

# Zero Trust for Cloud & Beyond with Cisco Hybrid Mesh Firewall

**cisco** Live !

Nadir Lakhani

Technical Solutions Architect - Hypershield, Workload & Cloud Security

# Cisco Webex App

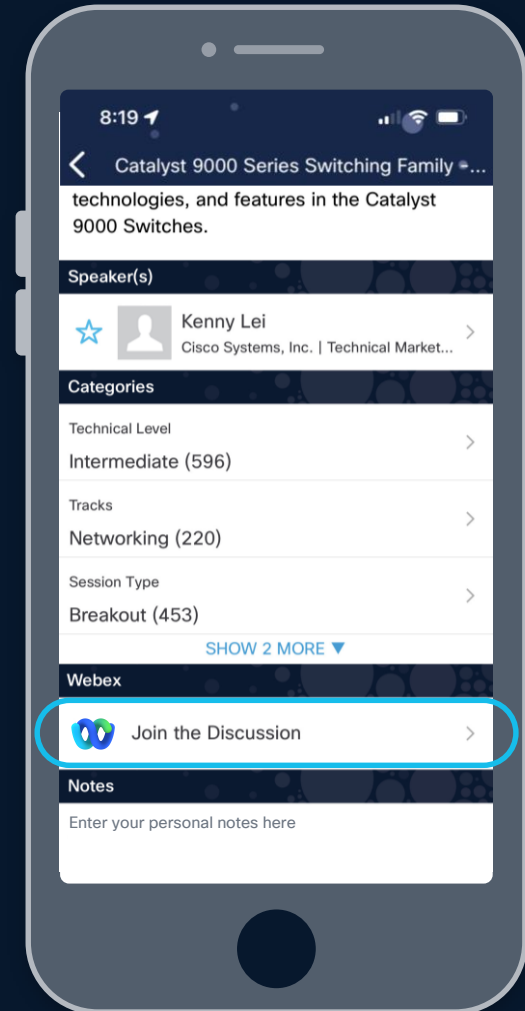
## Questions?

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**

The background features a dark blue field with dynamic, glowing light trails in shades of blue and orange. These trails curve and flow across the frame, creating a sense of motion and digital energy.

# Industry Perspective: The Evolution of Hybrid Security

# Hybrid Security



Customers

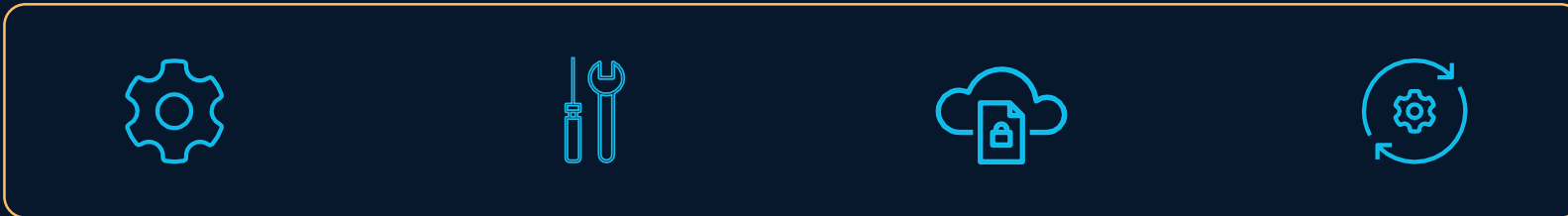
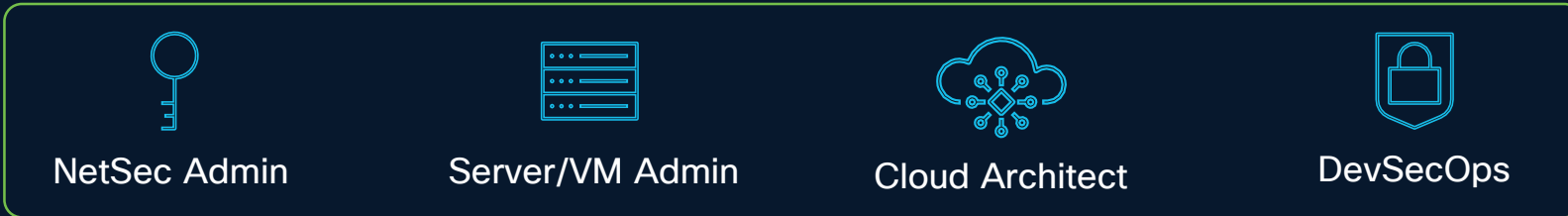
Industry/Analyst

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?



## Organizational Challenges

Multiple teams, organizations and environments

Inconsistent islands of policy controls across environments

# Gartner – Hybrid Mesh Firewall

## Core & Optional Capabilities

Gartner

Gartner

### Market Guide for Hybrid Mesh Firewall Platforms

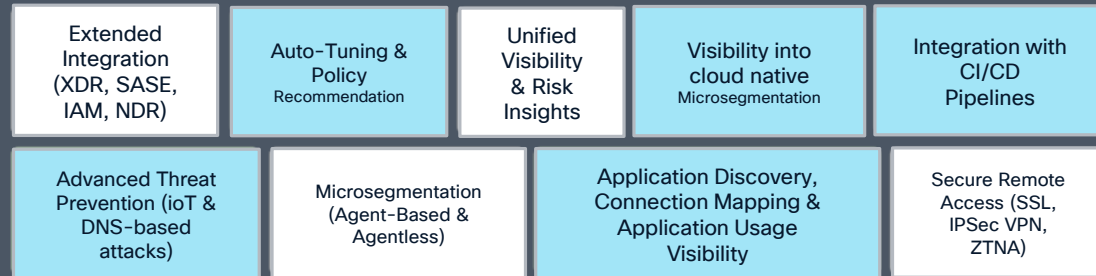
Published 16 January 2024 - ID G00794201 - 15 min read

By Analyst(s): Rajpreet Kaur, Adam Hills

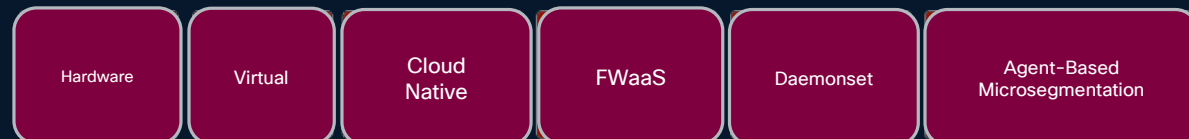
Initiatives: [Infrastructure Security](#); [Build and Optimize Cybersecurity Programs](#)



### Cloud Based Centralized Unified Management



### Multi-Deployment Flexibility (Must support more than two deployment options)



# Cisco's Hybrid Mesh Firewall: Vision & Foundation

# Cisco's Vision – Hybrid Mesh Firewall

## Our North Star

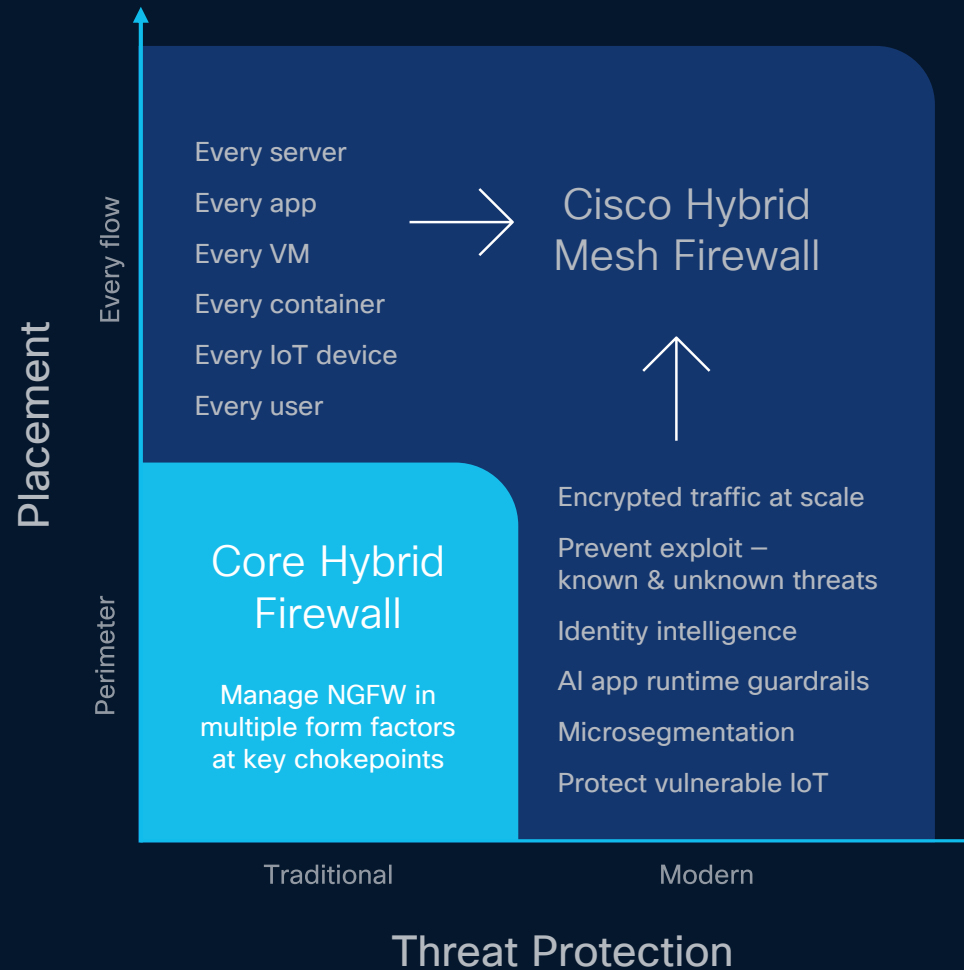
Make it easy for organizations to

Reduce attack surface

Prevent compromise

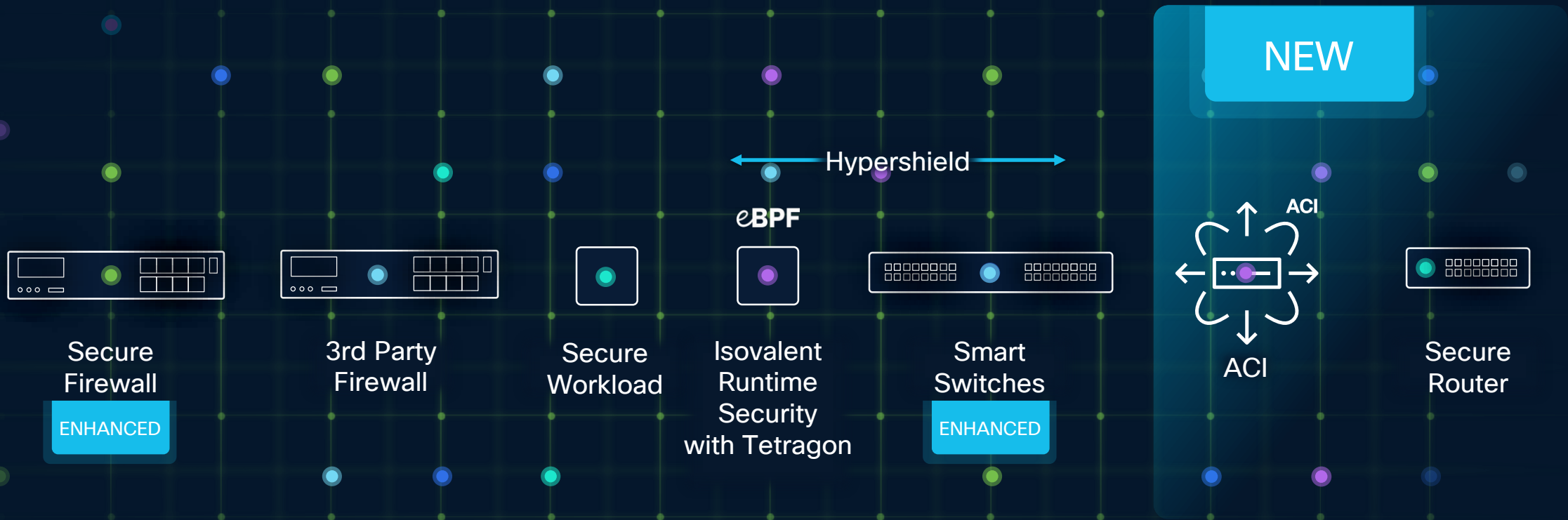
Stop lateral movement

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



# Cisco Hybrid Mesh Firewall

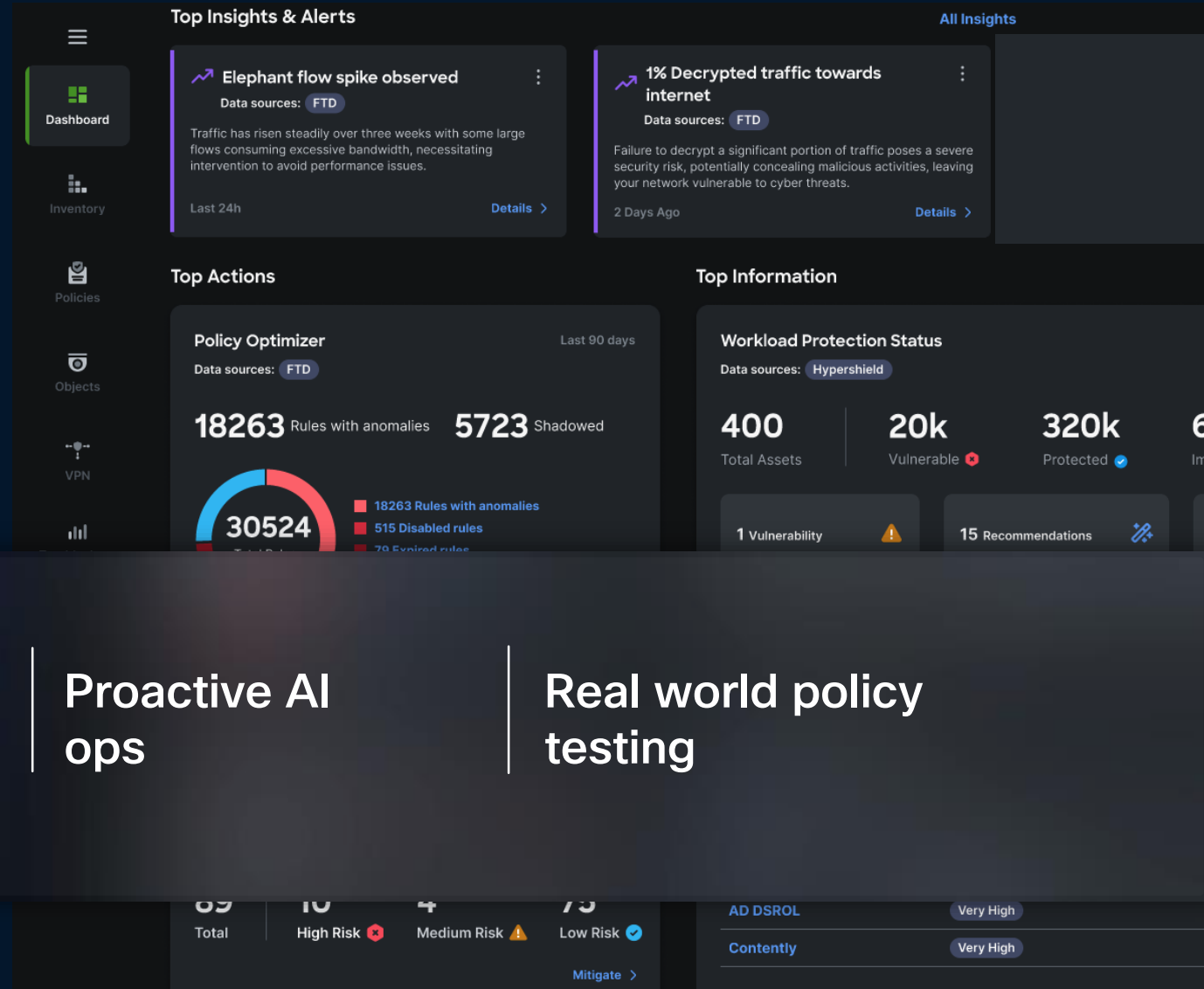
## SECURITY CLOUD CONTROL



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

# Cisco's Hybrid Mesh Firewall: Architecture

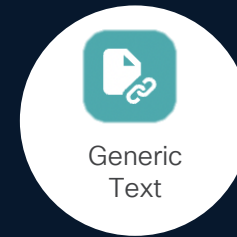
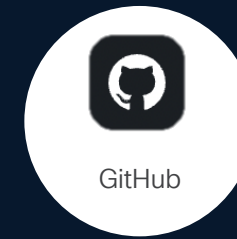
# Cisco Secure Dynamic Attribute Connectors

## Cloud connectors



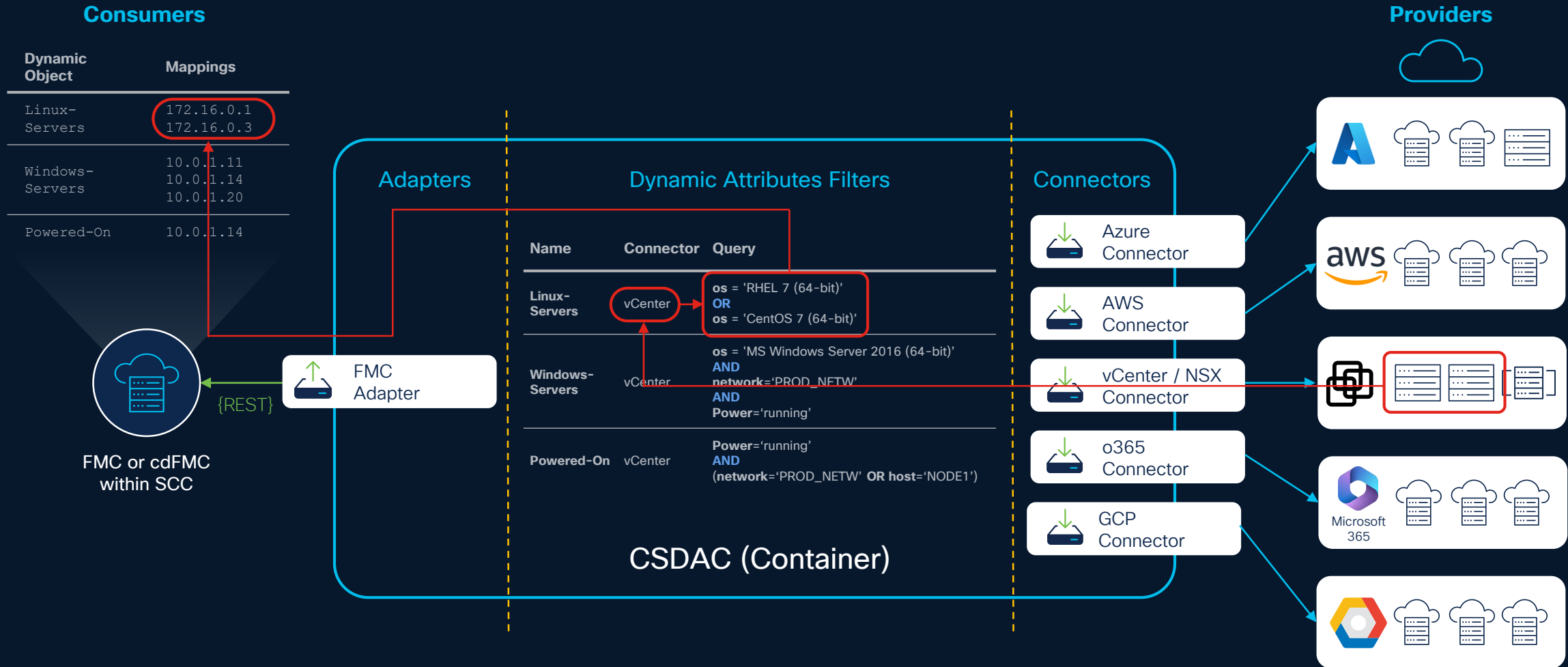
New!

## Public feeds and external connectors

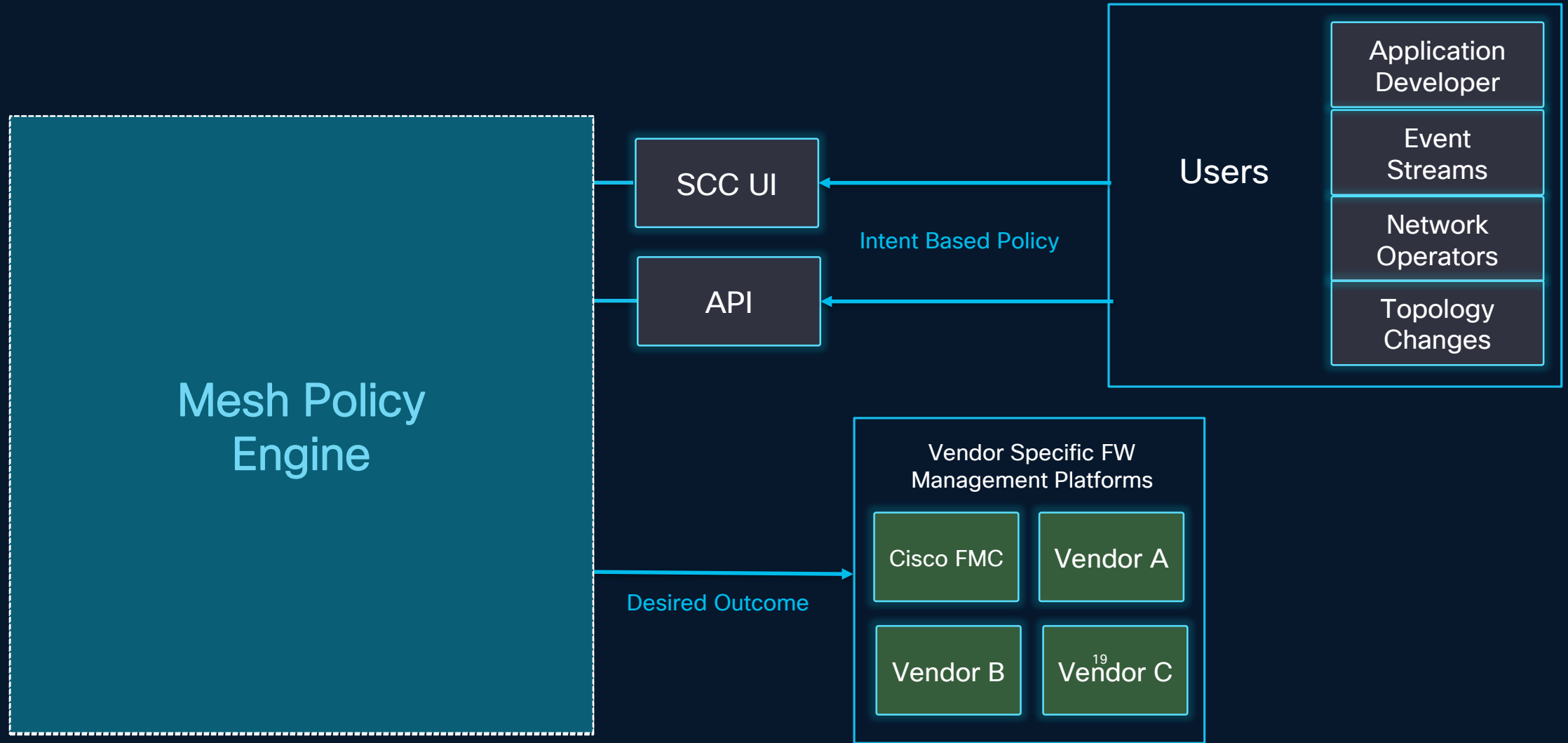


New!

# Dynamic Attribute Connector - 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



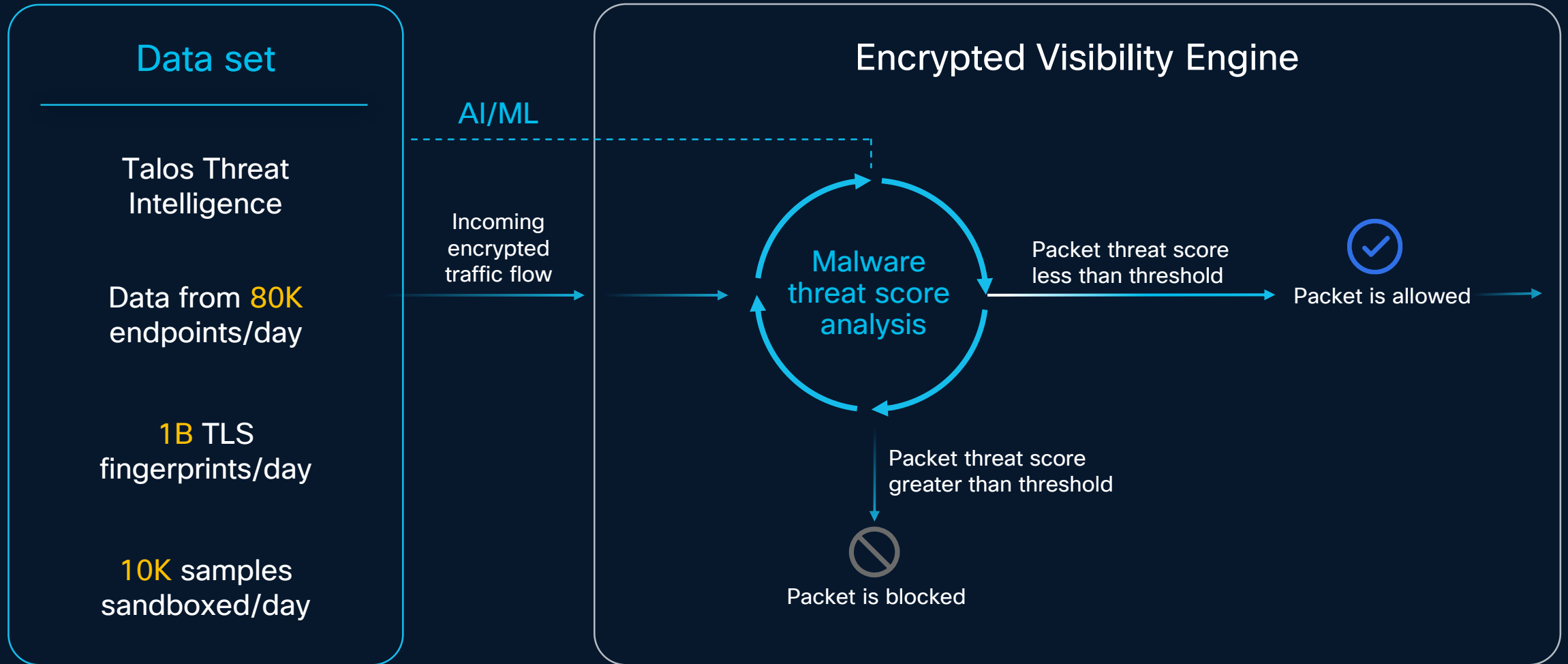
QUIC  
Decryption



Advanced  
Malware  
Protection

# Secure Firewall Capabilities

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



# Secure Firewall Capabilities

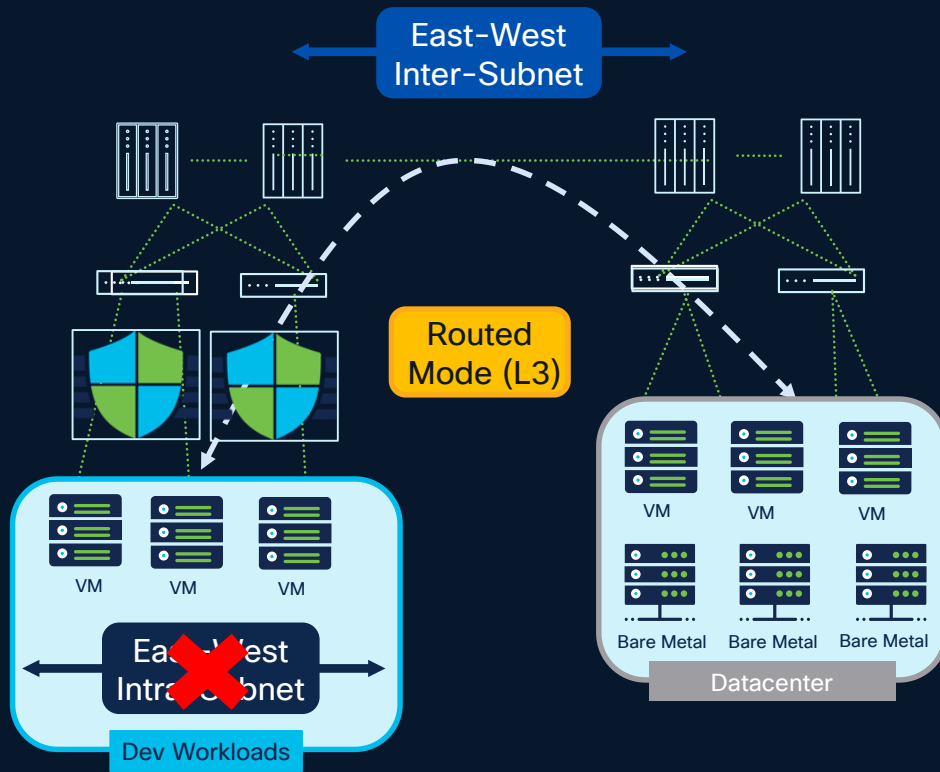
## Intelligent Selective Decryption

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

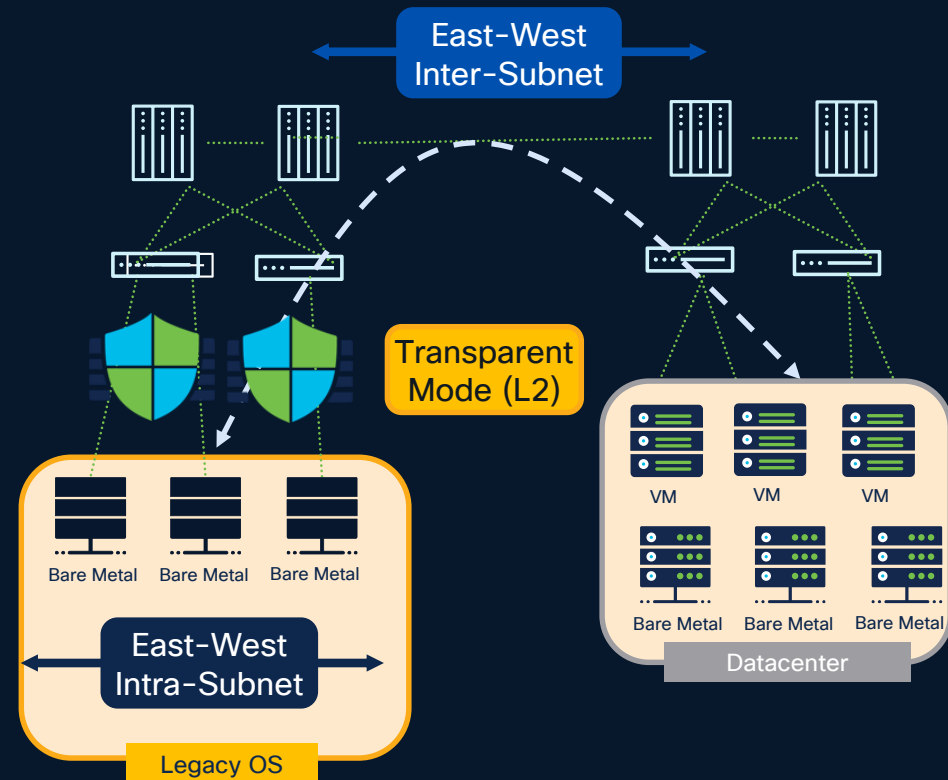


# Secure Workload Capabilities

## Firewall Integration (FTD/FMC)



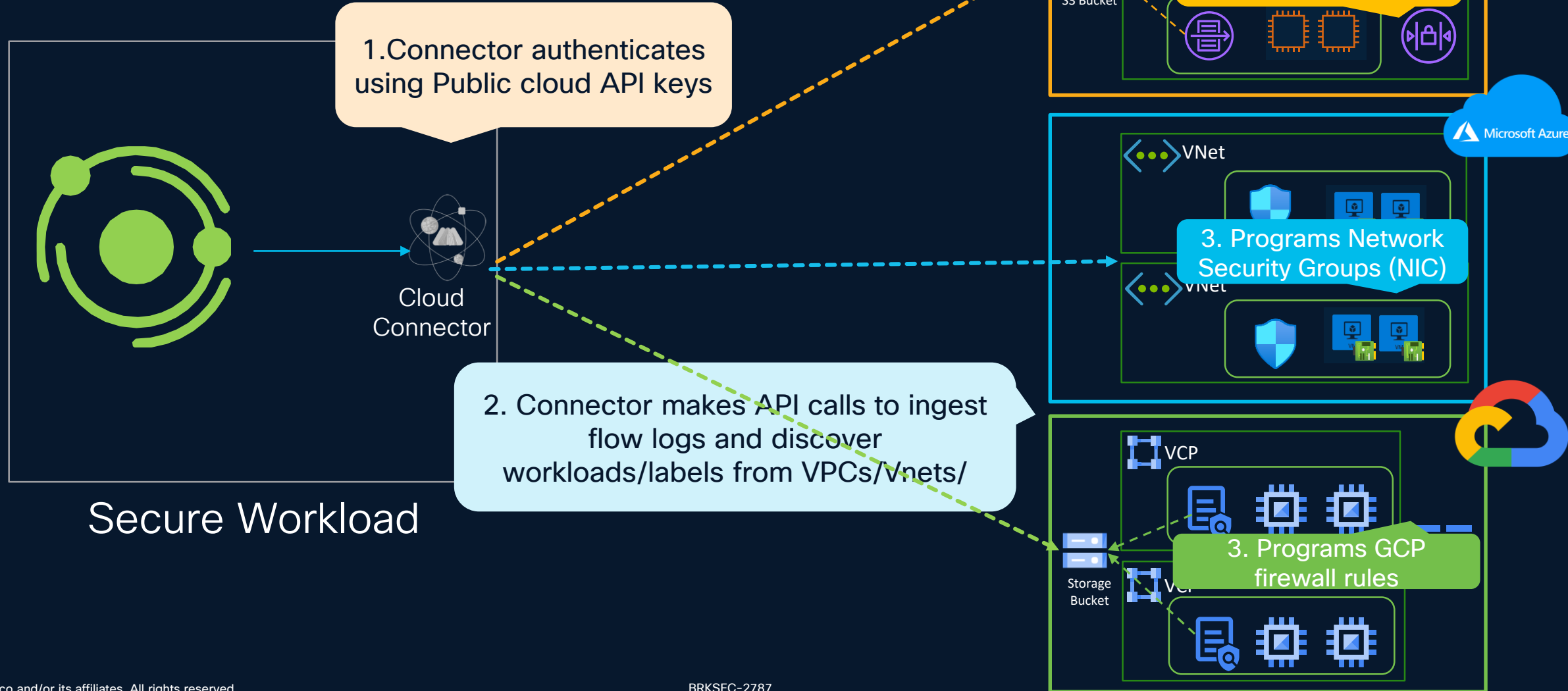
Layer 3 Firewall Insertion (Routed Mode)



Layer 2 Firewall Insertion (Transparent Mode)

# Secure Workload Capabilities

Cloud Native Firewall Integration (SGs, NSGs, GFWs)



# Hypershield Capabilities

## Distributed Exploit Protection

### 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

## Distributed Exploit Protection

The screenshot displays the Hypershield interface with a sidebar on the left containing navigation options like Overview, Summary, Vulnerabilities, Anomalies, Monitor, Insights & F, Events & L, Manage, Objects, Security D, Secure Cor, and Administr. The main content area is divided into several sections:

- Overview:** Shows a summary of shields, including an "Auto-deploy" toggle set to "Off" and a "Change" link. Below this, a donut chart indicates that 50% of shields are not deployed, with 1 shield specifically noted as not deployed.
- Vulnerabilities:** A table showing the status of vulnerabilities. One entry is highlighted as "Partially mitigated" with the identifier "CVE-2021-".
- Details:** A detailed view of a TracingPolicy object. The metadata includes a name "cve-2021-41773-e67d177a5481250ede2beb2d138c7c65f0b62a95c0ce49c96a7f9b3e16af7419" and a label "Exploitable". The spec defines a podSelector for "httpd\_app" and kprobes for "security\_bprm\_check". The matchBinaries list includes various system binaries like "/usr/local/apache2/bin/httpd", "/usr/local/apache2/bin/apache2ctl", "/usr/local/apache2/bin/apachectl", "/usr/local/apache2/bin/apache-ssl", "/usr/local/apache2/bin/apache-ssl2", "/usr/local/apache2/bin/rotatelogs", "/usr/local/apache2/bin/suexec", "/usr/local/apache2/bin/suexec2", "/usr/local/apache2/bin/cgiwrap", "/usr/local/apache2/bin/cgiwrapd", "/usr/local/apache2/bin/nph-cgiwrap", "/usr/local/apache2/bin/npg-cgiwrapd", "/usr/local/apache2/bin/httpd-ssl-pass-dialog", "/usr/local/apache2/bin/cgi-wrapper", "/usr/local/apache2/bin/dbmanage", "/usr/local/apache2/bin/htdigest", "/usr/local/apache2/bin/httpasswd", "/usr/local/apache2/bin/httpd", "/usr/local/apache2/bin/httxt2dmb", "/usr/local/apache2/bin/logresolve", and "/tetra". The matchActions section specifies an "Override" action with an "argError: 1".
- Security status:** A section indicating "Shield deployment in progress".
- Table:** A table listing various services with columns for TYPE, CLUSTER-IP, and EXTERNAL-IP. The EXTERNAL-IP column contains values like "6944eee0300b24b31b" and "<none>".
- Quick actions:** Buttons for "Quick actions" and "Refresh" are visible in the top right.

# The Power of Cisco & AMD Hardware

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



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



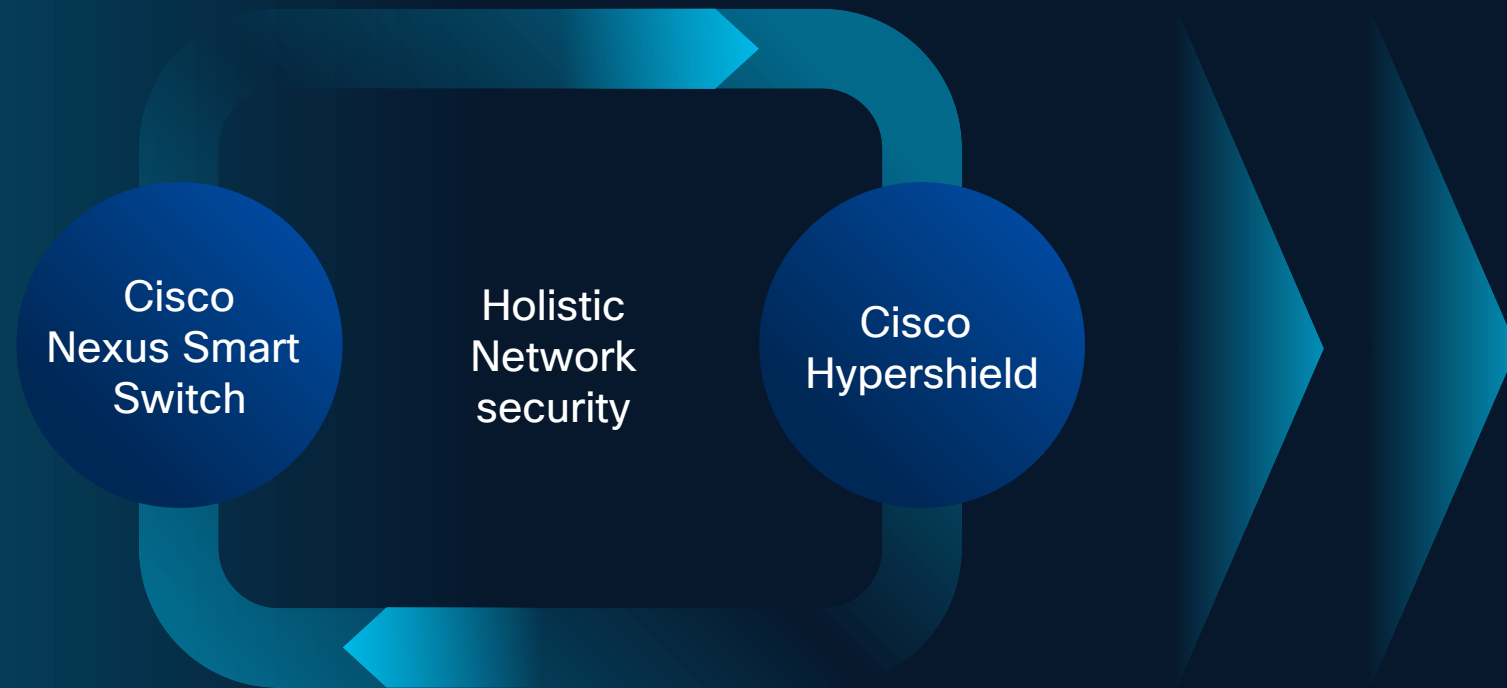
Event-Based  
Telemetry



DoS  
Protection

# Hypershield Capabilities

Nexus Smart Switch



Cloud Edge

Zone-based  
segmentation

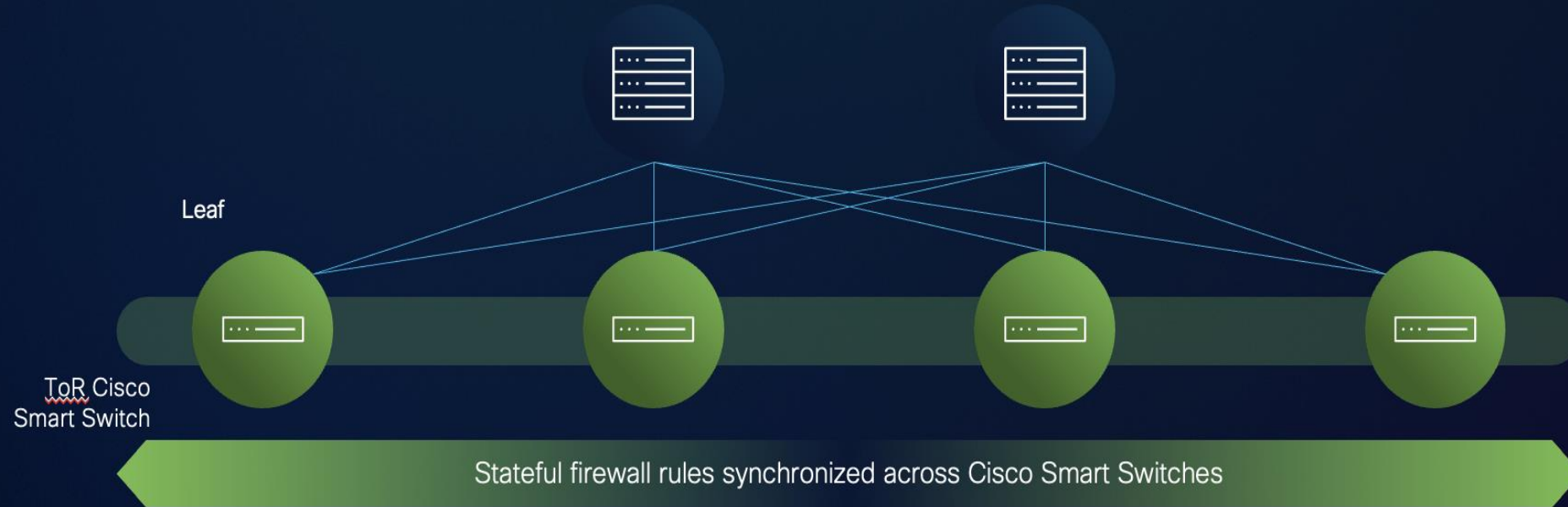
Data Center  
Interconnect (DCI)

Top of Rack (TOR)  
Segmentation &  
Enforcement

# Hypershield Capabilities

## Nexus Smart Switch – Use Cases

### Use Case # 4: Top of Rack (TOR) – Pervasive East-West autonomous segmentation



# 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



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

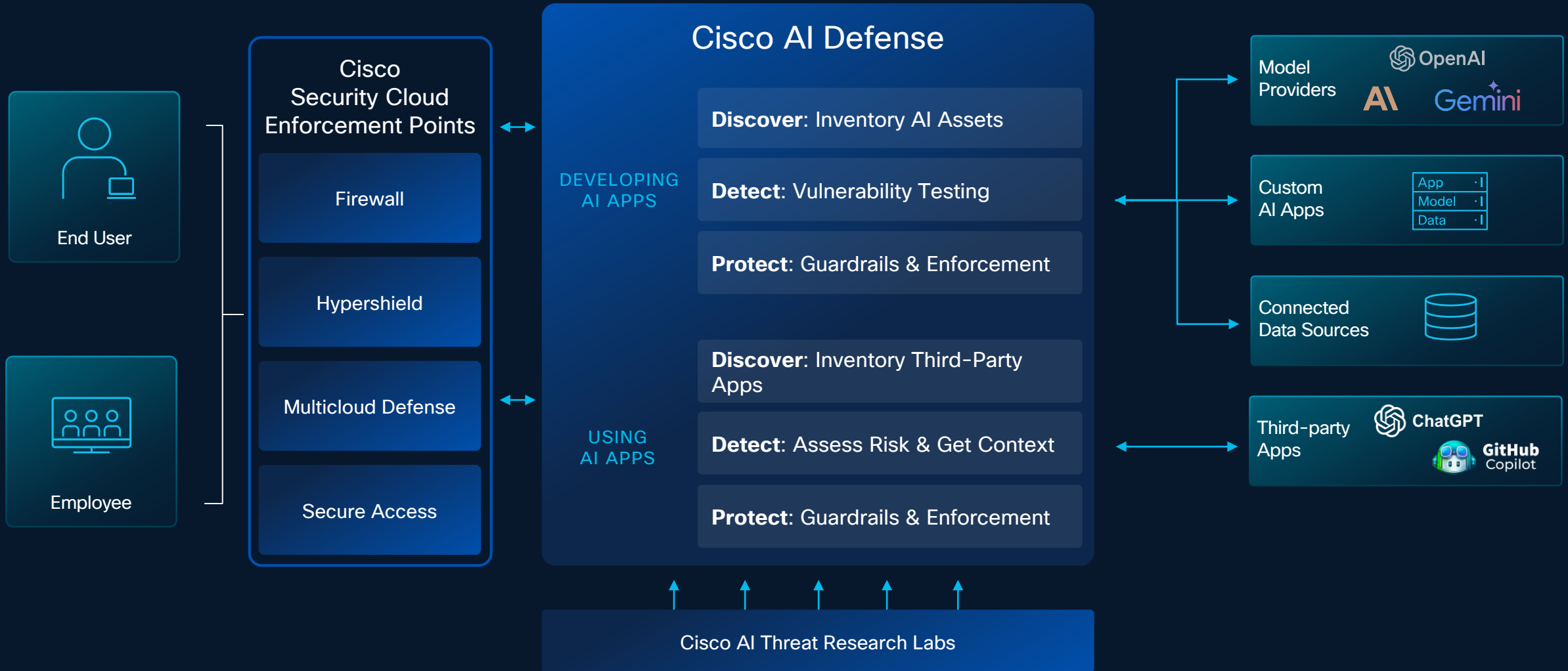
Misinformation from LLMs poses a core vulnerability for applications relying on these models. Misinformation occurs when LLMs produce...

## LLM10 Unbounded Consumption

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

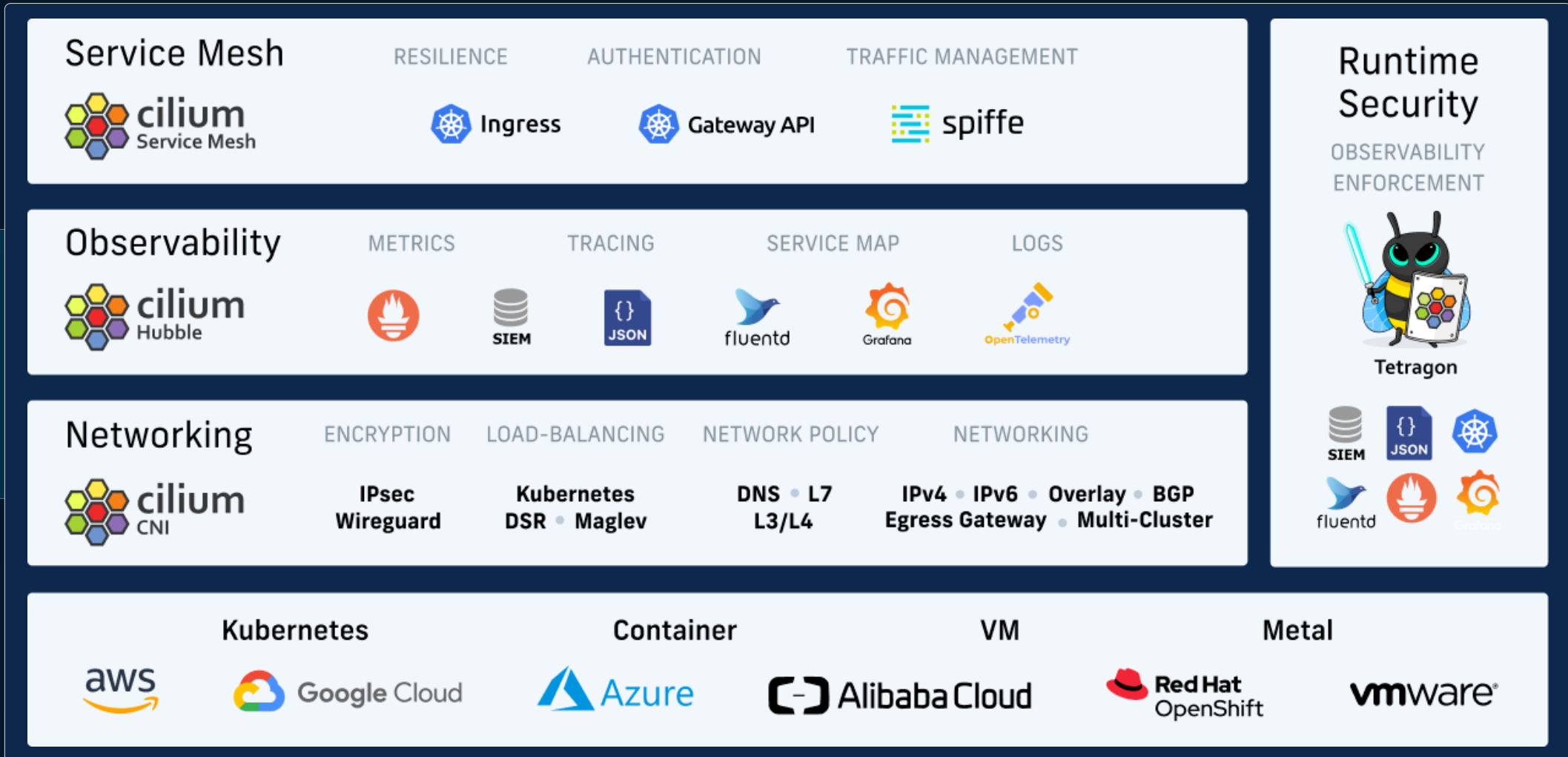
# AI Defense Capabilities

Model Protection, Flexible Enforcement Options



# Isovalent Capabilities

Cilium – Container Network Interface (CNI)



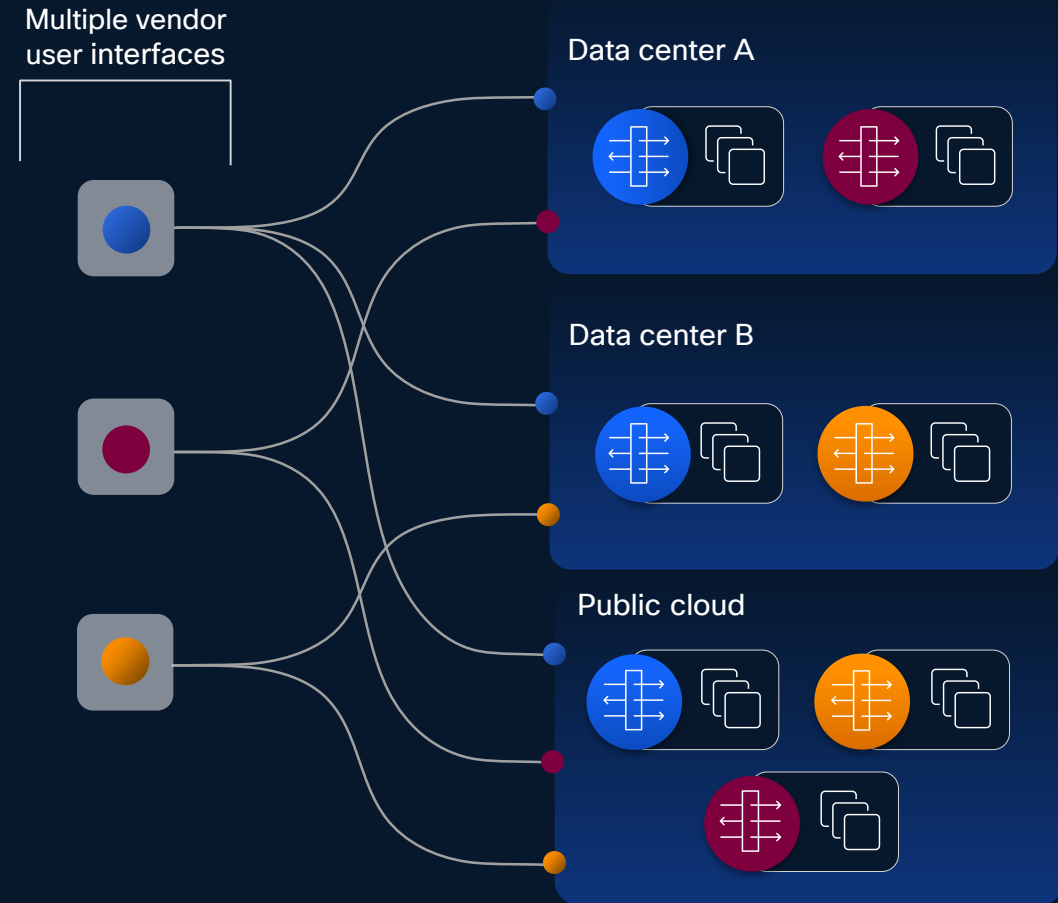
# Cisco Mesh Policy Engine

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

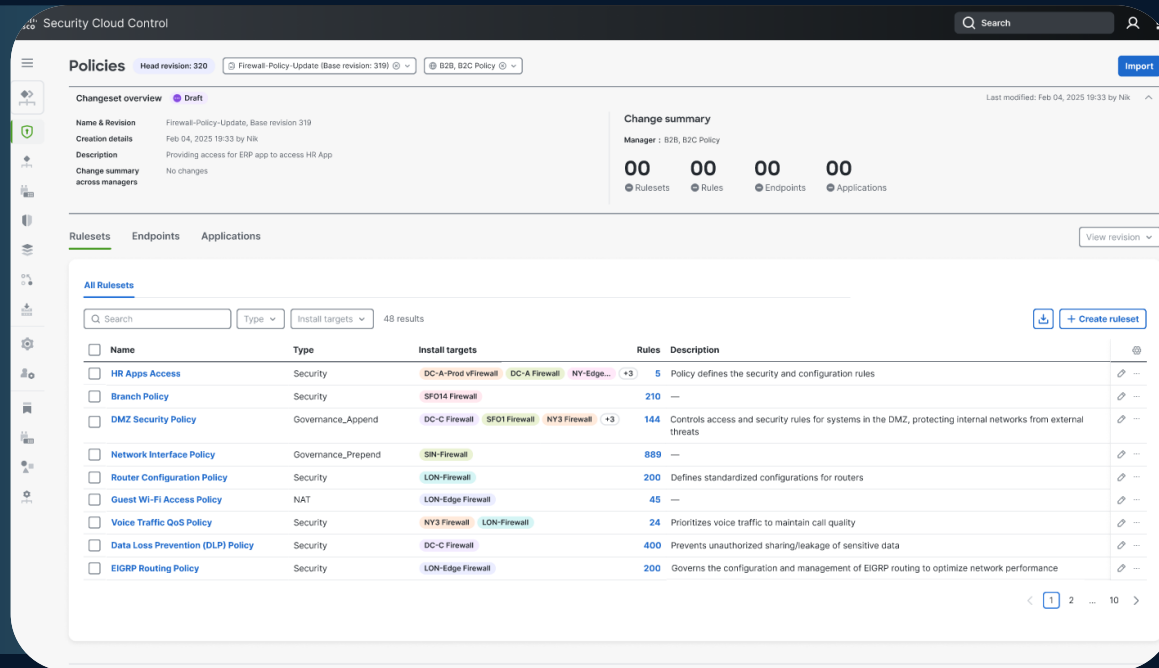
Solving these challenges requires a different approach



# 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

Data center A



Data center B



Public cloud



# Program once, enforce everywhere

The screenshot displays the Cisco Security Cloud Control interface for creating a new rule. The rule is titled "ERP-to-HR app" and is currently in a "Draft" state. It is associated with the "Firewall-Policy-Update (Base revision: 319)" policy. The rule is enabled, with logging set to "ON" and a time range specified. The rule's order is set to "01" and its description is "Controls traffic flowing from ERP to HR Application".

The "Specify Access" section is checked, indicating that users and endpoints can access resources. The "Review Deployment and impact" section is active, showing a network topology diagram. The diagram illustrates the rule's impact across different network segments: Public Cloud, Data Center\_A, and App Zone. The Public Cloud segment contains an ERP application and a Cloud Edge Firewall. The Data Center\_A segment contains a DC-A Firewall. The App Zone segment contains a DC-A-App vFirewall and an HR App. Arrows indicate the flow of traffic from the ERP application through the Cloud Edge Firewall and DC-A Firewall to the HR App.

At the bottom of the interface, there are buttons for "Delete", "Revert changes", "Back", and "Save".

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.

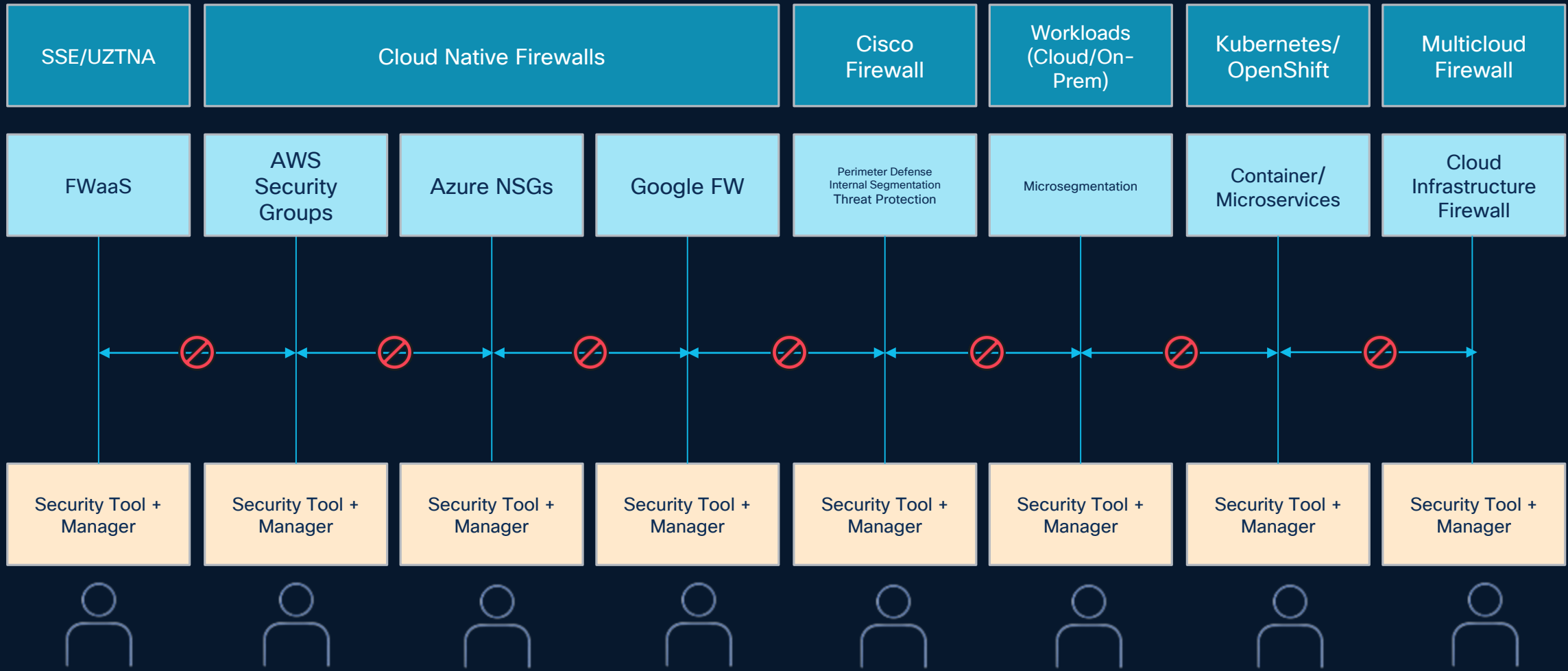
**Segmentation Compatibility Gap:** Their existing on-premises segmentation solution is incompatible with GCP, preventing consistent security enforcement.

**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.

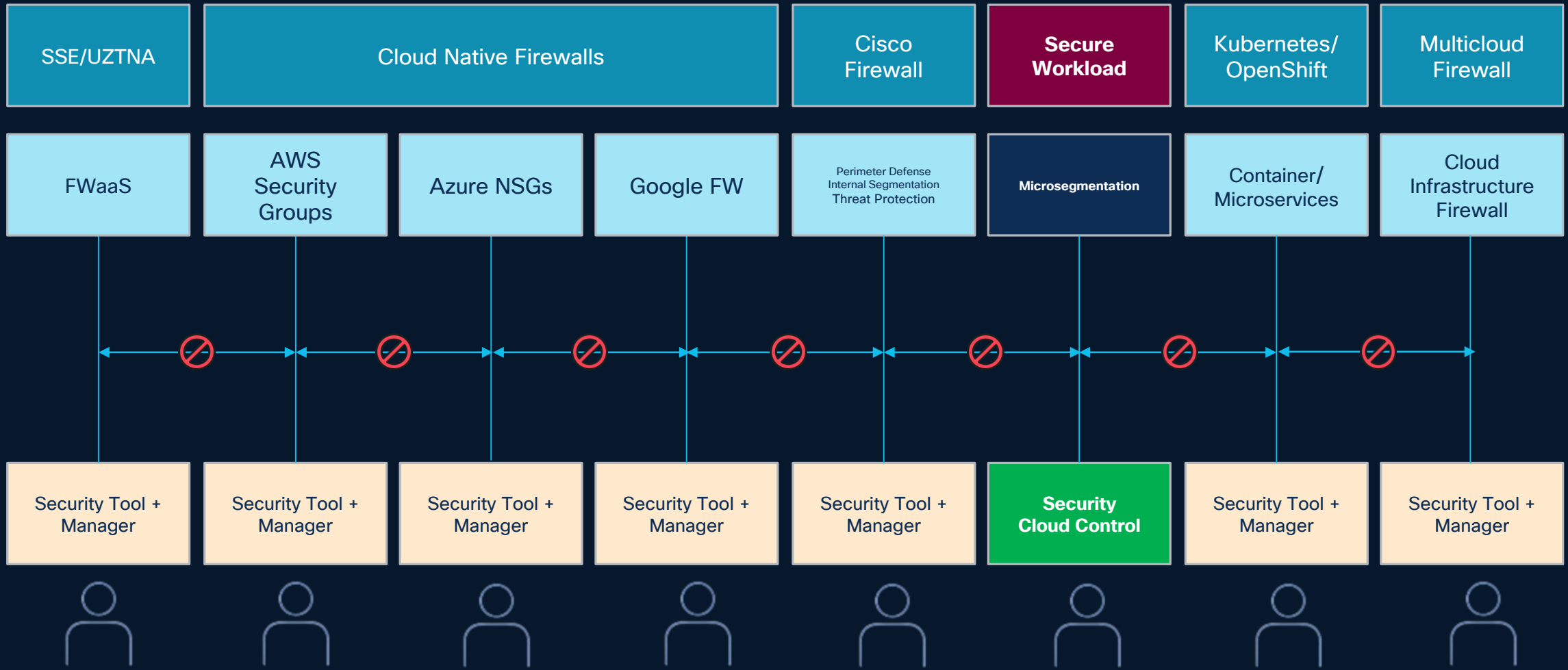
# Customer Use Case # 1

## Microsegmentation for Compliance



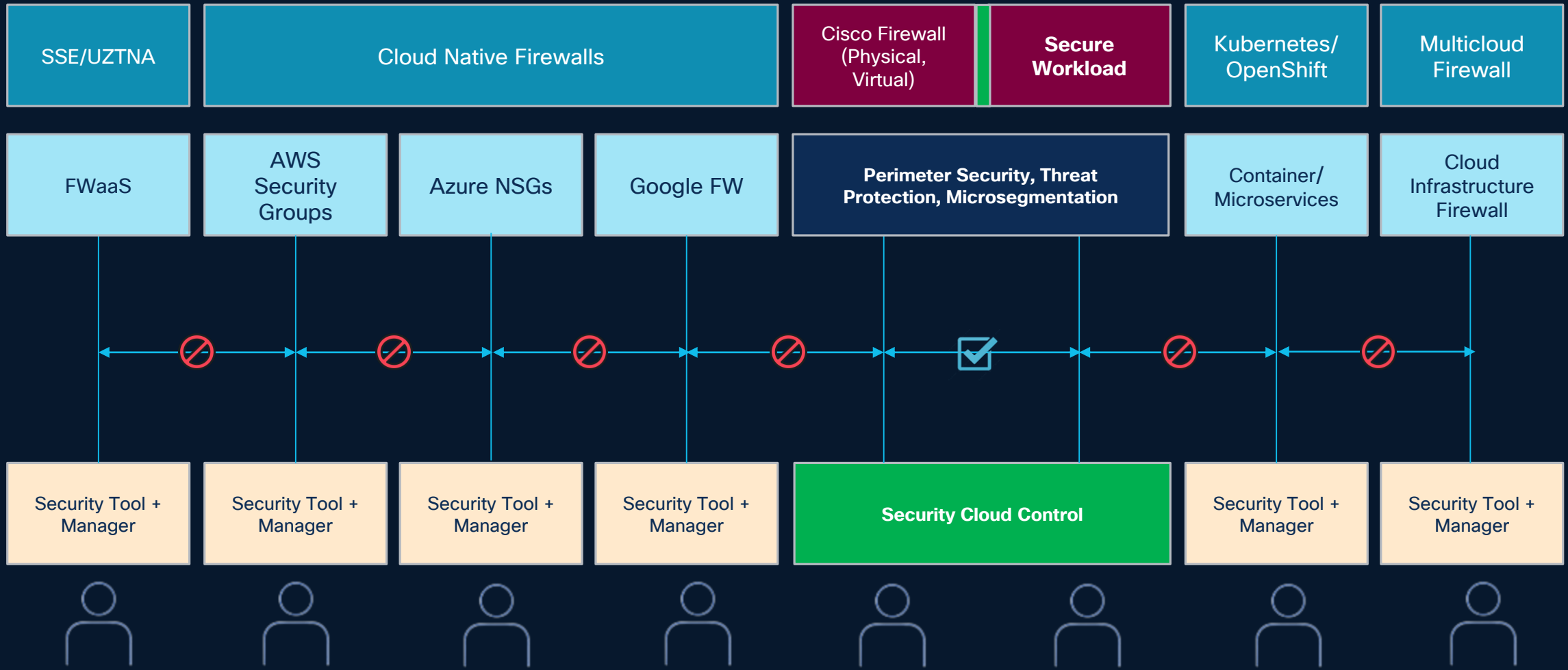
# Customer Use Case # 1

## Microsegmentation for Compliance



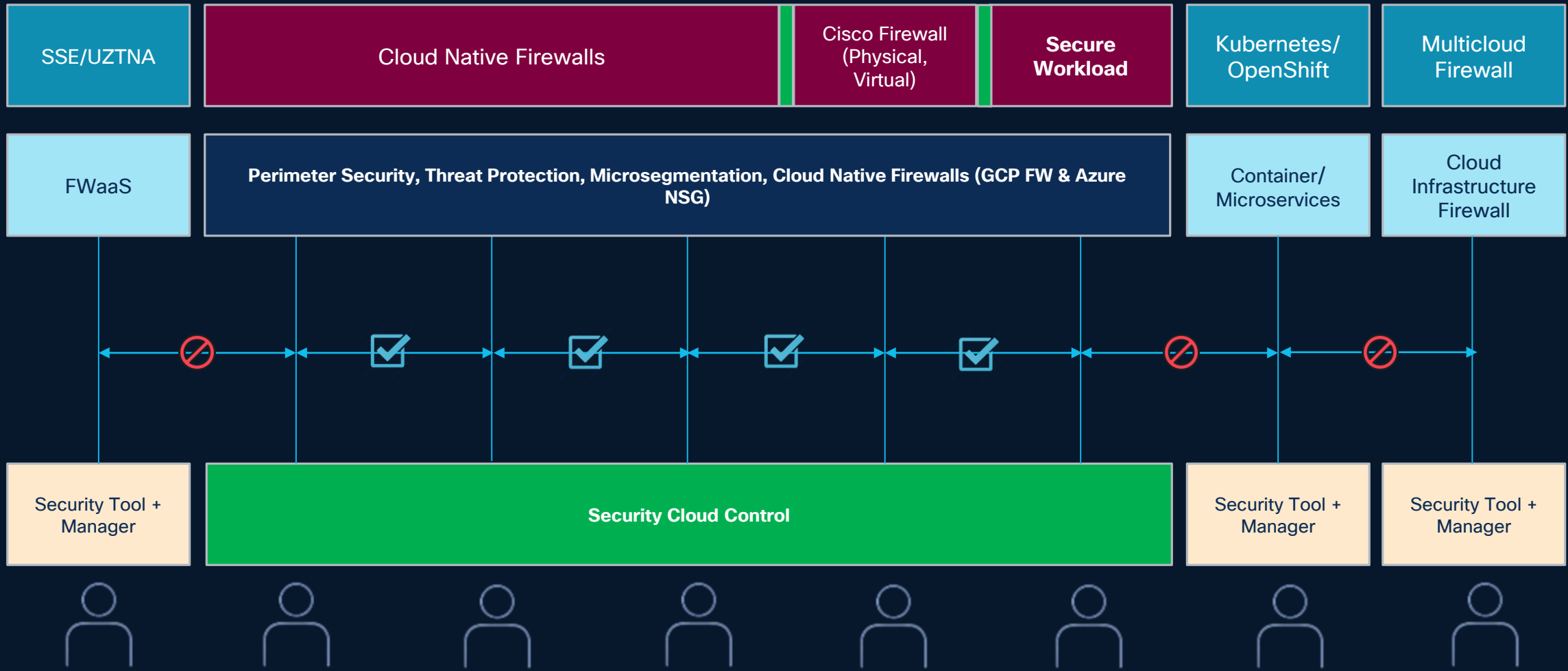
# Customer Use Case # 1

## Microsegmentation for Compliance



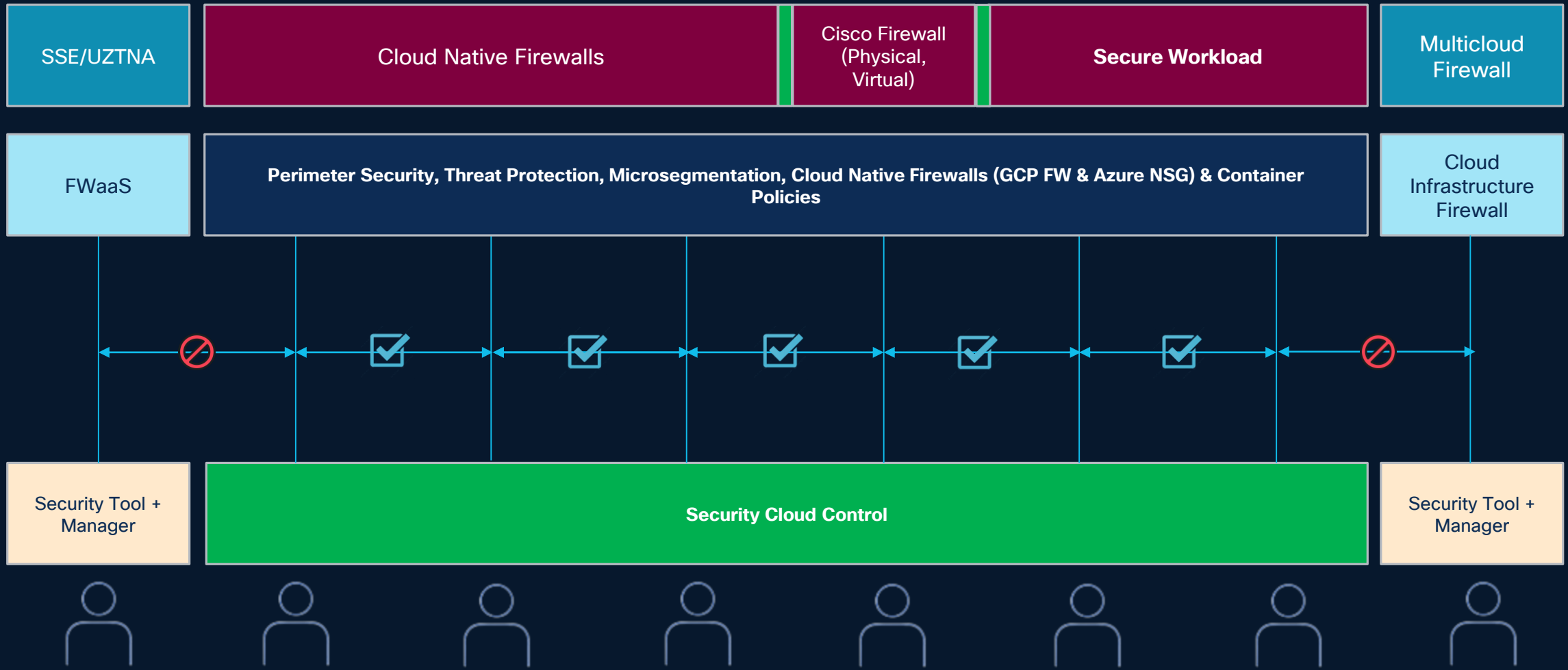
# Customer Use Case # 1

## 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.

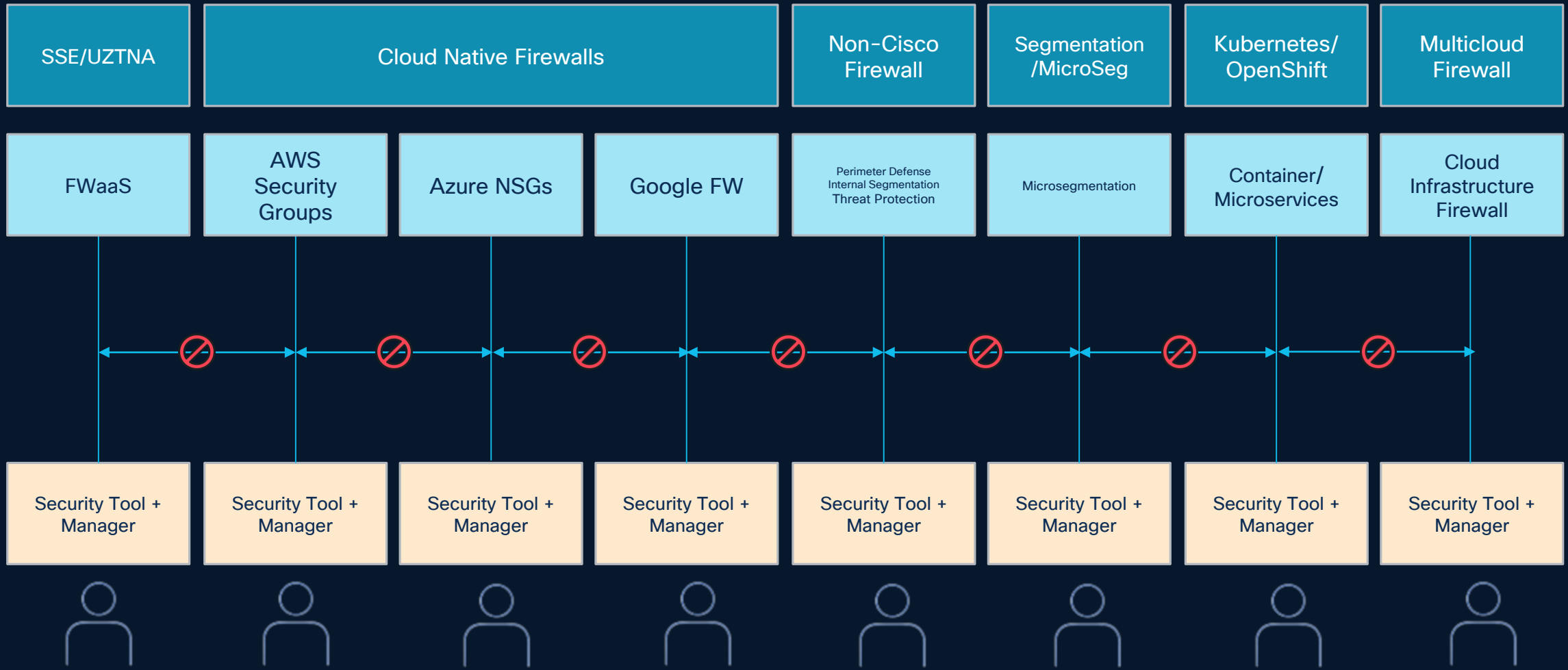
**Policy Inconsistency:** Fragmentation leads to inconsistent security policies across the environment.

**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.

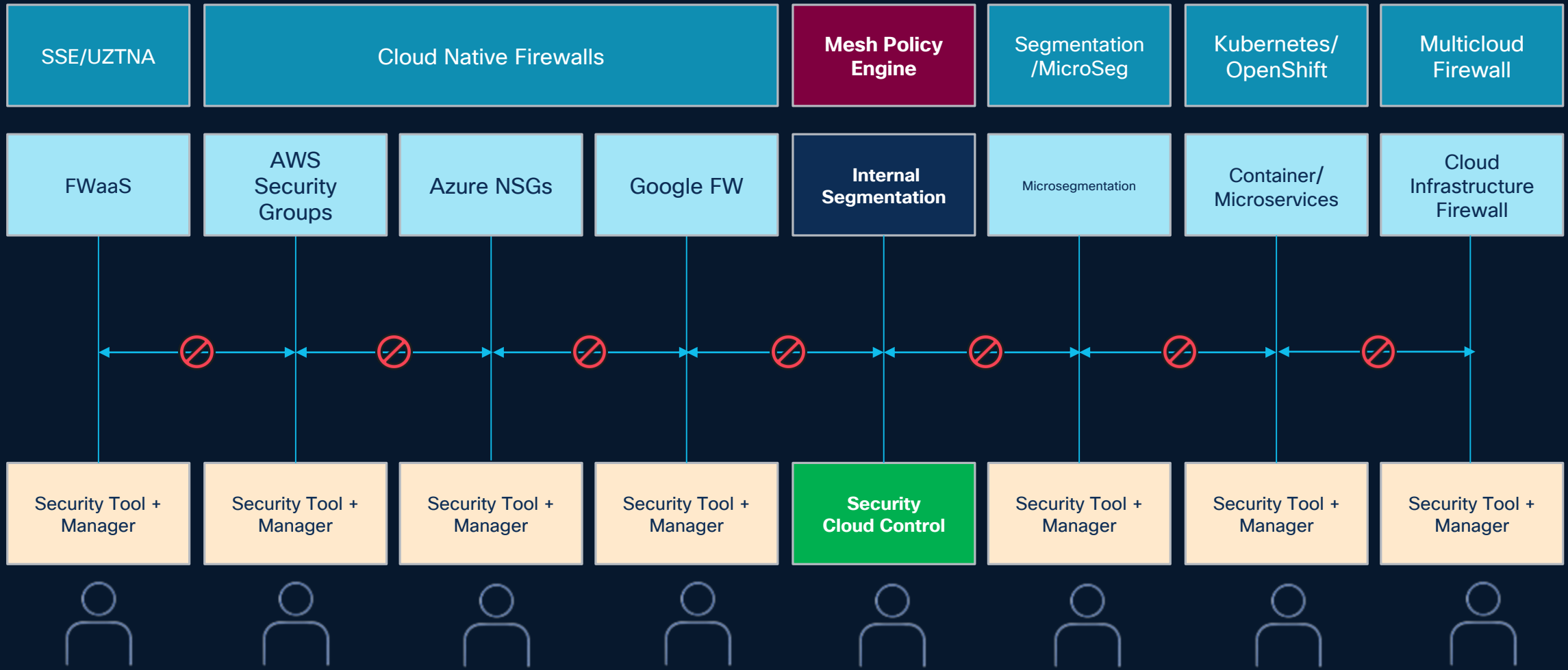
# Customer Use Case # 2

## Multi-Vendor Firewall Management



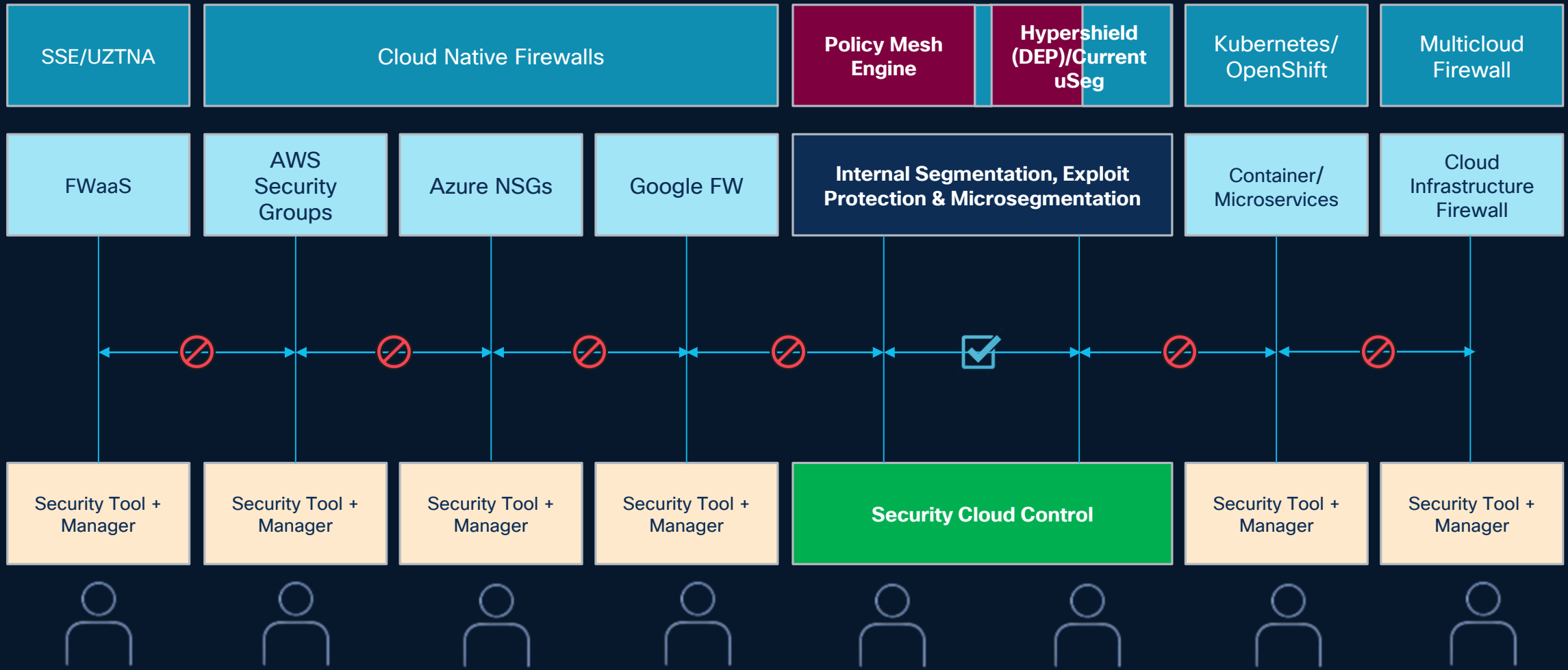
# Customer Use Case # 2

## 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.

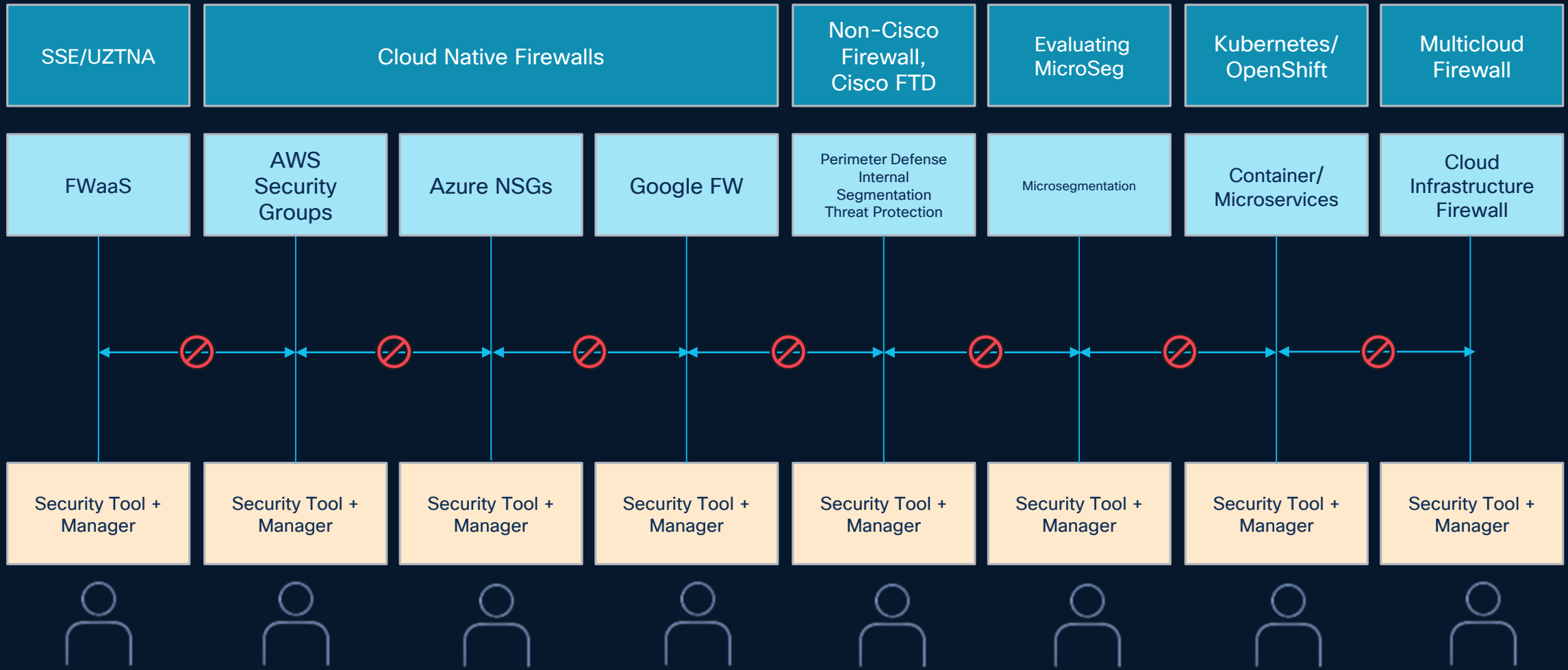
**Legacy Tooling Limitations:** Current tools lack the agility and granularity for dynamic, distributed containers.

**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, multcloud, and both traditional and container-native workloads.

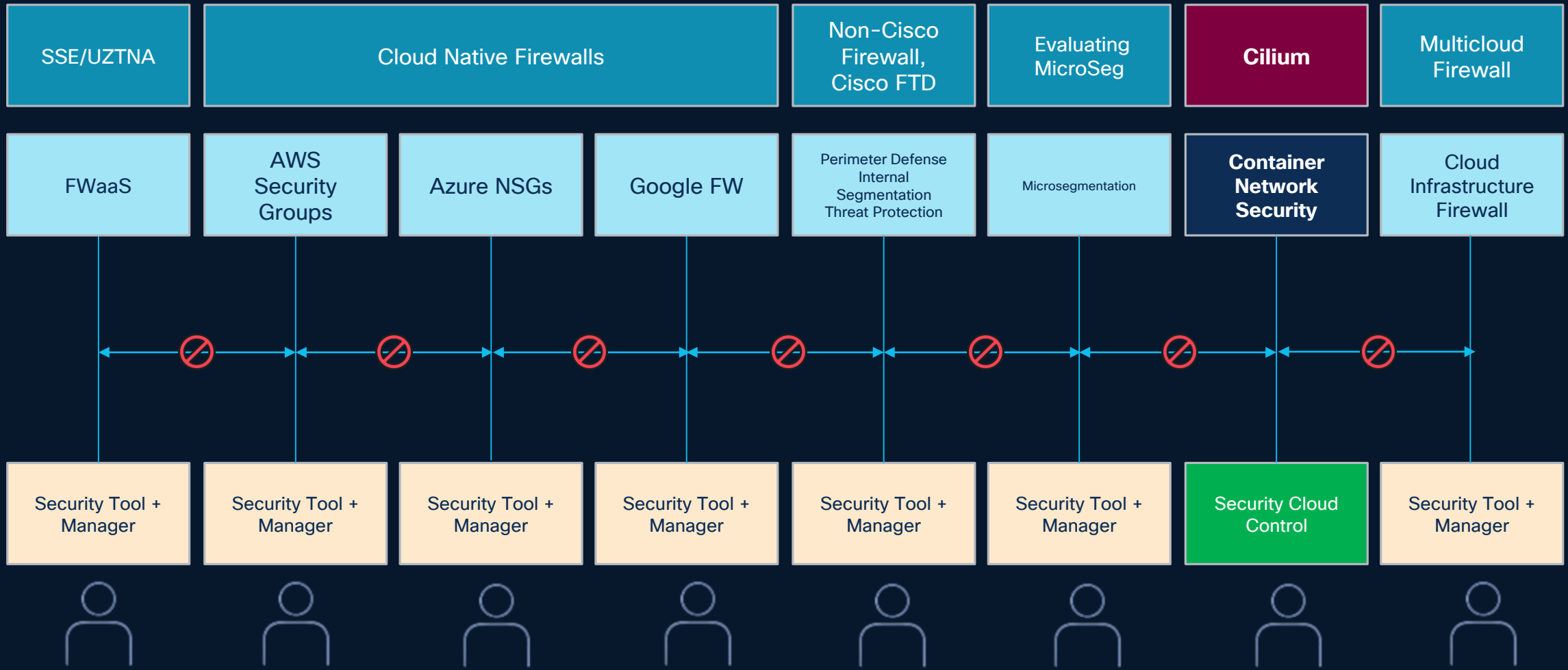
# Customer Use Case # 3

## Container Network Policy



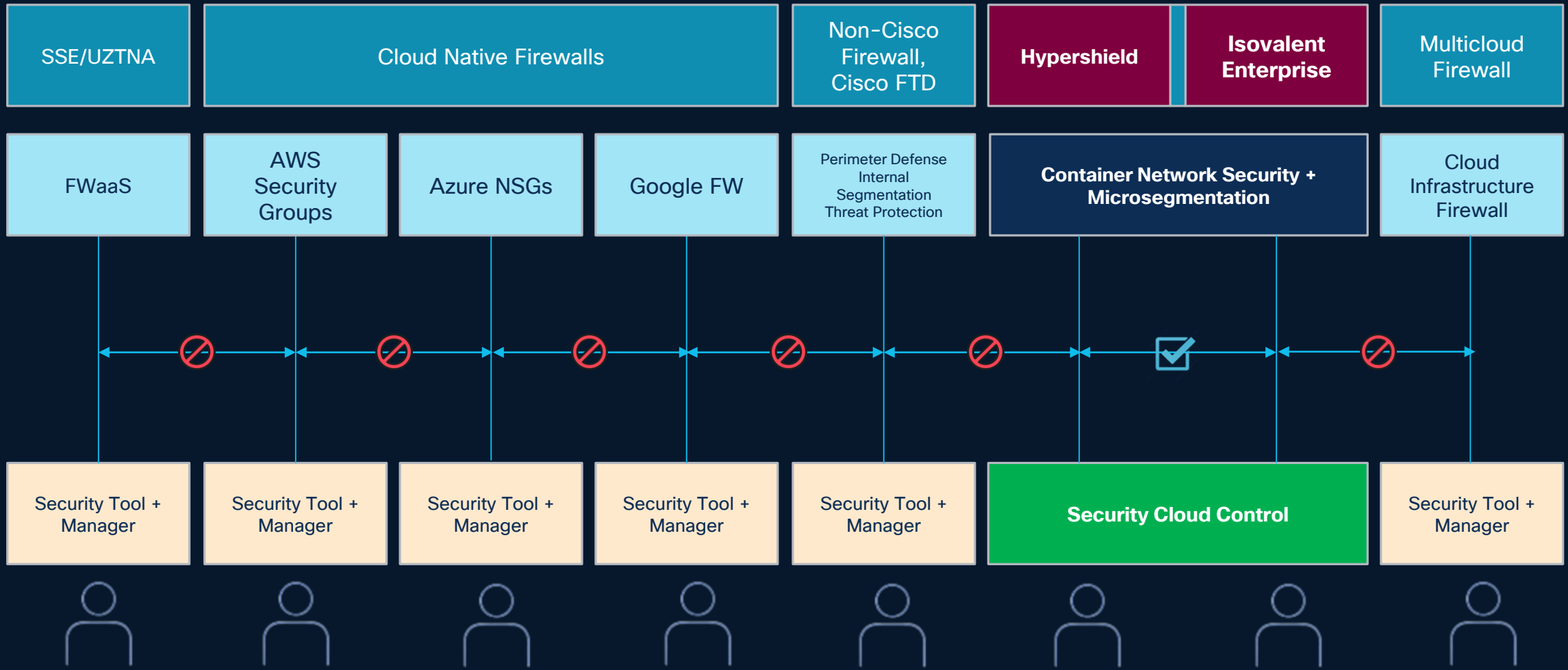
# Customer Use Case # 3

## Container Network Policy



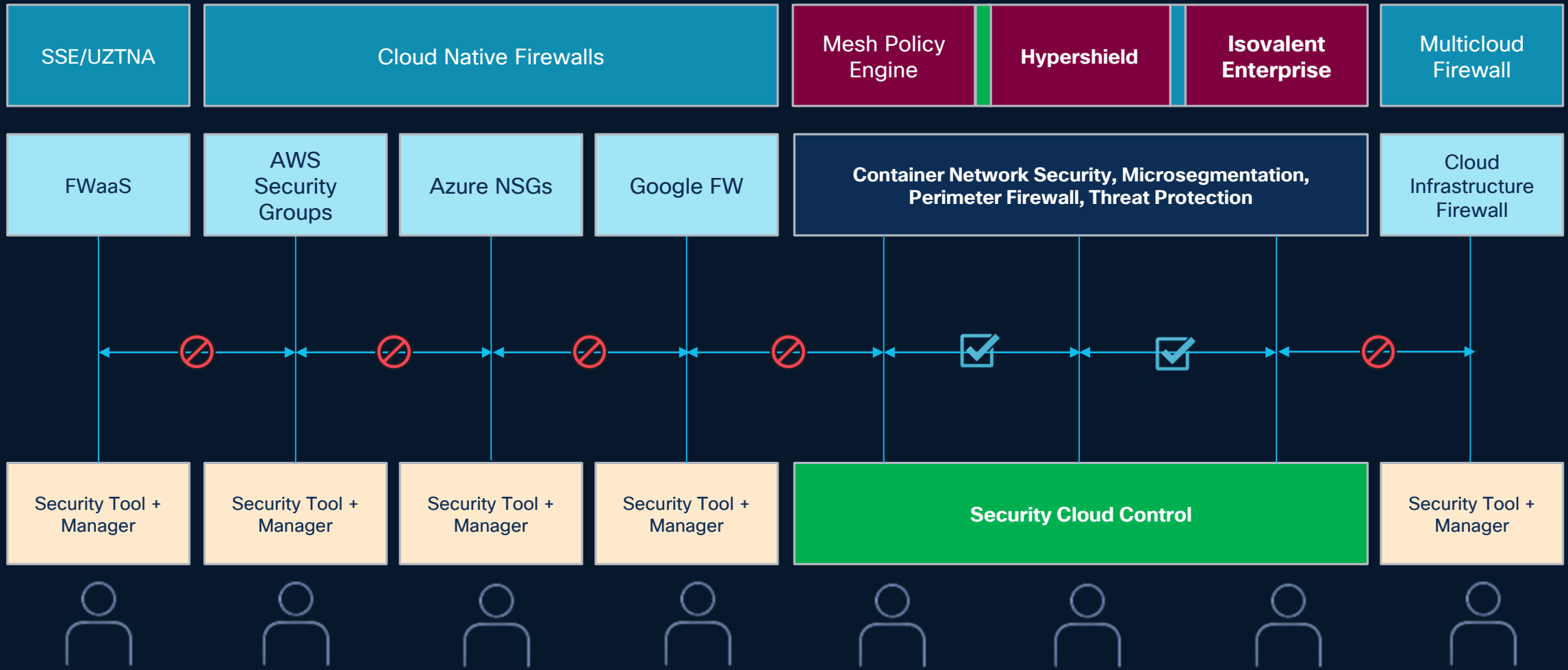
# Customer Use Case # 3

## Container Network Policy



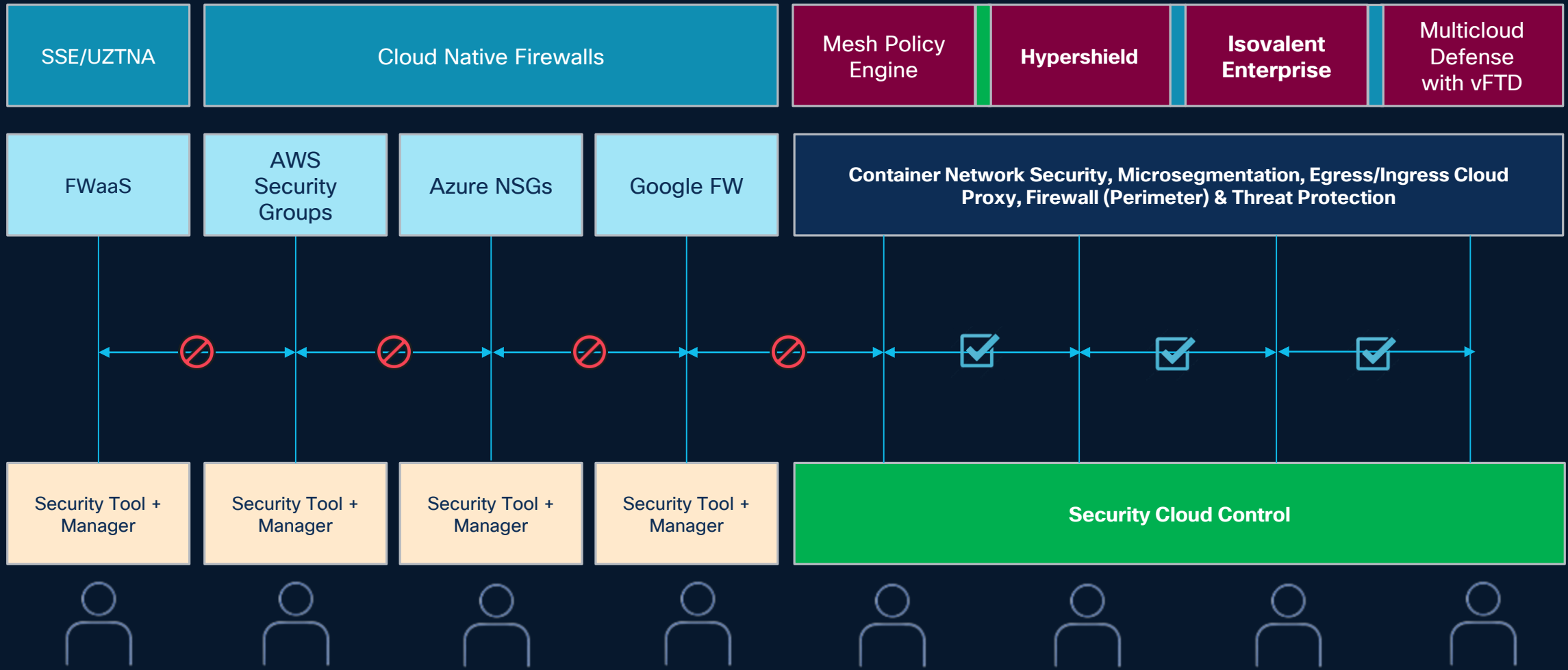
# Customer Use Case # 3

## 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 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](http://www.CiscoLive.com/on-demand)

**Contact me at:** [nlakhani@cisco.com](mailto:nlakhani@cisco.com)

Thank you

**CISCO** Live !

