
cisco Live!
ALL IN

The bridge to possible

Intro to ACI

Chris Merkel – Cross Solution DC TSA

BRKDCN-1001

Cisco Webex App

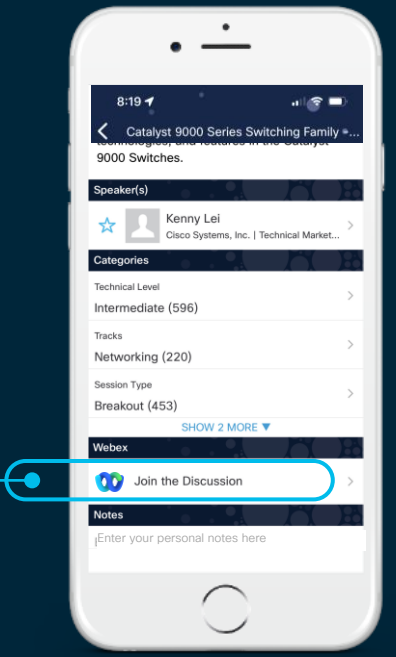
Questions?

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 by the speaker until June 17, 2022.



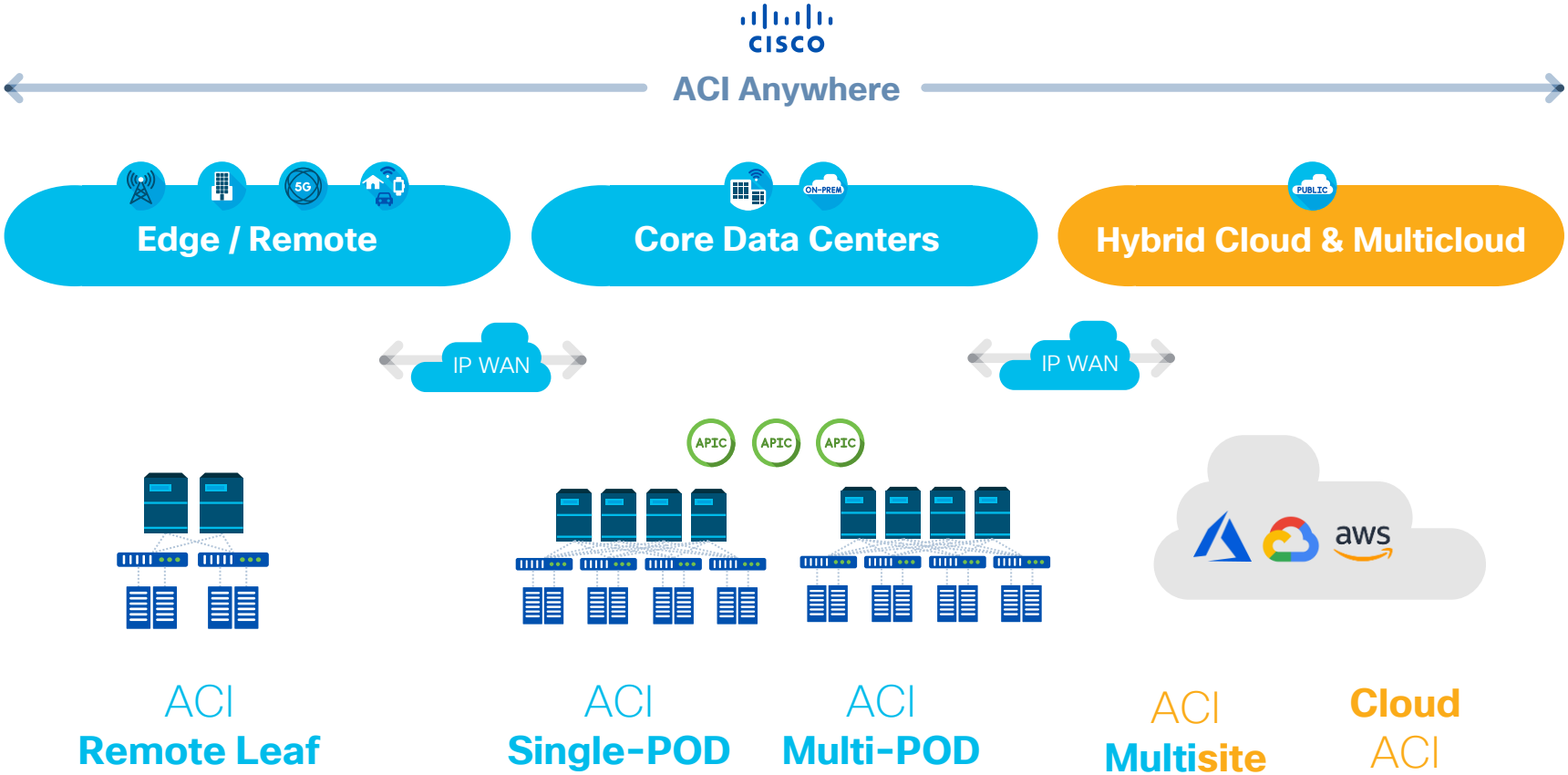
https://ciscolive.ciscoevents.com/ciscolivebot/#BRKDCN-1001

Agenda

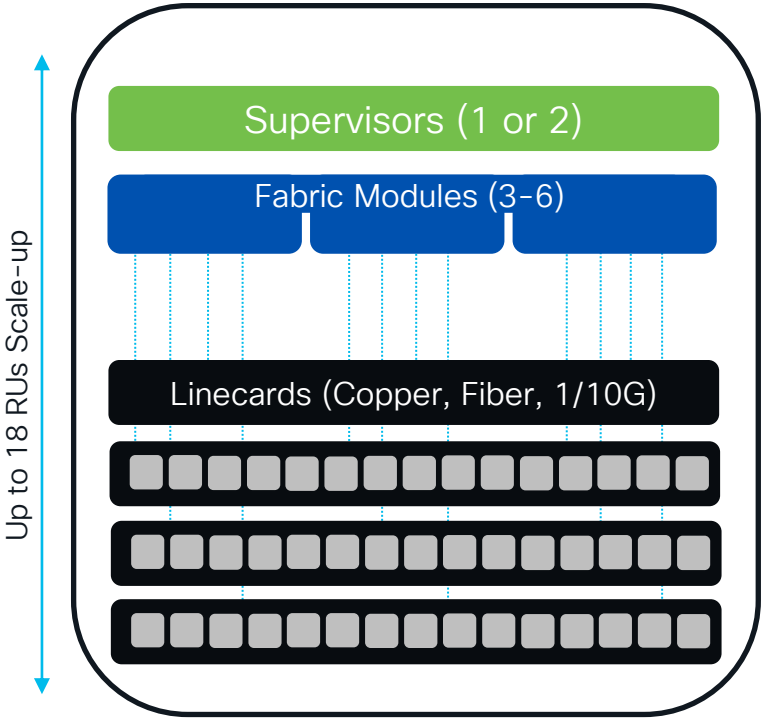
- Fabric Basics
- Policy Model
- Architectural Deployments
- Day 2 and beyond

Fabric Basics

ACI: One Network, any location

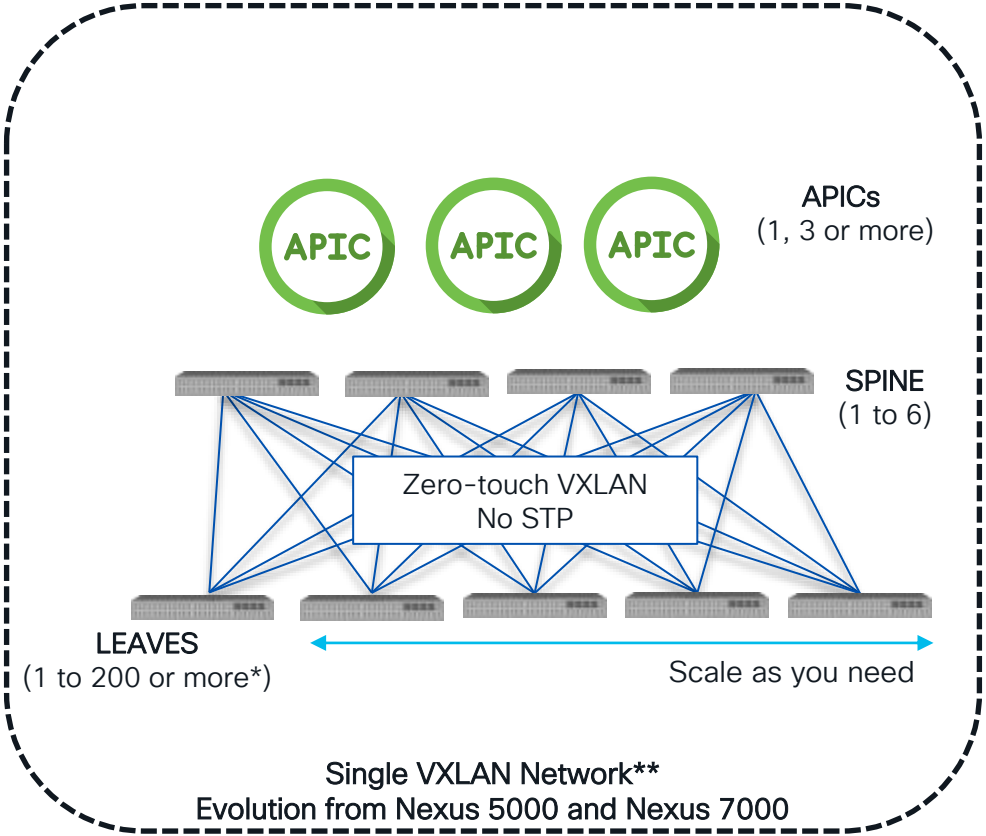


The DC network before
Classic modular switching



Single chassis (e.g. Nexus 7000)

The DC network NOW
ACI



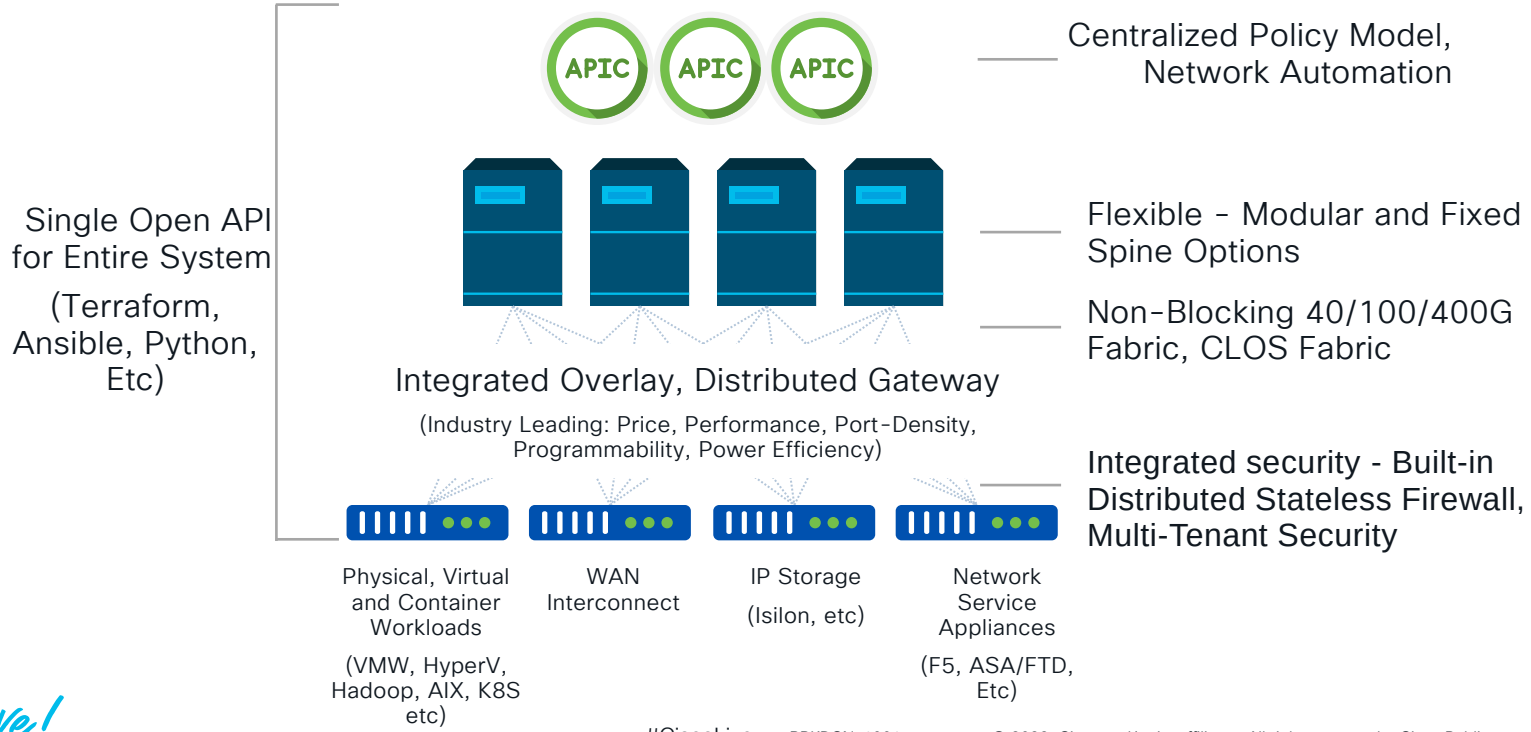
Single VXLAN Network**
Evolution from Nexus 5000 and Nexus 7000

cisco Live!

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

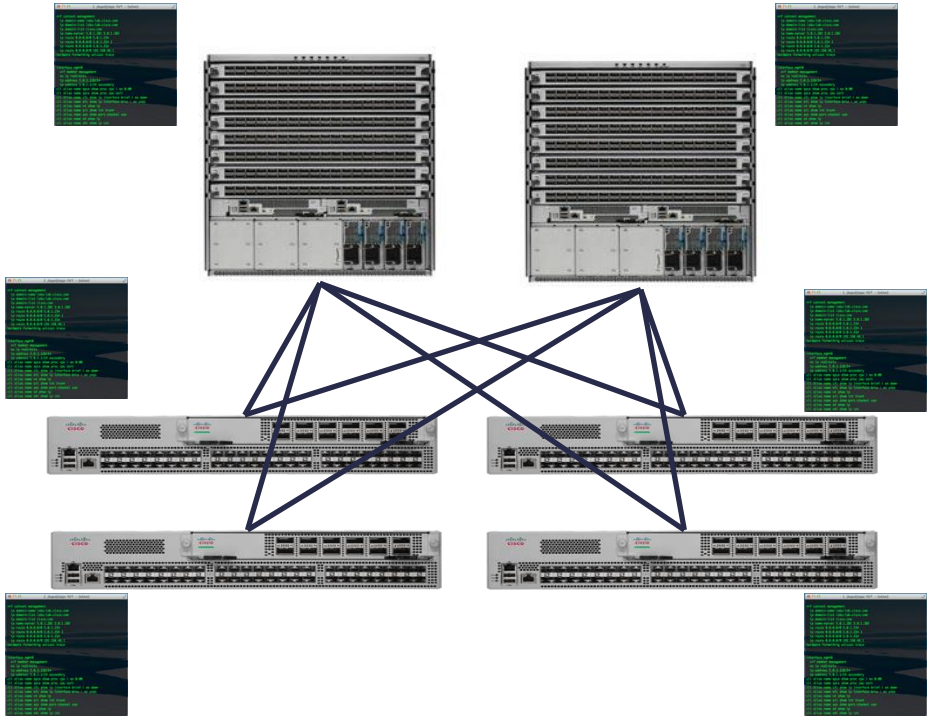
Application Centric Infrastructure Building Blocks

Built on the Nexus 9000



Traditionally, 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)

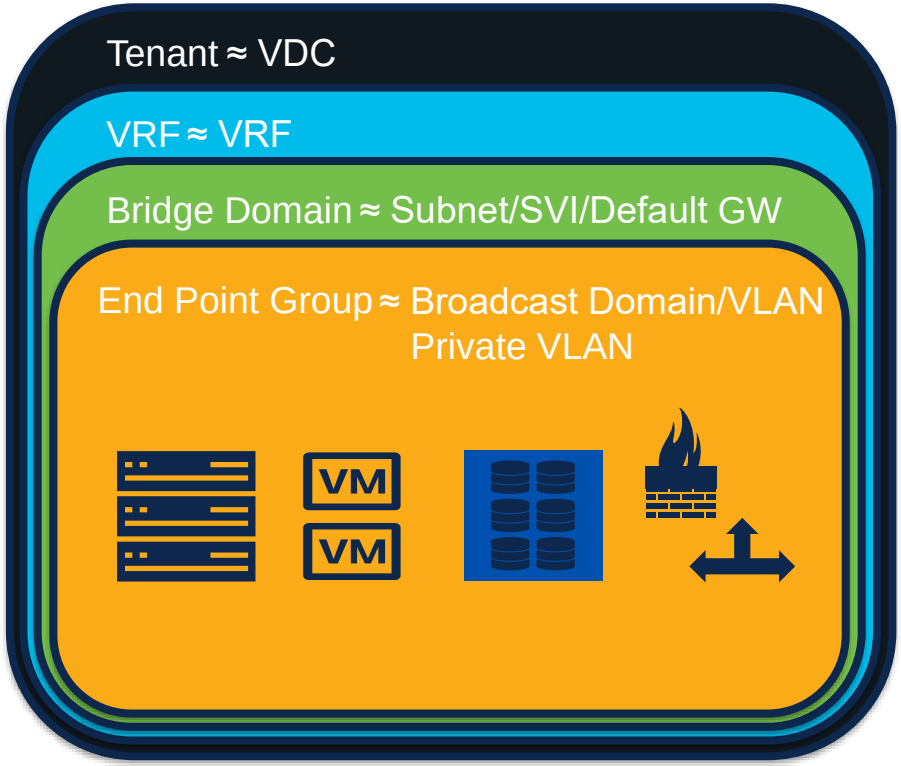
NOW

- 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!
Single Dashboard

ACI Policy Model Simplified

The ACI Policy Model



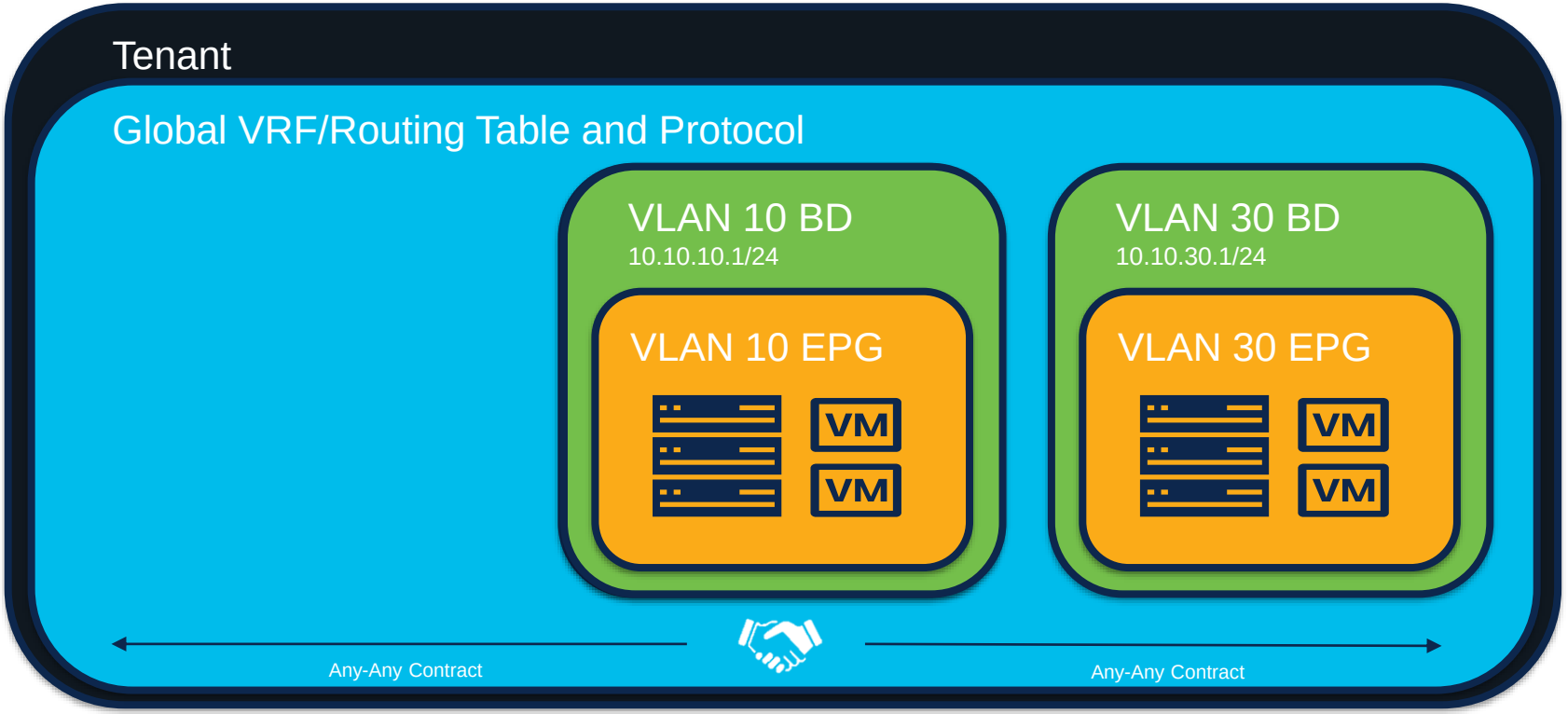
Contracts ≈ Access Lists

L2 External EPG ≈ 802.1q Trunk

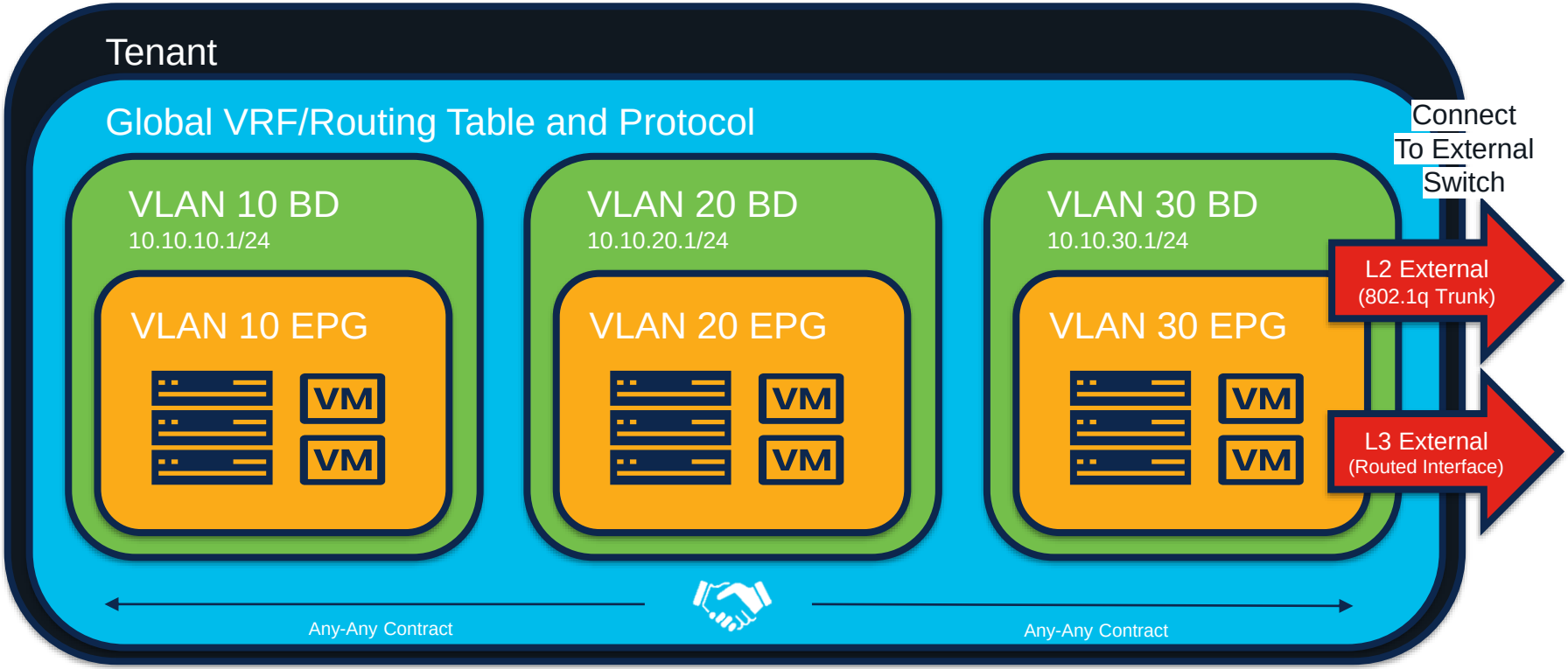
L3 External EPG ≈ L3 Routed Link

* Preferred group or vzAny achieve the same outcome

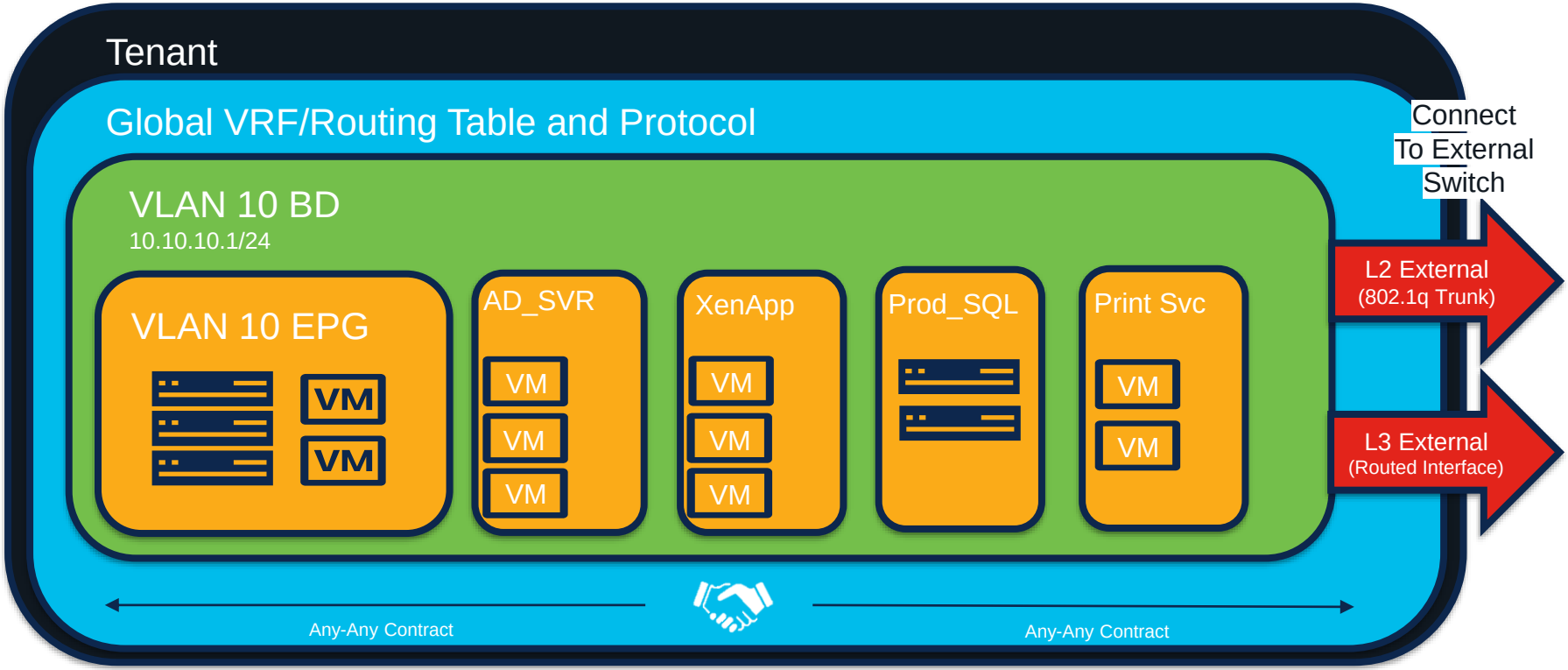
The ACI Policy Model – Migrating into ACI



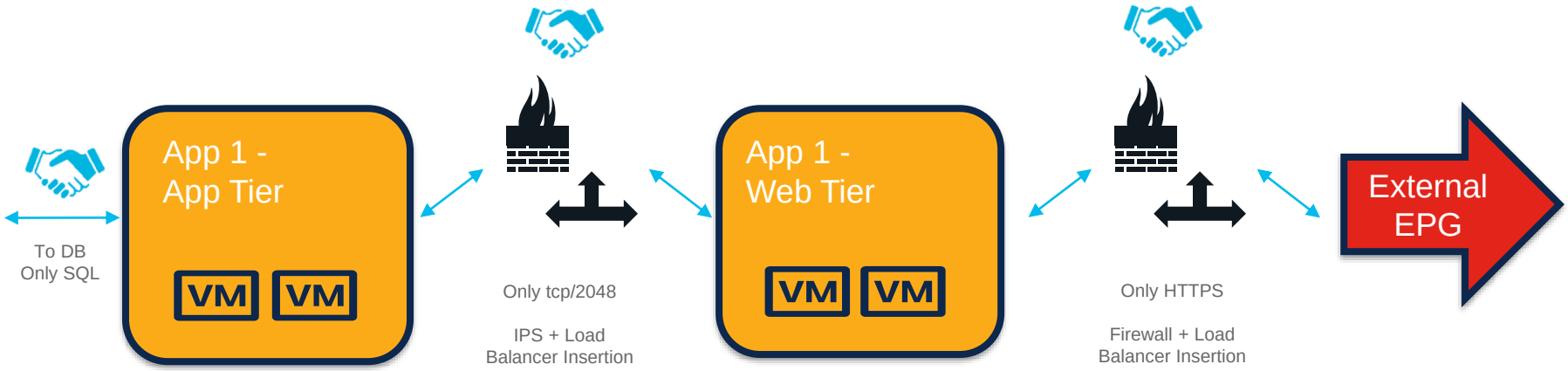
The ACI Policy Model – Migrating into ACI



The ACI Policy Model – Extending the configuration

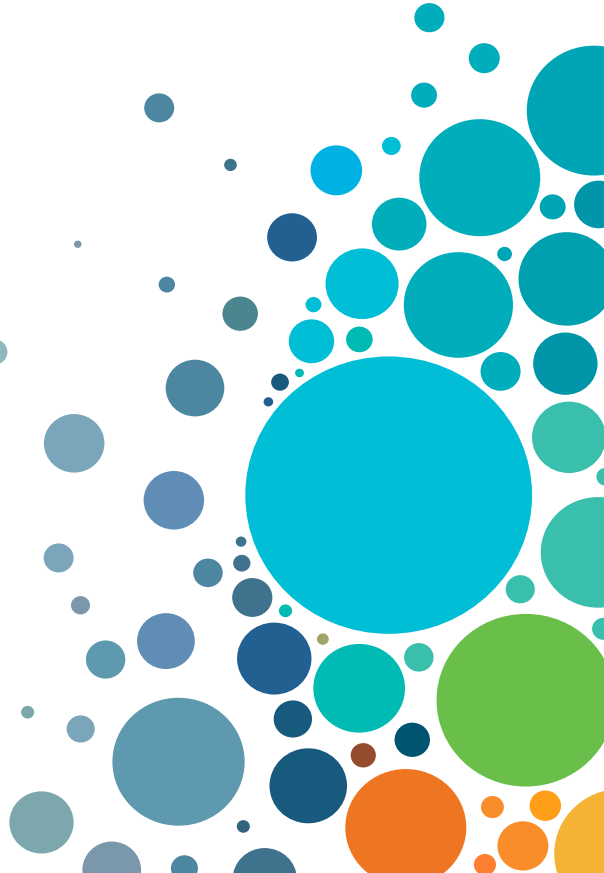


Advancing the ACI Configuration



Contracts with Policy Based Redirect

ACI Deployment Options



ACI Anywhere

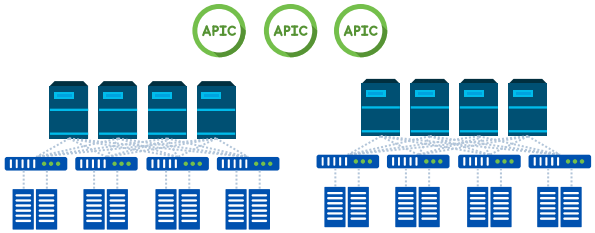
Edge / Remote

Core Data Centers

Hybrid Cloud & Multicloud

IP WAN

IP WAN



ACI
Remote Leaf

ACI
Single-POD

ACI
Multi-POD

ACI
Multisite

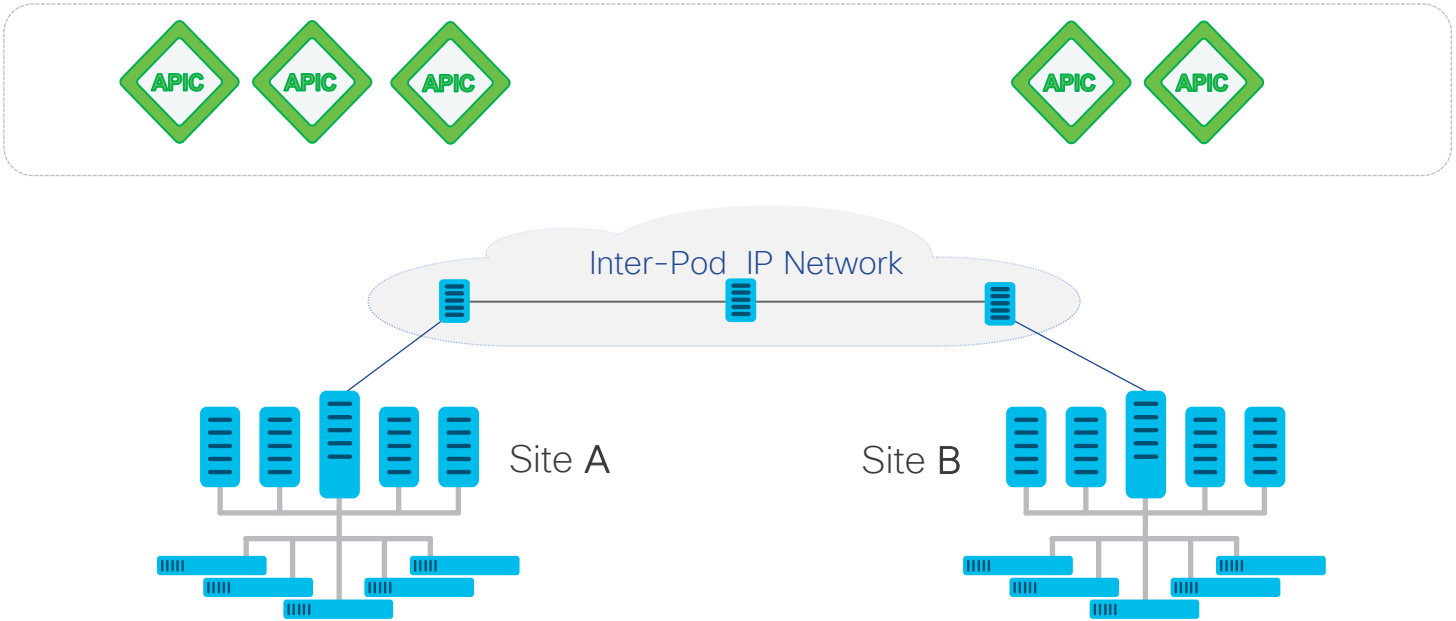
Cloud
ACI

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

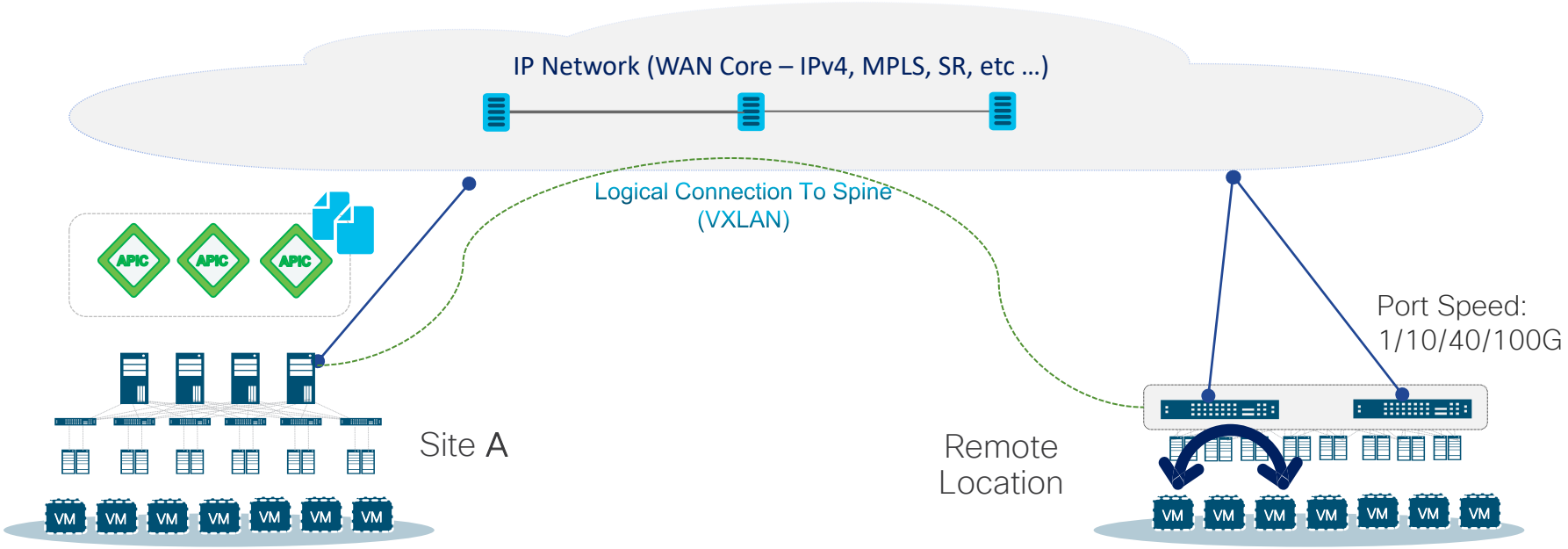
Virtual Metro Clusters

Stretch VRF, EPG, BD Across PoDs with VXLAN

Up to 50ms Latency

ACI: Physical Remote Leaf

Extend ACI to Satellite Data Centers



Zero Touch Auto Discovery of Remote Leaf

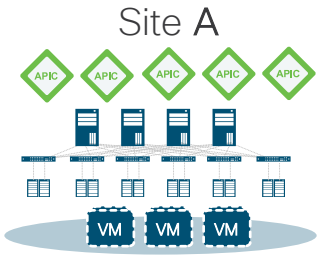
Two switches per site
Up To 128 Remote Leaf Switches

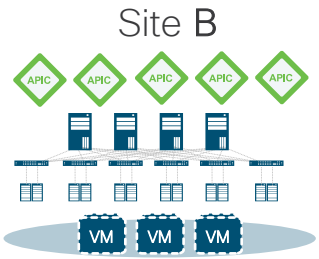
Stretch EPG, BD, VRF, Tenant, Contract

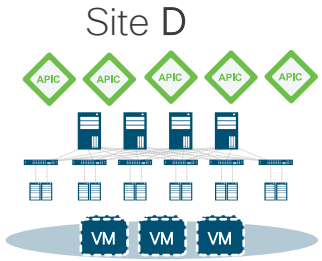
DC Migration / OTV replacement

ACI Multi-Site

- Consistent Policy across sites
- Single Point of Orchestration
- Fault Isolation
- Scale

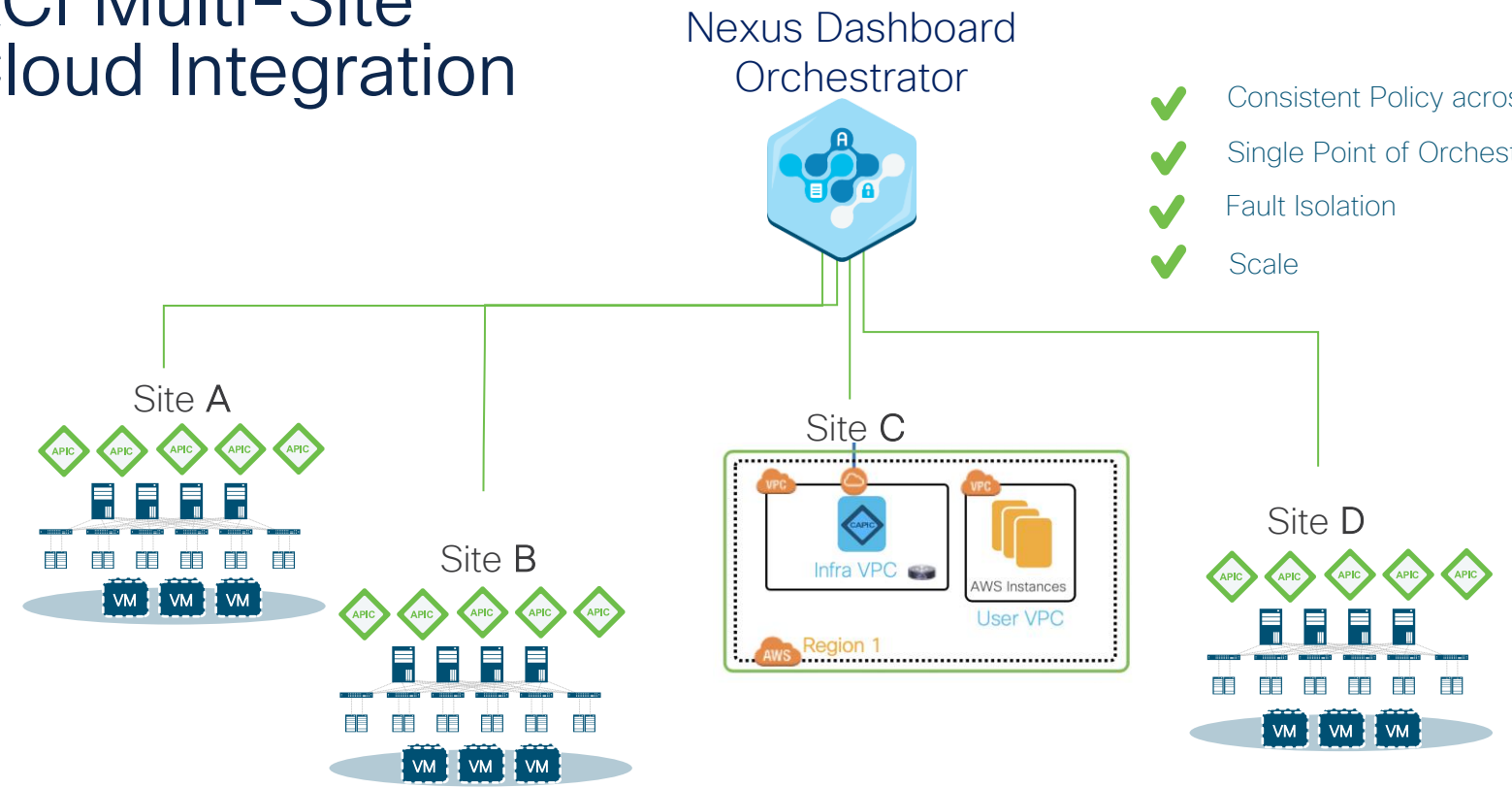






Policy Consistency | Single Point Of Orchestration | Availability Fault Isolation | Scale

ACI Multi-Site Cloud Integration



Policy Consistency

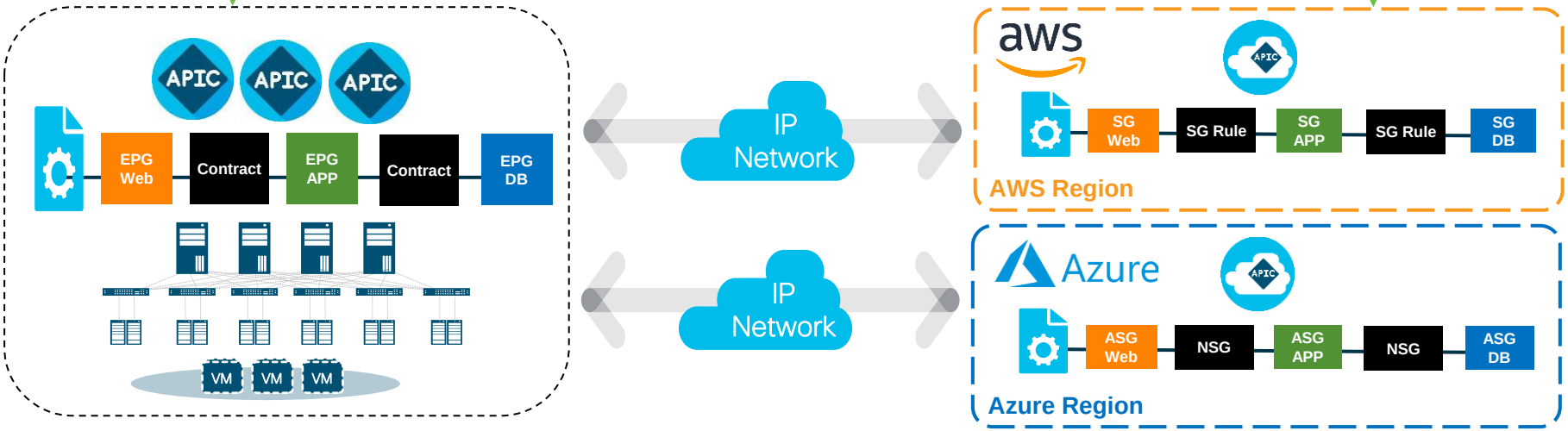
Single Point Of Orchestration

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

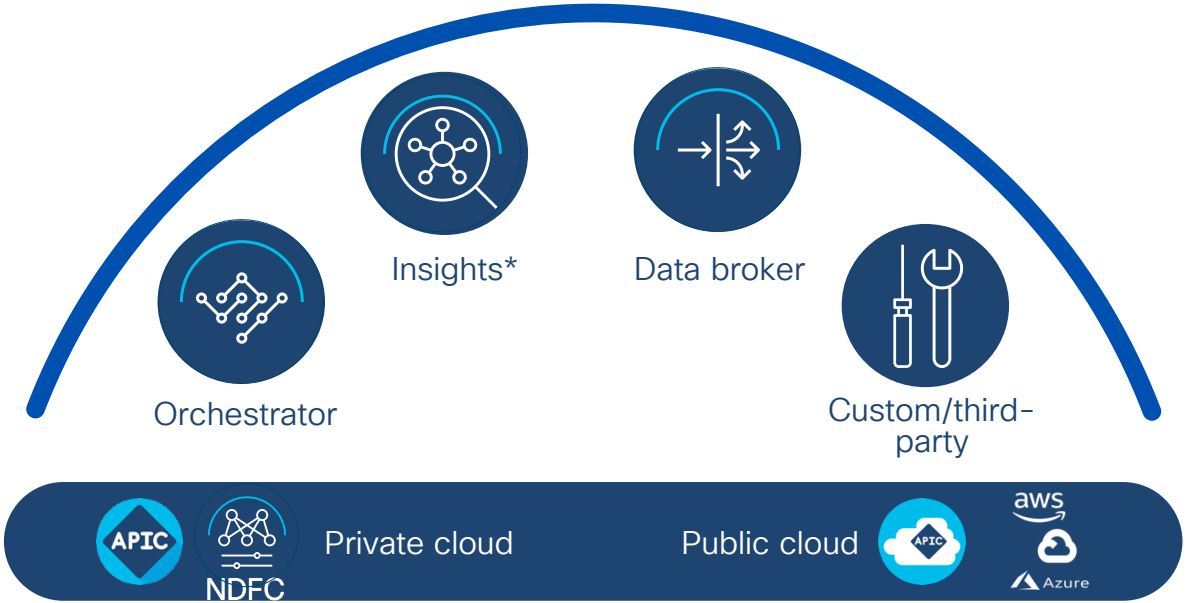
Provisioning and monitoring complexity = Risk

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	EPG	Security Groups	Application/Network Security Groups	Firewall
Access-list (ACL)	Contracts & Filters	Security Group Rules	Security Rules	Firewall Rules

ACI
Day 2 and Beyond

Cisco Nexus Dashboard
Simple to automate, simple to consume

Powering automation
Unified agile platform

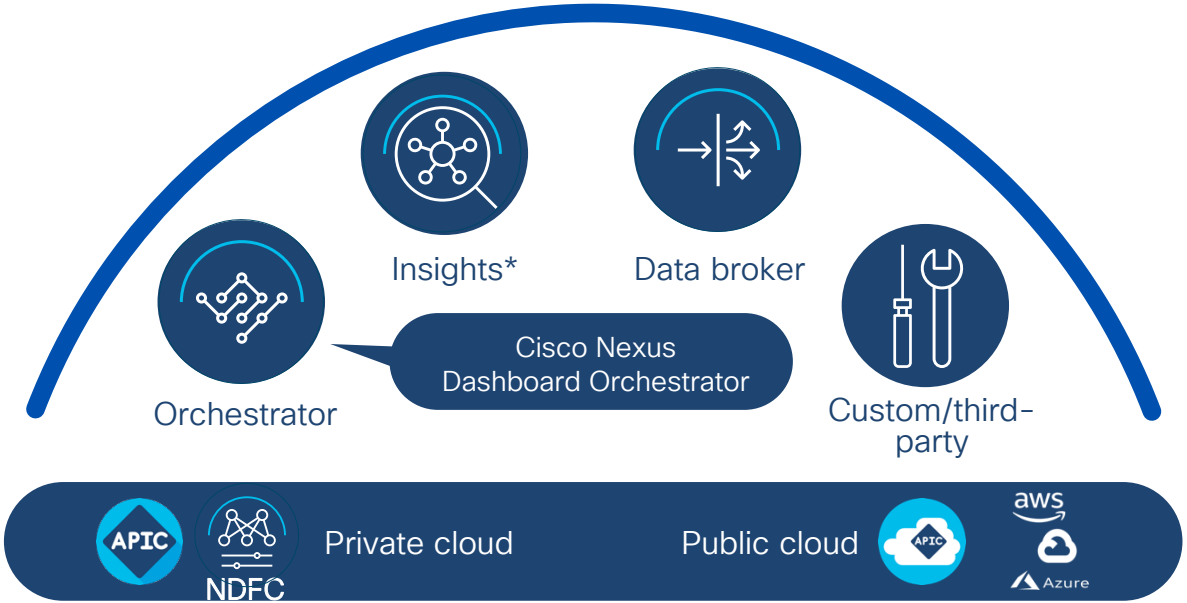


Consume all services in one place

* Includes Cisco Network Assurance Engine

Cisco Nexus Dashboard
Simple to automate, simple to consume

Powering automation
Unified agile platform



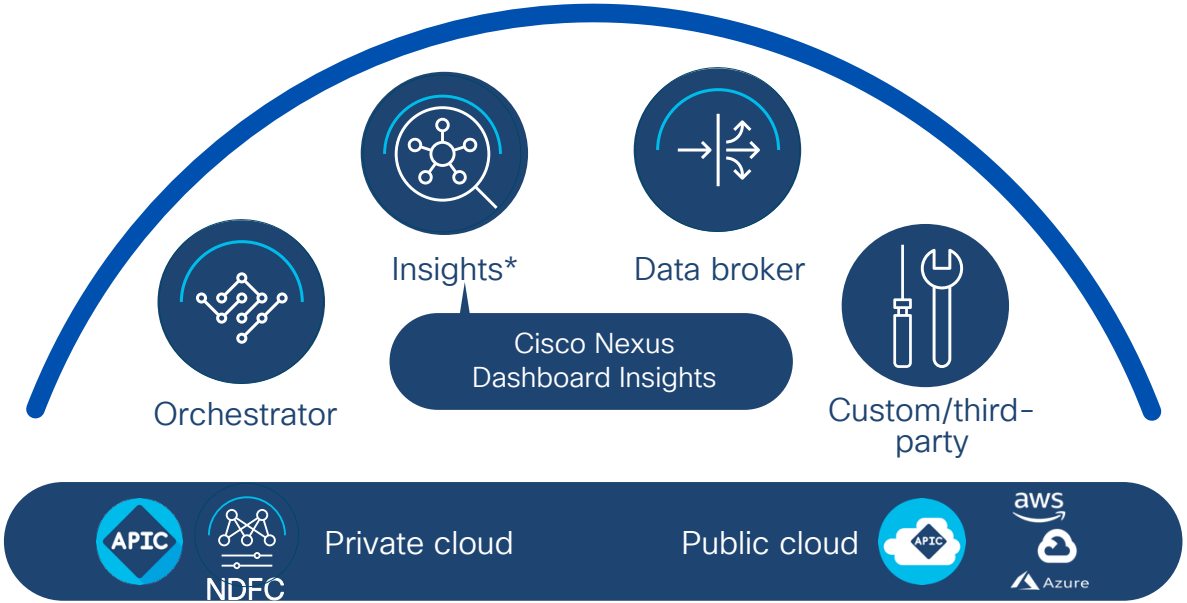
Consume all services in one place

* Includes Cisco Network Assurance Engine

Cisco Nexus Dashboard

Simple to automate, simple to consume

Powerful analytics
Proactive operation



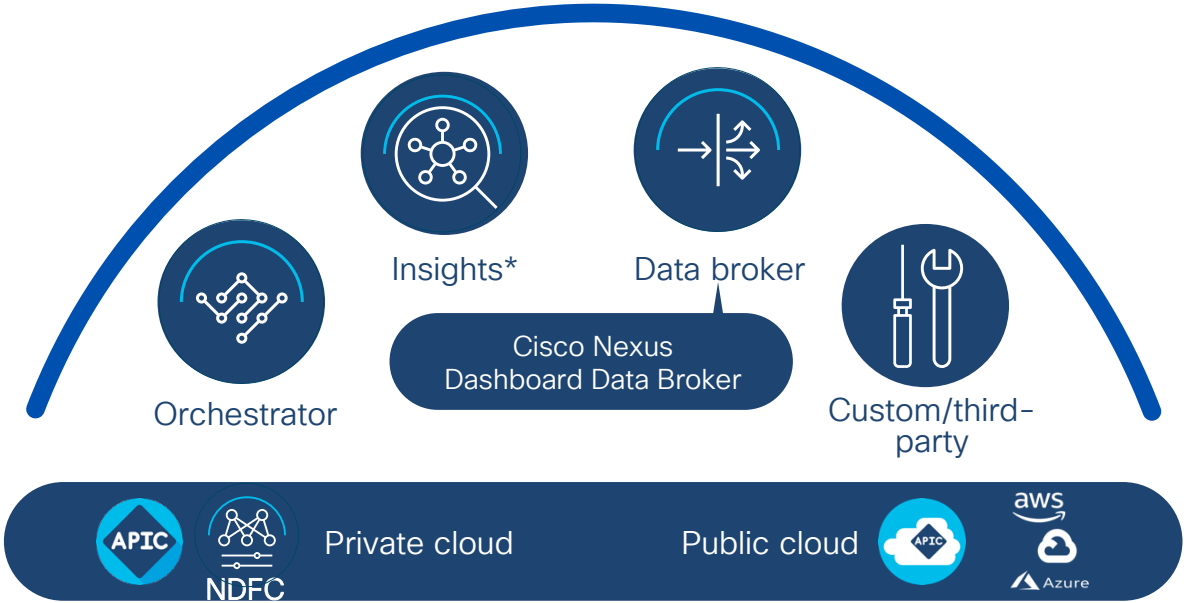
Consume all services in one place

* Includes Cisco Network Assurance Engine

Cisco Nexus Dashboard

Simple to automate, simple to consume

Packet capture
Deep packet inspection



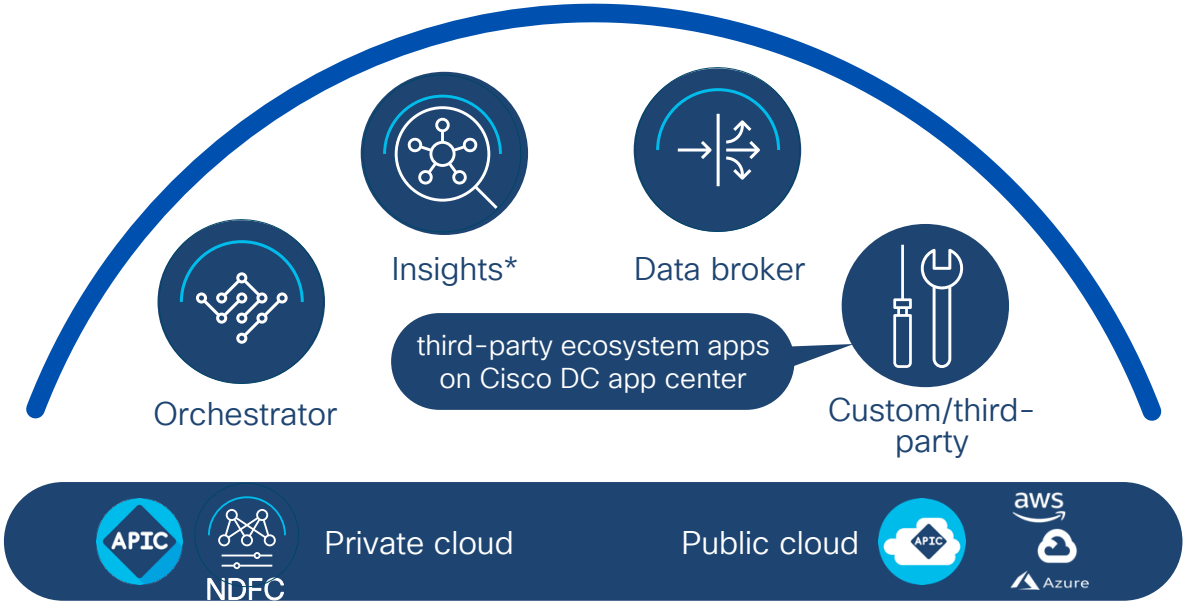
Consume all services in one place

* Includes Cisco Network Assurance Engine

Cisco Nexus Dashboard

Simple to automate, simple to consume

Infrastructure-as-code (IaC)
ITSM and SIEM integrations

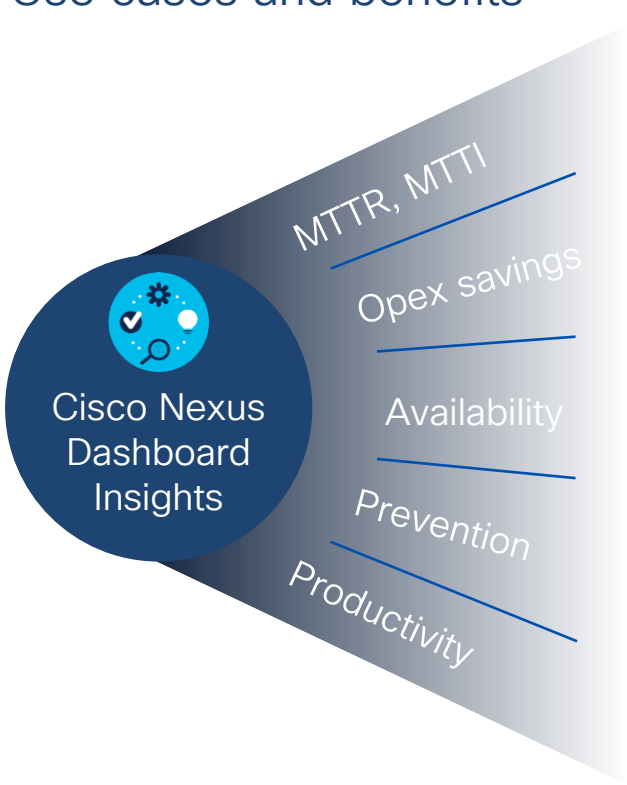


Consume all services in one place

* Includes Cisco Network Assurance Engine

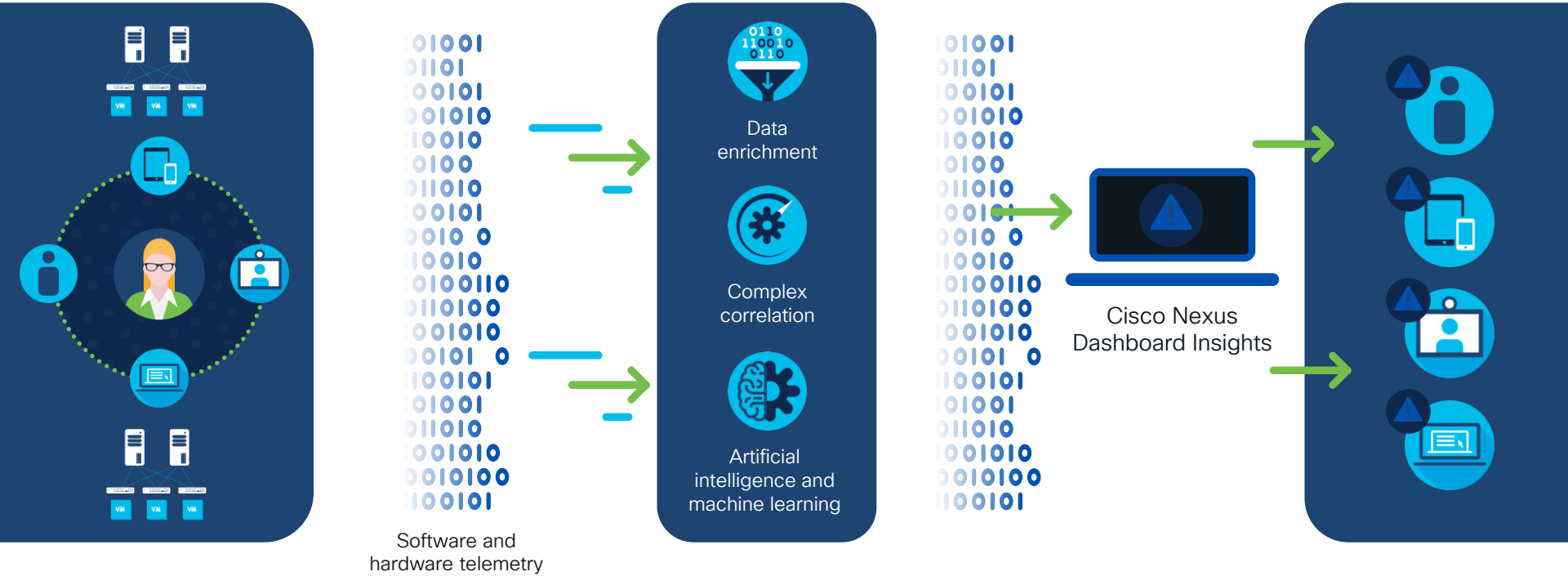
Cisco Nexus Dashboard Insights

Use cases and benefits



- 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
- Automated remediation
- TAC assist
- Topology checker

How it works



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 Dashboard Insights enabled 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.

Cisco Learning and Certifications

From technology training and team development to Cisco certifications and learning plans, let us help you empower your business and career. www.cisco.com/go/certs

Pay for Learning with Cisco Learning Credits

(CLCs) are prepaid training vouchers redeemed directly with Cisco.

Learn

Cisco U.
IT learning hub that guides teams and learners toward their goals

Cisco Digital Learning
Subscription-based product, technology, and certification training

Cisco Modeling Labs
Network simulation platform for design, testing, and troubleshooting

Cisco Learning Network
Resource community portal for certifications and learning

Train

Cisco Training Bootcamps
Intensive team & individual automation and technology training programs

Cisco Learning Partner Program
Authorized training partners supporting Cisco technology and career certifications

Cisco Instructor-led and Virtual Instructor-led training
Accelerated curriculum of product, technology, and certification courses

Certify

Cisco Certifications and Specialist Certifications
Award-winning certification program empowers students and IT Professionals to advance their technical careers

Cisco Guided Study Groups
180-day certification prep program with learning and support

Cisco Continuing Education Program
Recertification training options for Cisco certified individuals

Here at the event? Visit us at **The Learning and Certifications lounge at the World of Solutions**

Continue your education

- Visit the Cisco Showcase for related demos
- Book your one-on-one Meet the Engineer meeting
- Attend the interactive education with DevNet, Capture the Flag, and Walk-in Labs
- Visit the On-Demand Library for more sessions at www.CiscoLive.com/on-demand

Thank you


cisco Live!
ALL IN