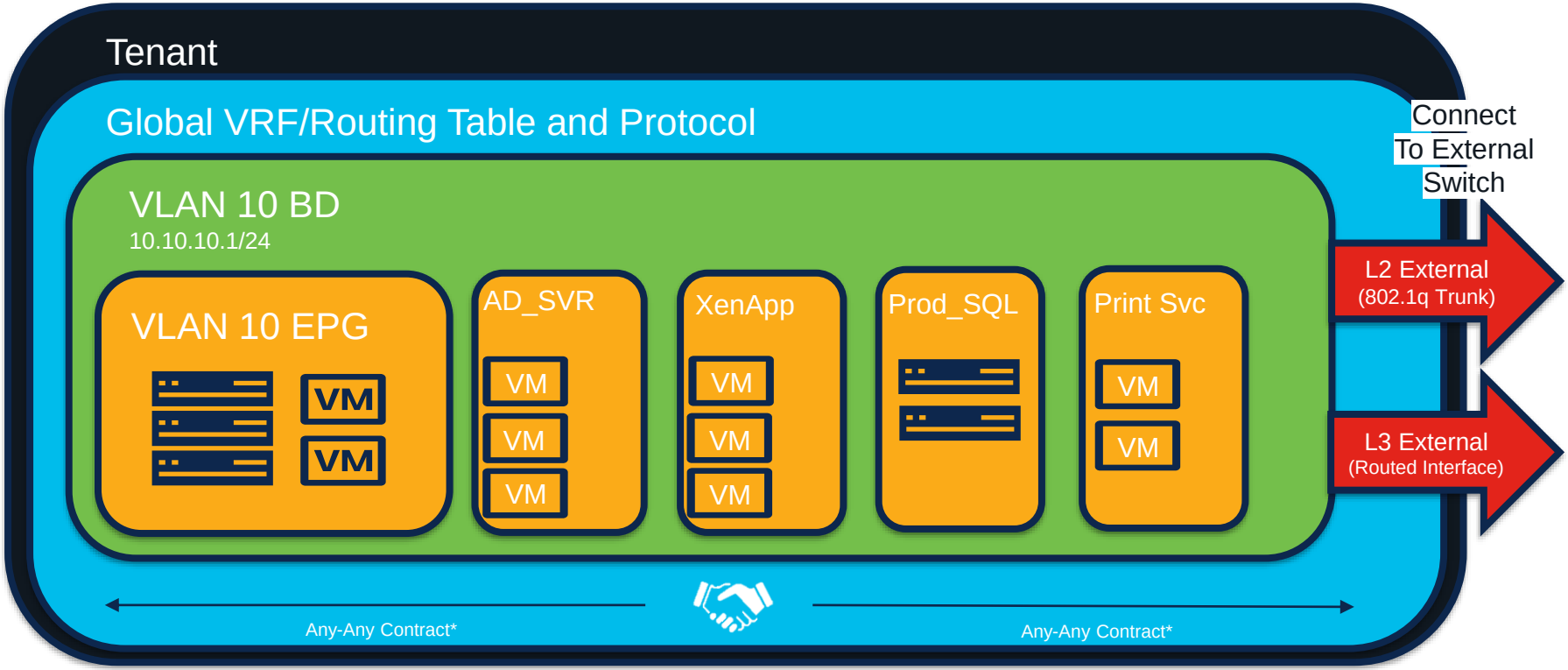
* Preferred group or vzAny achieve the same outcome

The ACI Policy Model – Migrating into ACI



* Preferred group or vzAny achieve the same outcome

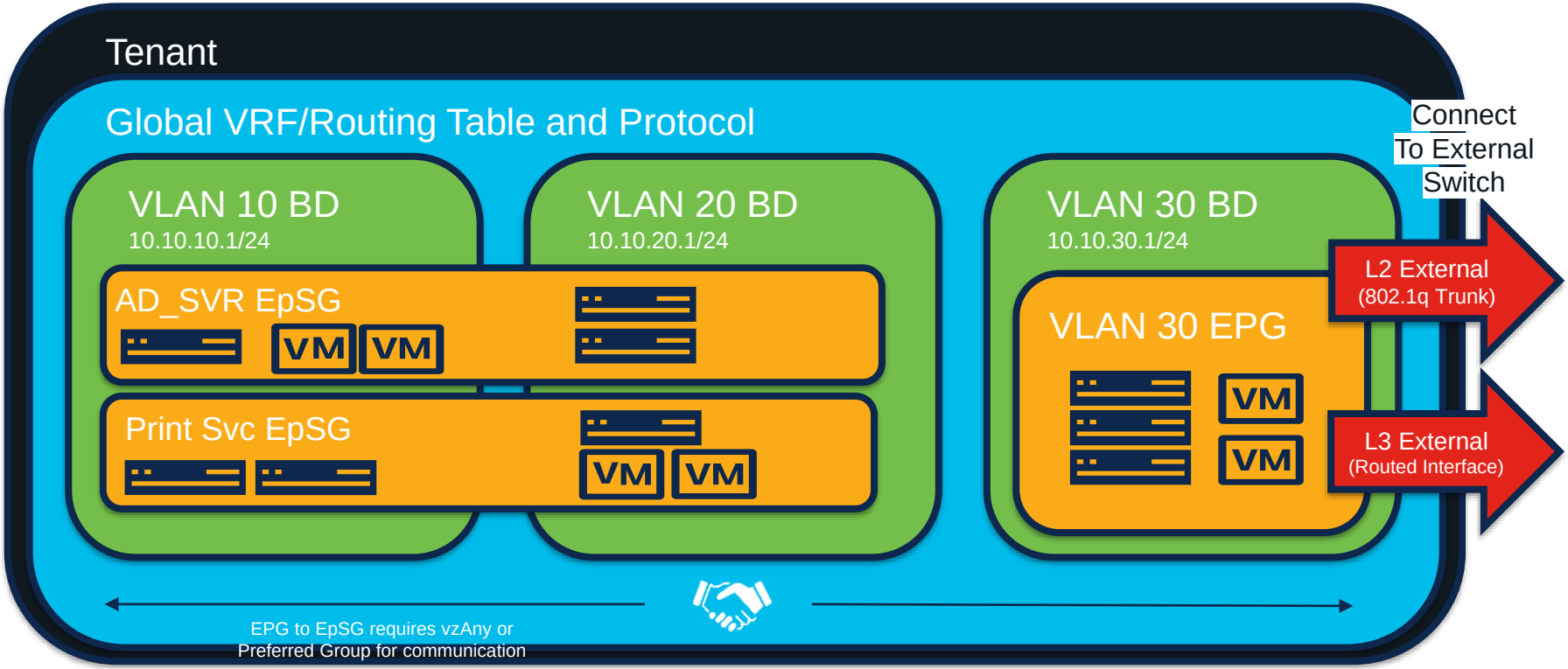
The ACI Policy Model – Extending the configuration
Endpoint Groups



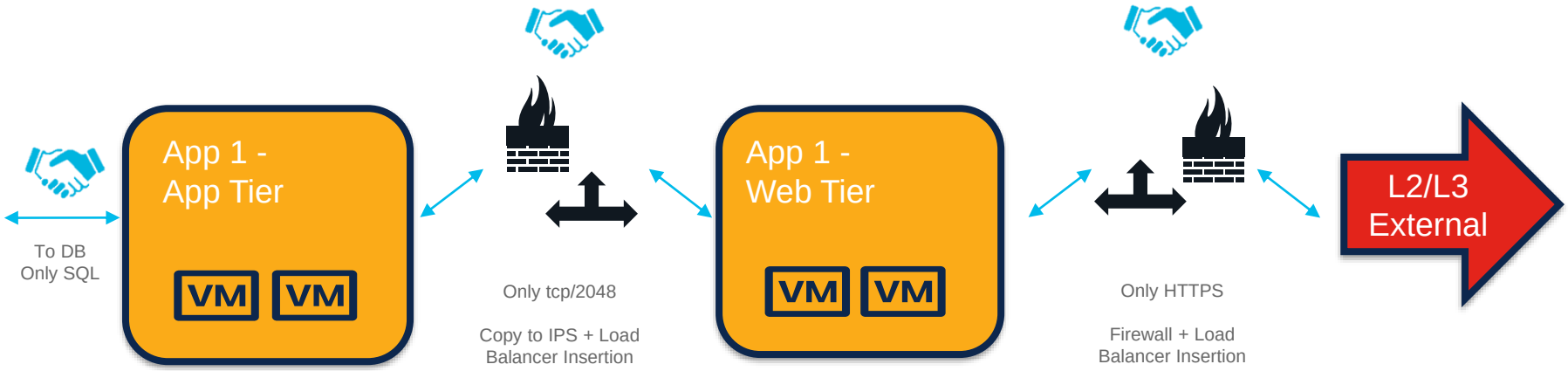
* Preferred group or vzAny achieve the same outcome

The ACI Policy Model – Extending the configuration

Endpoint Security Groups - ACI 5.0 and greater



Advancing the ACI Configuration



Policy Based Redirect with Service Graphs

ACI
Deployment Options

ACI Anywhere

Edge / Remote

Core Data Centers

Hybrid Cloud & Multicloud

IP WAN

IP WAN

ACI
Remote Leaf

ACI
Single-POD

ACI
Multi-POD

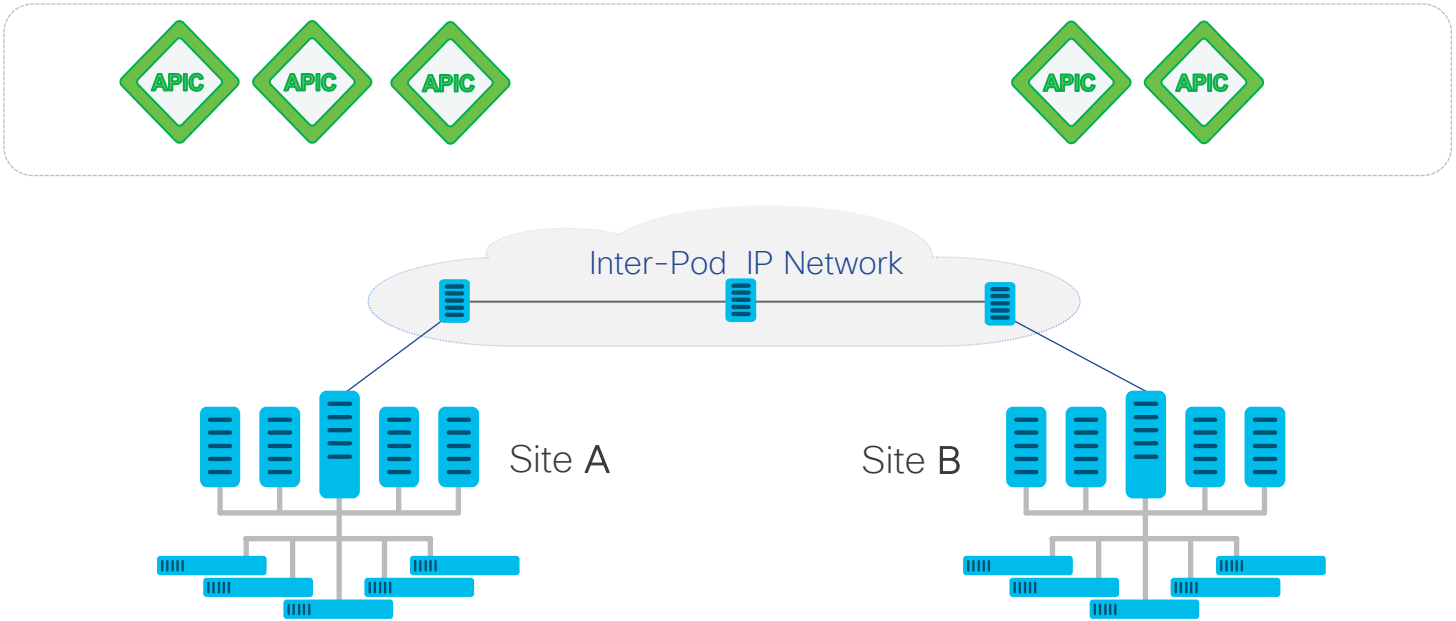
ACI
Multisite

Cloud
ACI

The easiest Data Center and Cloud Interconnect Solution in the Market **Try it today!**

ACI MultiPod

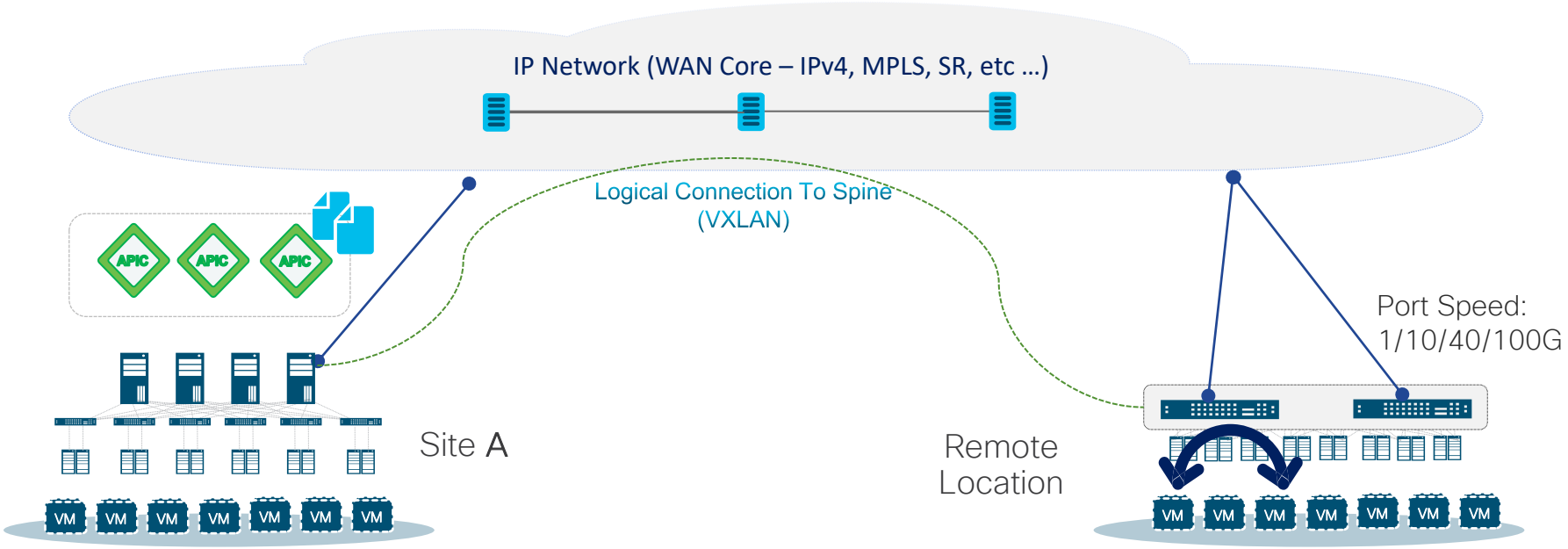
The evolution of a stretched fabric



Active-Active Datacenters | Virtual Metro Clusters | Stretch VRF, EPG, BD Across PoDs with VXLAN | Up to 50ms Latency / 500 Switches

ACI: Physical Remote Leaf

Extend ACI to Satellite Data Centers



Zero Touch Auto Discovery of Remote Leaf

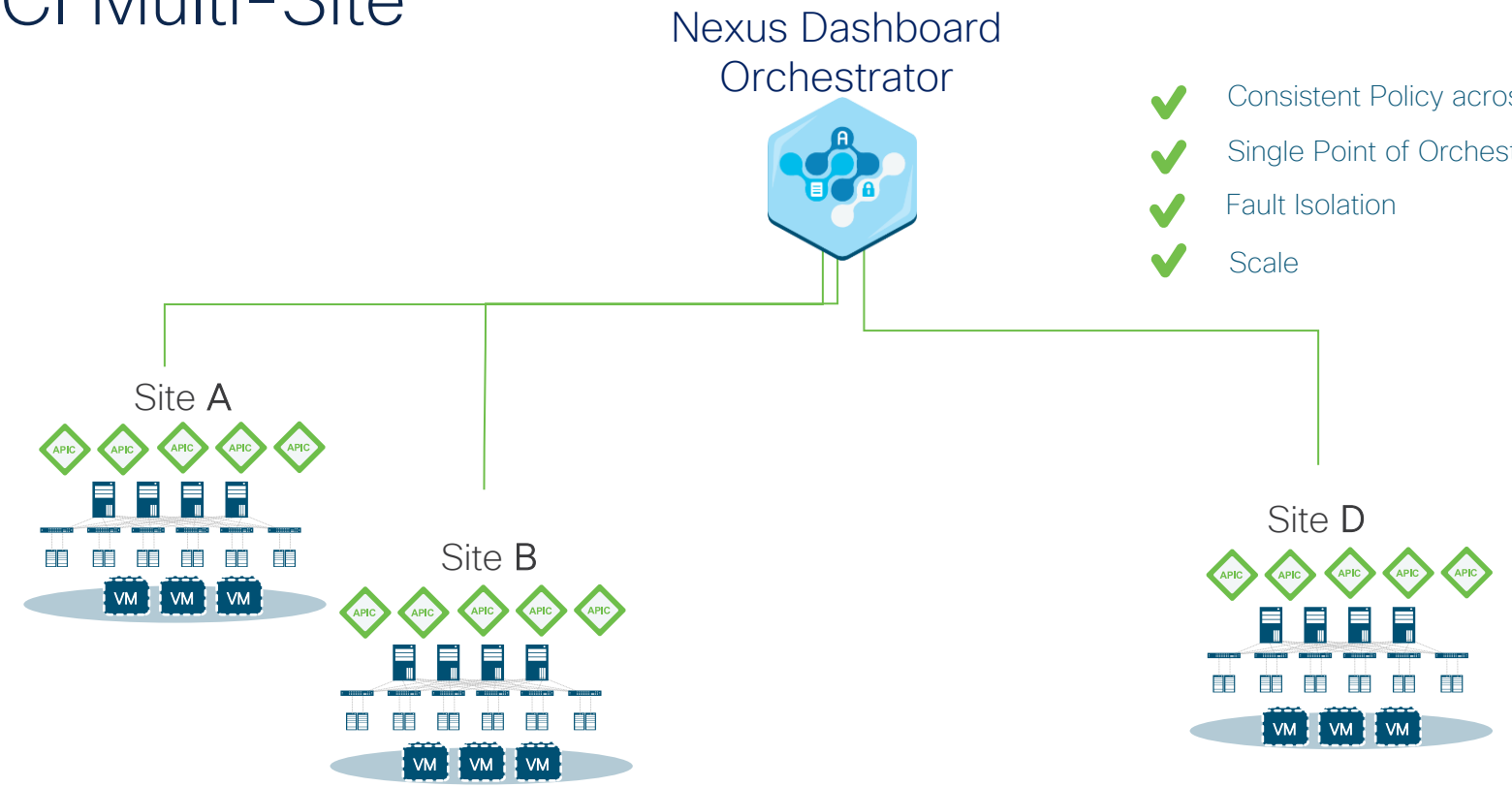
Two switches per site
Up To 200 Remote Leaf Switches (ACI 6.0)

Stretch EPG, BD, VRF, Tenant, Contract

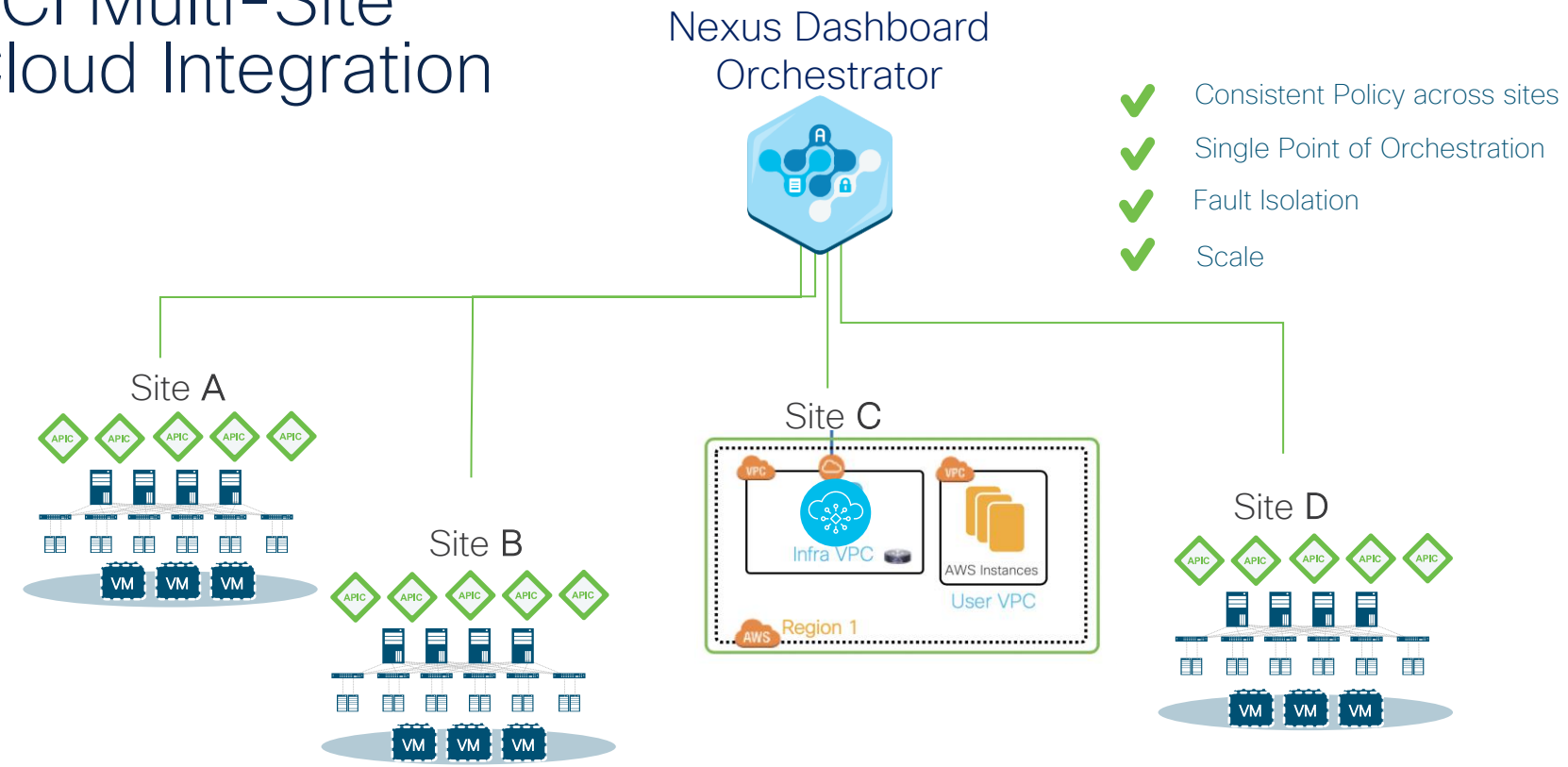
DC Migration / OTV replacement

cisco Live!

ACI Multi-Site



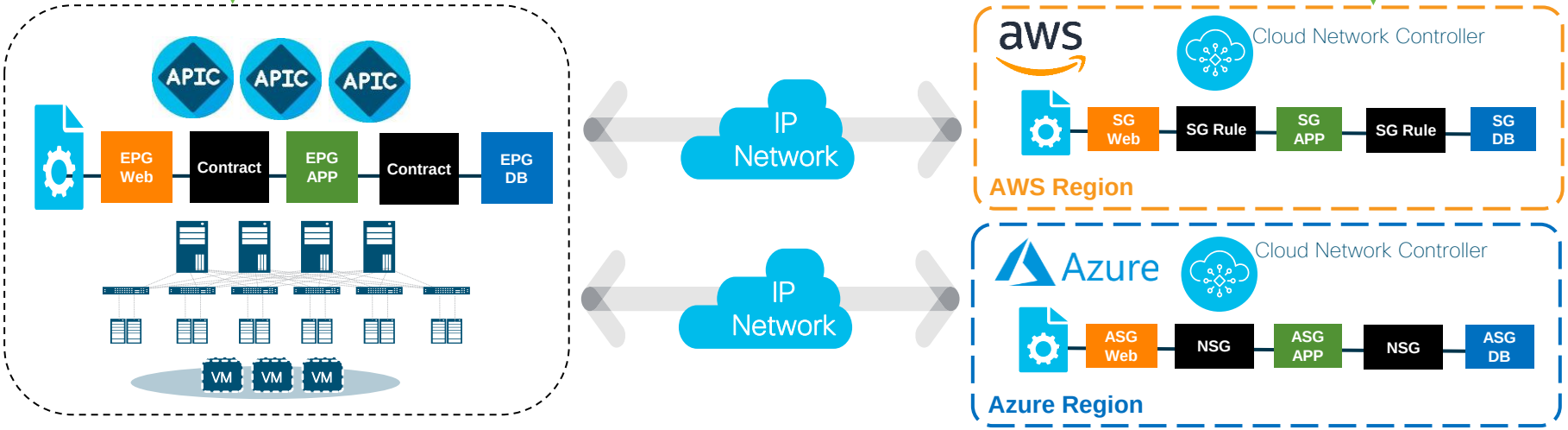
ACI Multi-Site Cloud Integration



Policy Consistency | Single Point Of Orchestration | Availability Fault Isolation | Scale

ACI Extension to Cloud

Nexus Dashboard Orchestrator



Consistent Policy Enforcement on-Premises & Public Cloud

Automated Inter-connect provisioning

Simplified Operations with end-to-end visibility

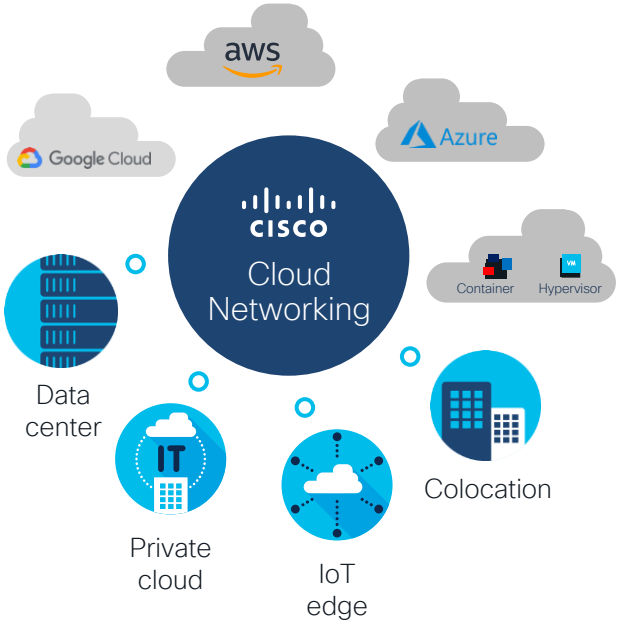
The network-admin challenge

Provisioning and monitoring complexity = Risk

NX-OS	ACI	aws		
Separate Infrastructure + VXLAN	Tenant	Account	Subscription/ Resource Group	Account/Project
Data Center	Site/Pod	Region	Region	Region
VRF	VRF	VPC	VNet	VPC
VLAN	Bridge Domain/ Subnet	CIDR/Subnet	Subnet	Subnet
VLAN Tag	Endpoint Groups / Endpoint Security Groups	Security Groups	Application/Network Security Groups	Firewall
Access-list (ACL)	Contracts & Filters	Security Group Rules	Security Rules	Firewall Rules

ACI
Day 2 and Beyond

Cloud Networking: Challenges



Connectivity and management

Workloads are increasingly distributed and diverse. Complex to connect workloads across multiple public cloud providers, data centers and edge locations.

Visibility and automation

Troubleshooting challenges due to more decentralized architectures with different environments.

Zero trust and security

Workload migration and mobility of users imposes significant challenges to enforce right security policies across different environments.

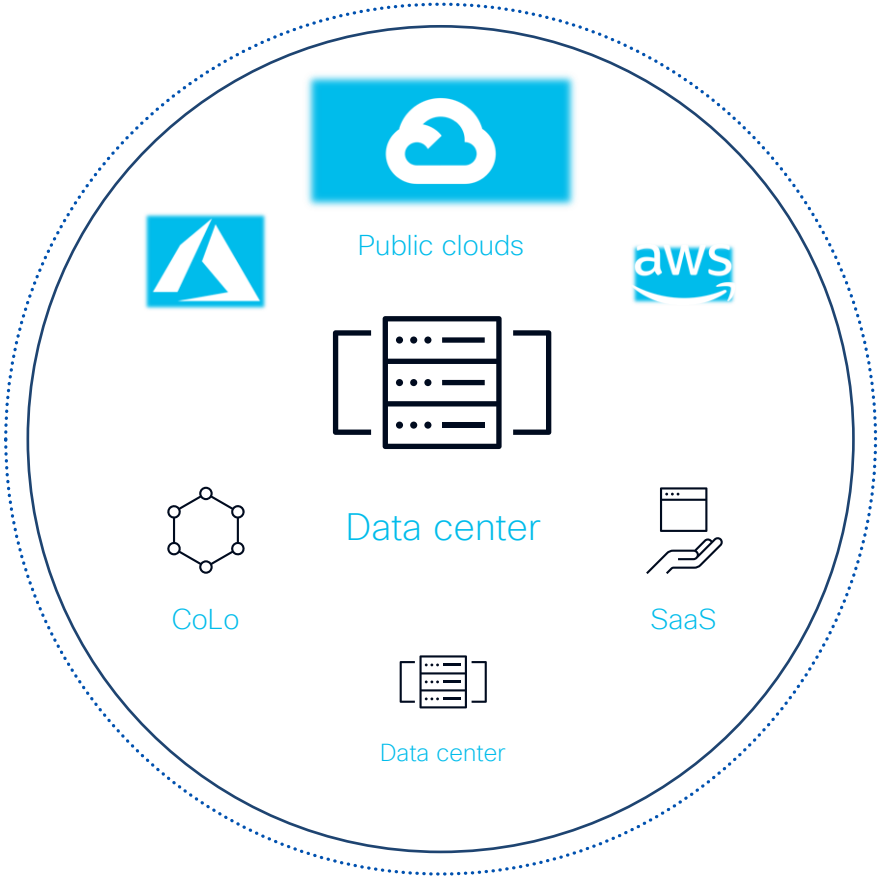
Need for homogenous experience across heterogenous cloud environments

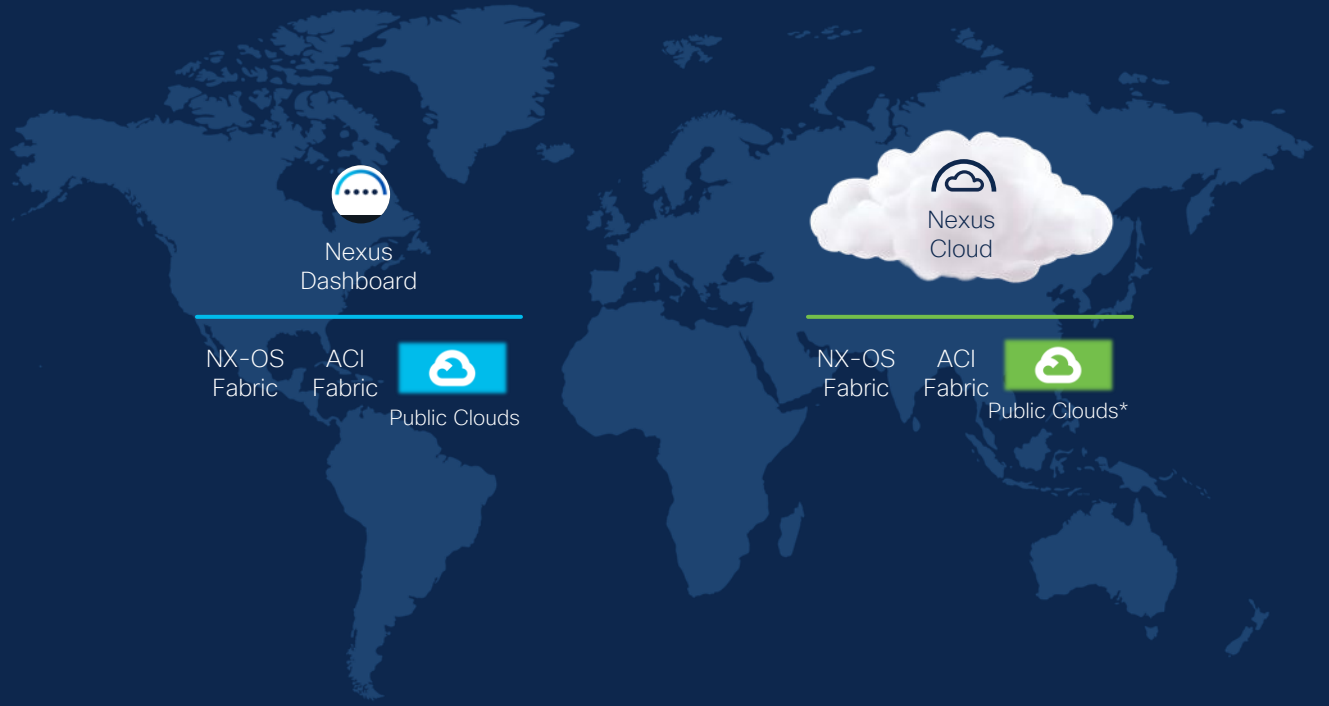
Solving the customer complexity

Customer Needs

Cloud-delivered or On-premise
Agility | Simplicity | Turn-key

High performance infrastructure
Speed | Scale | Sustainability





* Roadmap

For locally hosted operations
Cisco Nexus Dashboard

For cloud managed operations
Cisco Nexus Cloud

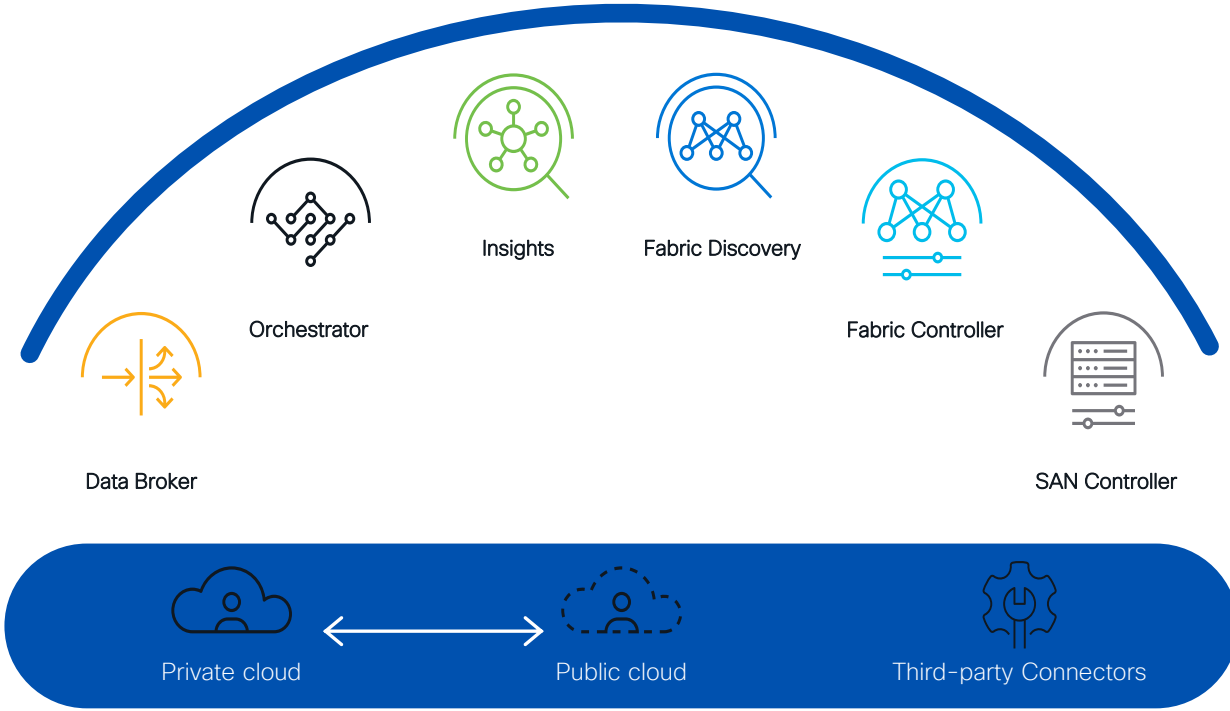
Flexibility and choice

Cisco Nexus Dashboard

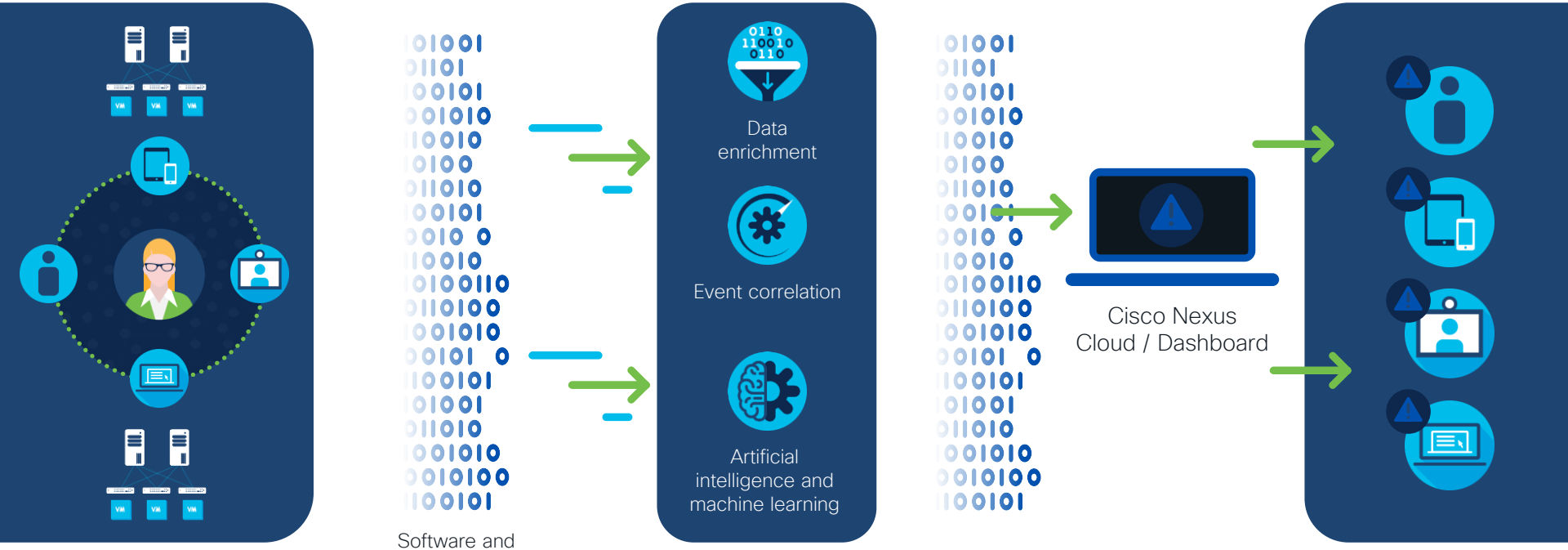
Simple to automate, simple to consume

Cisco Nexus Dashboard

Powering automation
Unified agile platform



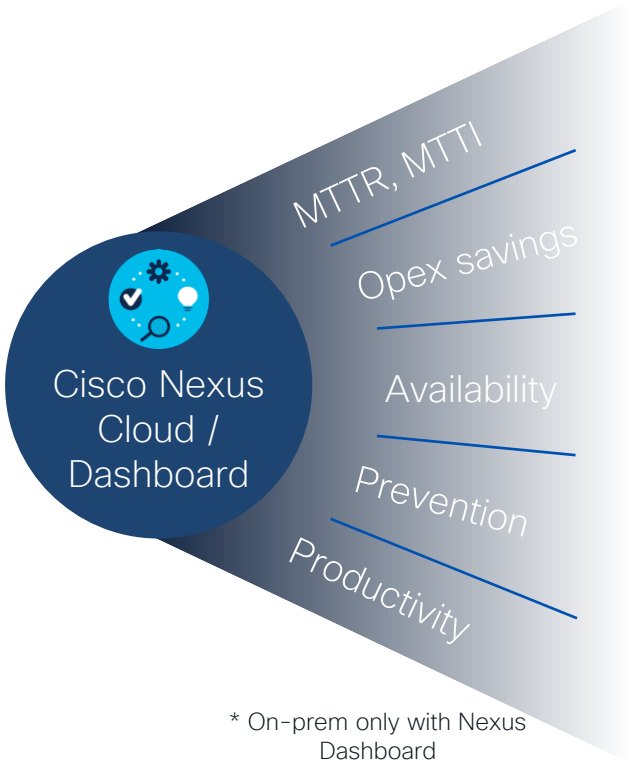
How it works



Software and hardware telemetry (HW telemetry not yet supported with Nexus Cloud)

Cisco Nexus Cloud / Dashboard

Use cases and benefits



* On-prem only with Nexus Dashboard

- Identify, locate, root cause, remediate
- Upgrade impact advisories
- Error detection, latency, packet drops*
  Control plane issue
- Mitigate
  Prevent outages
- Automated alerts
  Explorer
- Hardening checks
  Software hardware recommendations
- Pre-change analysis*
  Compliance alerts
- PSIRT notices
  EoS/EoL notices
- End-to-end workflows
  Guided remediation
- TAC assist
  Topology checker

Key Takeaways

- Consistent SDN enabled network policy across all the switches within a fabric
- The Multi-site architecture allows the same network policy to be applied across multiple sites, even cloud
- Nexus Cloud and Dashboard enables proactive day 2 operations for ACI to give a better understanding of how the applications interact with network

Technical Session Surveys

- Attendees who fill out a minimum of four session surveys and the overall event survey will get Cisco Live branded socks!
- Attendees will also earn 100 points in the Cisco Live Game for every survey completed.
- These points help you get on the leaderboard and increase your chances of winning daily and grand prizes.

Complete your Session Survey

- Please complete your session survey after each session. Your feedback is important.
- Complete a minimum of 4 session surveys and the Overall Conference survey (open from Thursday) to receive your Cisco Live t-shirt.

- All surveys can be taken in the Cisco Events Mobile App or by logging in to the Session Catalog and clicking the "Attendee Dashboard" at https://www.ciscolive.com/emea/learn/sessions/session-catalog.html

Continue Your Education

Visit the Cisco Showcase for related demos.

Book your one-on-one Meet the Engineer meeting.

Attend any of the related sessions at the DevNet, Capture the Flag, and Walk-in Labs zones.

Visit the On-Demand Library for more sessions at ciscolive.com/on-demand.

Early Access. Yes, please.

Cisco U.

Tech learning, shaped to you.

cisco


cisco
The bridge to possible
Thank you
cisco Live!


CISCO Live!
ALL IN