Zero Trust for Cloud & Beyond with Cisco Hybrid Mesh Firewall

Nadir Lakhani
Technical Solutions Architect - Hypershield, Workload & Cloud Security

Cisco Webex App

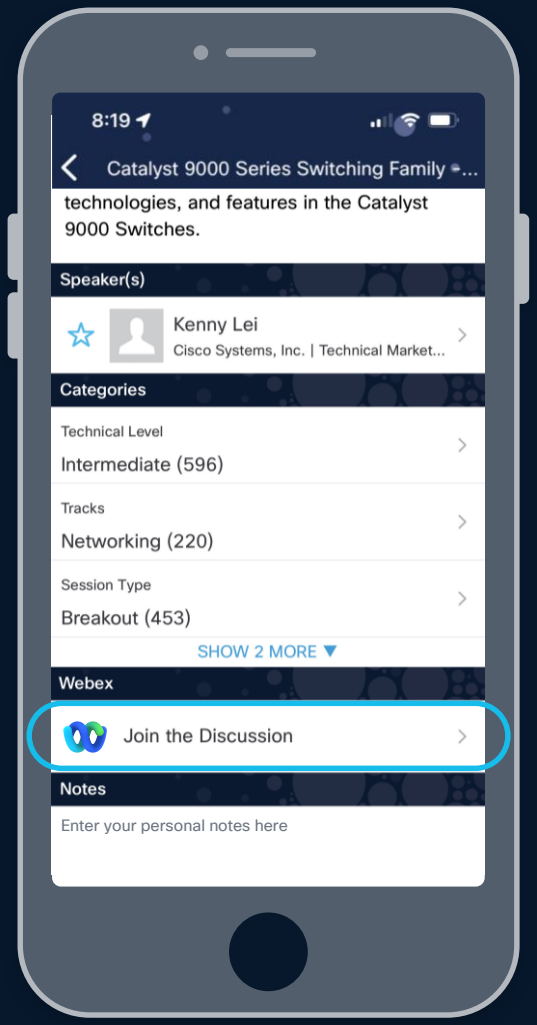
Questions?

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, 2025.



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.

Hybrid Mesh Firewall – Why the need?

Network

Private DC

Cloud

Cloud-Native

NetSec Admin

Server/VM Admin

Cloud Architect

DevSecOps

Organizational Challenges

Multiple teams, organizations and environments

Inconsistent islands of policy controls across environments

Gartner – Hybrid Mesh Firewall

Core & Optional Capabilities

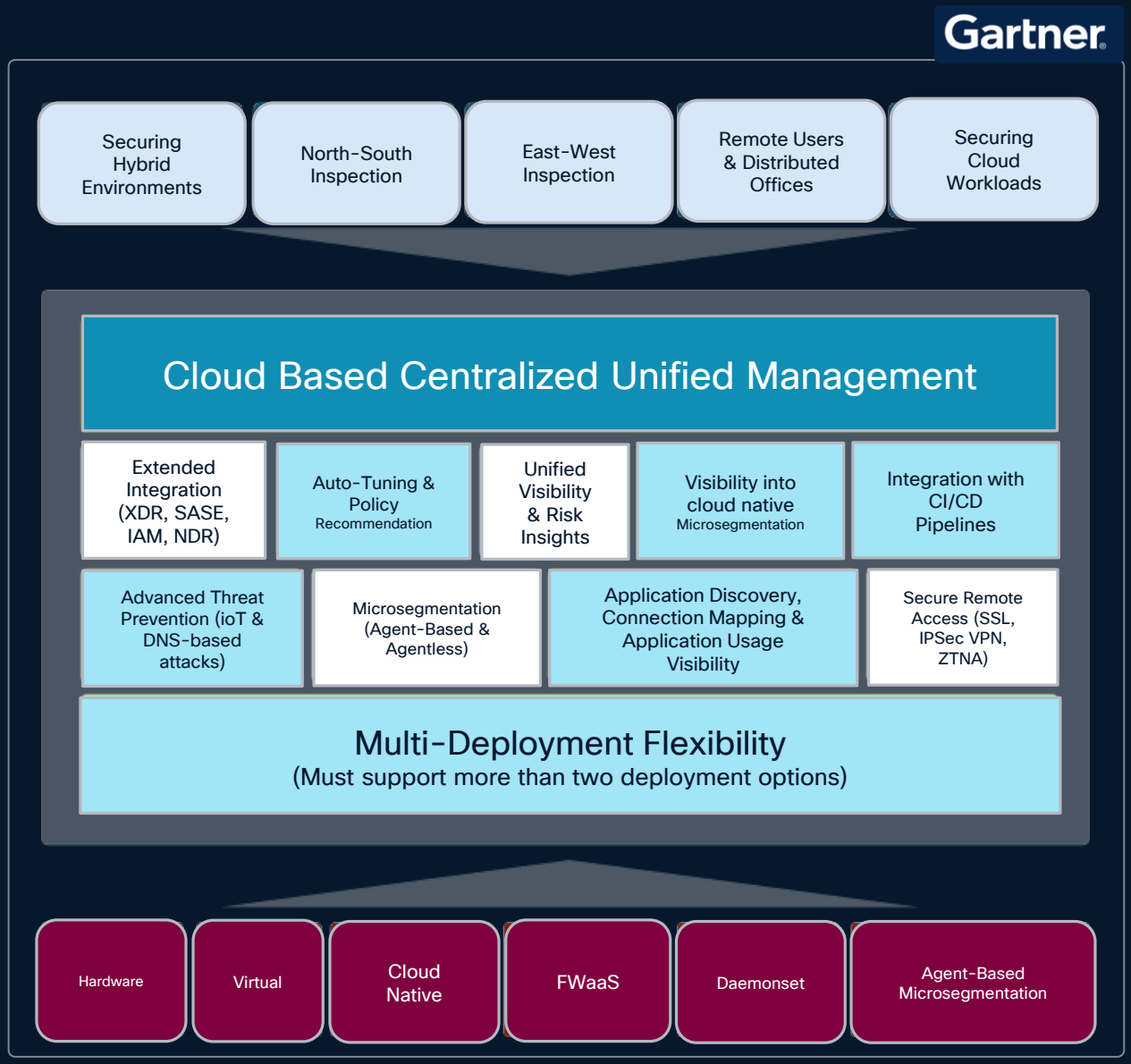
Gartner

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

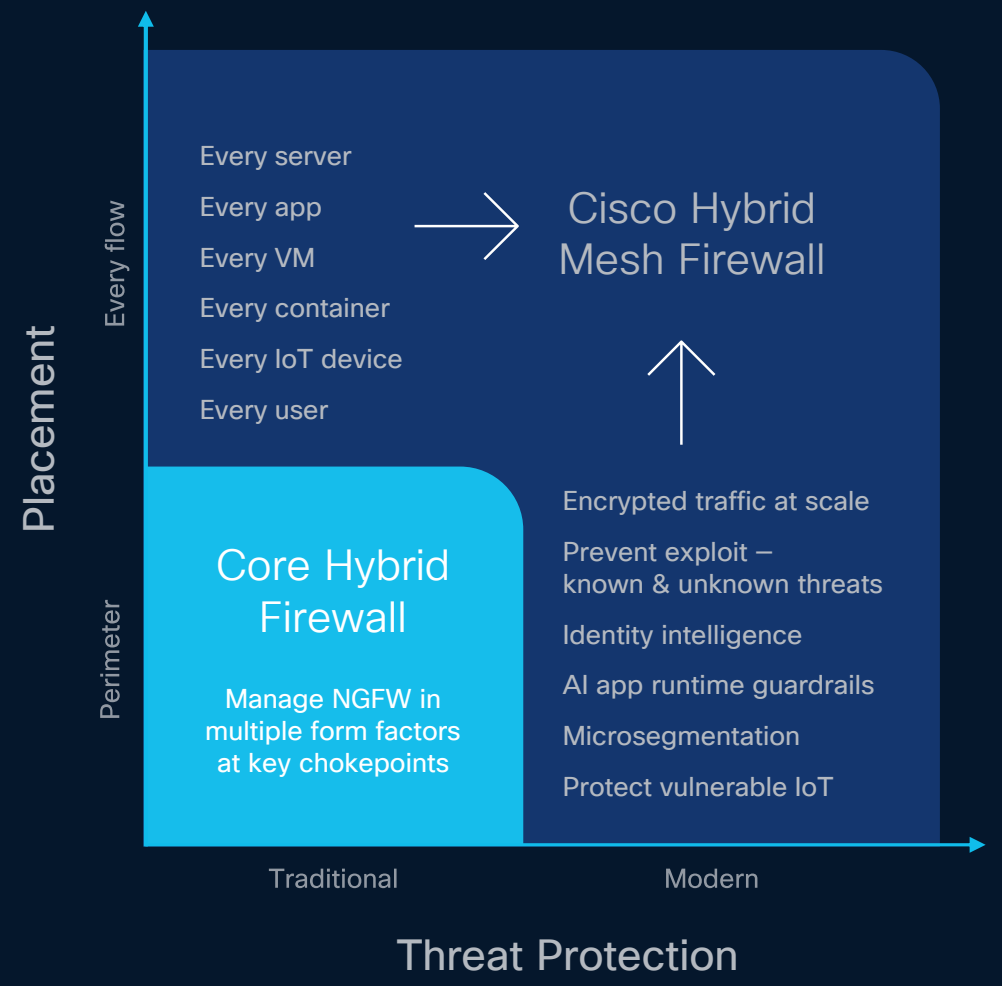
Cisco’s Vision – Hybrid Mesh Firewall

Our North Star

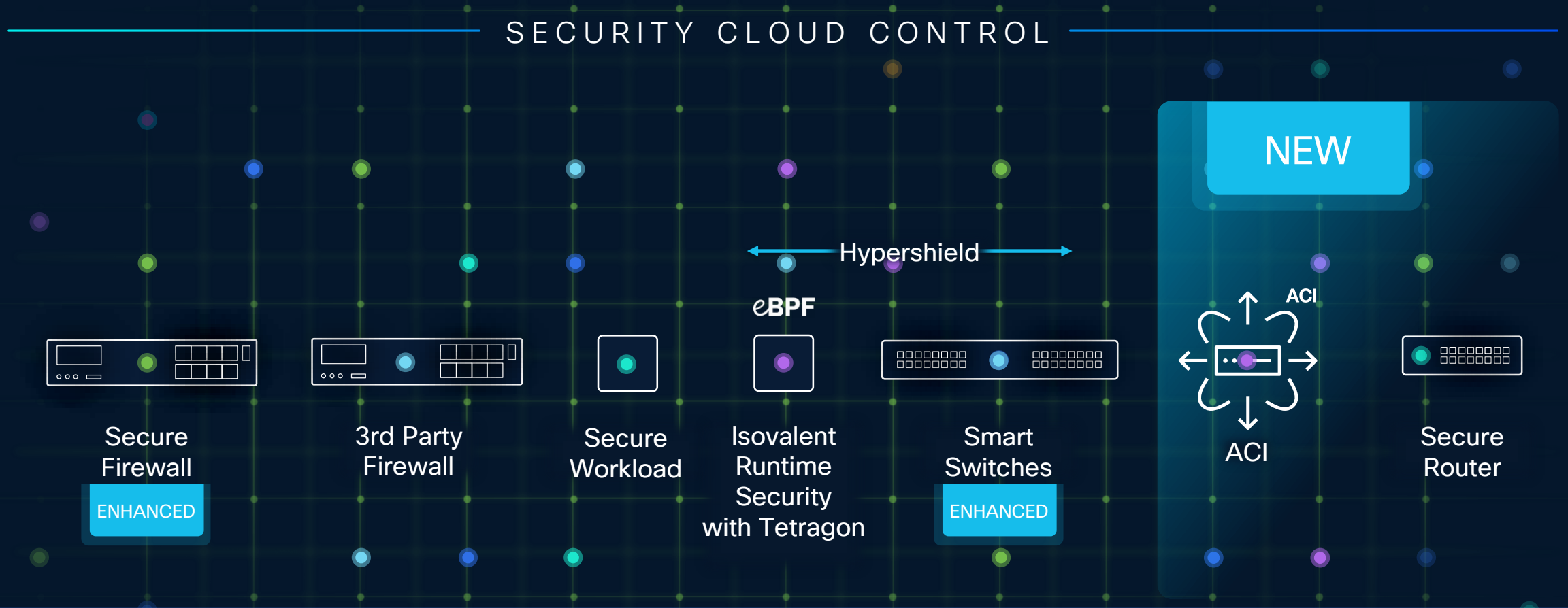
Make it easy for organizations to

- Reduce attack surface
- Prevent compromise
- Stop lateral movement

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



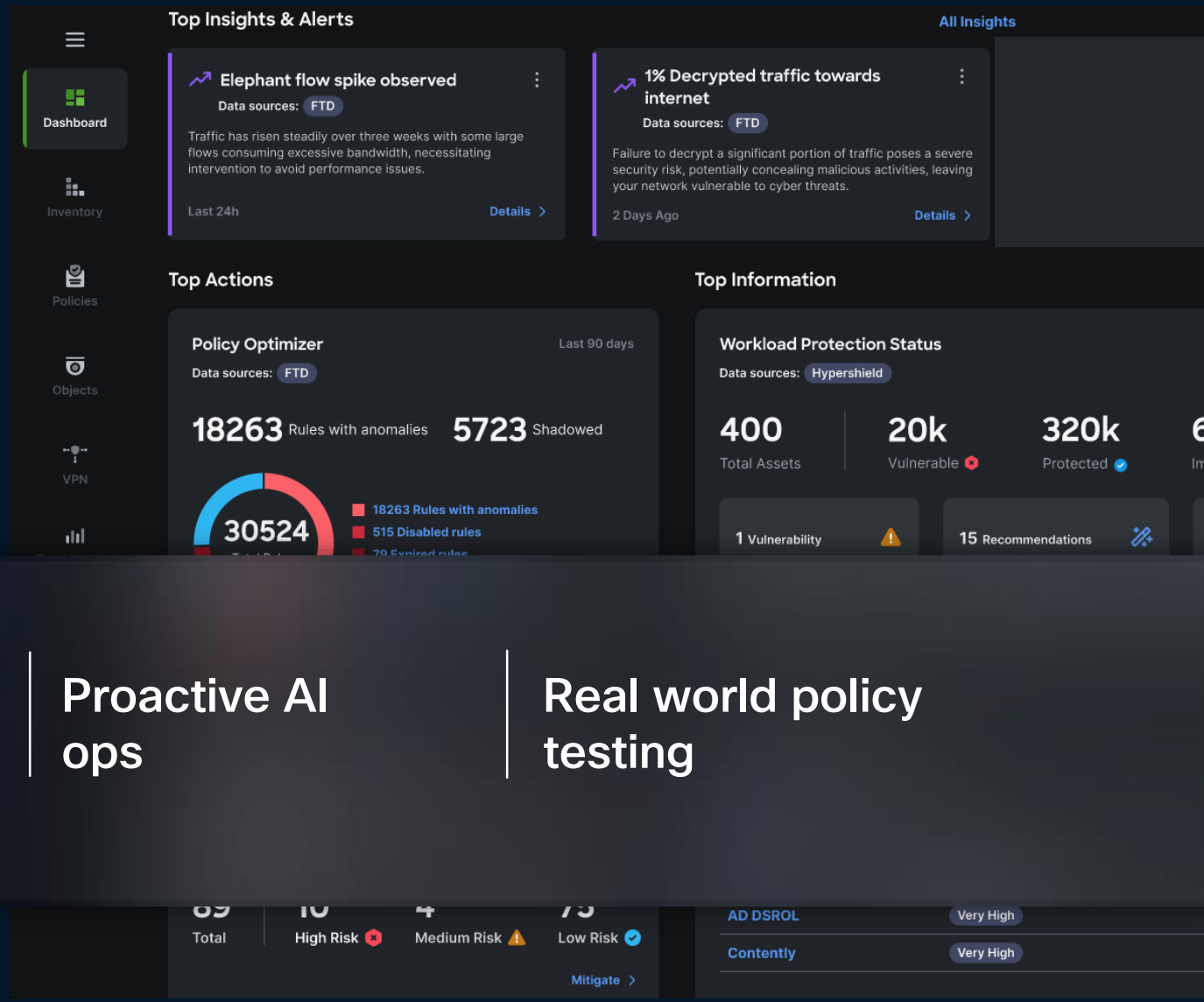
Cisco Hybrid Mesh Firewall



Write policy once, enforce across the mesh

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.

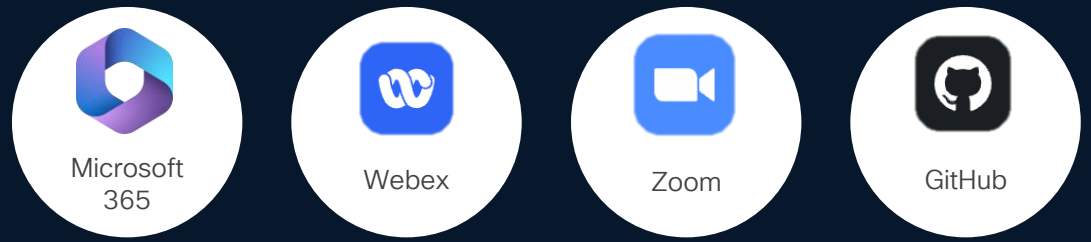
Cisco’s Hybrid Mesh Firewall: Architecture

Cisco Secure Dynamic Attribute Connecters

Cloud connectors

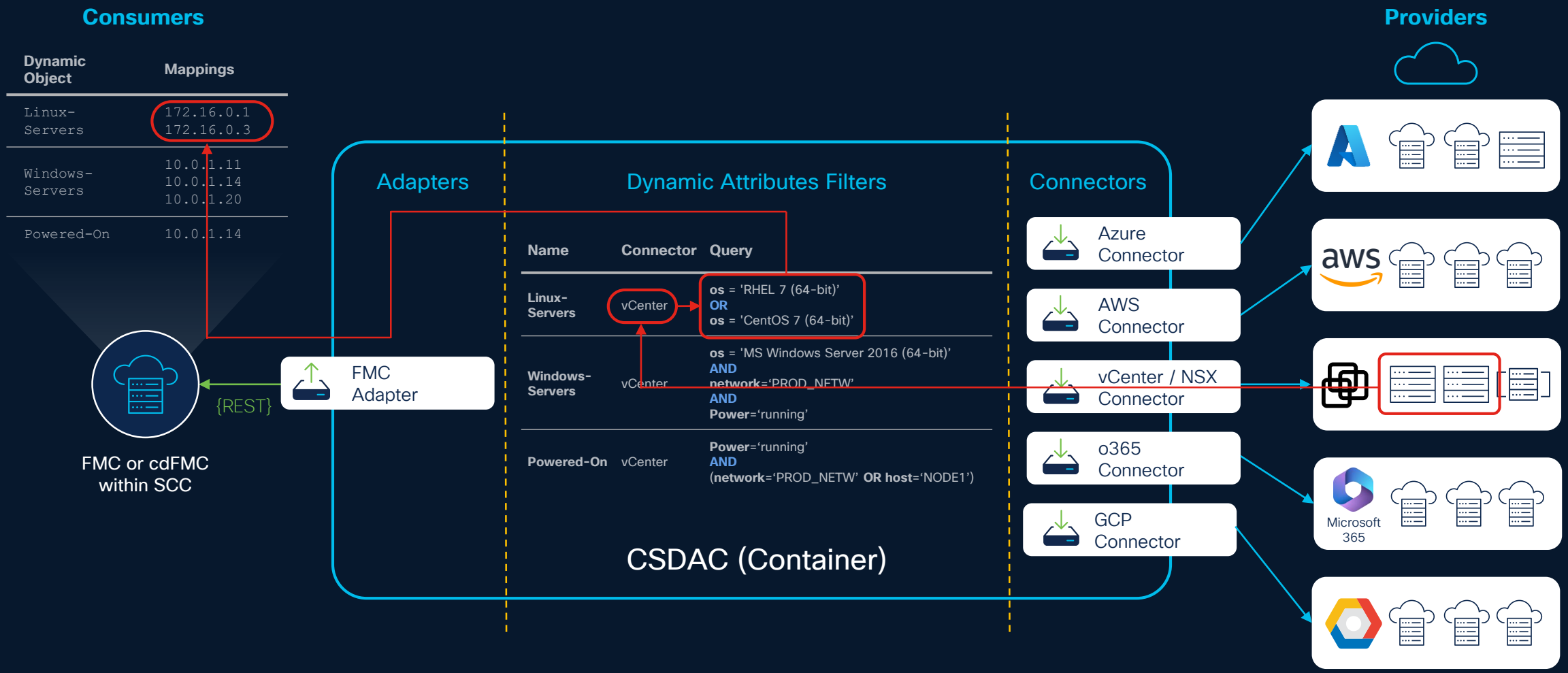
New!

Public feeds and external connectors

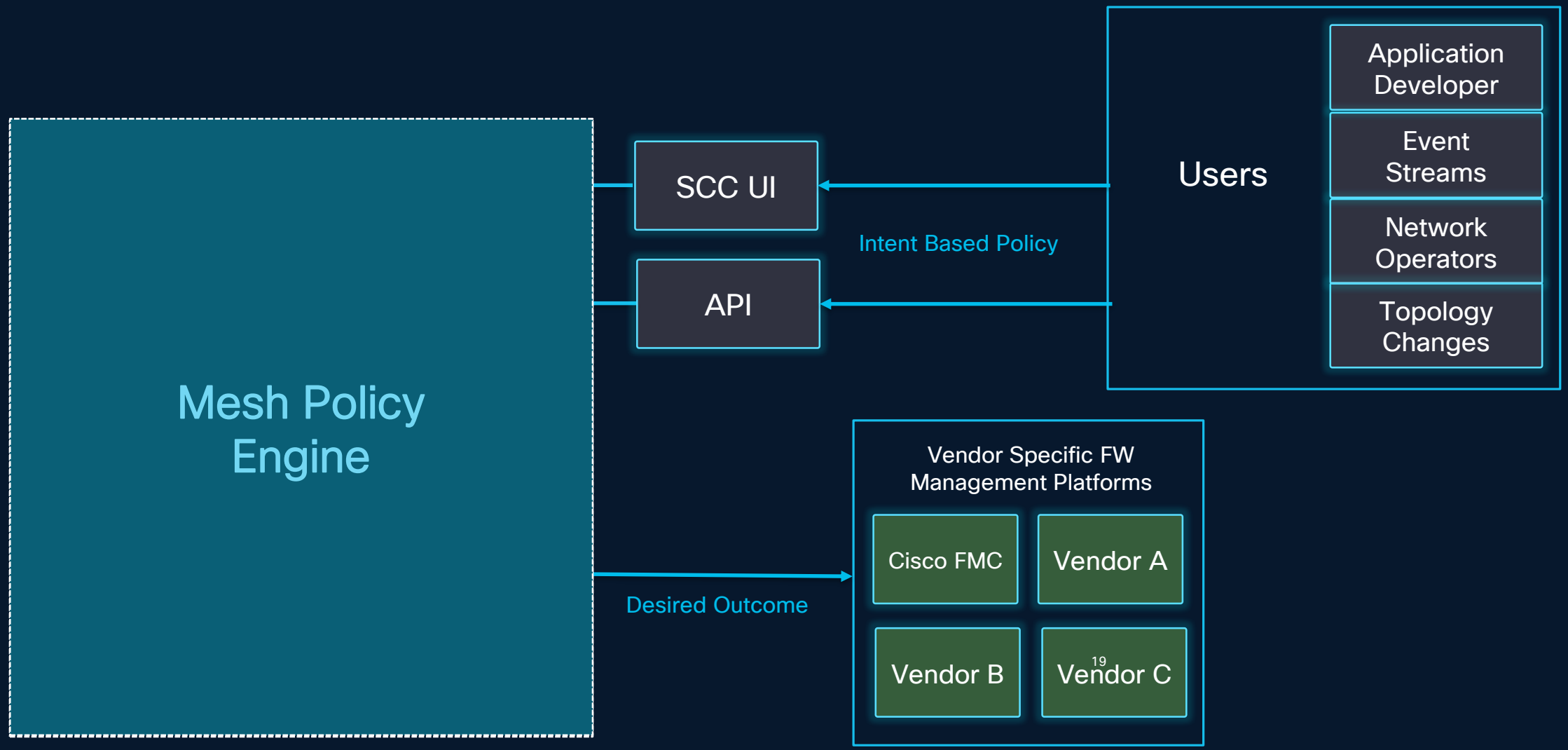


New!

Dynamic Attribute Connecter - Architecture



Policy Workflow & Architecture



Capabilities & Design Principles

Secure Firewall Capabilities

Superior visibility beyond deep packet inspection

Security Intelligence

Encrypted Visibility Engine

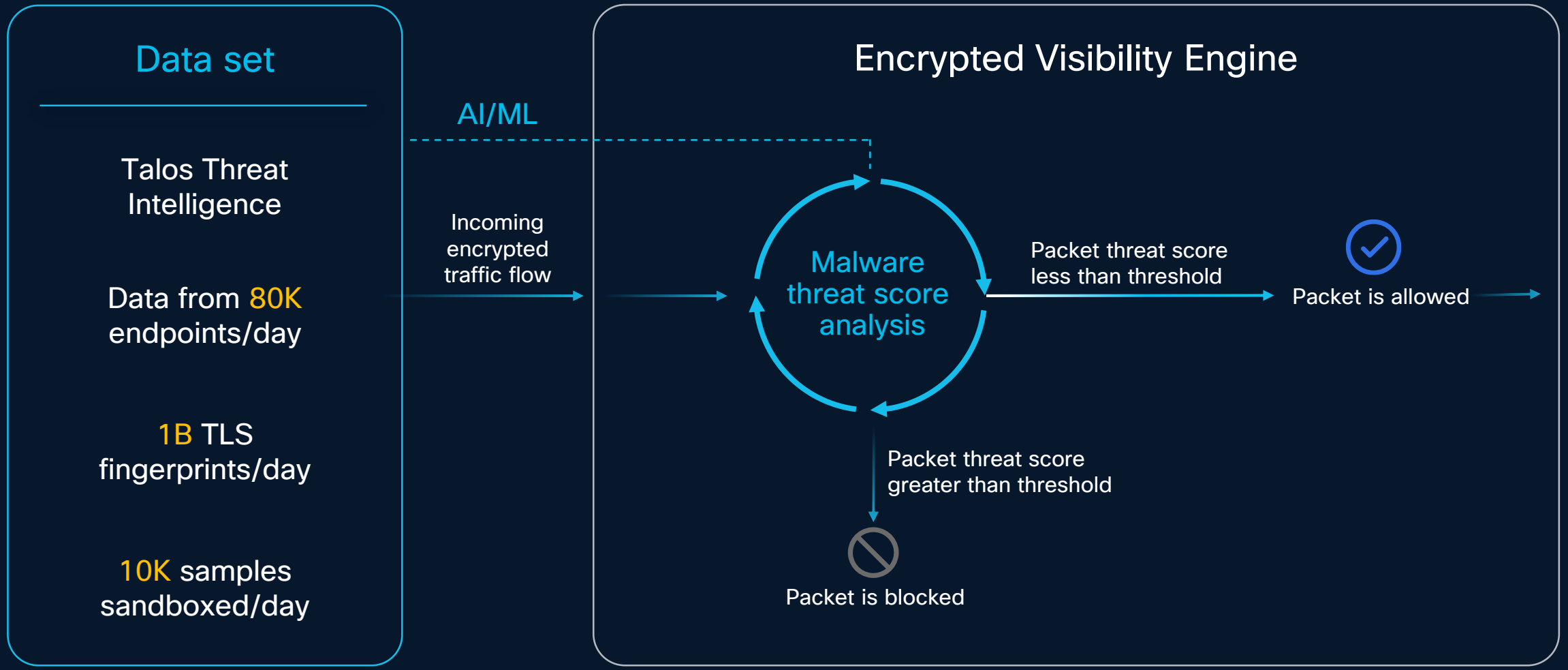
Snort 3 with SnortML

QUIC Decryption

Advanced Malware Protection

Secure Firewall Capabilities

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



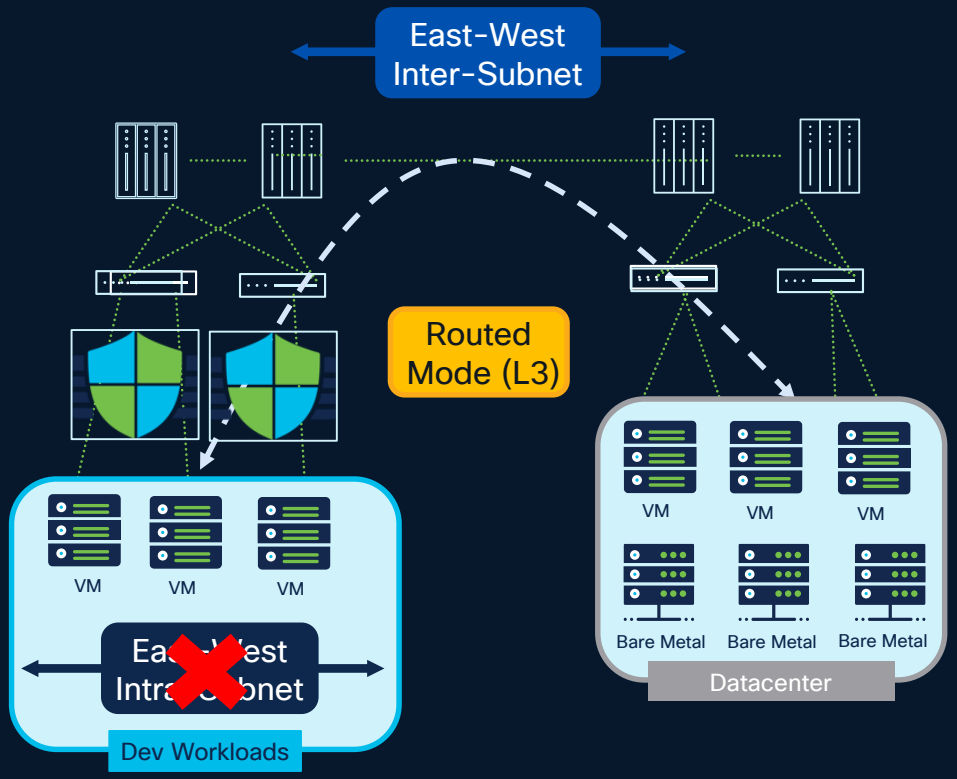
Secure Firewall Capabilities

Intelligent Selective Decryption

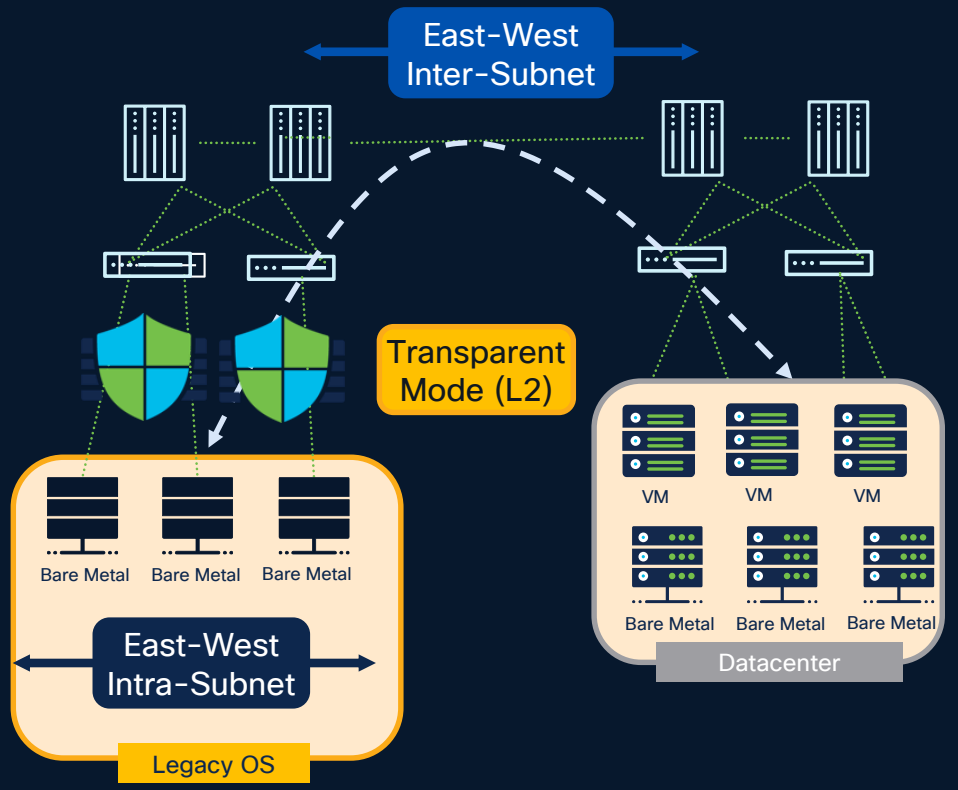
Risk-based intelligent decryption bypass, powered by EVE and Talos Server Reputation

Secure Workload Capabilities

Firewall Integration (FTD/FMC)



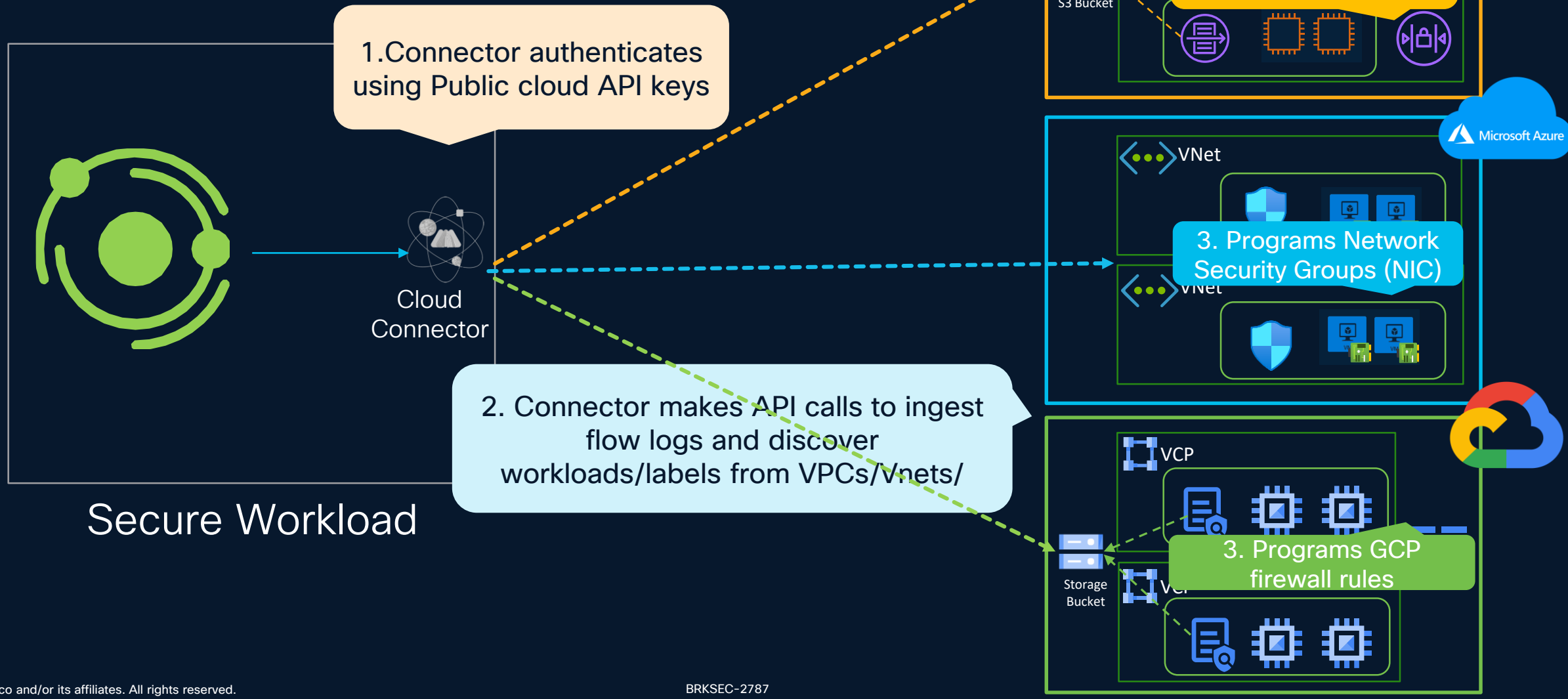
Layer 3 Firewall Insertion (Routed Mode)



Layer 2 Firewall Insertion (Transparent Mode)

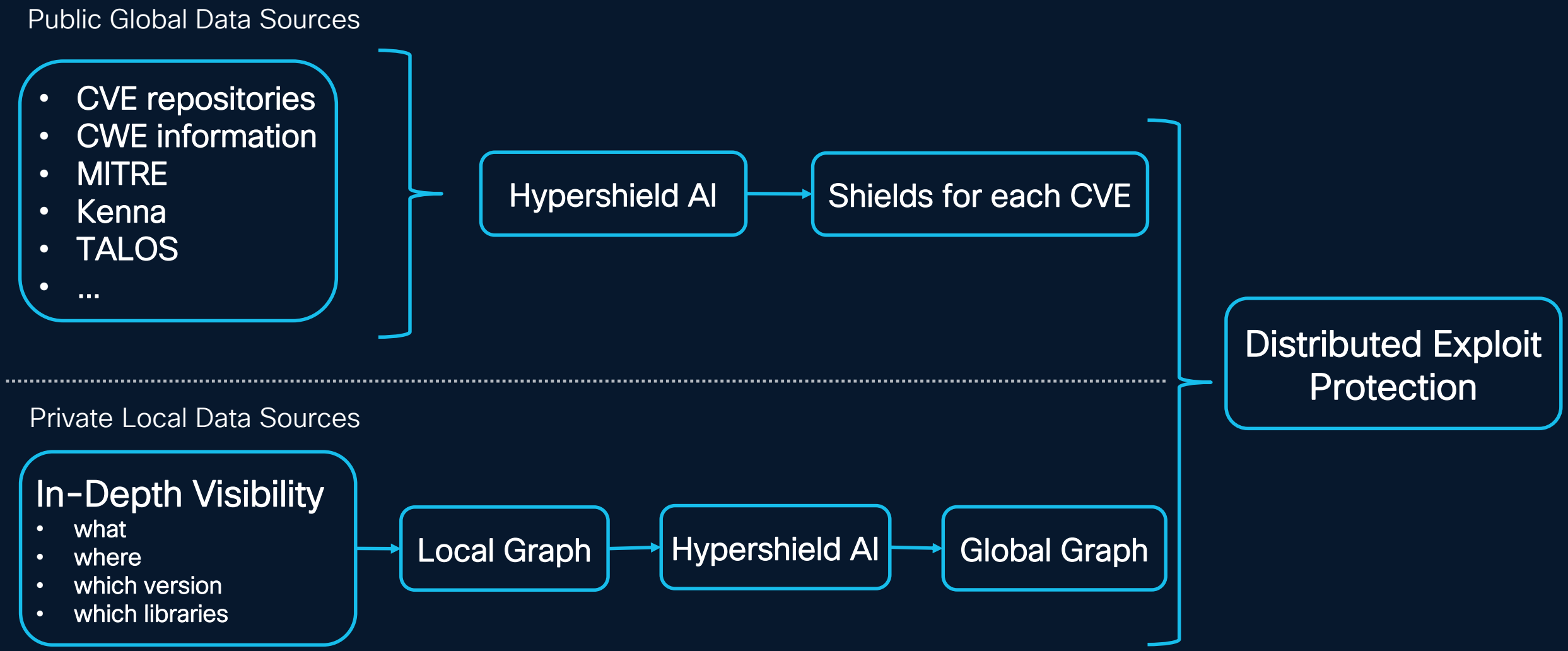
Secure Workload Capabilities

Cloud Native Firewall Integration (SGs, NSGs, GFWs)



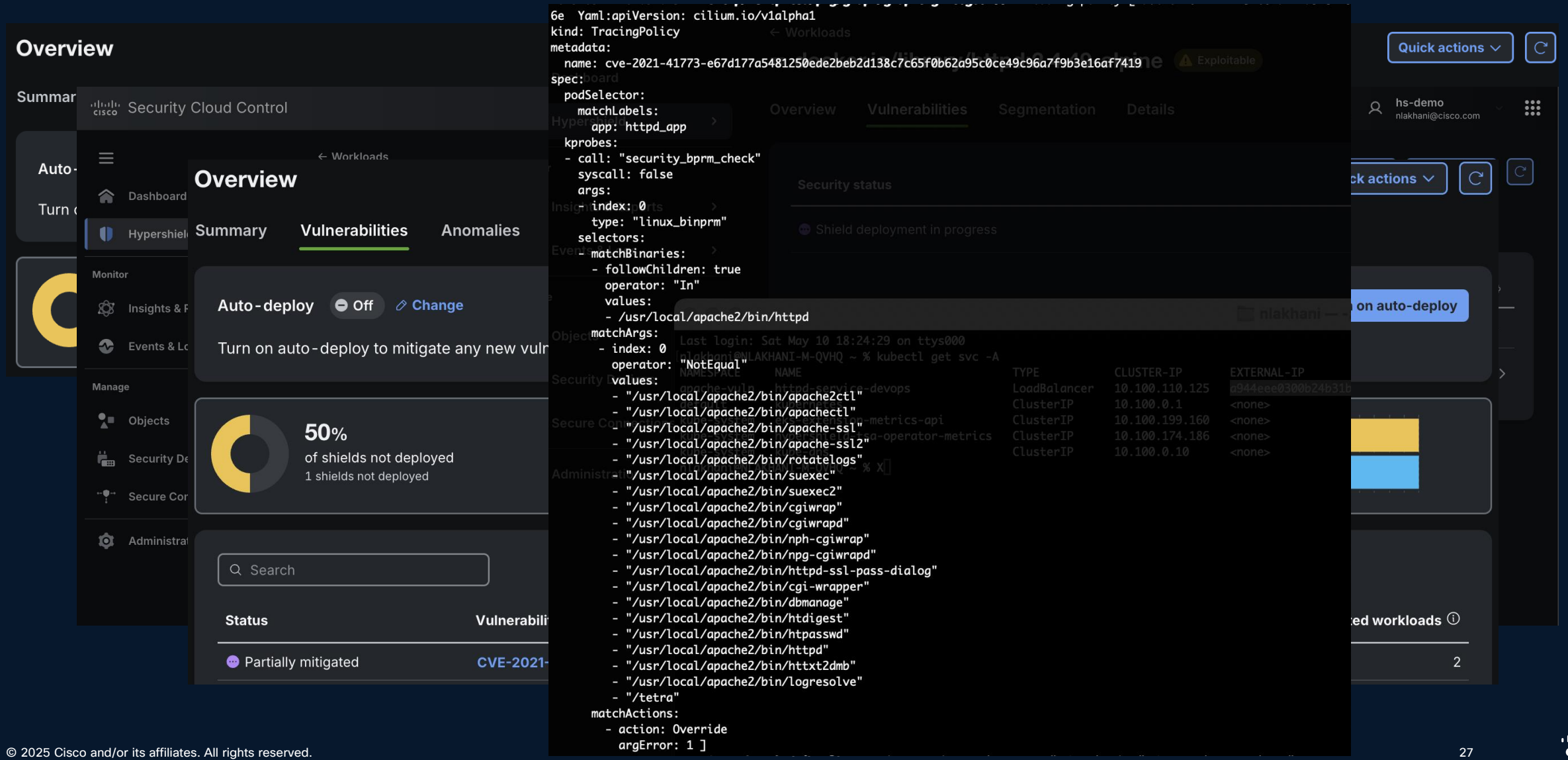
Hypershield Capabilities

Distributed Exploit Protection



Hypershield Capabilities

Distributed Exploit Protection



The Power of Cisco & AMD Hardware

Unmatched programmability, performance, flexibility, and efficiency with Silicon One and AMD DPU

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

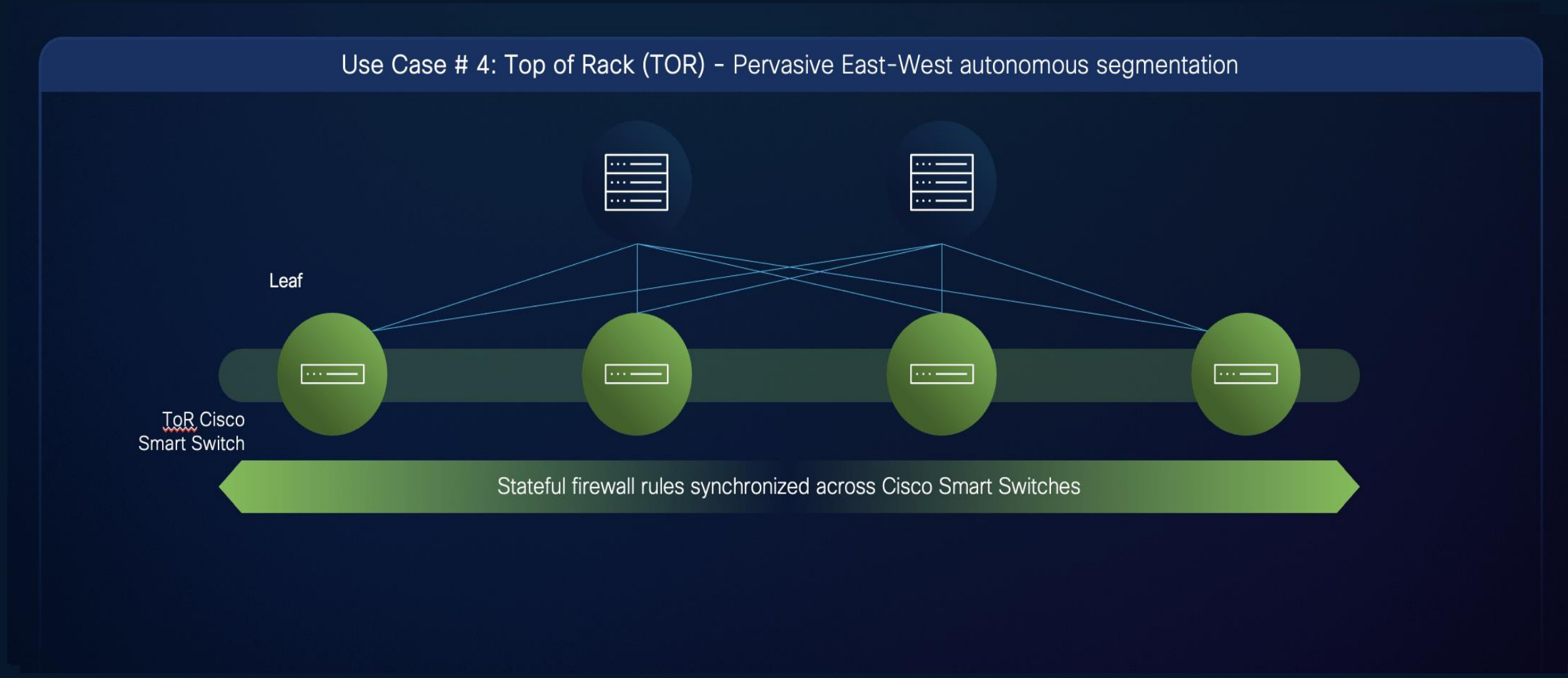
Large-Scale NAT | IPSEC Encryption | Distributed Firewall | Event-Based Telemetry | DoS Protection

Hypershield Capabilities

Nexus Smart Switch

Hypershield Capabilities

Nexus Smart Switch – Use Cases



Cisco Secure Access - 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

Cisco Secure Access - UZTNA

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

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™

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

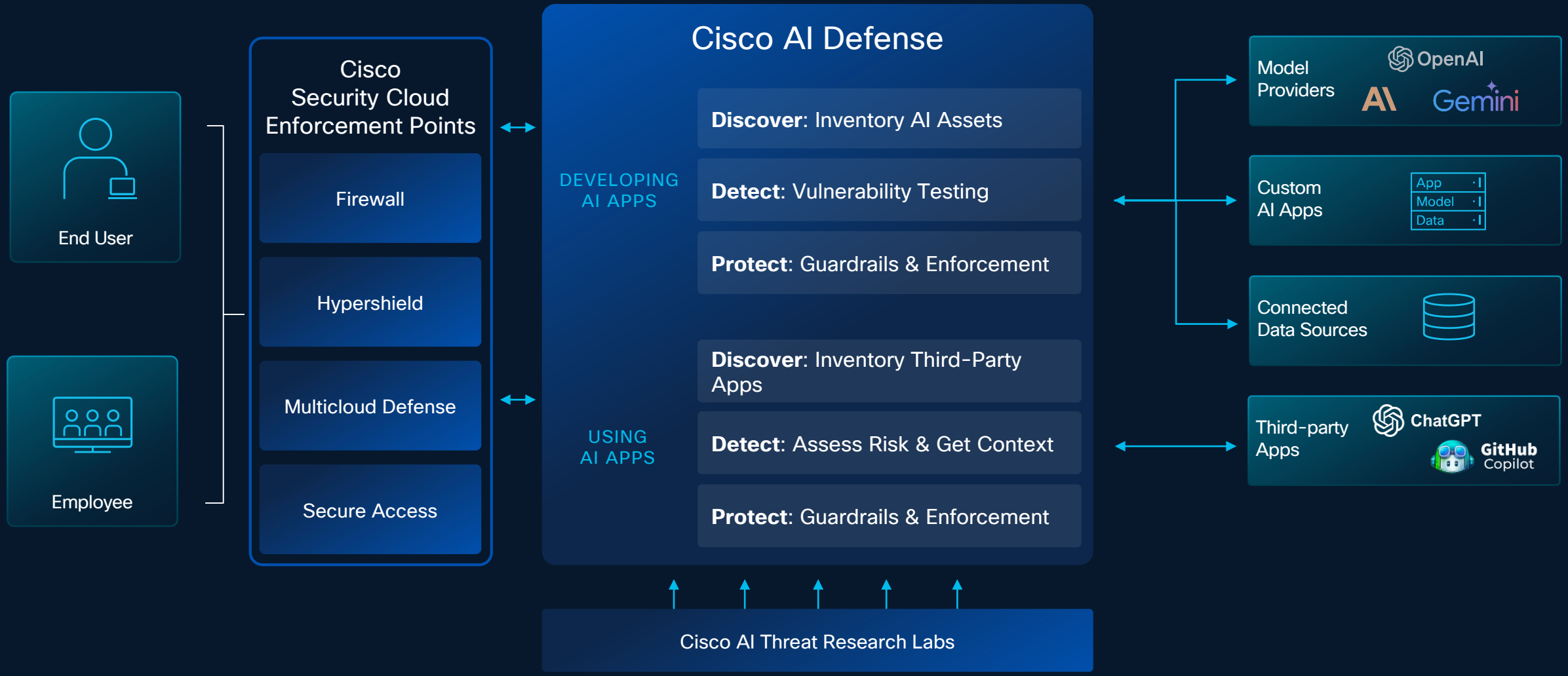
Misinformation from LLMs poses a core vulnerability for applications relying on these models. Misinformation occurs when LLMs produce...

LLM10 Unbounded Consumption

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

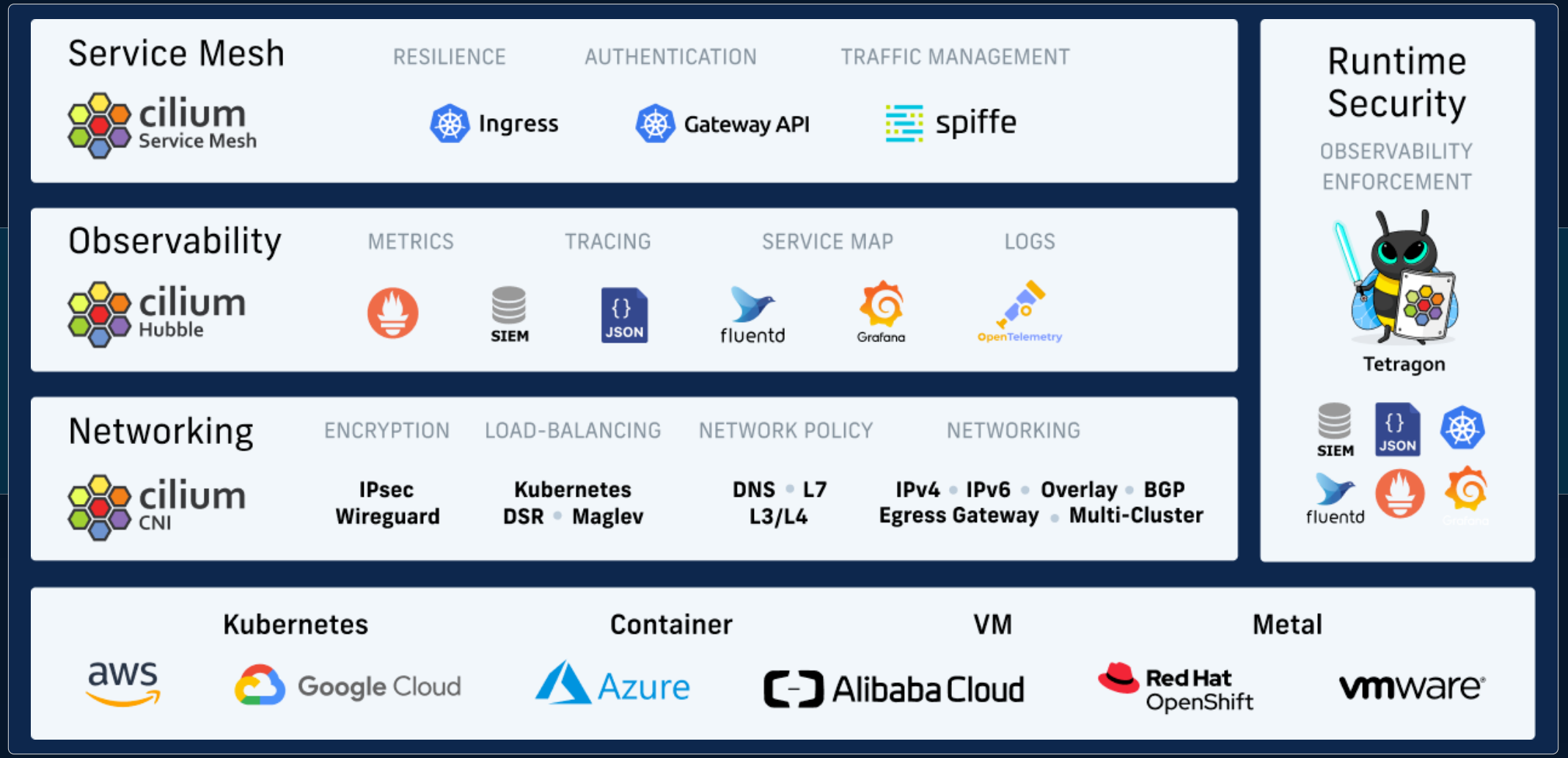
AI Defense Capabilities

Model Protection, Flexible Enforcement Options



Isovalent Capabilities

Cilium – Container Network Interface (CNI)



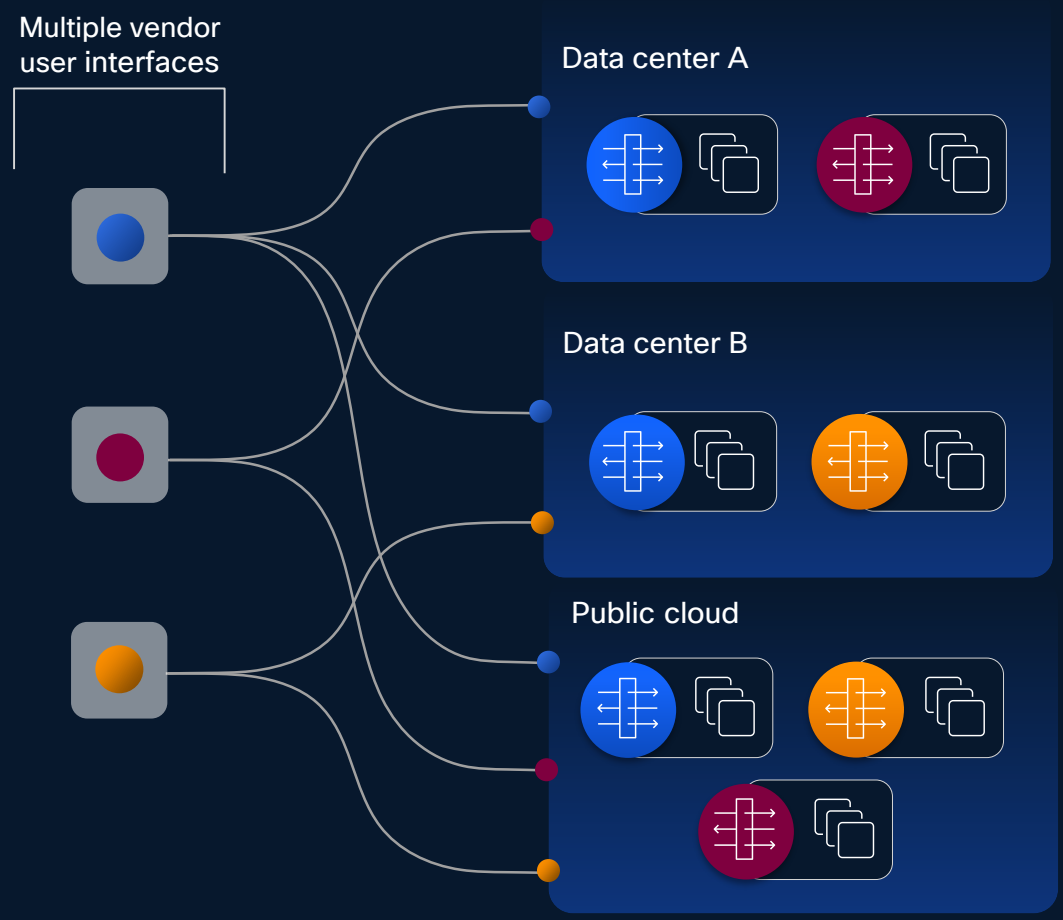
Cisco Mesh Policy Engine

Today, firewall policy management is fragmented

Traditional policy management

- Policy configuration is device-by-device
- Translating one intent to multiple policies across vendors takes time and is error-prone
- Adding firewall devices over time makes the problem exponentially worse

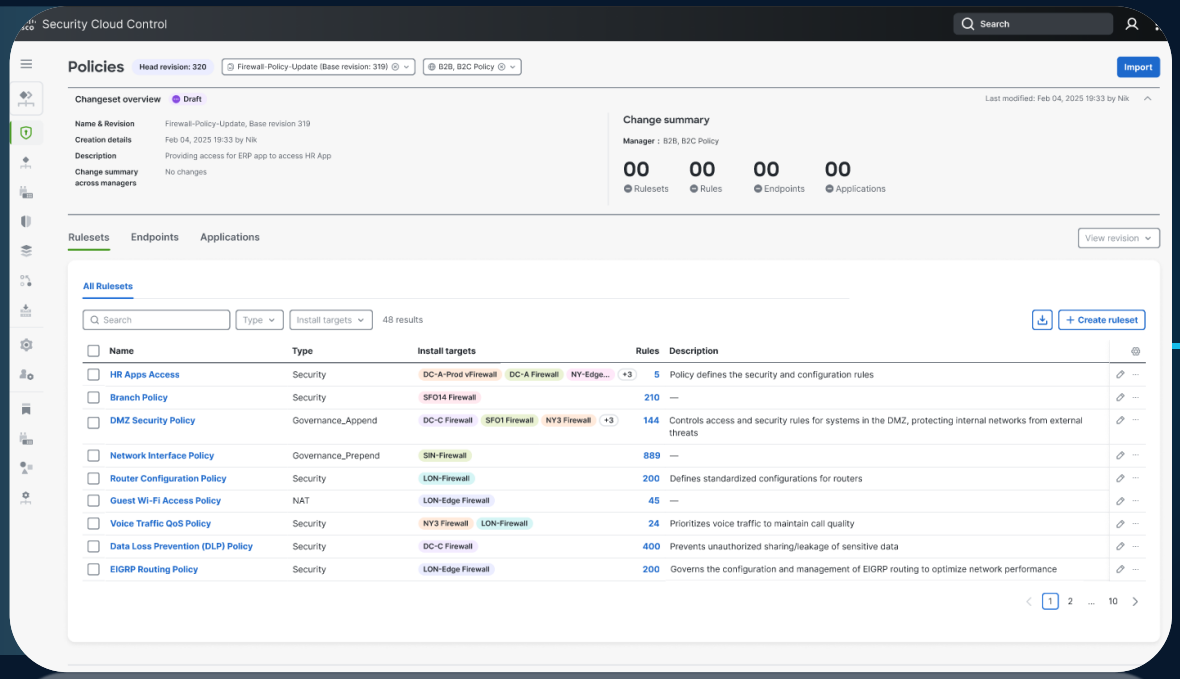
Solving these challenges requires a different approach



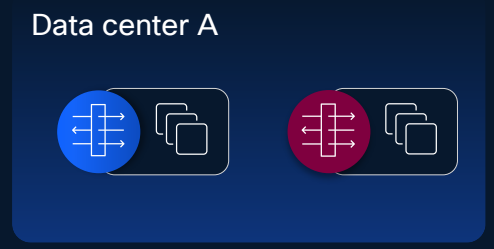
Cisco Mesh Policy Engine

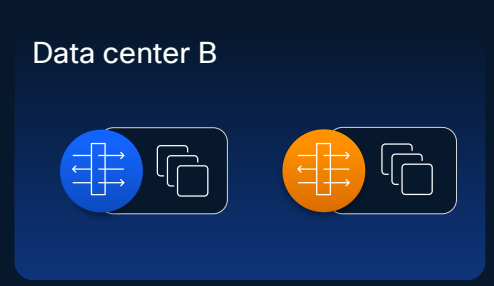
Cisco is the only enterprise firewall vendor that extends policy to non-Cisco enterprise firewalls

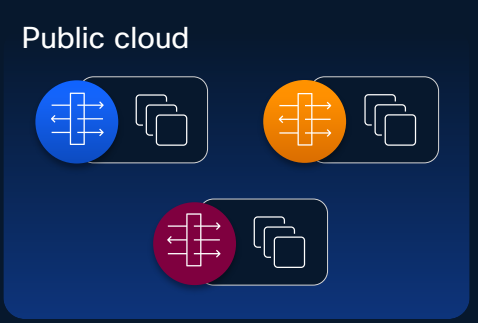
- A policy manager (not a device manager or policy converter)
- Retain the “what” and “where” of the policy **and** the “why”
- Change enforcement points, not policy
- Cisco plus the other enterprise firewall vendors



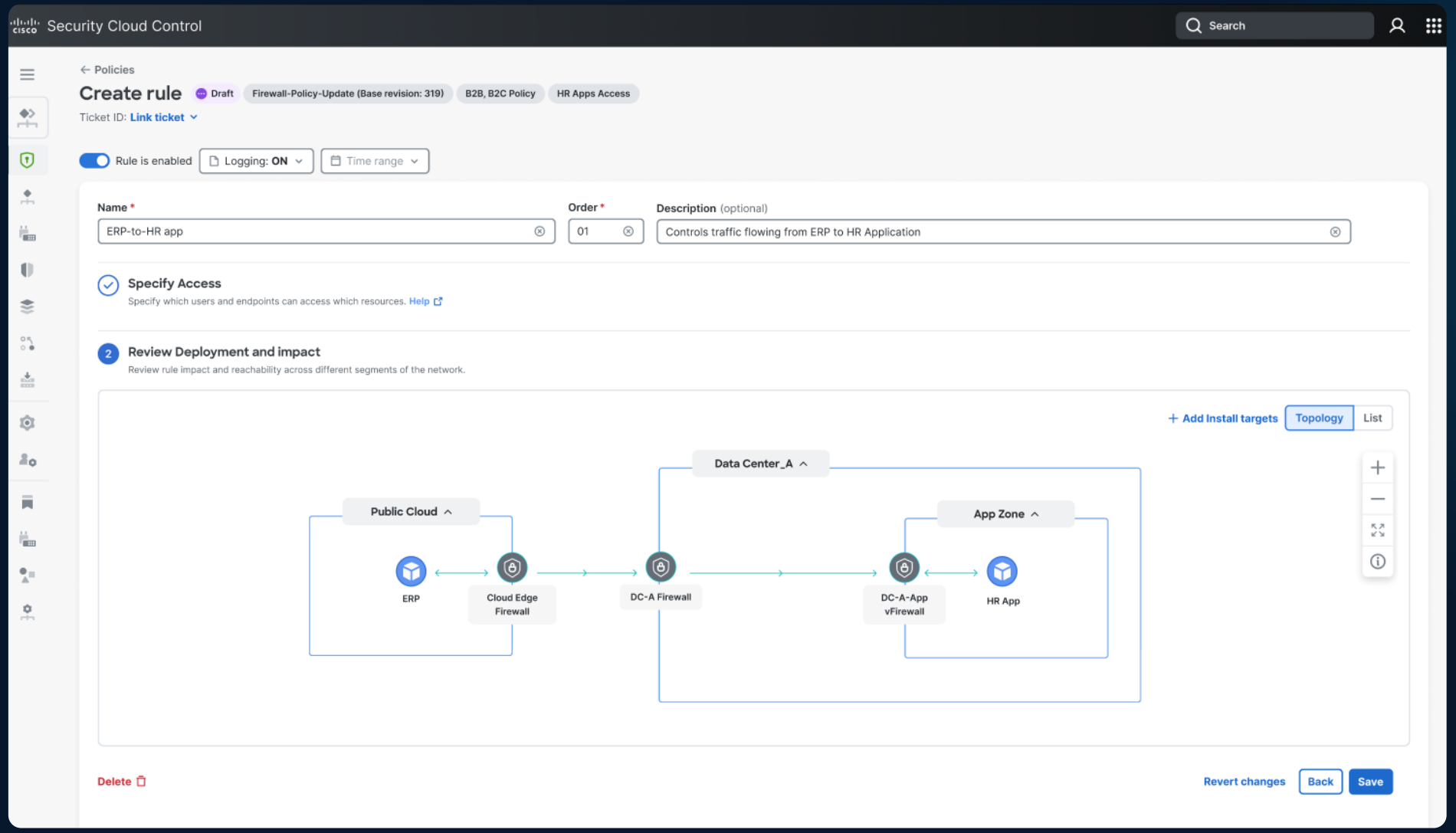
Cisco Security Cloud Control







Program once, enforce everywhere



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

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.

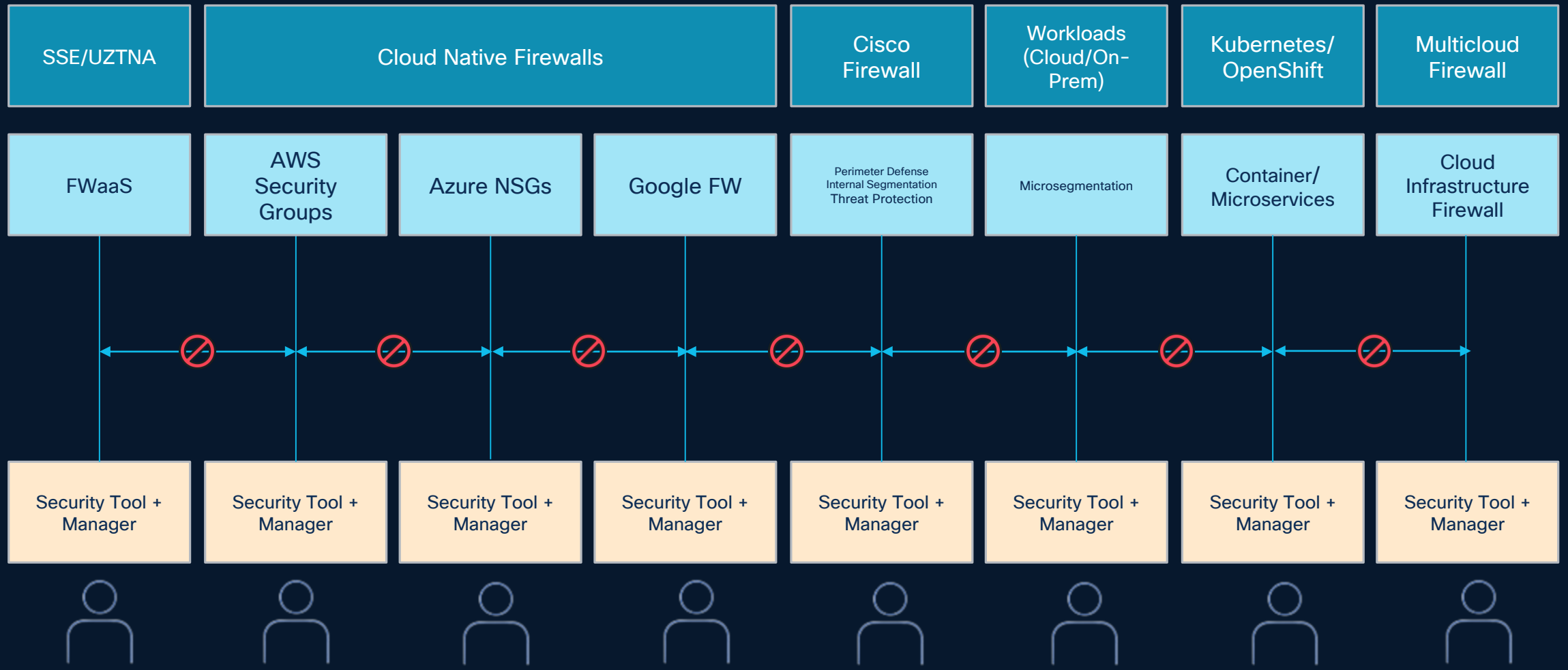
Segmentation Compatibility Gap: Their existing on-premises segmentation solution is incompatible with GCP, preventing consistent security enforcement.

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.

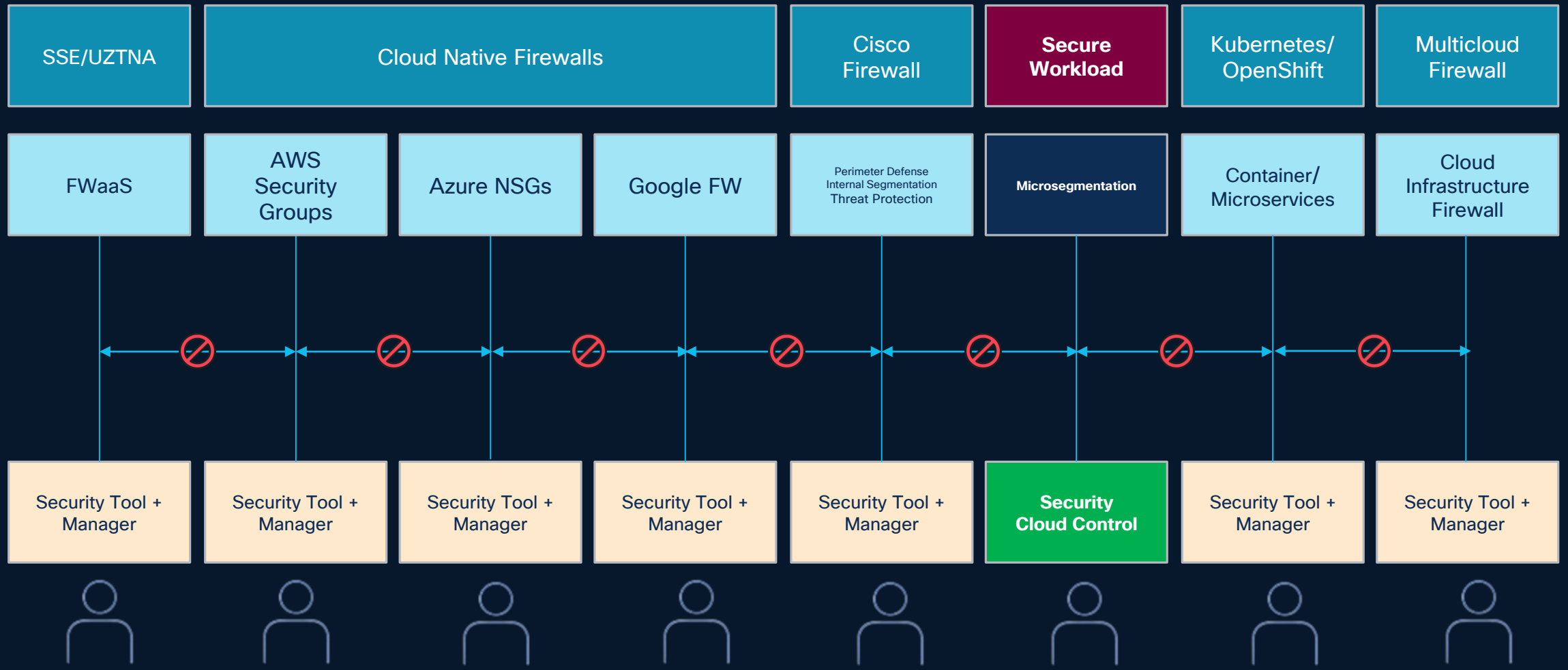
Customer Use Case # 1

Microsegmentation for Compliance



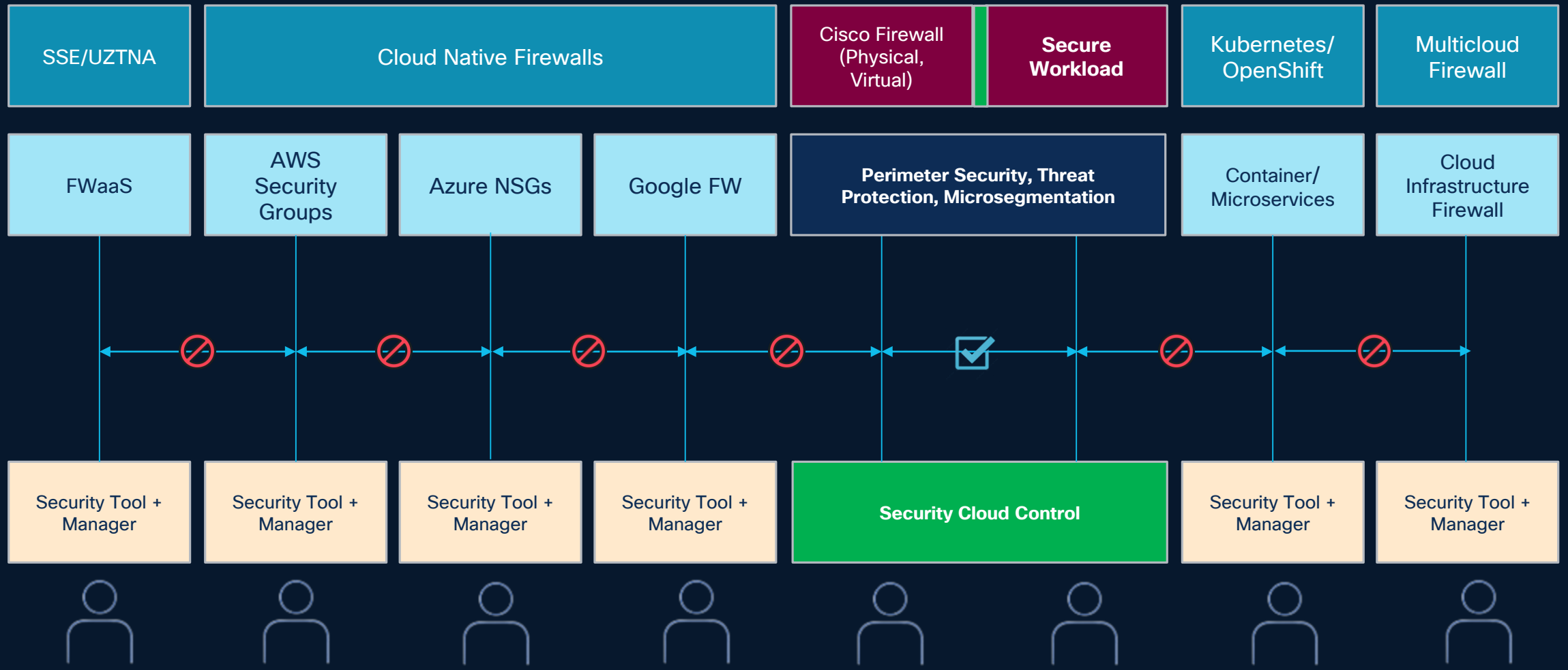
Customer Use Case # 1

Microsegmentation for Compliance



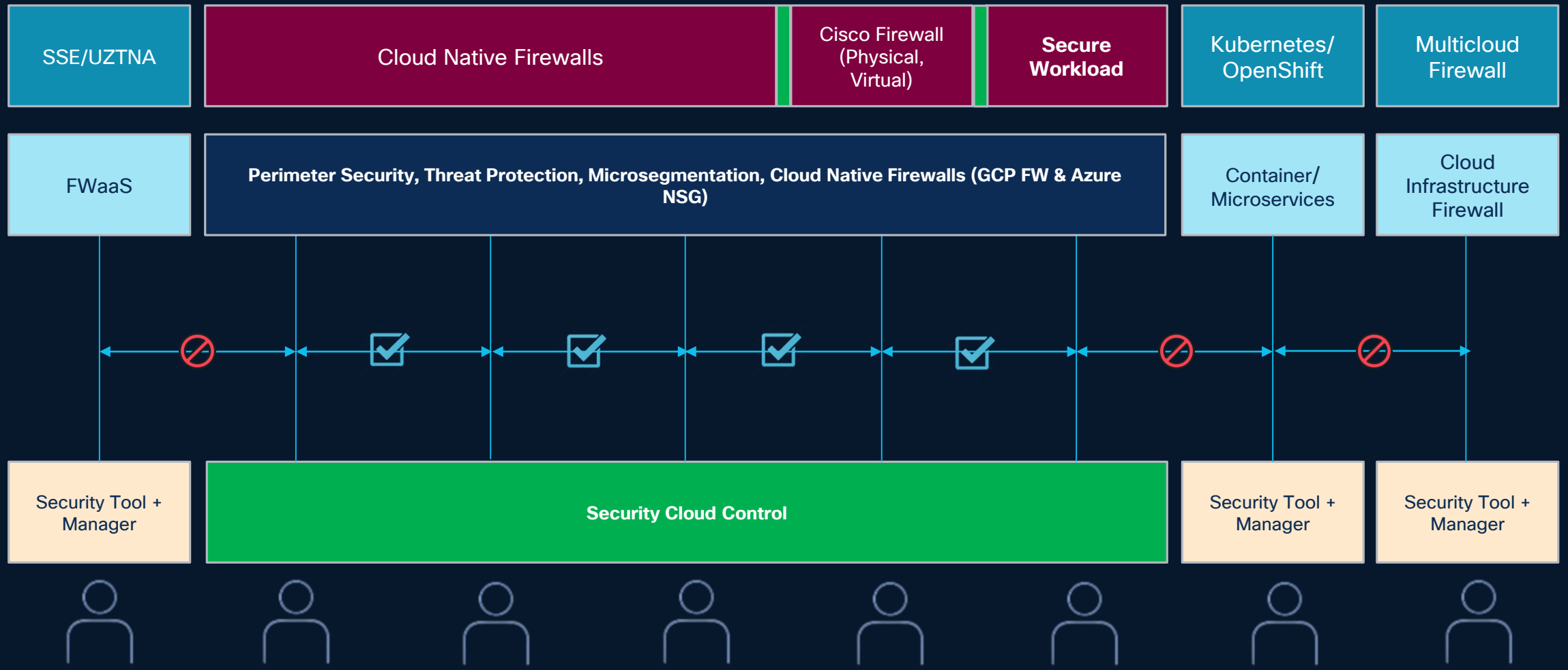
Customer Use Case # 1

Microsegmentation for Compliance



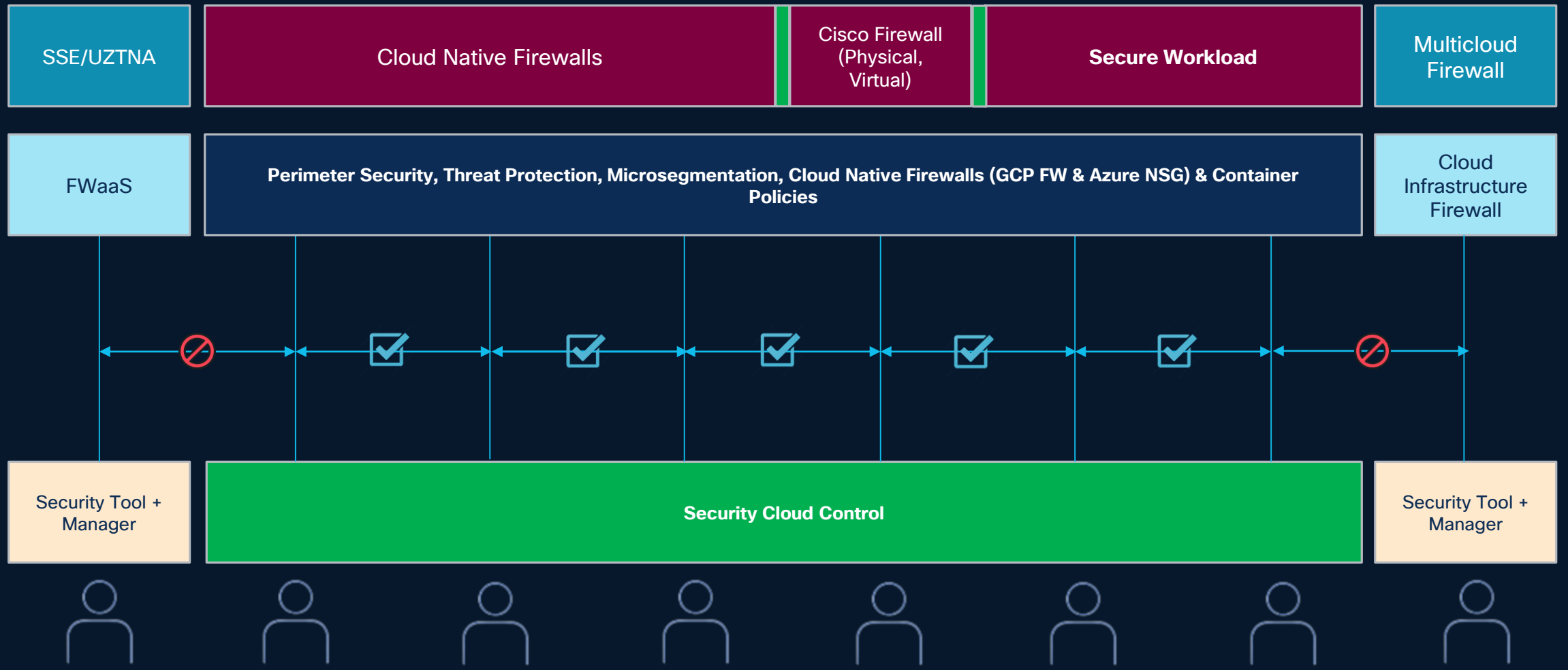
Customer Use Case # 1

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.

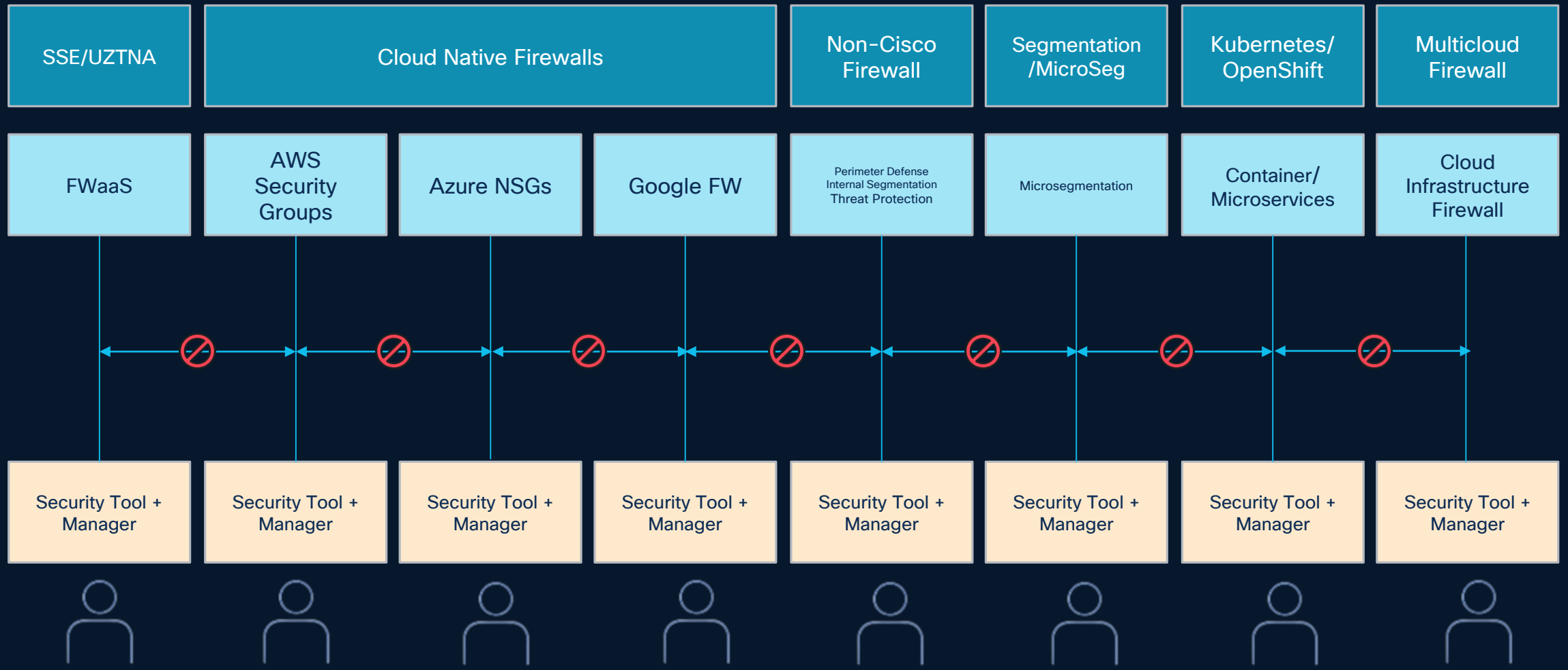
Policy Inconsistency: Fragmentation leads to inconsistent security policies across the environment.

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.

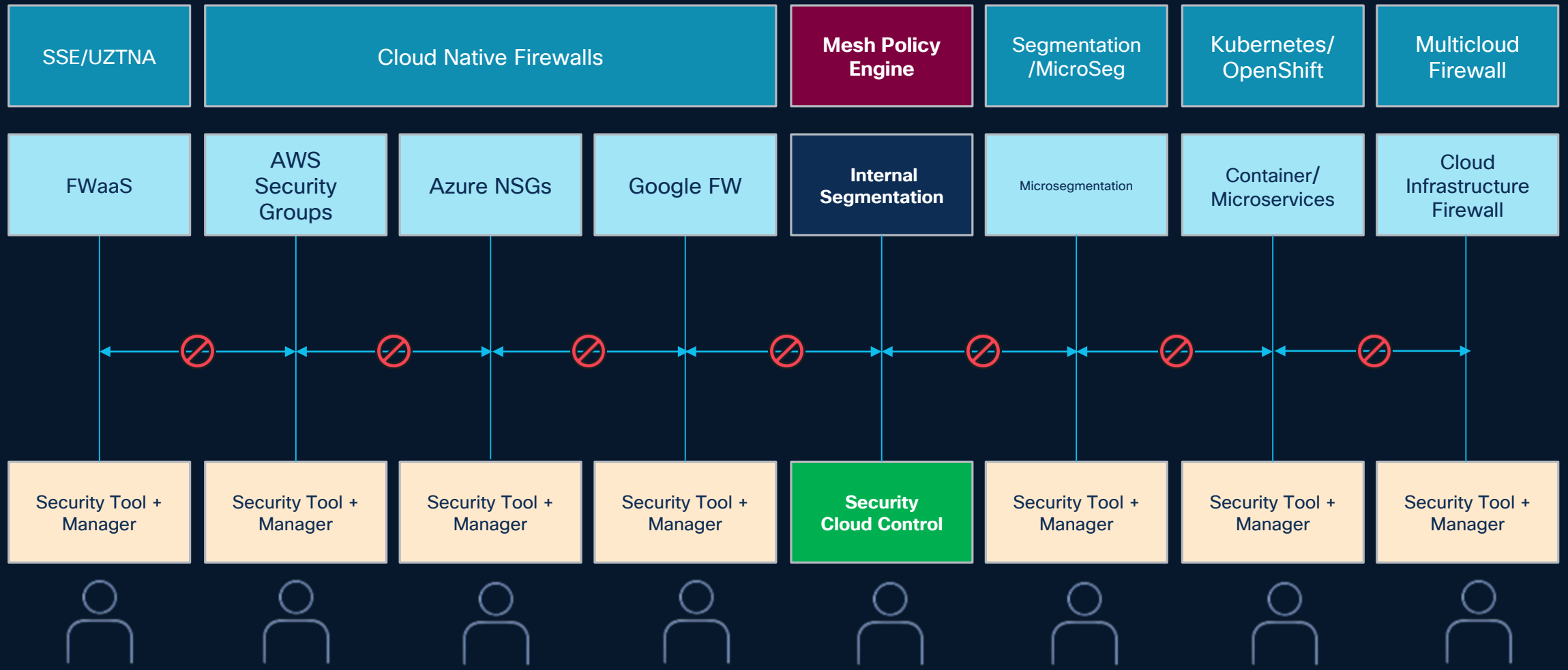
Customer Use Case # 2

Multi-Vendor Firewall Management



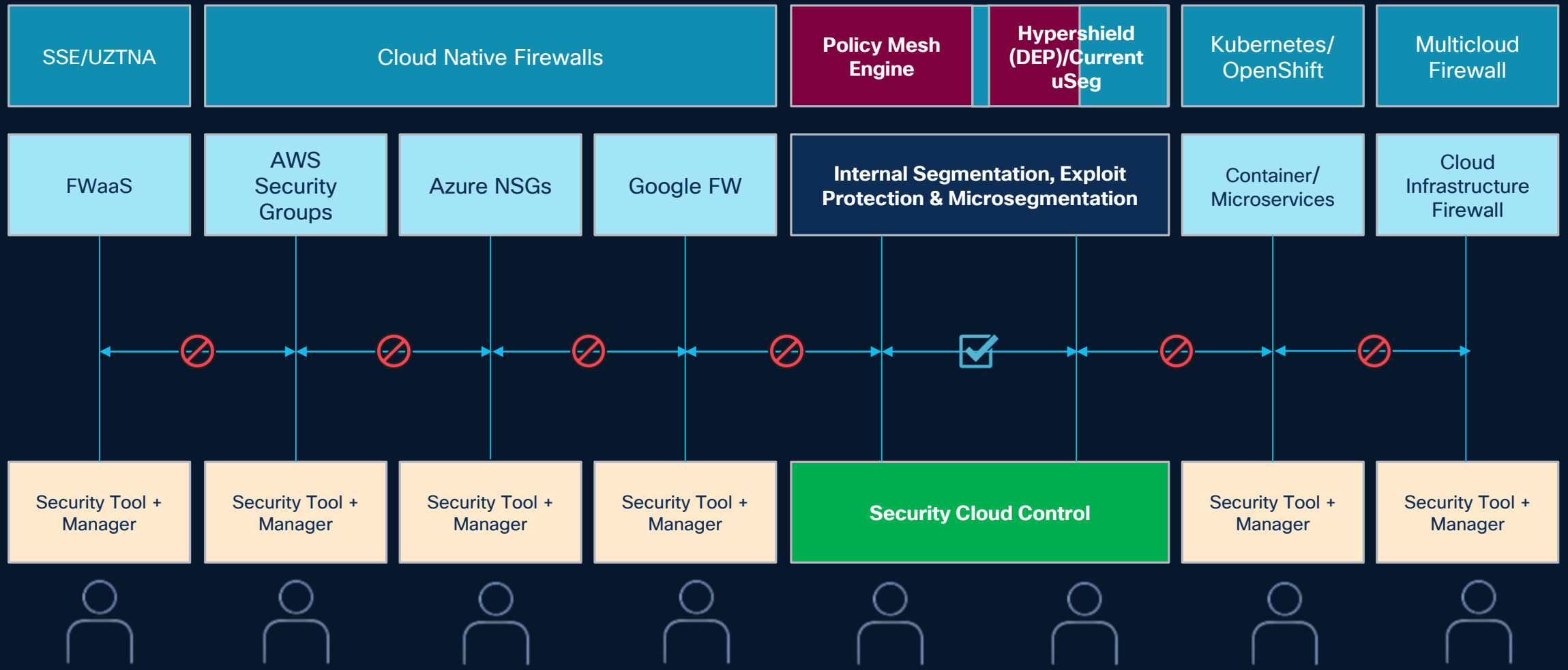
Customer Use Case # 2

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.

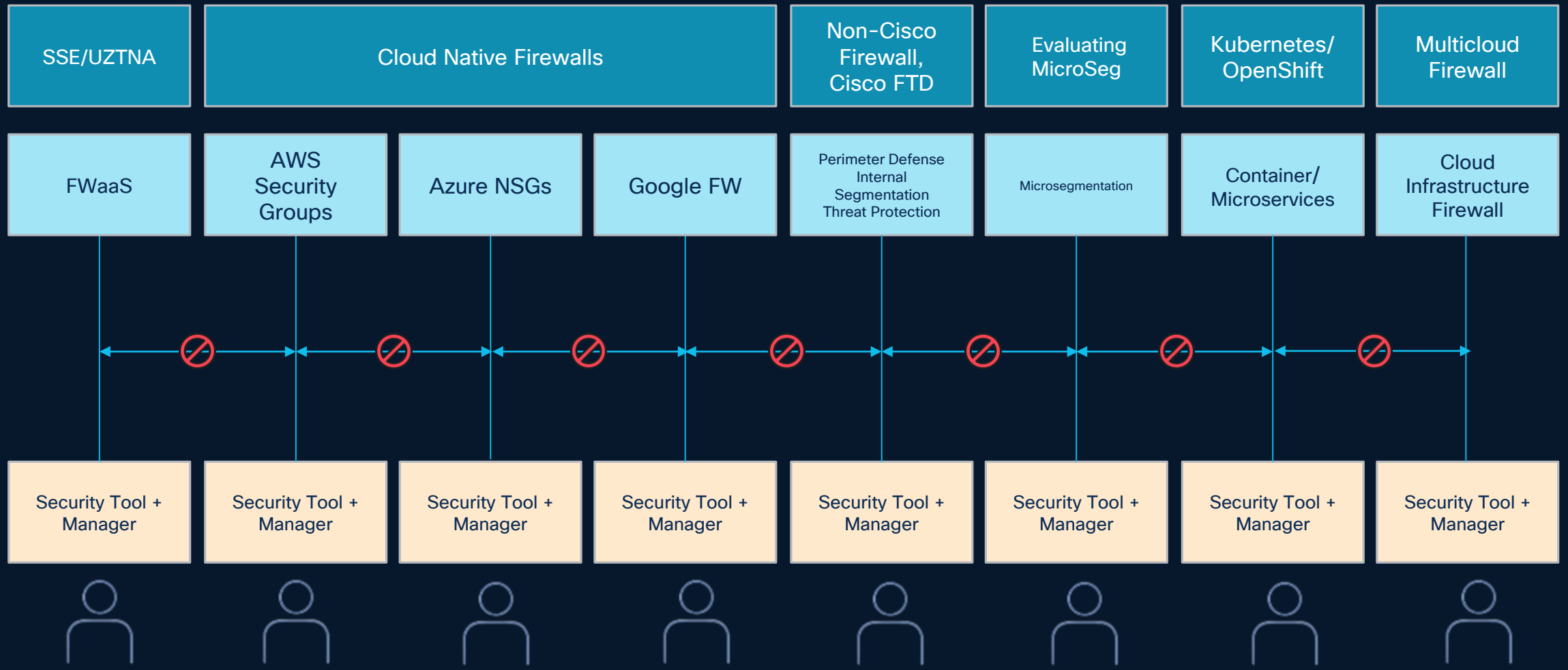
Legacy Tooling Limitations: Current tools lack the agility and granularity for dynamic, distributed containers.

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.

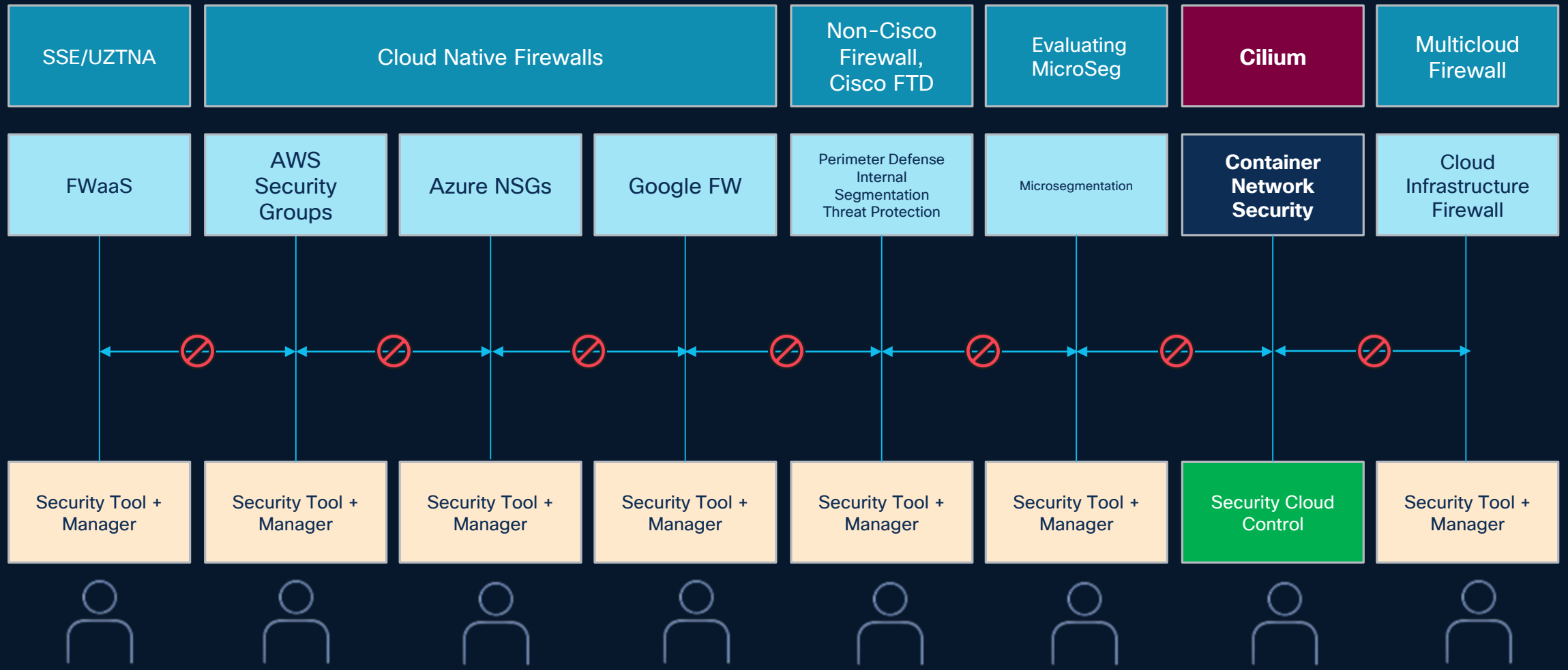
Customer Use Case # 3

Container Network Policy



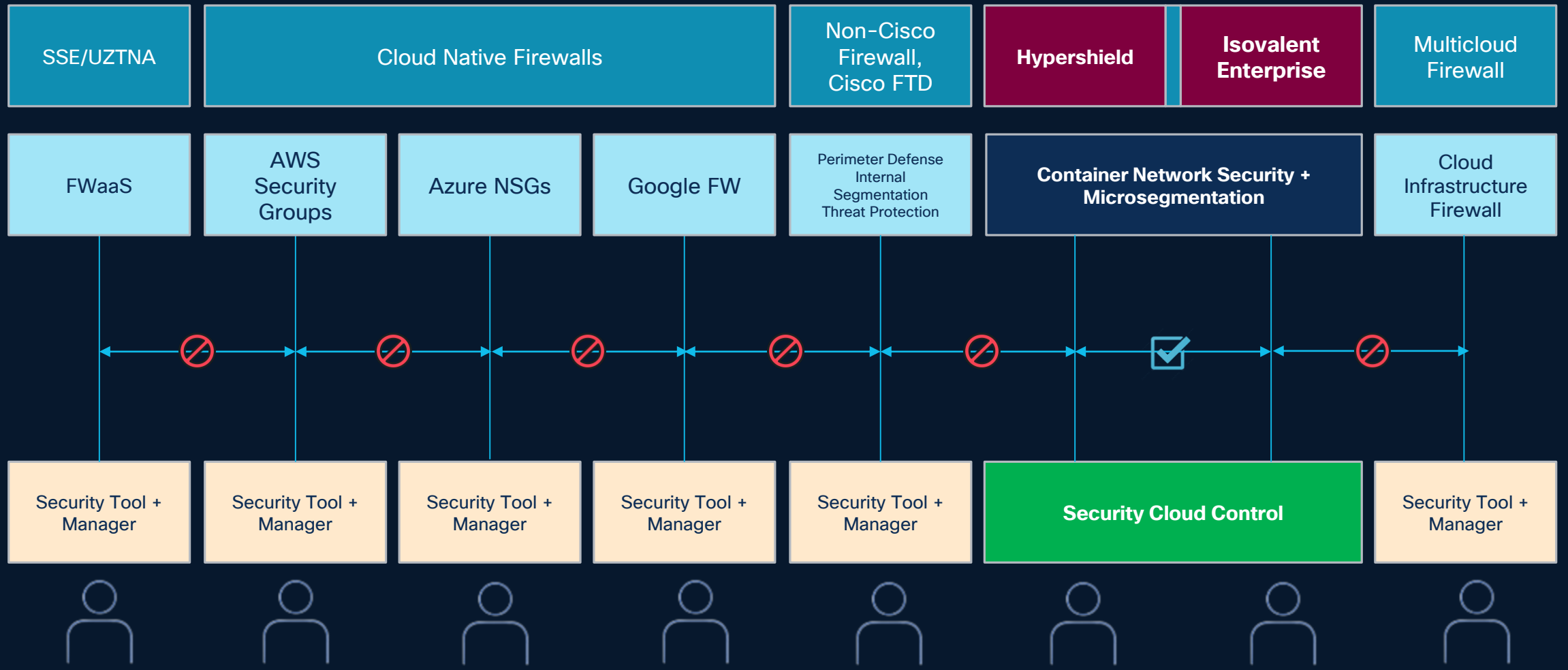
Customer Use Case # 3

Container Network Policy



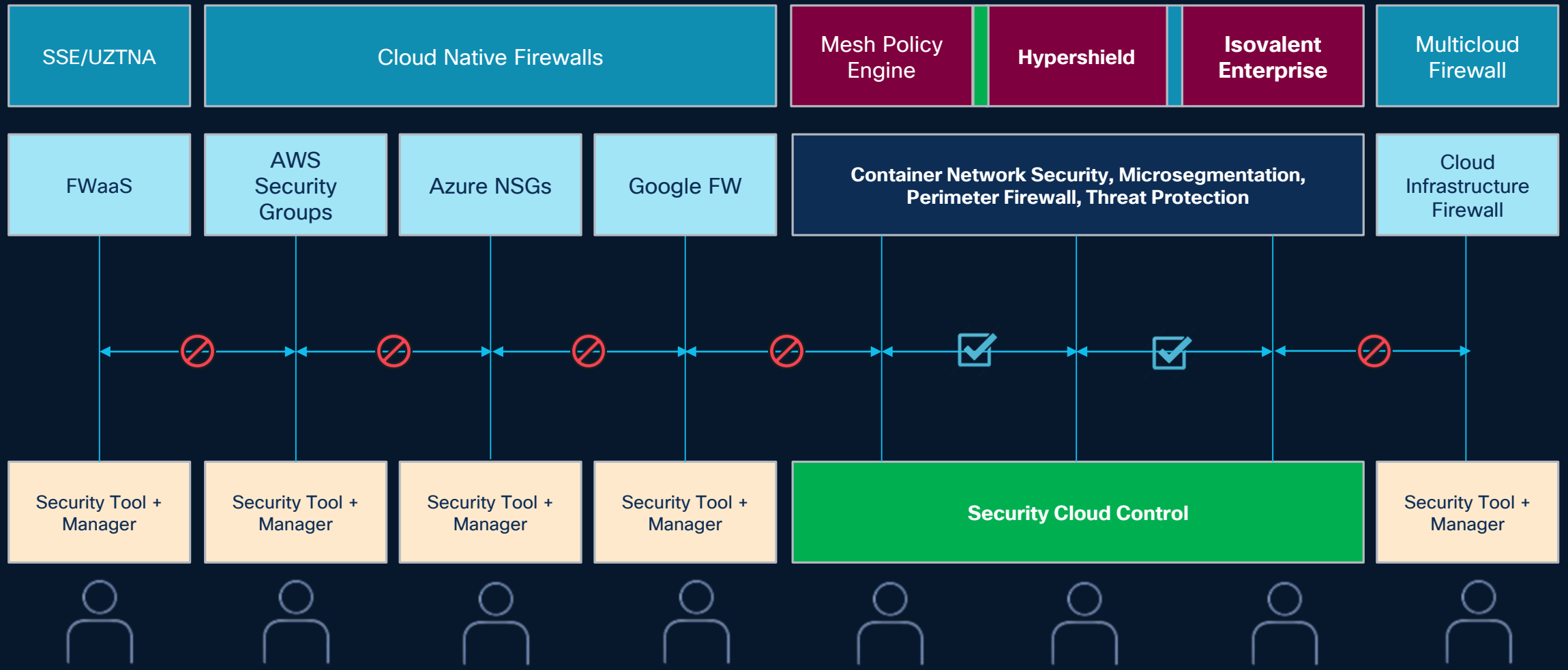
Customer Use Case # 3

Container Network Policy



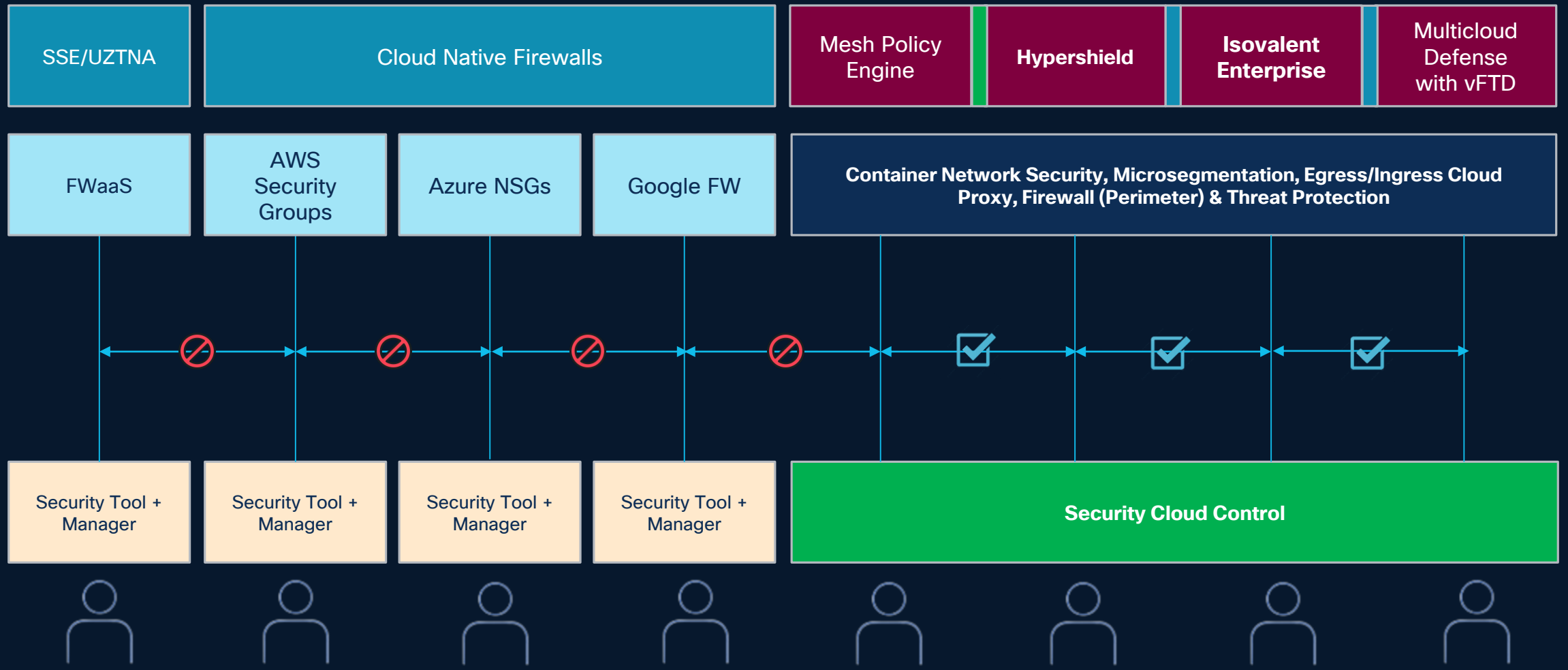
Customer Use Case # 3

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

- Secure Firewall
- Multicloud Defense

Workloads

- 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 be entered in a drawing to win 1 of 5 full conference passes to Cisco Live 2026.

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

Contact me at: nlakhani@cisco.com

Thank you


CISCO