cisco Live !

Campus Design
with Secure Networking
Reference Architecture

Cisco Secure Campus

Shawn Wargo

Principal TME

BRKENS-2614

Today's Agenda

Introduction

Why Secure Networking?

What is Secure Networking?

High-Level Design

Cisco Validated Design

Next Steps

cisco

Who am I?

I'm a Principal Engineer of Technical Marketing (Principal TME) for Cisco Enterprise '**Campus Networking**' Product Management team. I've been with Cisco since 1999.

I mainly focus on Enterprise Switching & Routing technology areas, with a special emphasis on 'next generation' Hardware & Software products and solutions.

As a Principal TME - I'm currently working on the next generation of Cisco Switching, Wireless & Routing products, and network solutions like Cisco Secure Networking & Secure Campus.

Shawn Wargo
Principal TME
swargo@cisco.com @shawn_wargo

Cisco Webex App

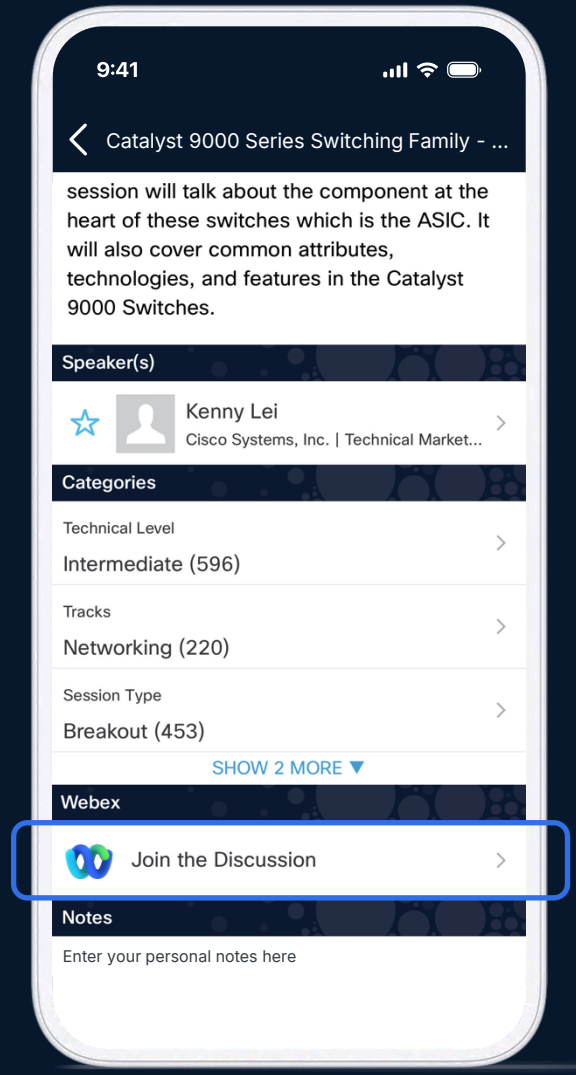
Questions?

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

How

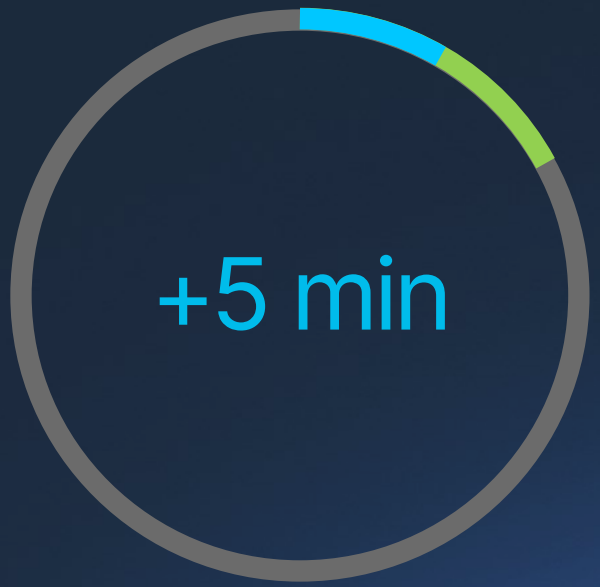
1. Find this session in the Cisco Live Mobile App
2. Click “Join the Discussion”
3. Install the Webex App or go directly to the Webex space
4. Enter messages/questions in the Webex space

Webex spaces will be moderated by the speaker until June 13, 2026.



https://ciscolive.ciscoevents.com/clamer26
/BRKENS-2614

Why Secure Networking?



Why Now?

What is the Challenge?

Why Secure Networking?

What can we do?

blogs.cisco.com/networking/the-agentic-ai-era-demands-a-new-network

thenewstack.io/how-agentic-ai-is-redefining-campus-and-branch-network-needs

Is your Campus Network AI ready?

- ⚠ for explosive traffic
- ⚠ for more complexity
- ⚠ for increased security risks

GeminiCLI
AI Agent

~31,000

pkts/sec peak

ChatGPT
Chatbot

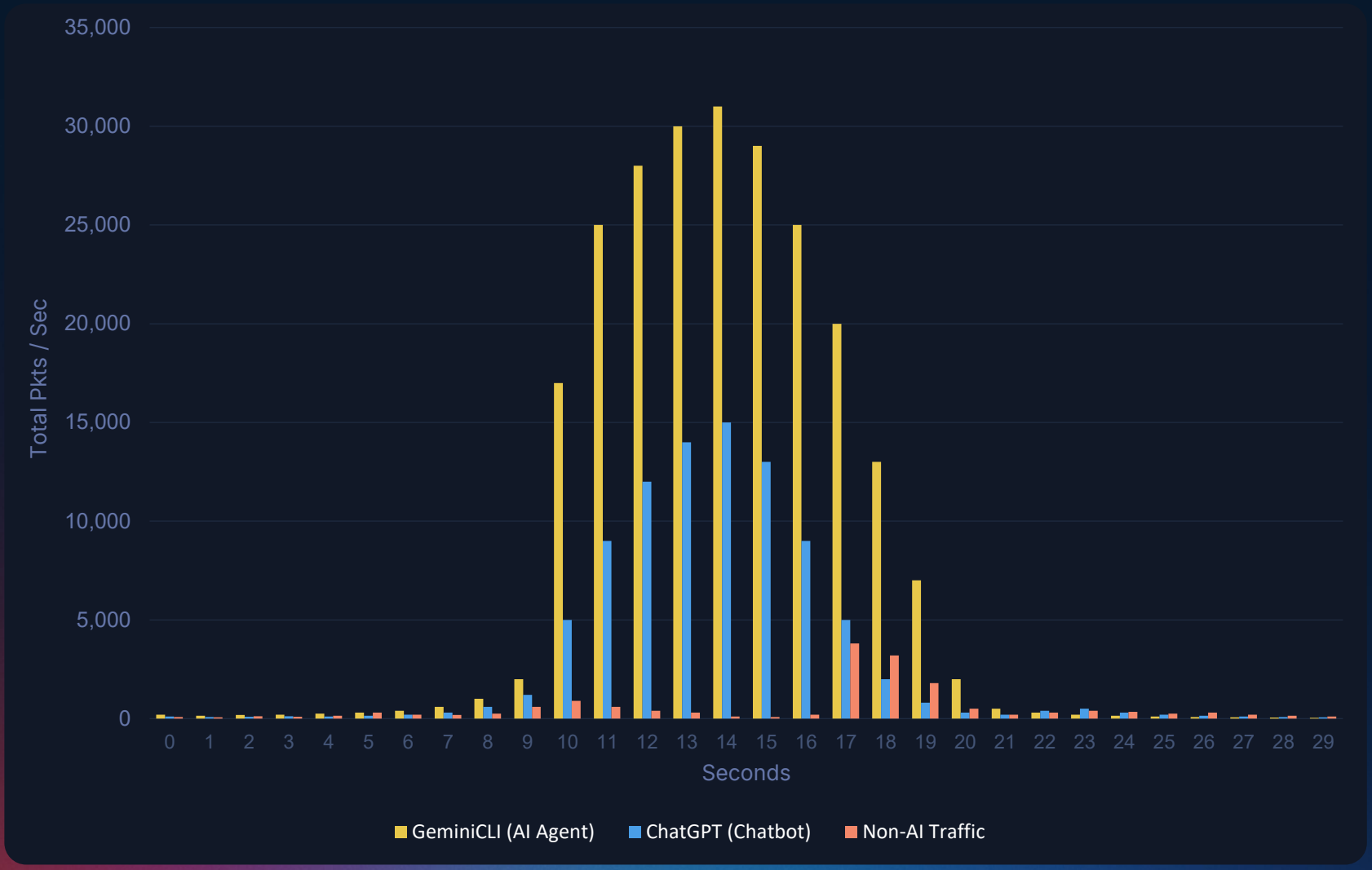
~15,000

pkts/sec peak

Non-AI
Traditional Browsing

< 1,000

pkts/sec peak



Cisco Lab Experiments with Real AI Applications

AI is Redefining Network Traffic Volume

The Enterprise Has Fundamentally Changed

Four structural shifts have dissolved the traditional security perimeter and created new attack surfaces

AI

Agentic AI

Massive east-west traffic creates new attack vectors

SaaS

Cloud-First

No single perimeter left to defend

IoT

Internet of Things

75B+ devices that cannot run security agents

GRC

Regulatory Pressure

Compliance mandates now drive architecture

These shifts have produced converging threat vectors that demand architectural change

What Enterprises Must Protect

Customer Data
PII, PHI, financial records, intellectual property

Financial System Integrity
Payment processing, trading platforms, ERP systems

Business Continuity
Applications, communications, supply chain operations

Regulatory Compliance
PCI-DSS, SEC, NIS2, NIST CSF 2.0, GDPR

These outcomes depend on the network — and the network is under attack

Workplaces today are not ready

Technology

More traffic,
more devices,
low latency needs

Security

Intensifying threats,
unmanaged devices,
wider attack surface

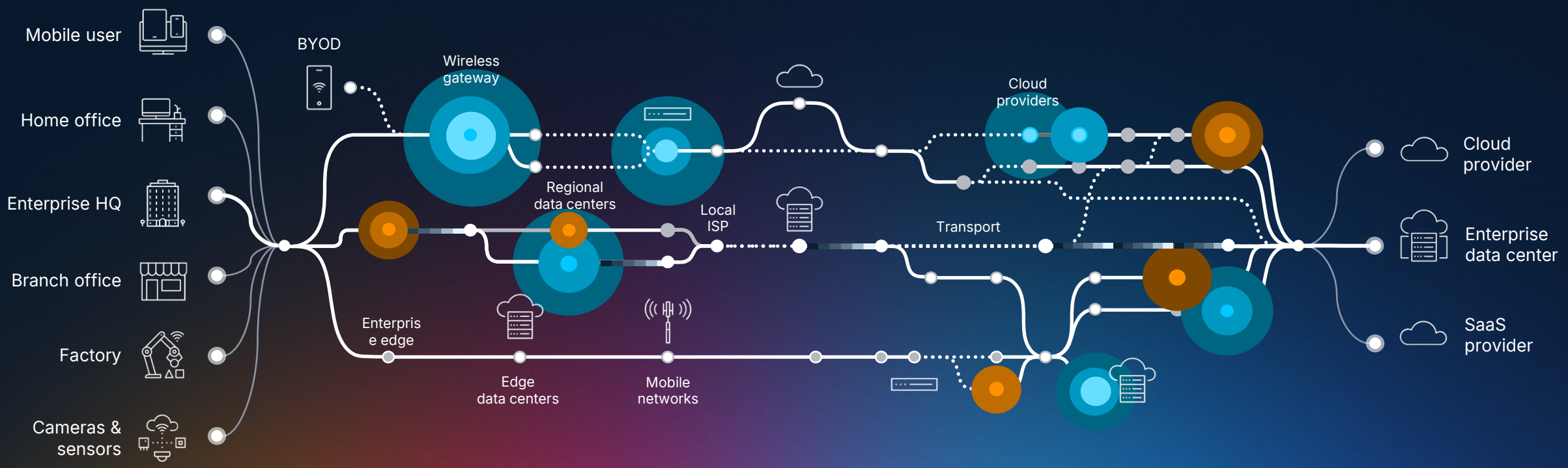
Operations

New complexities due
to AI, and a growing
skills shortage

People

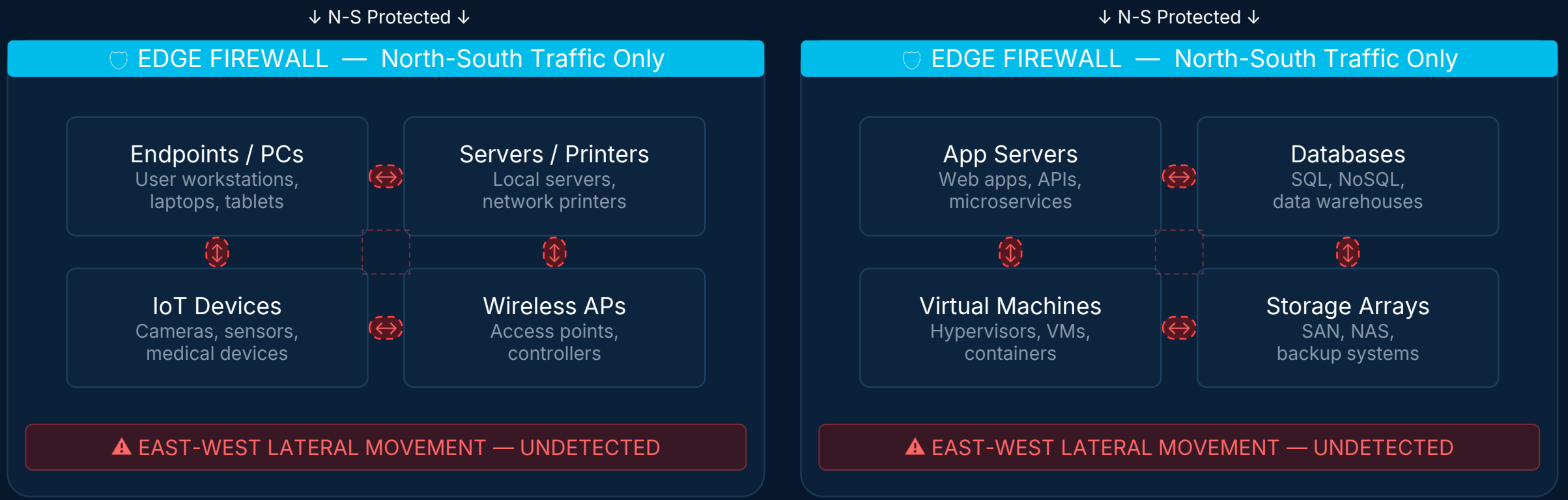
Demands for better
experiences
in every interaction

Digital experiences span owned and unowned networks



How Security Is Deployed Today

Edge firewall appliances only inspect traffic crossing the perimeter — not traffic moving laterally within your network



THE PROBLEM: Edge firewalls are blind to internal traffic

Malware and Ransomware spreads endpoint-to-endpoint on Campus and server-to-server in the DC — with no micro-segmentation, no inline encryption, no identity-based access control

What Security Should Be

Security must be fused into the network — not bolted on at the edge

1 Protect the Infrastructure

Hardware-rooted trust with secure boot and runtime integrity verification

Addresses: Salt Typhoon, BlackTech

2 Protect Data in Motion

Line-rate encryption campus to cloud with post-quantum readiness

Addresses: Harvest Now Decrypt Later

3 Prevent Lateral Movement

Identity-based segmentation and inline firewall at the switch stop ransomware and AI-driven lateral movement

Addresses: AI-Driven Lateral Movement, E-W blind spot

4 Continuous Verification

Every user and device continuously verified by identity and posture

Addresses: Implicit trust exploitation

5 Distributed & Coordinated

Policy enforced at every network point — not a single edge appliance

Addresses: Centralized bottleneck

6 Meet Every Mandate

Built-in compliance for PCI-DSS, SEC, NIS2, and NIST CSF 2.0

Addresses: Regulatory convergence

Centralized management enhanced with AI to speed up detection, diagnosis and resolution

Why the Network Is the Answer

Only the network has the position, visibility, and scale to deliver security everywhere

Sees All

Universal Visibility

Every packet traverses the network — no agent or appliance matches this reach.

Line Rate

Zero Performance Penalty

Security in silicon at wire speed. No hairpinning, no overhead.

One Fabric

Single Architecture

One policy model, coordinated enforcement at every point.

The network is the only universal control point:
Fuse security into it, and every device is protected by default.

Only Cisco unifies networking with security, observability and collaboration to power future-proofed workplaces.

Scalable Wi-Fi 7

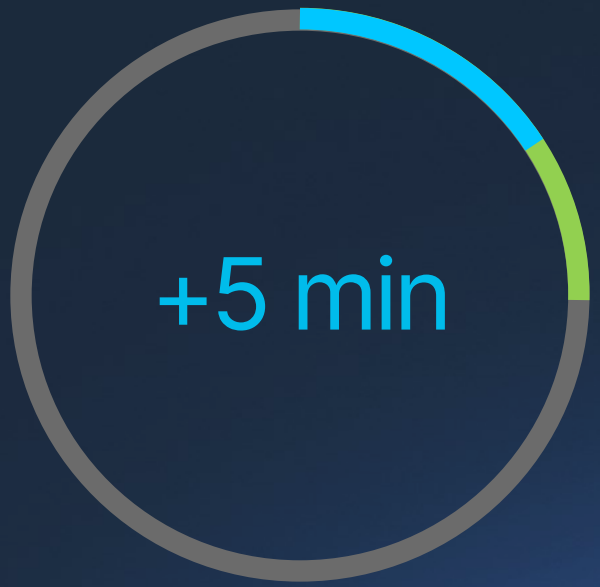
Smart Switches

Secure Routers

Secure Firewall

Rugged Networking

What is Secure Networking?



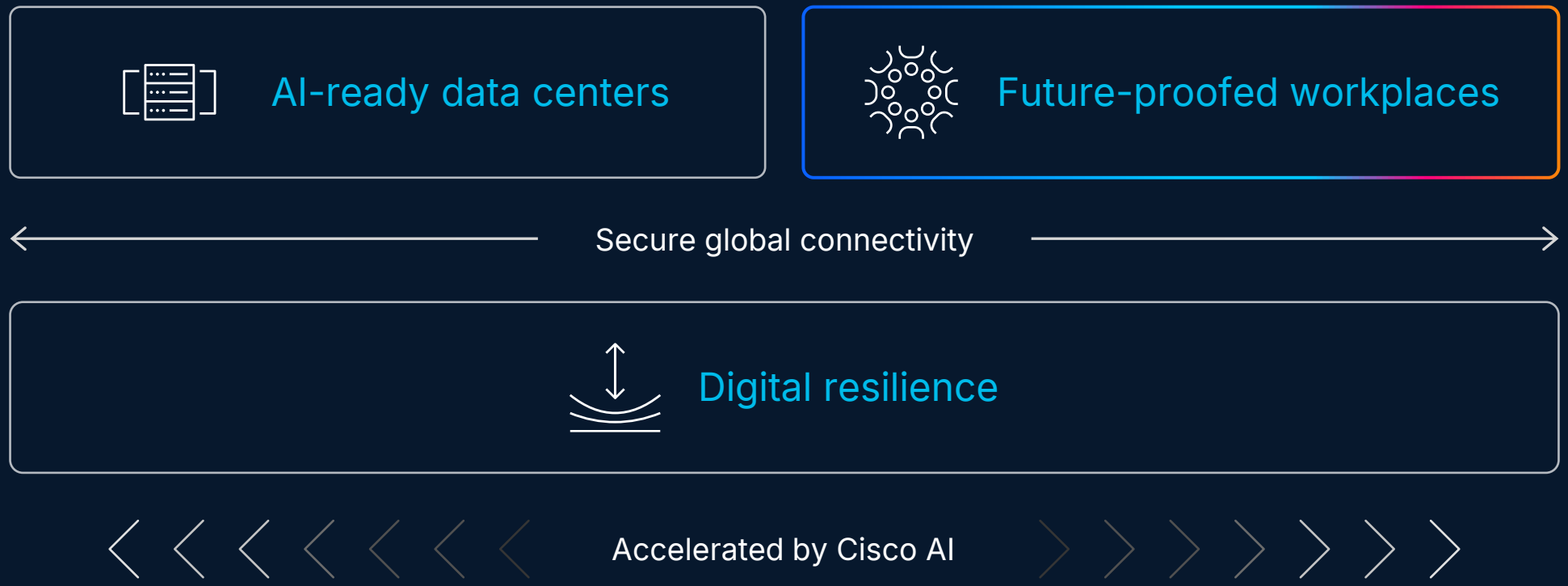
High-level Strategy & Outcomes

What is the Strategy?

What are the key elements?

How is it organized?

Cisco powers how people and technology work together



Powering your future-proofed workplaces with Cisco

Secure networking

Connect users and devices with a broad, flexible portfolio of networking solutions with embedded security, assurance and intelligence

Workforce protection

Secure humans, things, and agents everywhere work happens with frictionless zero trust access and layered security

Collaboration devices and software

Enable people to collaborate and connect effectively anywhere, delivering exceptional employee and customer experiences

Smart spaces

Transform devices on your network into sensors for better intelligence and control of physical spaces

Our products and solutions

Secure networking

- Switching
- Routing
- Wireless
- ThousandEyes
- Secure Campus
- Unified Branch
- AgenticOps
- Industrial
  - Switching
  - Routing (inc. CURWB)
  - Access
  - Security
- SD-WAN
- SASE
- SDA

Workforce protection

- Zero Trust Access
- User Protection Suite: Secure Access (SSE), Duo, Secure Endpoint, Email Threat Defense
- Firewall, ISE

Collaboration devices and software

- Room devices
- Desk devices
- Digital whiteboards
- Room accessories
- Phones
- Headsets
- Cameras
- Webex calling
- Webex Suite (Meetings, Calling, Messaging, and more)
- Webex Contact Center
- Webex Connect

Smart spaces

- Cisco Spaces
- Sensors and cameras
- Switching/ Power over Ethernet (PoE)
- Technology partner ecosystem

Cisco fuses security into every layer of your network

Workplaces

Secure Networking

Data Centers

- ✓ Simplify operations and reduce overhead costs
- ✓ Ensure consistent and secure access everywhere
- ✓ Remain in compliance while reducing operational risk
- ✓ Business continuity without compromise
- ✓ Adopt and secure Agentic AI with confidence

Introducing ‘Secure Networking’

What is Secure Networking?

“Secure networking is a modern network infrastructure design that fuses advanced security and deep visibility into every layer of the network – to protect confidentiality, integrity, and availability of data resources – and ensure digital resilience across future-proofed workplaces and AI-ready data centers.”

In an increasingly AI-driven world: an architecture built on Cisco Secure Networking principles is the most effective safeguard against unauthorized access, misuse & attacks.

Cisco Differentiation

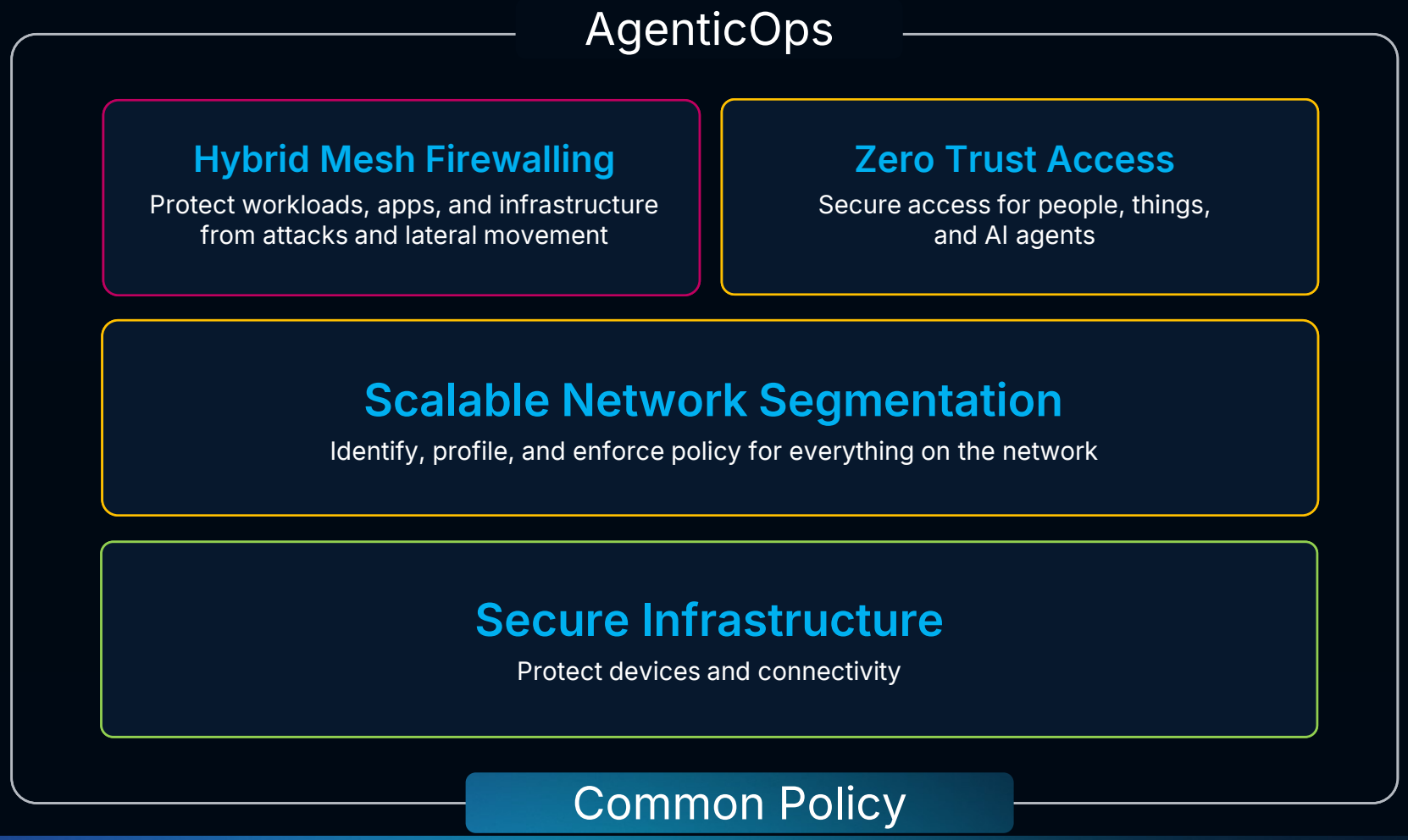
The Secure Networking architecture is:

- Identity and Threat-aware
- United by Common Policy
- Hyper Distributed
- Deeply Embedded

Introducing Cisco's Secure Networking

Security infused into the network

- Identity-first
- Continuously verified
- Enterprise-wide policies
- Comprehensive threat intel
- Distributed enforcement
- Streamlined Operations



Security and networking unified as one

Continuously verified, comprehensive threat intelligence

Secure Networking

One operational team | One unified solution | One set of controls

- ✓ Identify, profile, and enforce policy for everything on the network
- ✓ Protect devices and connectivity
- ✓ Secure access for people, things, and AI agents
- ✓ Protect workloads, apps, and infrastructure from attacks and lateral movement

Common policies, identity-first, with distributed enforcement

Architecture for the AI-Ready Secure Network

AgenticOps
for operational simplicity

Security
fused into the network

Scalable Devices
ready for AI networks

What technologies make up the Secure Campus?

Catalyst Center | Meraki Dashboard

Wi-Fi

Wi-Fi 7
Wireless Controllers
Campus Gateway

Switching

Cisco Smart Switches
Cisco Catalyst
Cisco Meraki

Routing

Cisco Secure Routers
Cisco Catalyst 8000

Assurance

Wireless, Wired and
Wide-Area Networks
Cisco ThousandEyes

Identity Services Engine (ISE), Scalable Group Tags (SGT) and Hybrid Mesh Firewall (HMF)

Secure Networking for Campus & Branch

Customer outcomes

Simplify operations & reduce overhead cost

IT talent is scarce, and manual processes are the leading cause of vulnerabilities.

Ensure consistent & secure access everywhere

Access is no longer confined to an office.

Remote workers, IoT devices and OT environments require the same level of protection.

Reduce risk while maintaining compliance

Regulatory pressure and the threat of data exfiltration are at an all-time high.

Adaptive business continuity, without compromise

Downtime is not just an IT issue; it's a revenue issue.

Resiliency and adaptability are requirements at all layers: NetOps and SecOps.

Adopt & secure Agentic AI, with confidence

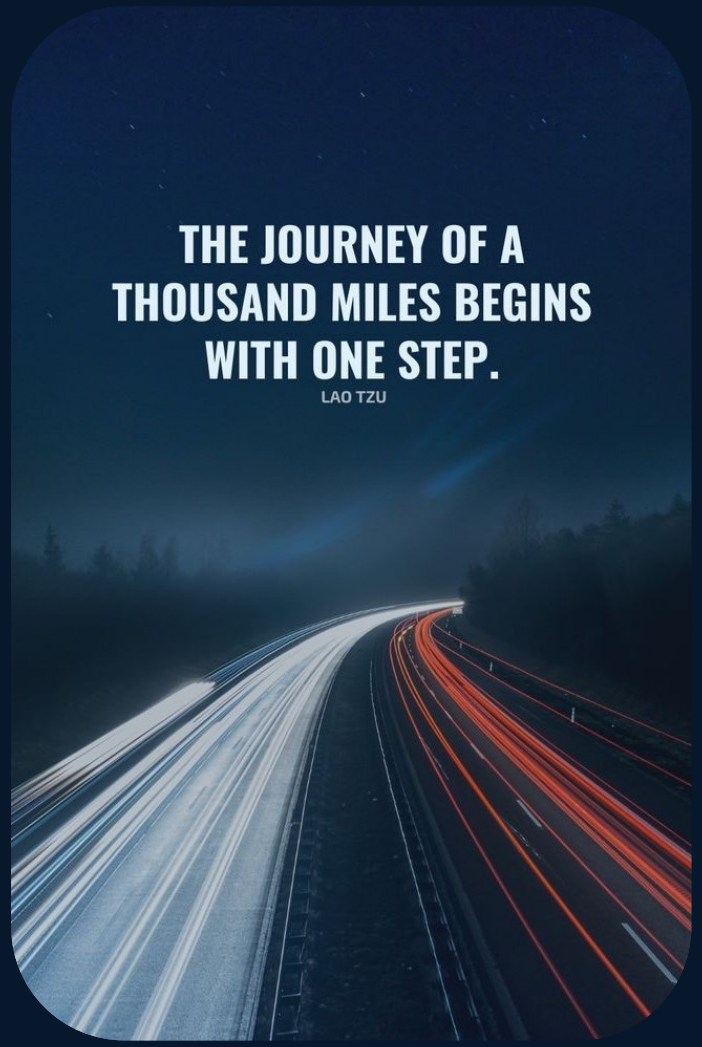
AI agents are moving from analysis to autonomous action - creating unpredictable traffic spikes and new security risks.

Secure Networking is just a Reference Model to design Security at every layer... backed by Cisco Validated Design testing.

Shawn Wargo
Principal TME, Cisco

Secure Networking v1.0

FYI



This is our first cross-domain and end-to-end Cisco reference architecture in the modern era!

- Version 1.0 delivers 'Secure Networking' outcomes
  - Many Domains, PINs, Products & Protocols
  - Based on the currently available Products
  - There are some challenges, limits and gaps
- We will continue to evolve in the future* (v2.0+)

SNRA v1.0 Versions:

- IOSXE 26.1.(latest)
- Meraki Q2CY26 (latest)
- Catalyst Center 3.2.1.(latest)
- SDWAN Manager 20.18.2.(latest)
- ISE 3.5.(latest)
- TE Q2CY26 (latest)
- SNA 7.6.(latest)
- FMC 10.0.(latest)
- SCC Q2CY26 (latest)

CISCO VALIDATED DESIGN

* Feature Roadmap aligned to SNRA

High-Level Design

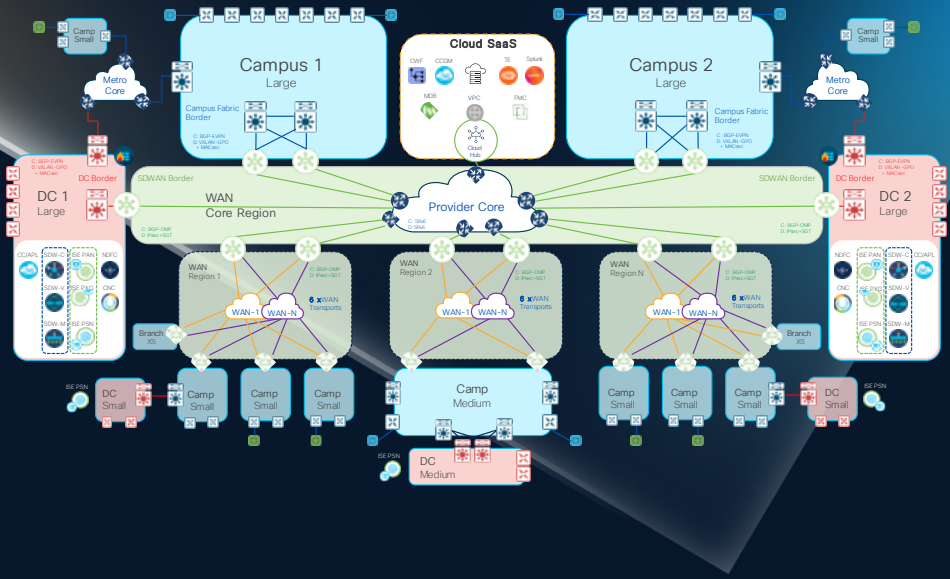
Design Approach & Key Considerations

What should we focus on?

What is the design approach?

How do use the design?

The Challenge of building an End-to-End ‘Reference Architecture’

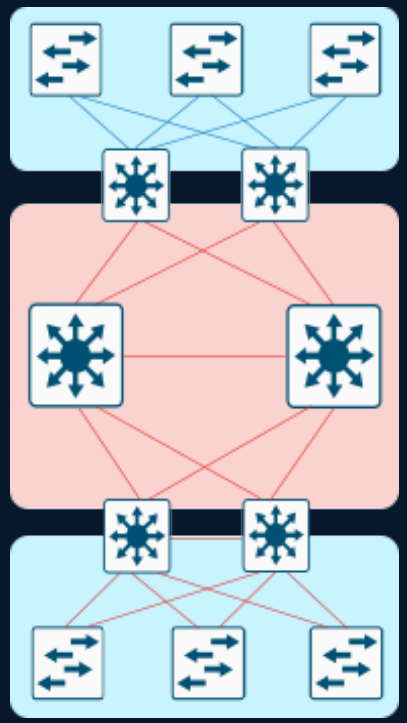


Why do we divide into Layers & Domains?

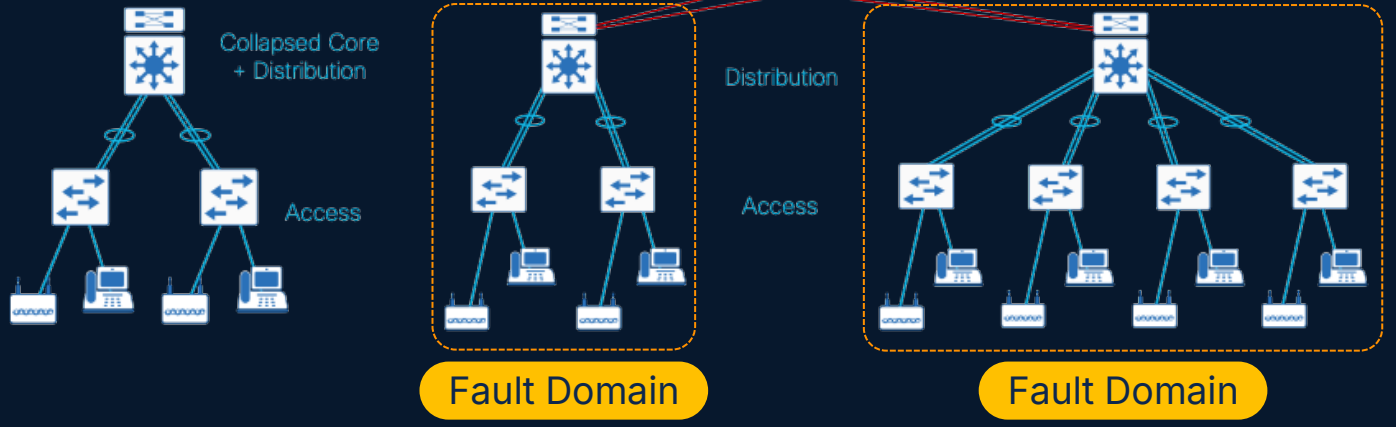
Why can't we just collapse the Layers & Domains?

The eternal battle between: "reducing complexity & costs" and "maximizing stability & reliability"

Separate Roles

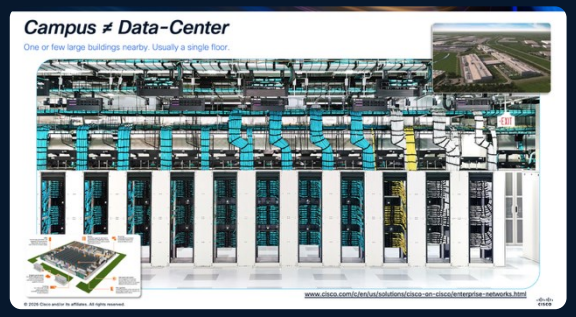


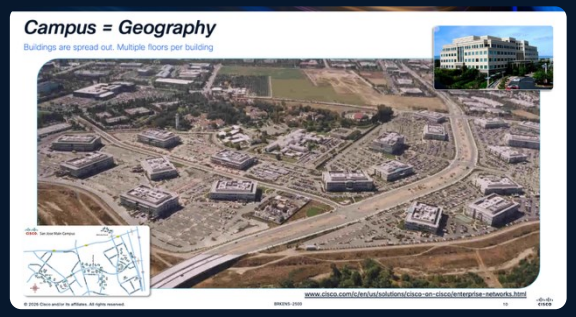
SCALE



Different Features

Different Ops Teams

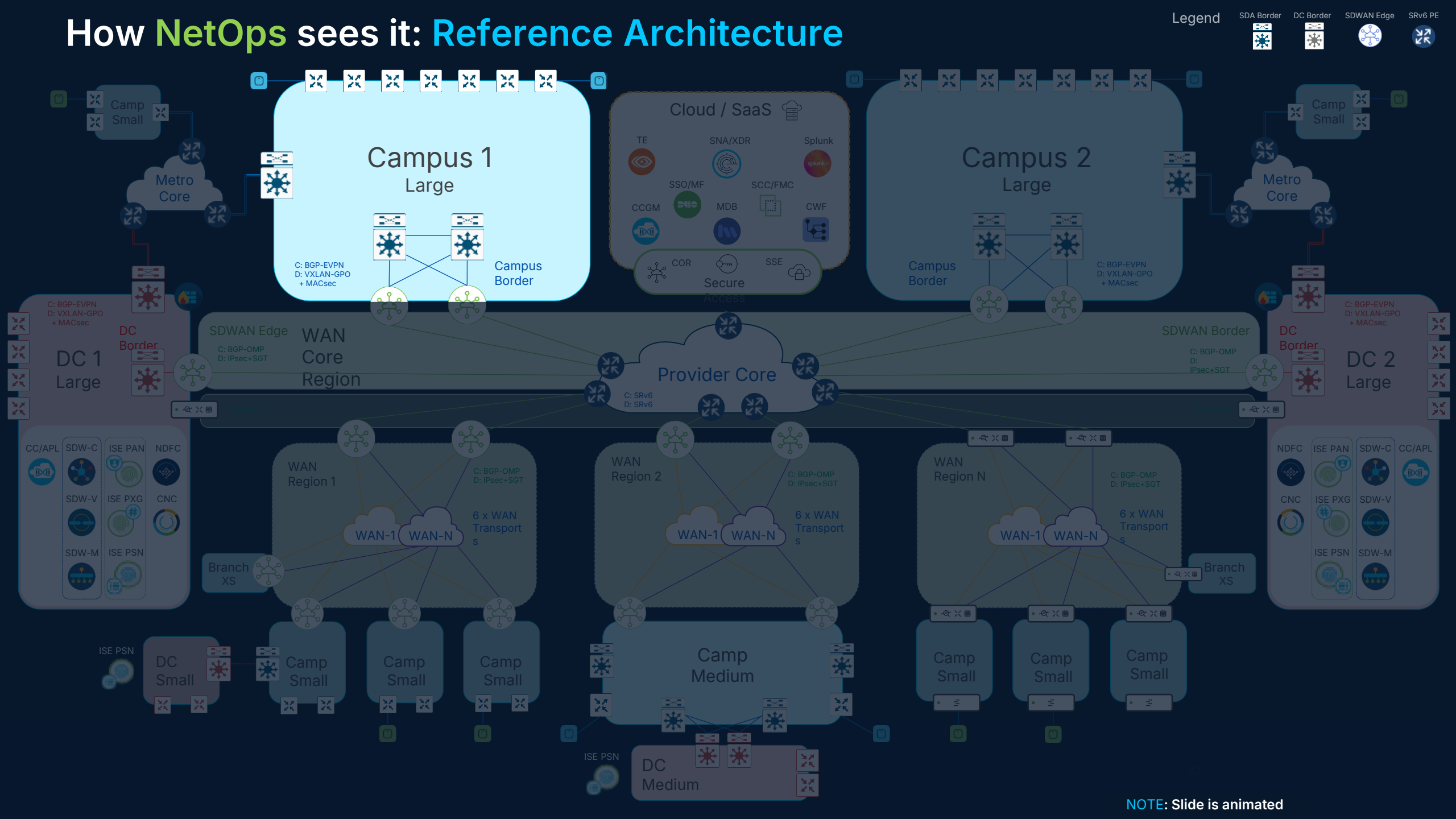




Different Environments

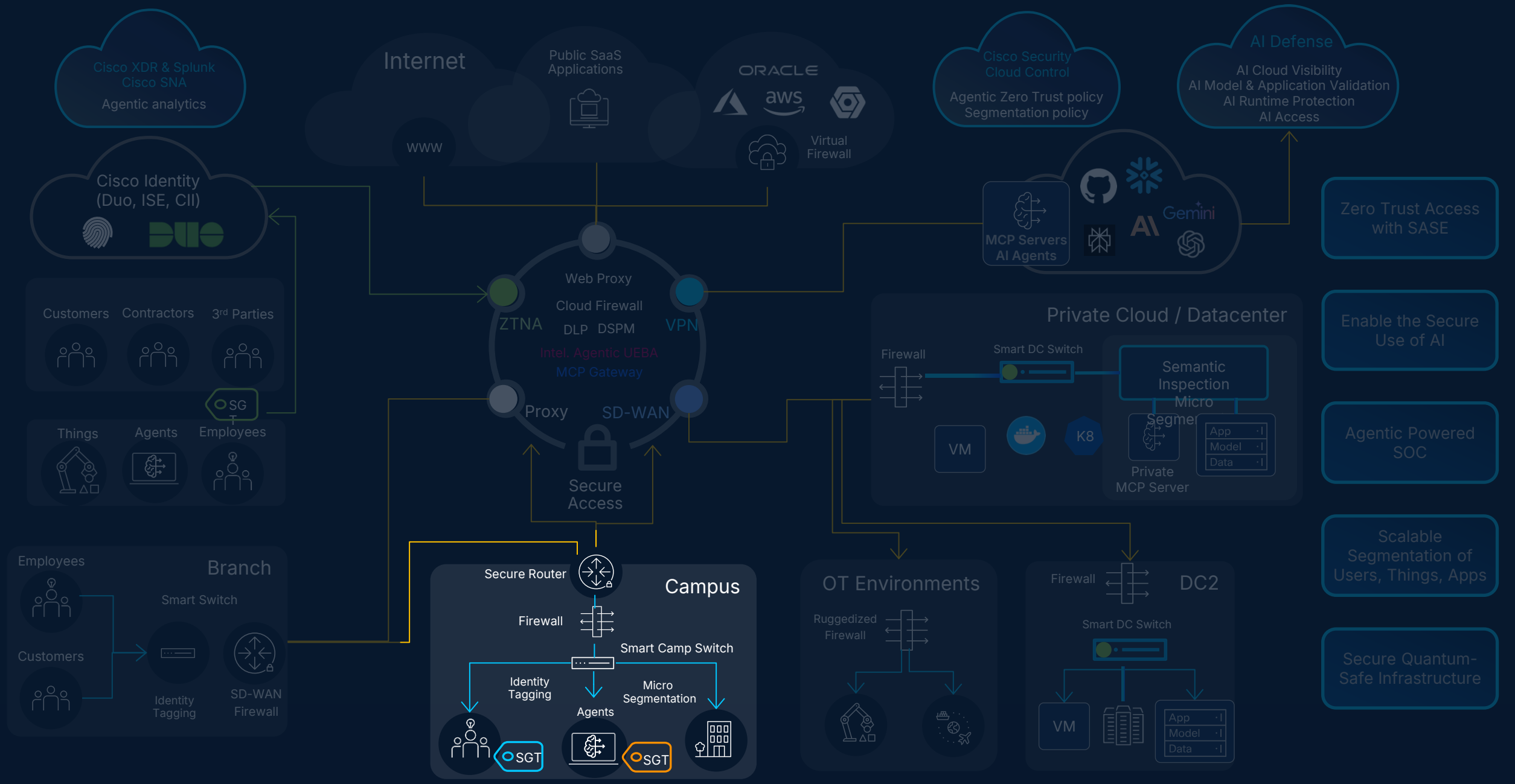
cisco

How NetOps sees it: Reference Architecture

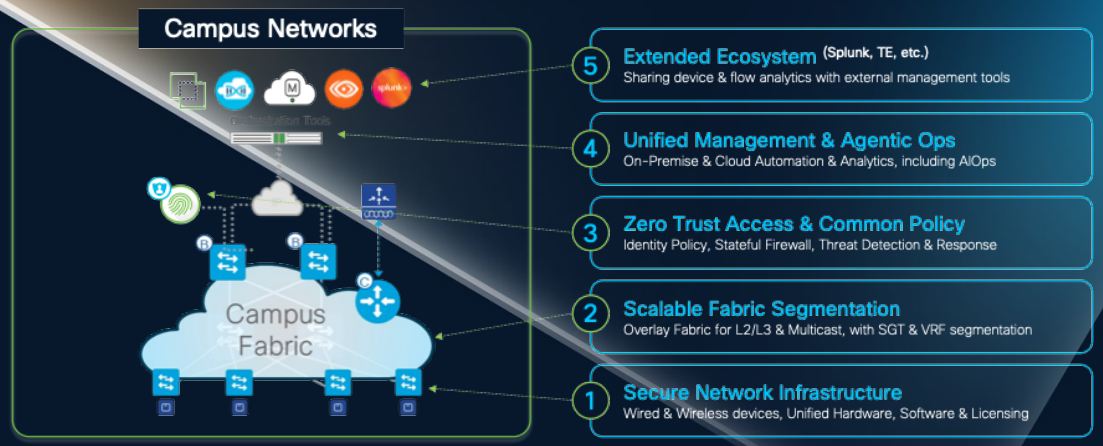


NOTE: Slide is animated

How SecOps sees it: Reference Architecture

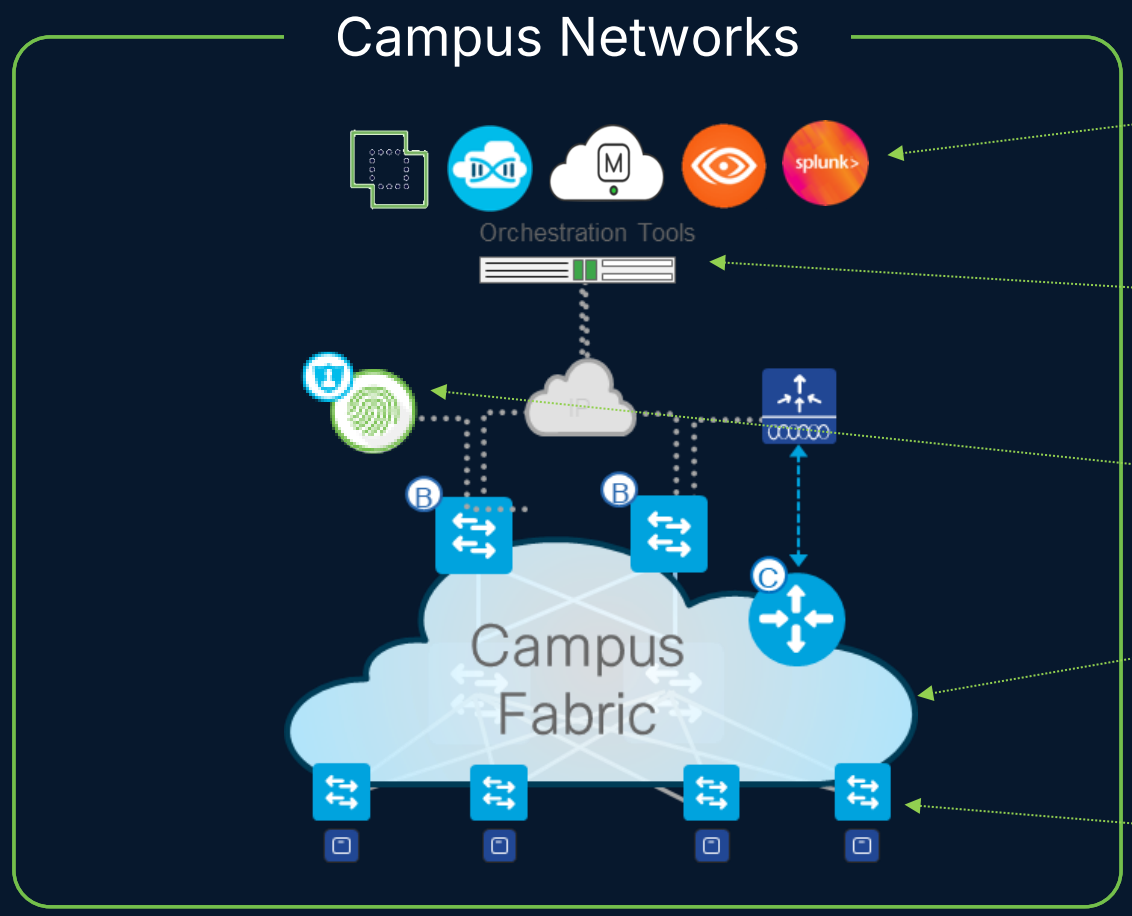


Introducing the SNRA Multi-Layer Reference Model



Secure Networks – Solution Layers

Full-Stack Multi-Layer Reference Model (like the OSI Model)



5 Extended Integrations (Splunk, ThousandEyes, etc.)
Sharing device & flow analytics with external management tools

4 Unified Management & Agentic Ops — ENTRY 1
On-Premise & Cloud Automation & Analytics, including AIOps

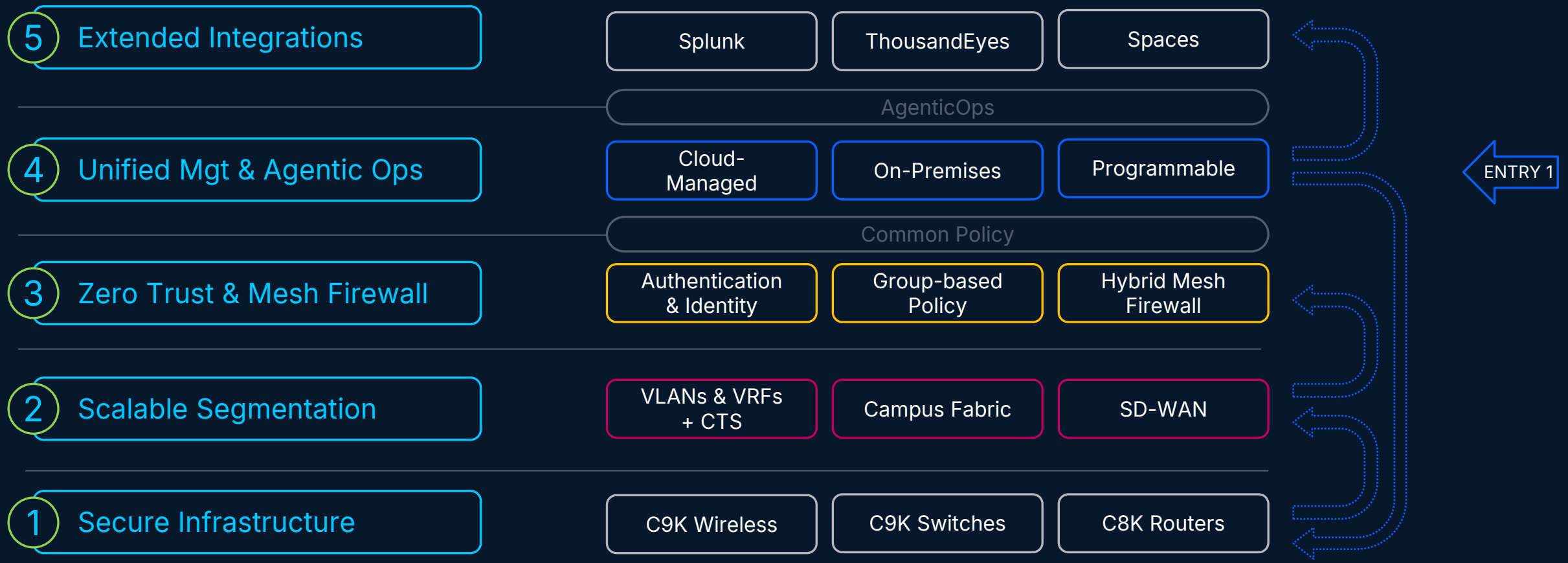
3 Zero Trust Access & Hybrid Mesh Firewall — ENTRY 2
Identity-based, Common Policy, Threat Detection & Response

2 Scalable Network Segmentation — ENTRY 3
Network for L2/L3 & Multicast, with SGT & VRF segmentation

1 Secure Infrastructure
Wired & Wireless devices, Unified Hardware, Software & Licensing

Secure Networks – Solution Layers

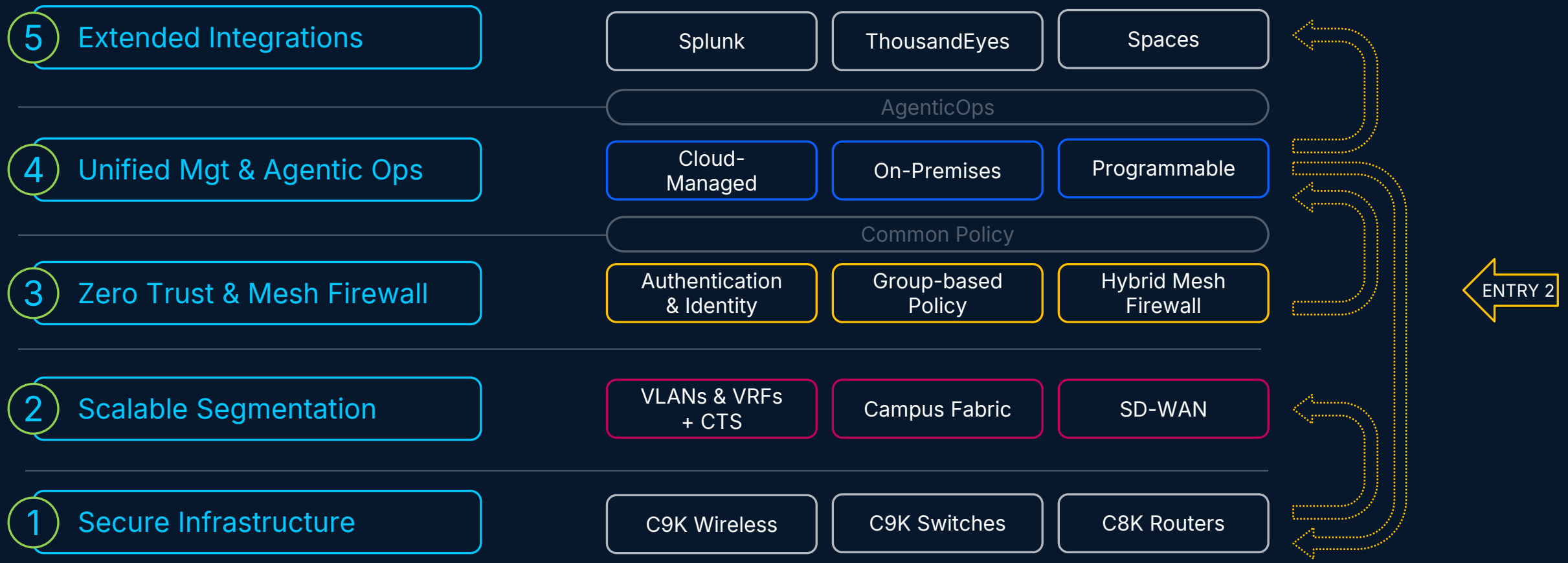
Each Layer can be designed independently (then connect to other layers)



4 ⇨ 1 ⇨ 2 ⇨ 3 ⇨ 5

Secure Networks – Solution Layers

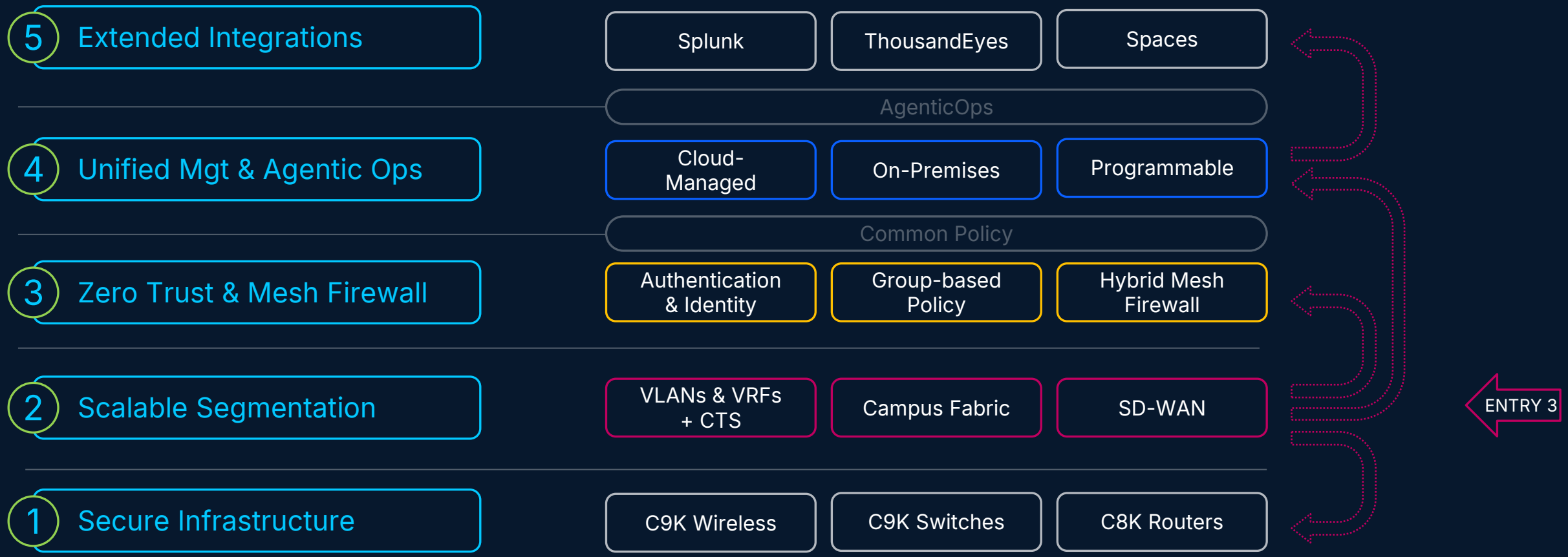
Each Layer can be designed independently (then connect to other layers)



3 ⇨ 4 ⇨ 1 ⇨ 2 ⇨ 5

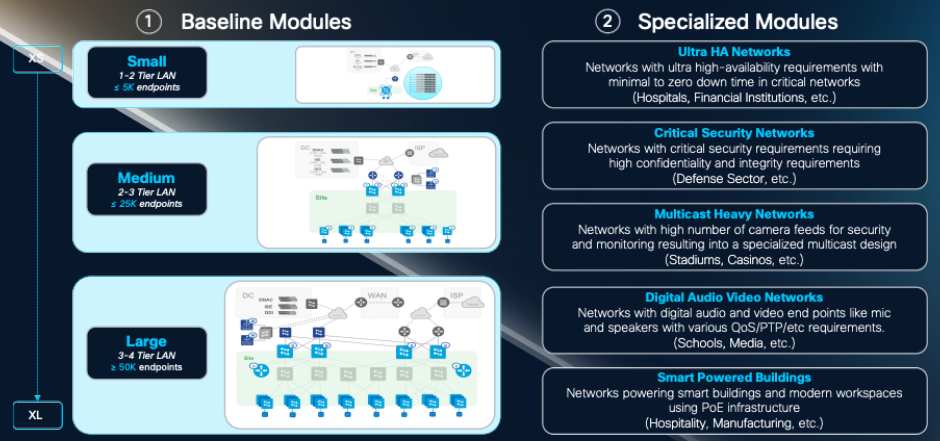
Secure Networks – Solution Layers

Each Layer can be designed independently (then connect to other layers)



2 → 3 → 4 → 1 → 5

Introducing the SNRA Modular ‘T-shirt Sizing’



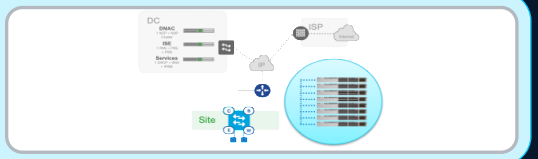
Secure Networks – Modular T-shirt Sizing

XS

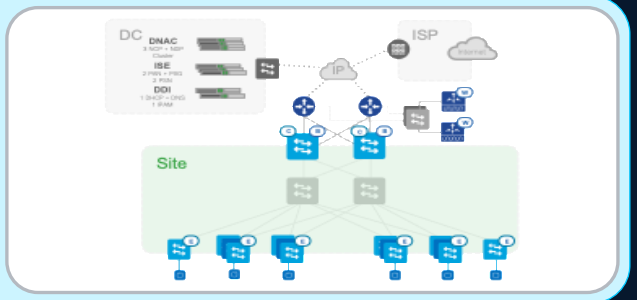
XL

1 Baseline Modules

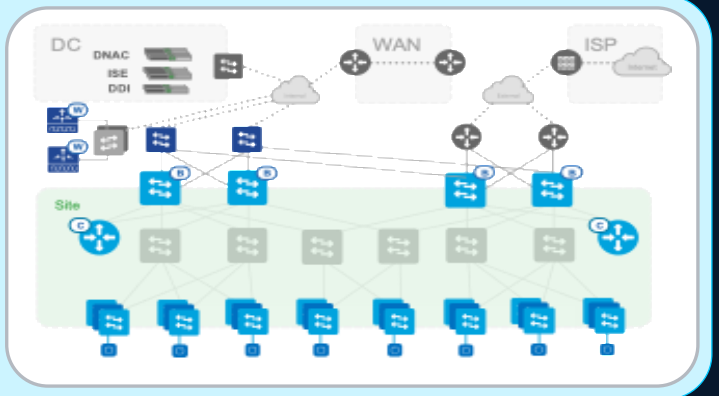
Small
1-2 Tier LAN
≤ 5K endpoints



Medium
2-3 Tier LAN
≤ 25K endpoints



Large
3-4 Tier LAN
≥ 50K endpoints



2 Specialized Modules

Ultra Reliable
Networks with ultra high-availability requirements, with minimal-to-zero down time in critical areas.
examples: Hospitals, Financial Institutions, etc.

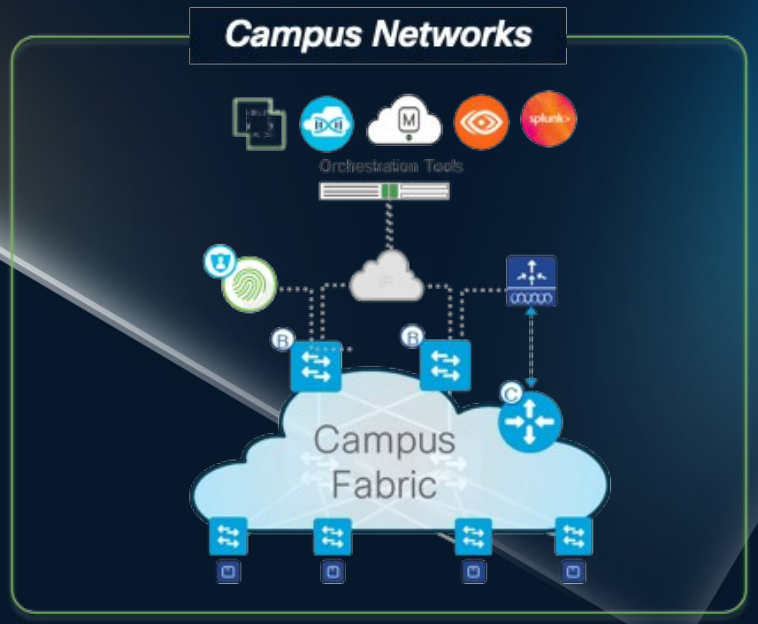
Critical Security
Networks with critical security requirements for maximum data confidentiality and integrity.
examples: Government, Defense, etc.

Multicast Heavy
Networks with high number of digital signage or streaming videos, requiring efficient data replication.
examples: Stadiums, Casinos, etc.

Digital Audio & Video
Networks with digital audio & video end points like cameras and speakers with various QoS & PTP requirements.
examples: Schools, Broadcasters, etc.

Smart Powered
Networks powering smart buildings and hybrid workspaces using network PoE & HVDC infrastructure.
examples: Manufacturing, Food & Lodging, etc.

Implementing the SNRA Reference Model for Secure Campus



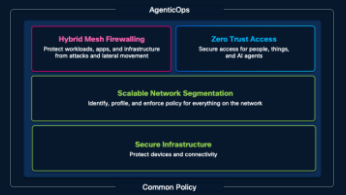
Secure Infrastructure

1 **Secure Infrastructure**
Wired & Wireless devices, Unified Hardware, Software & Licensing

www.cisco.com/site/us/en/products/networking/switches/index.html

blogs.cisco.com/networking/the-new-family-of-cisco-smart-switches-built-to-power-whats-next

Reference design for Secure Network Infra



2 **Scalable Network Segmentation**
Identify, profile, and enforce policy for everything on the network

1 **Secure Infrastructure**
Protect devices and connectivity

Secure Wireless: Cisco C9K APs & WLC/MCG
- Access Point
- Wireless Control

Secure Switching: Cisco C9K Series Switches
- Access & IOT
- Core & Distribution

Secure Routing: Cisco Secure Routers
- Branch and Campus
- Data Center

Secure Firewall: Cisco NG Firewalls
- Distributed Virtual
- Central Appliance

Cisco Enterprise Switching Portfolio

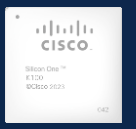
A switch model for every use case

Cisco C9350 Smart Switch

The next generation of fixed Access switches

1.6 Tbps stacking, 48 ports 90W PoE, Copper and Fiber 1/2/5/10G downlinks and 100/40G or 50/25/10/1G uplinks, and 2+1 Power & Stack Power, with Cisco Smart Stacking

Cisco C9610 Smart Switch



The next generation of modular Core switches

25.6 Tbps capacity 8-slot chassis for high-density mGig Copper, 10/25/50G SFP and 100/400G QSFP Fiber, and 7+1 Power, with Cisco Smart Stacking

Access Switching | **Core Switching**

Cisco IOS XE

C9200CX | C9200/L | C9300L/X/M | C9400/X | C9500/X | C9600/X

Compact | Entry Access | Critical Access | Modular Access | Fixed Core | Modular Core

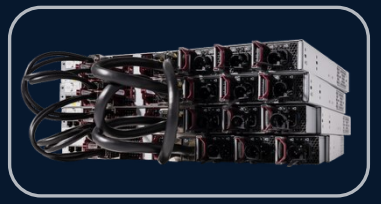
Cisco C9K Series Smart Switches

Key Concepts & Considerations (Why it matters)

1 Connectivity & Speed

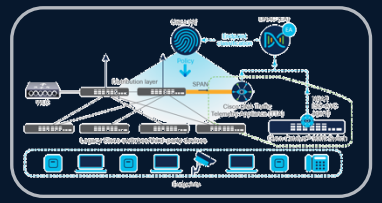
- Enables 2.5G-10G mGig to Access & WIFI APs
  - with existing Cat5E/6A copper
- Enables 25/50G SFP from Access to Distro
  - with existing OM3/4 LC fiber
- Enables 100/400G QSFP from Distro to Core
  - with existing OM3/4 MTP fiber

2 Power over Ethernet



- Enables 60W to WIFI6e & WIFI7 Access Points
  - C9170 uses 47W + mGig + mLAG
- Support 48 x 90W on ALL downlinks (≤ 384 total)
  - N+1 power supplies and StackPower
- Continuous power with Perpetual & Fast PoE
  - Smart Buildings with Smart Power

3 App Visibility & Control

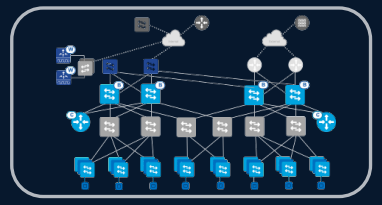


- Flow telemetry with Flexible NetFlow & NBAR
  - enables App-based QoS
- Endpoint Analytics with Device Sensor & SISF
  - enables Security Analytics
- Combined with real-time Streaming Telemetry

4 Infrastructure Security

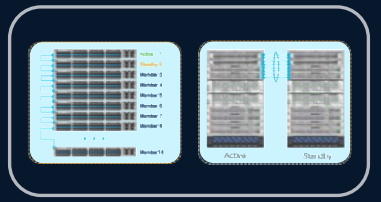
- Hardware & Software PQC Trustworthy Solutions
  - PQC TAM, Image Signing & Secure Boot
- Software Control-Plane Security for Access & Core
  - Live Protect, Runtime Defense & Resilient Infra
- Hardware PQC MACsec & PQC IPsec encryption

5 Standalone HA



- Conventional Network-based convergence
  - based on protocol (timers)
- Conventional per-Device device upgrades
  - each upgraded separately
- Sub-second Modular ISSU & Fixed XFSU

6 Stacking & SVL HA



- Simplified Single Management for up to 8 devices
  - Access Stacking & Core SVL
- Sub-second Multichassis EtherChannel convergence
  - supports L2 and/or L3 mLAG
- Sub-second SVL ISSU and Stack XFSU upgrades

Secure Platform with Trustworthy Technologies

Hardware-anchored Integrity: Establishing a foundation of trust through cryptographically verified boot processes

Every Cisco device proves its integrity before it joins the network

Secure Boot
Hardware root of trust validates firmware before execution

Hardened Linux OS
Reduced attack surface with locked-down IOS XE kernel

CISCO TRUSTWORTHY SYSTEMS

Image Signing
Cryptographic verification prevents tampered firmware

Runtime Integrity
Continuous verification detects in-memory tampering

Anti-Counterfeit

TAm chip + Secure Unique Device ID authenticates every device as genuine Cisco

Trustworthy Supply Chain

End-to-end integrity from manufacturing to deployment prevents interdiction

Cisco Trust Anchor

Hardware root of trust embedded in silicon — cannot be modified by software

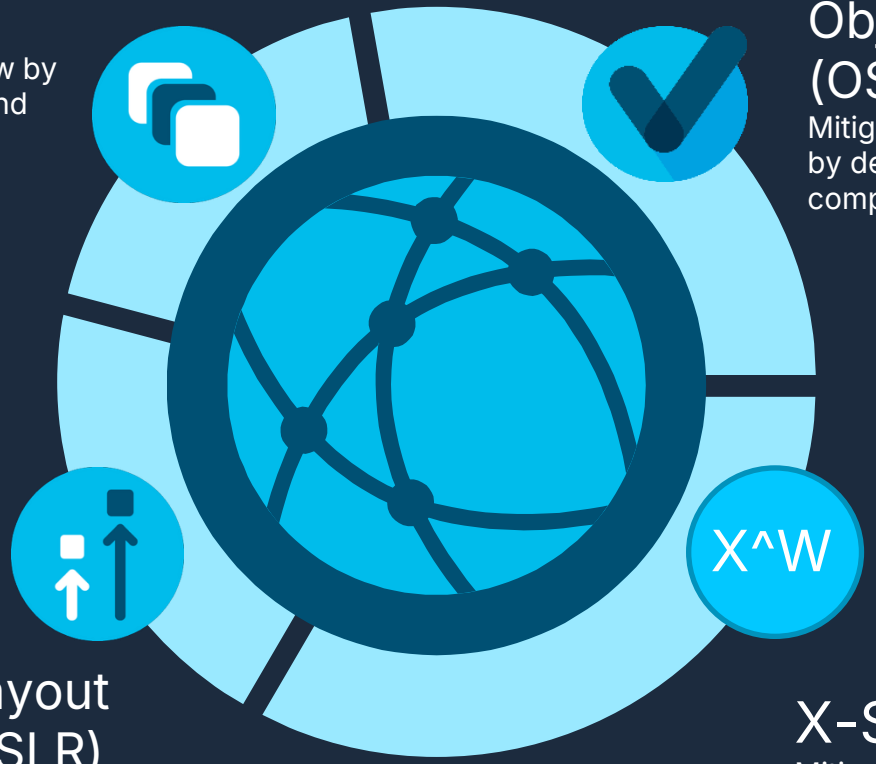
www.cisco.com/c/en/us/about/trust-center/technology-built-in-security.html

Run Time Defenses (RTD)

Active Process Protection: Safeguarding system memory and execution flows against runtime threats

Safe C Libraries

Protects against buffer overflow by bounds-checking of memory and all Copy functions



Object Size Checking (OSC)

Mitigate buffer overflow attacks by detecting many overflows at compile and runtime

Address Space Layout Randomization (ASLR)

Mitigates code injection attacks by randomizing the locations in memory where different code or data is loaded

X-Space

Mitigates code injection attacks by disallowing/excluding execution from data area in memory

- ✗ Attacker wants to exploit the Operating System when software is running
- ☑ Build software so that the possibility for exploitation is reduced
- ☑ Use Compiler, Kernel and Hardware capabilities to provide protections

www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/trustworthy-technologies-datasheet.pdf

Resilient Infrastructure

For more information, please visit: www.cisco.com/go/ir

Secure by Default: comprehensive improvements to our software security posture

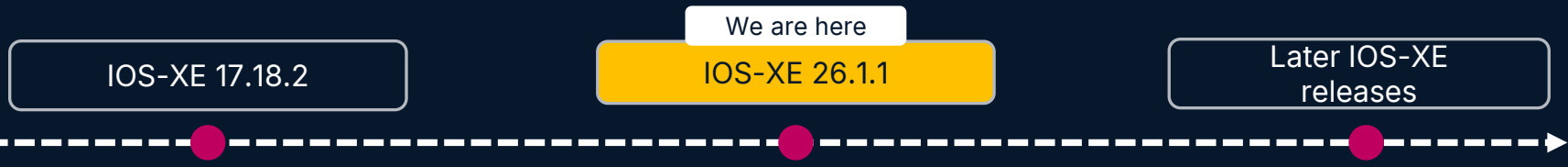
What is the issue?

Global threat actors have changed the game by exploiting known protocol vulnerabilities

What can we do?

Harden our devices by avoiding configuration of known insecure commands

How are we doing this?



Encourage gradual migration from known insecure commands to secure alternatives

Examples of insecure cli*

```
line vty 0-15
  transport input telnet
```

```
copy ftp: switch:
copy tftp: switch:
```

```
ip http server
```

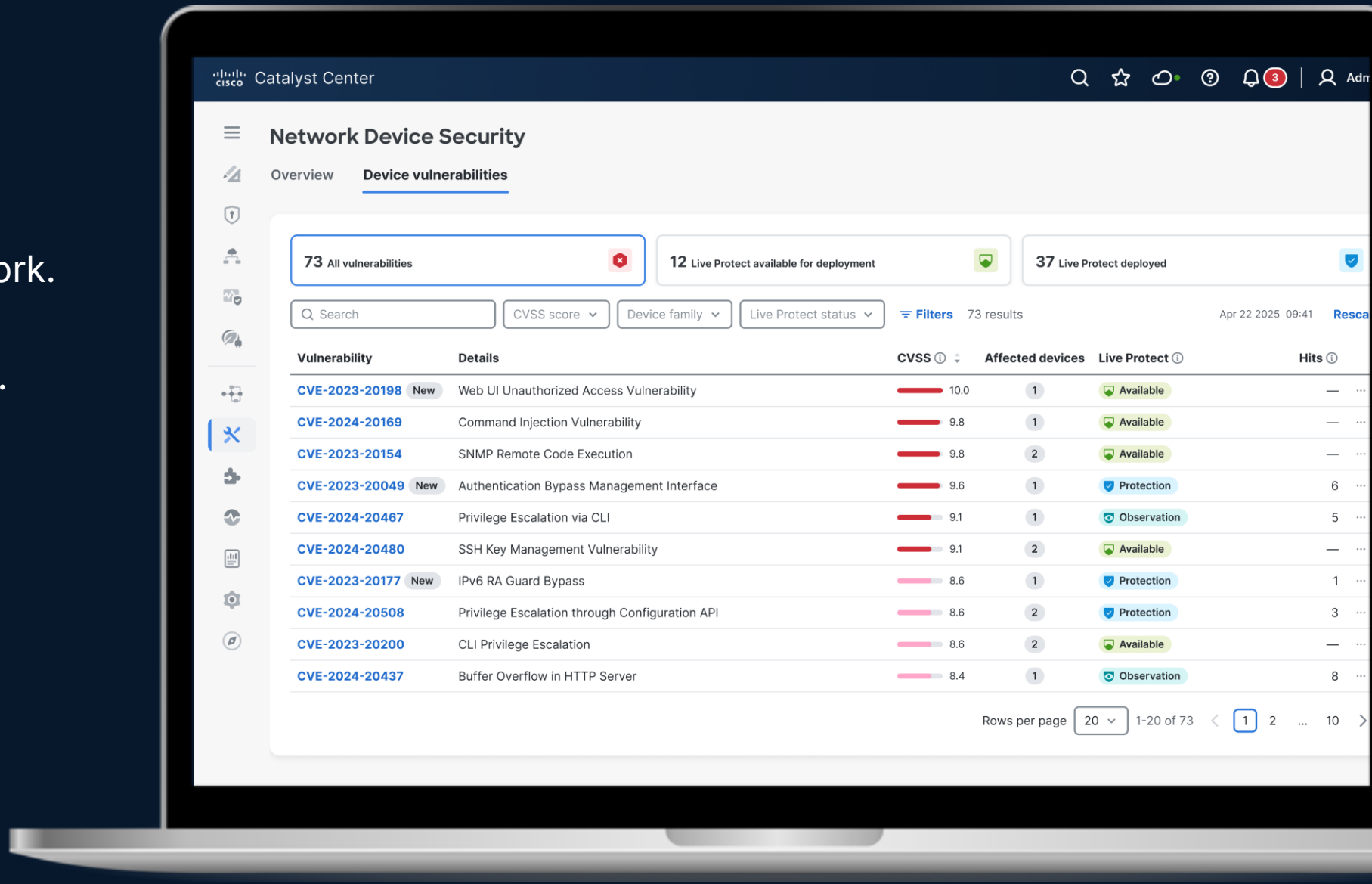
*Not an exhaustive list. Full list of commands here

Coming 26.2.x

Live Protect

Stop the attack, not the network.

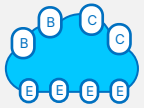
Block vulnerabilities instantly and update on your schedule.



Campus LAN/WLAN – Building Blocks

Definitions, Characteristics and Variations

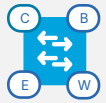
Campus Metro & Branch



Large Site

Medium Site

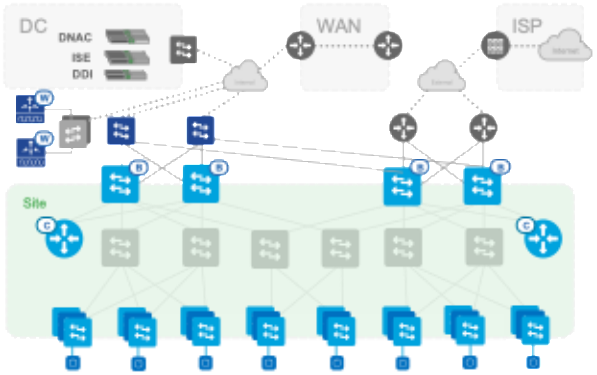
Small Site



Extra Small

Large

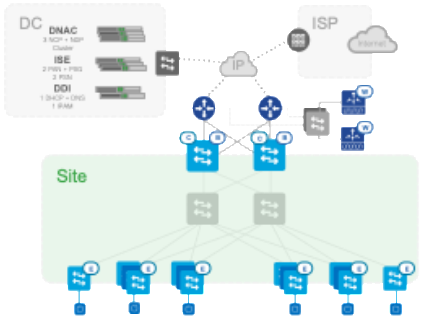
Many Buildings and/or Floors



- 3-4 Tier hierarchical LAN (WAN + MDF & IDF)
- ≥ 50K Client endpoints
  - Switching: Multiple 9500 or 9600 Core & Distro with high-density Stacked 9300 or 9400 Access
  - Wireless: Dedicated CW9800H1/H2 WLC or CCG at Core with large sets of 917X APs per Access
  - Routing: Dedicated SDWAN 8500 Pair per Core with multiple SDWAN regions for Branch

Medium

Several Buildings and/or Floors

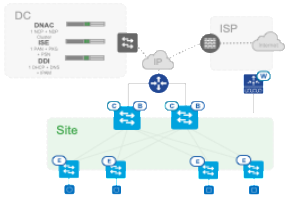


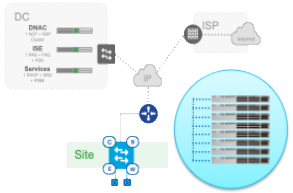
- 2-3 Tier hierarchical LAN (WAN + MDF & IDF)
- ≤ 25K Client endpoints
  - Switching: Pair of 9500 or 9600 Core & Distro with Standalone or Stacked 9300 or 9400 Access
  - Wireless: Dedicated CW9800M WLC or CCG at Core with small sets of 917X APs per Access
  - Routing: Dedicated SDWAN 8300 Pair per Core with few SDWAN regions for Branch

Small Small Small

Few Buildings and/or Floors

XS XS XS XS XS



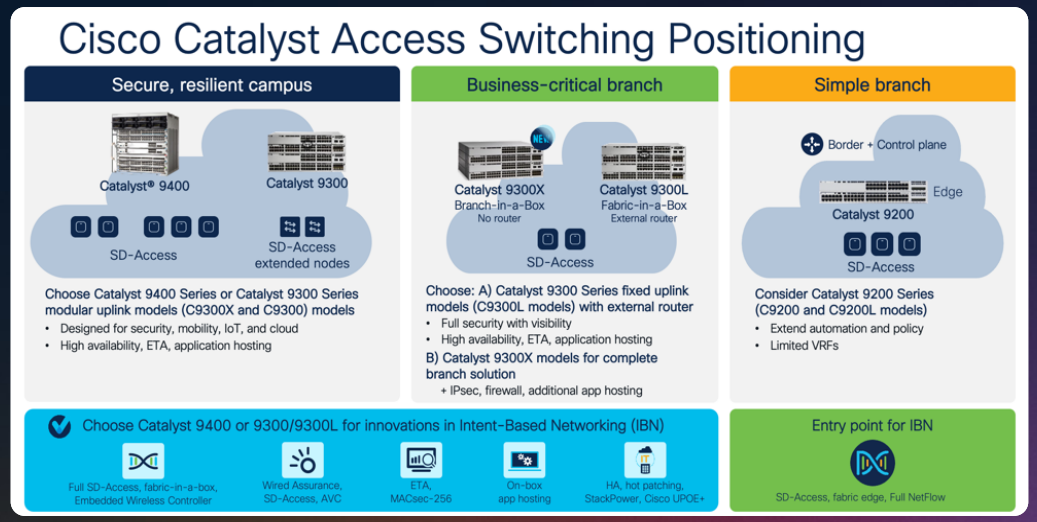


- 1-2 Tier Remote/Branch LAN (WAN + IDF)
- ≤ 5K Client endpoints
  - Switching: Single L2/L3 9300 Access (+Stacking) or separate Standalone 9300 Access & 9500 Core
  - Wireless: Cloud Controller or CW9800L with few 917X APs per Access
  - Routing: Dedicated SDWAN 8200 Pair per Branch

Cisco C9K Architecture Sessions

BRKARC-2098

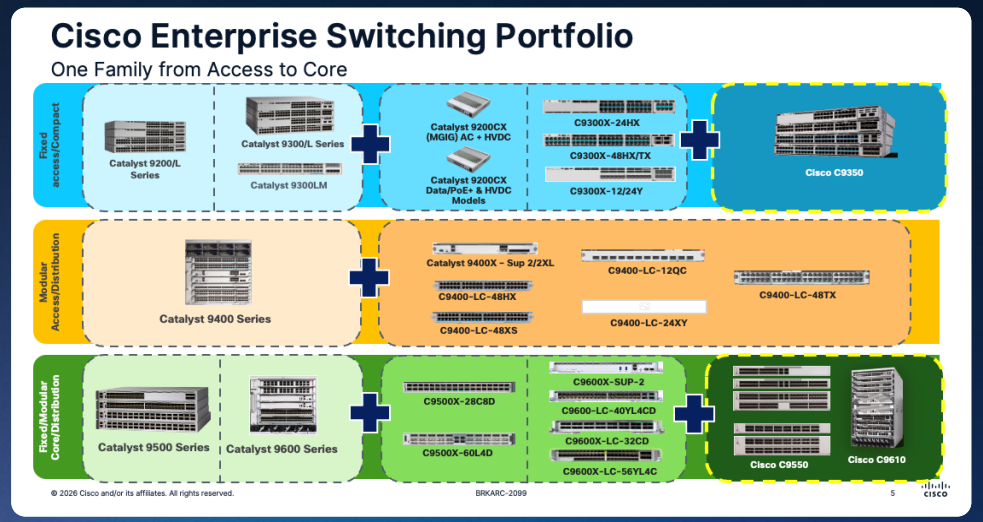
Cisco 9000 Series Switching Family – Access



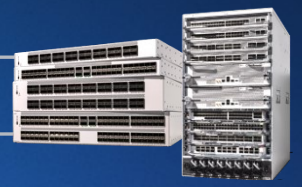
Includes **Cisco C9350 Smart Switches**

BRKARC-2099

Cisco 9000 Series Switching Family – Core & Distribution



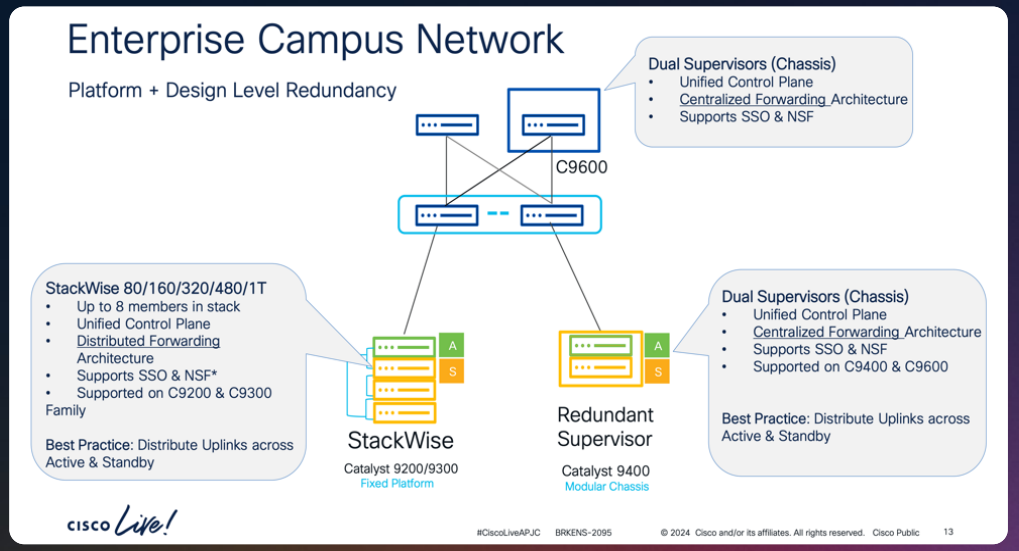
Includes **Cisco C9610 & C9550**



Cisco C9K High Availability Sessions

BRKENS-2095

Designing High Availability with Cisco C9K



This session will cover new and existing high availability features introduced in IOS-XE on Cisco C9000 Series switching platforms.

BRKENS-2504

Introducing Cisco Smart Stacking (NG-SVL)

This session includes a brief introduction of Cisco SD-Access components, and dives into design and scale considerations and deployment options, for single-site designs.

New @ CiscoLive Amsterdam

Scalable Segmentation

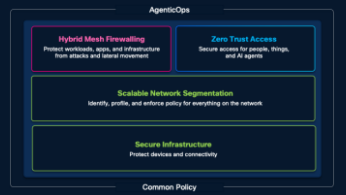
2 **Scalable Network Segmentation**
Overlay Fabric for L2/L3 & Multicast, with SGT & VRF segmentation

www.cisco.com/site/us/en/solutions/networking/sdaccess/index.html

blogs.cisco.com/networking/modernizing-campus-networks-with-fabric-architecture

www.cisco.com/c/en/us/products/collateral/networking/meraki-cloud-management-dashboard/cloud-evpn-campus-fabric.html

Reference design for Scalable Network Segmentation



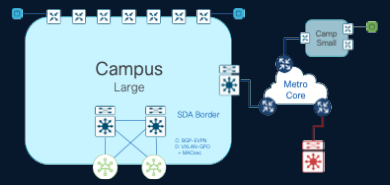
2

Scalable Network Segmentation

Identify, profile, and enforce policy for everything on the network

Secure Fabric:
Campus Overlay for Wired & Wireless LAN

- Wired Overlay
- Wireless Overlay



Secure SDWAN:
SDWAN Overlay for Core & Branch WAN

- Core Overlay
- Branch Overlay

Secure Data Center:
DC Overlay for Data Center LAN

- DC Overlay
- Storage Overlay

Secure Firewall:
Overlay integration for Hybrid Mesh Firewall

- Distributed Virtual
- Central Appliance

1

Secure Infrastructure

Protect devices and connectivity

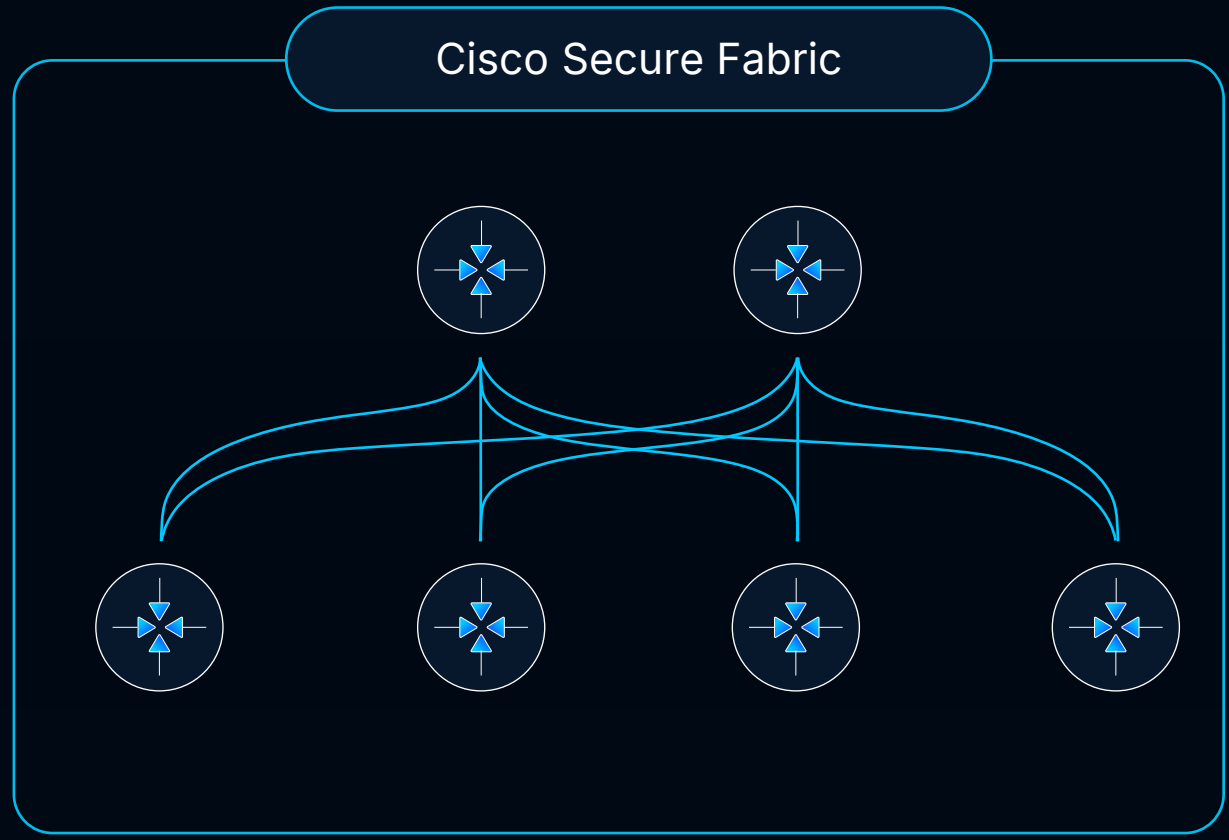
Simplifying network segmentation through automation with campus fabric

IOS XE Switches,
Access Points, Routers

Cloud Fabric

On-Premise Fabric (SDA)

Programmable Fabric



Scalable Network Segmentation

Securing network access and eliminating lateral movement

Native segmentation

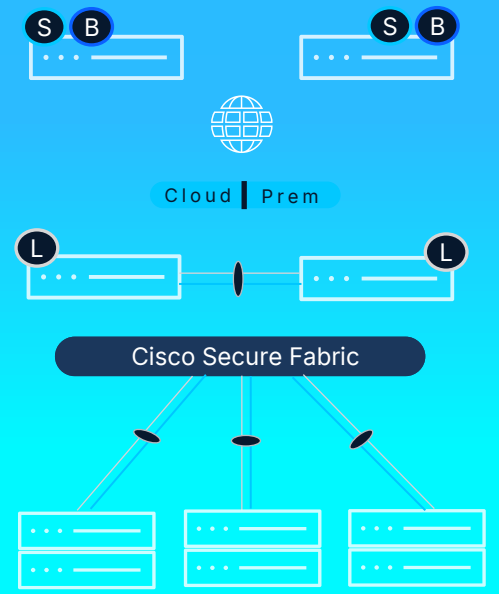
VLAN, SGT, VRF/VPN

Strengthened with NAC

ISE and Access Manager

Automated secure fabric

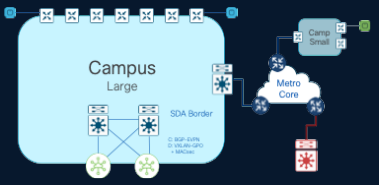
Cloud and On-Premise



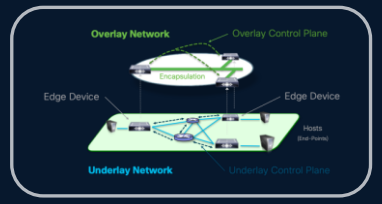
Scalable Network Segmentation

Cisco Campus Fabric

Key Concepts & Considerations (Why it matters)

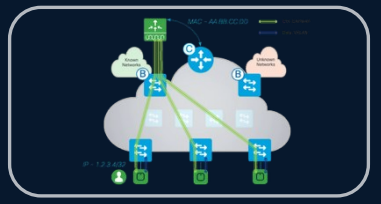


1 L2 & L3 Overlay



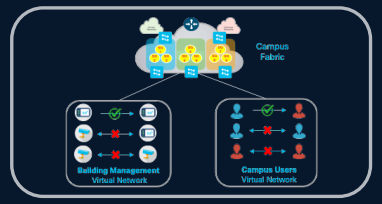
- Support L2 Broadcast & Multicast bridging behavior
  - without reliance on L2 protocols (eg. STP)
- Support IPv4 & IPv6 L3 routing protocols
  - abstracts IGP & EGP into single 'overlay'
- Enable L2 VLANs & L3 Anycast GW across Campus
  - without enabling L2 across the Core

2 Wireless Integration



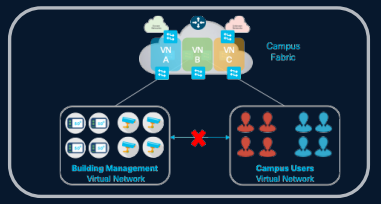
- Simplifies L2 & L3 wireless roaming in the 'overlay'
  - maximizes load-balance & redundancy
- Offload Wireless Data traffic to the Access switches
  - without tunneling back to WLC
- Enables a common policy for wired and wireless
  - single point of policy enforcement

3 Micro-Segmentation



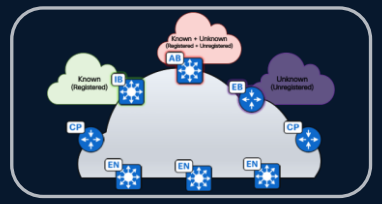
- Segments endpoints based on an Identity (SGT)
  - rather than based on VLAN or IP/subnet
- Enables Group (SGT) based ACL & QoS and more
  - address-independent services
- Fabric natively carries SGT inside of VXLAN-GPO

4 Macro-Segmentation



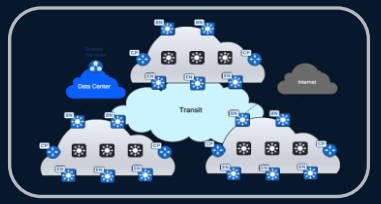
- Segments Groups (IP) into Virtual Networks (VN)
  - isolates VNs from other VNs
- Enables L2 & L3 VPN services and security
  - without MPLS or other VPNs
- Fabric natively carries VNID inside of VXLAN-GPO

5 Fabric Handoff



- Support for L2 or L3 hand-off at Fabric Border
- Native VXLAN hand-off to carry SGT & VRF
  - Includes Cisco NG Firewalls + VXLAN
- Simple IP/MPLS + CTS/SXP hand-offs
  - Includes legacy & third-party Firewalls

6 Multi-Site & Mult-Domain Fabrics



- Connects multiple Fabric Sites & Domains
- Native VXLAN + LISP Transit between Campuses
  - integration with EVPN multi-site
- Native VXLAN + EVPN Transit with Data Centers
  - hierarchical EVPN multi-site

Cisco Campus Fabric

Fabric Design Workflow

5 Multi-Domain

- Campus Fabric to DC Fabric
- Campus Fabric to SD WAN

4 Multi-Site

- Multiple LAN/MAN Fabrics
- Multi-Site Fabric Transits

3 External Services

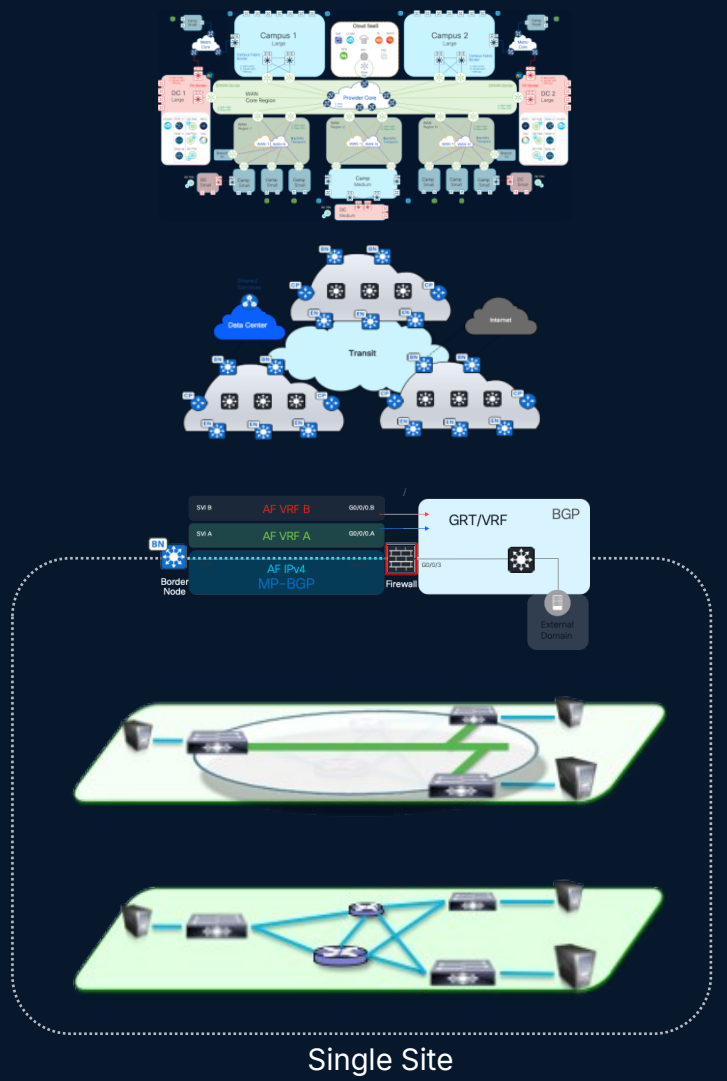
- External Services & Fabric Wireless
- Micro (SGT) & Macro (Firewall) Segmentation

2 Overlay

- Control-Plane Protocol (LISP or EVPN)
- Fabric Addressing (Host or IP/subnet)
- L2VNI vs. L3VNI, Unicast vs. Multicast

1 Underlay

- Underlay IPv4/v6 Routing from Access to Core
- Physical Network Devices & Topology

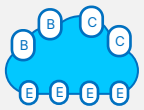


Single Site

Campus Fabric – Building Blocks

Definitions, Characteristics and Variations

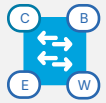
Campus & Branch Fabric



Large Site

Medium Site

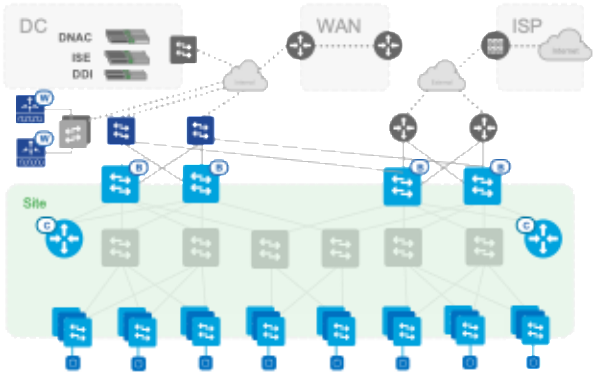
Small Site



Extra Small

Large

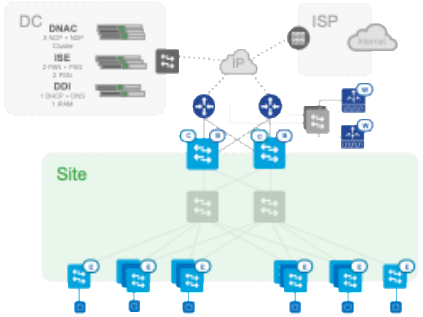
Many Buildings and/or Floors



- 3-4 Tier hierarchical LAN (WAN + MDF & IDF)
- ≥ 50K Client endpoints
- Dedicated CP/RR nodes for higher redundancy
  - Min CP/RR = 4
- Dedicated Border nodes for multiple site exits
  - Min Borders = 4
  - Metro to DC, SDWAN for SP

Medium

Several Buildings and/or Floors

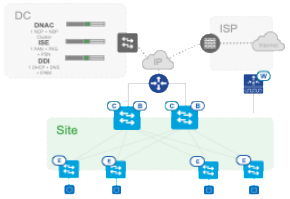


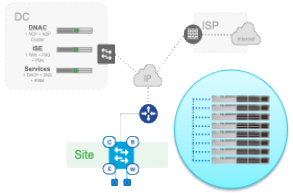
- 2-3 Tier hierarchical LAN (WAN + MDF & IDF)
- ≤ 25K Client endpoints
- 1-2 Collocated Border + CP/RR on same box
  - use separate CP/RR for scale
- Dedicated Edge/Leaf nodes

Small Small Small

Few Buildings and/or Floors

XS XS XS XS XS



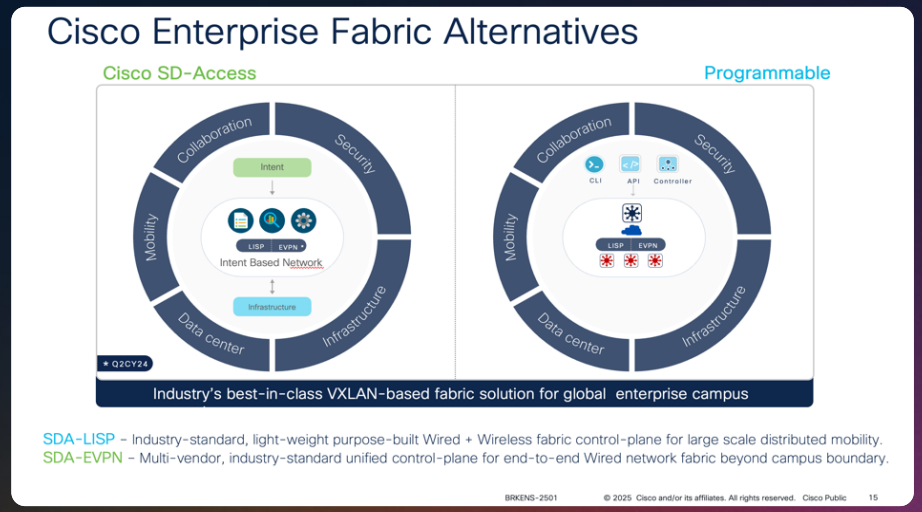


- 1-2 Tier Remote/Branch LAN (WAN + IDF)
- ≤ 5K Client endpoints
- 1-2 Collocated Border + CP/RR on same box
- Dedicated Edge/Leaf nodes
  - Single node (FIAB) as needed

Cisco C9K Fabric Sessions

BRKENS-2501

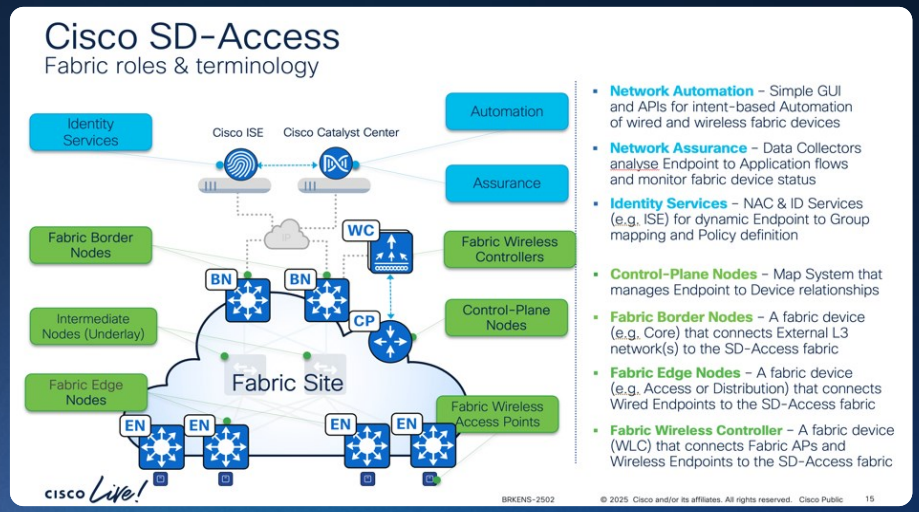
Overlay Design Options for Campus Networks



This presentation will delve into the various overlay design options available with the state-of-the-art Cisco C9000 Switching Platforms.

BRKENS-2502

Cisco SD-Access Fabric: Design and Deployment



This session includes a brief introduction of Cisco SD-Access components, and dives into design and scale considerations and deployment options, for single-site designs.

Zero Trust Access & Mesh Firewalling

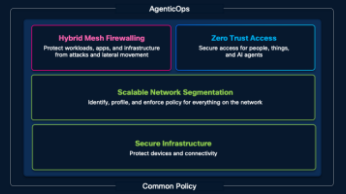
3 Zero Trust Access & Hybrid Mesh Firewall
Identity Policy, Stateful Firewall, Threat Detection & Response

www.cisco.com/c/en/us/solutions/collateral/enterprise/design-zone-security/zt-frameworks.html

www.cisco.com/c/en/us/products/collateral/security/identity-services-engine/common-policy-uniquely-aag.html

Cisco Zero Trust Segmentation

End to End identity-based segmentation from User to App



Unified security

Unified policy

Dashboard

Identity Services

Duo

ISE / Access Manager

Security Cloud Control

SNA

splunk>

XDR

Context Sharing

Context Sharing

Context Sharing

Context Sharing

Config

Auth

Policy

Telemetry

Campus & Branch

User	Device	SGT
Dana (Finance)		10
Contractor		20
IoT - Printer		30
IoT - Camera		40

Campus Fabric (L2/L3 Segmentation)

WiFI

VLAN

VRF

VXLAN

Switching

SGT enforcement in Campus wire & wireless 10 20 30 40

Campus Firewall

Threat Detection & Compliance

Secure SDWAN

SGT enforcement in SDWAN & Firewalls

Security Service Edge

Zero Trust for Public, Private and SaaS

Hybrid DC

DC Firewall

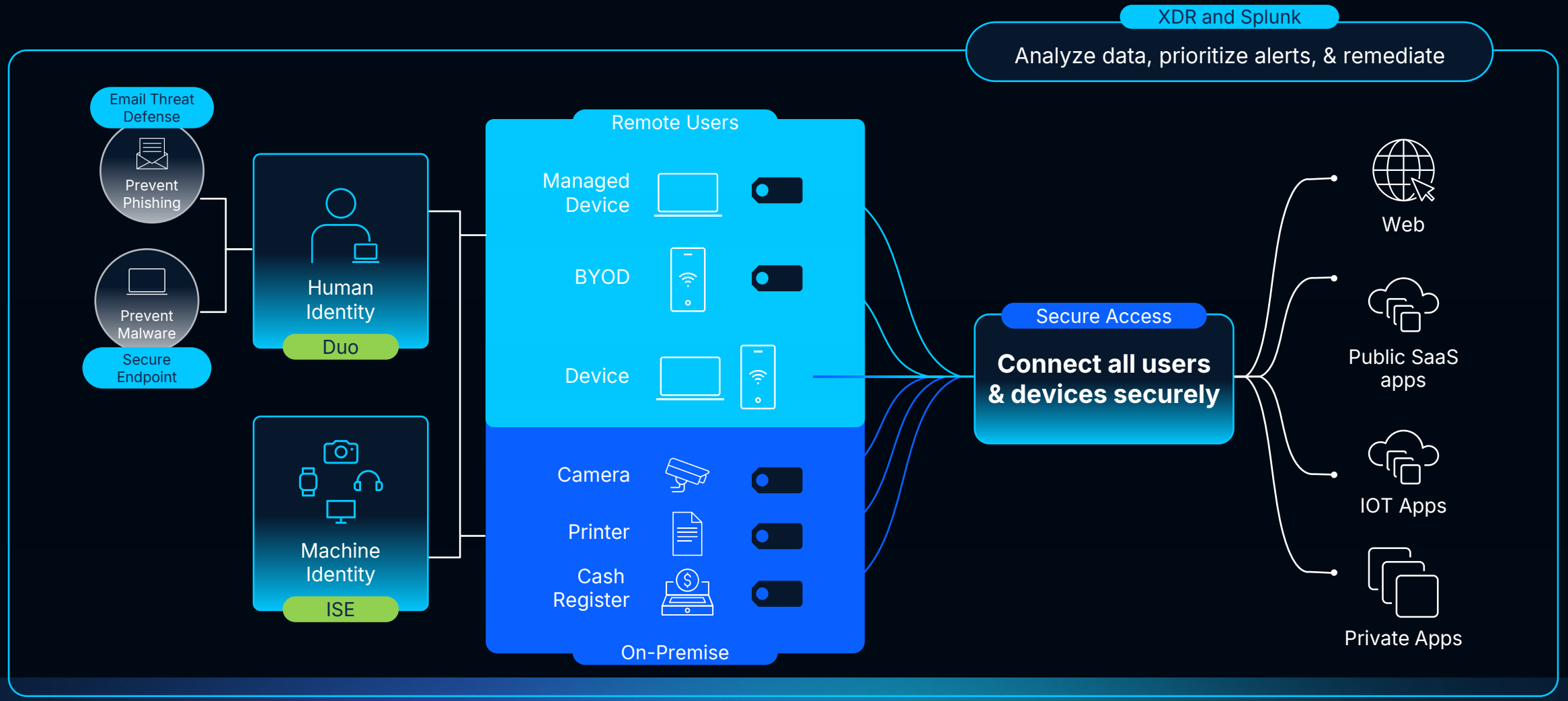
DC Fabric

ACI

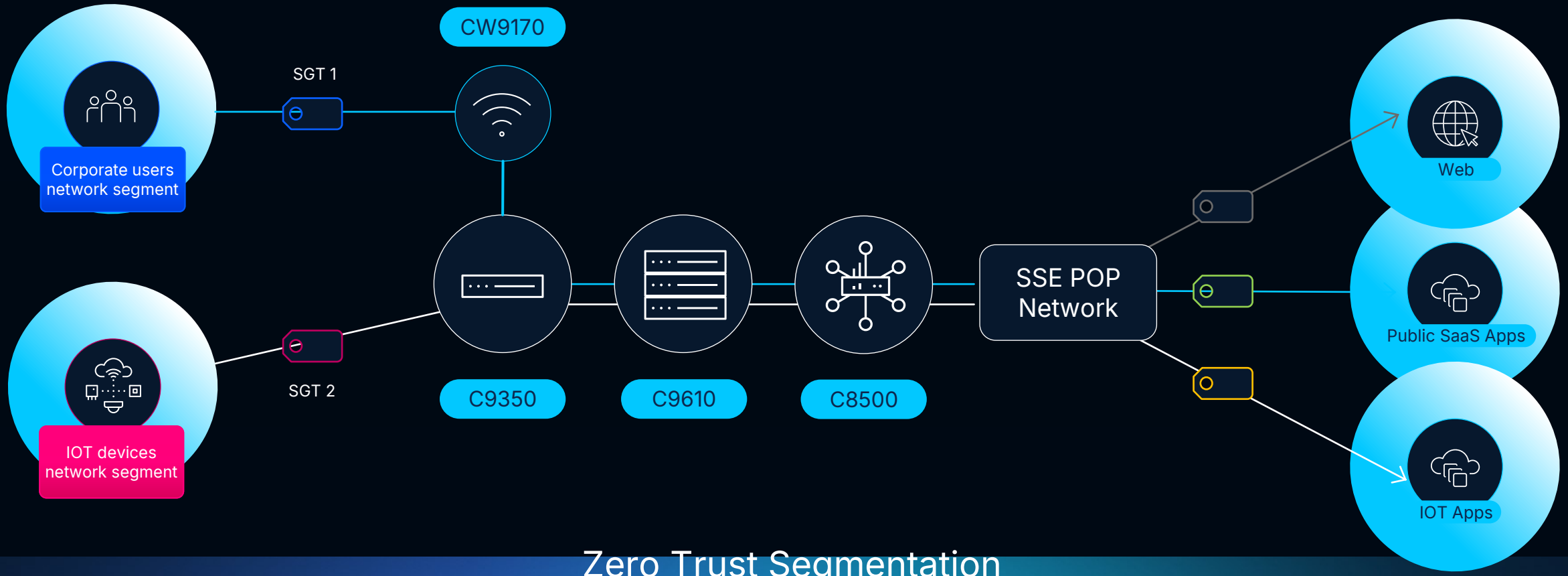
10 20

SGT enforcement in Security Service Edge & Data Centers

Protect users on any device, anywhere they connect



A unified framework for managing security policies across diverse IT environments



Zero Trust Segmentation

Zero Trust Access & Common Policy

Design Workflow

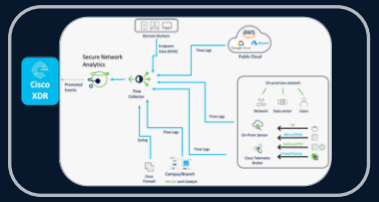
1 Identity & Group Policy

- Identity & Group-based Policy Micro Segmentation - powered by Cisco ISE

2 Mesh Firewall Policy

- Stateful Firewall-based Macro Segmentation - powered by Cisco SCC

3 Threat Detection & Response



- Threat Detection and Response - powered by Cisco SNA and Cisco Splunk

1

Zero Trust Access & Common Policy

Identity and Group Policy

www.cisco.com/site/uk/en/products/security/identity-services-engine/index.html

documentation.meraki.com/Platform_Management/Access_Manager

www.cisco.com/site/us/en/products/security/duo/index.html

Cisco ISE's role in Zero Trust

Establish Trust

User & Device Authentication and Trust

Enforce Trust Based Access

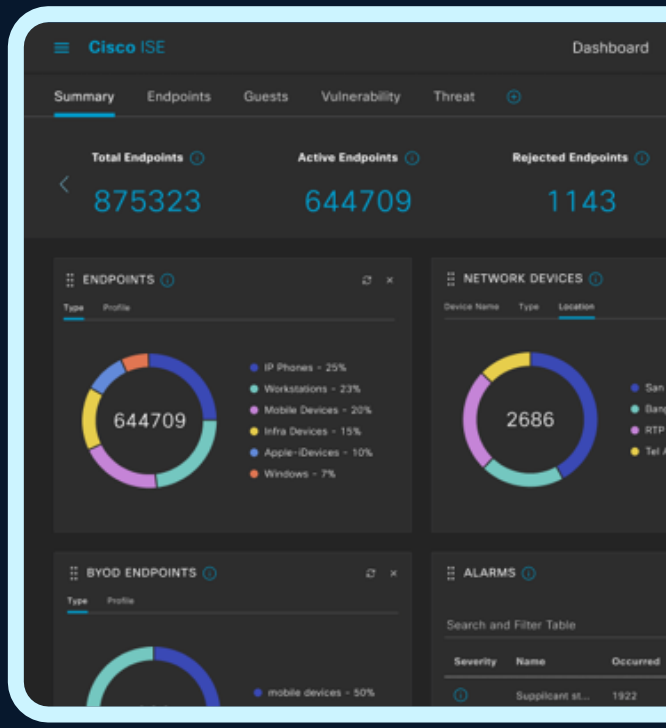
Network Segmentation enabled by Granular Context

Continuously Verify Trust

With Integrated Threat Intelligence

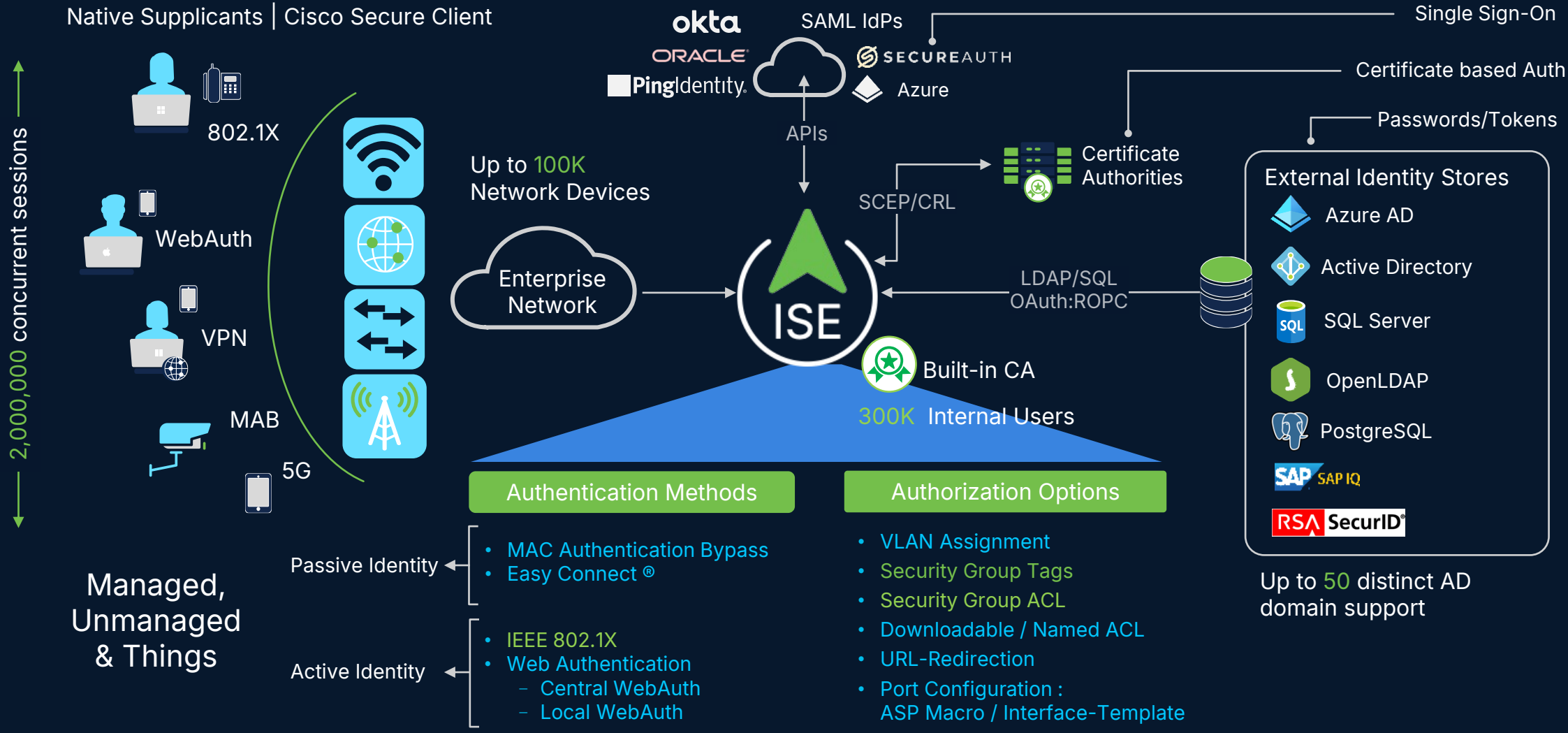
Respond to Change in Trust

With Adaptive Network Control



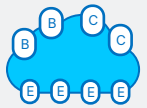
Identity Services Engine (ISE): Identity & Group Policy

Identity is the first step towards Zero Trust and Common Policy



Identity & Group Policy: ISE

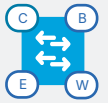
ISE Node Building Blocks



Large Site

Medium Site

Small Site



Very Small

cs.co/ise-scale

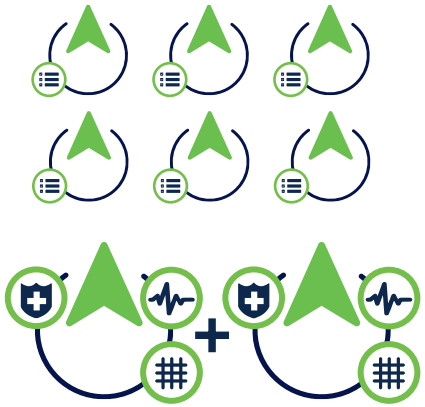
Extra Small

1 x (PAN+MNT+PSN+PXG)

Small

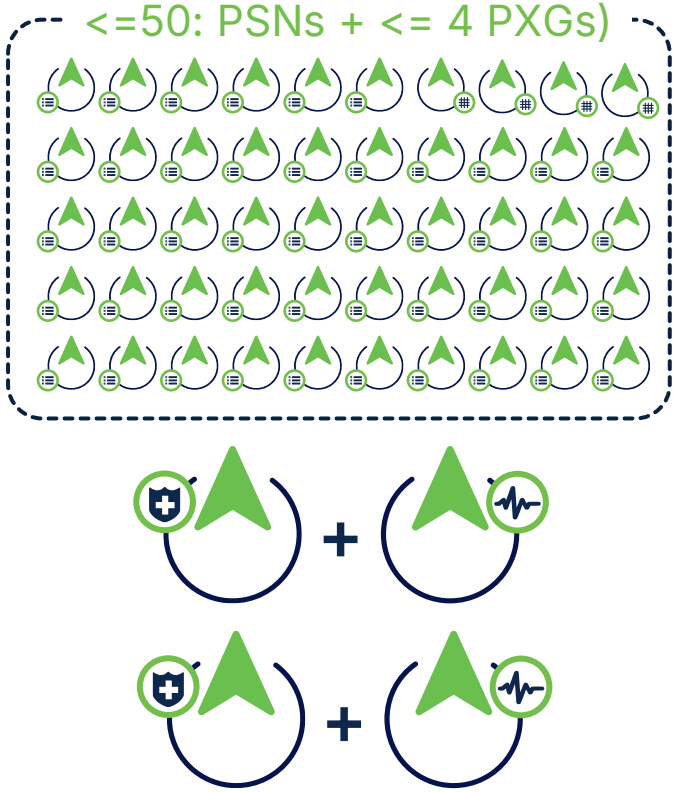
2 x (PAN+MNT+PSN+PXG)

Medium



2 x (PAN+MNT+PXG), <= 6 PSN

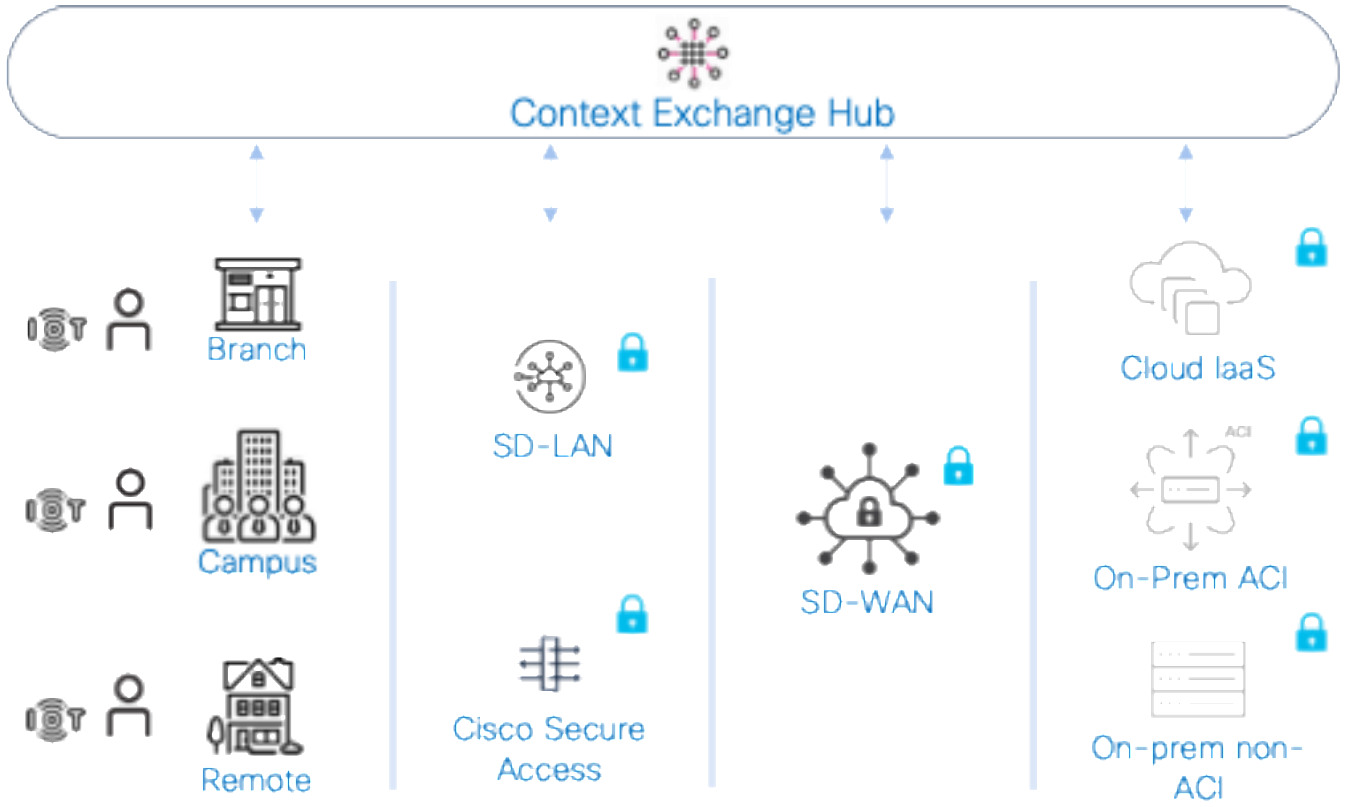
Large



2 PAN, 2 MNT, <=50: PSNs + <= 4 PXGs

What Common Policy Enables

Policy Enforcement Points: Consistent Policies



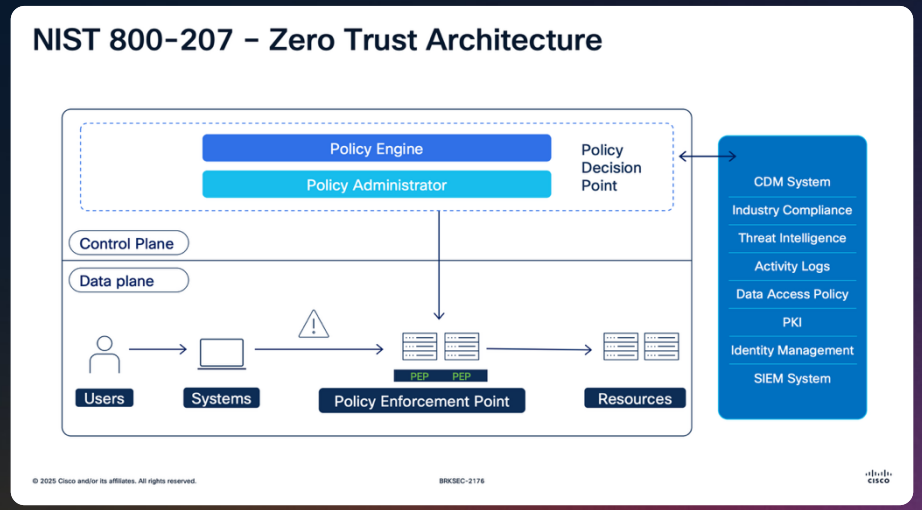
- Build context in its local domain and store it as standard security group tags (SGT)
- Share context everywhere, across networking and security domains
- Enforce consistent SGT based policies, enable simple and unified policy experience

Context-aware policies for on-prem app and cloud workloads for multiple enforcement points

Cisco Zero Trust & Common Policy Sessions

BRKSEC-2176

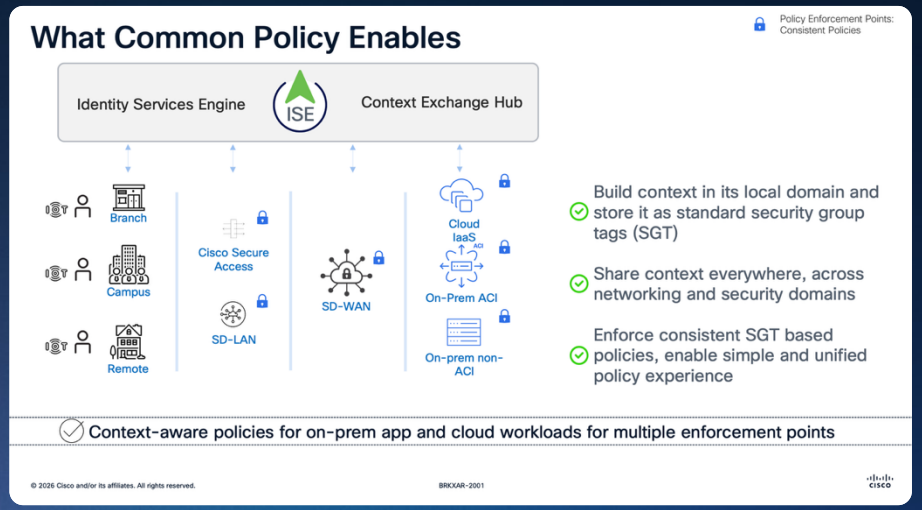
Keeping Up with Zero Trust



This session will cover the topmost commonly deployed use cases (i.e. Universal ZTNA) that spans from user to workload-data-application (*north-south traffic*) and workload–data-application to workload-data-application (*east-west traffic*).

BRKXAR-2001

Common Policy to rule them all

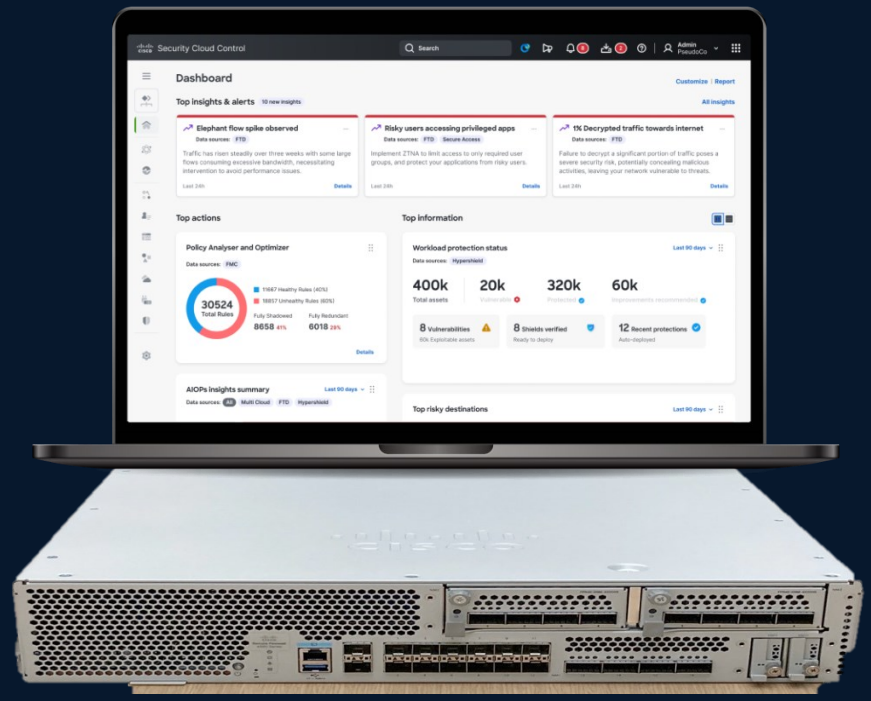


This session demonstrates how ISE brokers policies across multiple domains - Campus, WAN, and Data Center. It also includes a live demo showcasing how the ISE policy model can reduce reliance on firewalls in the campus environment and simplify enforcement consistently across all domains.

2

Zero Trust Access & Common Policy

Mesh Firewall Policy

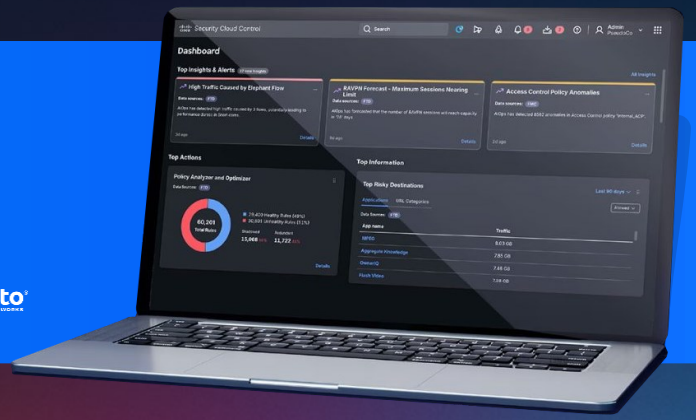


www.cisco.com/site/us/en/solutions/security/hybrid-mesh-firewall/index.html

www.cisco.com/site/us/en/learn/topics/security/what-is-hybrid-mesh-firewall.html

Security Cloud Control

Now powering industry's first multi-vendor intent-based segmentation



Write policy once, enforce everywhere

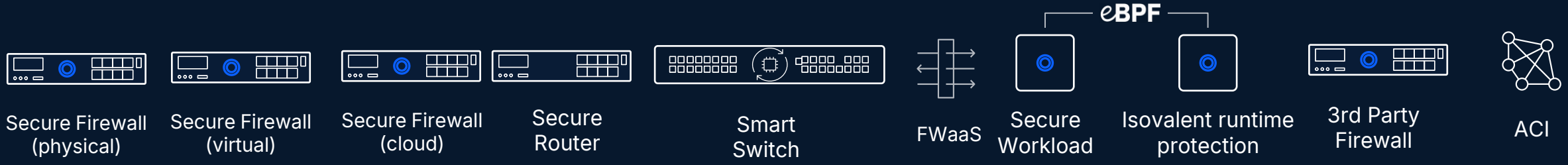
Absorb and optimize existing rules

Change enforcement points, not policy

Hybrid Mesh Firewall: Distributed Firewall Policy

Advanced protection, simplified operations and real-time intelligence for a more secure, scalable future

Security Cloud Control



← Native enforcement points go deeper → Integrate with existing

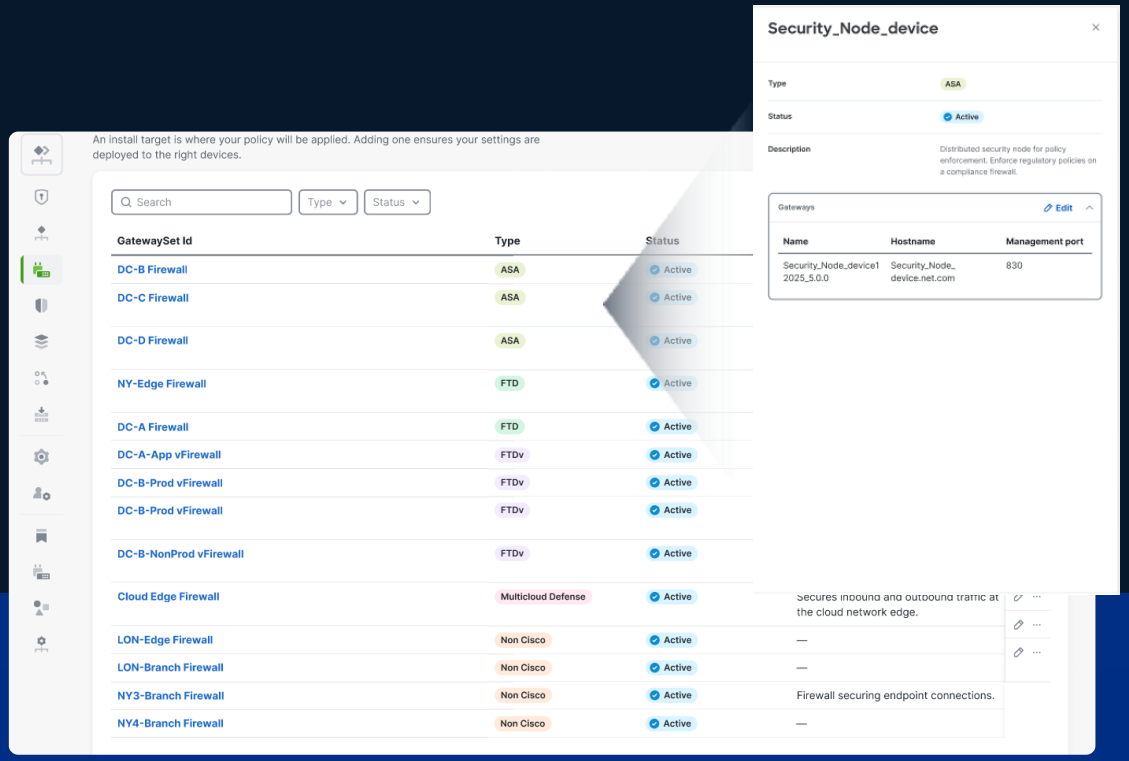
Write policy once - enforce across the mesh

Change enforcement points - not policy

Intent-based policy examples

- Provide HR app access to timekeeping app
- Allow cloud access from ERP to HR app
- Allow HR app to access HR data app
- Block non-prod access to production zone

The “why” of the policy remains connected across devices and adapts dynamically to new devices

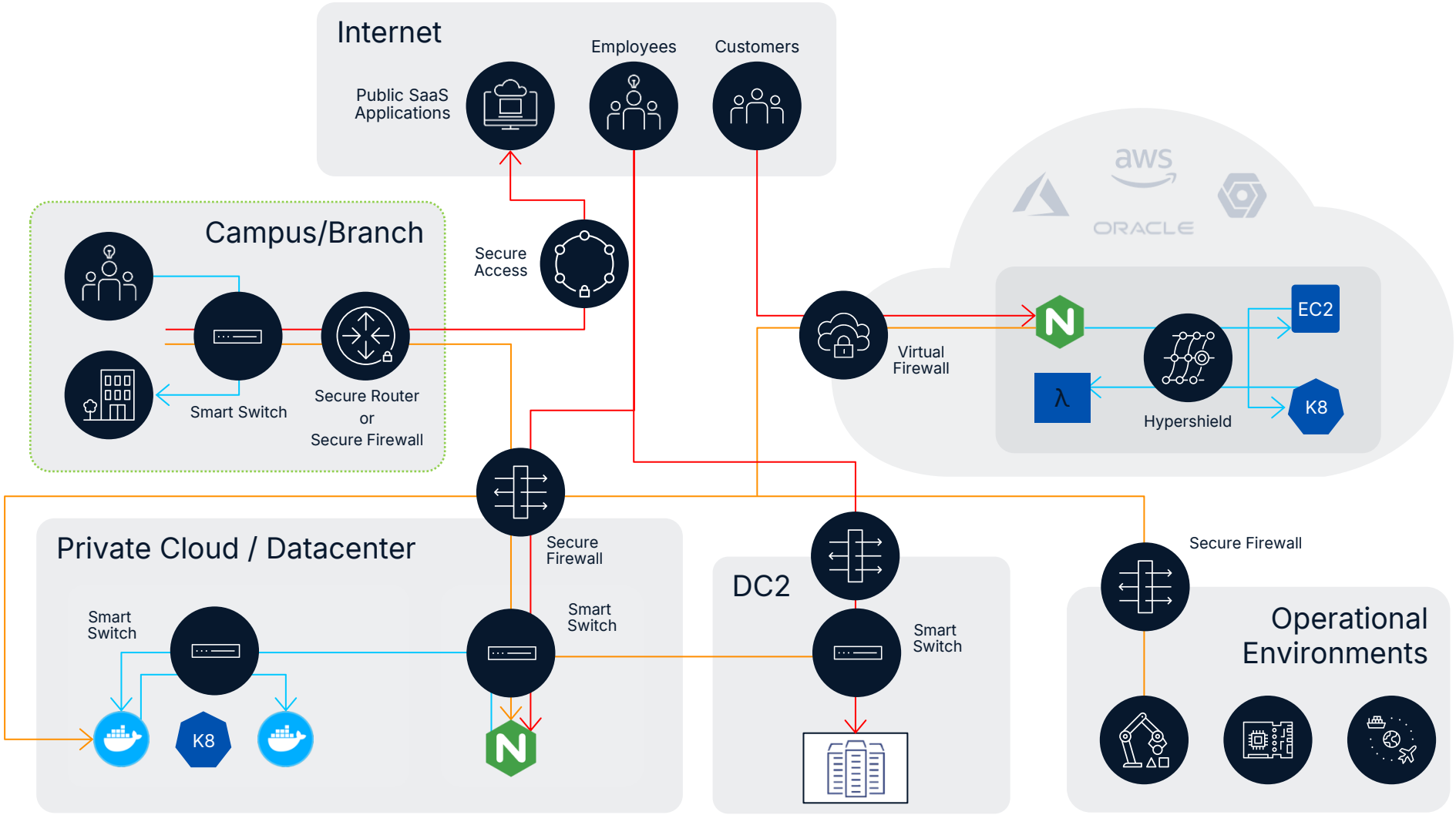


No rip-and-replace

Cisco makes it easy to add hybrid mesh firewall into your existing network

Hybrid Mesh Firewall: Distribtued Firewall Policy

Goes broader and deeper



Secure connectivity between campus, branch, and private cloud

Securely connect campus to Internet and SaaS apps, and employees to private apps

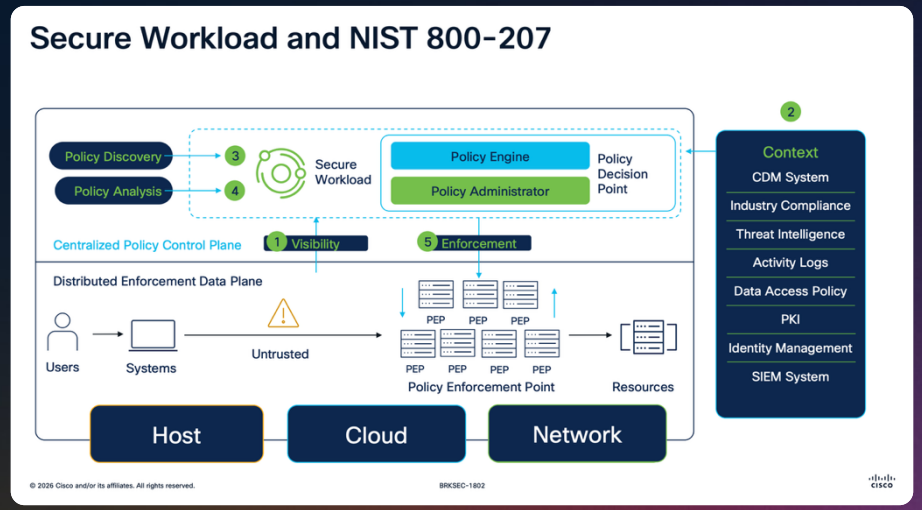
Apply full security stack (IPS, WAF, DLP at virtual public cloud (VPC) edge

Inline security for every workload, microservice, and switch port

Cisco Hybrid Mesh Firewall Sessions

BRKSEC-1802

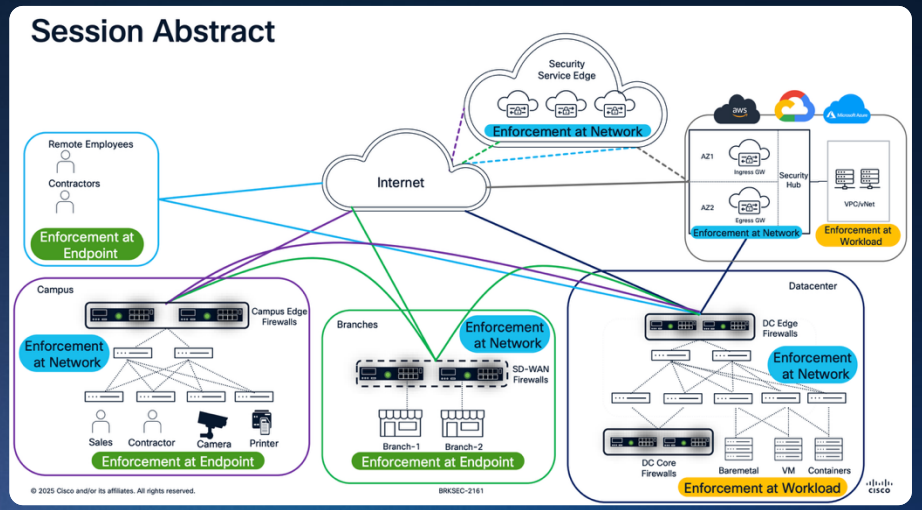
Unifying Security with Hybrid Mesh Firewalls



This session focuses on building hybrid mesh firewalls using Cisco Secure Workload, Firepower Threat Defense (FTD), Secure Cloud Controls, and Multicloud Defense. We'll present how these technologies interoperate to deliver unified security policies, automated threat response, and seamless segmentation across hybrid deployments.

BRKSEC-2161

Solving the Segmentation Puzzle

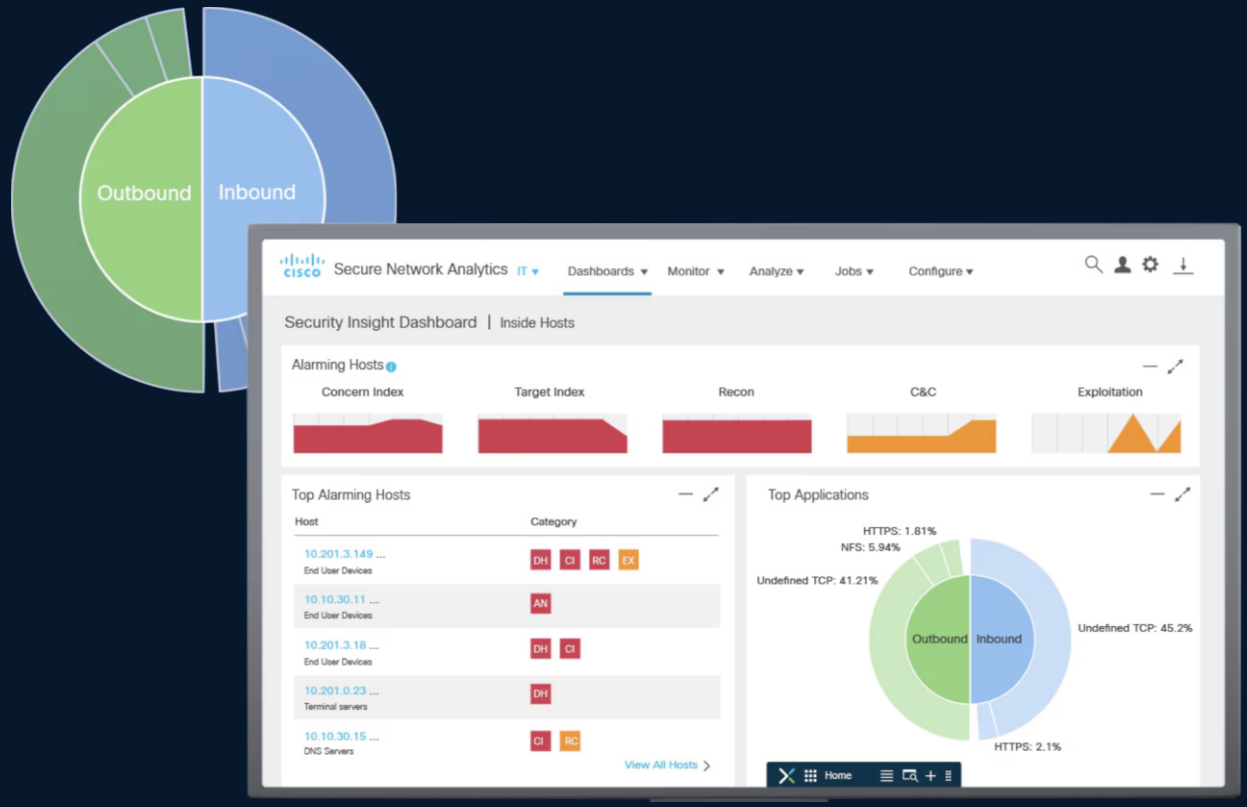


This session will navigate through the Network/NetSec team lenses on how you can leverage Secure Workload to define a common policy model for your applications using agent and agentless approaches to protect your application workloads regardless of their form factor (baremetal, VM or container) or location (on-prem or multi-cloud).

3

Zero Trust Access & Common Policy

Threat Detection & Response



www.cisco.com/site/uk/en/products/security/xdr/index.html

www.cisco.com/site/uk/en/products/security/security-analytics/secure-network-analytics/index.html

Cisco Threat Detection & Response

Cisco SNA with XDR to act on Endpoint and Network Telemetry

Behavioral & Machine Learning modeling

Behavioral analysis of every activity within the network to pinpoint anomalies

Cisco XDR

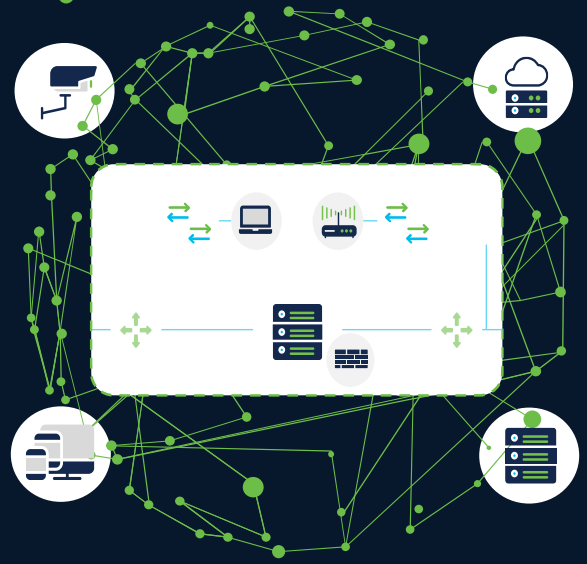
Extended Detection and Response with Cisco XDR. Advanced analytics extends local detections with global intelligence and integrations for accelerated response

Cisco SNA

Secure Network Analytics

Network Telemetry

Rich telemetry from the existing network infrastructure including enhanced telemetry for encrypted traffic analytics and firewall connection logs and security events.



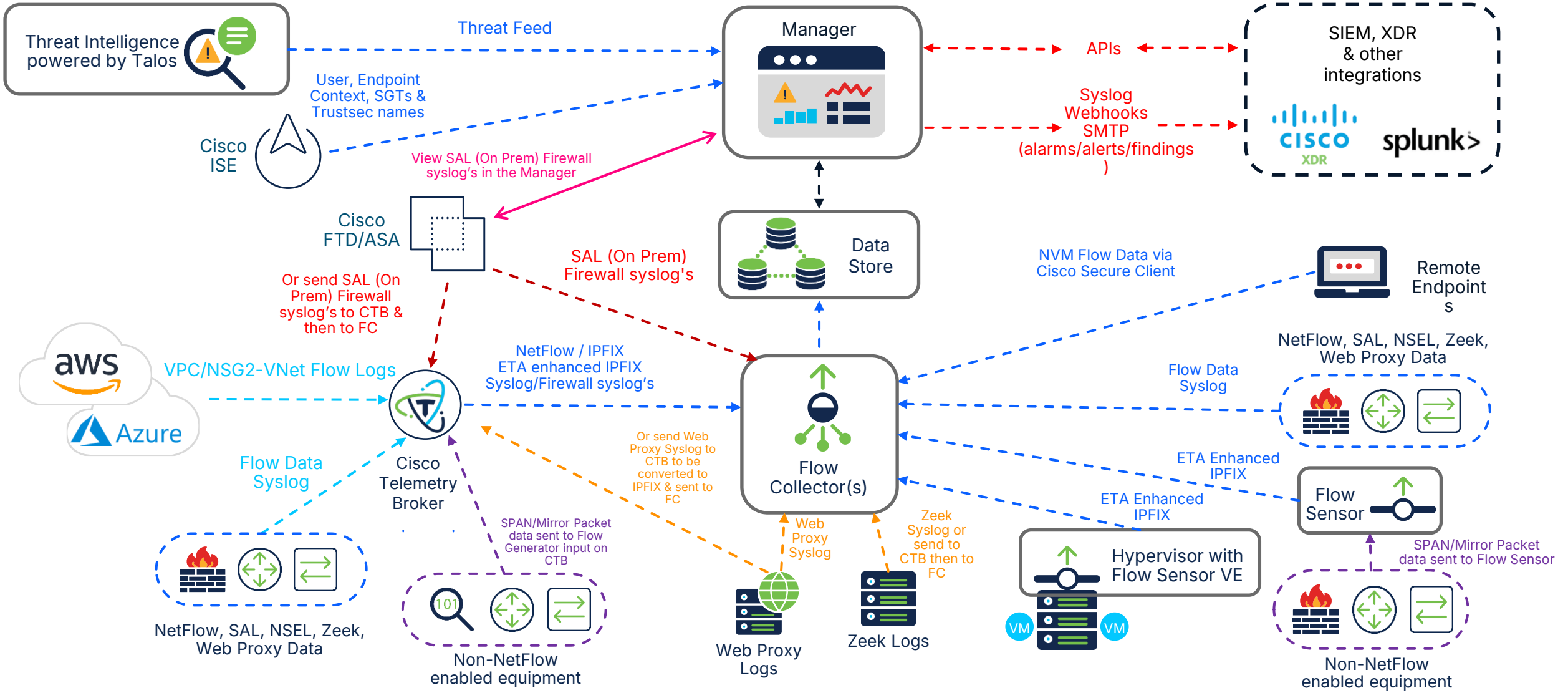
Endpoint Telemetry

Device and process insight with flow telemetry from Cisco Secure Client

Threat Detection & Response: SNA

Cisco SNA Detailed Architecture

cisco.navattic.com/BRKSEC-2928



Secure Networking + Assurance in action

Zero trust policy change

Policy without validation = blind risk

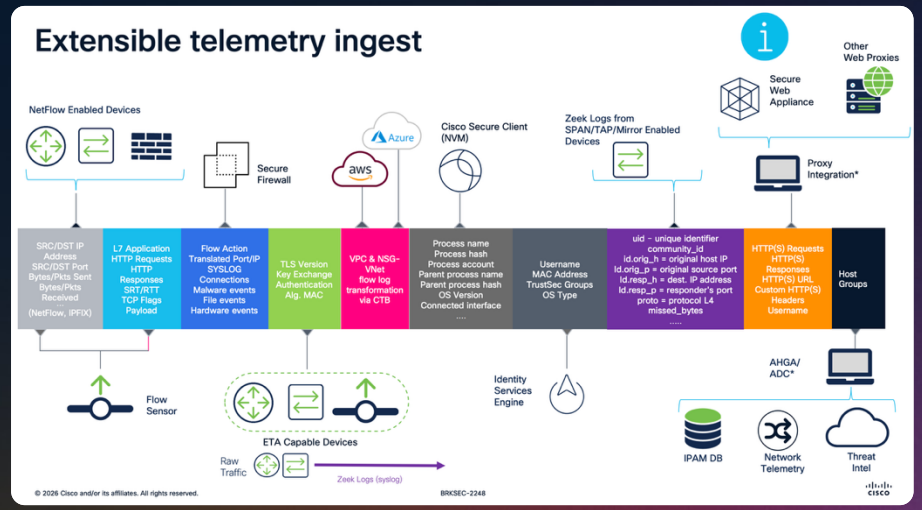
- Policy optimizes access for one region
- Unexpected impact degrades user experience

Assurance turns policy into trusted outcomes

Cisco Detection & Response Sessions

BRKSEC-2248

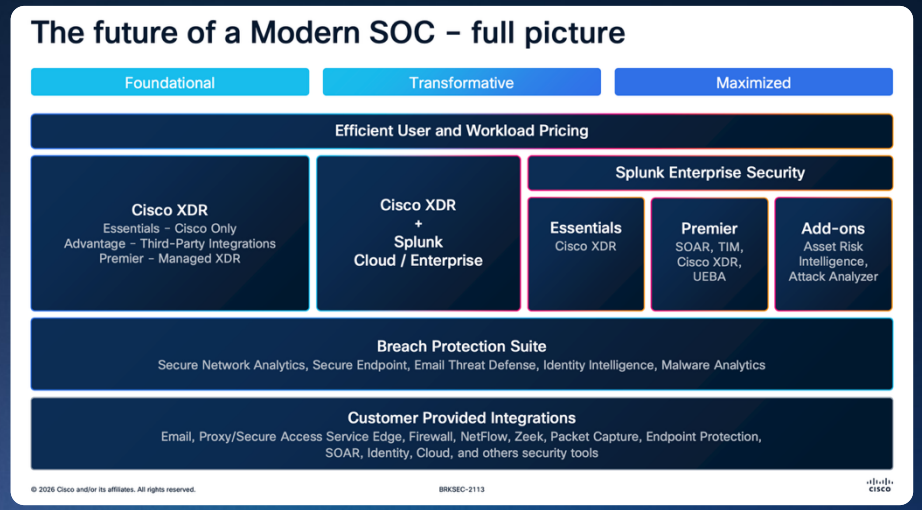
Design and Deploy Network Detection & Response



This session will provide details on how to design and deploy Secure Network Analytics (SNA) in a hybrid environment. The attendees will learn how to integrate the different telemetry sources and their contribution into the analytics including firewall, network, endpoint and cloud data.

BRKSEC-2113

Cisco XDR - Making Sense of all the Parts & Pieces



This session offers a comprehensive walkthrough of Cisco XDR's feature set, latest innovations, and real-world use cases with demos designed to empower your SOC to detect, investigate, and respond faster and more confidently.

Unified Management & Agentic Ops

4 Unified Management & Agentic Ops
On-Premise & Cloud Automation & Analytics, including AIOps

blogs.cisco.com/tag/unified-experiences

www.cisco.com/c/en/us/products/collateral/networking/software/networking-subscription-ds.html

www.cisco.com/c/en/us/solutions/collateral/industries/drive-operational-excellence-with-it-competencies-so.html

Unified management to simplify operations

PLATFORM

Management

API / Integrations

Assurance

Intelligence - AgenticOps

HARDWARE

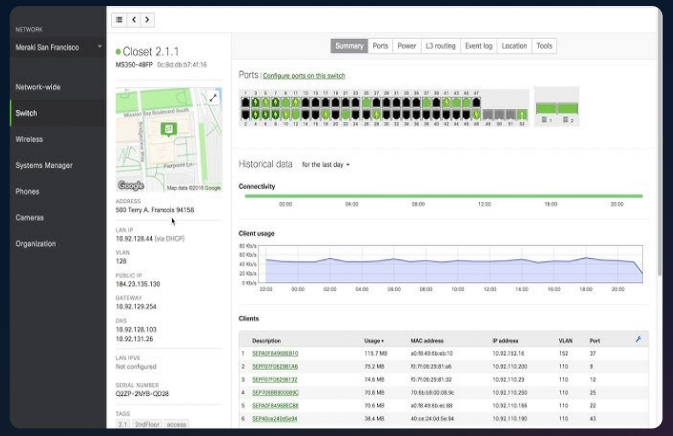
Smart Switches

Secure Routers

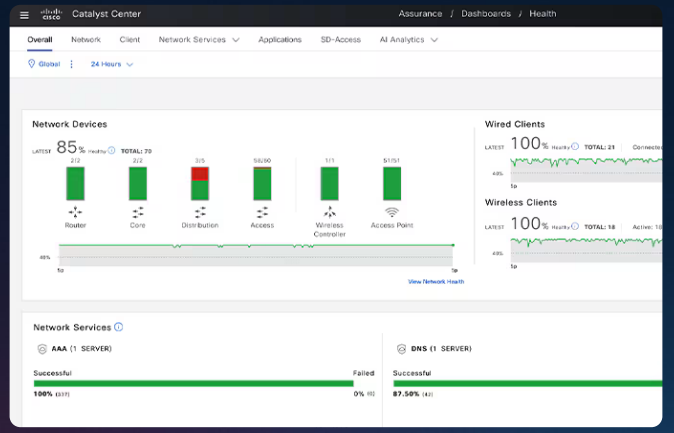
Wireless

Industrial IoT

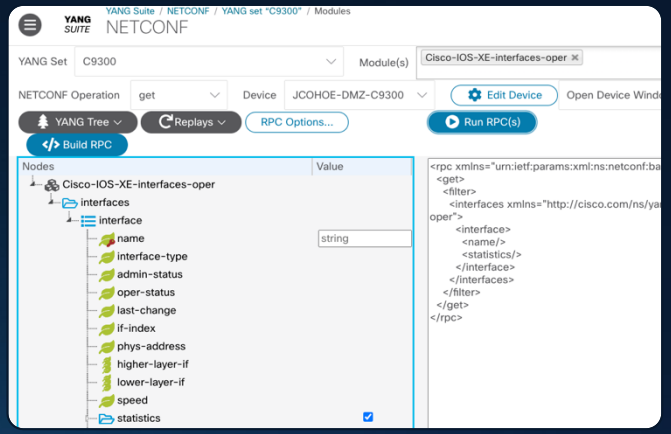
Management and Assurance Choices



Cloud Management
via Meraki dashboard



On-Premise Management
via Catalyst Center (CC)

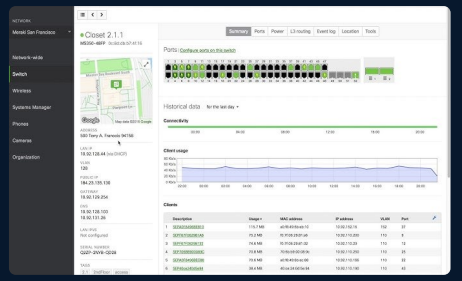


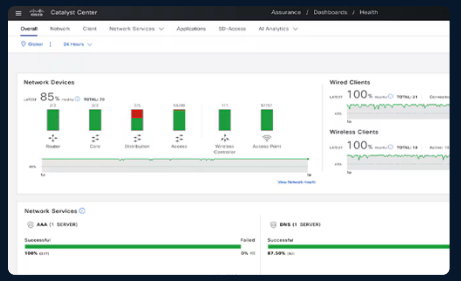
Programmable (DIY)
via Programmable interfaces

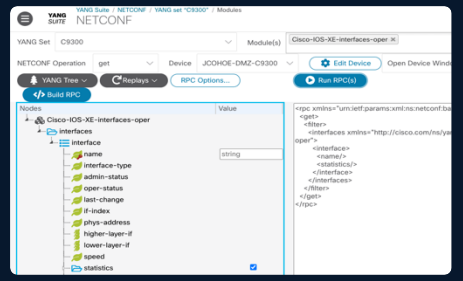
One Device, One OS, One License: Multiple Ways to Manage

https://community.meraki.com/t5/Feature-Announcements/Introducing-the-Meraki-and-Catalyst-Center-Global-Overview-all/ba-p/286891

Cisco Management & Assurance

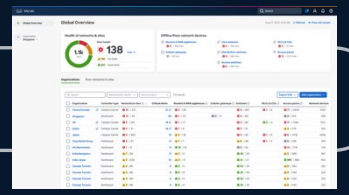






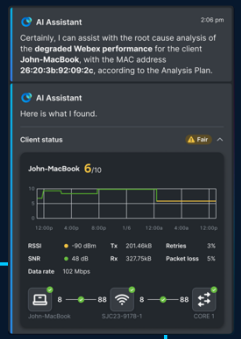
	Meraki Dashboard	Cisco Catalyst Center	Programmability
Deployment	Cloud-native, cloud-managed	On-premises or cloud (physical/virtual)	Device-level programmability interfaces
Management Style	Simplified, intuitive, zero-touch	automation, assurance, policy	Model-driven, API-based automation
Target Users	Enterprise IT, managed services	Enterprise IT teams needing full lifecycle	Network engineers/developers with automation skills
Automation & Provisioning	Automated firmware upgrade, guided provisioning	Intended based deployment and provisioning	Full programmability with YANG models
Visibility & Assurance	Network-wide assurance, alerts	End-to-end health, AI assisted diagnostics	Telemetry and model-driven monitoring
Extensibility & Integration	Rich API ecosystem	APIs for third-party integration	Integration with automation tools (Terraform, Ansible)
Security	Built-in zero-trust security	Integrated security suite, zero-trust	Secure platform with trusted boot
Use Case	Cloud-managed networks, hybrid environments	Campus and branch network management	Advanced automation and customization

NEW: Introducing Meraki & Catalyst Center ‘Global Overview’



Management & Assurance

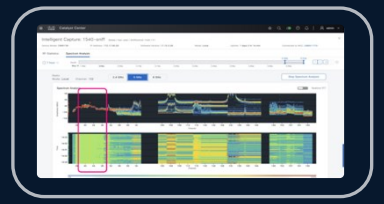
Key Concepts & Design Considerations (Why it matters)



1 Operations Model

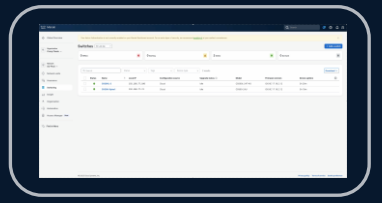
- On-Premises, Cloud & Programmable
- Controller redundancy (Physical & Virtual)
- API support (Northbound & Southbound)

2 Analytics & Agentic Ops



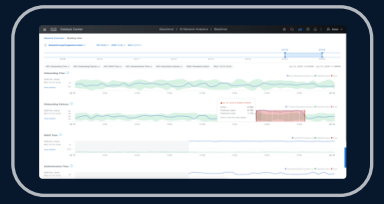
- Real-time & historical analytics (Intelligent Capture)
- AI/ML anomaly detection (AI Assistant & Canvas)
- Machine Reasoning Engine (MRE)

3 Lifecycle Management



- Device Onboarding (PNP, ZTP)
- Configuration Management
  (templates, golden config, software version, validation, verification and rollback)

4 Performance & Monitoring

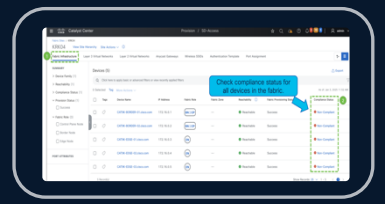


- Client Health (link, apps, uptime)
- Device Health (CPU, memory, ports)
- Link Health (errors, drops, utilization)
- App Health (performance, drops, latency)

5 Network Visibility

- Network Inventory
  - Users/Clients
  - Devices
  - Applications
- Network Topology (Physical, L2, L3)

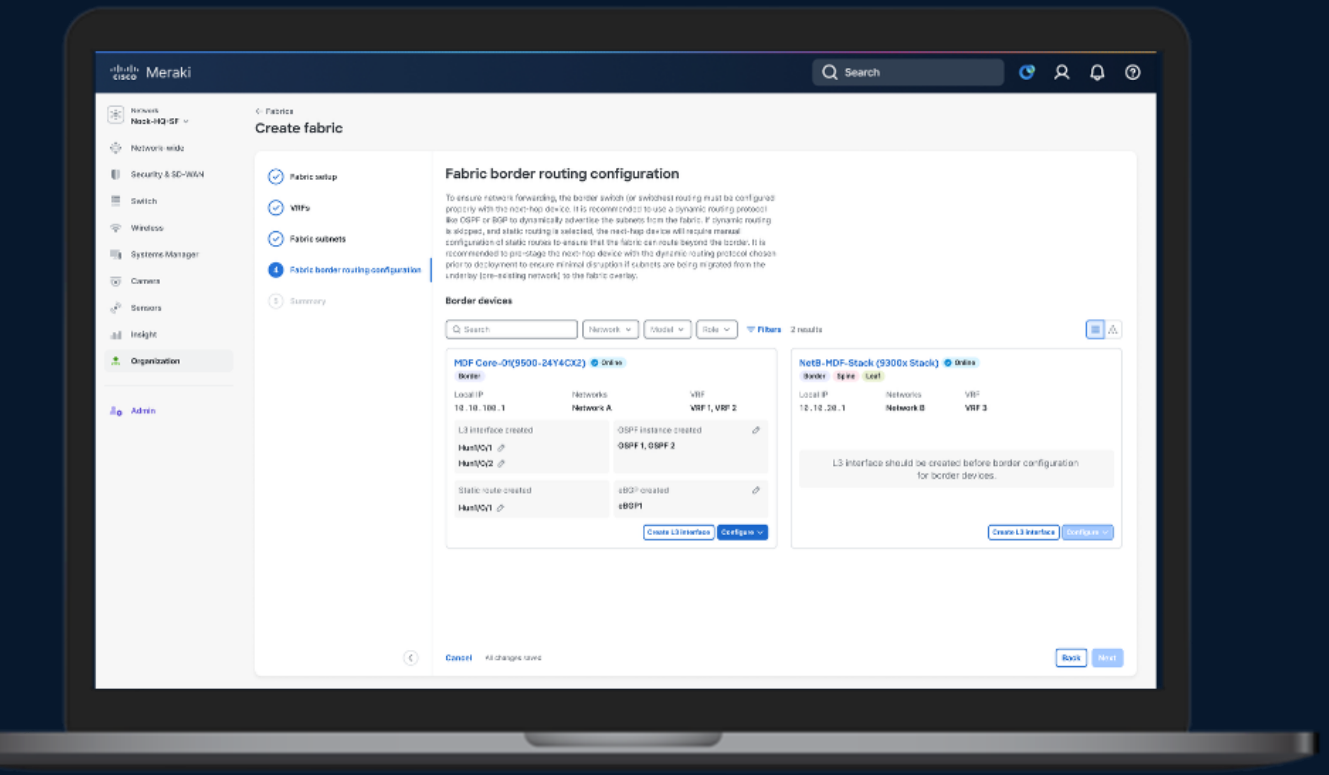
6 Software & Compliance



- Software Image Management (SWIM)
  - SMU, ISSU & XFSU
- Unified License Management
- Compliance (PSIRT, EoX, Configuration)

Introducing Cloud-managed Campus Fabric

Fabric Orchestration from Meraki Dashboard



Cloud Managed Fabric Value

Cloud Simplicity
Build and manage many sites from an intuitive cloud networking platform

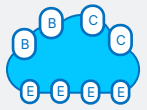
Leverage Existing Investments
Modernize the network while utilizing existing C9K or MS infrastructure

Migrate at Your Own Pace
Incrementally migrate devices and subnets to the cloud over time

Campus Automation – Building Blocks

Definitions, Characteristics and Variations

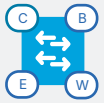
Cloud Automation & Analytics



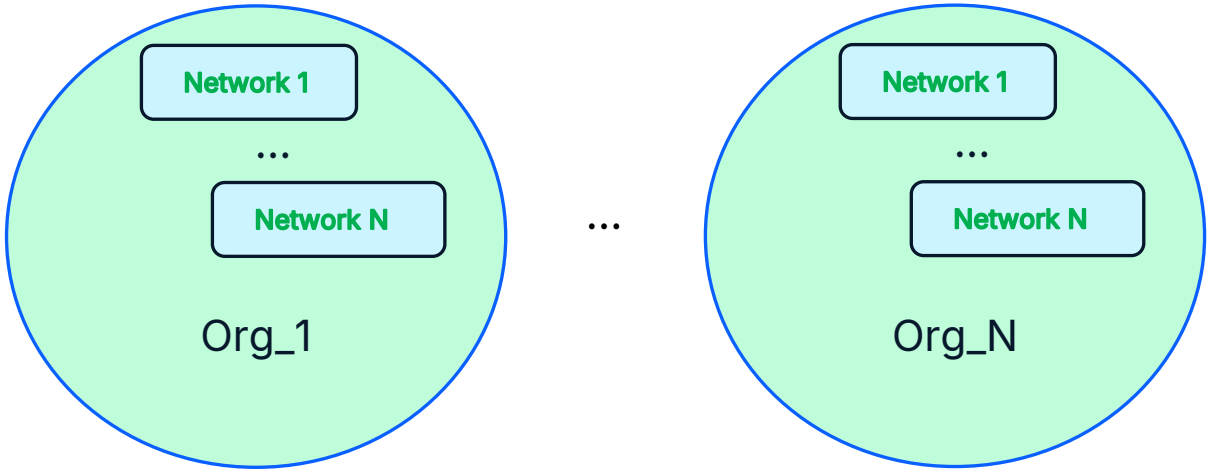
Large Site

Medium Site

Small Site



Very Small



Devices per Organization:

- 35,000

Devices per Network (standalone and combined):

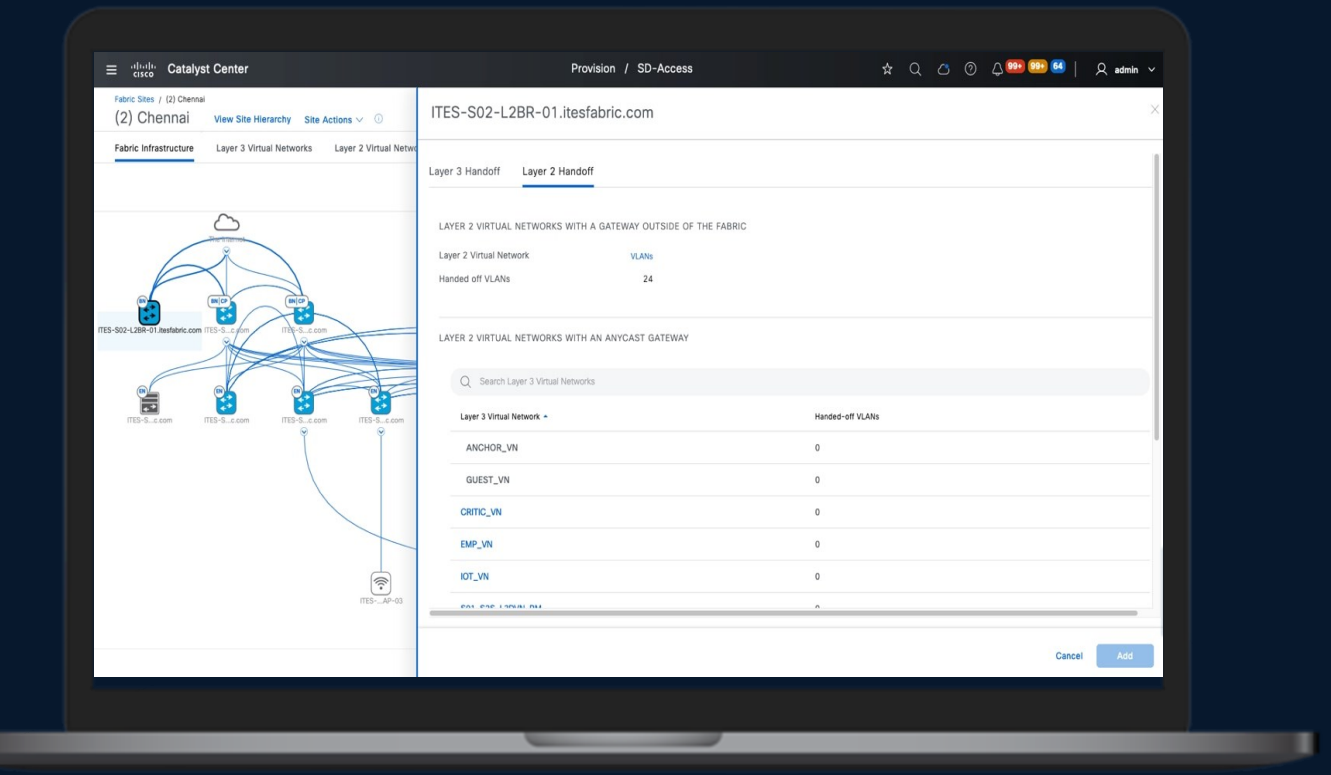
- 5,000

	Total Devices	Wireless APs	Wired Switches	MT	MV	MX	MG	CG	WLC
Per Network	5,000	5,000	5,000	1,700	1,000	2	4	2	2

documentation.meraki.com/Platform_Management/Dashboard_Administration/Design_and_Configure/Architectures_and_Best_Practices/Cisco_Meraki_Best_Practice_Design/Meraki_Cloud_Sizing_and_Scaling_Considerations_and_Best_Practices#Device_Limits

High-scale On-Premises Campus Fabric

Fabric Orchestration from Catalyst Center (or Global Overview)



On-Premises Fabric Value

Appliance Scalability

Build and manage large sites from an intuitive on-premises platform

Maximum Integration

Seamlessly integrate multiple Clusters with Cisco ISE, Thousand Eyes, Spaces and more

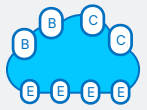
Proven Maturity

Supports 5500+ deployments, across 2900+ customers, with an average 40K+ endpoints

Building Blocks – LAN Management

Definitions, Characteristics and Variations

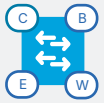
On-Prem Automation & Analytics



Large Site

Medium Site

Small Site



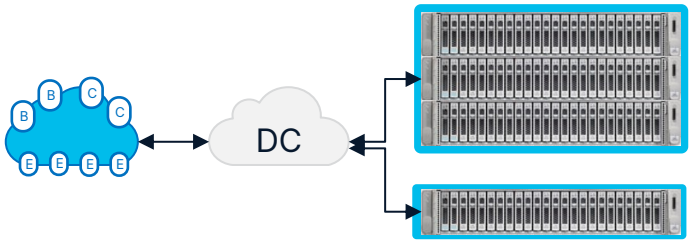
Very Small

Large

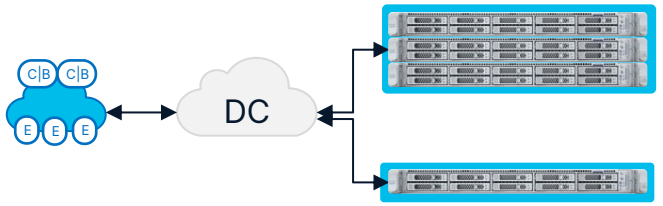
Medium

Small | Small | Small

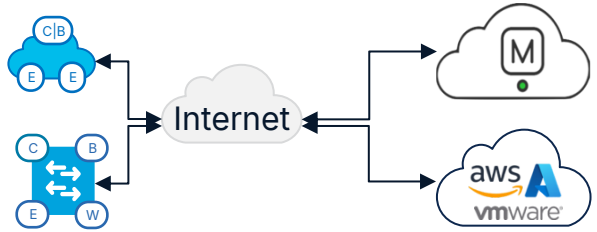
XS | XS | XS | XS | XS



- Large Campus + On-Premises
- Total active Endpoints ≤ 250K
- Total Fabric Devices ≤ 10K
- Total Fabric Sites ≤ 5K
- Dedicated Appliances (DC) + HA
  - HW-APL-XL (x3)
  - RTT Latency ≤ 200ms
- Local RBAC for DevOps & SecOps



- Medium Campus + On-Premises
- Total active Endpoints ≤ 100K
- Total Fabric Devices ≤ 5K
- Total Fabric Sites ≤ 2K
- Dedicated Appliances (DC) + HA
  - HW-APL-L (x3)
  - RTT Latency ≤ 200ms
- Local RBAC for DevOps & SecOps

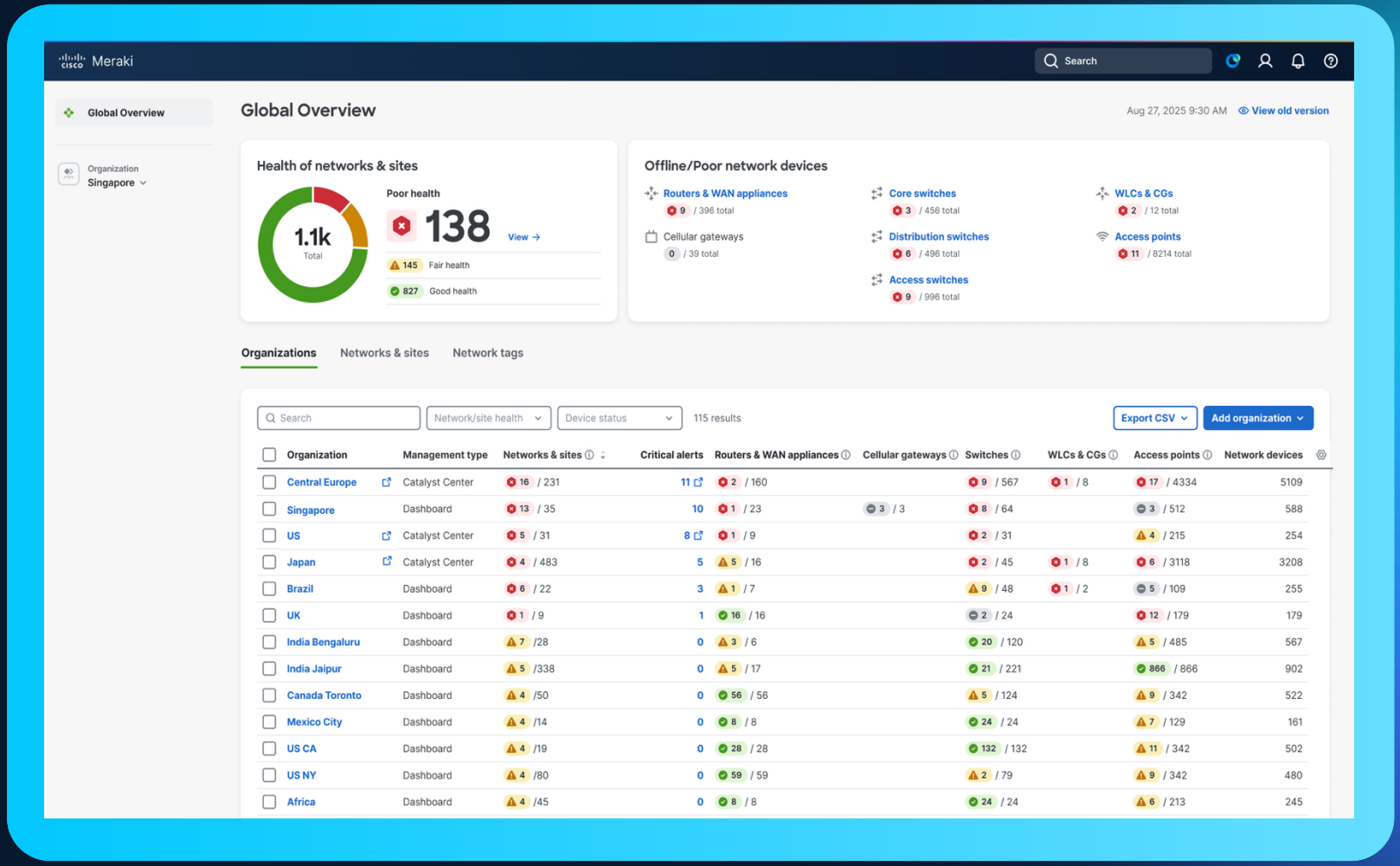


- Small Branch + Cloud
- Total active Endpoints ≤ 25K
- Total Fabric Devices ≤ 1K
- Total Fabric Sites ≤ 1K
- SaaS (or IaaS VA) + HA
  - RTT Latency ≤ 500ms
- Global RBAC for DevOps & SecOps

Global Overview

A single cloud experience integrating Meraki dashboard and multiple Catalyst Centers

- Simplify hybrid operations - global view across Meraki and Catalyst Center
- Resolve issues faster - network, sites, and device alerts in one view
- Troubleshoot seamlessly - secure SSO, no re-authentication



AgenticOps

The New Standard for IT Operations

Cut MTTR to near seconds with AI-driven root cause and resolution.

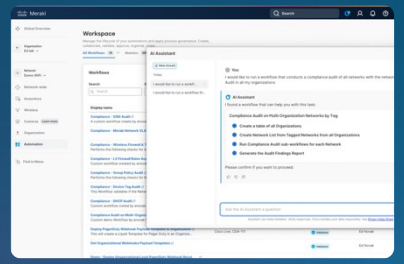
Catch critical issues early with AI that sees across the stack.

Operate at scale with lean teams and built-in AI expertise.

Troubleshoot faster together with shared context across teams.

Agentic Workflows (GA)

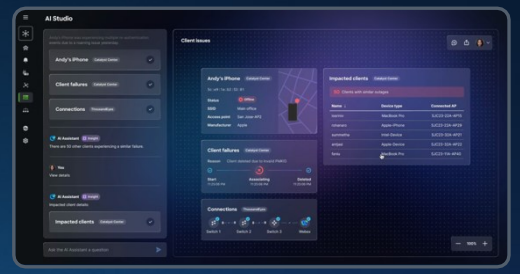
AVAILABLE NOW



AI Assistant

Accelerate network operations

ALPHA



AI Canvas

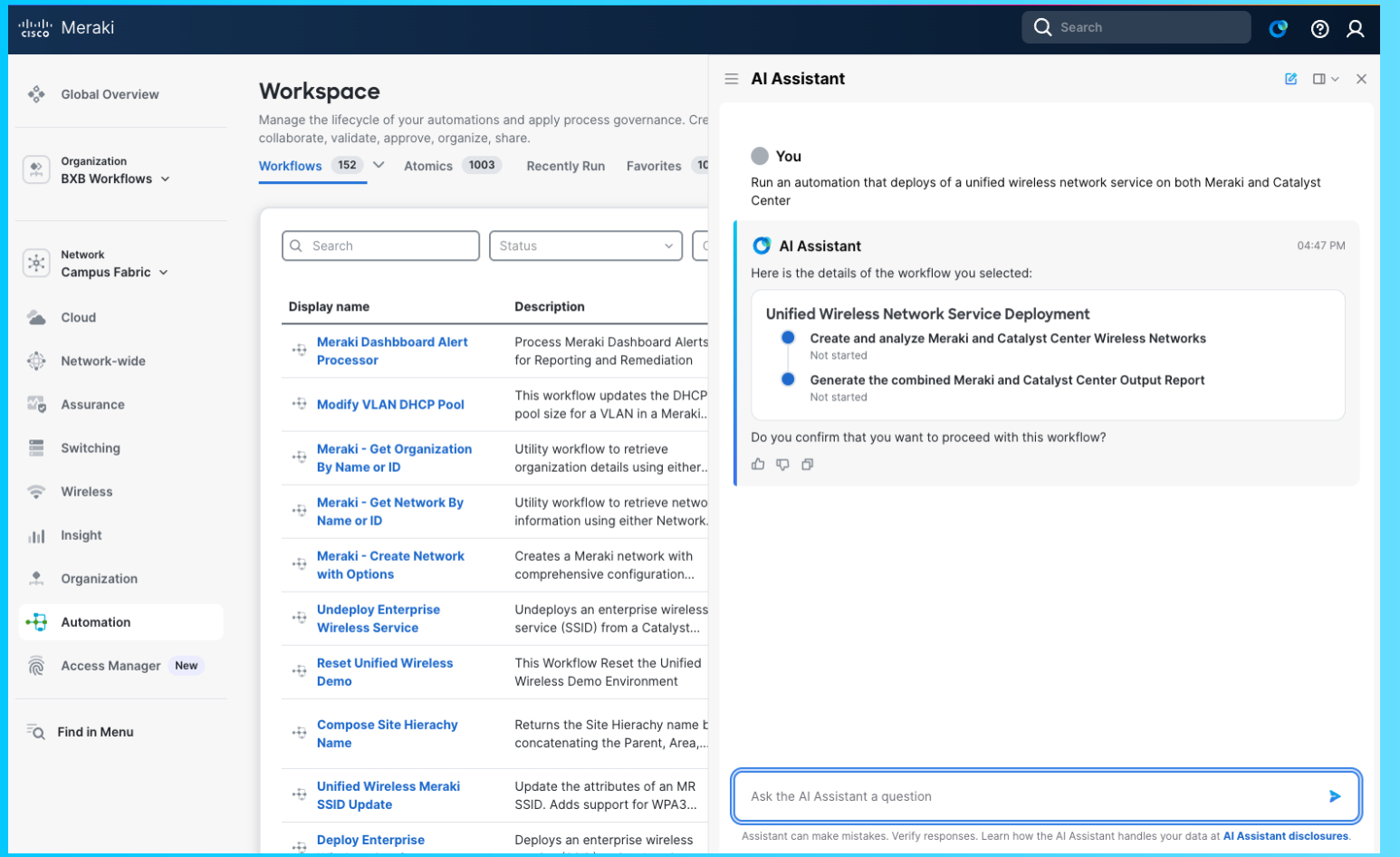
Cross-domain collaborative troubleshooting

Powered by Deep Network Model

Agentic Workflows

Agentic automation across cloud and on-prem deployments

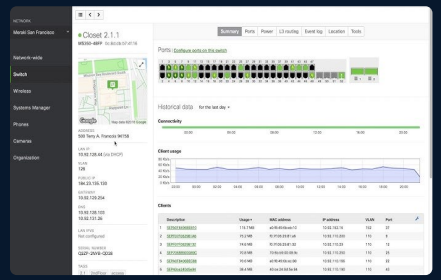
- AI-powered automation natively in the Meraki dashboard
- Leverage built-in AI Assistant integration for agentic operations
- Automate workflows across Meraki, Catalyst Center, Catalyst SD-WAN Manager, ISE, Nexus, and more



Management Type – Journey Map

Start from your Management or Operational model

Cloud Managed



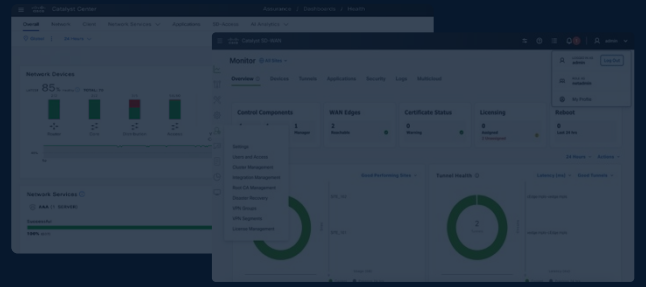
4 **Meraki Dashboard**
Cloud-Managed LAN, WLAN & WAN

3 **Access-Manager + SCC**
Cloud-managed NAC + Group Policy

2 **Cloud Fabric & SD-WAN**
Cloud-automated Underlay & Overlay

1 **Meraki for C9K & C8K**
Cloud Switching, Wireless & Routing

On-Premises



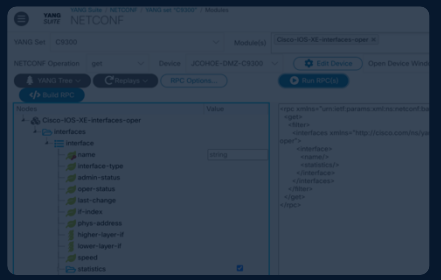
4 **Cat Center & SDWAN Mgr**
On-Premises LAN, WLAN & WAN

3 **Cisco ISE + FMC**
On-Premises NAC + Group Policy

2 **SD-Access & SD-WAN**
Premises-automated Underlay & Overlay

1 **CC for C9K & SDW for C8K**
Premises Switching, Wireless & Routing

Programmable (DIY)



4 **Programmable (DIY)**
Customer-managed APIs or CLIs

3 **RADIUS + CTS + SCC API**
Customer-managed NAC + Group Policy

2 **Custom Fabric & WAN**
Customer-managed Underlay & Overlay

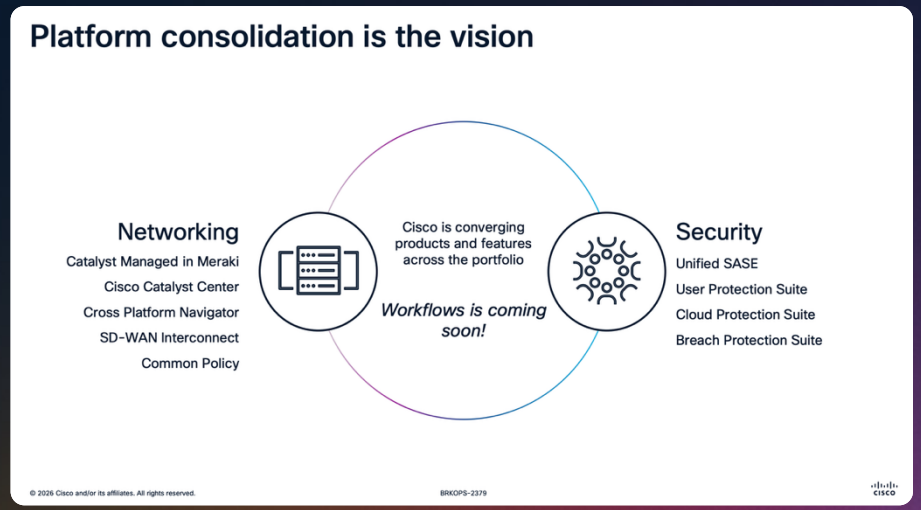
1 **Programmable C9K & C8K**
Custom Switching, Wireless & Routing

NOTE: Slide is animated

Cisco C9K Unified Management Sessions

BRKOPS-2379

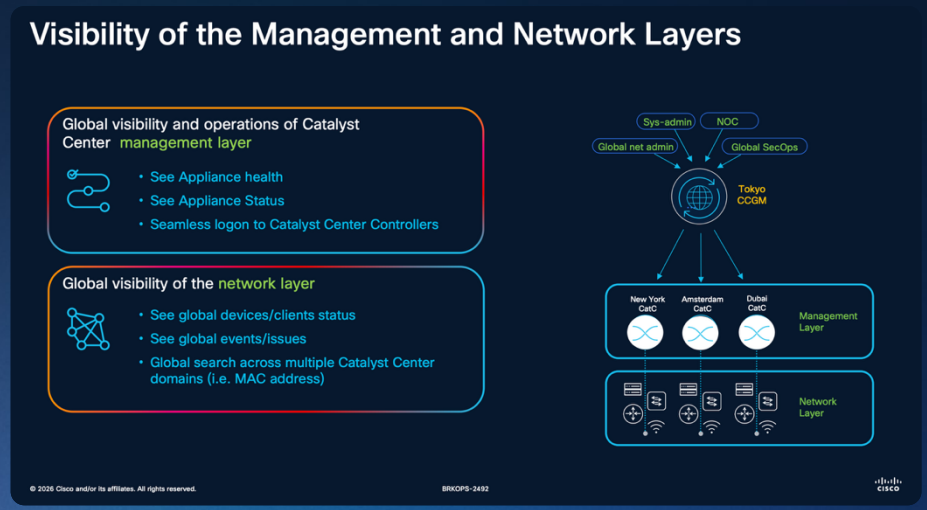
Automate Cisco Catalyst Center with Cisco Workflows



This session provides an in-depth overview of the platform, demonstrating its capabilities with on-prem management platforms and showcasing complete network automation. It highlights the benefits of a collaborative DevOps approach in overcoming deployment challenges.

BRKOPS-2492

Deploy Unified Global Management for Catalyst Centers and Meraki Organizations



This session explores how to bridge these environments using Catalyst Center Global Manager (CCGM) and Meraki Dashboard's Global Overview to monitor your entire Campus footprint, including both Meraki Organizations and Catalyst Centers.

3

Management & Assurance

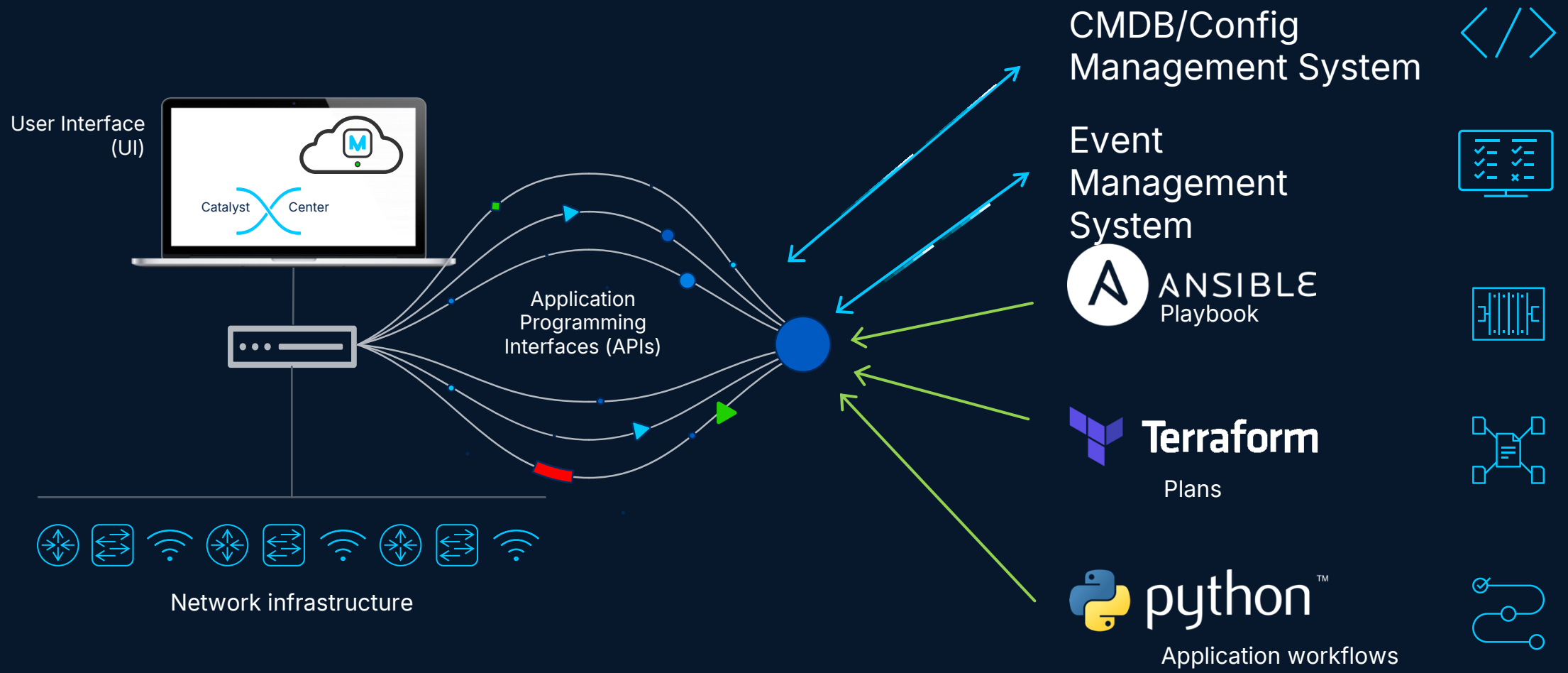
3rd Party tool / DIY With Programmability

```
terraform apply

An execution plan has been generated and is shown below.
Resource actions are indicated with the following symbols:
  + create

Terraform will perform the following actions:

  # dna_site.area will be created
  + resource "dna_site" "area" {
      + id           = (known after apply)
      + last_updated = (known after apply)

      + item {
          + id          = (known after apply)
          + name        = "Terraform"
          + parent_name = "Global"
          + type        = "area"
        }
    }

  # dna_site.building_10 will be created
  + resource "dna_site" "building_10" {
      + id           = (known after apply)
      + last_updated = (known after apply)

      + item {
          + address     = "Cisco - Building 10, 300 E Tasman Dr, San Jose, California 95134, United
States"
          + id          = (known after apply)
          + name        = "Building_10"
          + parent_name = (known after apply)
          + type        = "building"
        }
    }

  # dna_site.building_10_floor1 will be created
  + resource "dna_site" "building_10_floor1" {
      + id           = (known after apply)
      + last_updated = (known after apply)

      + item {
          + height      = 100
          + id          = (known after apply)
          + length      = 100
          + name        = "Floor 1"
          + parent_name = (known after apply)
          + rf_model    = "Cubes And Walled Offices"
          + type        = "floor"
          + width       = 100
        }
    }

Plan: 3 to add, 0 to change, 0 to destroy.

Do you want to perform these actions?
  Terraform will perform the actions described above.
  Only 'yes' will be accepted to approve.

  Enter a value:
```

github.com/cisco-en-programmability/terraform-provider-catalystcenter

Scaling and simplifying APIs with Infra-as-Code tools

From Configuration Management to Orchestration



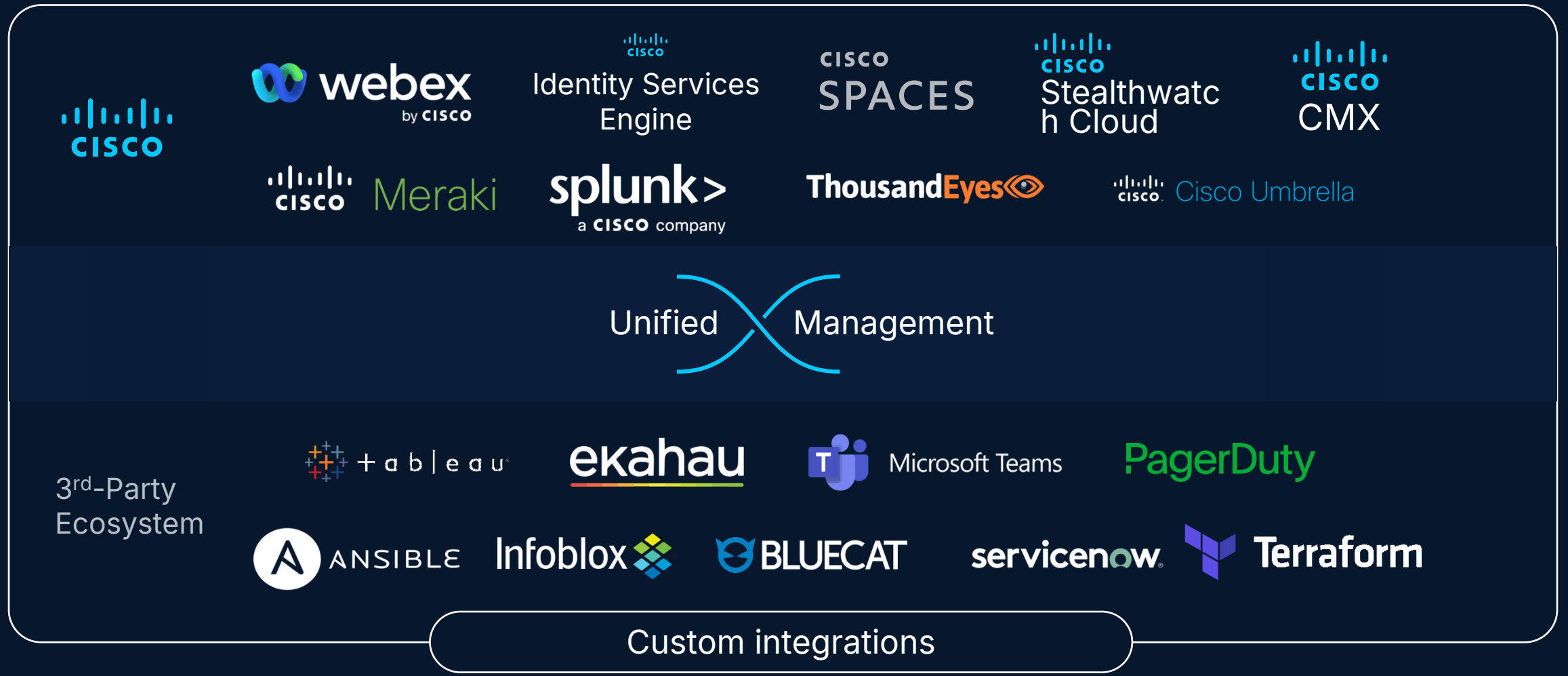
Extended Integrations

5 **Extended Integrations** (Splunk, TE, etc.)
Sharing device & flow analytics with external management tools

www.cisco.com/site/us/en/partners/360-partner-program

Extended Integrations

Cisco & Partner integration services for orchestration, observability & security



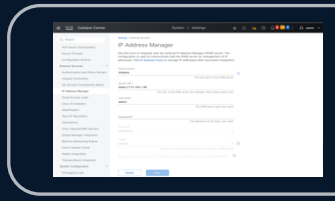
Extended Integrations

Key Concepts & Design Considerations (Why it matters)

1 Sites, Maps & Locations

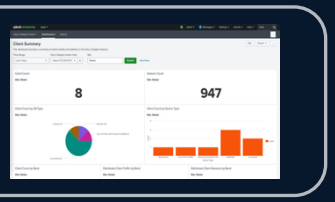
- Cisco Spaces
- Ekahau

2 DNS, DHCP & IPAM



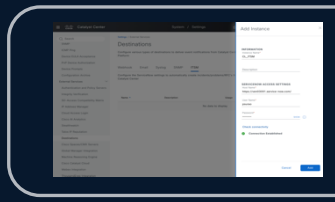
- Infoblox
- Bluecat
- NS1

3 Telemetry & Data Management



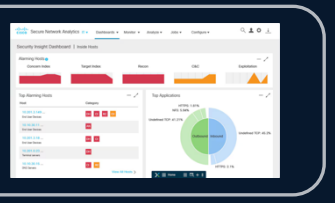
- Splunk (Telemetry)
- Cloud Analytics

4 ITSM, CMDB & SEIM



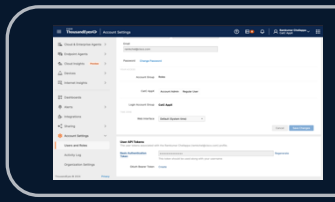
- ServiceNow
- Splunk (SEIM)

5 Endpoint & Policy Analytics



- Extended Detect & Response (XDR)
- Cyber Vision

6 Application & Path Analytics



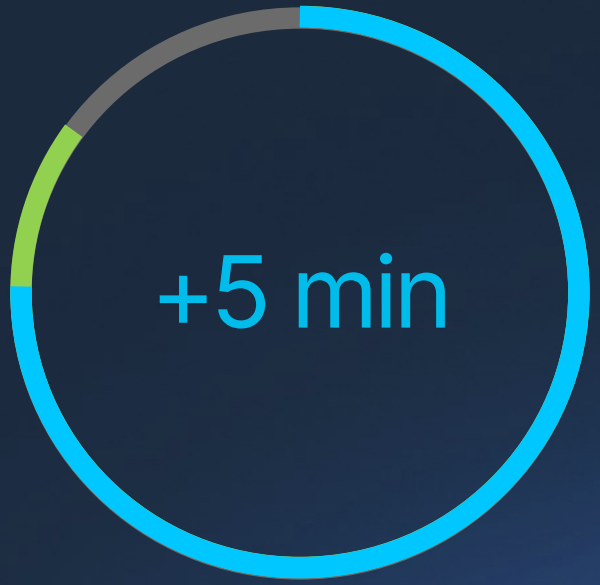
- ThousandEyes
- Appx (MS Teams)
- LiveAction

Cisco + Splunk Unique Differentiators for Secure Networking

How This Shows Up For Customers

Correlate Network, Apps + Infrastructure	Reduce Alert Noise	**Accelerate Detailed Root Cause Analysis**	Service Issues In External Networks
Holistic Visibility & Business Prioritization	**Rapid Reduction and Prioritization**	**Rapid Root Cause Identification**	External Network Optimization
• Gain holistic visibility to prioritize incidents based on business impact and eliminate blind spots	• Reduce alert noise by grouping related alerts and prioritize incidents based on business impact for faster resolution	• Quickly identify network-related application issues to reduce troubleshooting and escalations	• Manage service dependencies and optimize routing using Splunk and Cisco performance data

Cisco Validated Design



Validated Testing & Documentation

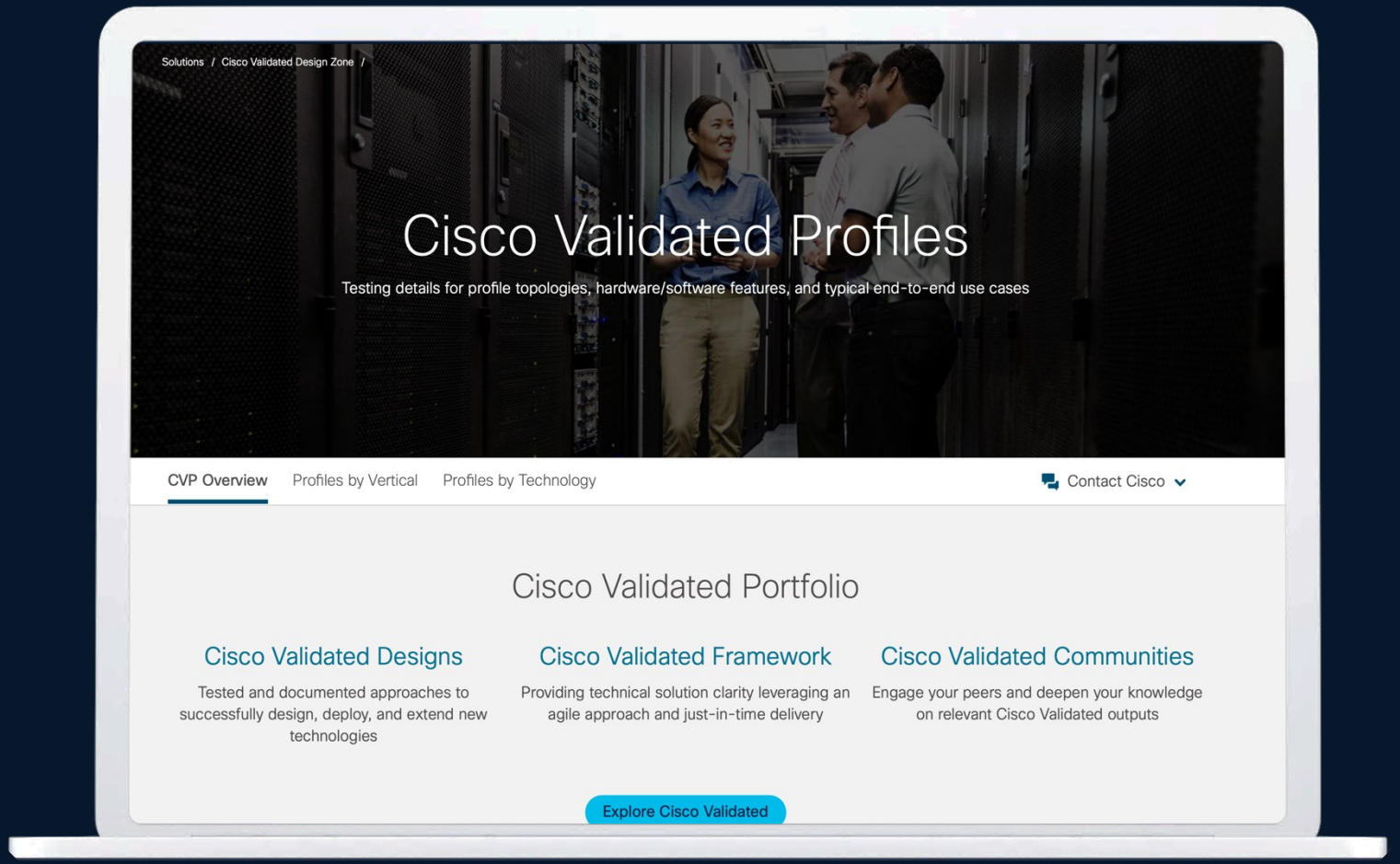
Is this design validated?

What resources are available?

How do I use this design?

Deploy consistent designs using CVPs & CVDs

- Based on Cisco Validated “best practices”
- Industry Vertical focus
- Release over release validation of use-cases
- Use case mapping to Business needs



www.cisco.com/site/us/en/solutions/cisco-validated/

High-Level End-to-End ‘Architecture Guide’

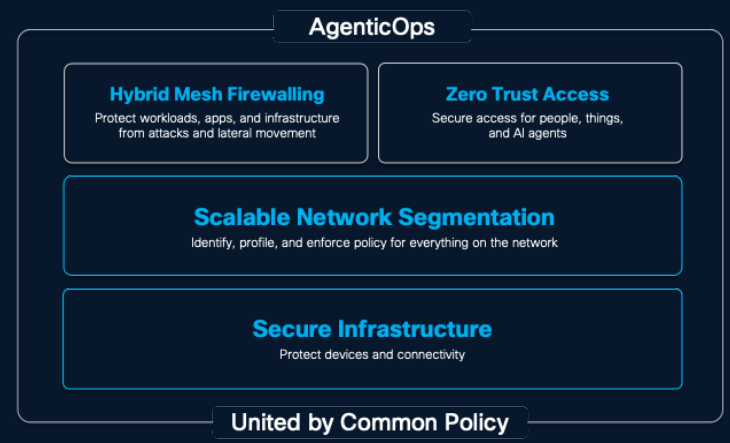
1

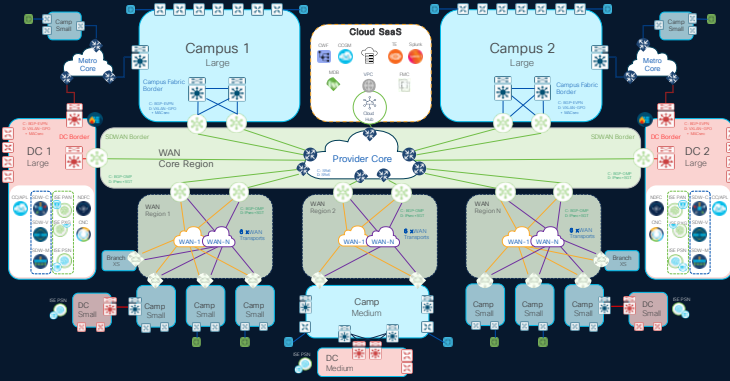
High-level ‘Architecture Guide’ CVD document

- Target Audience: CxOs & Generalists
- Relatively short & summary format
- Focuses on the end-to-end architecture building blocks
- Describes how SNRA achieves the Customer Outcomes

Key Elements

- End-to-End Architecture Reference Diagrams
- Describes using the SNRA Reference Model
- Describes the characteristics of SNRA T-shirt Sizing
- Links audience to Deployment Guides, etc.





Low-Level Per-Type SNRA ‘Deployment Guide’

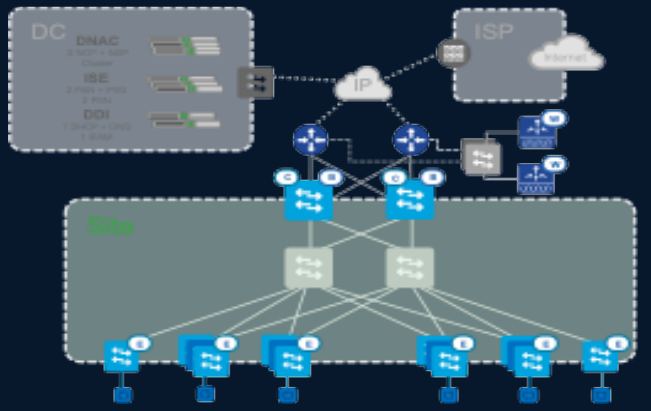
CISCO VALIDATED DESIGN

3 Low-level ‘Deployment Guide’ CVD documents

- Target Audience: Architects & Specialist
- Longer, detailed & prescriptive format
- Focuses on the specific Domains & PINs
- Describes how to design & build each Deployment Type

Key Elements

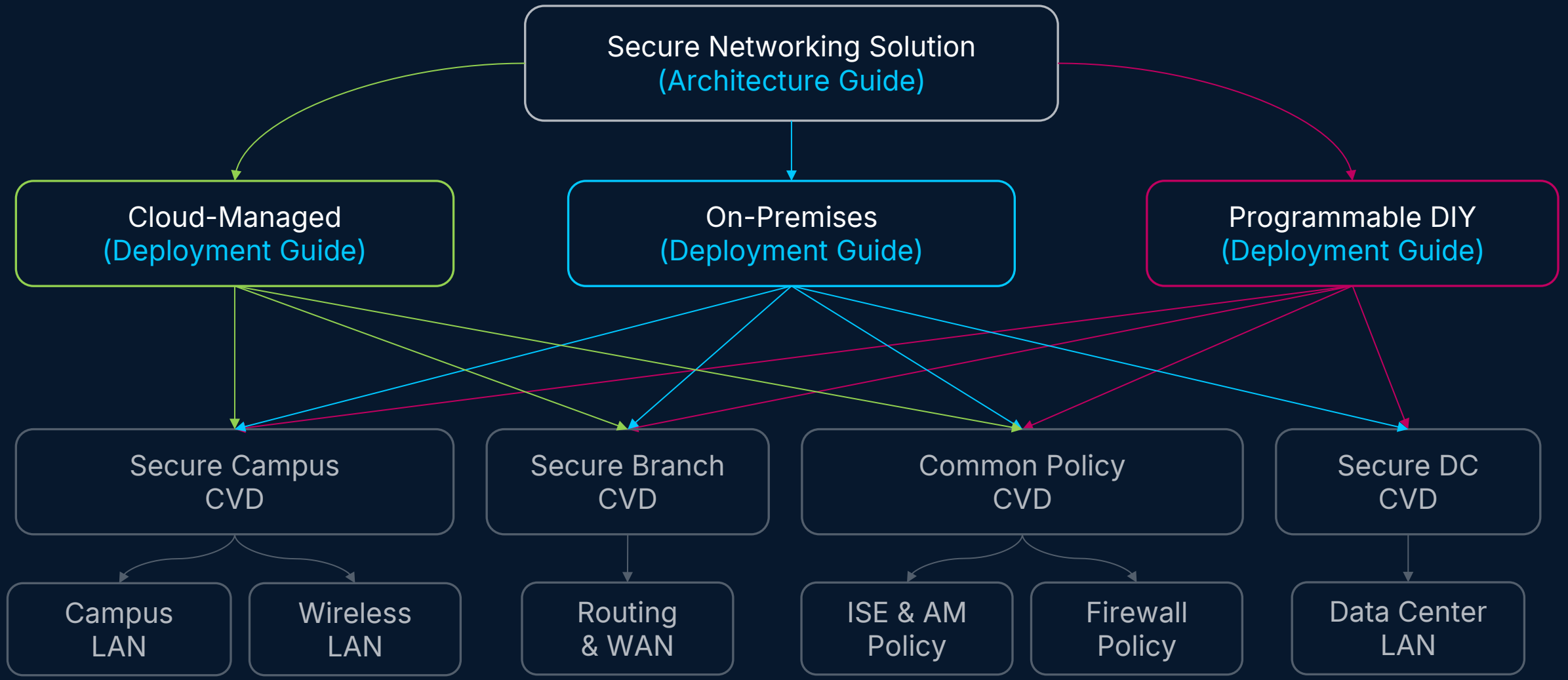
- Low-level Domain & PIN Topology Diagrams
- Details the network deployment steps & procedures
- Demonstrates a series of tests to validate the outcomes
- Links to Config Guides & Release Notes, etc.



Focus for CLUS (June 2026) is: Medium-Sized Cloud-Managed

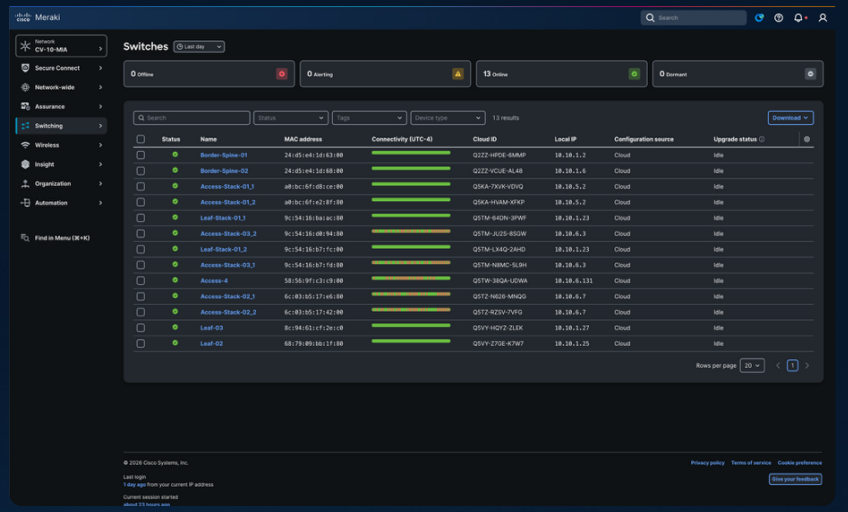
Secure Networking Architecture

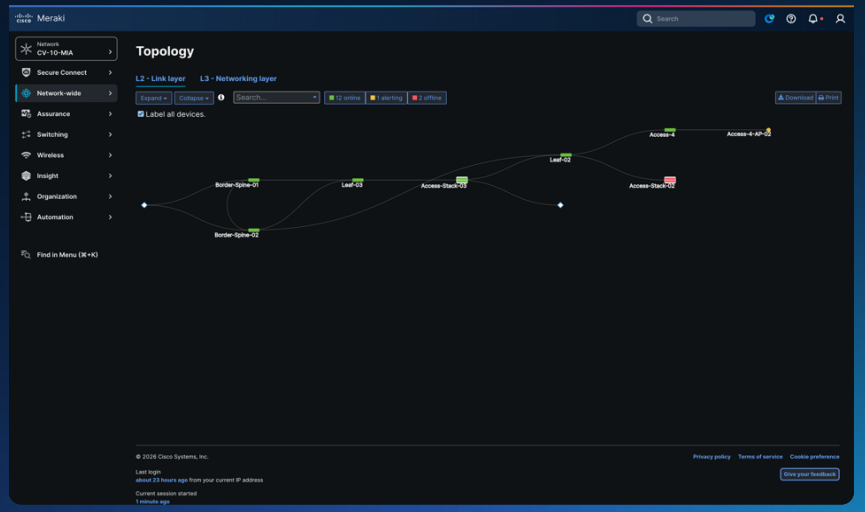
Multiple levels of interrelated documentation

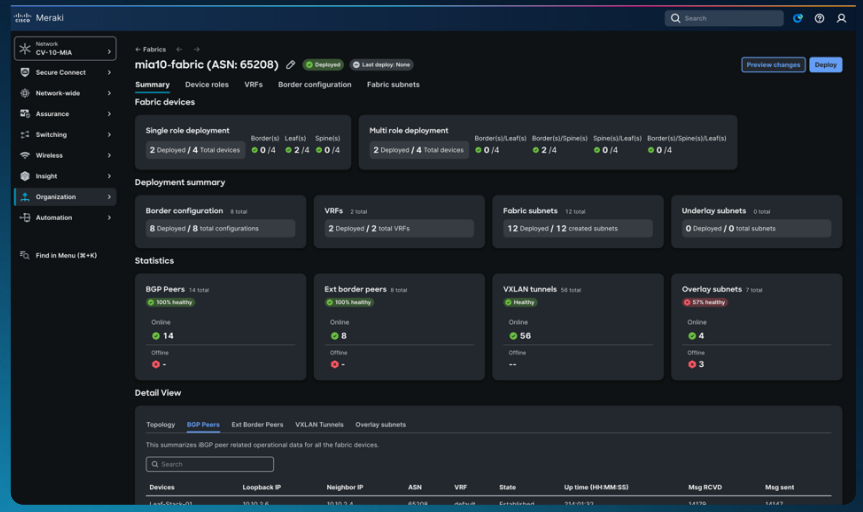


SNRA CVD Test Validation

Cloud-Managed Campus Fabric Test Topology







Next Steps

Next Steps & Call to Action

What's Next?

Key Points

Call to Action

Call to Action

Implementing SNRA – Layer by Layer

5 Extended Integrations

4 Unified Mgt & Agentic Ops

3 Zero Trust & Mesh Firewall

2 Scalable Segmentation

1 Secure Infrastructure

CHECKLIST

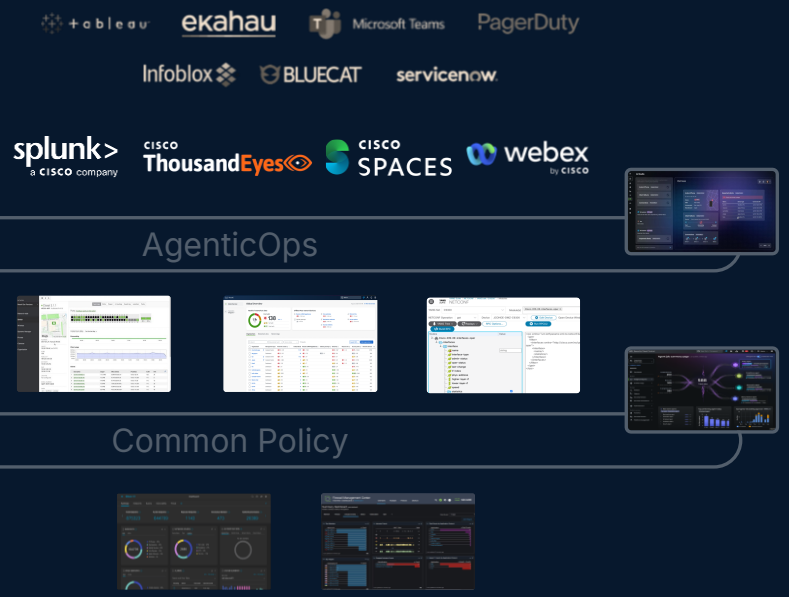
Increase your Observability & Assurance
- *leverage the robust ecosystem of Cisco and third-party tools and data-sources to increase observability and integrate multiple support systems.*

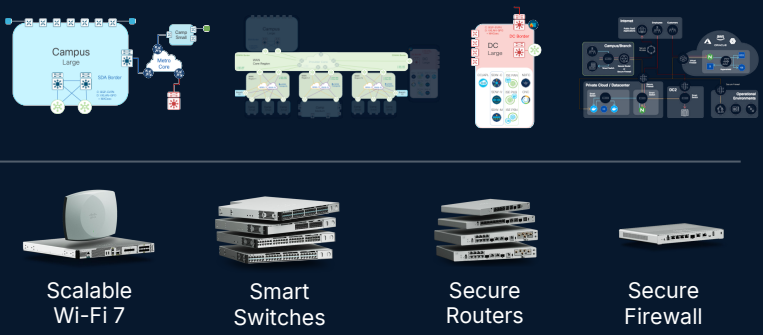
Simplify Ops with Unified Tools & AI
- *consistently deploy fabrics globally, leveraging a unified management experience, using model-driven programmability and Agentic Ops.*

Embrace Cisco ZTA & Common Policy
- *employ easy endpoint identification & authentication, integration of hybrid mesh firewall, with end-to-end identity-based common policy.*

Migrate Traditional to Fabric Overlay
- *leverage network automation to simplify migration, implementing consistent a design, to easily transport identity-based segments.*

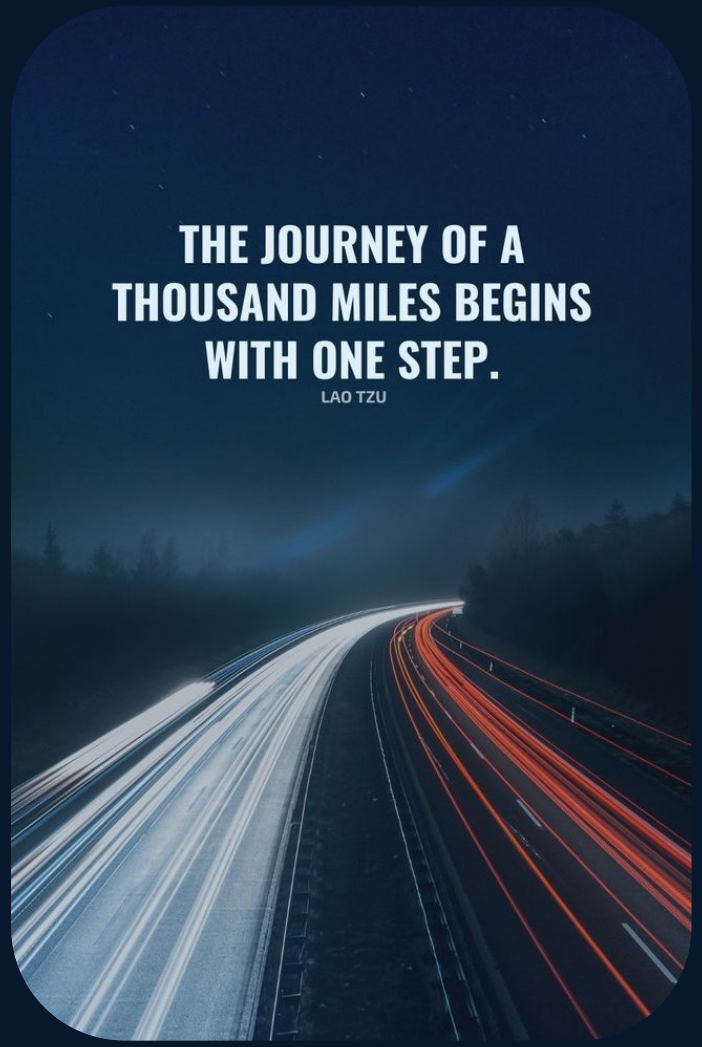
Refresh to latest Cisco Secure products
- *install scalable devices, with security fused in, using Unified Hardware, Unified Software, Unified Licensing & Unified Support.*





Secure Networking v1.0

RECAP



This is our first cross-domain and end-to-end Cisco reference architecture in the modern era!

- Version 1.0 delivers 'Secure Networking' outcomes
  - Many Domains, PINs, Products & Protocols
  - Based on the currently available Products
  - There are some challenges, limits and gaps
- We will continue to evolve into the future* (v2.0+)

SNRA v1.0 Versions:

- IOSXE 26.1.(latest)
- Meraki Q2CY26 (latest)
- Catalyst Center 3.2.1.(latest)
- SDWAN Manager 20.18.2.(latest)
- ISE 3.5.(latest)
- TE Q2CY26 (latest)
- SNA 7.6.(latest)
- FMC 10.0.(latest)
- SCC Q2CY26 (latest)

CISCO VALIDATED DESIGN

Where are we going?

Cisco Cloud Control

New @ CiscoLive US 2026

Cloud Control

The future of unified management starts here

20 : 15 : 25 : 42

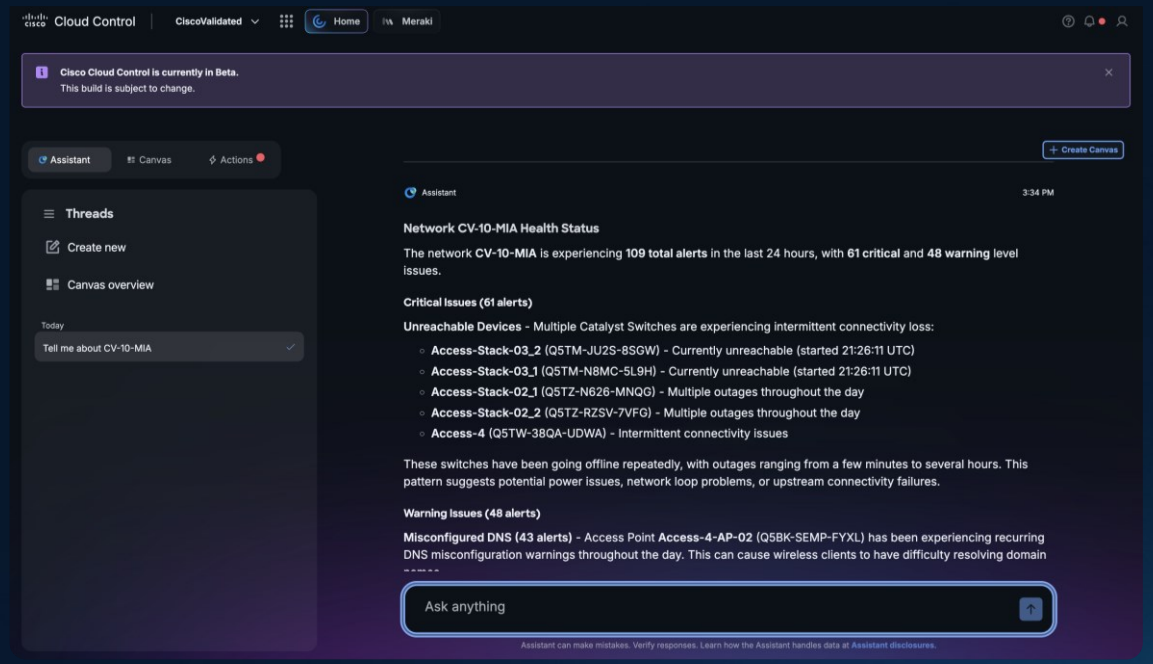
DAYS HOURS MINUTES SECONDS

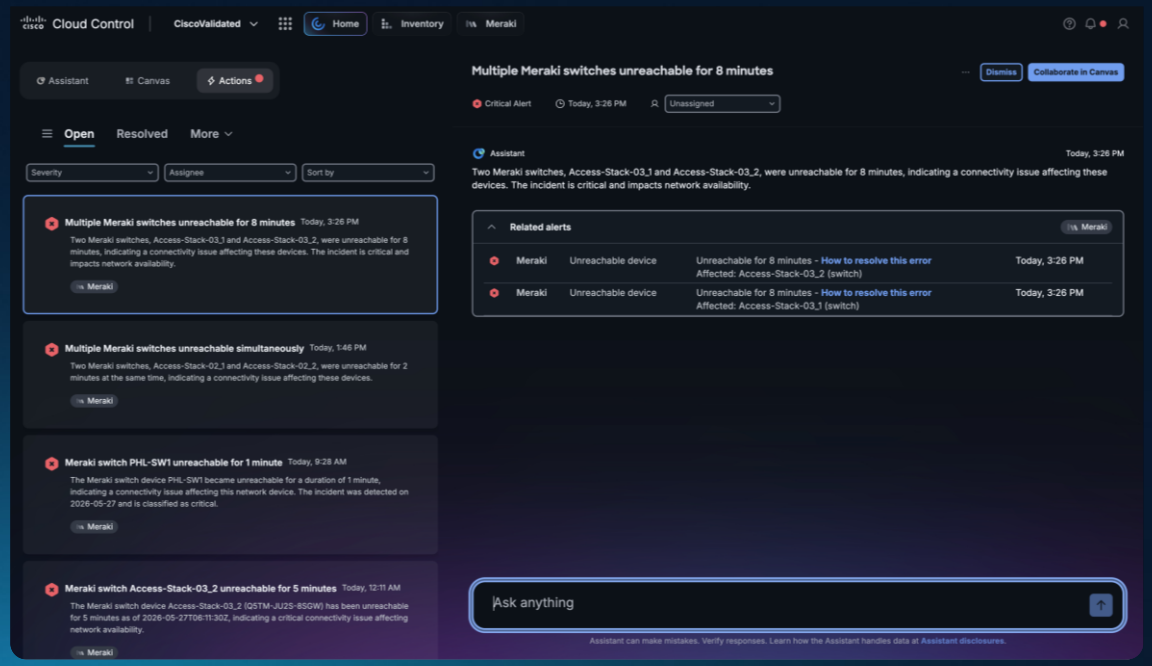
Redefining how you manage your Cisco products and beyond

Cisco Live 2026 · Las Vegas · May 31 – June 4

SNRA CVD Test Validation

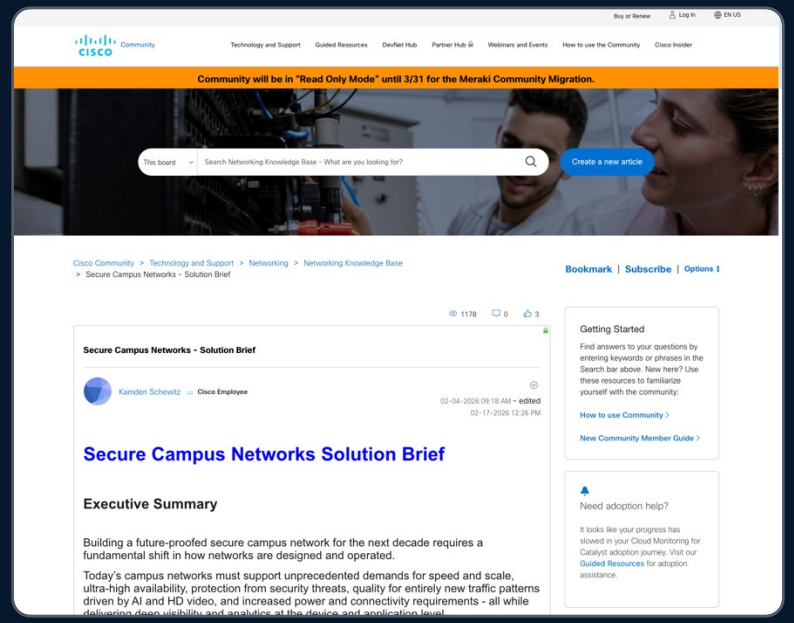
Cloud-Managed Campus Fabric – with Cisco Cloud Control





Secure Networking Resources

Start your Secure Network Reference Architecture



Public SNRA References

- Secure Networking Overview
- Secure Campus & Branch Networking
- Secure Campus Networks – Solution Brief
- Modernizing Campus Networks with Fabric-Architecture
- Secure Network Architecture to accelerate workplace AI transformation

Published

SNRA Cisco Validated Designs

- Secure Network Reference Architecture – End-to-End Architecture Guide

NEW

- Secure Network Reference Architecture – Cloud-managed Design Guide
- Secure Network Reference Architecture – On-Premises Design Guide
- Secure Network Reference Architecture – Programmable Design Guide

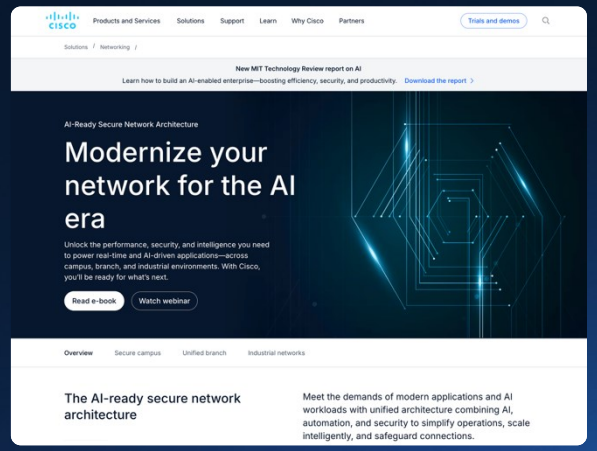
June 2026

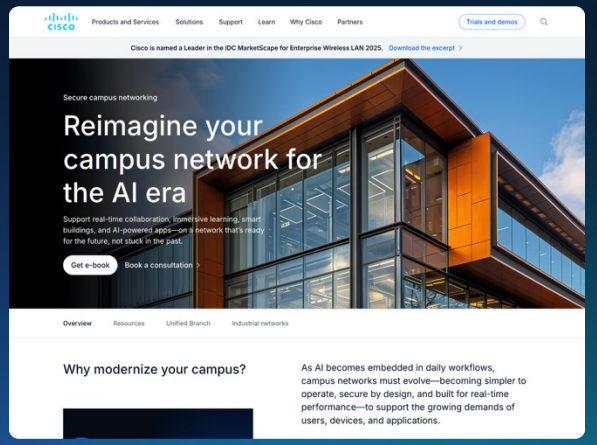
Existing Cisco Validated Designs

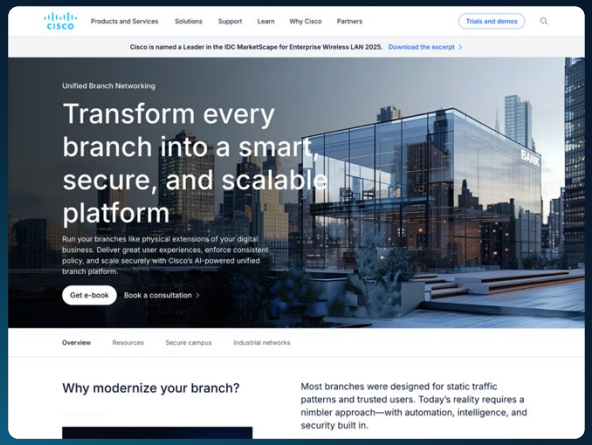
- Cisco Cloud Fabric Validated Case Study — NEW
- Cisco SD-Access Design Guide — Updated
- Cisco Unified Branch Design Guide — Updated
- Cisco Common Policy Integration Guide — Updated

Secure Networking on Cisco.com

www.cisco.com/site/us/en/solutions/transform-infrastructure/secure-networking-overview.html







www.cisco.com/site/us/en/solutions/networking/campus-branch-networking/index.html

Your Journey to Modernization

Deploy AI-ready Hardware: with security fused into the network

+

Secure the Campus & Branch: with secure access & common policy

+

Simplify NetOps & SecOps: with Unified Management & Agentic Ops

Cisco Secure Networking

Complete your session evaluations

Complete a minimum of 4 session surveys and the Overall Event Survey to be entered in a drawing to win 1 of 5 full conference passes to Cisco Live 2027.

Earn 100 points per survey completed and compete on the Cisco Live Challenge leaderboard.

Level up and earn exclusive prizes!

Complete your surveys in the Cisco Live mobile app.

Continue your education

Visit the Cisco Showcase for related demos

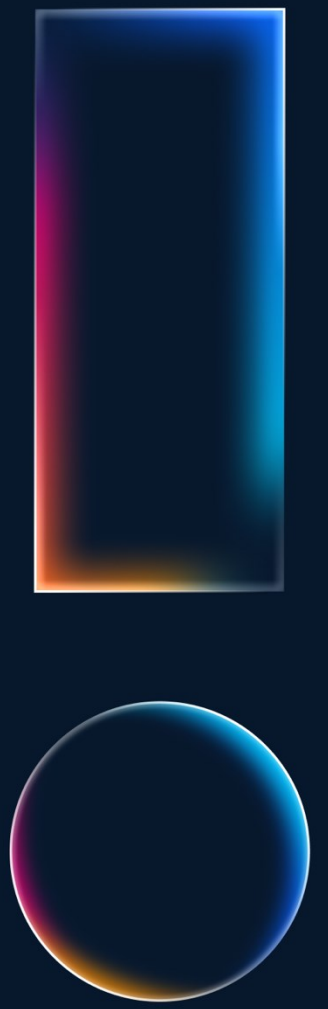
Book your one-on-one Meet the Engineer meeting

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

cisco Live !

Thank you




CISCO