

Zero Trust for Cloud & Beyond with Cisco Hybrid Mesh Firewall

cisco Live !

Nadir Lakhani

Technical Solutions Architect – Hybrid Mesh, Workload & Cloud Security

Session ID: BRKSEC-2787

Cisco Webex App

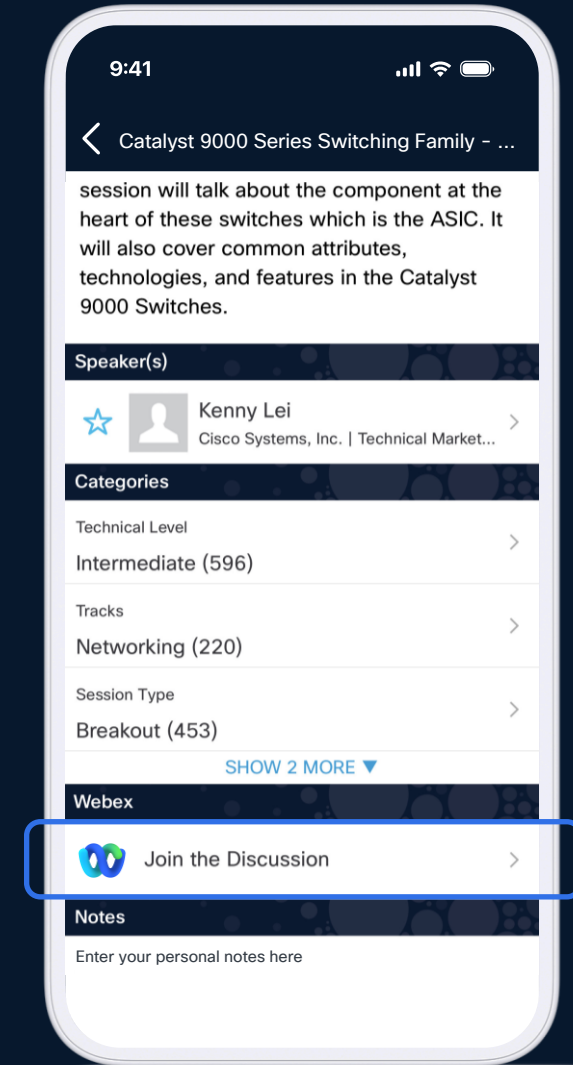
Questions?

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 14 November 2025.



<https://ciscolive.ciscoevents.com/ciscolivebot/#BKRSEC-2787>

About Me

Nadir Lakhani

Almost 25 years in the industry, more than half spent at Cisco :)

Started off as an SE in 2012, then moved to Incubation in 2014 – Since then worked on many new products such ACI, Tetration (Secure Workload), Argento (Secure Apps) & Hypershield.

Currently I am working on building the next generation of security with Cisco Hypershield & Hybrid Mesh Firewall.

I am a husband & father and live in Canada with my wife and 3 kids.

Outside of Cisco technical world, I love traveling, exploring new food, and an ardent cricket lover. I grew up watching Waugh Brothers!!



Agenda

- 01 Session Objective
- 02 Industry Perspective: The Evolution of Hybrid Security
- 03 Cisco's Hybrid Mesh Firewall: Vision & Foundation
- 04 Cisco's Hybrid Mesh Firewall: Architecture
- 05 Capabilities & Design Principles
- 06 Real-World Customer Use Cases
- 07 Key Takeaways
- 08 Q&A

Session Objective

Learning Objectives

**Understand the
Evolution of Hybrid
Security**

**Explore Cisco's
Vision and
Architecture for
the Hybrid Mesh
Firewall**

**Examine Core
Capabilities and
Design Principles**

**Analyze Real-
World Use Cases
and Practical
Applications**



Industry Perspective: The Evolution of Hybrid Security

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

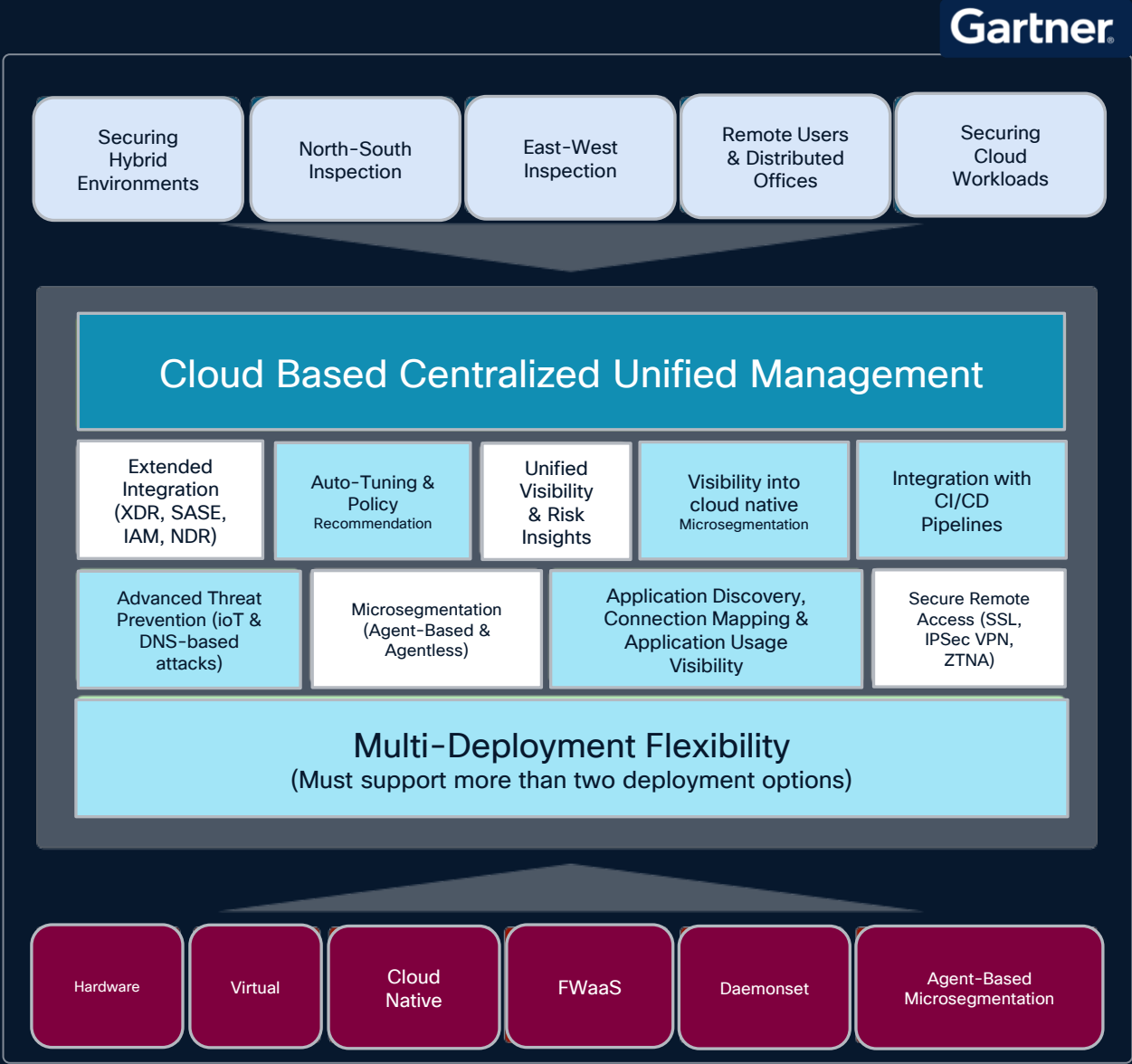
Gartner

Market Guide for Hybrid Mesh Firewall Platforms

Published 16 January 2024 - ID G00794201 - 15 min read

By Analyst(s): Rajpreet Kaur, Adam Hills

Initiatives: Infrastructure Security; Build and Optimize Cybersecurity Programs



Hybrid Mesh Firewall – Why the need?



Network



Private DC



Cloud



Cloud-Native

Organizational Challenges



NetSec Admin



Server/VM Admin



Cloud Architect



DevSecOps

Multiple teams,
organizations and
environments



Inconsistent islands
of policy controls
across
environments





Cisco's Hybrid Mesh Firewall: Vision & Foundation

Cisco's Vision – Hybrid Mesh Firewall

Our North Star

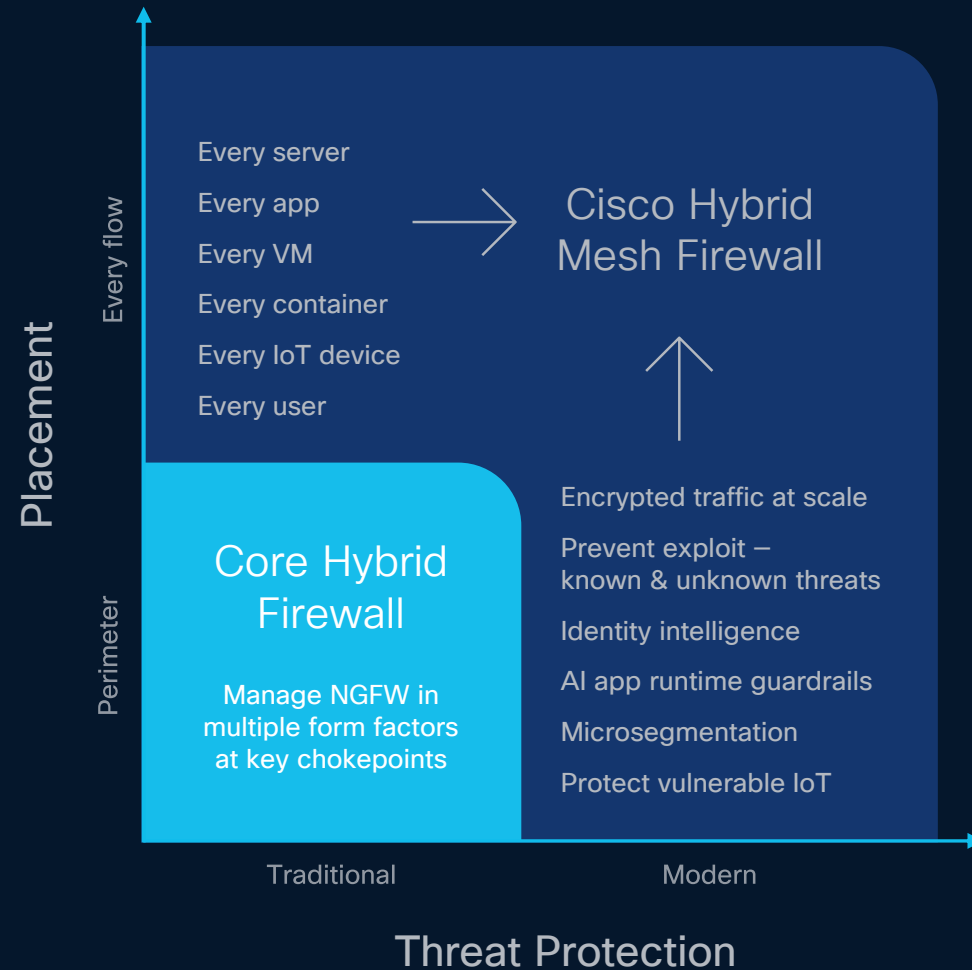
Make it easy for organizations to

Reduce attack surface

Prevent compromise

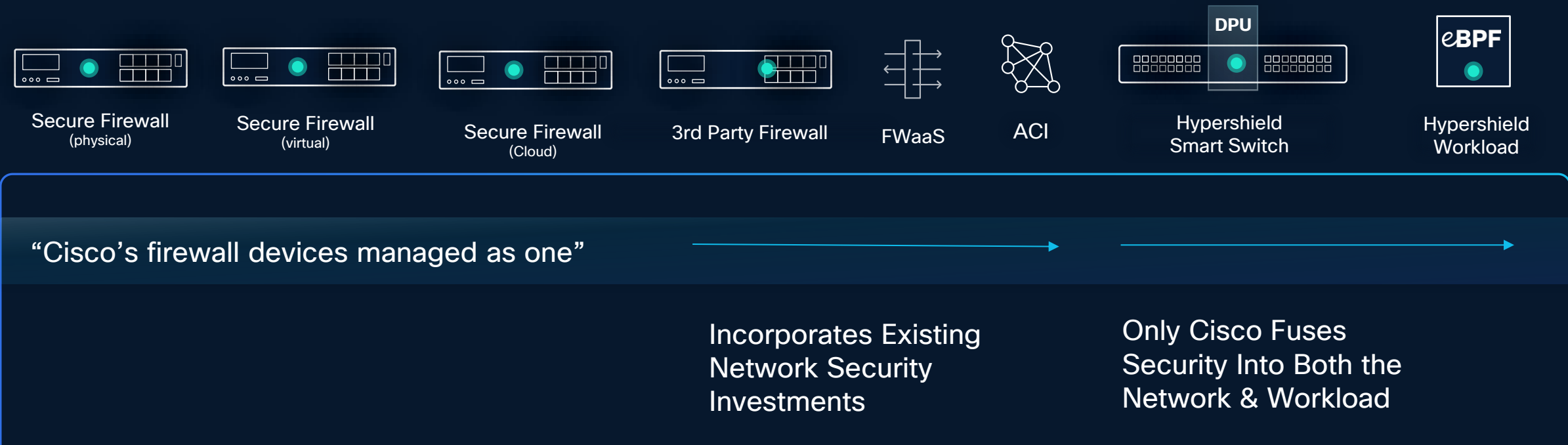
Stop lateral movement

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



Cisco Hybrid Mesh Firewall Goes Deeper & Broader

SECURITY CLOUD CONTROL



Write policy once, enforce across the mesh

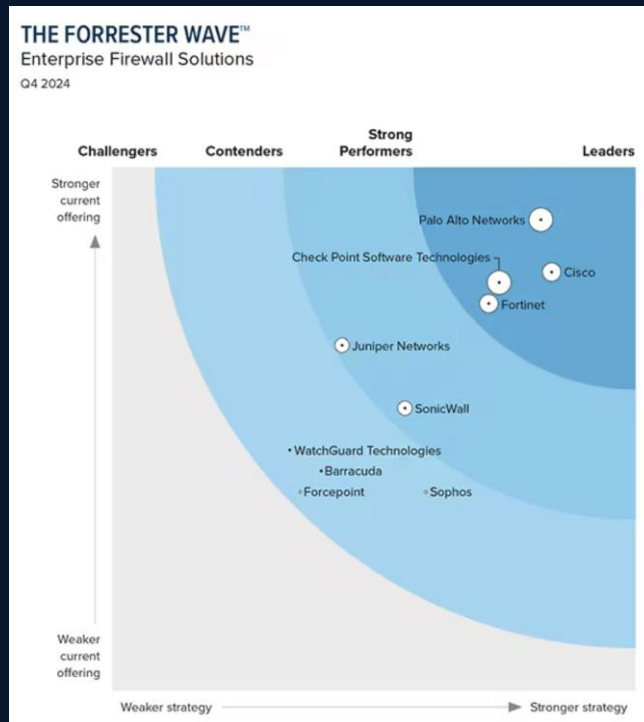
BRKSEC-2787



FORRESTER®

2024 Forrester Wave: Enterprise Firewall Solutions

LEADER



IDC

2025 IDC MarketScape: Worldwide Enterprise Hybrid Firewall

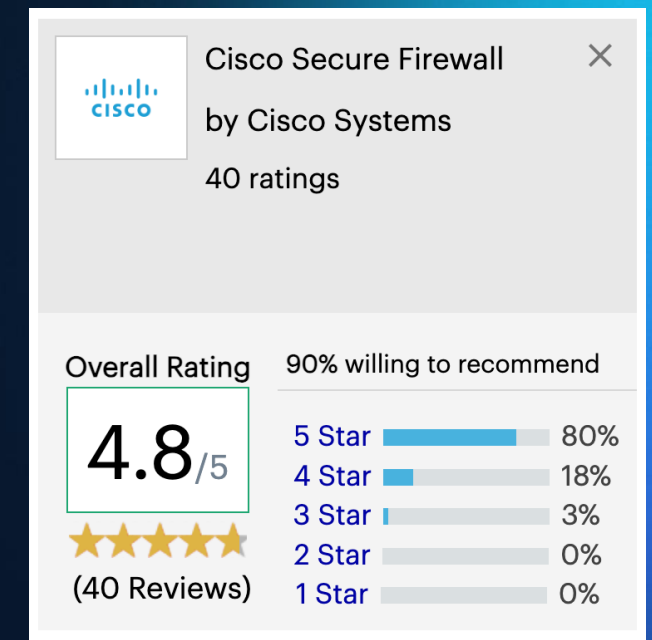
LEADER



Gartner
Peer Insights™

Network Firewalls

SCORE LEADER*



* Vs Palo Alto Networks 4.6, Fortinet 4.7. All scores for last 12 months as of Aug 19, 2025.

The background of the slide is a dark blue field filled with dynamic, flowing light streaks in various shades of blue and a hint of orange. These streaks create a sense of motion and depth, resembling light trails or data flow.

Cisco's Hybrid Mesh Firewall: Architecture

Security Cloud Control

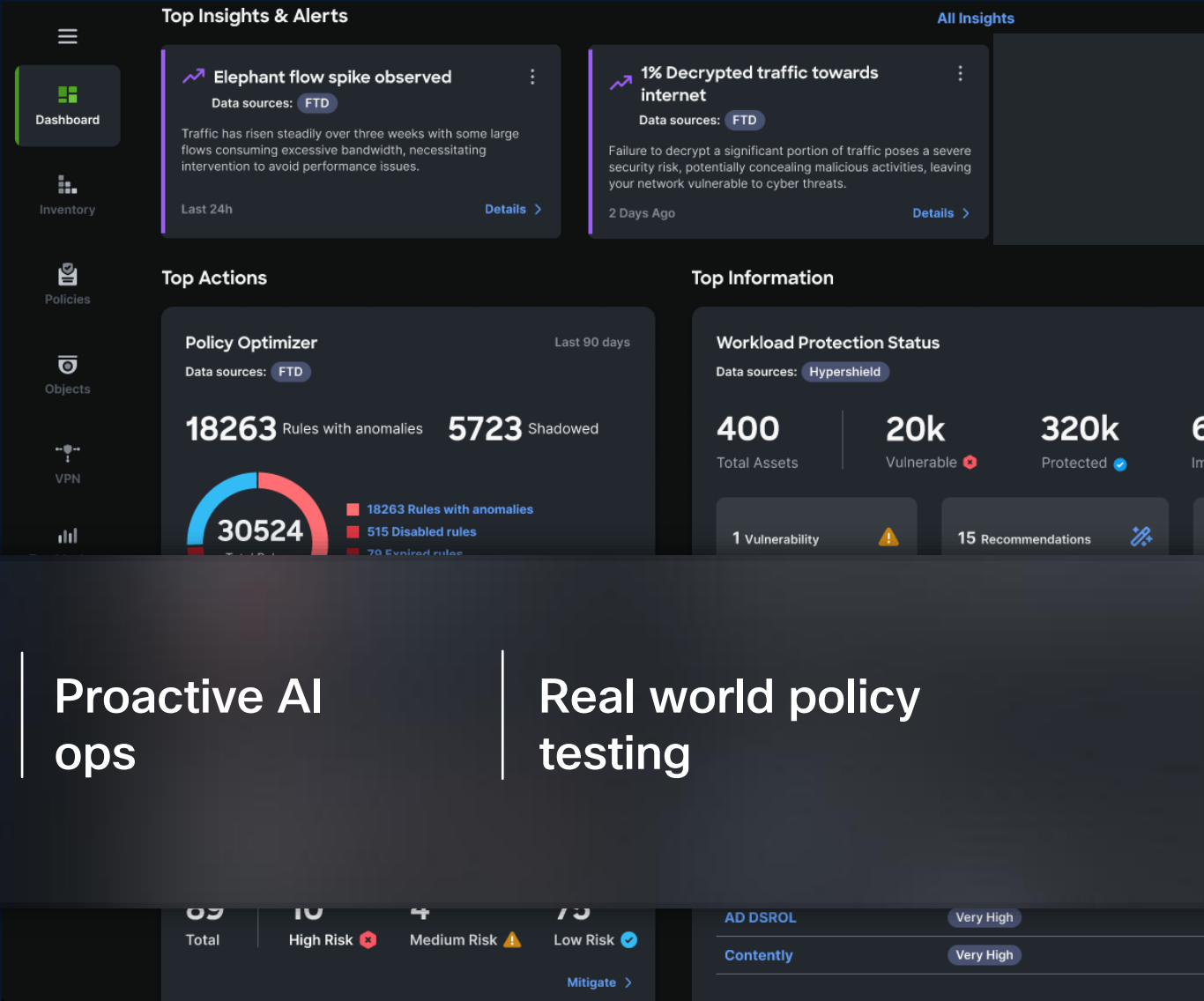
Simplify policy administration
by up to 70%



AI assistance
for policy

Proactive AI
ops

Real world policy
testing



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



Enterprise
**Stark Enterprises -
North America**



Products



AI Defense



Firewall



Hypershield



Multicloud Defense



Secure Access



Secure Workload



Favorites



Platform Administration



Activity Log

Capabilities & Design Principles

Secure Firewall Capabilities

Superior visibility beyond deep packet inspection



Security
Intelligence



Encrypted
Visibility Engine



Snort 3
with SnortML



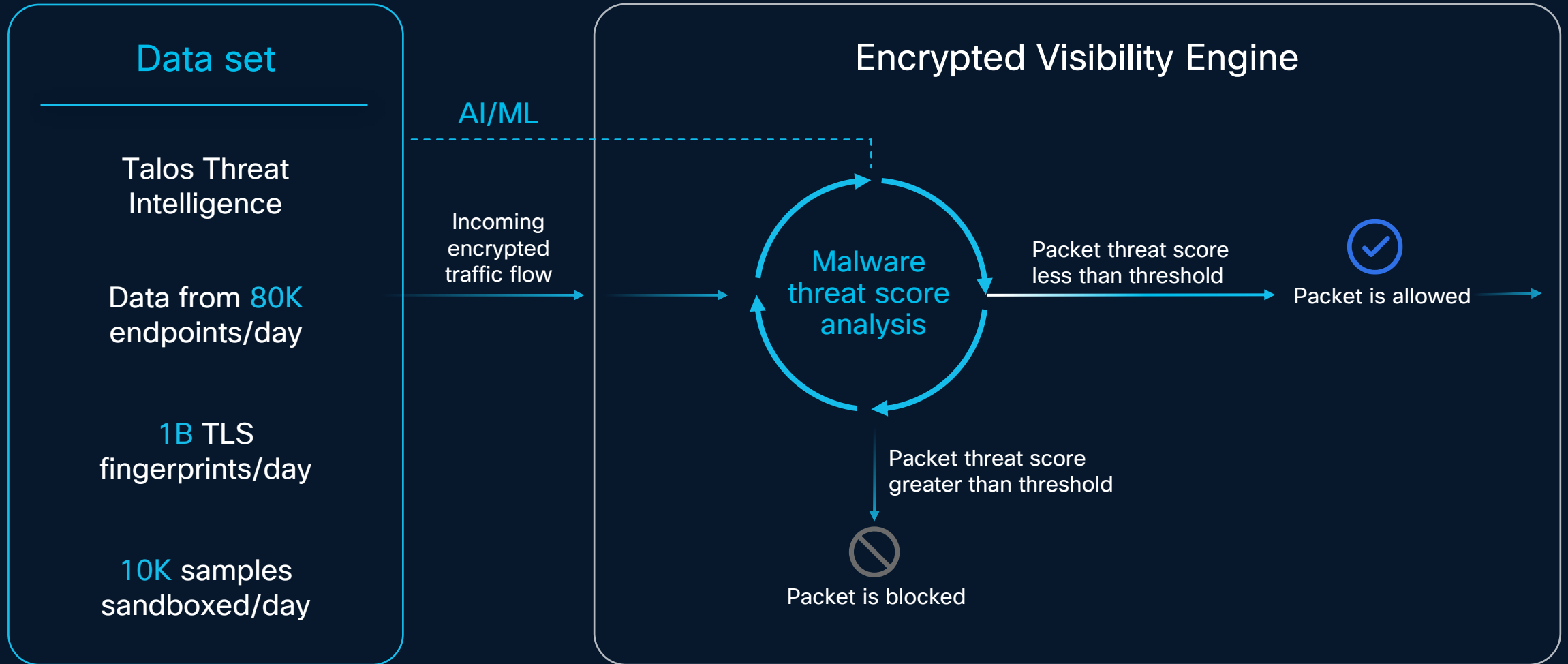
QUIC
Decryption



Advanced
Malware
Protection

Secure Firewall Capabilities

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



Secure Firewall Capabilities

Intelligent Selective Decryption

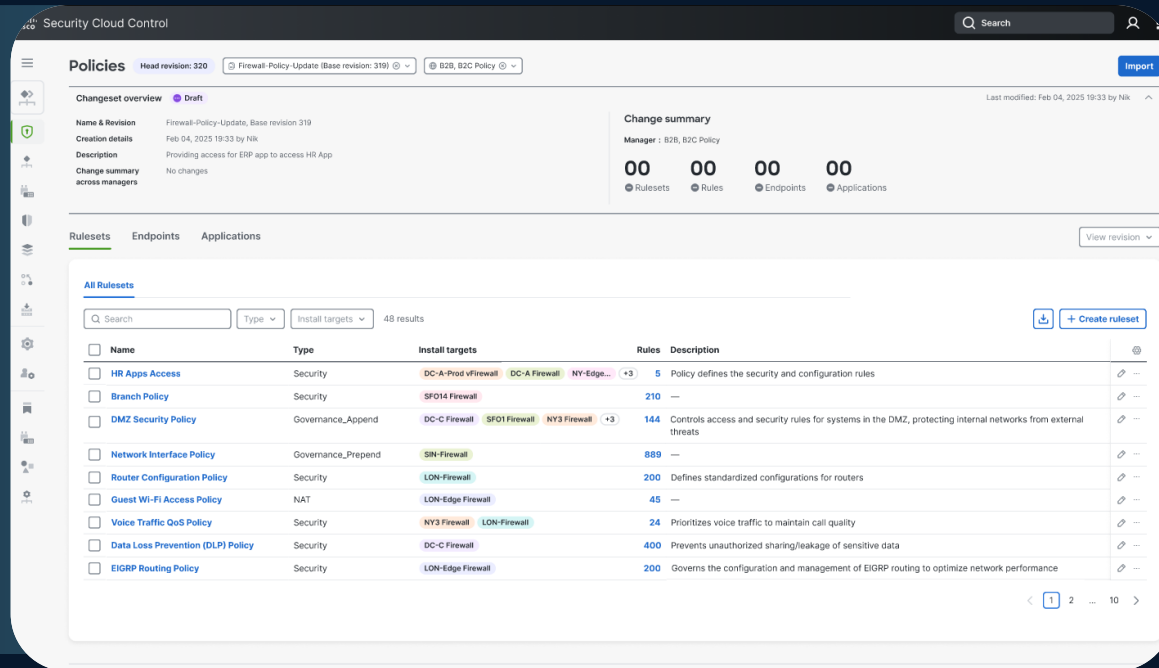
Risk-based intelligent decryption bypass, powered by EVE and Talos Server Reputation



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

Data center A



Data center B



Public cloud



Mesh Policy Engine Capabilities

Program once, enforce everywhere

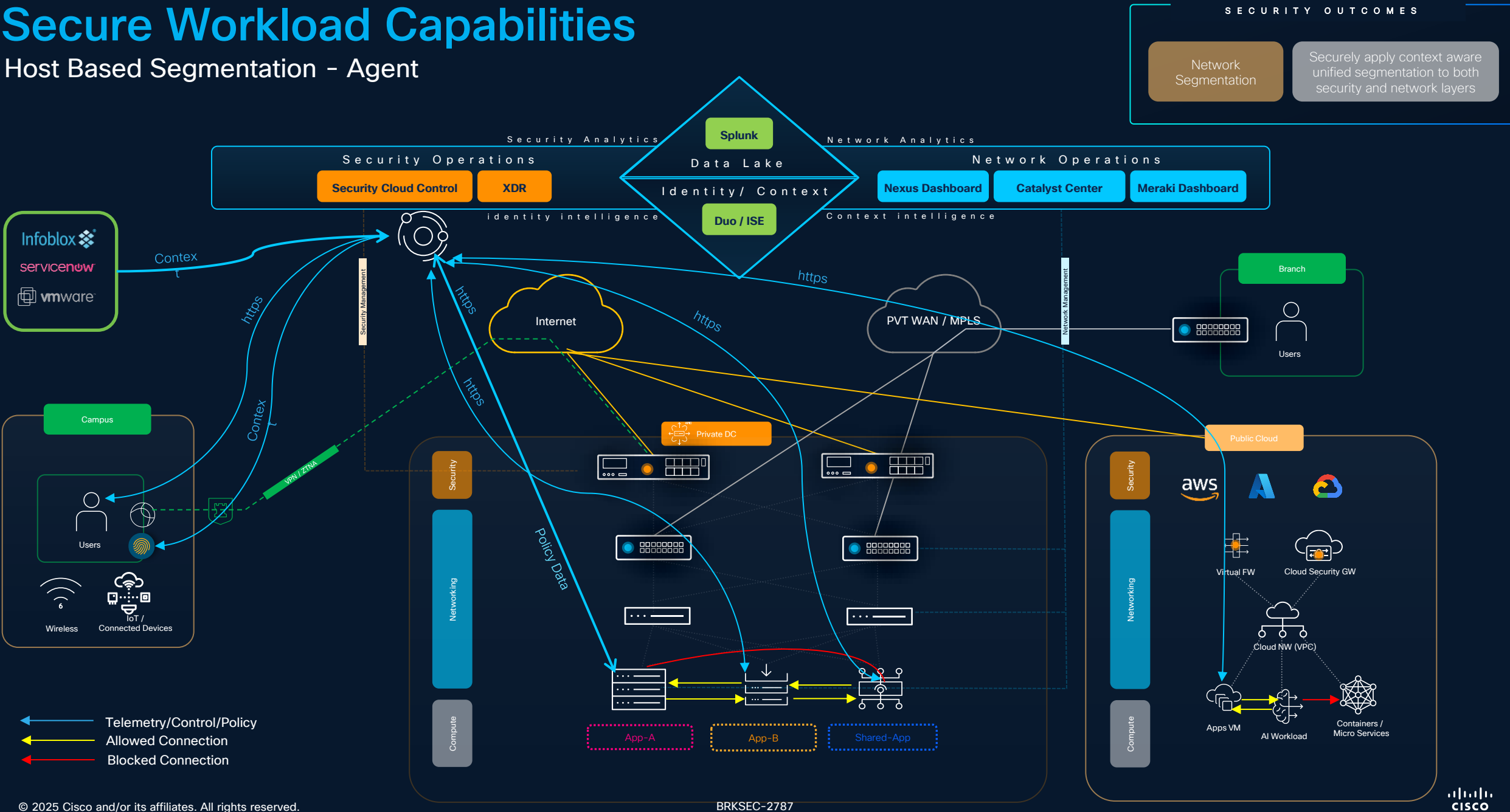
The screenshot shows the Cisco Security Cloud Control interface for creating a new rule. The rule is named "ERP-to-HR app" with an order of 01 and a description "Controls traffic flowing from ERP to HR Application". The rule is enabled, and logging is turned on. The "Specify Access" step is completed, and the "Review Deployment and impact" step is active. A network topology diagram is displayed, showing the flow from the Public Cloud (ERP) through a Cloud Edge Firewall to the Data Center (DC-A Firewall), which then connects to the App Zone (DC-A-App vFirewall) and finally to the HR App. The diagram includes expandable sections for Public Cloud, Data Center_A, and App Zone.

Mesh Policy Engine intelligently 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

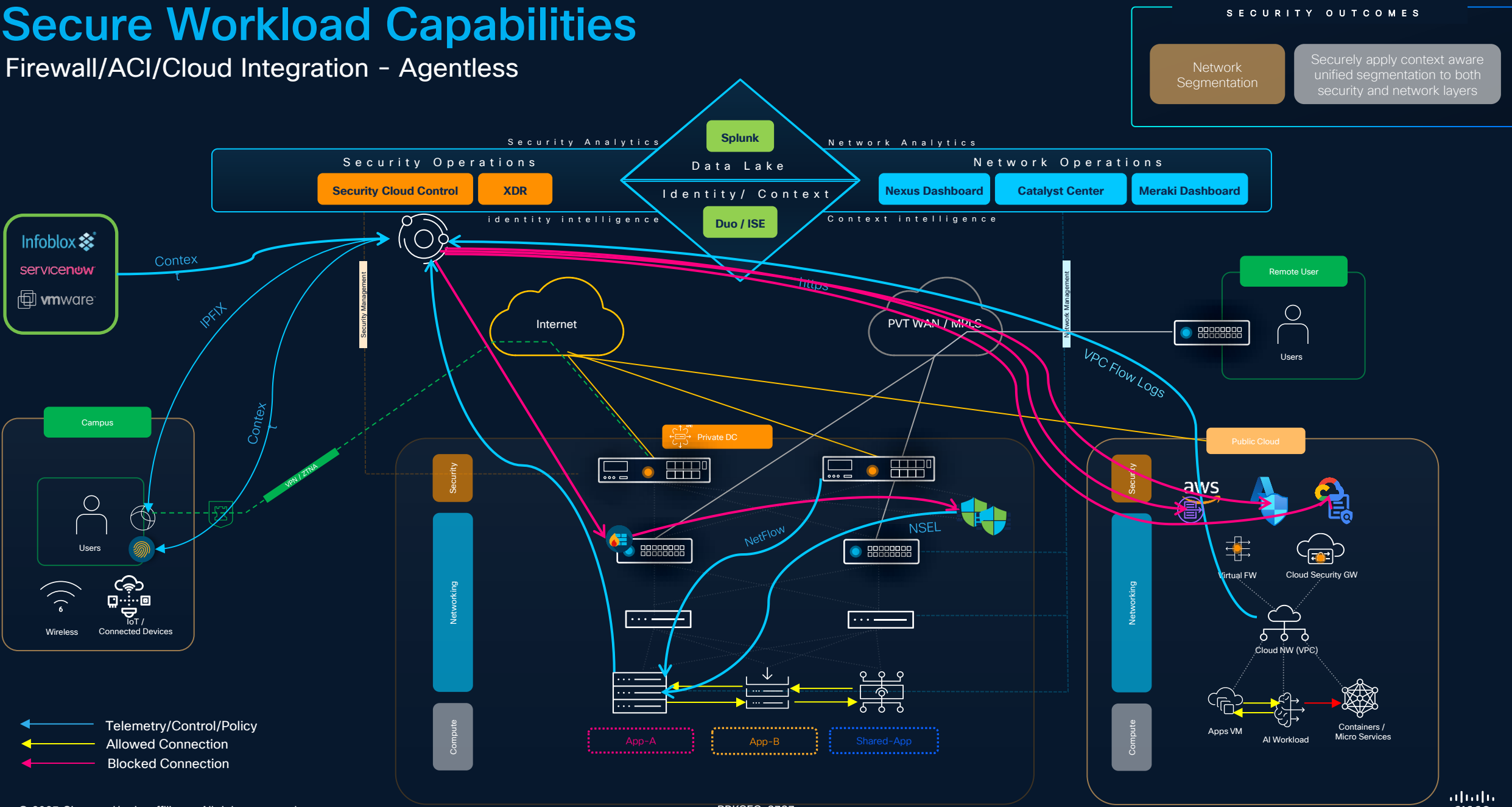
Secure Workload Capabilities

Host Based Segmentation - Agent



Secure Workload Capabilities

Firewall/ACI/Cloud Integration - Agentless



Hypershield Capabilities

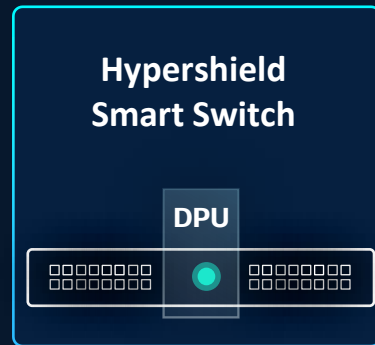
Cisco's Key Network Security Differentiator

Only Hypershield fuses security into....

the Network

&

the Workload



ONLY
CISCO

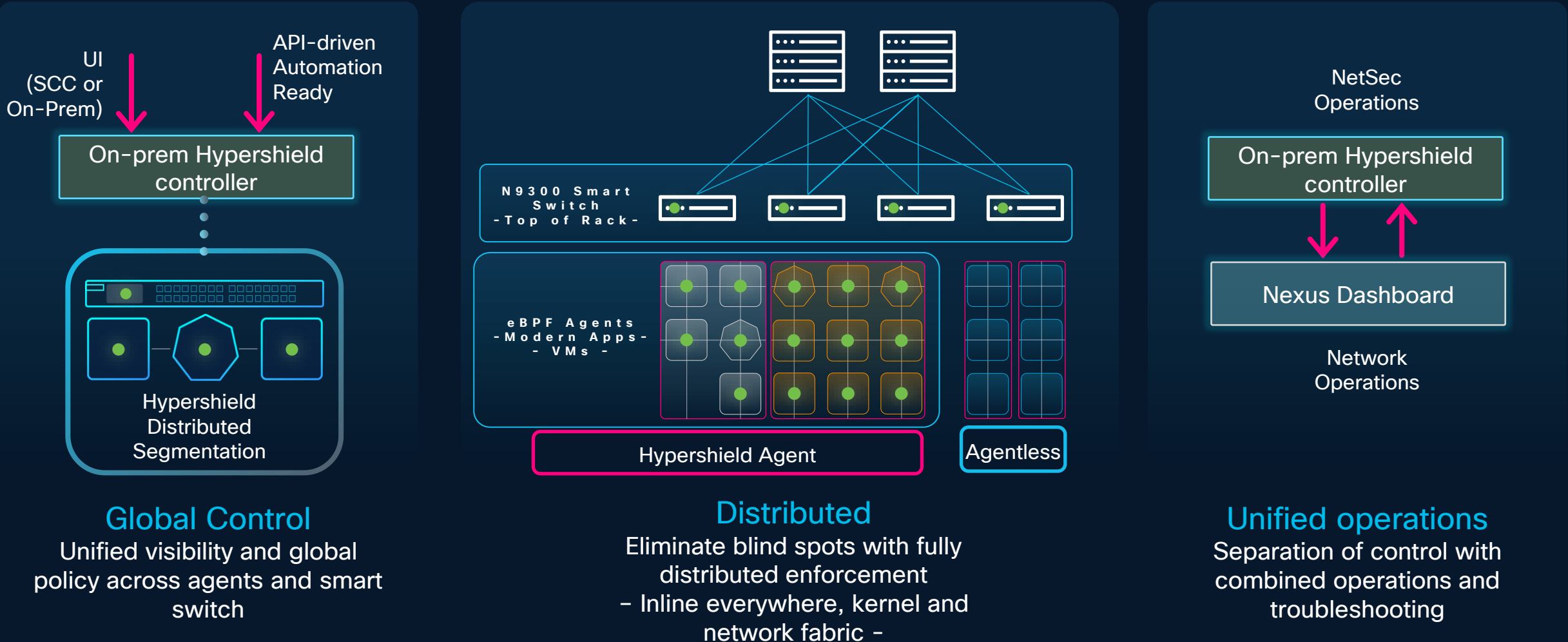


Eliminates east/west security blind spots in the datacenter with no changes to application workloads

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

Hypershield Capabilities

Distributed Segmentation Architecture



Hypershield Capabilities

Distributed Exploit Protection

Public Global Data Sources

- CVE repositories
- CWE information
- MITRE
- Kenna
- TALOS
- ...

Hypershield AI

Shields for each CVE

Distributed Exploit Protection

Private Local Data Sources

In-Depth Visibility

- what
- where
- which version
- which libraries

Local Graph

Hypershield AI

Global Graph

Hypershield Capabilities

Nexus Smart Switch



Cisco Nexus 9000 Smart Switch



- 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

- 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

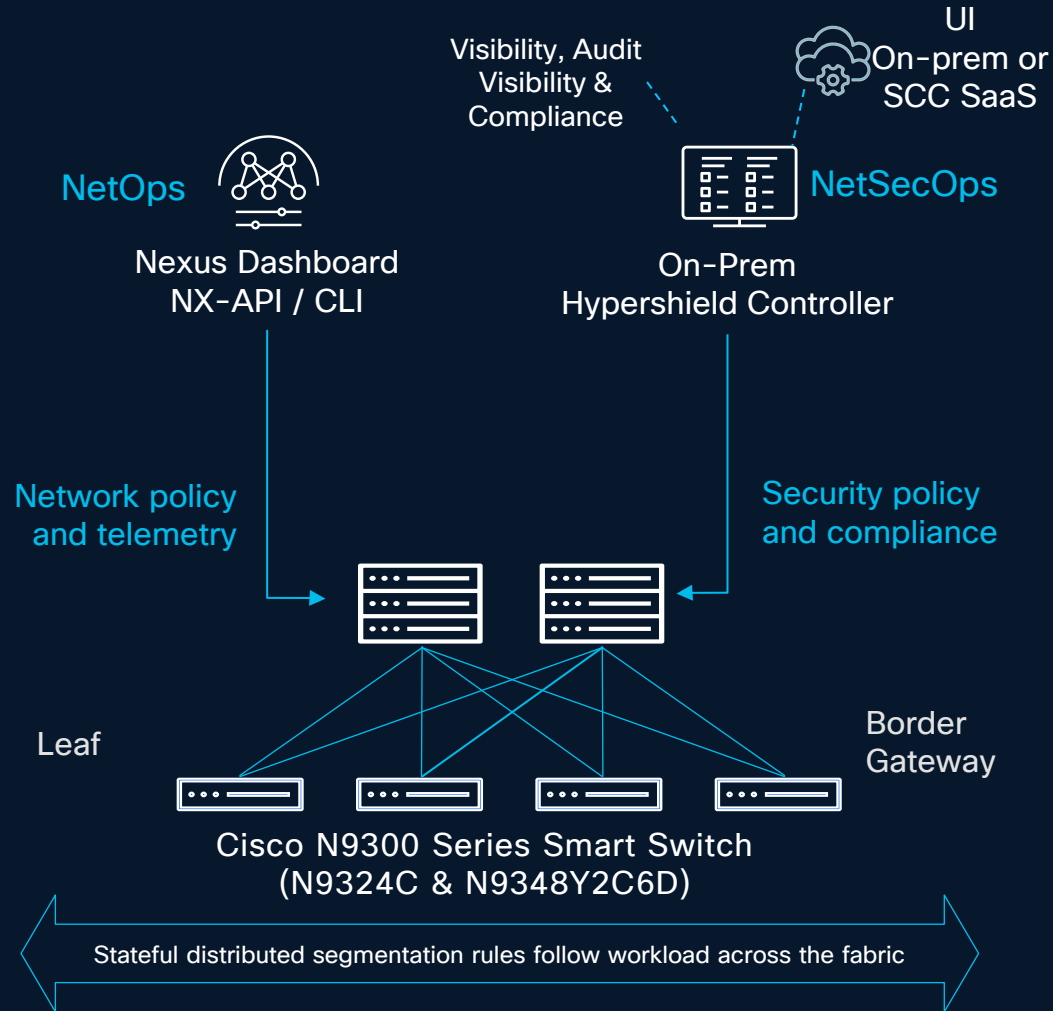
Hypershield Capabilities

Nexus Smart Switch



Hypershield Capabilities

Smart Switch – Networking & Security



Security Infused in Data Center Fabric

Version: NXOS 10.6(2), Hypershield 1.2

Smart Switches: N9348Y2C6D-SE1U, N9324C-SE1U

Fabric: VXLAN-EVPN, VXLAN-multi-site, BGP fabric, brownfield

Segmentation: VRF/VLAN + CIDR rules, stateful/stateless, 100K rules, 800G throughput (final scale based on benchmarking)

Policy: CRD schema, policy validation and canary rollout/rollback

Hypershield: Air-gap ready on-prem controller and optional Security Cloud Control SaaS

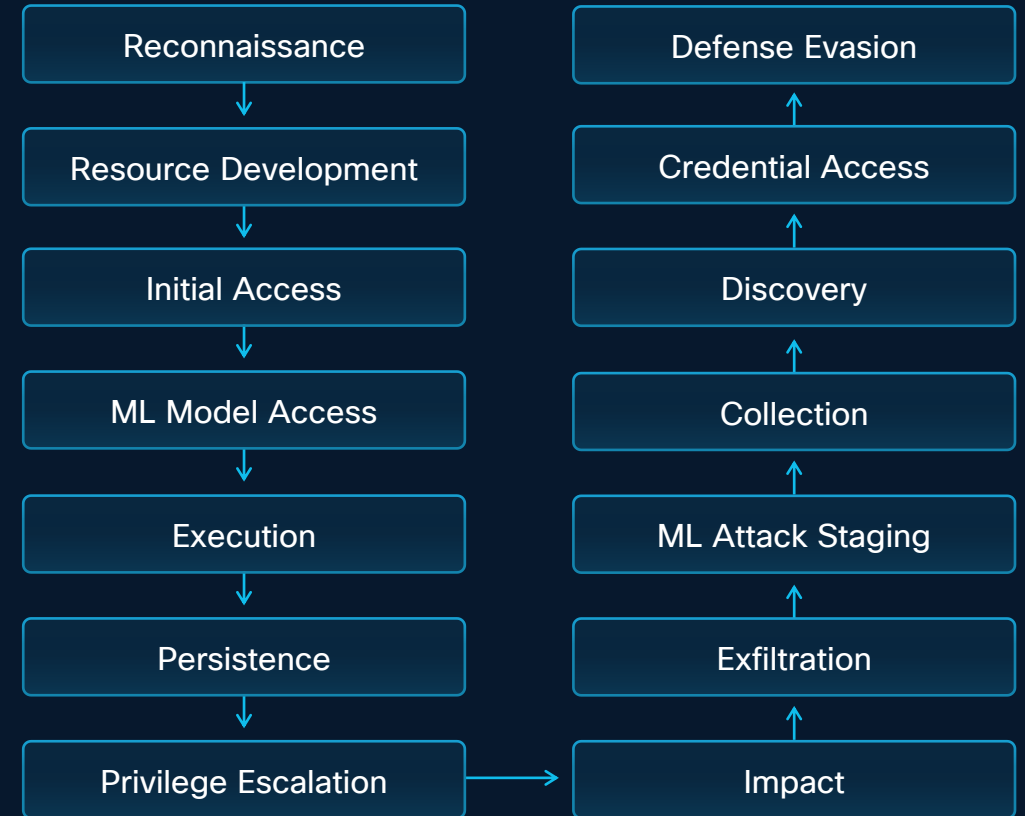
Upgrade: NXOS CLI for DPU load, SMU for Hypershield agent

Observability: Nexus Dashboard, Splunk, Prometheus/Grafana

New Standards for AI Security



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



What does the AI threat landscape look like?

LLM01 Prompt Injection

A Prompt Injection Vulnerability occurs when user prompts alter the LLM's behavior or output in unintended ways. These inputs can affect the model even if they are...

LLM02 Sensitive Information Disclosure

Sensitive information can affect both the LLM and its application context. This includes personal identifiable information (PII)...

LLM03 Supply Chain

LLM supply chains are susceptible to various vulnerabilities, which can affect the integrity of training data, models, and deployment platforms....

LLM04 Data and Model Poisoning

Data poisoning occurs when pre-training, fine-tuning, or embedding data is manipulated to introduce vulnerabilities, backdoors, or biases....

LLM05 Improper Output Handling

Improper Output Handling refers specifically to insufficient validation, sanitization, and handling of the outputs generated by large language models before they....

LLM06 Excessive Agency

An LLM-based system is often granted a degree of agency by its developer - the ability to call functions or interface with other systems via extensions...

LLM07 System Prompt Leakage

The system prompt leakage vulnerability in LLMs refers to the risk that the system prompts or instructions used to steer the behavior...

LLM08 Vector and Embedding Weaknesses

Vectors and embeddings vulnerabilities present significant security risks in systems utilizing Retrieval Augmented Generation (RAG)...

LLM09 Misinformation

Misinformation from LLMs poses a core vulnerability for applications relying on these models. Misinformation occurs when LLMs produce...

LLM10 Unbounded Consumption

Unbounded Consumption refers to the process where a Large Language Model (LLM) generates outputs based on input queries or prompts...

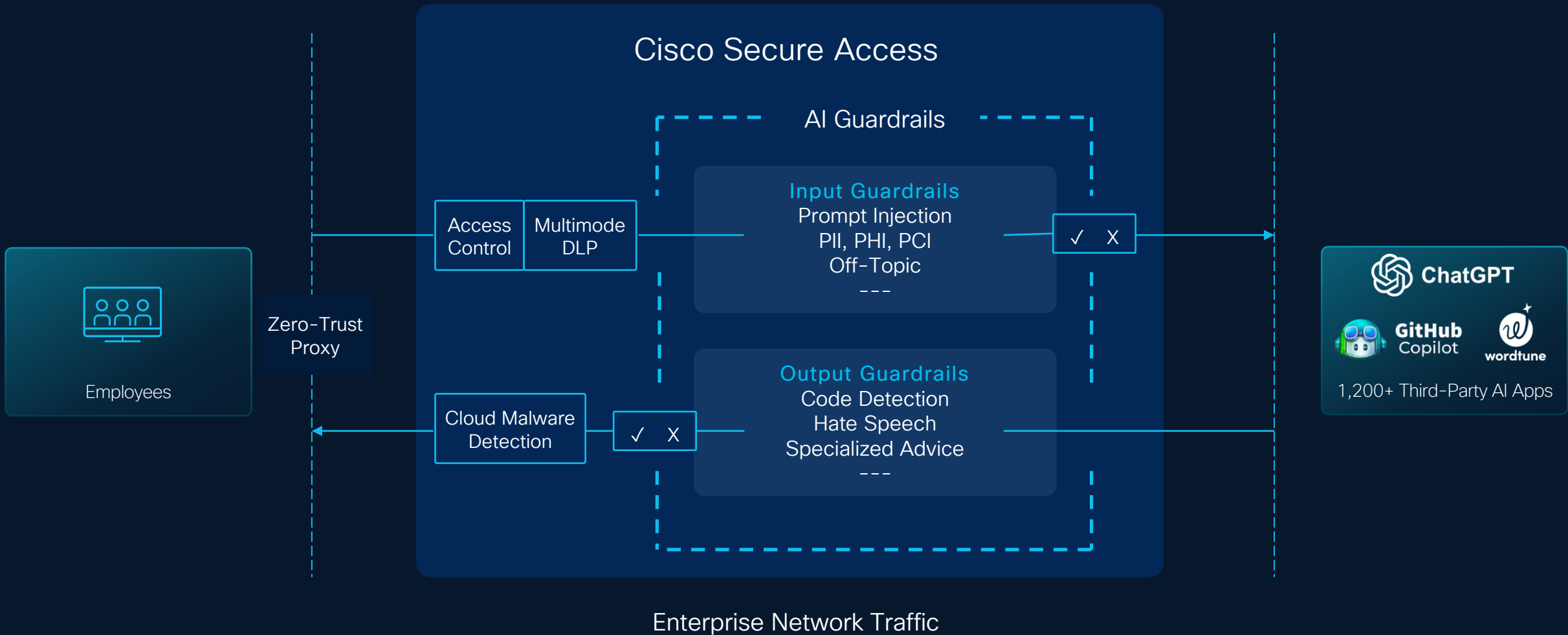
AI Defense Capabilities

Model Protection, Flexible Enforcement Options



Secure Access Capabilities

Third Party AI App Protection – AI Access Policies



Secure Access Capabilities

UZTNA

Extend identity
context

Unify application
access

Build operational
resilience

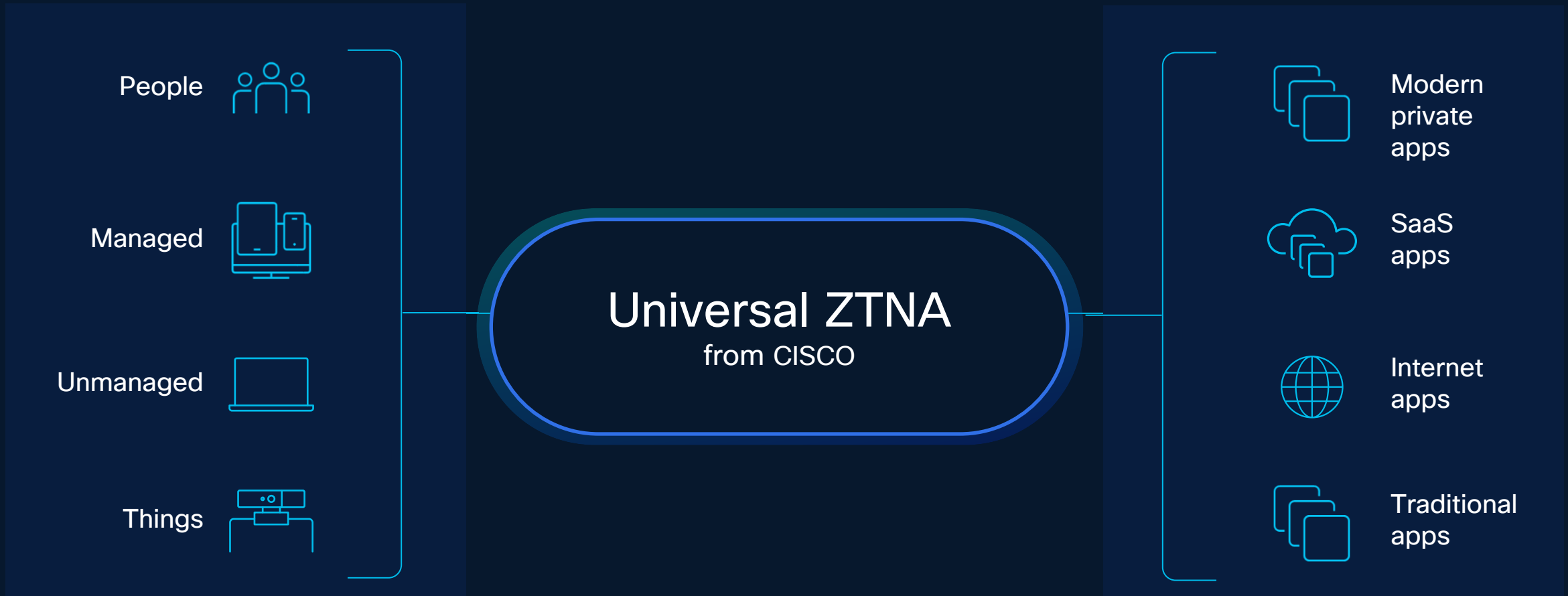
Network and security convergence makes it possible

Zero trust for IT and IOT,
users and devices

Least privilege enforcement
everywhere

Policy and experience
assurance, zero downtime

Secure Access Capabilities



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

Real-World Customer Use Cases

Customer # 1 – Problem Statement

Cisco Secure Firewall Customer, looking to meet the compliance target for uSegmentation

Cloud Migration Acceleration: Rapidly moving critical workloads to Google Cloud Platform (GCP) to meet demands for agility and scalability.

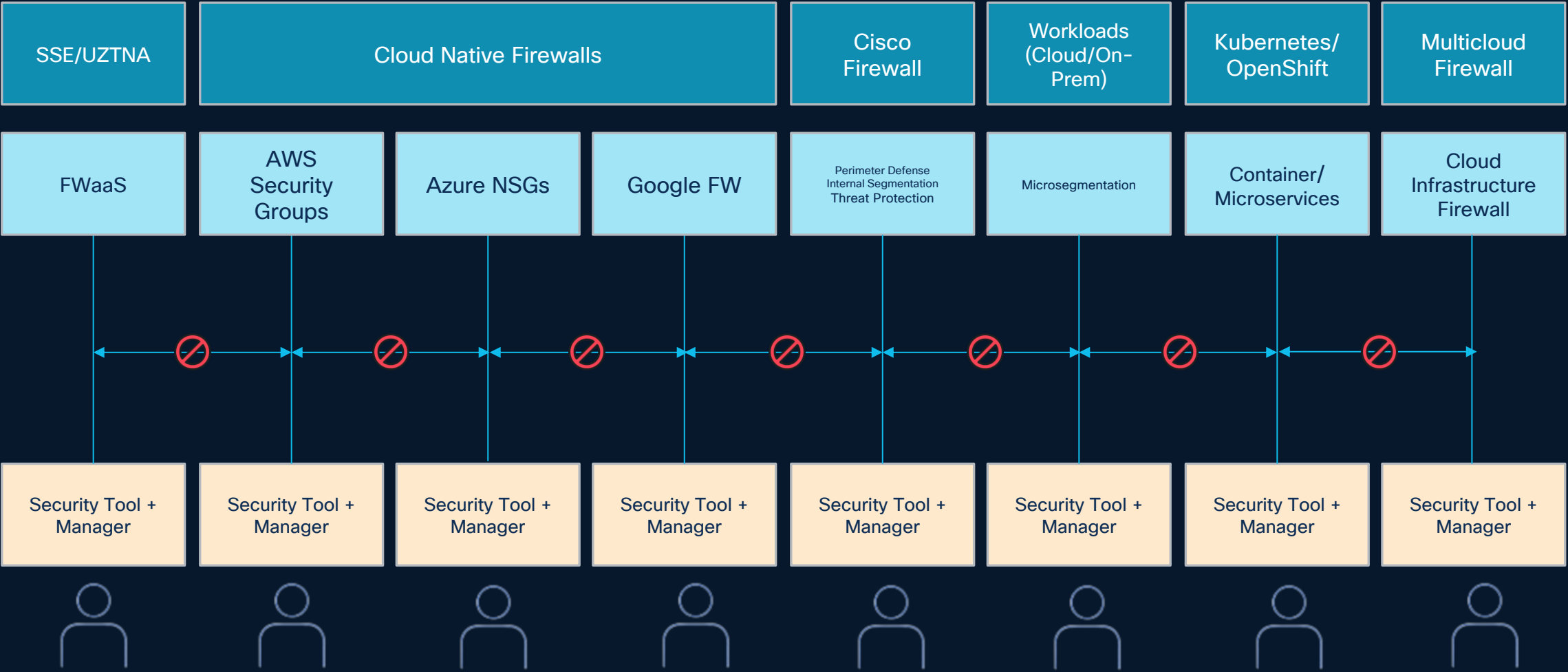
Segmentation Compatibility Gap: Their existing on-premises segmentation solution is incompatible with GCP, preventing consistent security enforcement.

Compliance Risk Exposure: This disconnect introduces a significant compliance risk, as policies cannot be uniformly applied across hybrid infrastructure.

Need for Unified Policy Management: Immediate requirement is to meet the compliance for workloads moving to GCP, with forward looking Unified Policy Management.

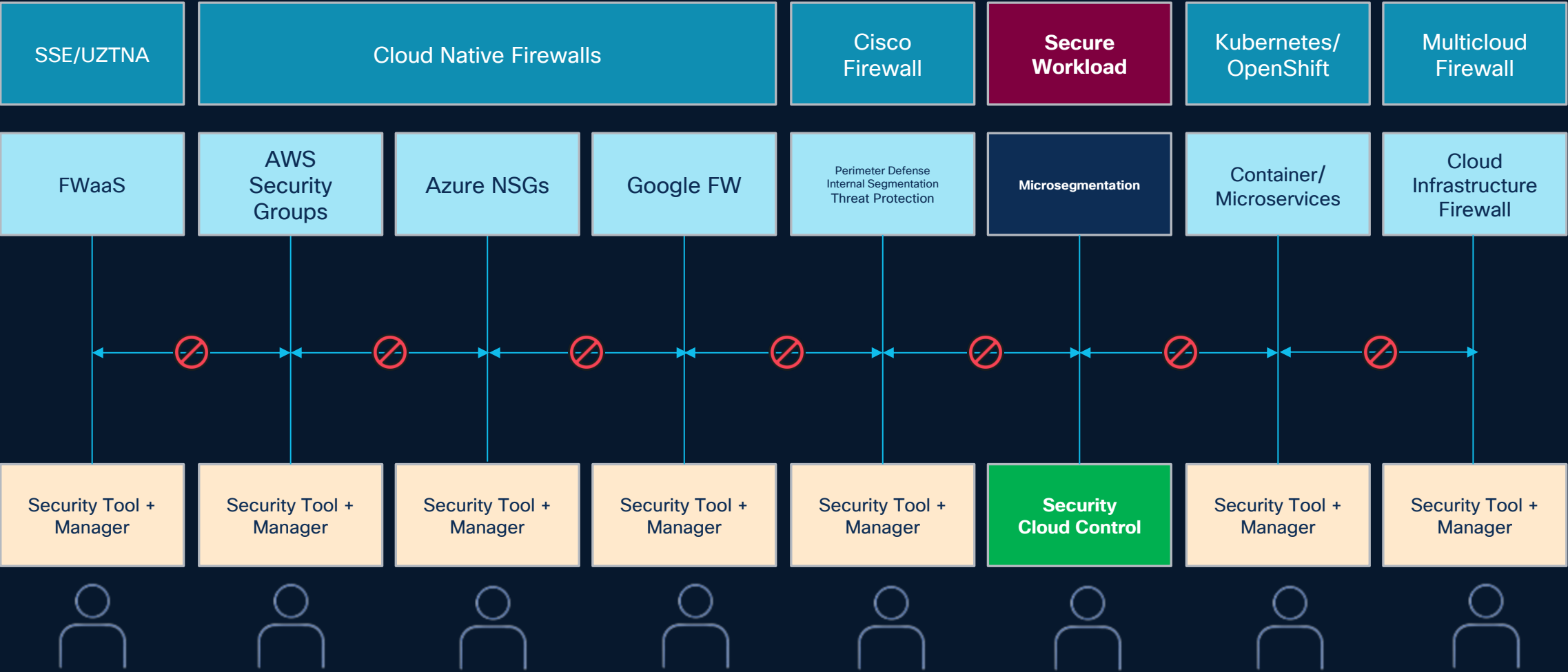
Customer Use Case # 1

Microsegmentation for Compliance



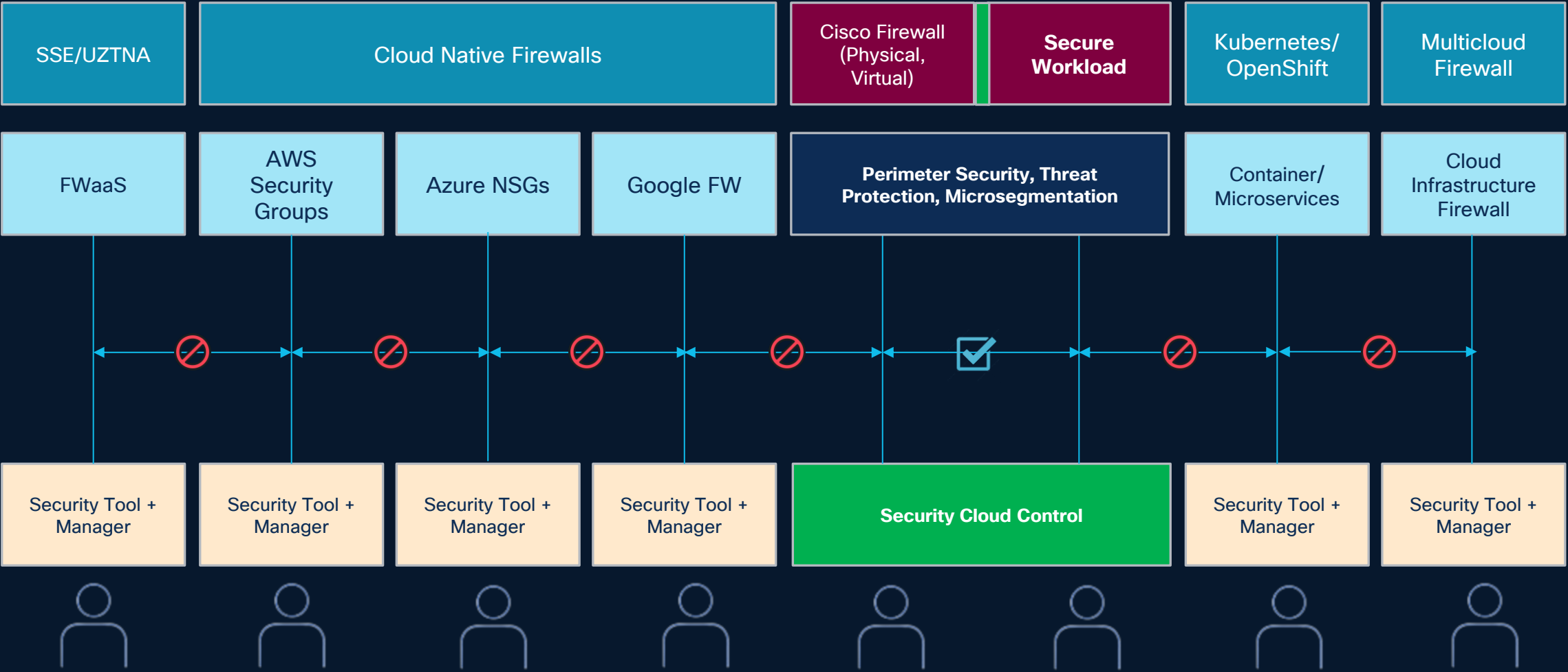
Customer Use Case # 1

Microsegmentation for Compliance



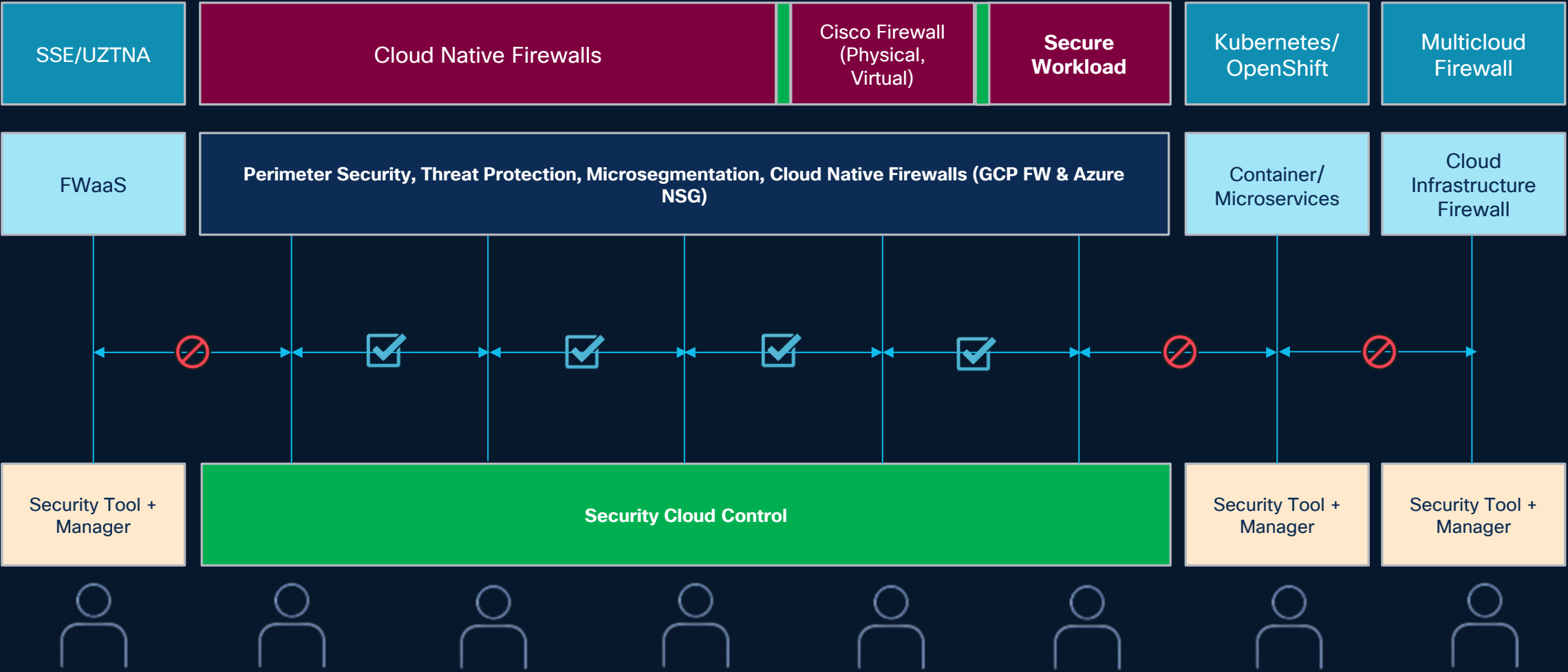
Customer Use Case # 1

Microsegmentation for Compliance



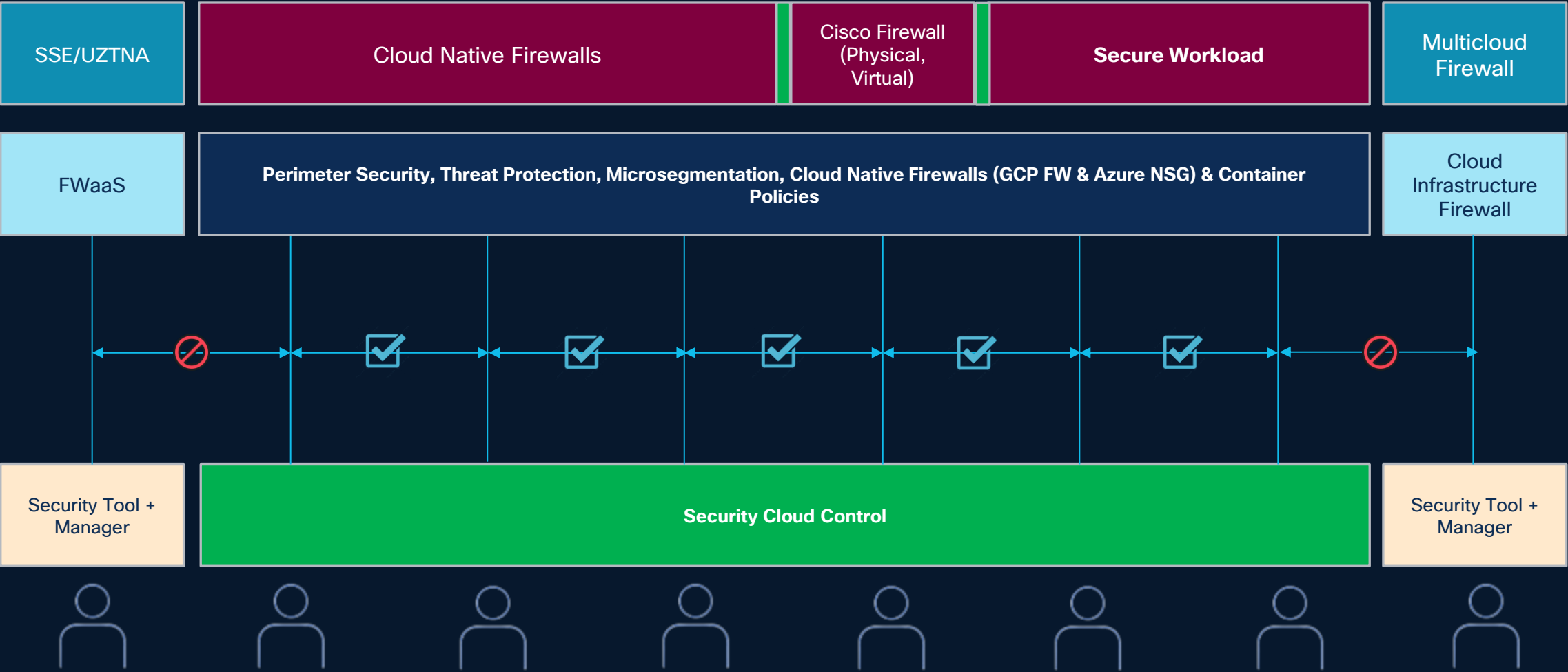
Customer Use Case # 1

Microsegmentation for Compliance



Customer Use Case # 1

Microsegmentation for Compliance



Customer # 2 – Problem Statement

Zero Cisco Security Footprint with Established Competitive Products

Firewall Policy Management Challenges: Managing policies across multiple firewall vendors is complex and inefficient.

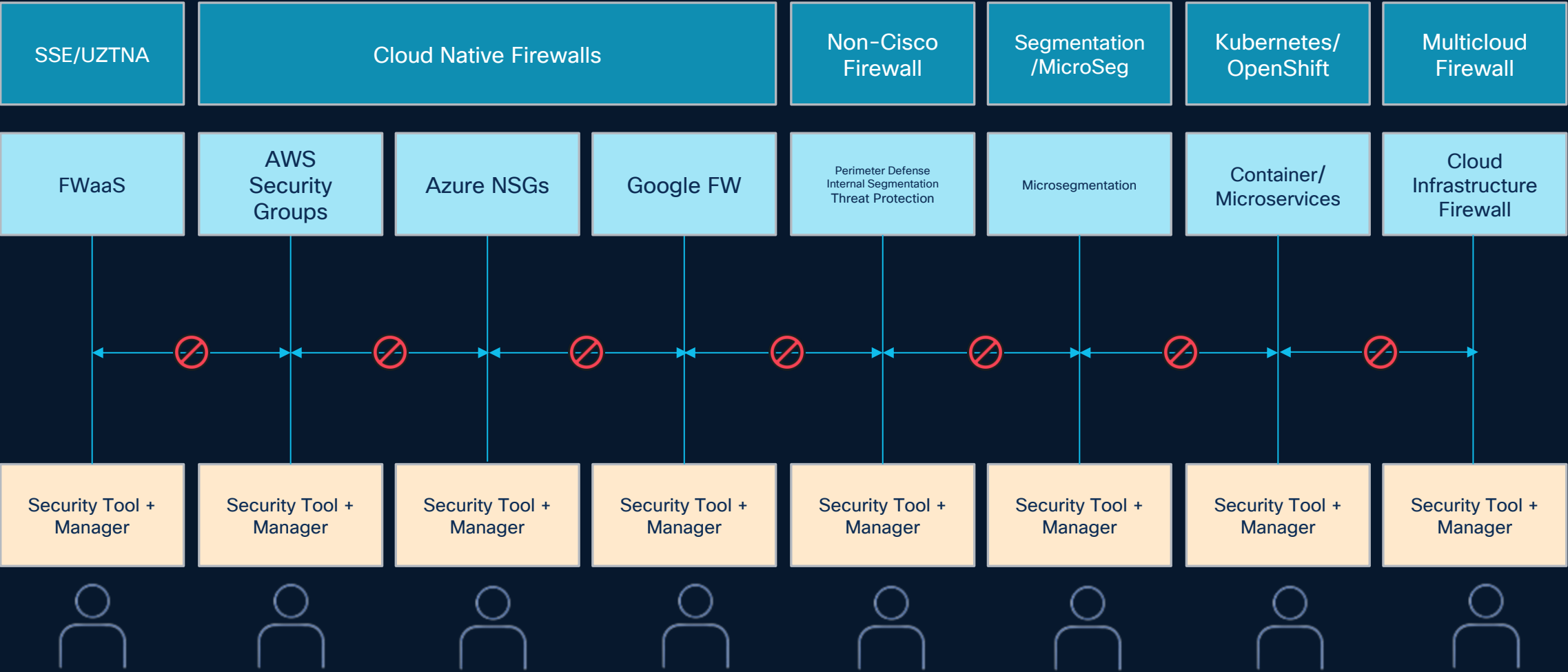
Policy Inconsistency: Fragmentation leads to inconsistent security policies across the environment.

Workload Hardening: Currently use many Vulnerability Management solutions with no cohesive visibility & mitigation.

Seeking a Scalable, Unified Solution: Looking for a centralized approach to enforce policies and enhance visibility across hybrid environments.

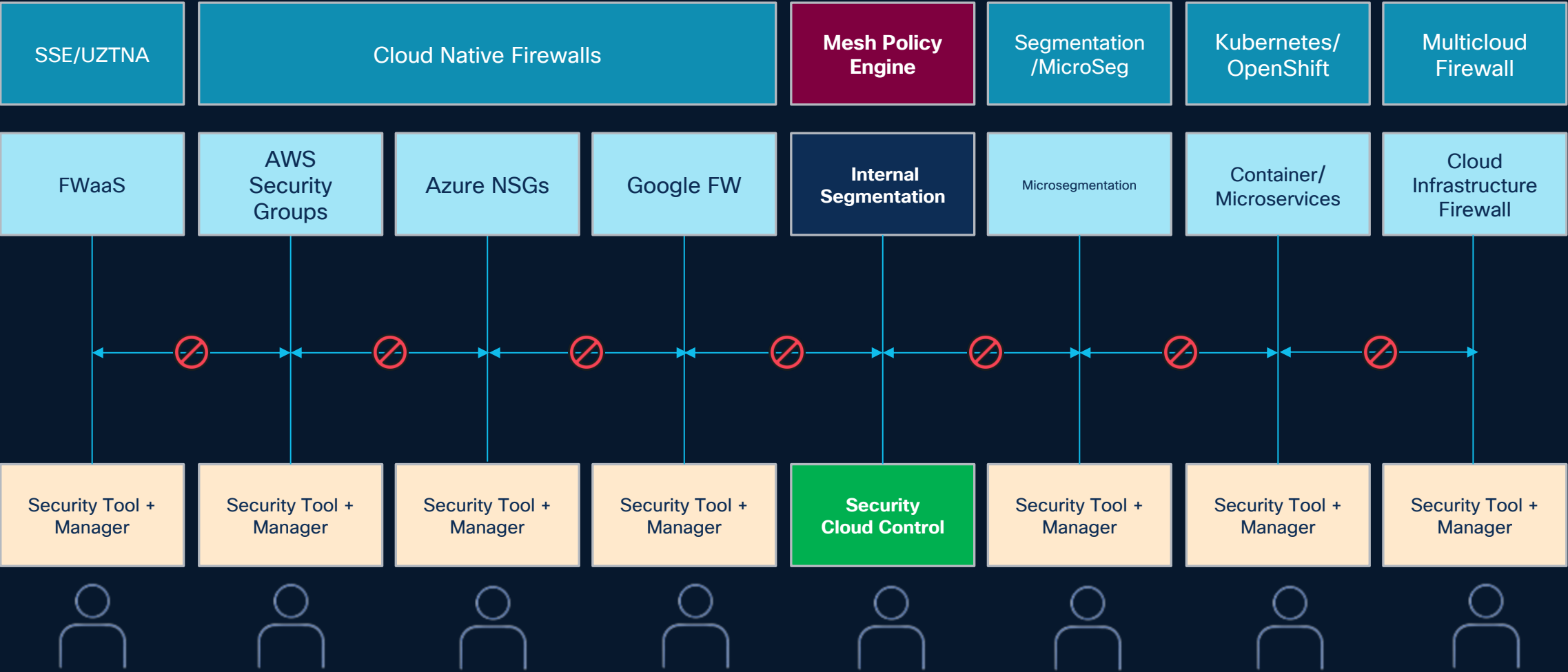
Customer Use Case # 2

Multi-Vendor Firewall Management



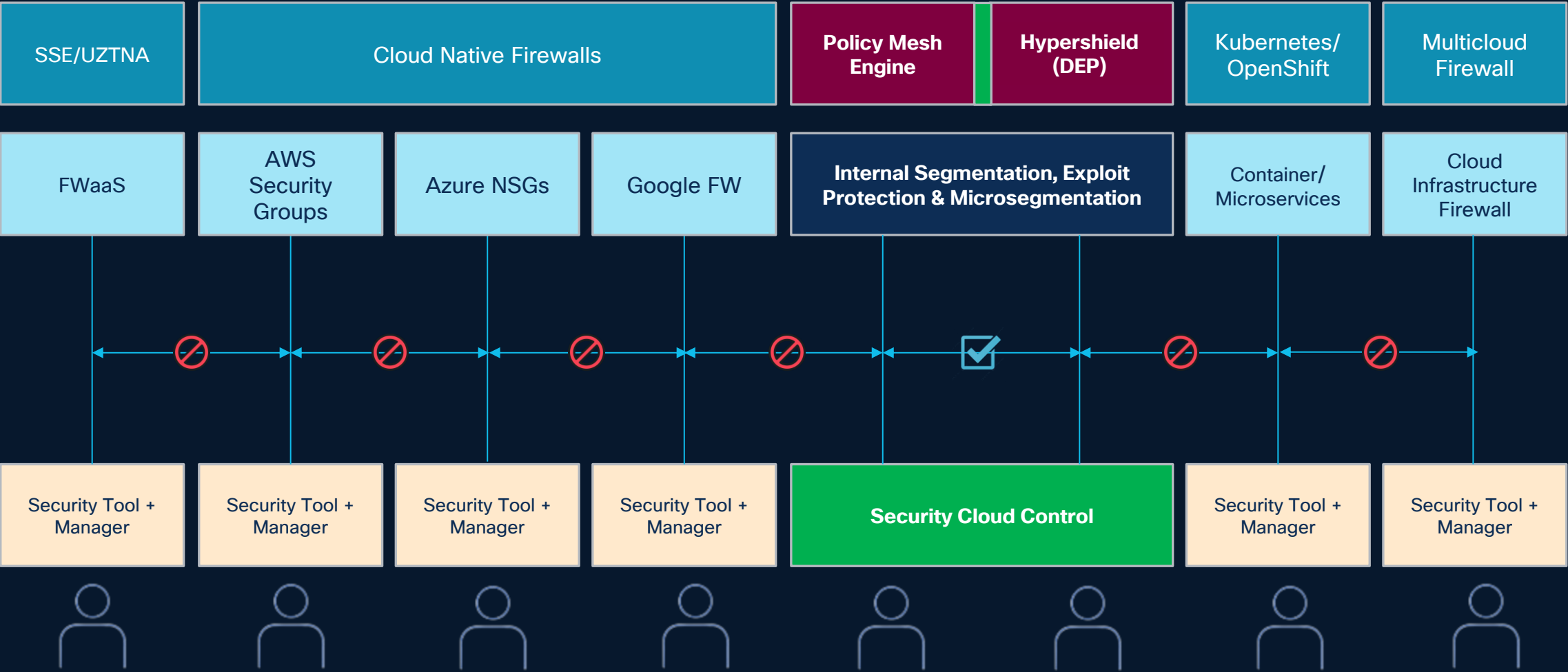
Customer Use Case # 2

Multi-Vendor Firewall Management



Customer Use Case # 2

Multi-Vendor Firewall Management



Customer # 3 – Problem Statement

Low Cisco Security Footprint with Established Competitive Products

Container Network Challenges: Facing issues with network policy enforcement and visibility in OpenShift environments.

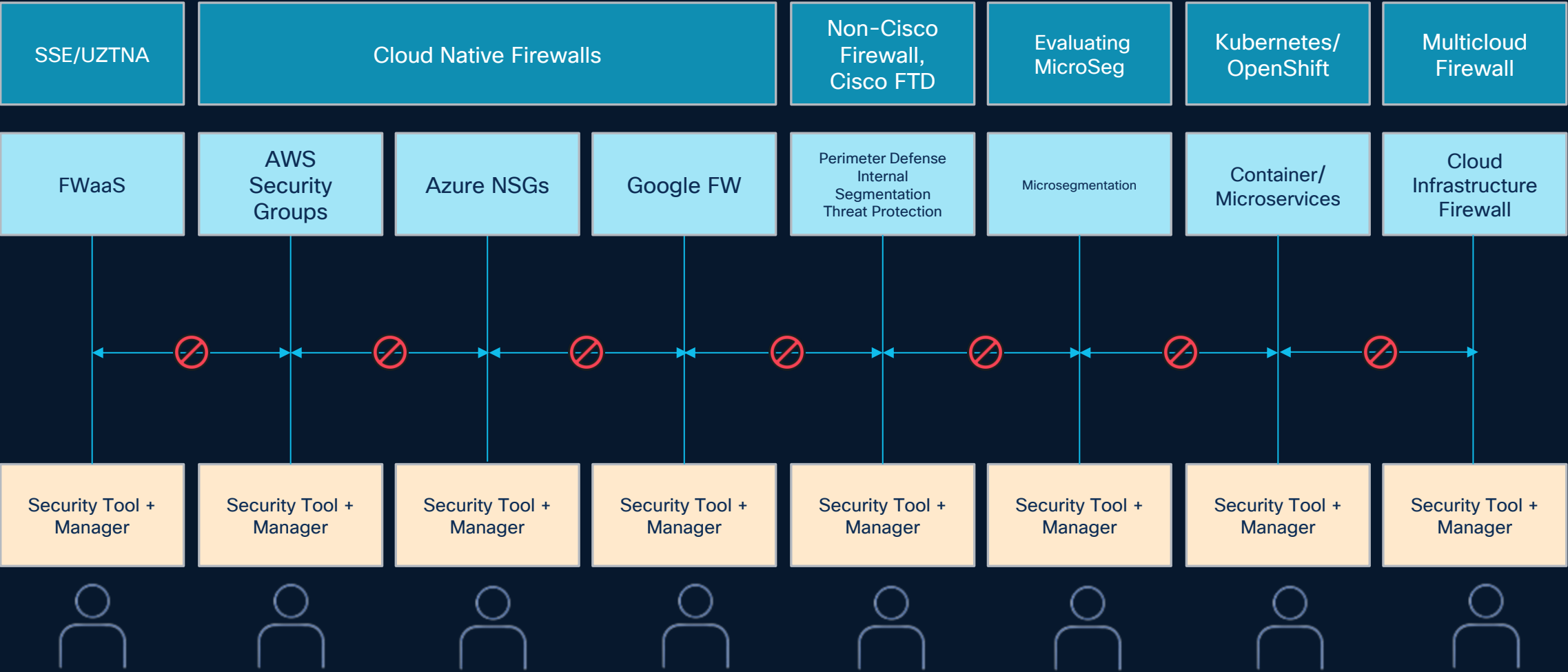
Legacy Tooling Limitations: Current tools lack the agility and granularity for dynamic, distributed containers.

Microsegmentation Under Evaluation: Exploring microsegmentation to enhance lateral threat containment by year-end.

Need for Unified Architecture: Seeking a scalable, unified security solution that works across hybrid, multicloud, and both traditional and container-native workloads.

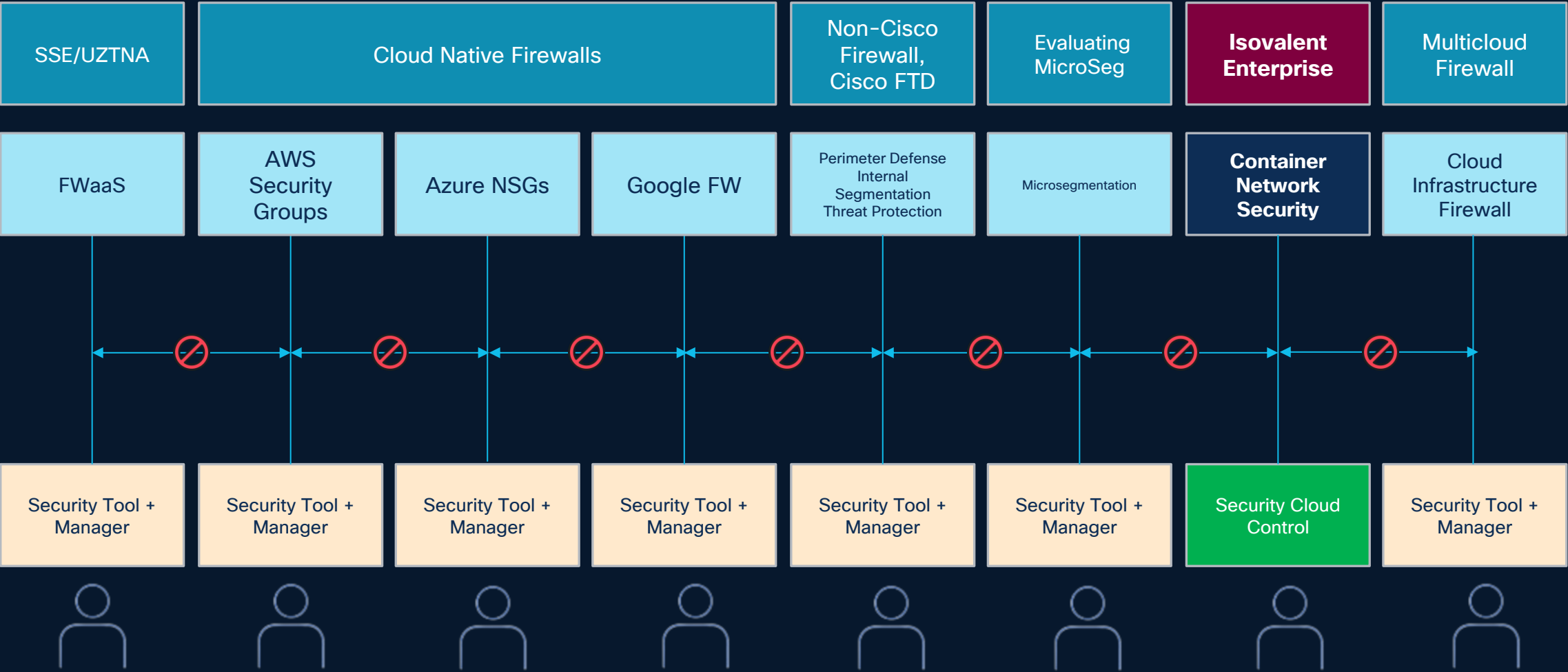
Customer Use Case # 3

Container Network Policy



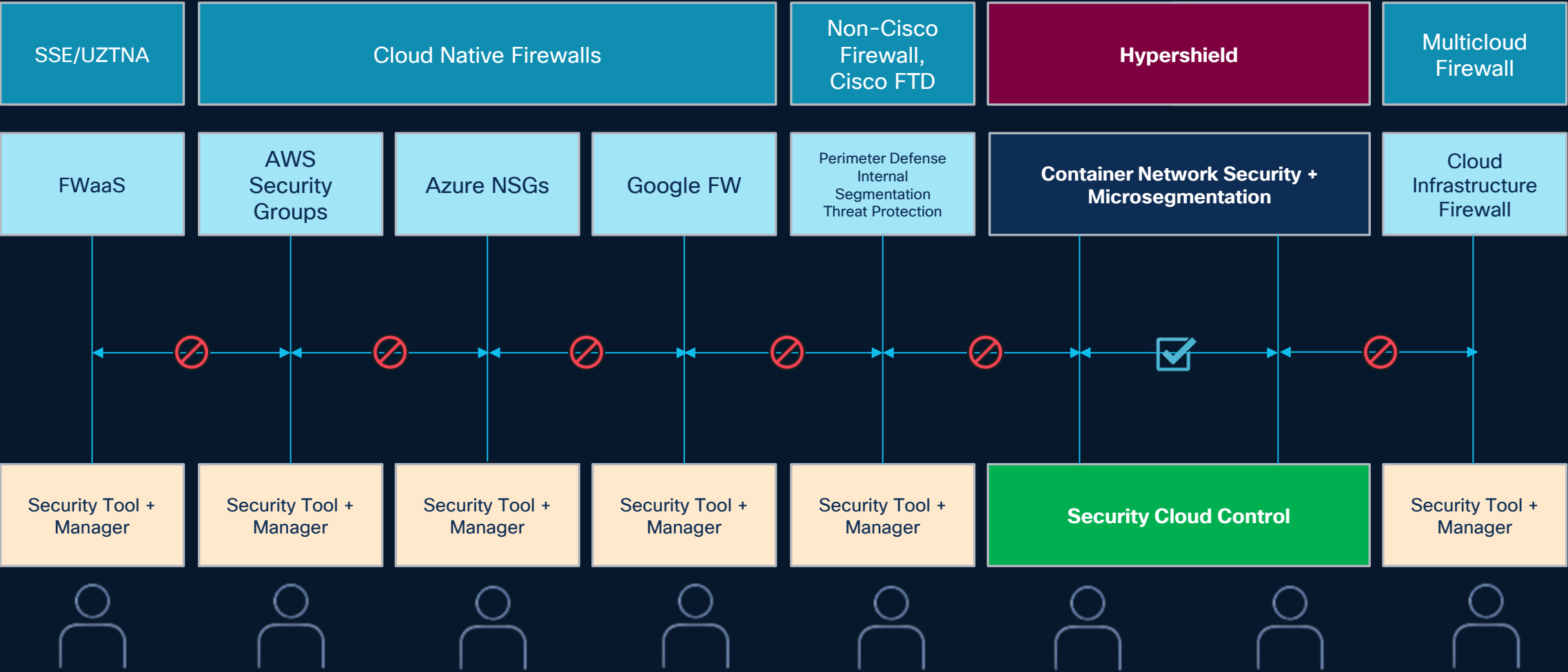
Customer Use Case # 3

Container Network Policy



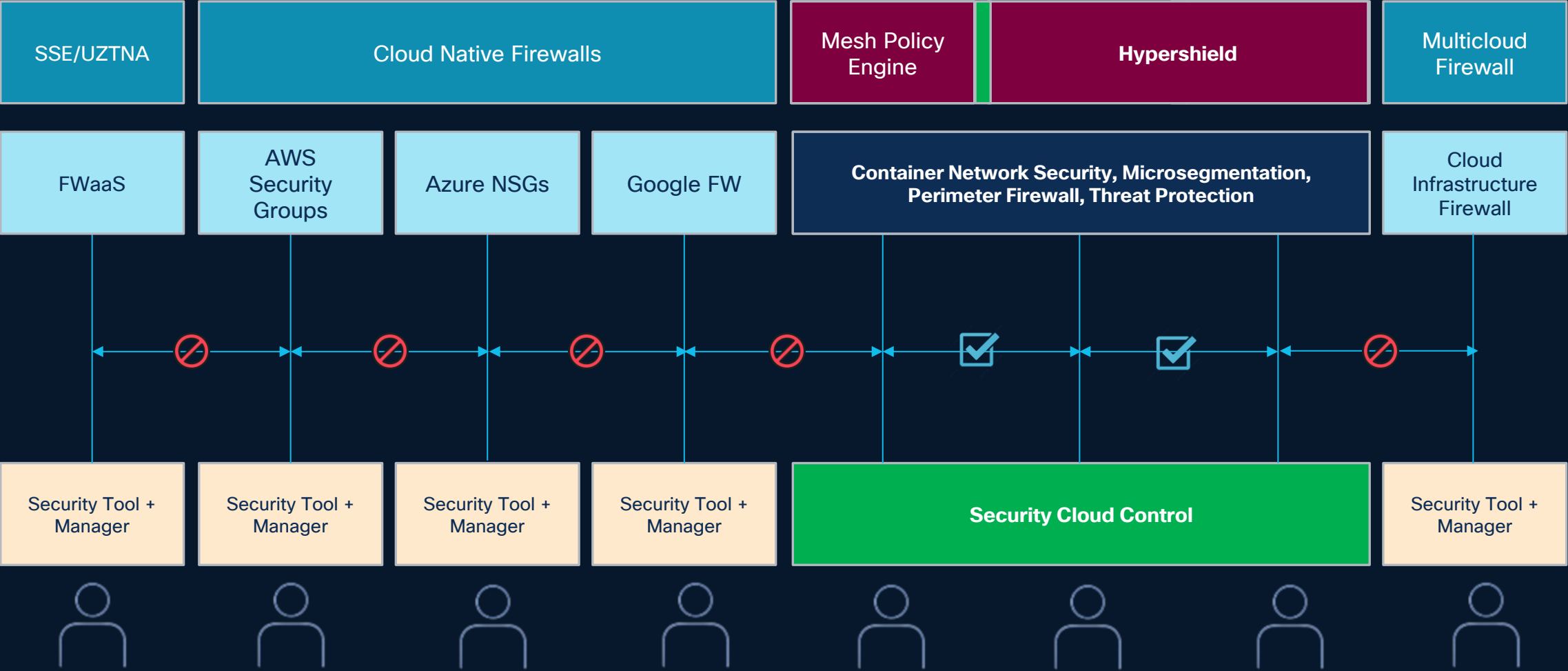
Customer Use Case # 3

Container Network Policy



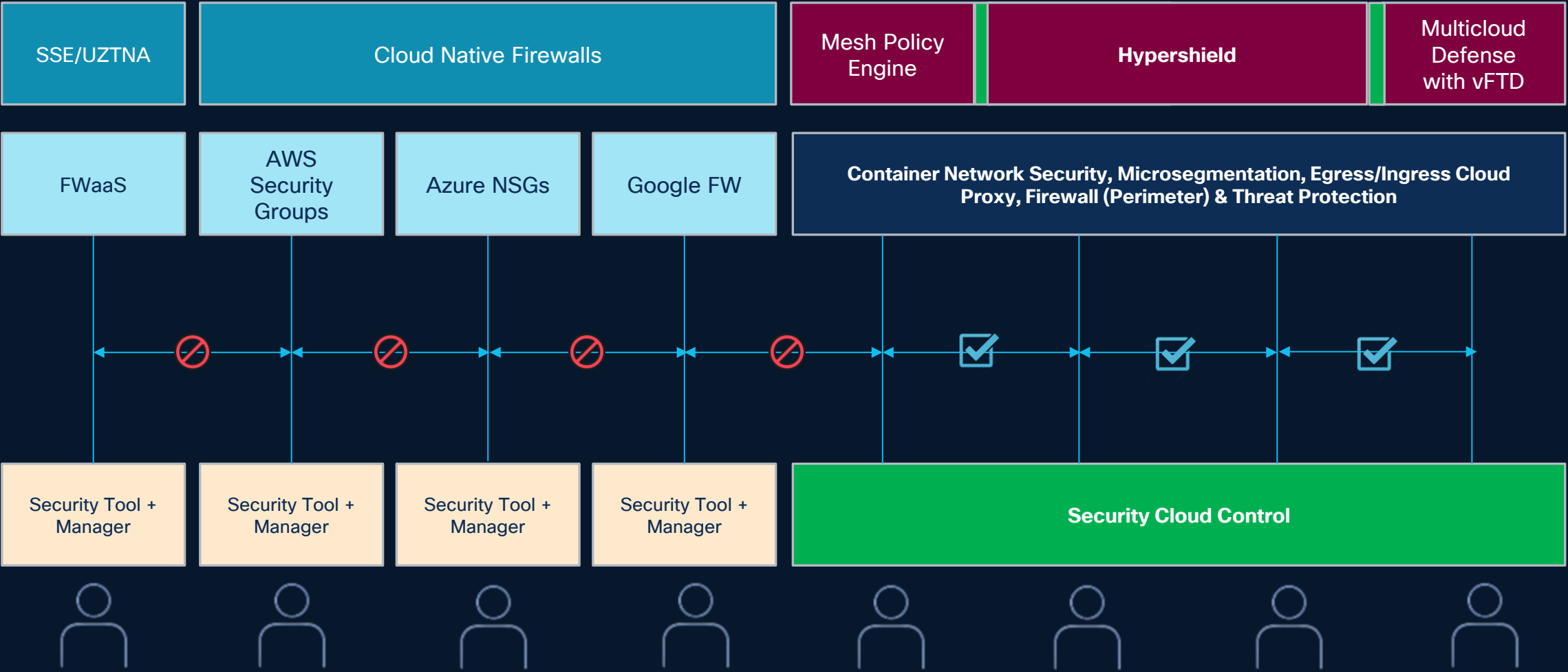
Customer Use Case # 3

Container Network Policy



Customer Use Case # 3

Container Network Policy



Key Takeaways

Key Takeaways

- ❖ **Micro-Perimeter Security:** Moves beyond traditional perimeters to secure hybrid cloud, containers, and SDNs
- ❖ **Unified, Distributed Firewall:** Centrally managed security across dynamic, distributed environments.
- ❖ **AI-Driven Protection:** Uses AI to detect and respond to evolving threats.
- ❖ **Consistent Policy & Integration:** Ensures unified governance and streamlined operations.

Simple, future-proof licensing

Cloud Protection Suite

Gateways

Workloads

Secure
Firewall

Multicloud
Defense

Secure
Workload

Isovalent
Enterprise

Hypershield

Call to Action



**Evaluate The Current
Security Posture**



**Initiate or Accelerate
Security Modernization**



**Engage Cisco or
Partners for a
Strategic Assessment**



**Apply Key Learnings to
Upcoming Projects**

Q & A

Complete your session evaluations



Complete a minimum of 4 session surveys and the Overall Event Survey to claim a Cisco Live T-Shirt.



Earn up to 800 points by completing all surveys and climb the Cisco Live Challenge leaderboard.



Level up and earn exclusive prizes!



Complete your surveys in the Cisco Live Events app.

Continue your education



Visit the Cisco Stand for related demos



Book your one-on-one Meet the Expert meeting



Attend the interactive education with Capture the Flag, and Walk-in Labs



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

Thank you

CISCO Live !

