CISCO Engage | Tech Day NYC

Cisco Hybrid Mesh Firewall & Segmentation

Ty Rost, CCIE #12708, CISSP

March 4th, 2026

WHO IS TY?

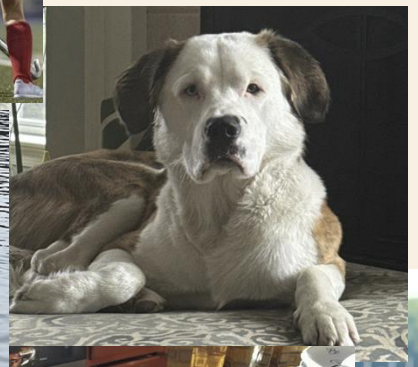
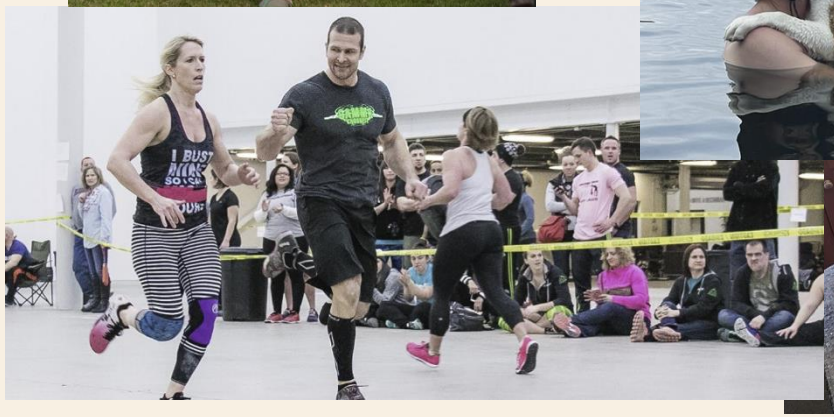
Husband and Dad

- Married almost 25 years to Meredith
- Daughters Janie (22), Mya (19), and Lily (17)

Diversified Portfolio

- YouTube Golf Sim Influencer (articulate)
- Dog Whisperer and Trainer Extraordinaire (behaviorist)
- Triple Sport Nationally Ranked Athlete (competitive)
- Prime Rib Expert (connoisseur)








Agenda

01 Industry Perspective: The Evolution of Hybrid Security

02 Cisco’s Hybrid Mesh Firewall: Vision & Foundation

03 Cisco’s Hybrid Mesh Firewall: Architecture

04 Capabilities & Design Principles

05 Key Takeaways

Industry Perspective:
The Evolution of Hybrid Security

What's the problem? Why the need?

Organizational Challenges

Multiple teams, organizations and environments

Inconsistent islands of policy controls across environments

cisco

Hybrid Security

Customers Industry/Analyst Vendors

Hybrid Security = Hybrid Mesh Firewall

A **Hybrid Mesh Firewall** is a multideployment firewall platform with centralized cloud-based management, designed for hybrid environments. It integrates with CI/CD pipelines, supports cloud-native features, and provides advanced threat protection across diverse use cases, including IoT and DNS-based threats.

Gartner – Hybrid Mesh Firewall

- Core & Optional Capabilities

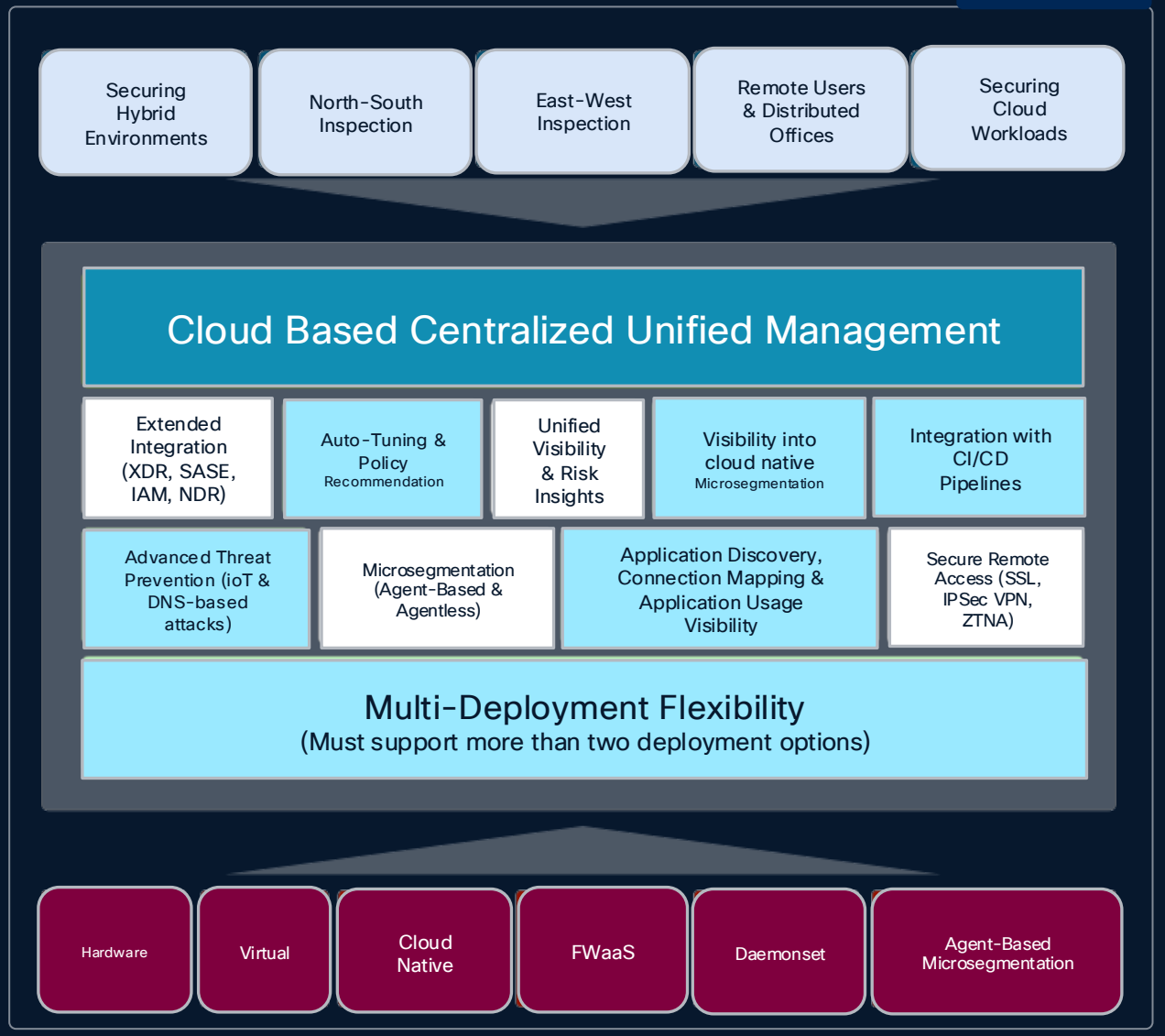
Gartner

Market Guide for Hybrid Mesh Firewall Platforms

Published 16 January 2024 - ID G00794201 - 15 min read

By Analyst(s): Rajpreet Kaur, Adam Hils

Initiatives: Infrastructure Security; Build and Optimize Cybersecurity Programs



Cisco's Hybrid Mesh Firewall:
Vision & Foundation

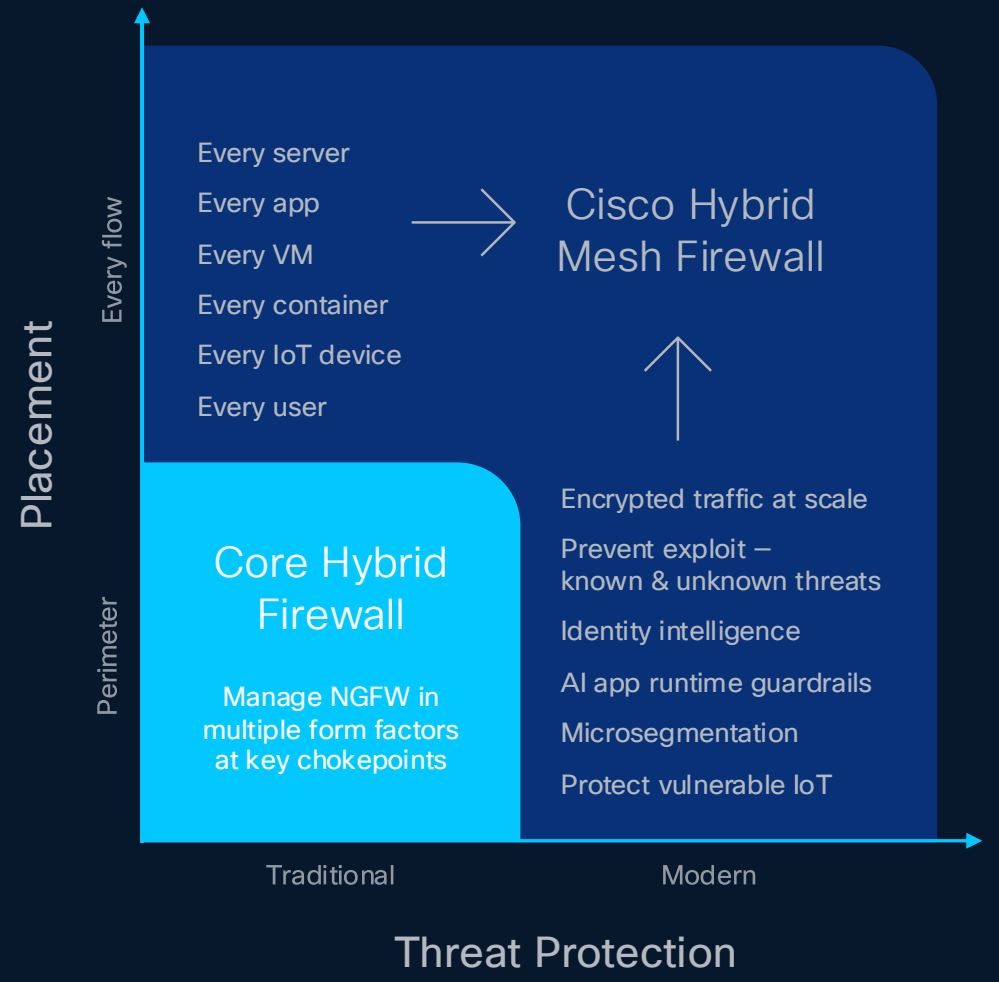
Cisco’s Vision – Hybrid Mesh Firewall

Our North Star

Make it easy for organizations to

- **Reduce** attack surface
- **Prevent** compromise
- **Stop** lateral movement

in the modern data center, cloud, campus, and factory



Cisco Hybrid Mesh Firewall Goes Deeper & Broader

SECURITY CLOUD CONTROL

Secure Firewall (physical)

Secure Firewall (virtual)

Secure Firewall (Cloud)

3rd Party Firewall

FWaaS

ACI

Hypershield Smart Switch

Hypershield Workload

"Cisco's firewall devices managed as one"

Incorporates Existing Network Security Investments

Only Cisco Fuses Security Into Both the Network & Workload

Write policy once, enforce across the mesh

FORRESTER®

2024 Forrester Wave:
Enterprise Firewall Solutions

LEADER

IDC

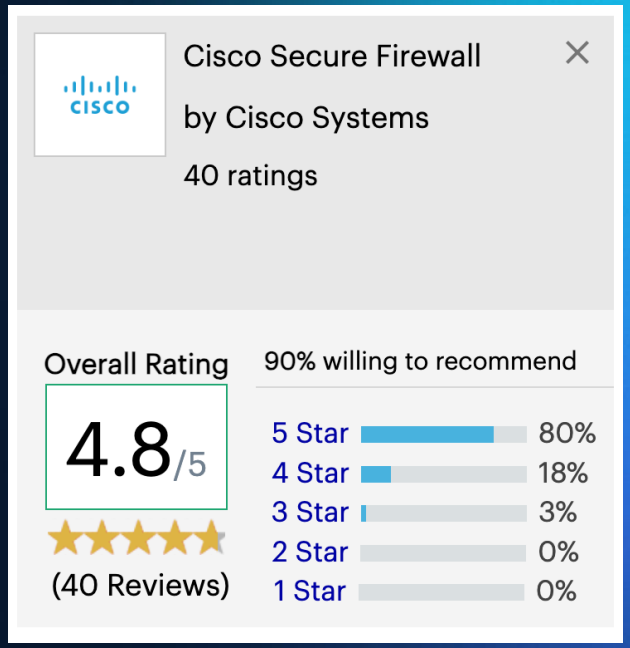
2025 IDC MarketScape:
Worldwide Enterprise Hybrid Firewall

LEADER

Gartner Peer Insights™

Network Firewalls

SCORE LEADER



Cisco’s Hybrid Mesh Firewall: Architecture

Security Cloud Control

Guiding Architectural Principles

Simplified experience

Streamlined activation and deployment

Accelerated time to value

Consistent user experience

Operational Efficiency

Intelligent security

AI-driven best practices

Improved security hygiene

Proactive insights

Swift and informed decision making

Outcome-centric management

Centralized visibility across solutions

Rapid threat investigation

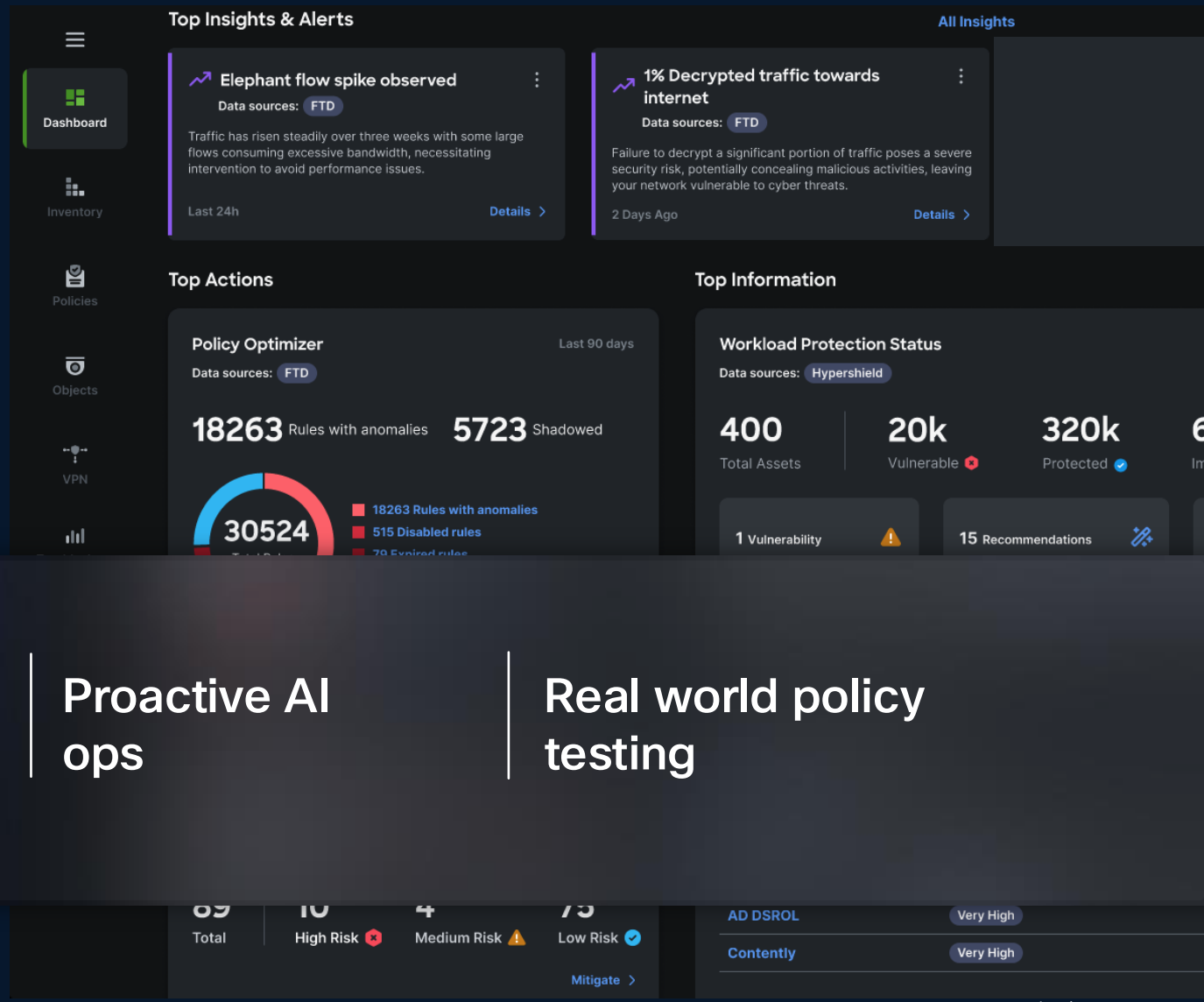
Optimized configurations

Reduced duplication across products

cisco

Security Cloud Control

Simplify policy administration by up to 70%



AI assistance for policy

Proactive AI ops

Real world policy testing

Some capabilities are future.

cisco

Cisco Hybrid Mesh Firewall announcement timeline

	Cisco Live AMER ‘25	Cisco Live APJC, Partner Summit ‘25	Cisco Live EMEA ‘26
Security Cloud Control	Mesh Policy Engine	Multi-tenant management for Managed Service Providers (MSPs)	AgenticOps for firewalling
	Simpler upgrades with AIOps	Multi-org management for enterprises GA	Mesh Policy Engine GA
	Secure Router policy management		
Firewall	Cisco Secure Firewall 200 & 6100 series		Cisco Secure Firewall 200 & 6100 series GA
	Firewall Threat Defense (FTD) 10.0		Firewall Threat Defense (FTD) 10.0 GA
	Firewall Threat Defense virtual (FTDv) orchestrating Cisco Multicloud Defense (MCD)		
Firewall + Splunk	Cisco Secure Firewall and Splunk 5GB offer		
Smart Switches	Cisco Smart Switches		
Secure Workload	Cisco Secure Workload integration with ACI	Cisco Secure Workload integration with ACI GA	
Identity Services Engine (ISE)		Cisco Access Manager	

© 2025 Cisco and/or its affiliates. All rights reserved.

TARGETED AVAILABILITY MAY 2026

Cisco Live EMEA announcement

Turbocharge your firewall operations with built-in agentic capabilities

AgenticOps in Security Cloud Control

Proactive recommendations

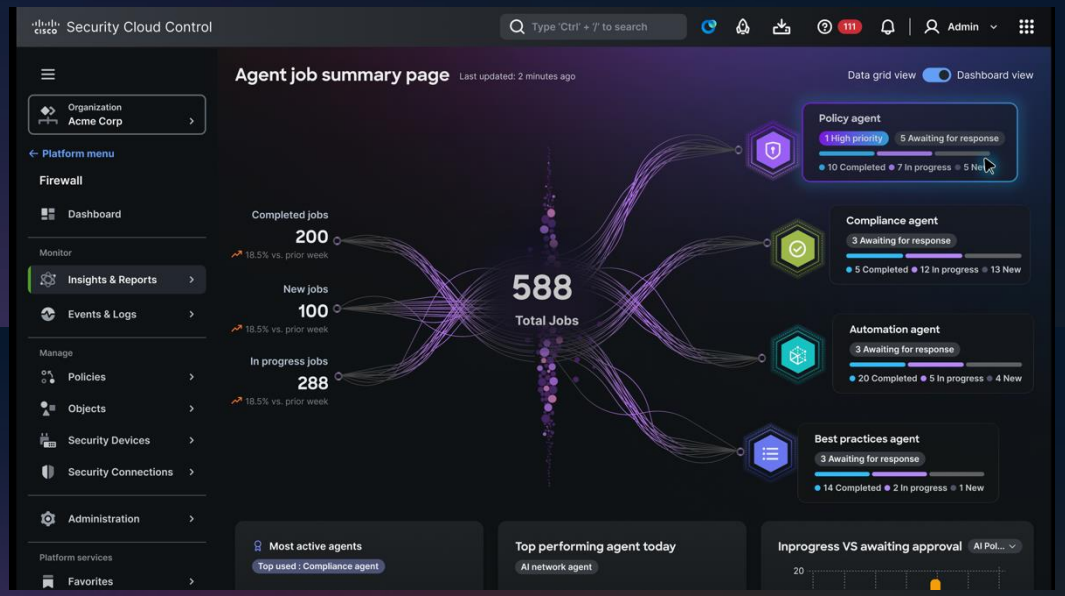
For Zero Trust access policies, VPN capacity planning, best practices for policy

Boost operational efficiency

With one-click execution of proposed remediations for elephant flows and policy optimization

Maintain compliance standards

Automatically identify PCI-DSS deviations with recommended remediations to stay compliant



© 2025 Cisco and/or its affiliates. All rights reserved.

GA THIS MONTH!

Cisco Live EMEA announcement

Adopt hybrid mesh firewall more easily by defining policy once and enforcing everywhere

Mesh Policy Engine in Security Cloud Control

Define policy intent once in Security Cloud Control

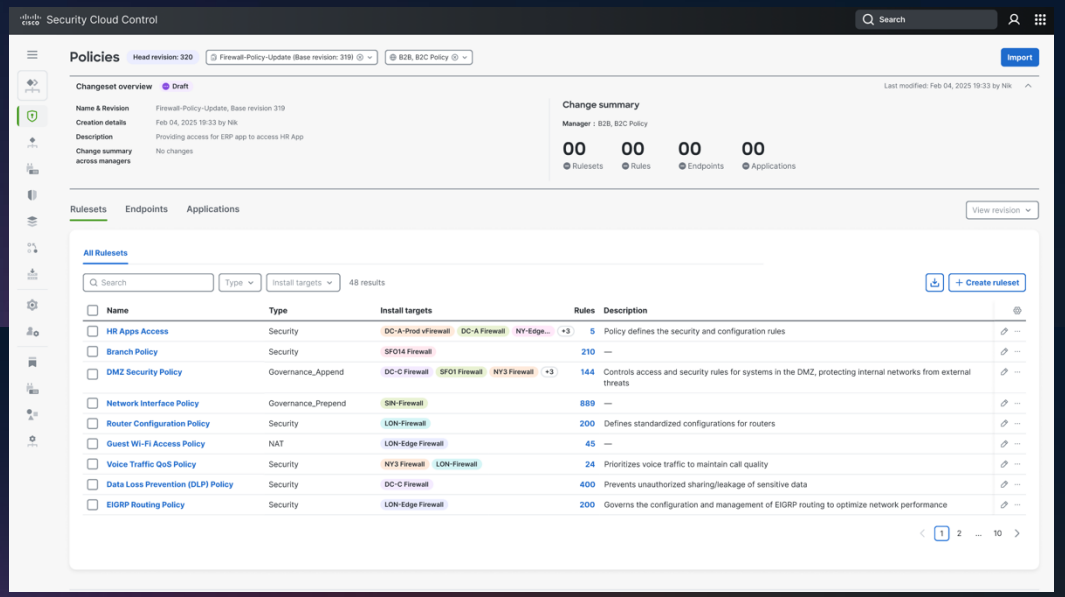
And deploy across Cisco and non-Cisco firewalls (Palo Alto, Fortinet, Juniper)

Deploy policy across network topology in minutes

Instead of translating policy across multiple vendor interfaces

Optimize rules and objects automatically

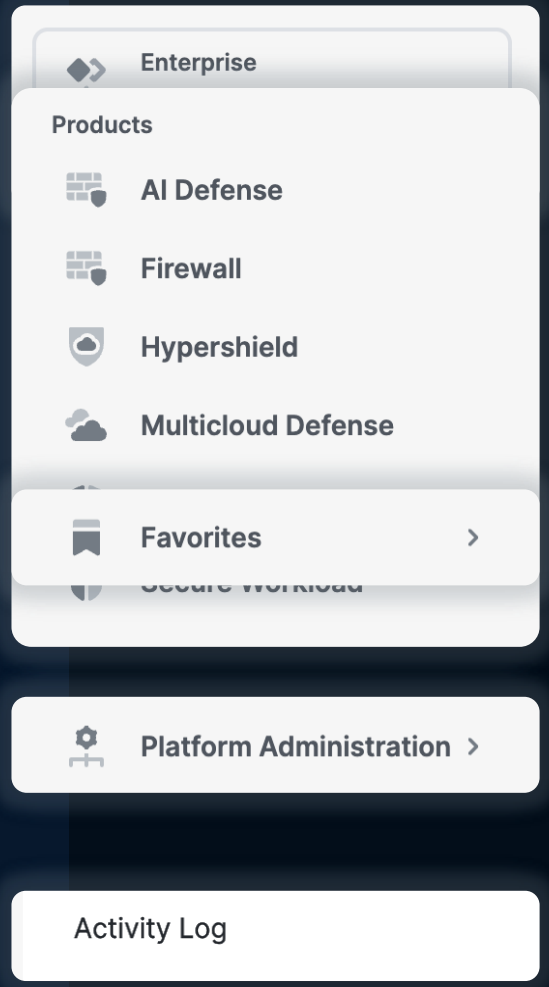
When deploying policy changes in Mesh Policy Engine



© 2025 Cisco and/or its affiliates. All rights reserved.

Security Cloud Control

- Manage all your organizations
- Access full product capabilities from single interface
- Personalize your admin experience
- Manage roles and groups across products
- Centralized audit log for compliance



Cisco Hybrid Mesh Firewall Capabilities & Design Principles

Secure Firewall Capabilities

Superior visibility beyond deep packet inspection

Security Intelligence

Encrypted Visibility Engine

Snort 3 with SnortML

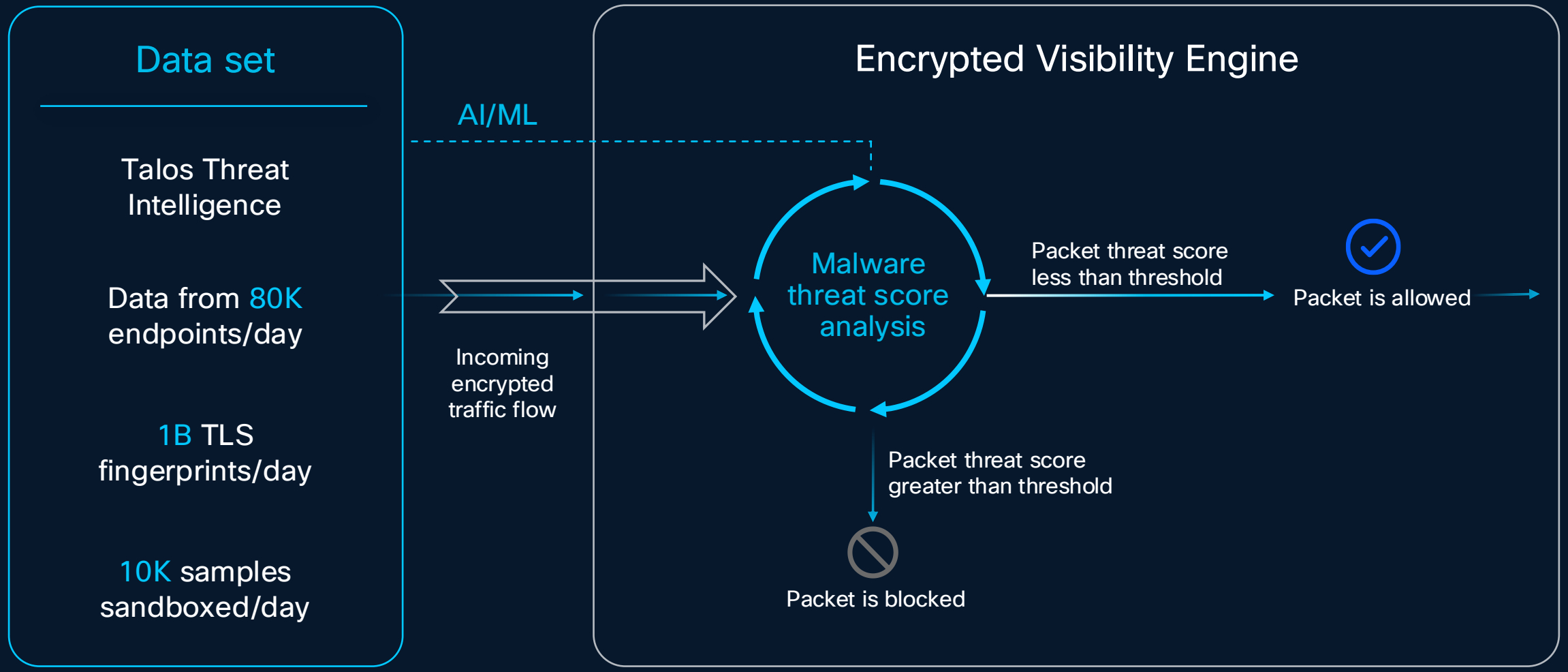
QUIC Decryption

Advanced Malware Protection

cisco

Secure Firewall Capabilities

Encrypted Visibility Engine (EVE) - Optimized for an encrypted world



Secure Firewall Capabilities

Intelligent Selective Decryption

Risk-based intelligent decryption bypass, powered by EVE and Talos Server Reputation

Post-quantum cryptography (PQC) ready

Firewall price-performance leader

Top to bottom

Branch — Campus — Data center — Cloud

NEW

200 Series

1 Model
Firewalling + IPS

Up to 1.5 Gbps

1200 Series

6 Models
Firewalling + IPS

Up to 18 Gbps

3100 Series

5 Models
Firewalling + IPS

Up to 45 Gbps

4200 Series

3 Models
Firewalling + IPS

Up to 140 Gbps

NEW

6100 Series

2 Models
Firewalling + IPS

Up to 570 Gbps

Public/Private

20+ cloud variants

HyperFlex
NUTANIX
KVM
openstack
vmware ESXi
aws
Microsoft Azure
Google Cloud Platform
alkira
rackspace technology.
EQUINIX
Alibaba Cloud
ORACLE CLOUD INFRASTRUCTURE

PQC will be included in Firewall Threat Defense 10.5 release

cisco

Cisco Live EMEA announcement

AVAILABLE DEC 2025

Advanced threat protection, delivered faster than ever

Firewall Threat Defense 10.0 software release

Security efficacy

Advanced visibility and control over encrypted traffic, including latest internet protocols and evasive activity

Faster access to threat and compliance insights in Splunk with Cisco Security Cloud app

Adaptive security policies for user behavior and risk with Cisco Identity Intelligence integration

Increased network resilience and segmented connectivity with encrypted security tags

Operational efficiency

Complete software upgrades 3x faster

Centralize management of 1500+ firewalls

Flexible, high-performance virtual and cloud security

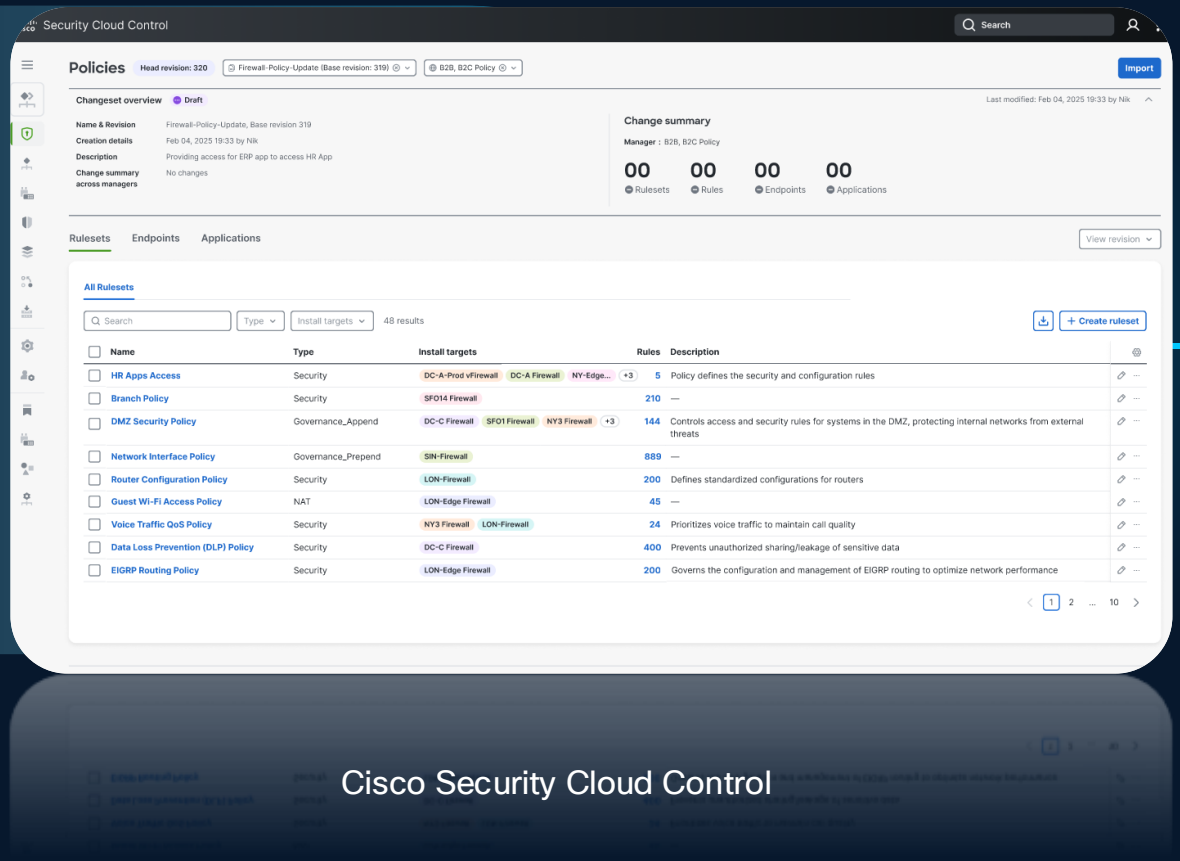
© 2025 Cisco and/or its affiliates. All rights reserved.

WATCH THE VIDEO WALKTHROUGH

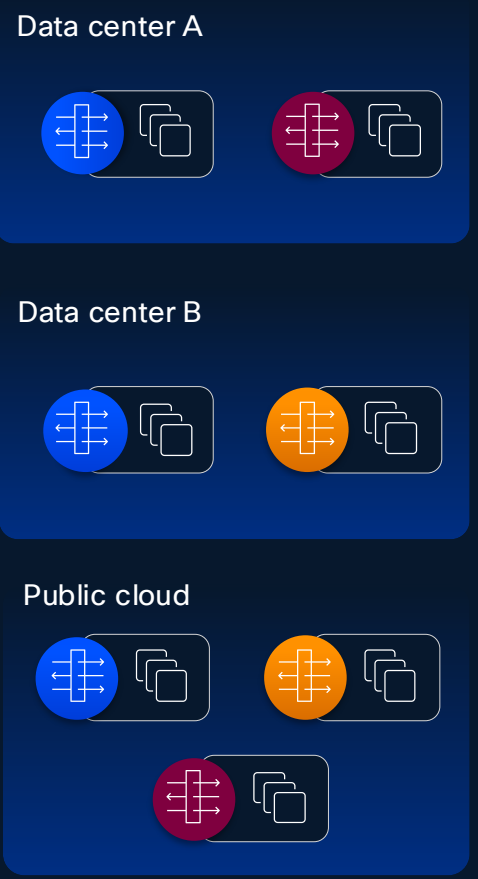
Mesh Policy Engine Capabilities

Extends policy to non-Cisco enterprise firewalls

- A policy manager (not a device manager or policy converter)
- Retain the “what” and “where” of the policy **and** the “why”
- Change enforcement points, not policy
- Cisco plus the other enterprise firewall vendors

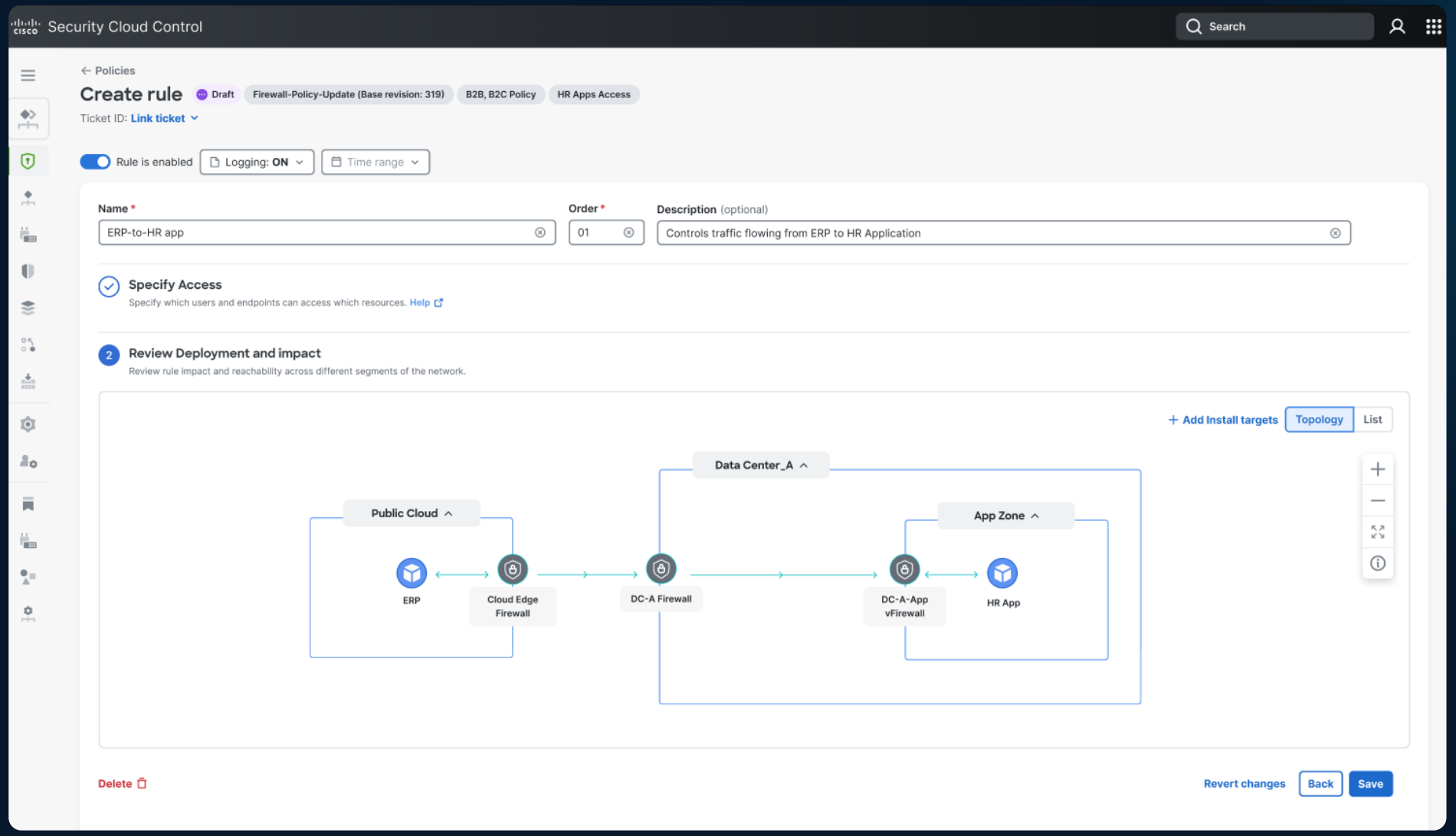


Cisco Security Cloud Control



Mesh Policy Engine Capabilities

Program once, enforce everywhere



Mesh Policy Engine understands your network topology to place the most effective policy on the relevant firewalls

1. Describe rule name and purpose
2. Define user and endpoint access
3. Deploy across network topology

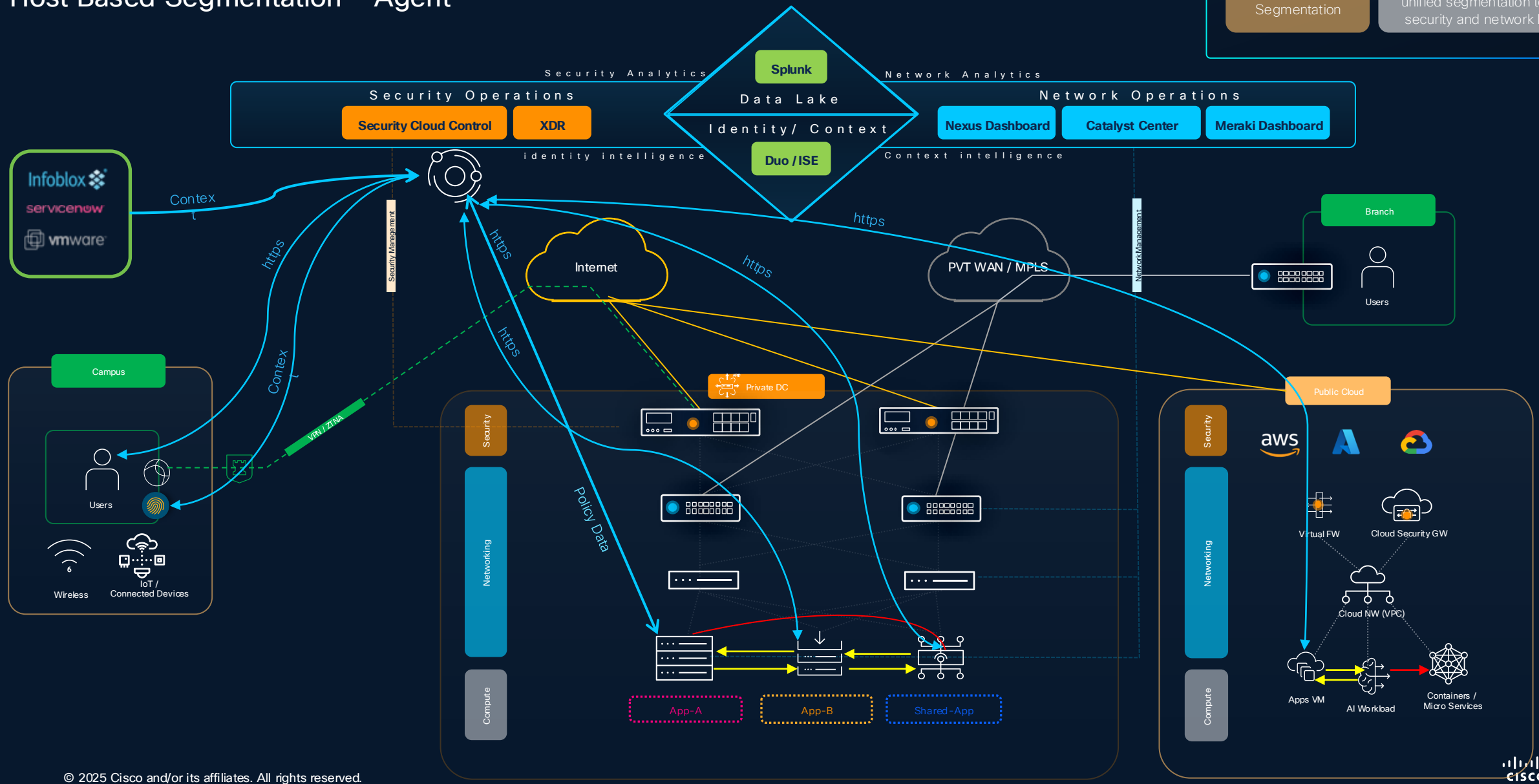
Mesh Policy Engine Demo

Secure Workload Capabilities

Host Based Segmentation - Agent

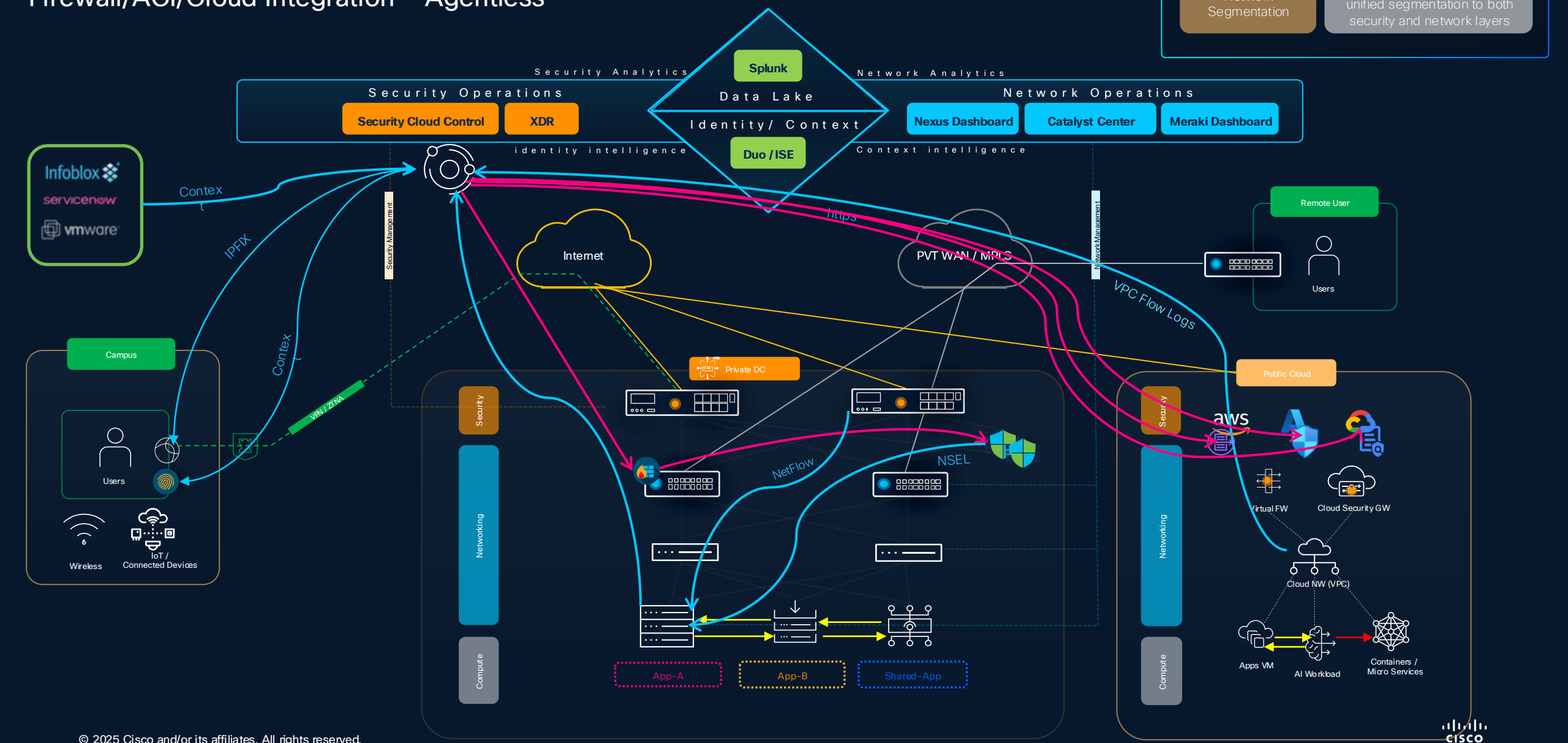
SECURITY OUTCOMES

- Network Segmentation
- Securely apply context aware unified segmentation to both security and network layers



Secure Workload Capabilities

Firewall/ACI/Cloud Integration – Agentless



Hypershield Capabilities

Only Hypershield fuses security into....

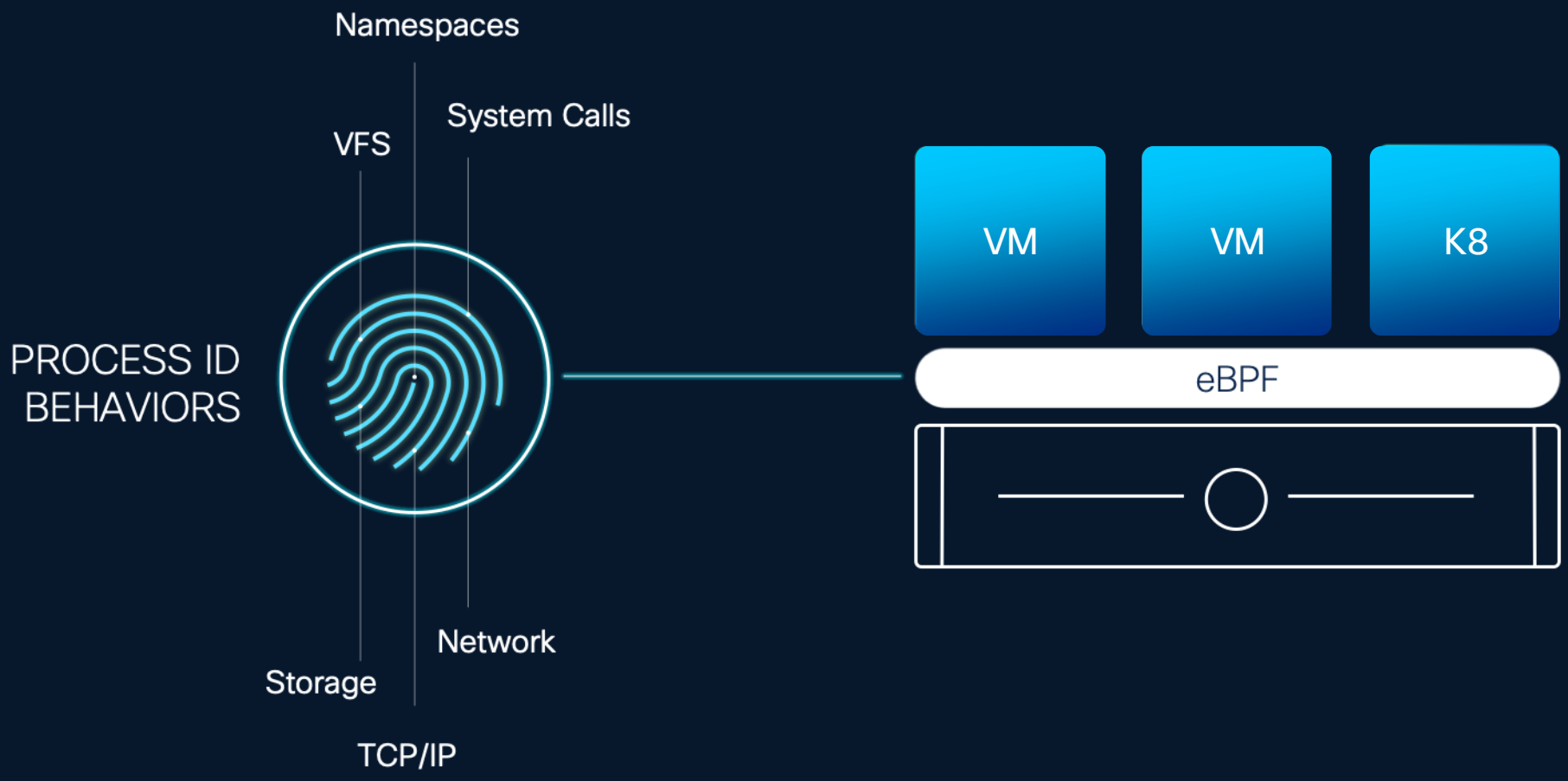
the Network & the Workload

Eliminates east/west security blind spots in the datacenter with no changes to application workloads

Adds deep application awareness and extends east/west security to the public cloud and Kubernetes

Hypershield Capabilities

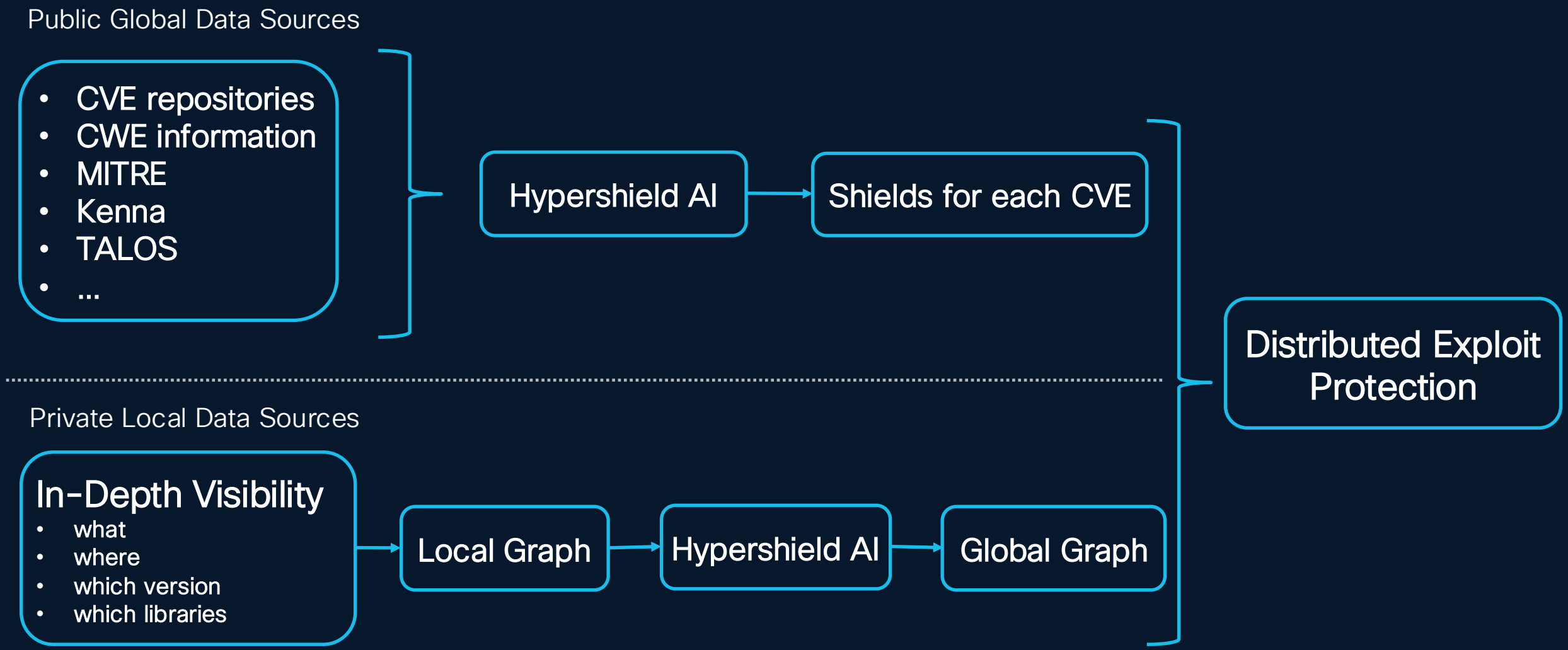
eBPF Provides Visibility Deep into the Workload



Check out “eBPF Unlocking the Kernel”

Hypershield Capabilities

Distributed Exploit Protection



Hypershield Capabilities

Nexus Smart Switch

Cisco Nexus 9000 Smart Switch

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

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

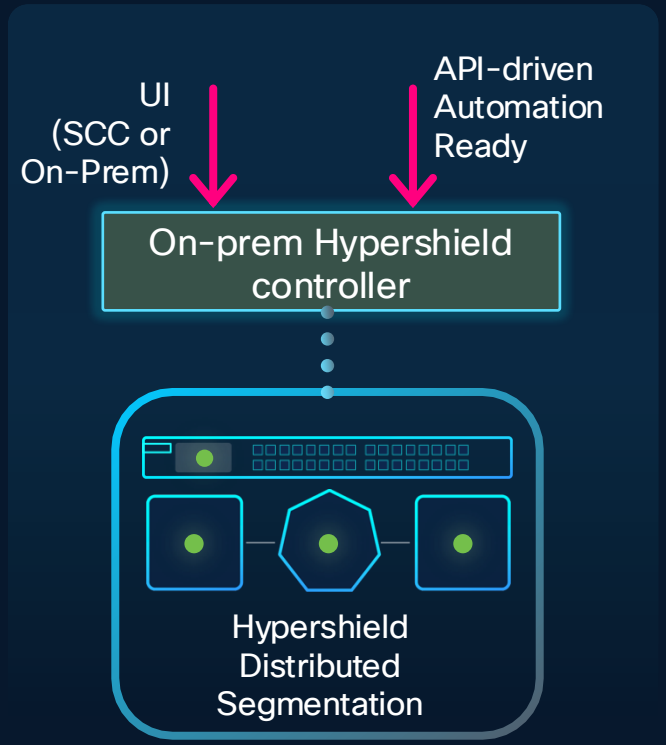
Large-Scale NAT | IPSEC Encryption | Distributed Firewall | Event-Based Telemetry | DoS Protection

Hypershield Capabilities

Nexus Smart Switch

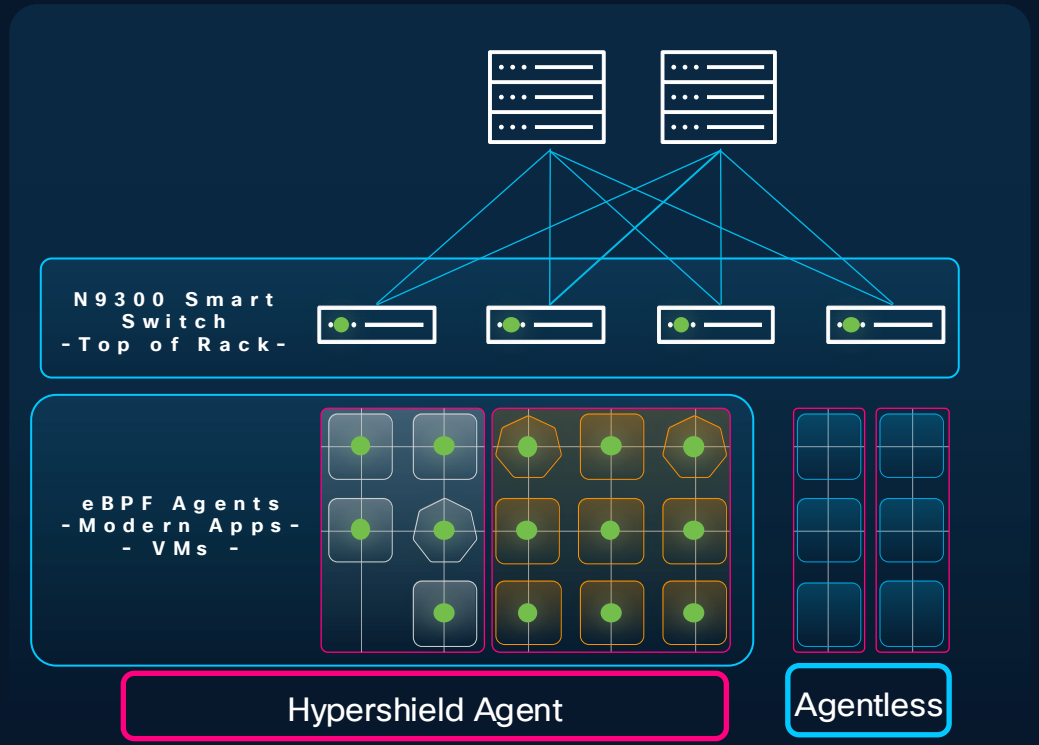
Hypershield Capabilities

Distributed Segmentation Architecture



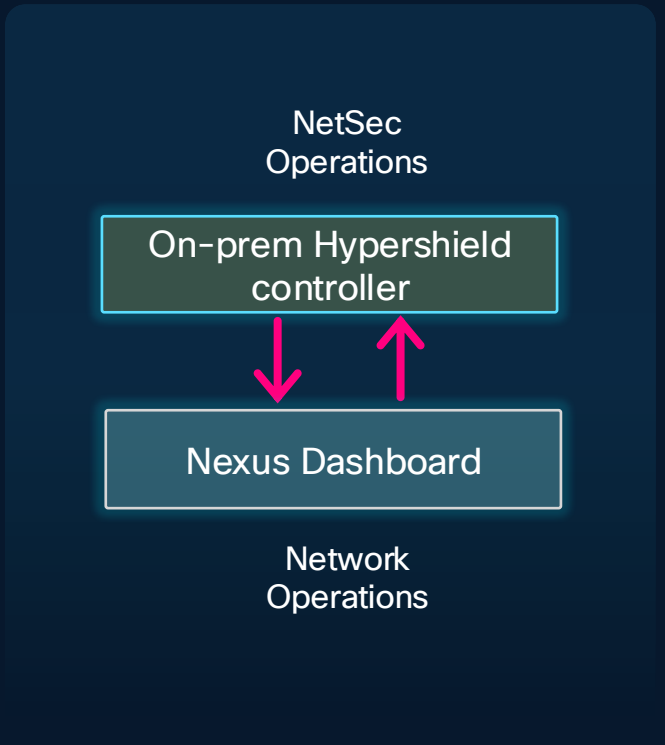
Global Control

Unified visibility and global policy across agents and smart switch



Distributed

Eliminate blind spots with fully distributed enforcement
– Inline everywhere, kernel and network fabric –



Unified operations

Separation of control with combined operations and troubleshooting

New Standards for AI Security

OWASP

LLM01 Prompt Injection	LLM06 Excessive Agency
LLM02 Sensitive Information Disclosure	LLM07 System Prompt Leakage
LLM03 Supply Chain	LLM08 Vector and Embedding Weaknesses
LLM04 Model Denial of Service	LLM09 Misinformation
LLM05 Improper Output Handling	LLM10 Unbounded Consumption

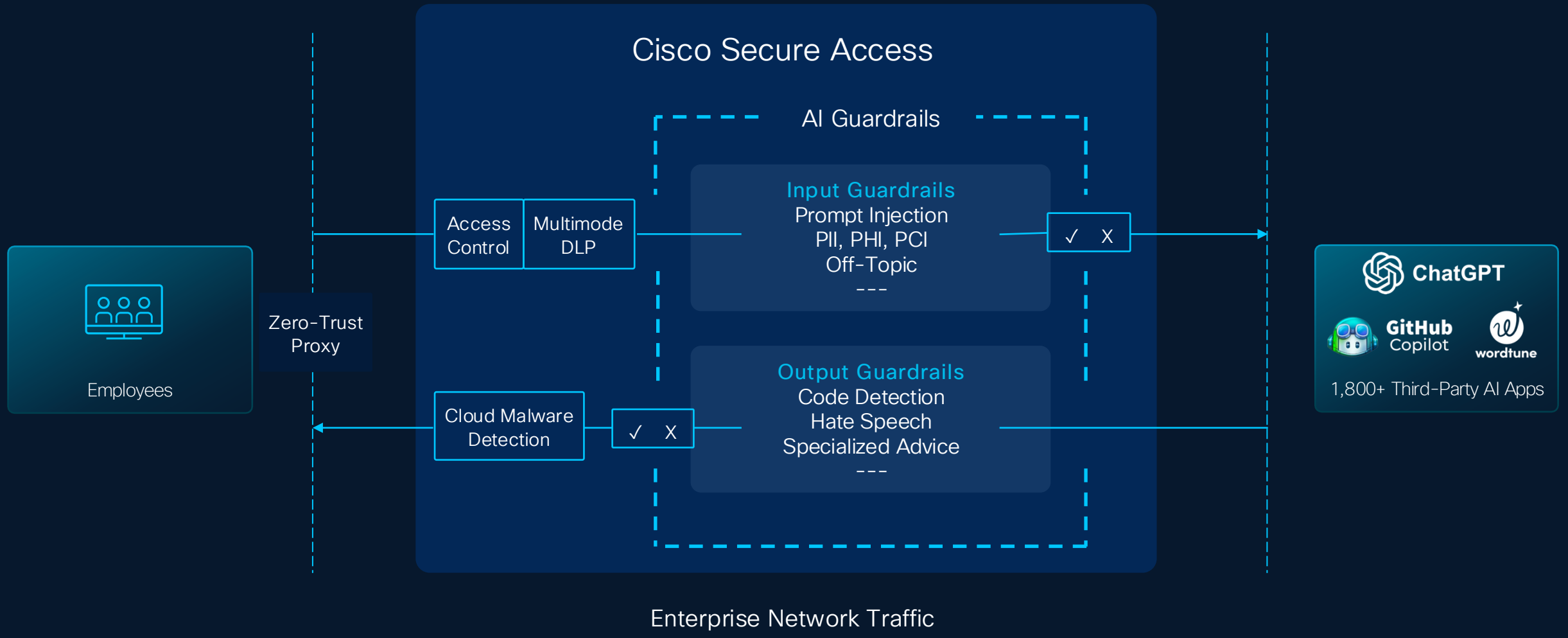
MITRE ATLAS

AI Defense Capabilities

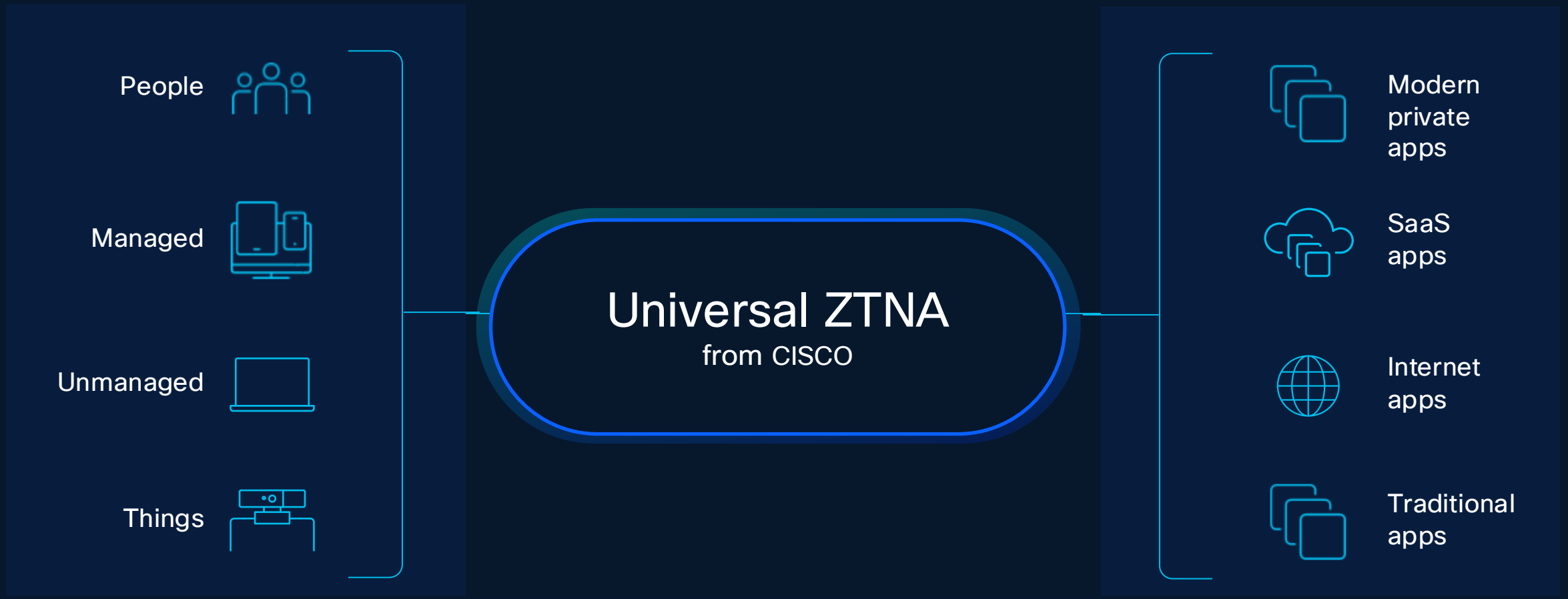
Model Protection, Flexible Enforcement Options

Secure Access Capabilities

Third Party AI App Protection – AI Access Policies



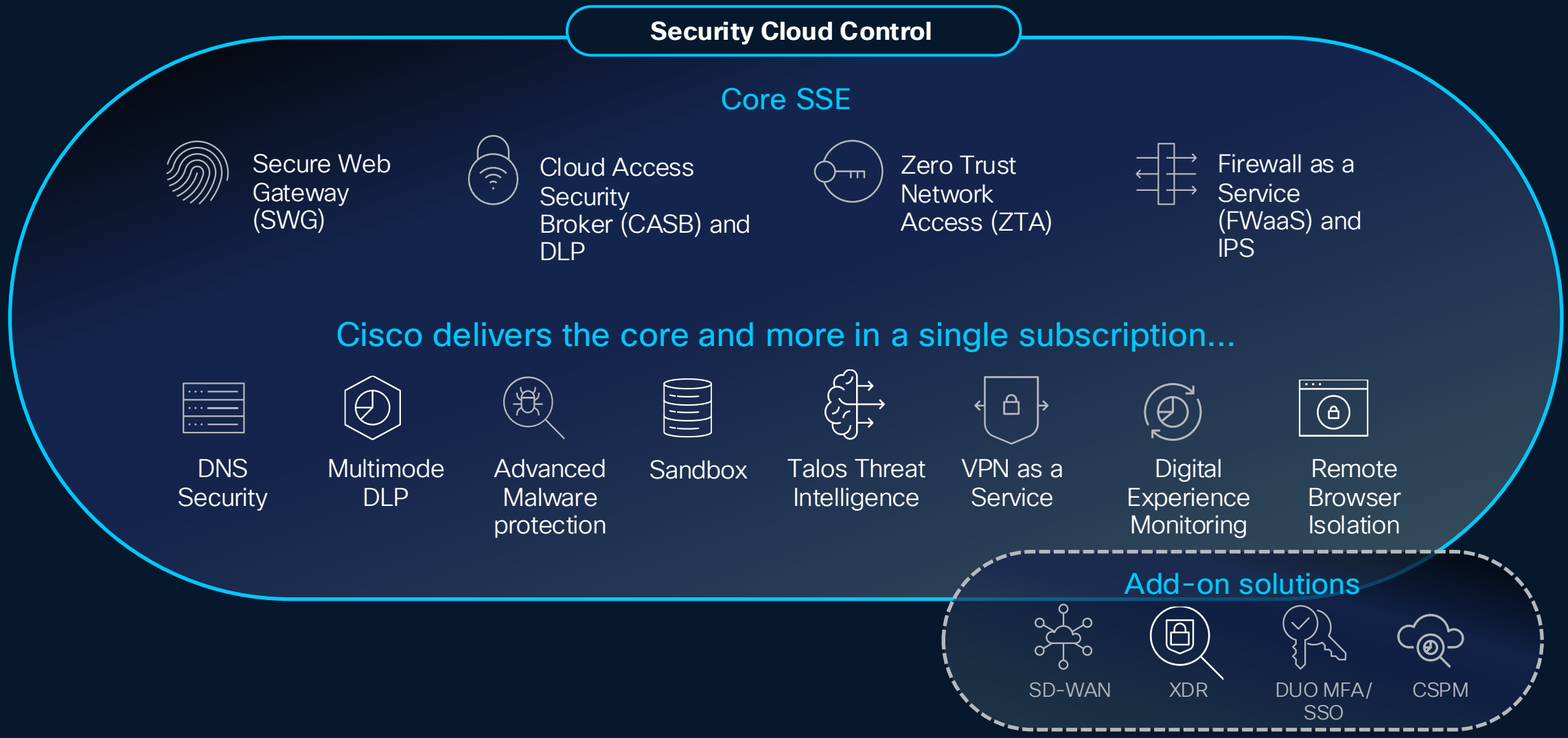
Secure Access Capabilities



There is no universal zero trust
without ubiquitous, shared identity across the enterprise

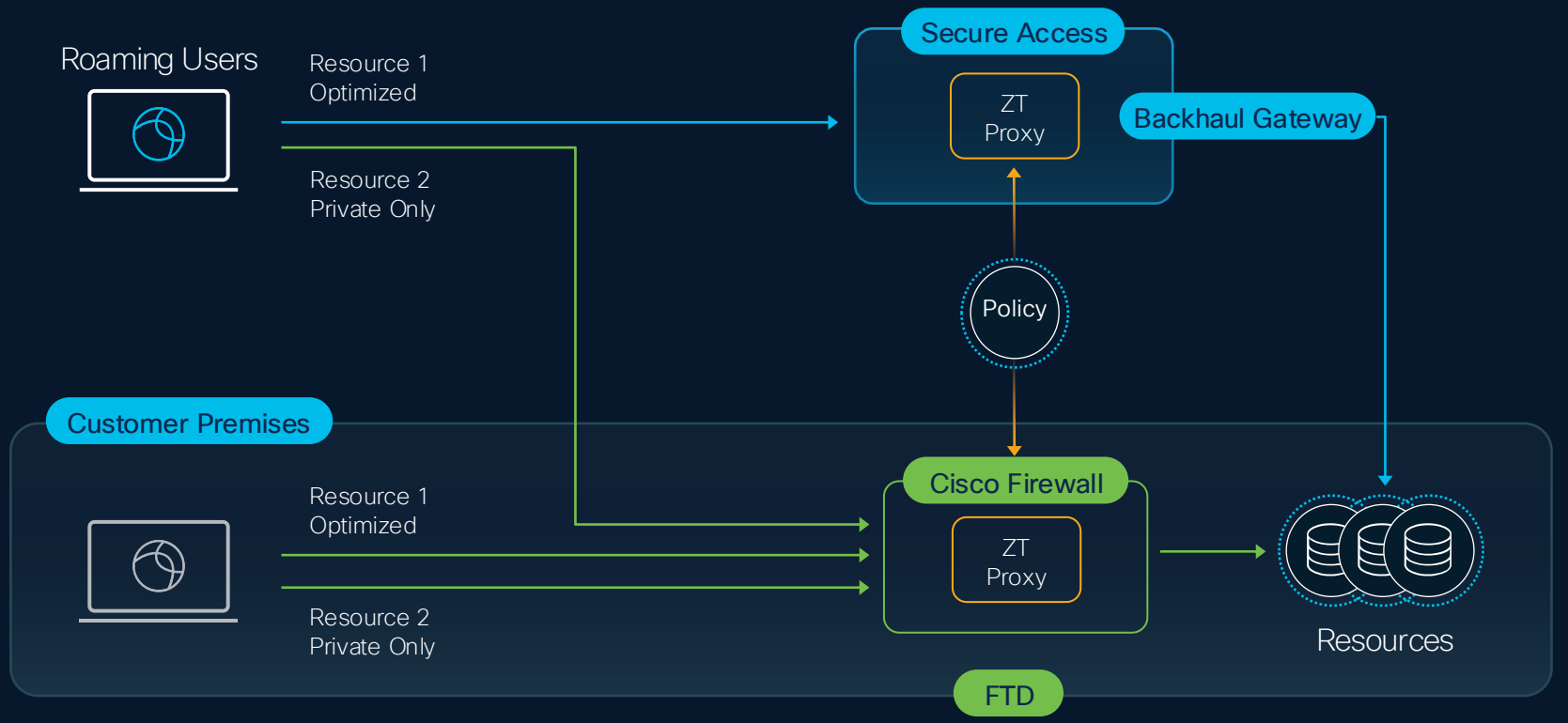
Cisco Secure Access Capabilities

Go beyond core Secure Service Edge (SSE) to better connect and protect your business



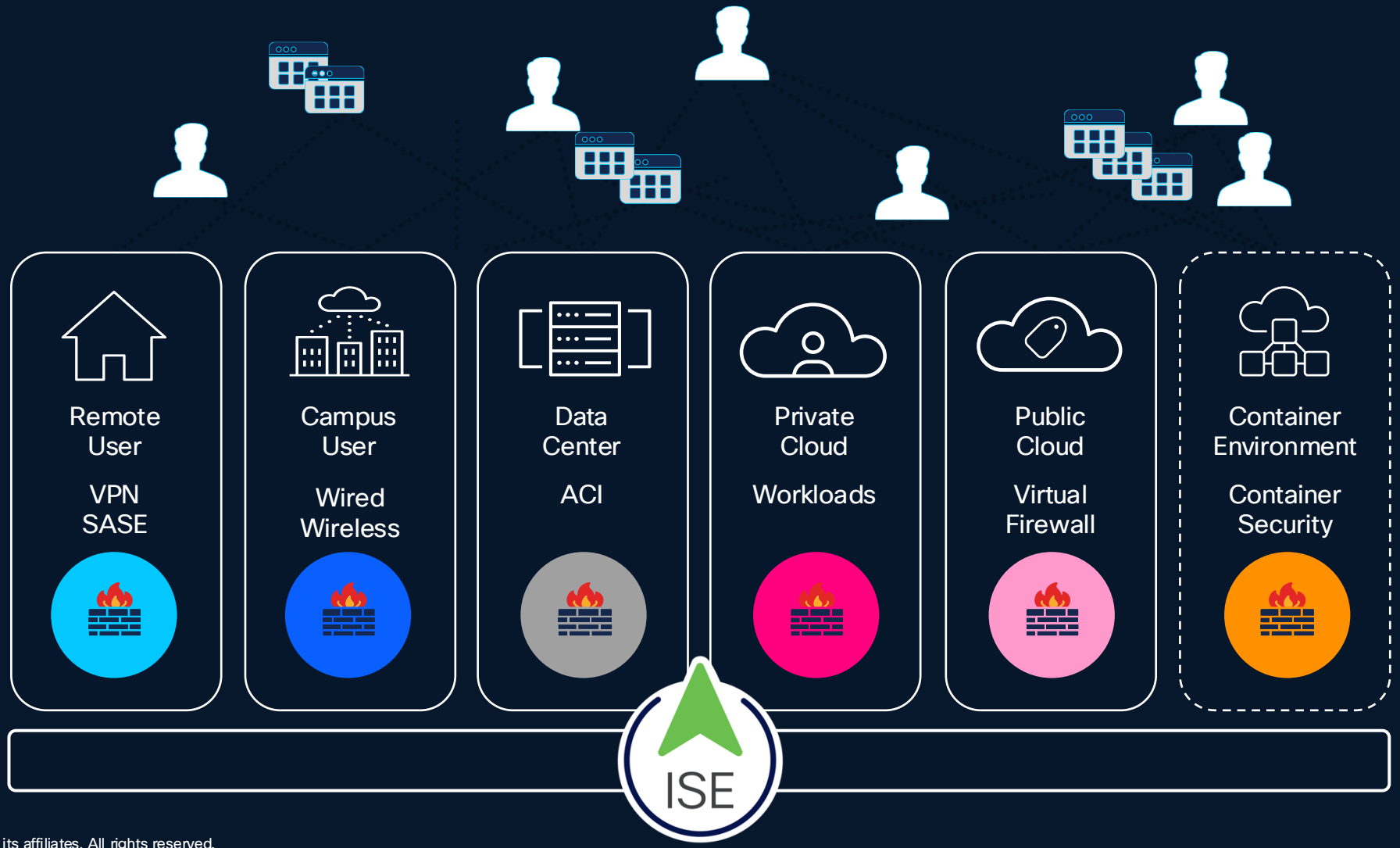
Secure Access Capabilities

Hybrid Private Access Leveraging Cisco Firewalls



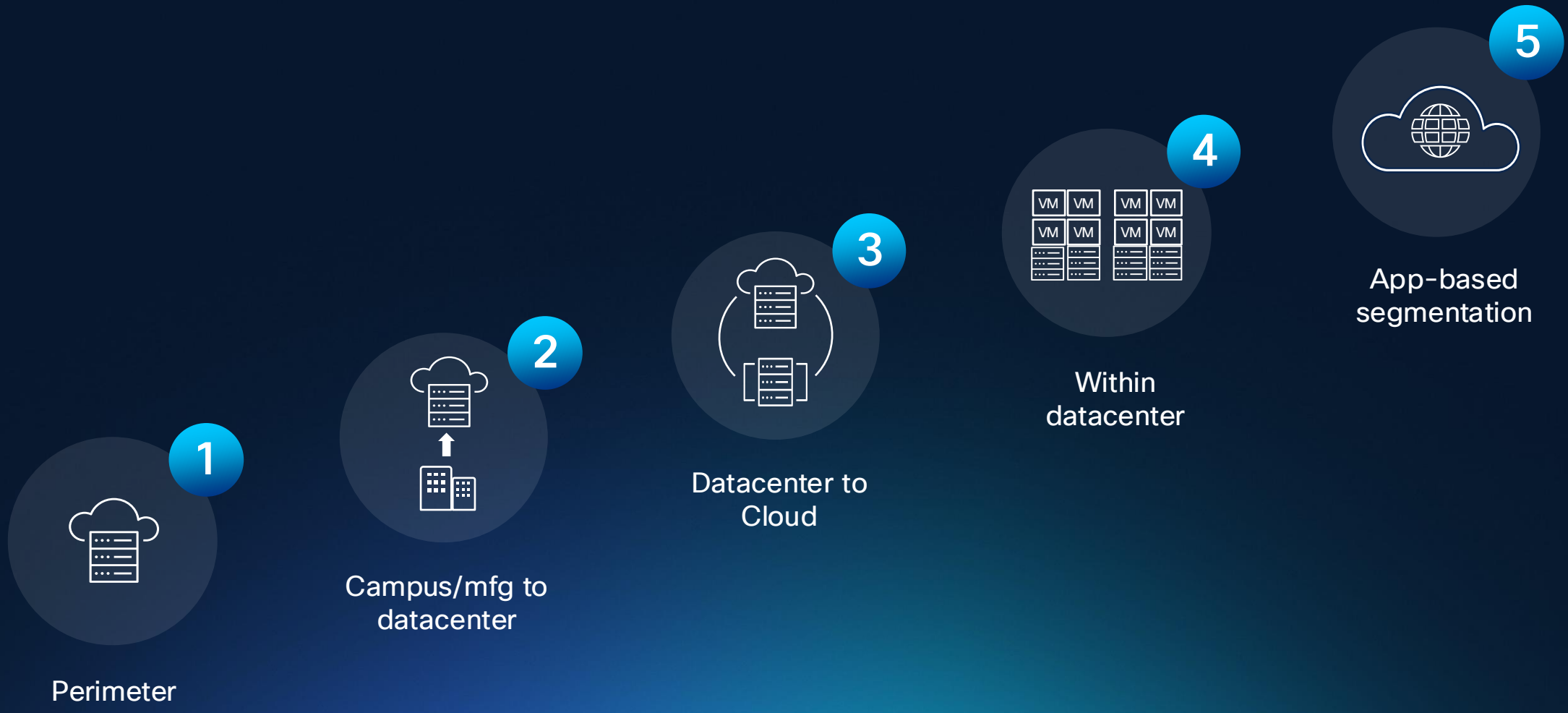
Common Policy with Security Group Tags (SGTs)

The common context across Security Cloud Control



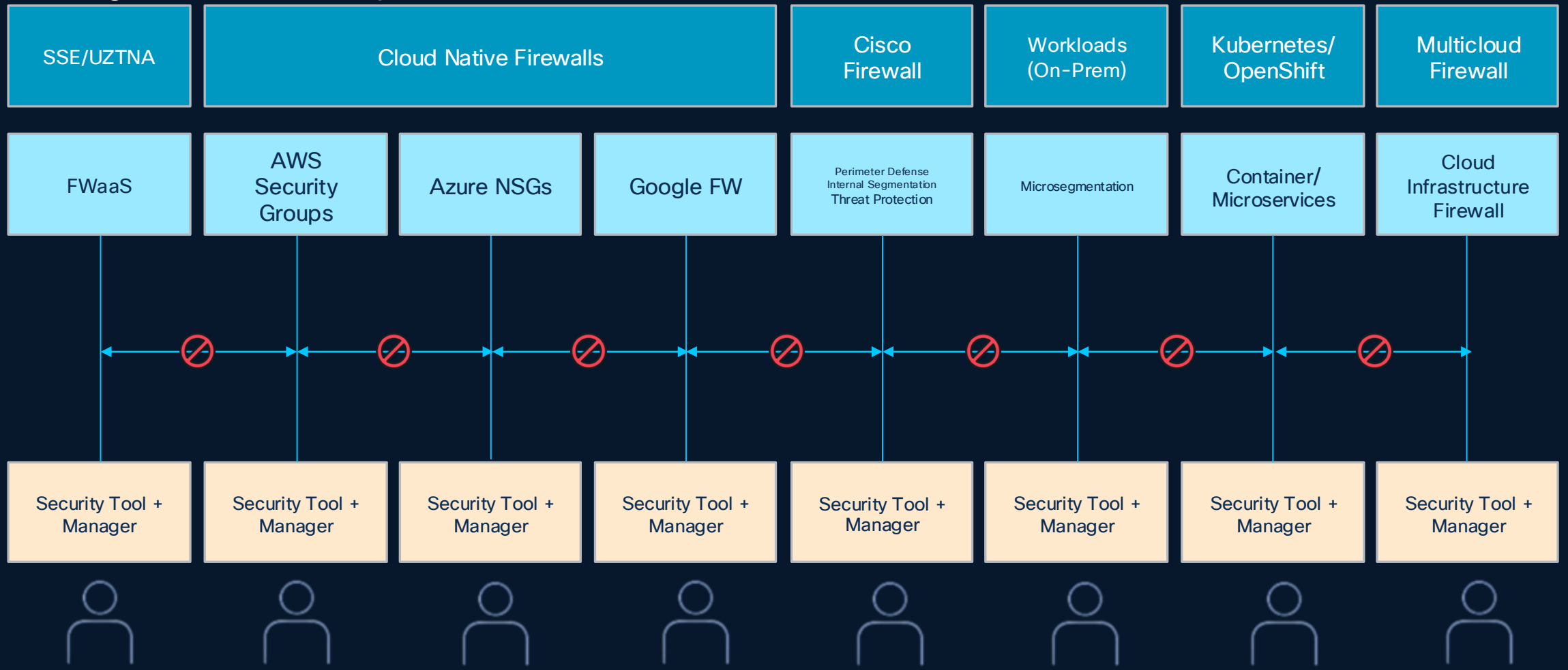
Key Takeaways

Segmentation that meets you where you are



Customer Example

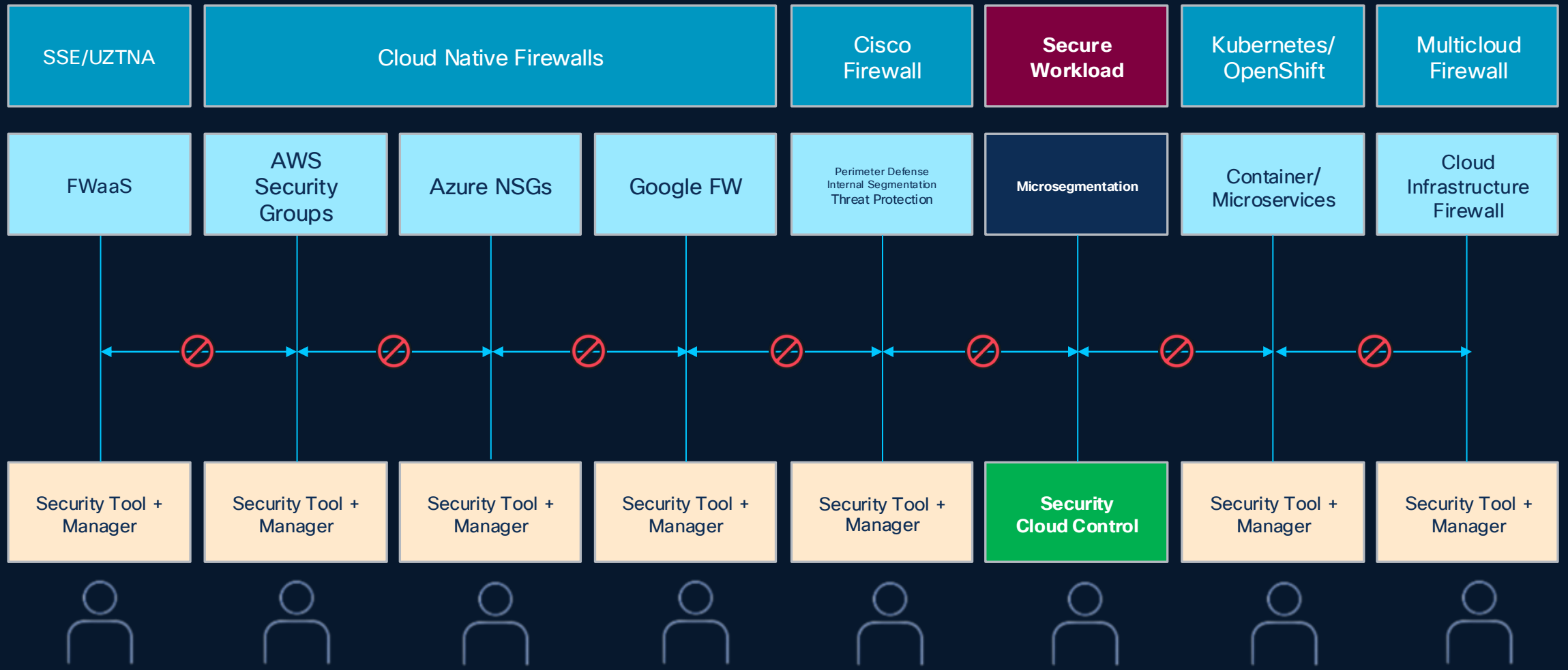
Microsegmentation for Compliance



cisco

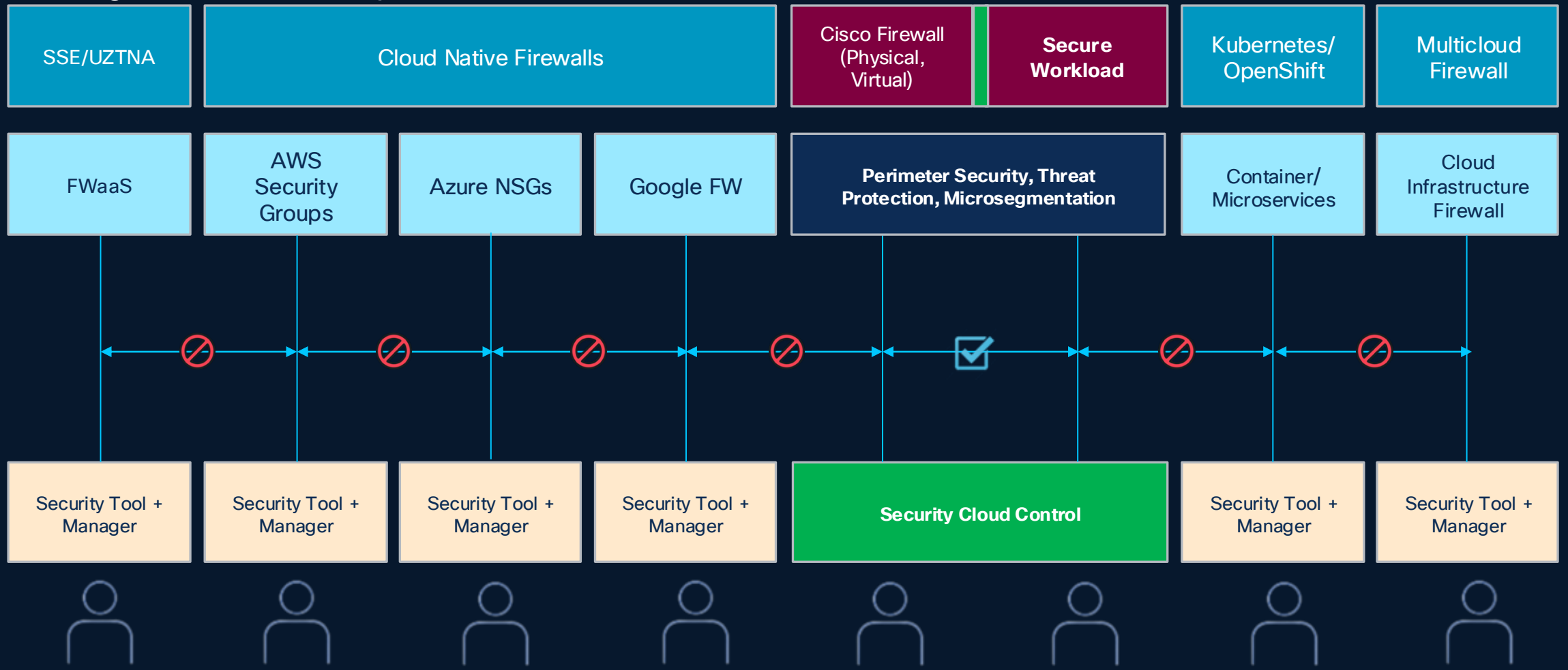
Customer Example

Microsegmentation for Compliance



Customer Example

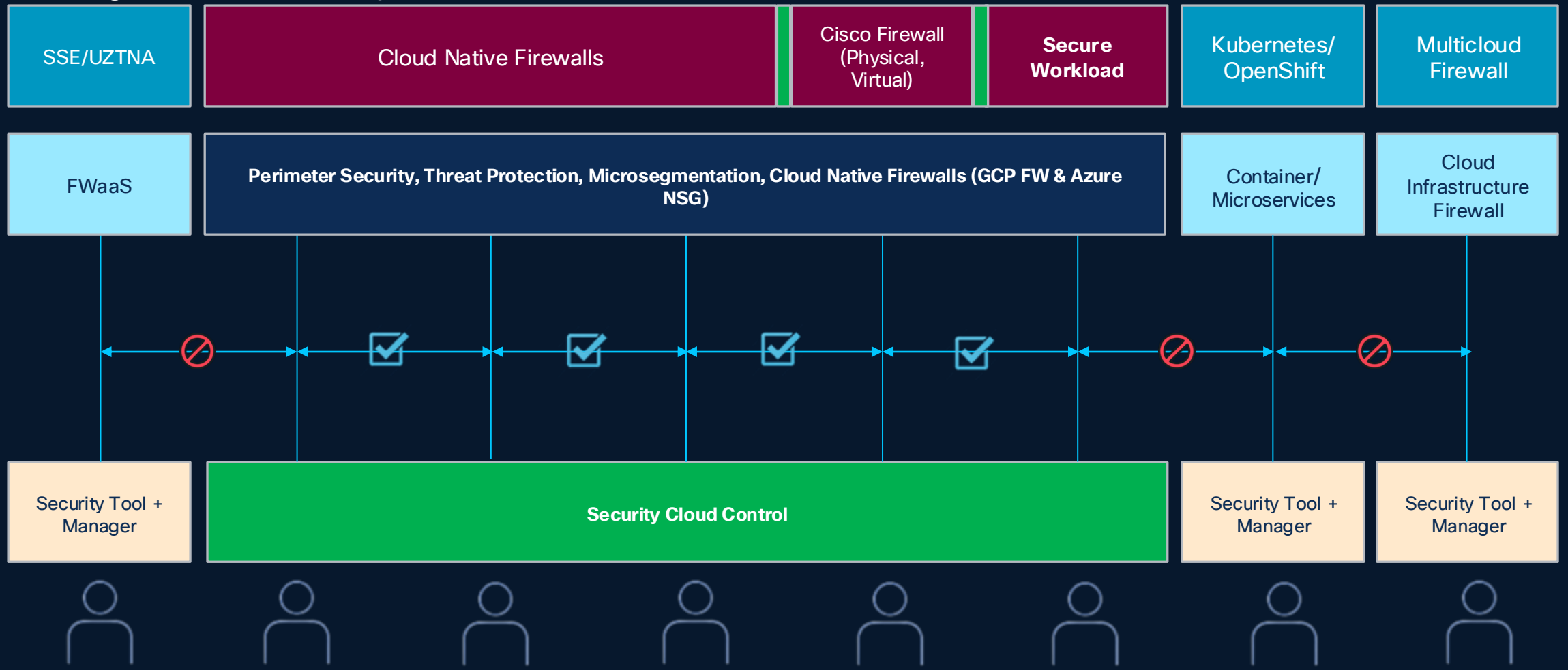
Microsegmentation for Compliance



cisco

Customer Example

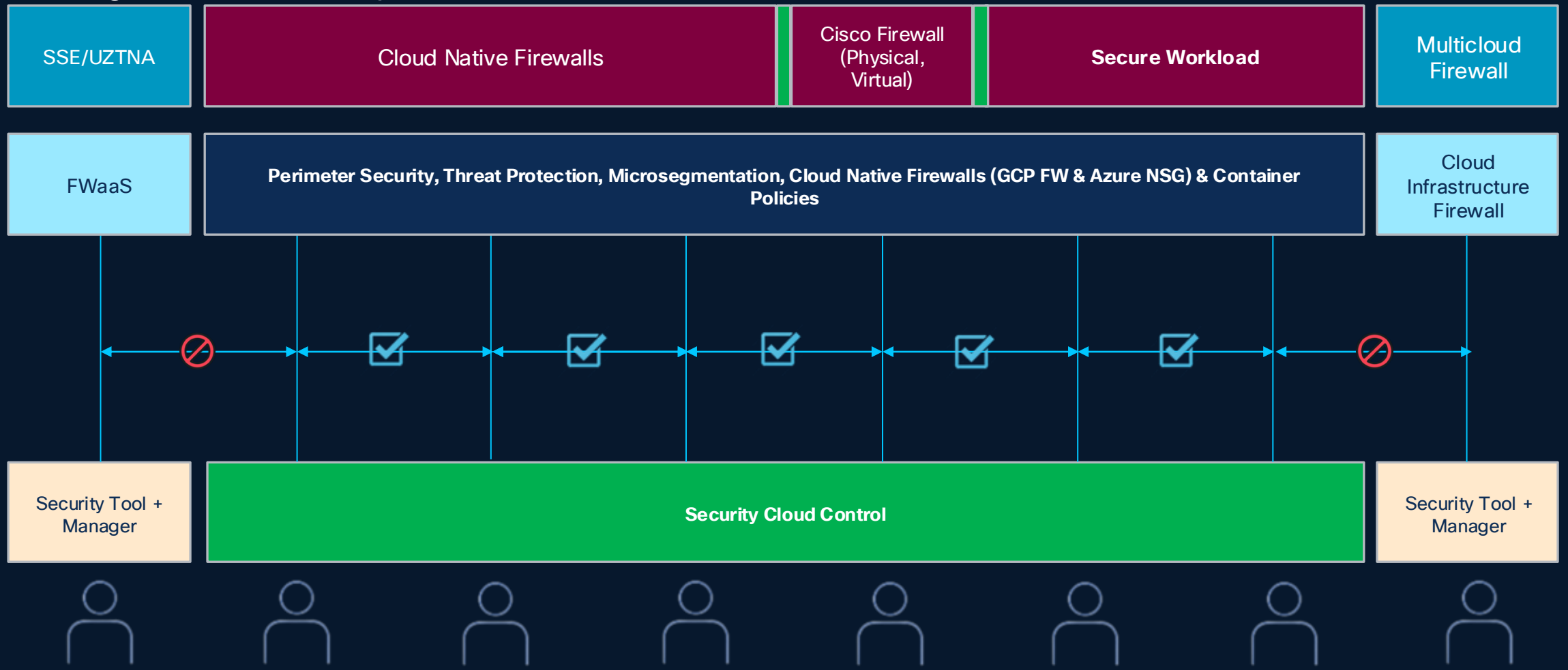
Microsegmentation for Compliance



cisco

Customer Example

Microsegmentation for Compliance



cisco

Simple, future-proof licensing

Cloud Protection Suite

Gateways

- Secure Firewall
- Multicloud Defense

Workloads

- Secure Workload
- Isovalent Enterprise
- Hypershield

Thank you