CISCO Engage | Tech Day Milwaukee

Cisco Zero Trust Segmentation

Corey Moomey – Principal Advisor

Steven Gerhart – Solutions Architect

Date placeholder

Agenda

1. Cisco’s Architectural Shift
2. Ut laoreet dolore magna
3. Road To Segmentation
4. Isolation and Control
5. Multi-Domain Segmentation
6. Best Practices

The Industry Reality – Where We are Focused

77%
report too many security solutions

75%
considering vendor consolidation

85%
of intrusions are malware-free

51 sec
fastest breakout time observed

50%
unknown devices on net

Sources: Cisco 2025 Cybersecurity Readiness Index | CrowdStrike 2025 Global Threat Report | Gartner 2024

The common thread in recent breaches — Change Healthcare, MOVEit, Okta, MGM Resorts is not a failure of detection. It's a **failure of least-privilege enforcement** at the access layer. Attackers gain initial access and move laterally because segmentation is absent or IP-based.

> **The question is not whether your perimeter will be breached — it's whether your architecture limits the blast radius when it is.**

The Policy Complexity Problem

Enterprise security architectures have been assembled from discrete, domain-specific components — each with its own policy model, management plane, and operational overhead.

The Accumulation Problem

Every new use case — cloud, IoT, remote work, M&A, AI agents — has historically required a new tool, a new policy domain, and a new team. This is how enterprises end up with 50+ security solutions.

The Fragmentation Tax

Each domain defines “policy” differently. A firewall rule ≠ an ACL ≠ a VPC security group ≠ an SSE policy. Same intent, five implementations, five management interfaces.

The Coupling Problem results in OPERATIONAL COMPLEXITY

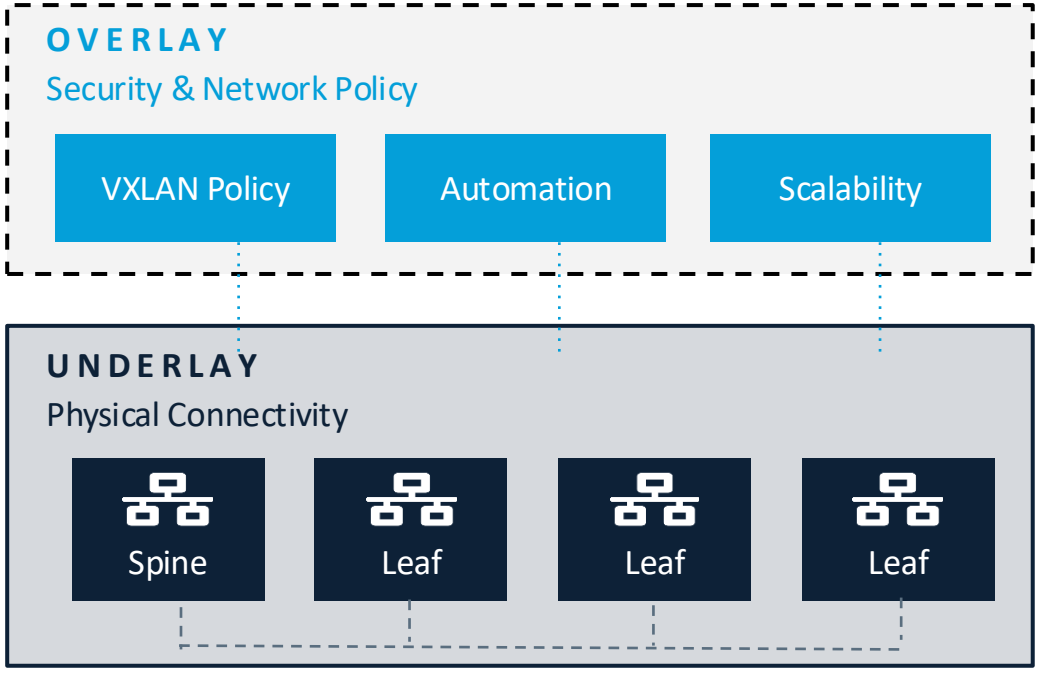
Traditional security methods tightly couple network design to security outcomes. Static and rigid structures are the decades old methodology for segmentation. Traffic routes through firewalls for inspection. The network team can’t optimize topology without breaking security. The security team can’t change policy without a network change. This coupling is the **root cause**.

Building the Security Fabric

Cisco extends the fabric architecture model — proven in data center and campus networking — to unify security policy across every domain. One overlay. One policy. Every enforcement point.

THE FABRIC CONCEPT

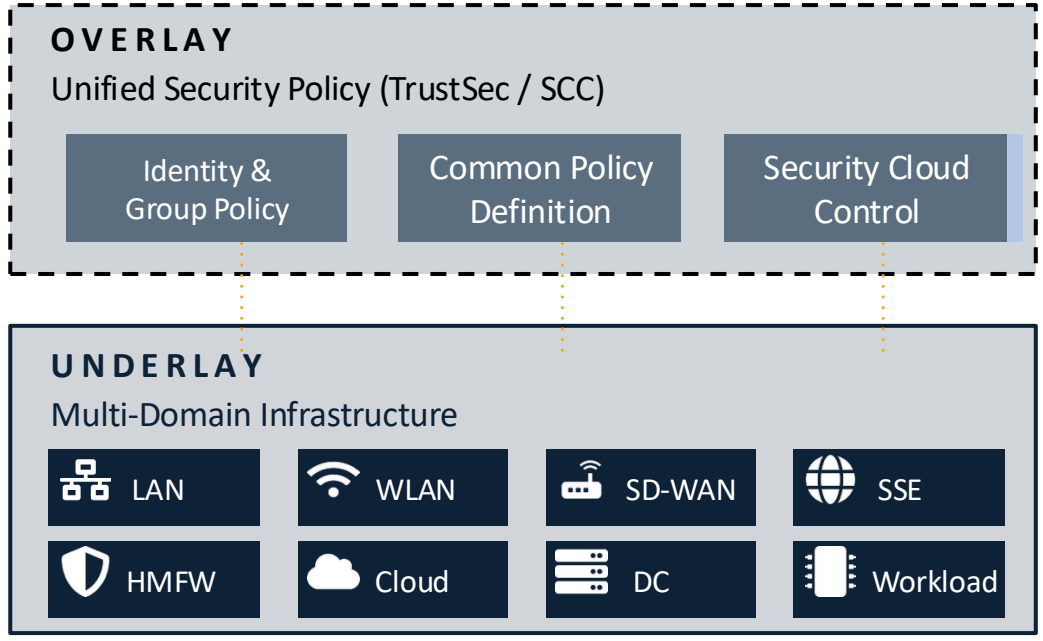
A fabric separates WHAT connects from HOW policy is applied



Data Center Fabric Analogy

CISCO SECURITY FABRIC

Same model, applied to multi-domain security policy



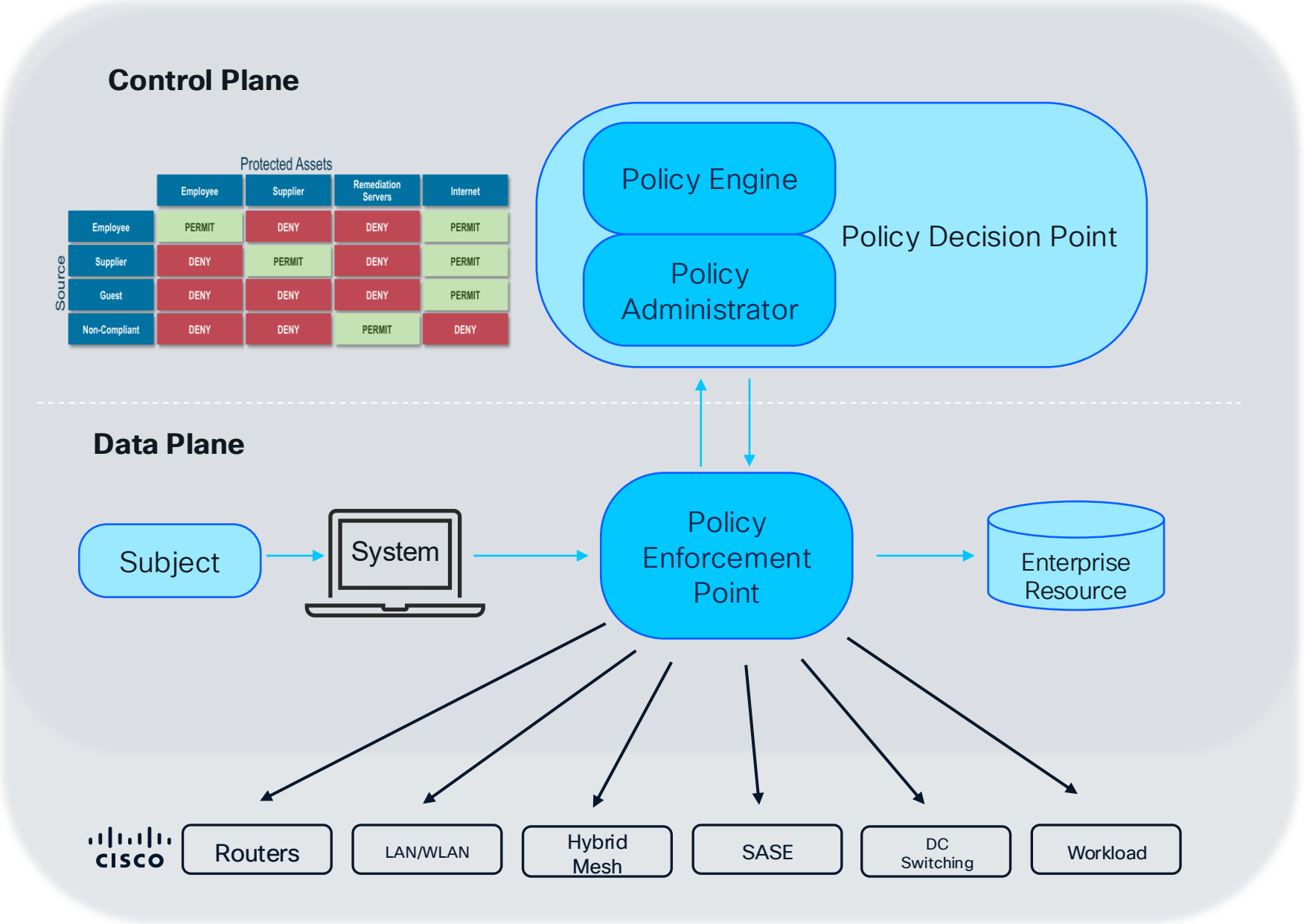
Cisco Multi-Domain Security Fabric

Key Insight: Just as a DC fabric separates connectivity from policy, Cisco's Security Fabric separates network construction from security outcomes — enabling one policy definition expressed across every infrastructure domain.

NIST Zero Trust Framework

Principles:

- Assume Breach
- Least Privilege Construct
- No Policy linked to network location (IP)
- State Tracking



Divorcing Network Construction from Security Outcomes

Your network team builds fast, resilient infrastructure.
Security operates as a fabric on top. Neither team constrains the other.

Traditional: Security-Driven Network

- VLANs/VRFs built for security zones
- Static and Rigid Constructions
- Traffic hairpins through firewalls
- New security zone = new VLAN = network redesign
- Network ops and security ops tightly coupled
- Changes risk both systems simultaneously

Cisco: Security-Abstracted Network

- Network optimized for performance & scale
- Security is an overlay via TrustSec tags
- New use case = new tag assignment, no redesign – Software-Defined
- Network ops and security ops independent
- Hours → minutes for new capability delivery

Key Insight: Security is abstracted from network construction, network team build networks, and security teams apply governing controls

Packet-Centric vs. Connection-Centric Security

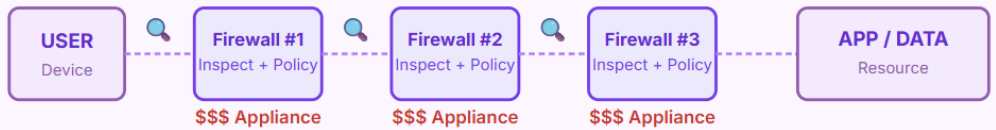
AN ARCHITECTURAL SHIFT TOWARD TRUE ZERO TRUST

CISCO
SECURITY CLOUD

TRADITIONAL MODEL

⚠️ Packet-Centric Security

Palo Alto & legacy firewall model — inspect every packet at every boundary



Repeated inspection required at every network domain boundary

High cost · Manual rule management · Siloed enforcement

- 💸 **High CapEx & OpEx**
  Expensive appliances required at every network boundary
- ⚙️ **Manual, Process-Heavy Operations**
  Firewall rule changes are slow, siloed, and error-prone
- 🎯 **Reactive Security Posture**
  Control applied too late — trust is assumed at the edge
- 🧩 **Disconnected Security Domains**
  OT, IoT, wireless, and cloud each require separate stacks

VS

CISCO MODEL

CISCO PLATFORM

✅ Connection-Centric Security

Authenticate once, assign a TrustSec tag, enforce policy everywhere automatically

One trust decision at the edge — SGT tag carries policy across all domains

Dynamic · Scalable · Pervasive Zero Trust at Scale

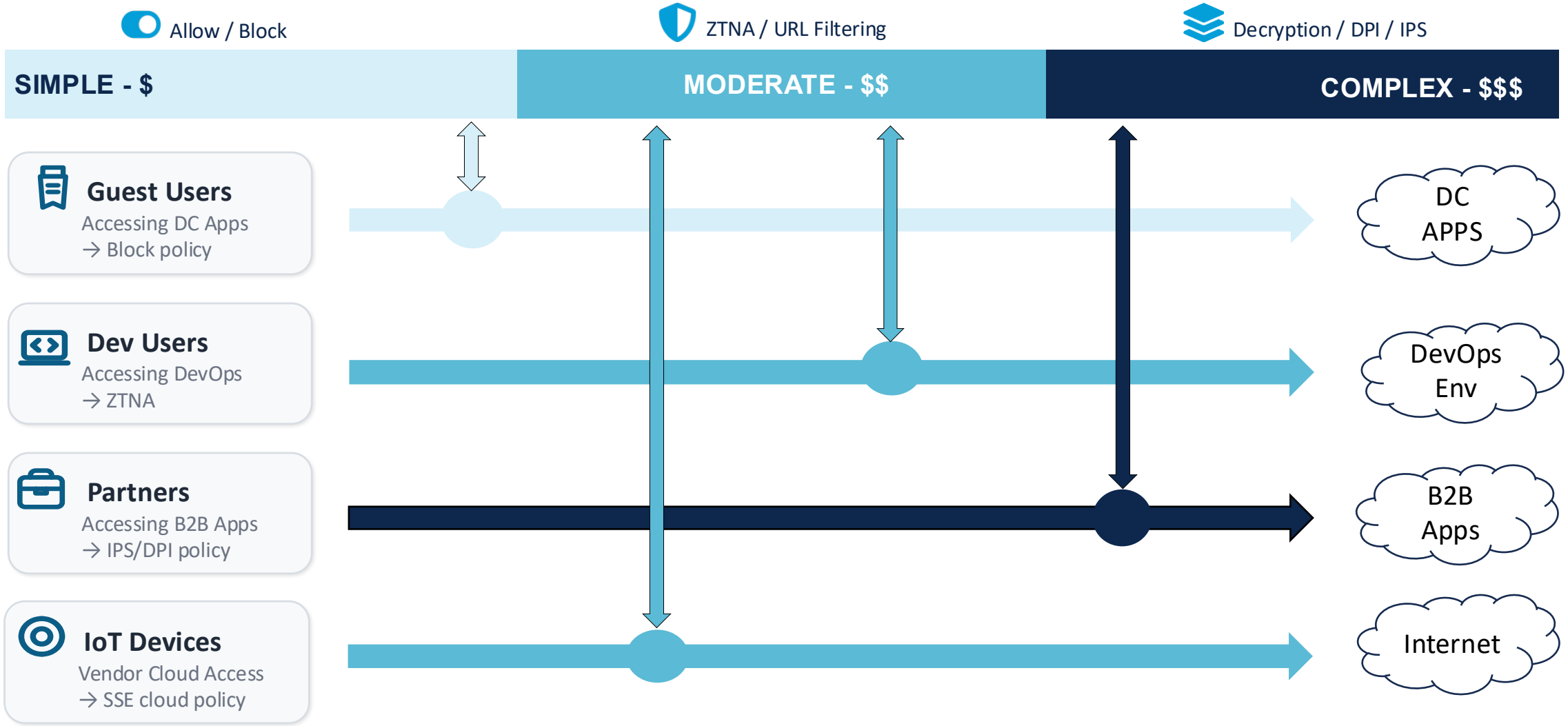
- 💰 **~10x Lower Security Hardware Cost**
  Leverage existing Cisco infrastructure — eliminate redundant appliances
- ⚡ **Dynamic, Agile Operations**
  Policy tied to trust tags — changes propagate automatically across all domains
- 🛡️ **Preventative Security Posture**
  Least privilege enforced at the access layer from the first connection
- 🌐 **Unified Across All Domains**
  One policy framework spans OT, IoT, wireless, cloud, DC, and hybrid

The Cisco Advantage: Shift from scattered, expensive inspection appliances to a **single intelligent trust decision at the access layer** — your existing infrastructure becomes the enforcement engine. This is **business-aligned risk investment** at scale.

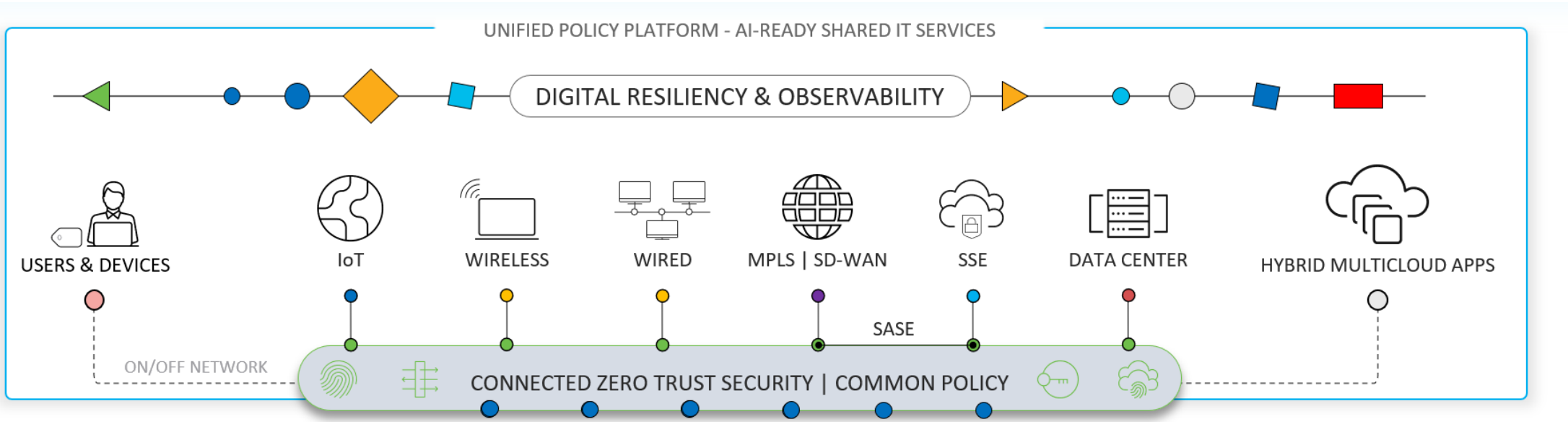
Security Cost/Complexity Continuum

Key Insight: Align cost to desired risk reduction

Align control complexity to business risk — not uniform policy across all traffic



Cisco Unified Policy



Cisco Security Cloud Control

IP Policy

	Employee	BYOD	Contractor	IoT G1	Guest	Unknown
Employee	PERMIT	DENY	DENY	PERMIT	DENY	DENY
BYOD	DENY	DENY	DENY	DENY	DENY	DENY
Contractor	DENY				DENY	
IoT G1	DENY	DENY	DENY		DENY	DENY
Guest	DENY	DENY	DENY	DENY	DENY	DENY
Unknown	DENY	DENY	DENY	DENY	DENY	DENY

FW Policy

DC	Internet
PERMIT	PERMIT
	PERMIT
	PERMIT
DENY	
DENY	

SSE Policy

IntA	IntB
PERMIT	PERMIT
	PERMIT

SDWAN Policy

WAN A	WAN B
PERMIT	PERMIT
	PERMIT

ACI Policy

Enclave1	Enclave2
PERMIT	PREMIT
PERMIT	

AppSec Policy

Prod	Dev
DENY	PERMIT
DENY	DENY
PERMIT	DENY
DENY	DENY
DENY	DENY
DENY	DENY

The Journey of Tag 🏷️

Road to Segmentation

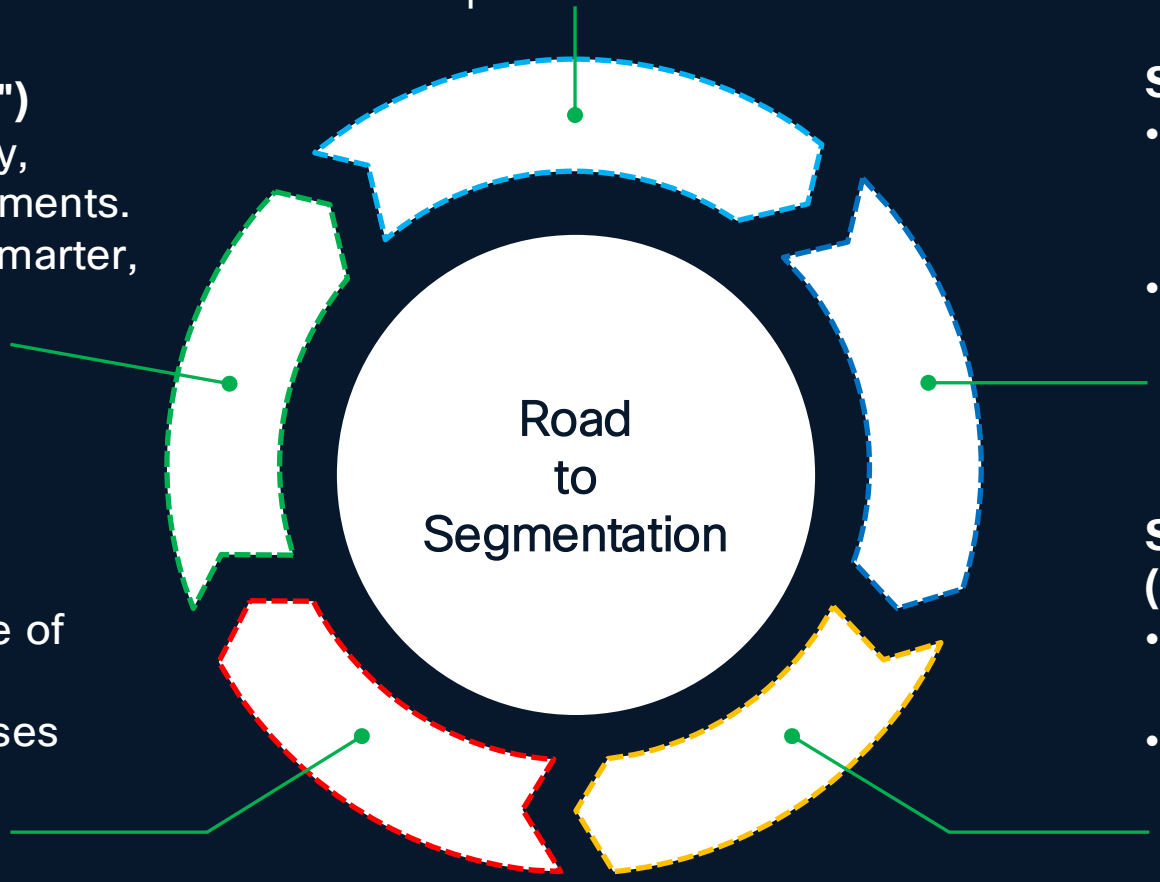
Step 1. Real-Time Visibility
- Understands all asset and network activity before acting.
- Forms the basis for defining trust zones and smart policies.

Step 2. Actionable Policies
- Converts visibility into specific, enforceable access rules.
- Shrinks the attack surface by enforcing least privilege.

Step 3. Effective Implementation ("Enforcement Strategies")
- Applies policies safely without disrupting business operations.
- Validates all controls post-deployment with key stakeholders.

Step 4. Policy Life-Cycle Management
- Treats segmentation as a cycle of monitoring and refining.
- Keeps policies effective and uses rollbacks for stability.

Step 5. Modern Approach ("The Evolution of The Network")
- Layers controls across identity, workloads, and cloud environments.
- Uses AI-driven methods for smarter, future-proof security.



A Strategic Approach to Isolation and Control

Two Layers of Modern Segmentation

Application Segmentation

Frontend Auth DB

Policies Between Services, API Gateways, Service Mesh

Application Isolation

Network Segmentation Zones

Users IoT OT Data Centers Cloud

VLANs, Firewall Rules, SGTs

Network Isolation

Prevents service-to-service abuse and enforces least-privilege at runtime to prevent the spark

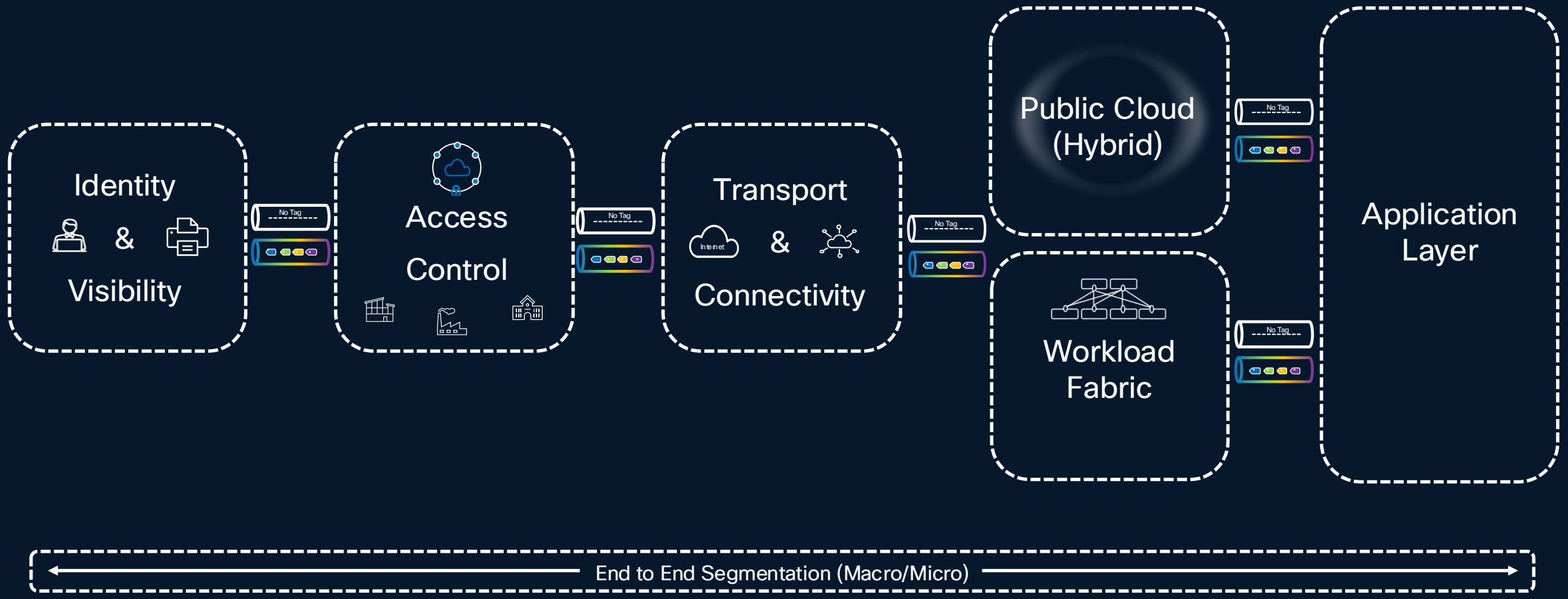
+

Prevents device-to-device and zone-to-zone lateral movement to stop the blast

Together

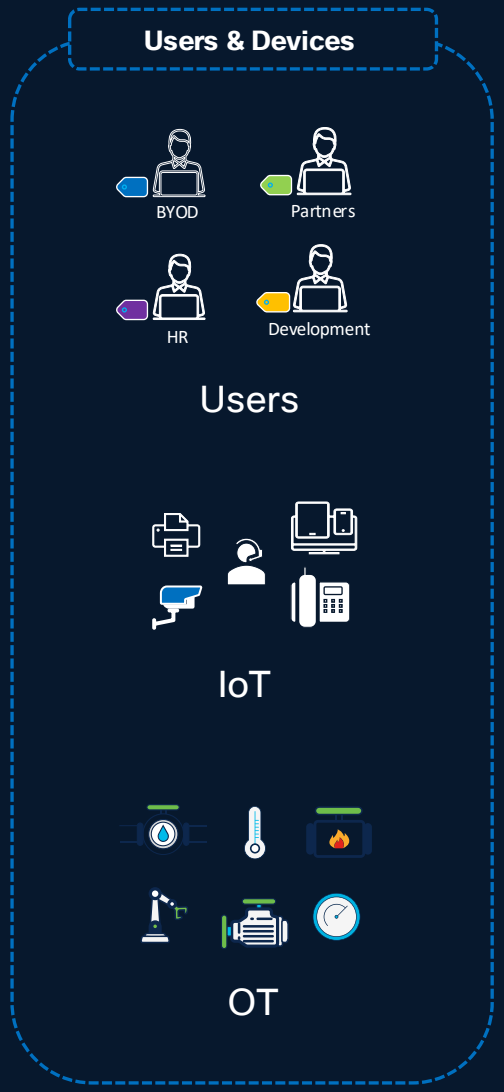
They help enable Zero Trust and contain threats no matter where they emerge

Cisco's Unique Approach to Multi-Domain Segmentation



Visibility and Identification

From User, Devices to Applications



Identification:

- Detect user/device identity via 802.1X, MAB, and profiling data
- 802.1X, MAB, DHCP, RADIUS, SNMP, CDP

Profiling:

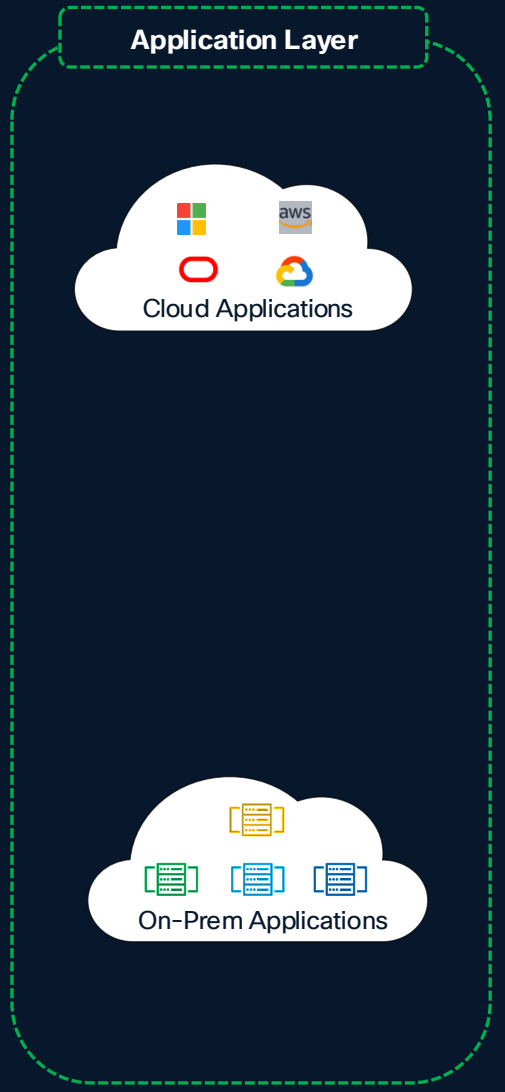
- Classify device/user type and role based on collected data
- Cisco ISE, DNAC or Third-party profiling, device classification

Authentication:

- Authenticate user/device credentials and verify network device trust
- 802.1X, MAB, Web Auth

Network:

- Netflow: Understand traffic patterns, map them



Identification

- Process-level telemetry and binary signatures.
- K8s labels, namespaces, and identity mapping.

Profiling

- Automated dependency mapping and flow baselining.
- Service-to-service communication and API interaction mapping.

Enforcement

- Process-verified micro-segmentation.
- L7-aware security policies.

Observability

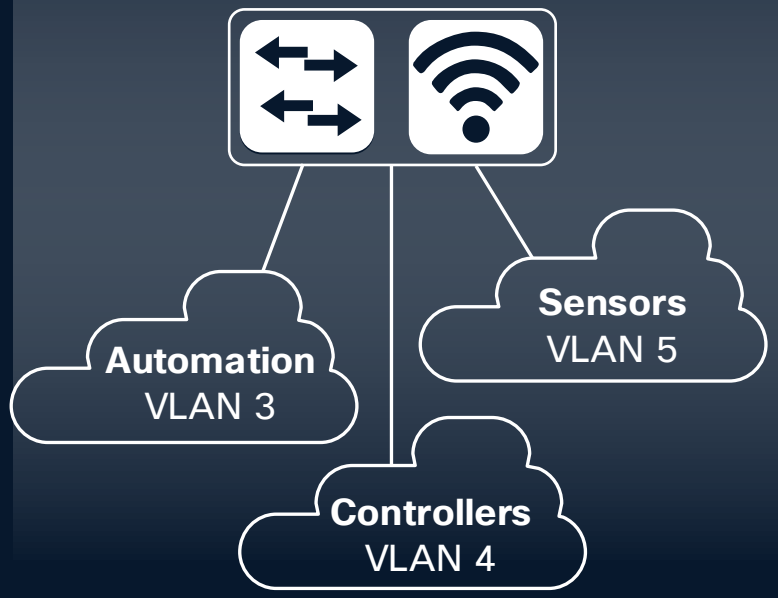
- Network and Agent-based flow logs and lateral movement detection.
- Hubble-based real-time flow and DNS monitoring.

Segmentation Option

The evolution to Tags

VLANs

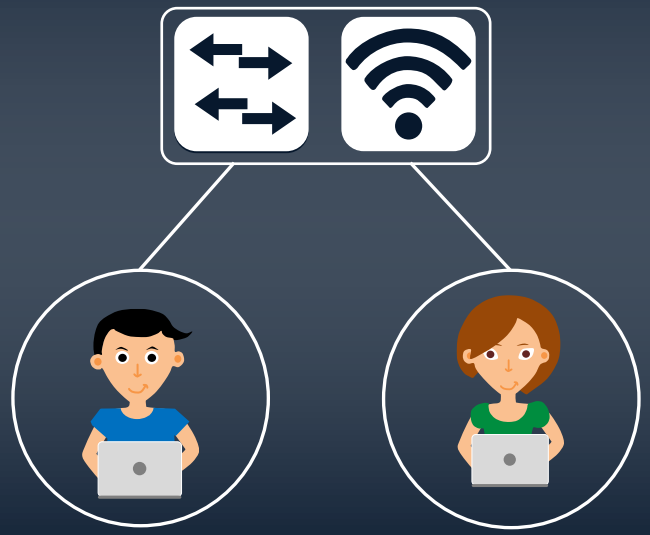
Dynamic VLAN Assignments



Per port / Per Domain / Per MAC

ACLs: DL, Named, DNS

Downloadable ACL (Wired) or
Named ACL (Wired + Wireless)

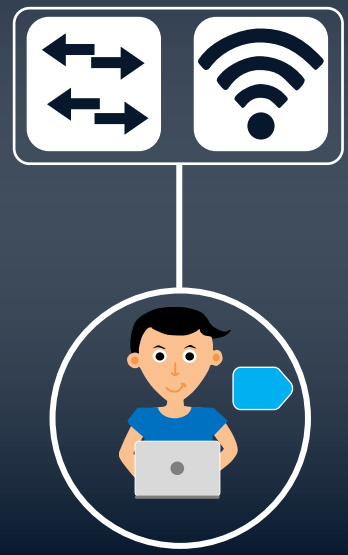


Employee
`permit ip any any`

Contractor
`deny ip host <critical>`
`permit ip any any`

Security Group Tags

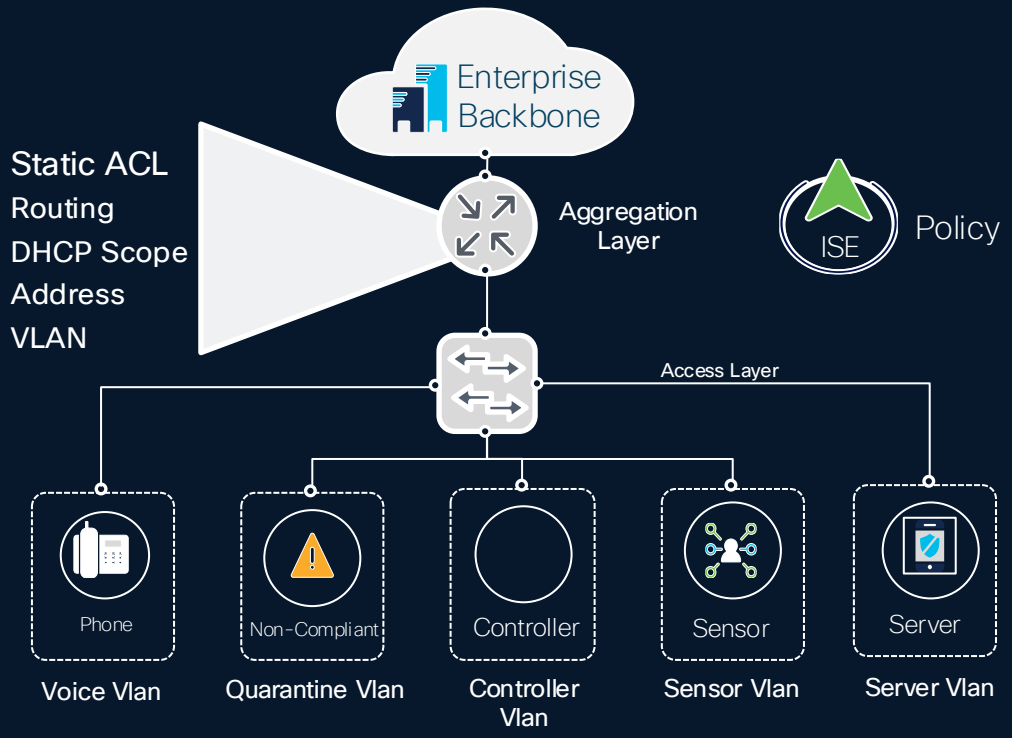
Cisco Group-Based Policy
Adaptive Policy



16-bit SGT assignment and
SGT based Access Control

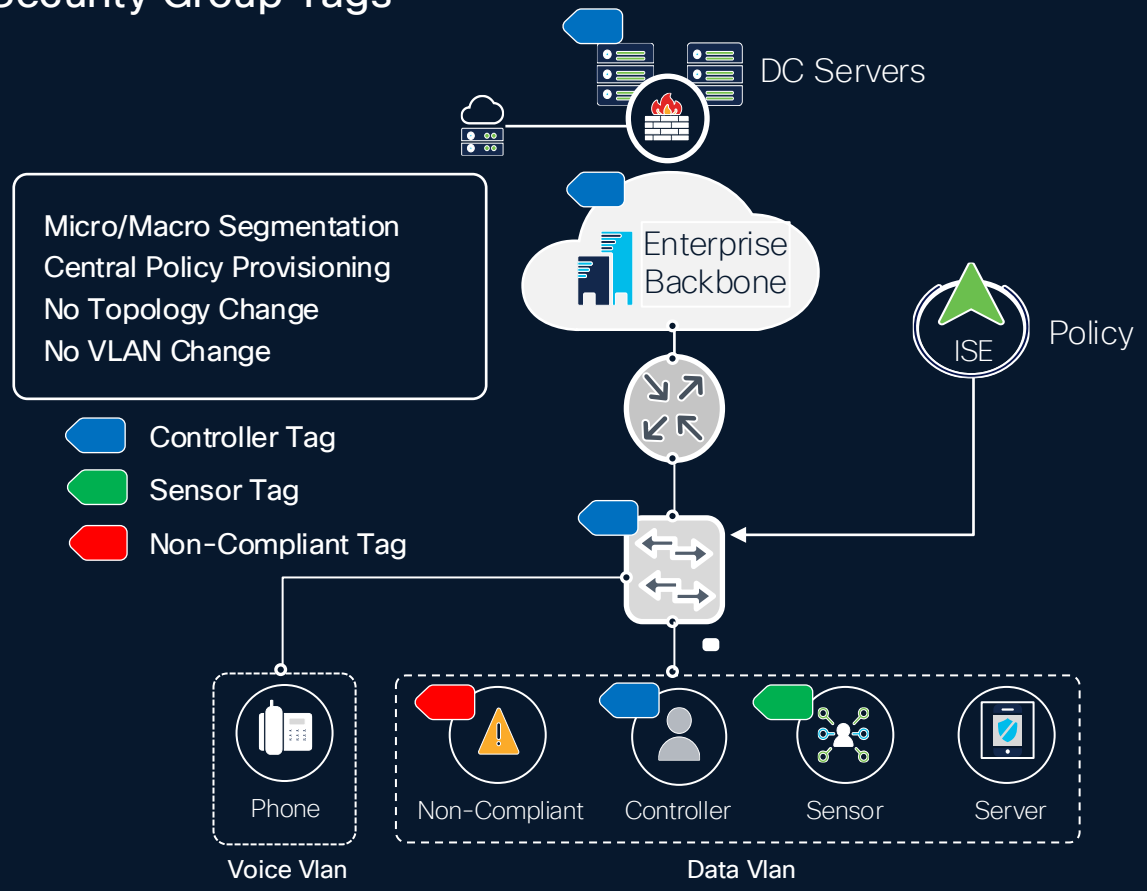
Group Based Policy Simplifies Segmentation

Traditional Segmentation



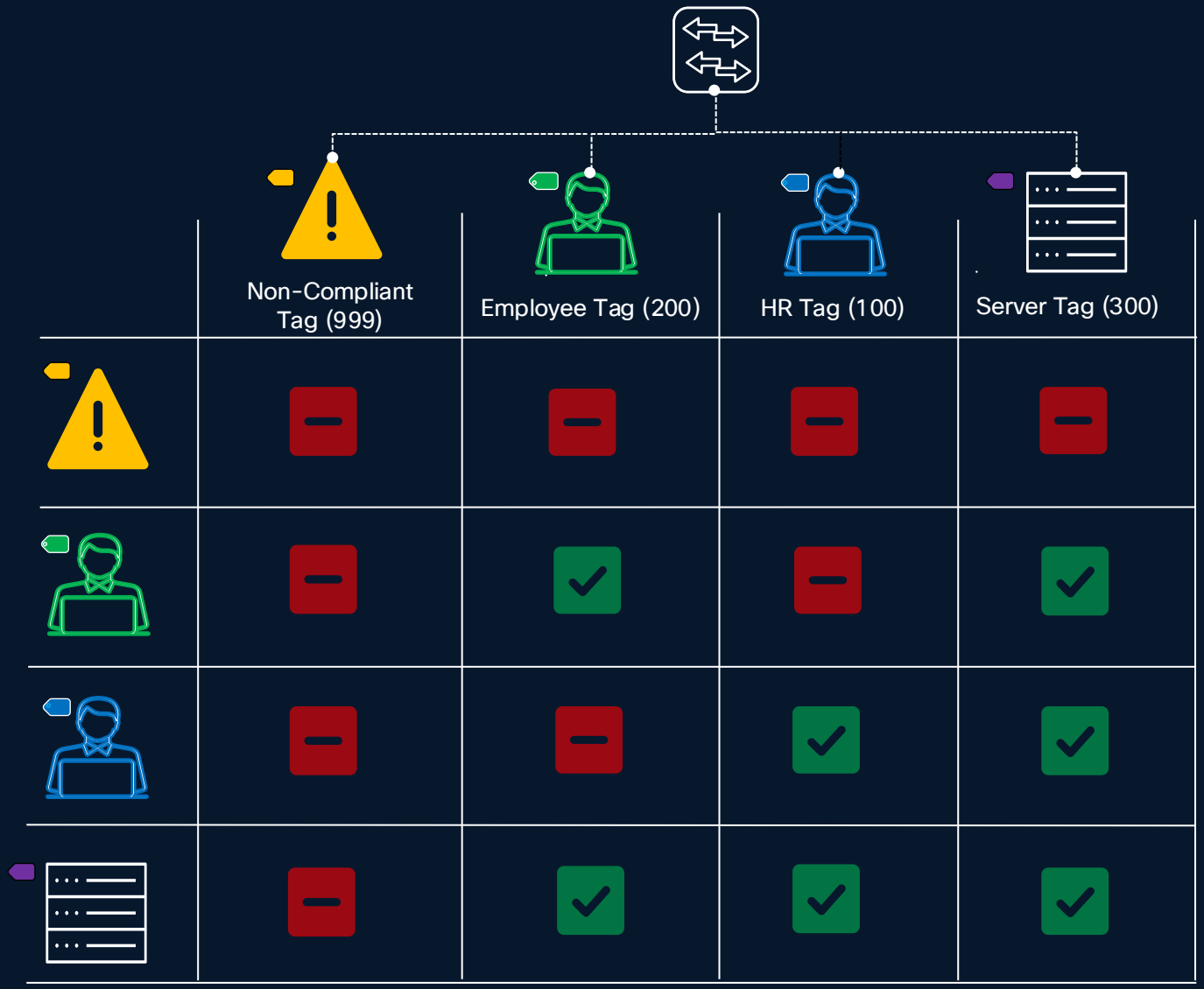
Security Policy based on Topology
High Cost and Complex Maintenance

Security Group Tags



Use existing topology and automate
security policy to reduce OpEx

Group Based Segmentation Matrix
Security Group Tags

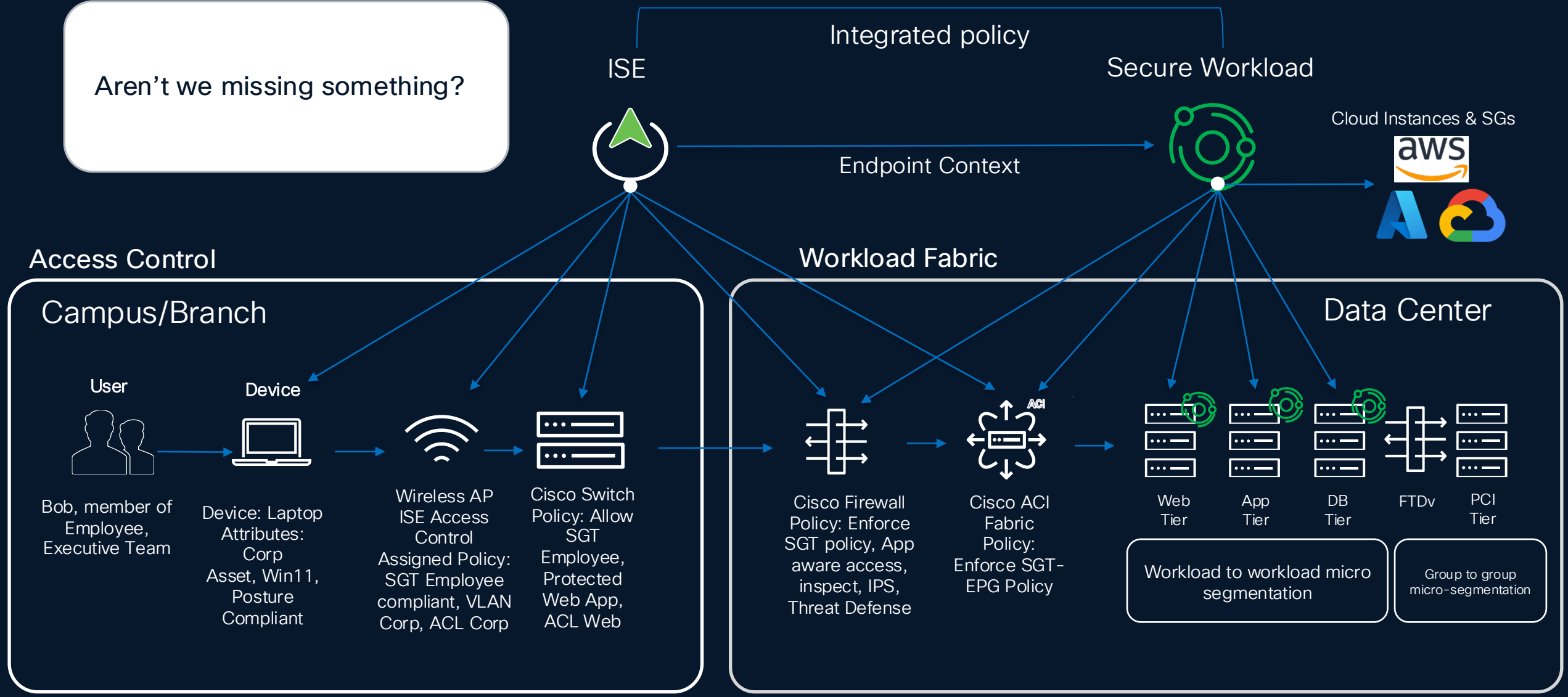


Authentication
Who are you?

Authorization
What can you do?

Cisco's Zero Trust Segmentation Strategy

Aren't we missing something?



Access Control

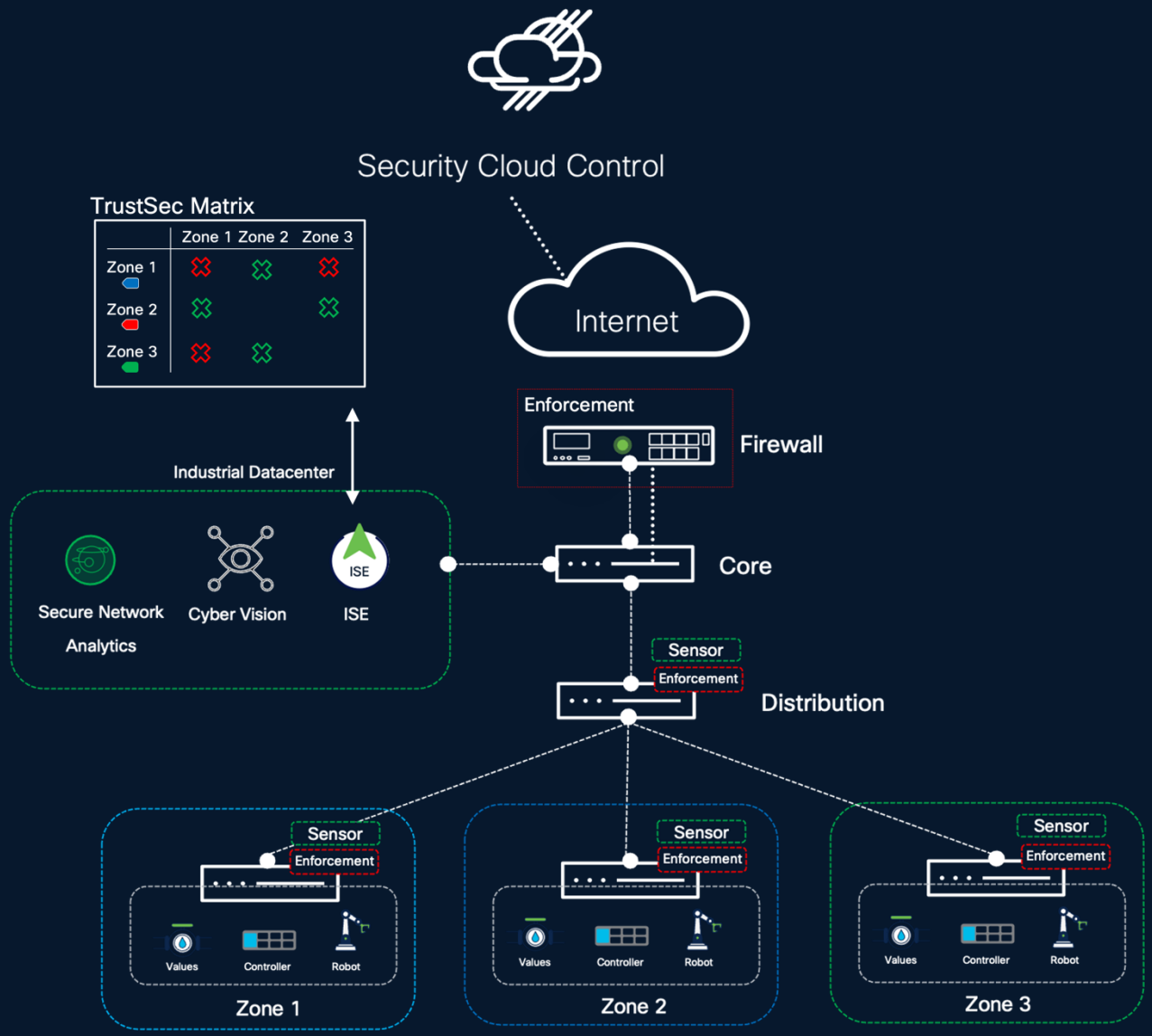
Manufacturing

Cisco Cyber Vision: Delivers deep visibility into OT assets and industrial protocols to map baseline communication flows.

Cisco ISE: Enables identity-based micro-segmentation by assigning SGTs to OT devices, restricting access to authorized systems only. PxGrid integration with Cyber Vision

Secure Network Analytics: Monitors traffic for behavioral anomalies, providing real-time detection of unauthorized lateral movement and security threats.

Cisco FMC: Centralizes firewall policy management, enforcing granular security rules at the IT/OT boundary to block unauthorized cross-zone traffic. Cyber Vision integration



Access Control

Secure Access

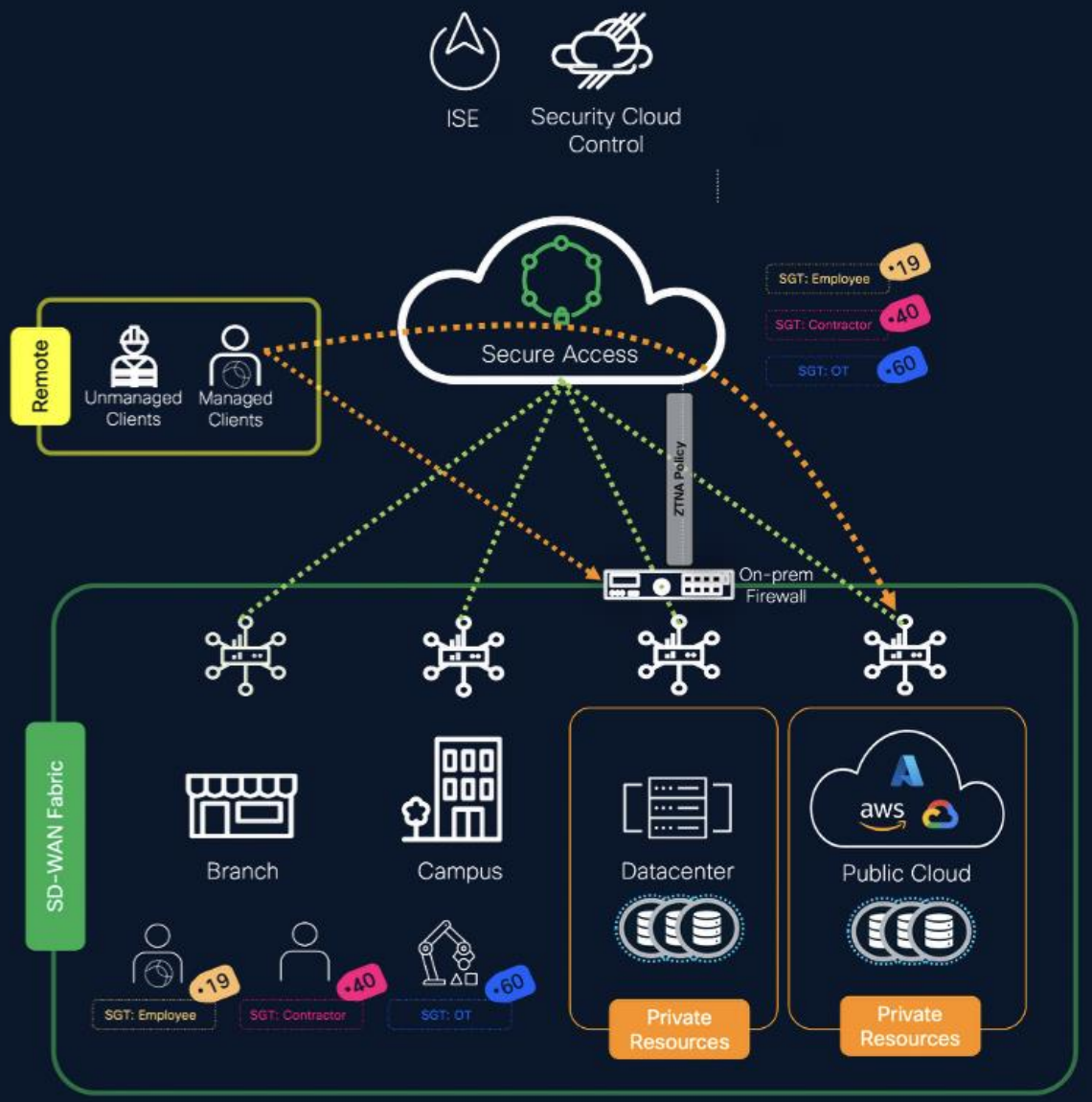
Cisco's Universal Zero Trust Network Access (ZTNA)

Identity-Based Micro-segmentation: Leverages Cisco ISE and Security Group Tags (SGTs) to enforce granular, role-based access, ensuring users are segmented by their specific job function rather than broad network subnets.

Application-Level Isolation: Cisco Secure Access creates direct, authorized tunnels to specific private resources, effectively isolating applications from the wider network and preventing unauthorized lateral movement.

Contextual Trust Segmentation: Access levels are dynamically adjusted based on continuous trust verification (Duo MFA, posture checks, and device health), segmenting users into different trust tiers based on their current security state.

Hybrid Perimeter Enforcement: Combines cloud-based ZTNA policies with on-premise firewall enforcement to segment traffic at the application edge, ensuring consistent security for both cloud-hosted and data-center-hosted resources.



Transport Connectivity
SDWAN

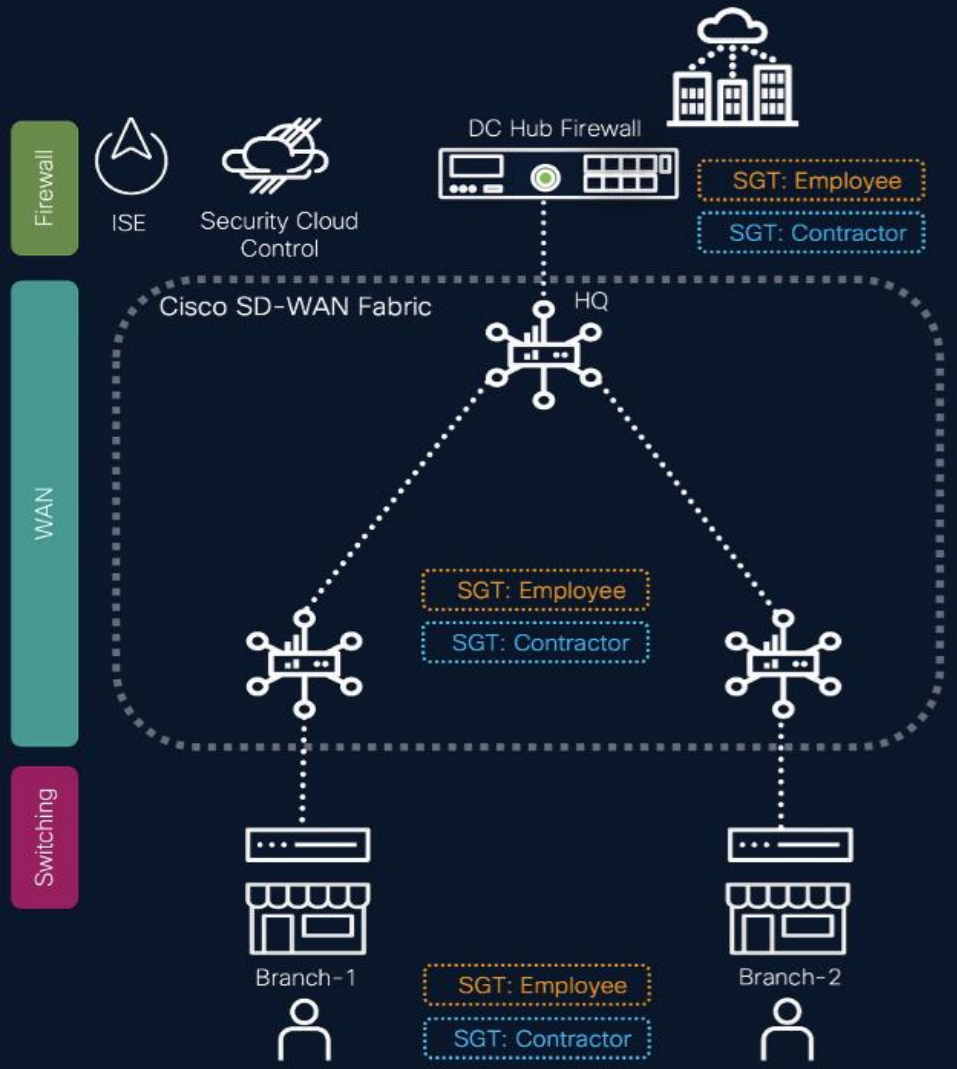
Identity-Centric Zero Trust: Access is granted based on user roles rather than static IP addresses, ensuring users only reach the resources they need.

Unified Cloud Management: Simplify operations by managing security policies across your entire enterprise WAN from a single, centralized console.

Consistent Policy Enforcement: Security Group Tags (SGTs) maintain identity context across the SD-WAN fabric, ensuring policies follow the user everywhere.

Automated Threat Containment: Instantly isolate compromised devices to stop lateral movement and contain malware at the network edge.

Optimized Secure Connectivity: Deliver high-performance, application-aware SD-WAN traffic without sacrificing granular, role-based security.



Data Center / Applications

Network Segmentation Spectrum

Defense in Depth

Between Processes

Process Level, System Calls, Identity Context

Between Workloads

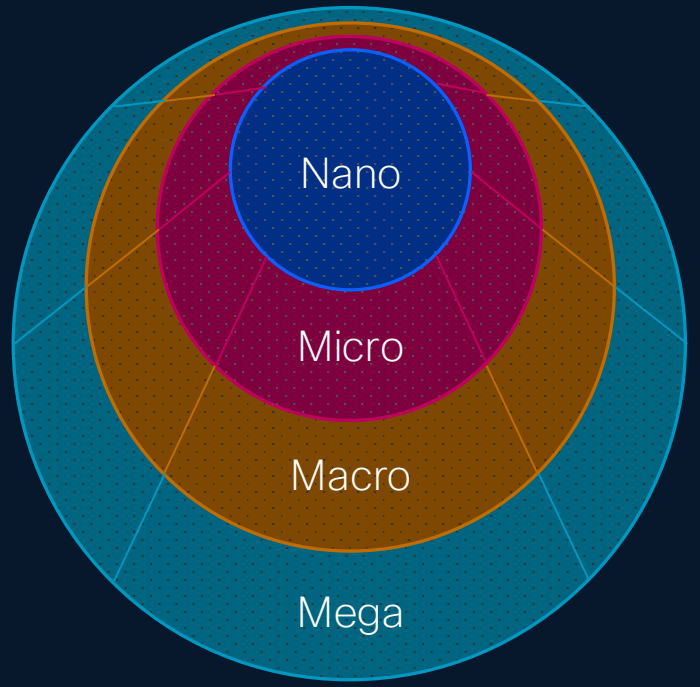
Applications, VMs, Containers, etc.

Between Environments

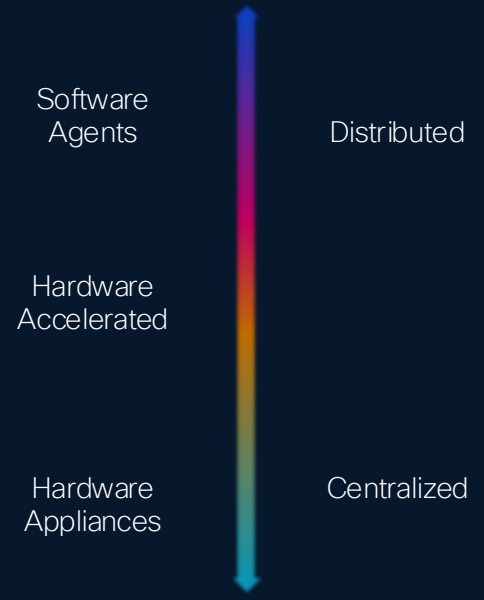
Prod and Dev, Tenants, Cloud, Compliance, etc.

Between Organizations

Organization and Everyone

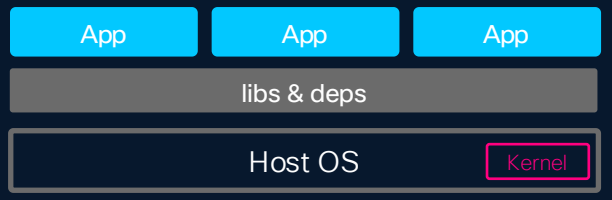


Diverse Form Factors

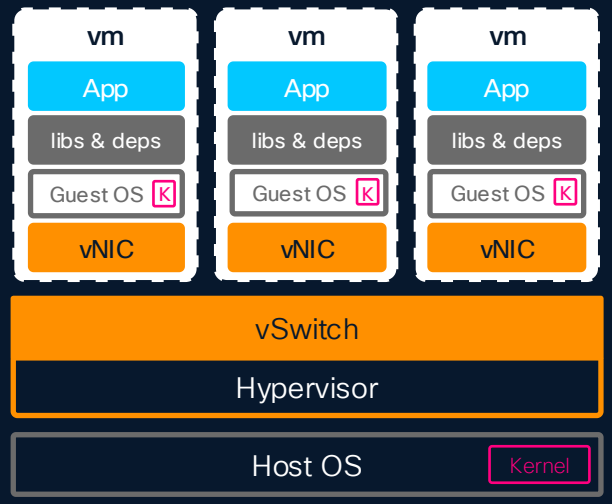


Distributed Observability and Enforcement

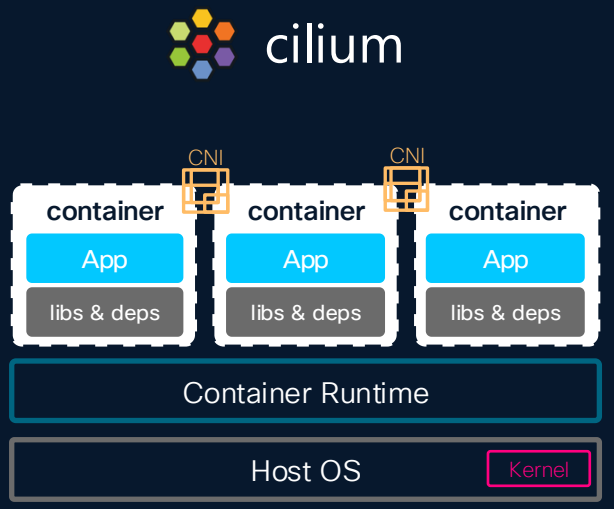
Bare Metal



Virtualized



Kubernetes



Agent-based

workload eBPF

tetragon

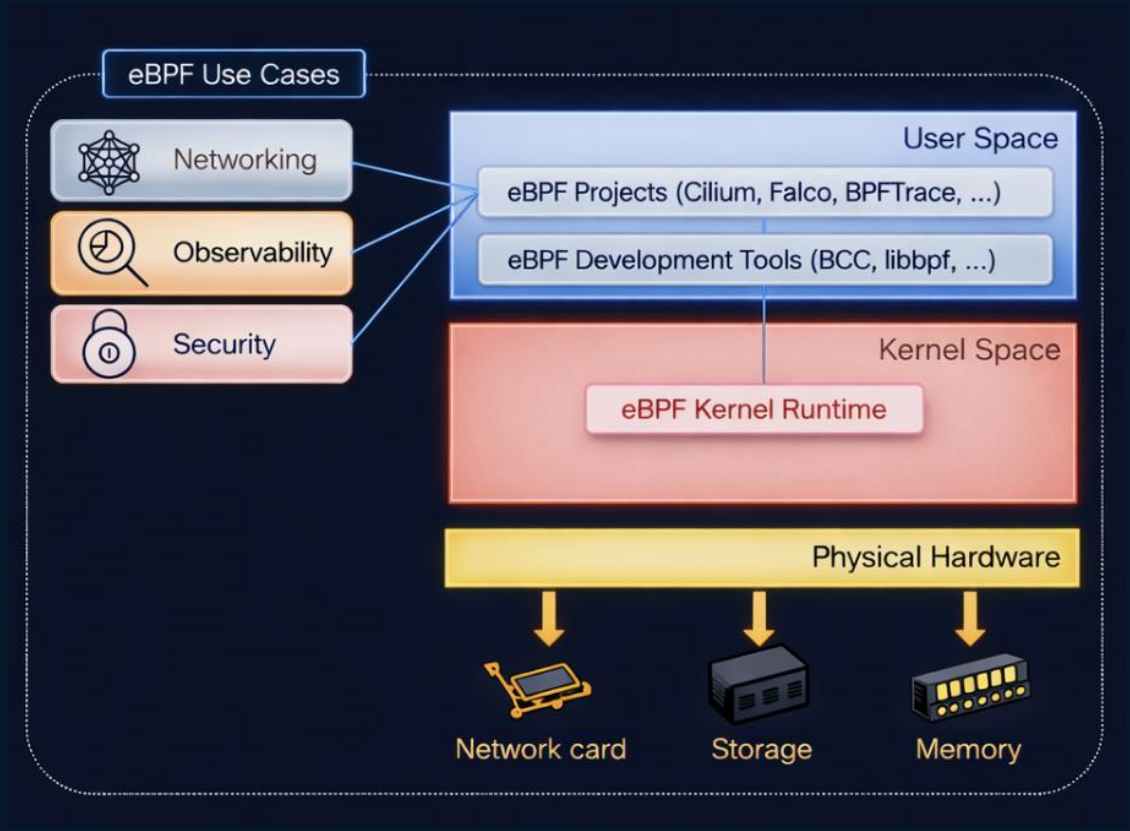
Cloud

Agentless

smart switch

cisco

- Originated from the Berkeley Packet Filter, it’s subsystem in the Kernel
- Safely and efficiently extend the capabilities of the kernel
  - **Sandboxed VM:** A safe, kernel-embedded engine that runs custom code without risking system stability.
  - **"JavaScript for the Kernel":** Executes custom logic within the kernel without modifying its source code or loading risky modules.
  - **Programmable Kernel:** Dynamically adds networking, security, and observability capabilities to the kernel at runtime.

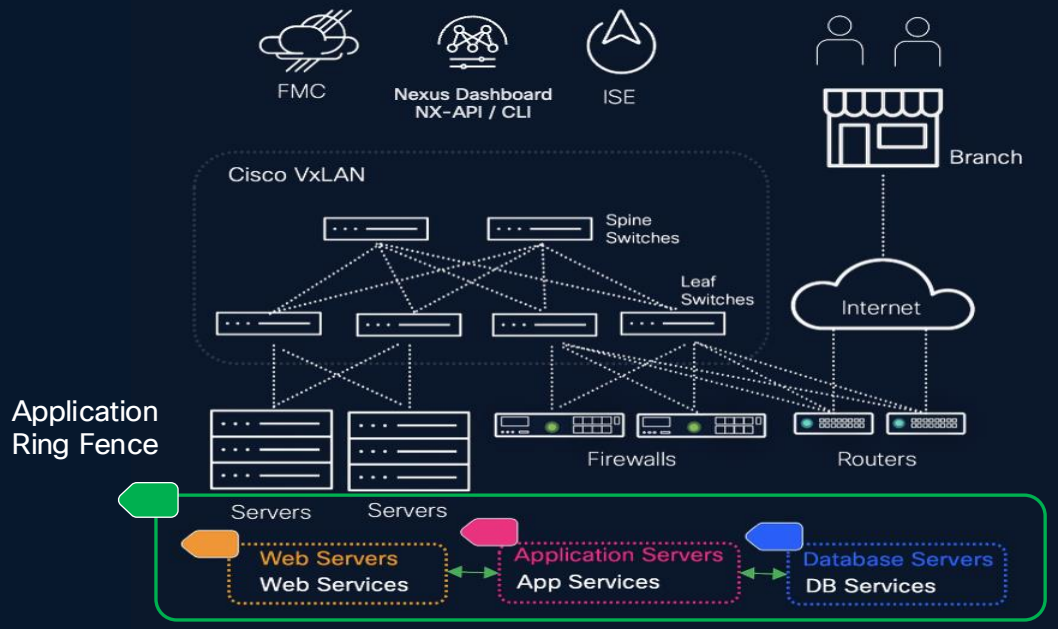


Network Security

- Advanced packet filtering and processing
- DDoS mitigation
- Intrusion detection and prevention
- Runtime security enforcement
- Data exfiltration prevention
- Application sandboxing

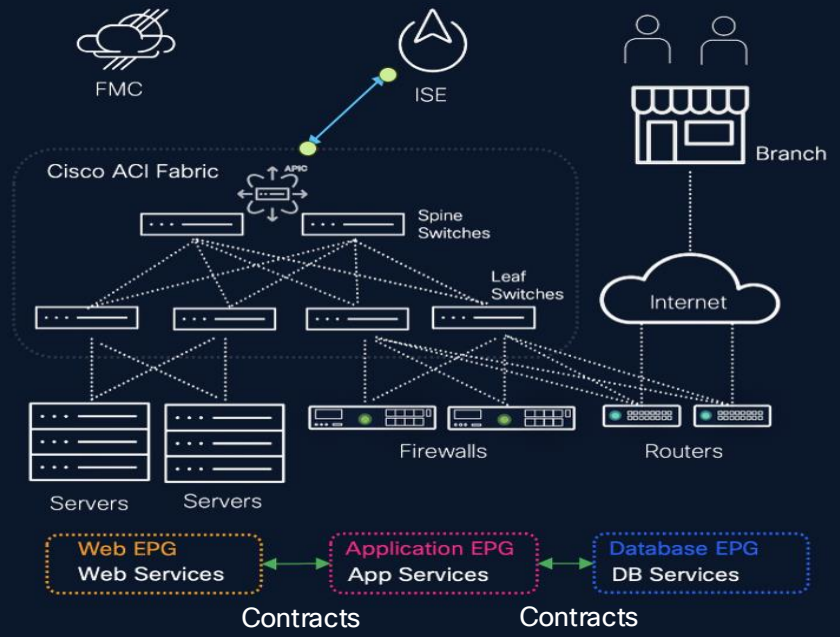
Workload Fabrics

VxLAN Fabric with GPO



- VXLAN EVPN uses VXLAN encapsulation with MP-BGP EVPN control plane for scalable L2/L3 virtualization.
- Segmentation is done via VLANs, VNIs or VRFs, without security group tagging or policy enforcement.
- GPO has been added VXLAN to allow for granular segmentation beyond, VLANs, VNI and VRFs
- VXLAN GPO Embeds Security Group Tags (SGTs) directly into the VxLAN header, enabling consistent, identity-based segmentation and policy enforcement across the entire fabric.

ACI Fabric

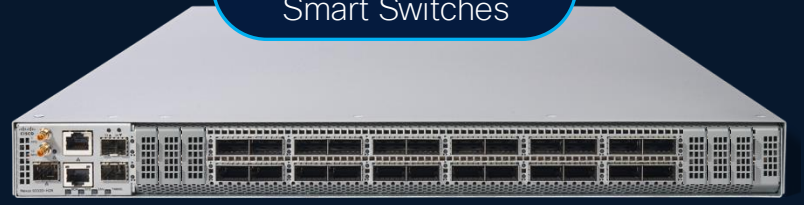


- Integrated hardware/software fabric with centralized APIC controller.
- Segmentation via Endpoint Groups (EPGs), Endpoint Security Groups (ESGs) and contract-based policies.
- Supports micro segmentation with fine-grained policy enforcement.
- Policy enforcement tightly integrated within the fabric.
- Integrations with other security solutions

Nexus Smart Switch

Unmatched Flexibility, Performance, and Efficiency

Cisco
Smart Switches



Cisco Nexus 9300 Services Accelerated Switch

Networking

Cisco Silicon One

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

Routing Switching | EVPN/MPLS/ VXLAN/SR | Rich Telemetry | Line-rate Encryption | Power Efficiency

Hypershield

AMD PENSANDO

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

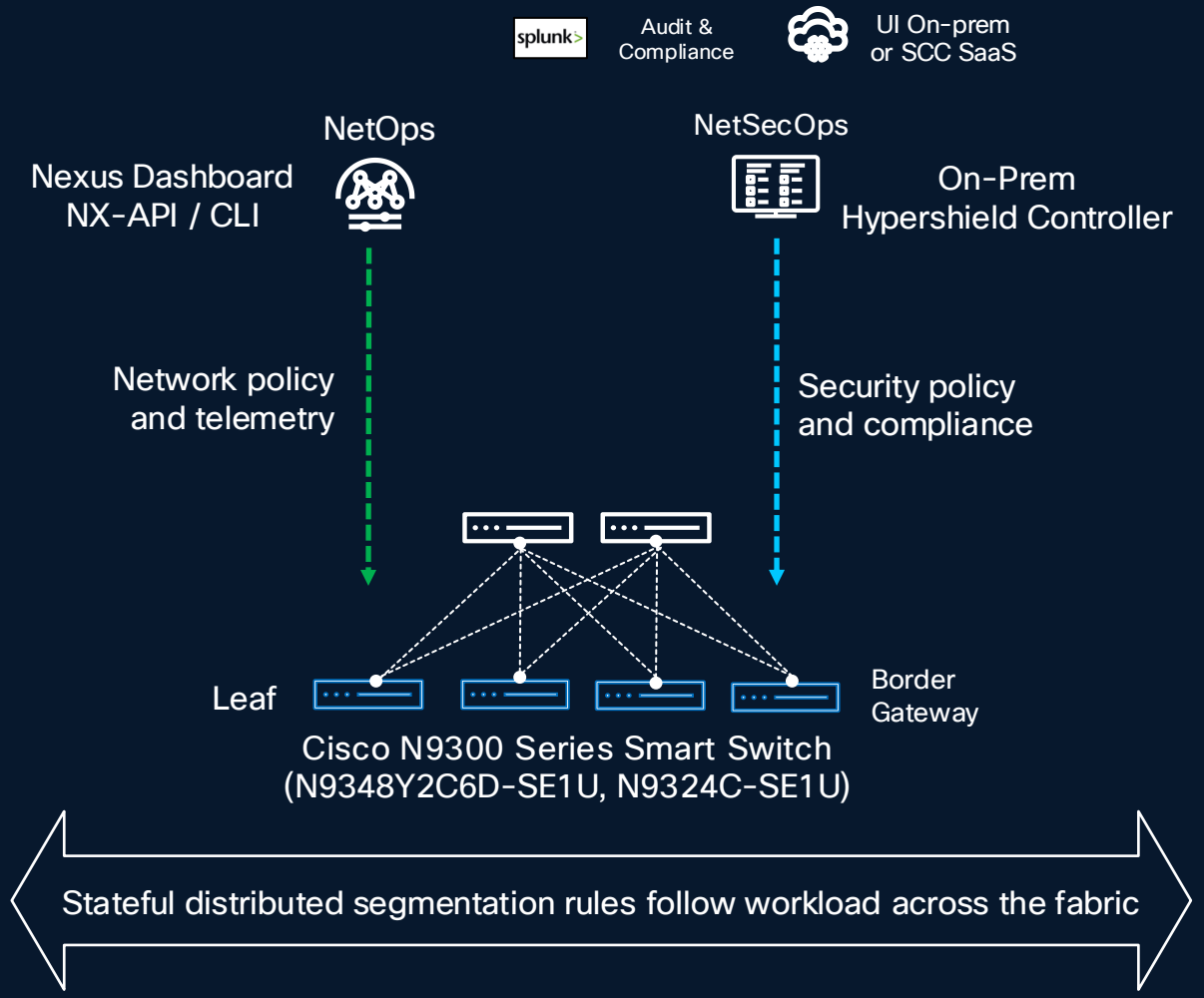
Distributed Security

IPSEC Encryption | Large-Scale NAT | Event-Based Telemetry | DoS Protection

Future Use Cases

cisco

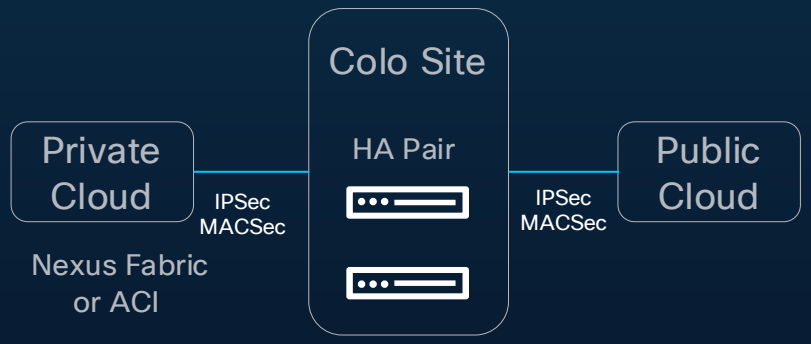
Workload Fabrics
Smart Switches



Security Infused in Data Center Fabric

- ✓ Fabrics
- ✓ Traffic redirection
- ✓ Segmentation Policy
- ✓ Policy Sync and HA
- ✓ Hypershield On-prem Controller
- ✓ Visibility & Observability

Smart Switch Use Cases



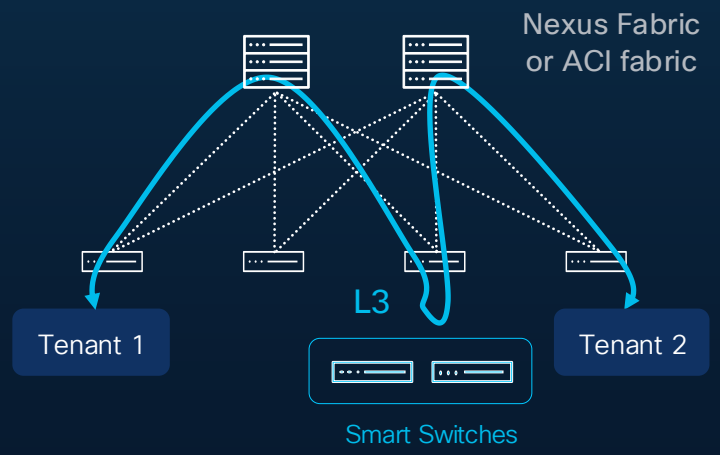
Cloud Edge

Smart Switch provides stateful L3/L4 East-West segmentation and visibility between private and public clouds

Secure peering gateway via IPSec (only Nexus fabric) or MACSec

Applies to brownfield NXOS and ACI deployments

NXOS 10.6(3)F – Planning



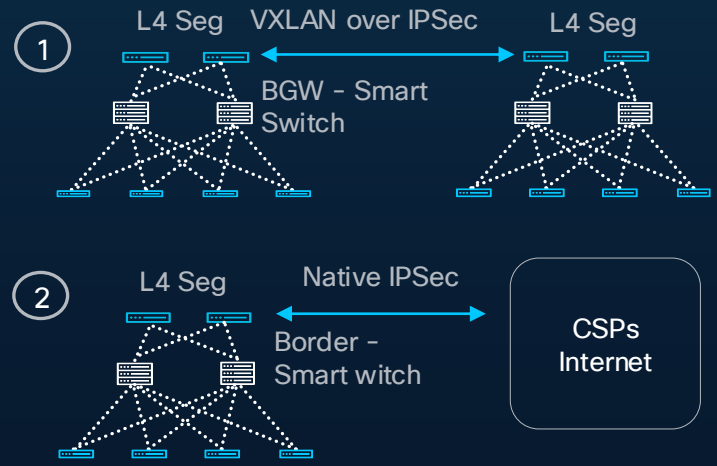
Zone Segmentation

Smart Switches provide external East-West L4 stateful segmentation and visibility

High scale and performance

Applies to brownfield NXOS and ACI deployments

NXOS 10.6(3)F – Planning



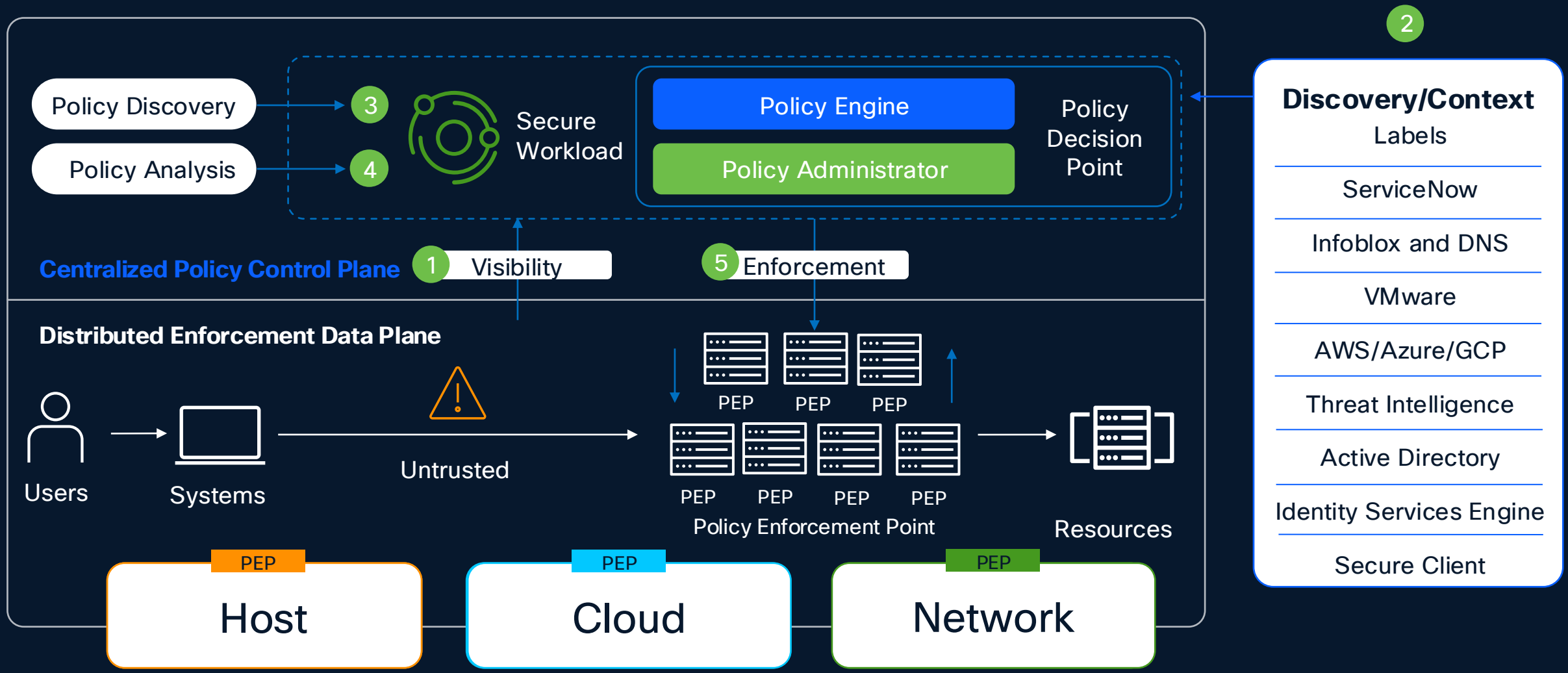
Secure Peering for DCI

Consistent L4 segmentation policy extending between all border gateway of VXLAN EVPN fabric.

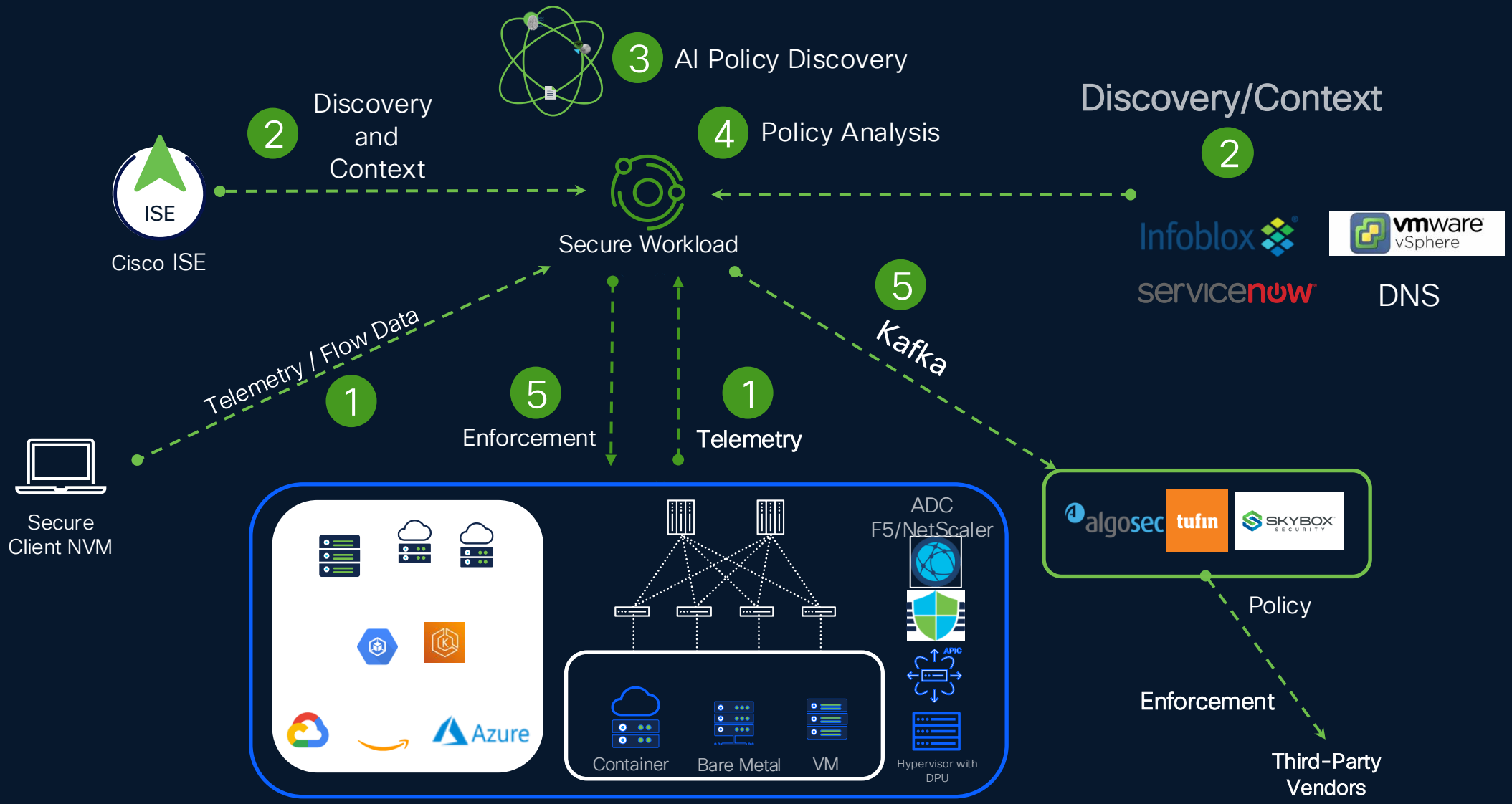
Encrypt VXLAN traffic between fabrics using IPSec or native IPSec to CSPs or Internet

NXOS 10.6(3)F – Beta

Application Layer
Secure Workload – Zero Trust Segmentation

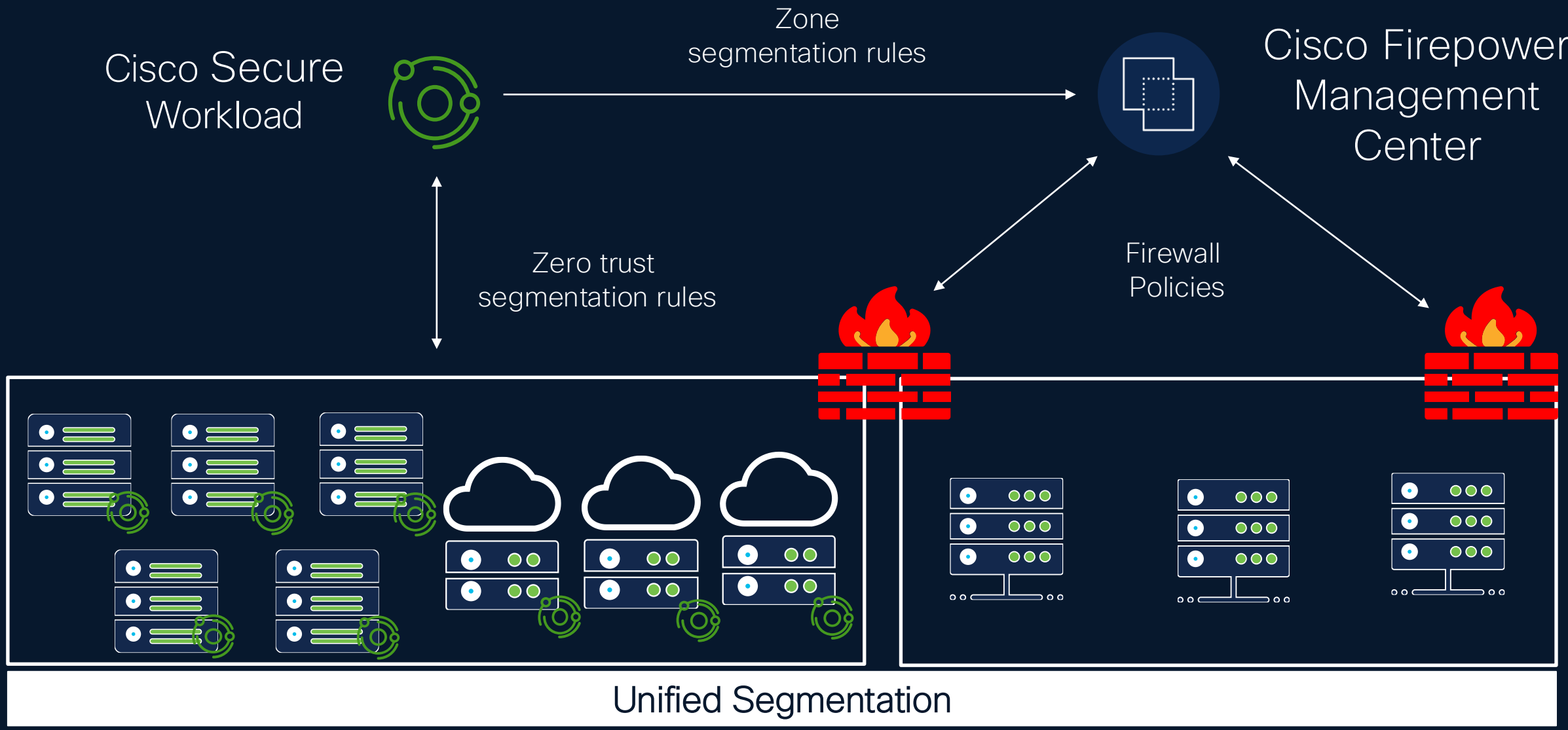


Macro/Micro-Segmentation Reference Architecture



Application Layer

Secure Workload & Firewalls



Successful Segmentation Projects

Best Practices and Recommendations

Start with Visibility

- Inventory all assets
- Understand the network flows

Tools

Secure Network Analytics

Cyber Vision

Secure Workload

Cross-team Collaboration

- Align IT, security, operations, and business units early.
- Share insights on asset criticality and compliance.
- Use centralized platforms for unified policy control.

Leverage Automation and AI

- Automate policy discovery, lifecycle management, and enforcement.
- Use AI for behavioral monitoring and anomaly detection.
- Integrate segmentation with SOC workflows for rapid response.

Continuous Refinement

- Monitor policies in real-time and adjust using analytics and threat intelligence.
- Conduct regular audits and test changes before deployment.
- Incorporate feedback from incidents and user experience.

Prioritize Segmentation

- Focus on business-critical and high-risk assets first.
- Protect legacy systems with tighter zones.
- Implement segmentation in phases from macro to micro and nano layers.
- Align with compliance and audit requirements.

Integrated Cisco Zero Trust platform

Cisco ISE, Secure Workload, Catalyst Center, Meraki, Cyber Vision, Secure Firewall for End-to-End Enforcement and Visibility

Thank you