# Cisco Tech Day

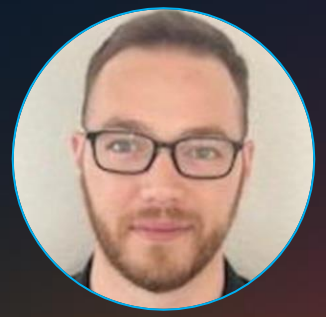
Denver

March 3, 2026

# Protect your applications everywhere

Cisco Tech Day
Denver

## Hybrid Mesh Firewall with Cloud Protection Suite




## Andrew Merica

Security Solutions Engineer

M.S. in Cybersecurity and Information Assurance – CISSP – USAF Vet
US Commercial West – Northwest – Denver, CO

Email: america@cisco.com
LinkedIn: america0x79B

# Thank you to our sponsors!









Where Technology Means More®


# Agenda

1. Why now?
2. Security Driven Outcomes
3. Secure Firewall 10.0
4. End-to-End Segmentation
5. AI Defense
6. Key Takeaways

# Securing the enterprise is increasingly challenging

Highly distributed applications

Nothing can be trusted

More vulnerabilities, exploited faster

AI adoption makes it more challenging

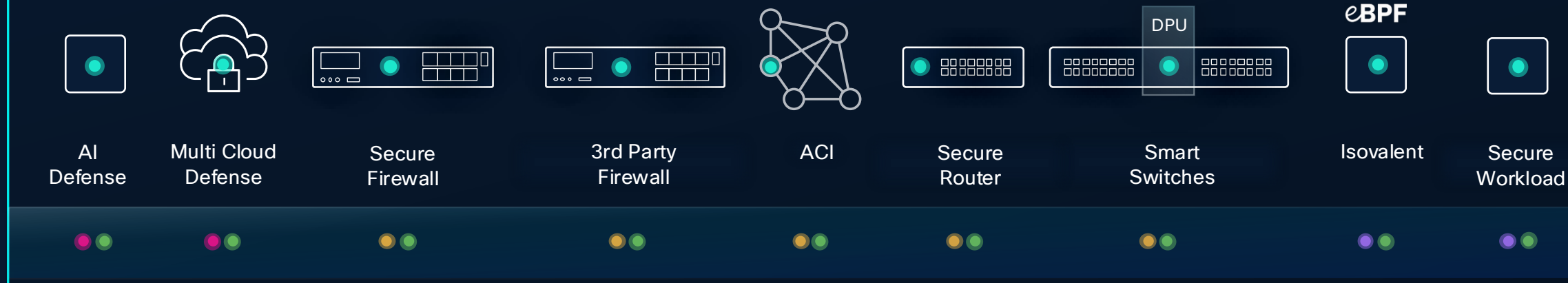
# Firewalling needs to evolve to meet today's challenges

| | Stateful Firewall<br>1990-2007 | Next Generation Firewall<br>2008-2024 | Hybrid Mesh Firewall<br>2025-> |
|---|---|---|---|
| Drivers | Growing internet access<br>Basic attacks<br>Need perimeter control | Rise of SaaS/cloud apps<br>Mobile users<br>App layer threats | Increasingly distributed apps<br>Rise of AI<br>Zero trust imperative |
| Needs | Tracks connection state<br>Filters by IP/port<br>Basic traffic control | App & user aware<br>Integrated threat prevention<br>SSL/TLS decrypt | Hyper-distribution<br>Integrated AI protection<br>AI-powered management |

# Cisco Hybrid Mesh Firewall

CUSTOMER SECURITY OUTCOMES

Network Segmentation | Macro & Micro Segmentation | Threat Detection & Exploit Protection | AI Security




SECURITY CLOUD CONTROL

Write policy once, enforce across the mesh

# Security Cloud Control

Define policy once and enforce anywhere

Cisco Firewalling | AI Defense | 3rd Party Firewalls

Secure Firewall | Secure Workload | Hypershield

Secure Access (FW as a service) | Secure Router NGFW

Cisco Live EMEA announcement

# Security Cloud Control

## Industry's first multi-vendor intent-based policy


Absorb and optimize existing rules

Change enforcement points, not policy

No rip and replace

## Industry recognition

Gartner

2025 Magic Quadrant for Hybrid Mesh Firewall

**Visionary**

IDC

2025 IDC MarketScape: Worldwide Enterprise Hybrid Firewall

**Leader**

## Customer recognition

Gartner Peer Insights™

Network Firewalls

Overall Rating

4.9/5

★★★★★

* vs Palo Alto Networks 4.6, Fortinet 4.7. All scores for last 12 months as of Jan 29,2026.



cisco

# Security Driven Outcomes and Use Cases

# Security Outcomes

Network Zone Based Segmentation

Macro & Micro Segmentation

AI Security

Threat Detection & Exploit Protection

# Cisco Hybrid Mesh Firewall

CUSTOMER SECURITY OUTCOMES

Network Segmentation | Macro & Micro Segmentation | Threat Detection & Exploit Protection | AI Security

Security Use Cases

## Network (L4 /L7) Zone based Segmentation

Enhances security, performance, and compliance by dividing networks into application-aware zones. It minimizes the attack surface, controls access, limits congestion and supporting zero-trust with granular controls and visibility.

## L4 Switch Fabric Segmentation

Enable high-performance, distributed stateful segmentation and enforcement directly within the data center fabric, simplifying network security architecture while reducing costs and improving scalability and operational efficiency

## Macro & Micro Segmentation

Reduce risk by enforcing least-privilege access across networks and applications. Cisco strengthens this with AI-driven security that adapts to application behavior, ensuring protection without sacrificing agility.

## AI Model Protection

Safeguards intellectual property and development investments, ensures the integrity of AI-driven decisions, supports compliance with data and AI ethical standards and minimize financial and reputational risks.

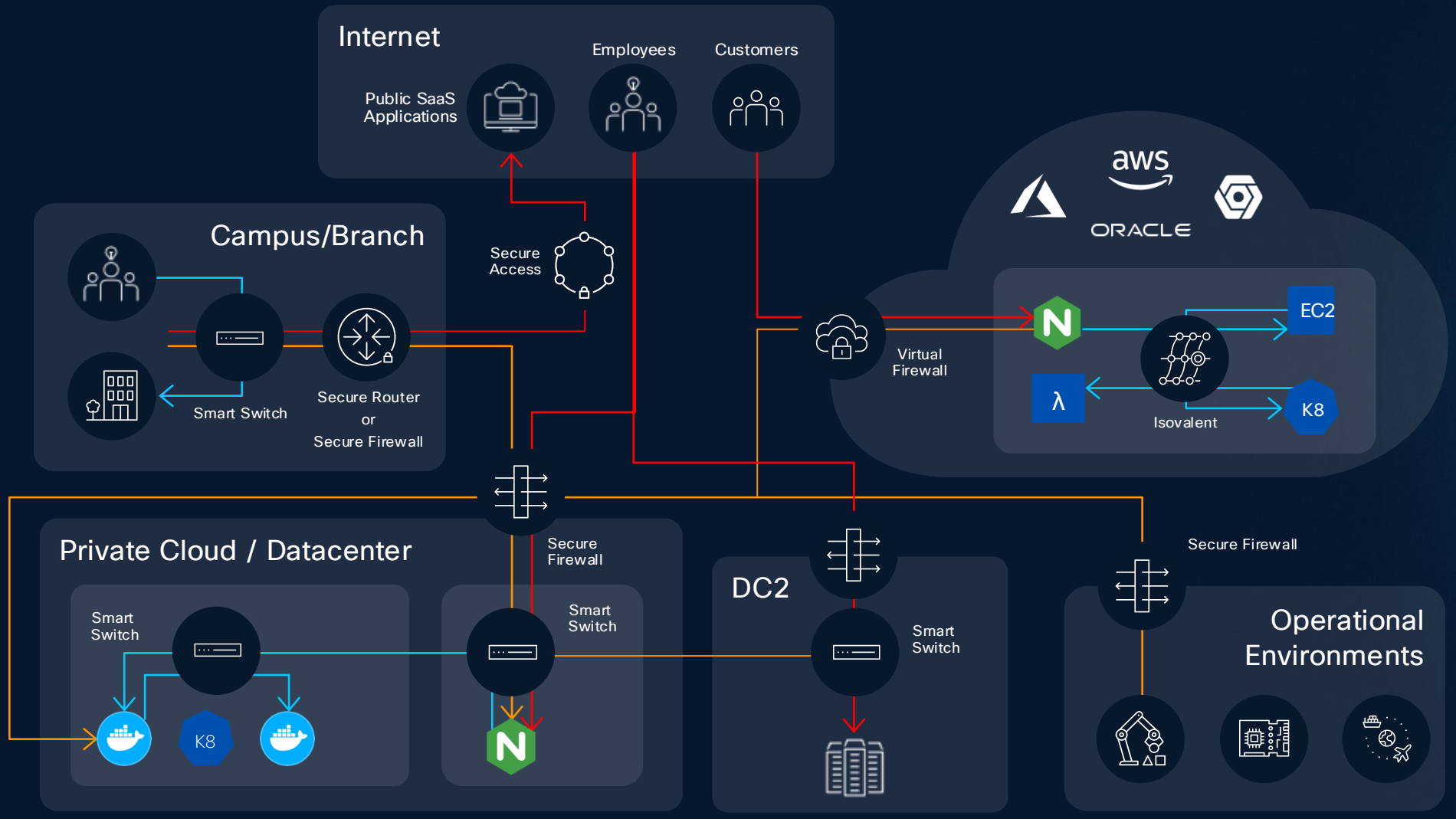
## DC Edge - Perimeter Firewall

Safeguard north-south traffic by blocking external threats, securing critical DC workloads, enforcing least-privilege access, supporting compliance, and ensuring uninterrupted business operations.

## Cloud Edge

Deliver consistent, automated, and scalable security across hybrid and multi-cloud environments, reduces operational complexity, enhances threat visibility, and enables scalable security enforcement closer to the cloud application workloads.

# Cisco Hybrid Mesh Firewall goes broader and deeper




Secure connectivity between campus, branch, and private cloud

Securely connect campus to Internet and SaaS apps, and employees to private apps

Apply full security stack (IPS, WAF, DLP at virtual public cloud (VPC) edge

Security inline at workload, microservice, and switch port

# Secure Firewall

Firepower Threat Defense 10.0 for every use case

# Superior visibility beyond deep packet inspection

Security Intelligence

Encrypted Visibility Engine

Snort 3 with SnortML

QUIC Decryption

Advanced Malware Protection

# Cisco Talos global threat intelligence

Our job is your defense.

## Global Network Visibility

Analyzing **886B+** security events daily

from **46M+** devices

across **193** countries

in **46+** languages

## A legacy of innovation. AI-optimized services for the future.

**Talos Intrusion Prevention**

**65K** Rules targeting threat actor behavior

**Talos Vulnerability Research**

**200+** vulnerabilities discovered annually

**Talos Web Filtering**

**5B** malicious URIs blocked annually

**Talos Malware Protection**

**95M** malware samples blocked monthly

**Talos DNS Security**

**400M** malicious domains blocked monthly

**Talos Anti-Virus**

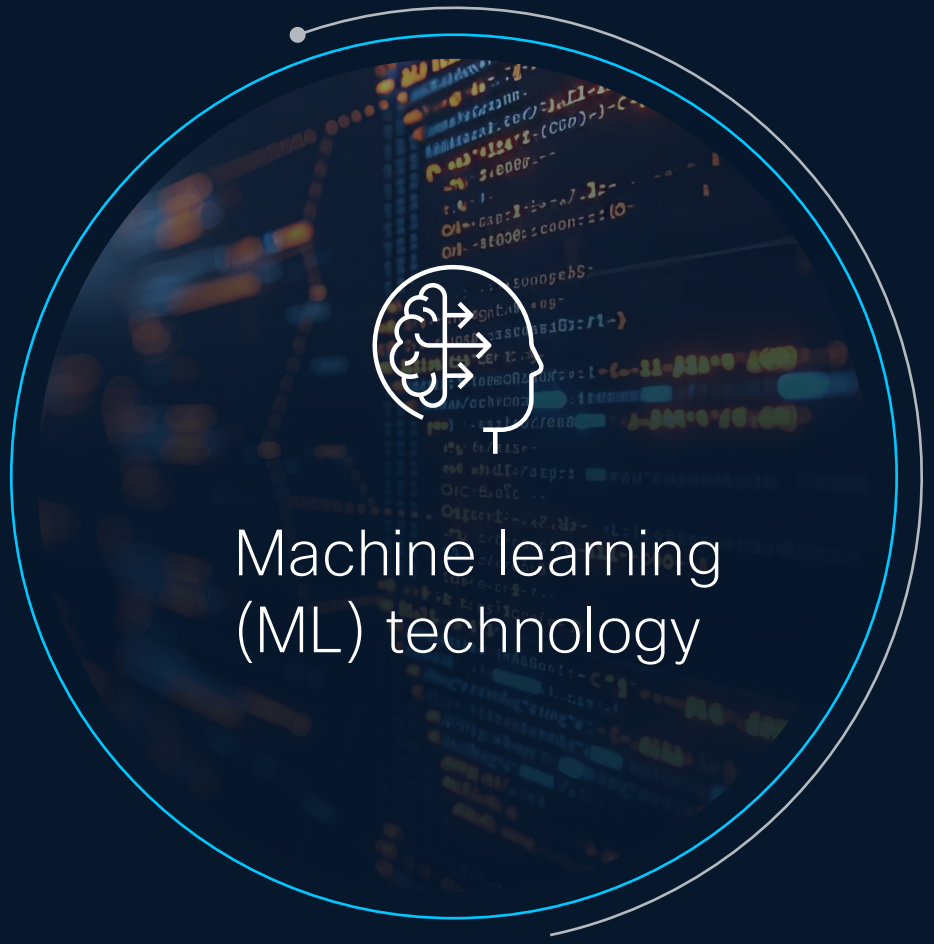
**85K** malicious files found daily

# Encrypted Visibility Engine

## Visibility for malicious flows in encrypted traffic

**1B+TLS**

fingerprints,
10K+ malware
samples daily

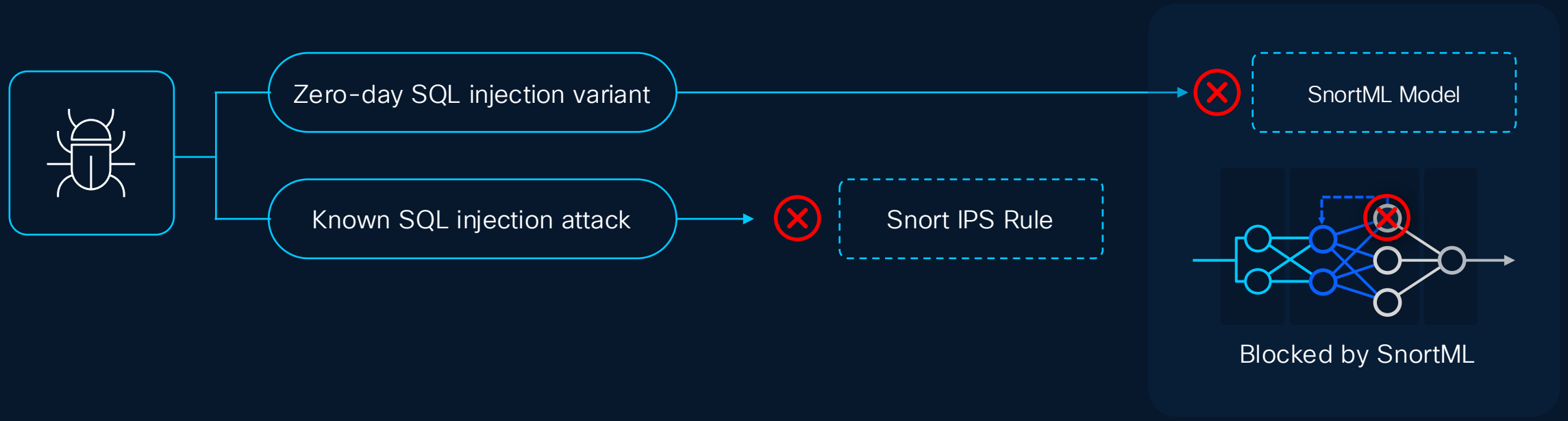


Machine learning
(ML) technology

**10x**

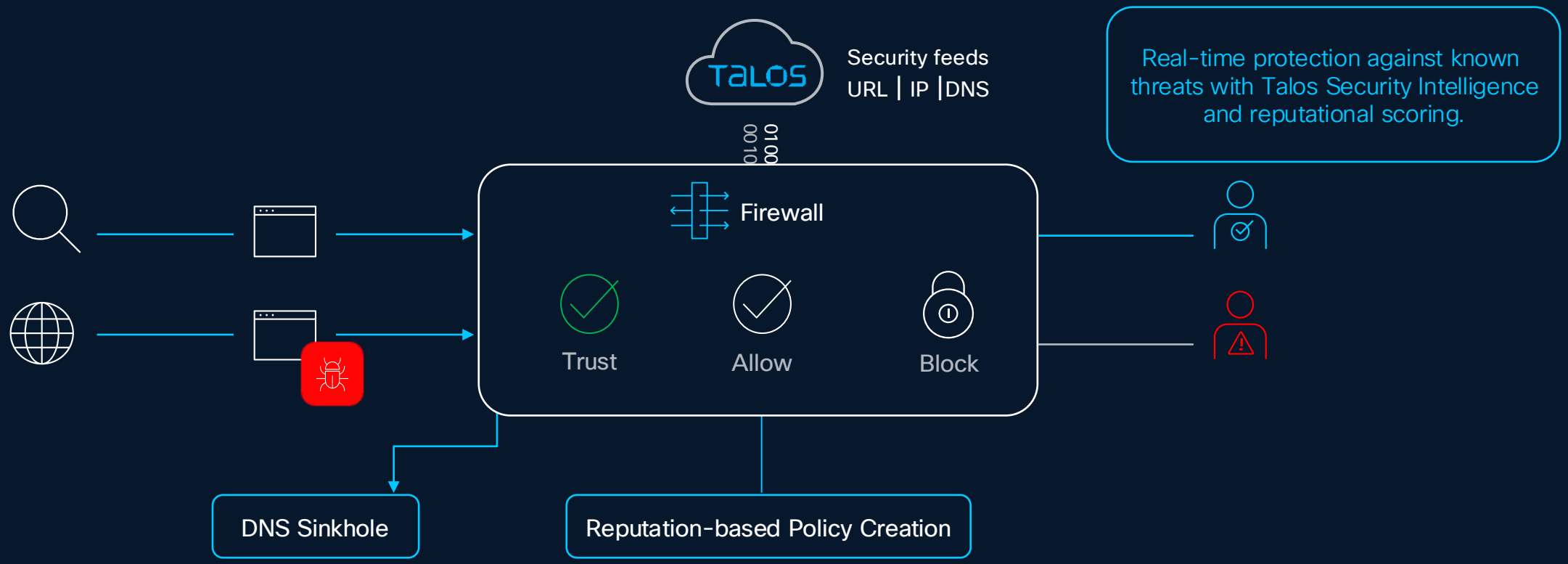
performance
with selective
decryption

# Stop known and unknown attacks



# Supercharge access control

## Enhanced by Talos Security Intelligence and AppID




Security Intelligence:
Up-to-the-minute protections from known-bad IP/URL/DNS

Application ID:
Identify and control over 7,300+ pre-defined apps

AVC with OpenAppID:
Easily create custom application detectors

URL Reputation:
Allow/Block sites based on reputational scoring from Talos

# Firewalls for every use case

**ISA 3000 Series**

≦0.4Gbps NGFW

**200 Series**

1.5Gbps NGFW

**1010 & 1100 Series**

≦3Gbps NGFW

**1200 Compact Series**

≦9Gbps NGFW

**1200 Series**

≦18Gbps NGFW

**3100 Series**

≦45Gbps NGFW 16x Clustering

**4200 Series**

≦145Gbps NGFW 16x Clustering

**6100 Series**

520-630Gbps NGFW 16x Clustering

IOT | Branch | Campus / Data Center

## Private Cloud

HyperFlex

NUTANIX

KVM

openstack

VMware ESXi

## Public Cloud

aws

Google Cloud Platform

Microsoft Azure

rackspace technology.

ORACLE CLOUD INFRASTRUCTURE

EQUINIX

Alibaba Cloud

alkira

## Gov/IC Cloud

aws

Google Cloud Platform



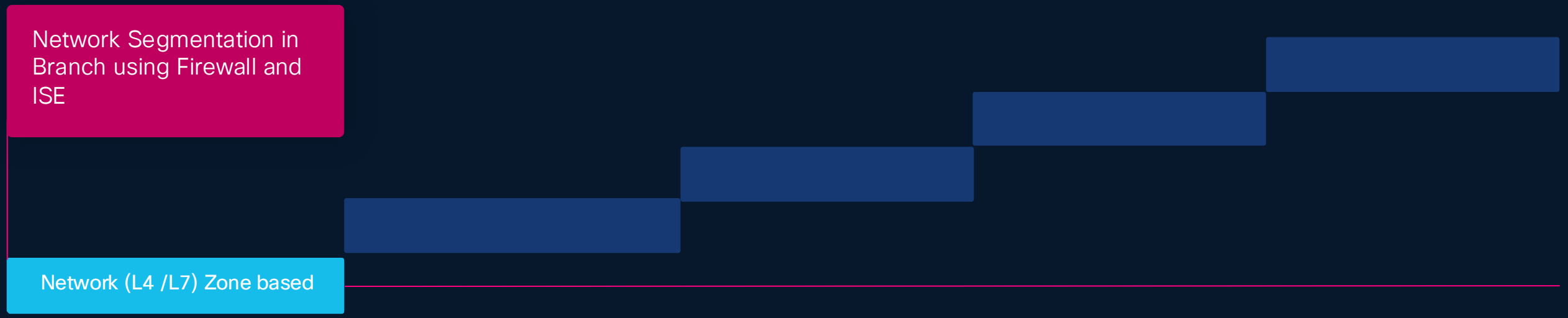
cisco

# Multicloud Defense Deploys FTDv

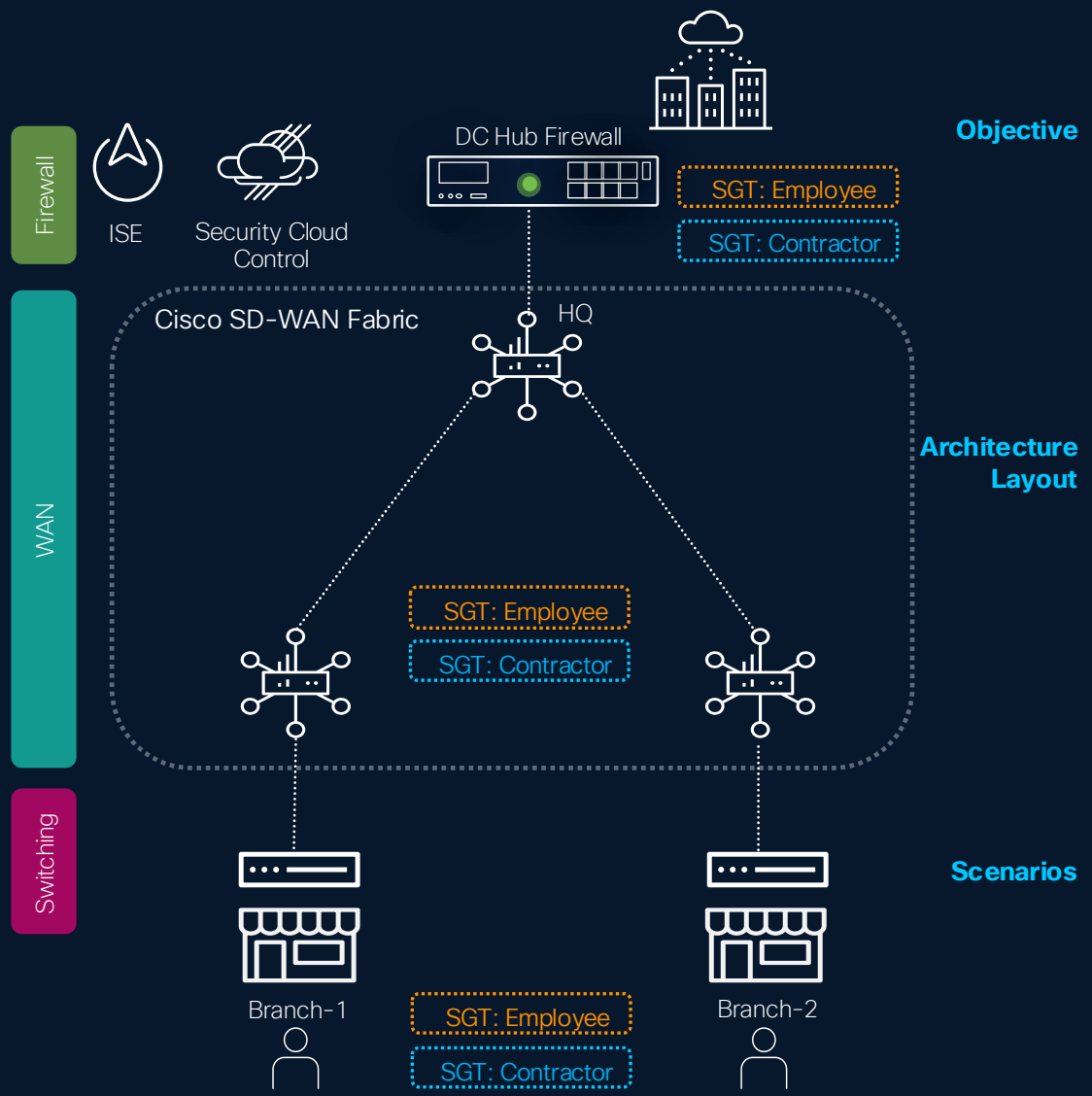

- Comprehensive visibility of clouds, assets, and their risks
- Cloud-agnostic automation and orchestration
- Automatically deploy, scale, and heal, from Multicloud Defense
- Hourly price; unlike other offers based on size and bandwidth
- Or use with your existing FTDv licensing

# End-to-End Segmentation

# End-to-End Segmentation



# Branch Segmentation Reference Architecture




**Objective**

This architecture simulates a real-world Enterprise WAN environment designed to showcase the capabilities of Cisco Secure Firewall with Cisco SD-WAN in providing a zero-trust segmentation architecture.

It demonstrates how the Identity based segmentation propagates from the User Onboarding through SD-WAN network to the DC Hub Firewall where role-based policy is enforced.

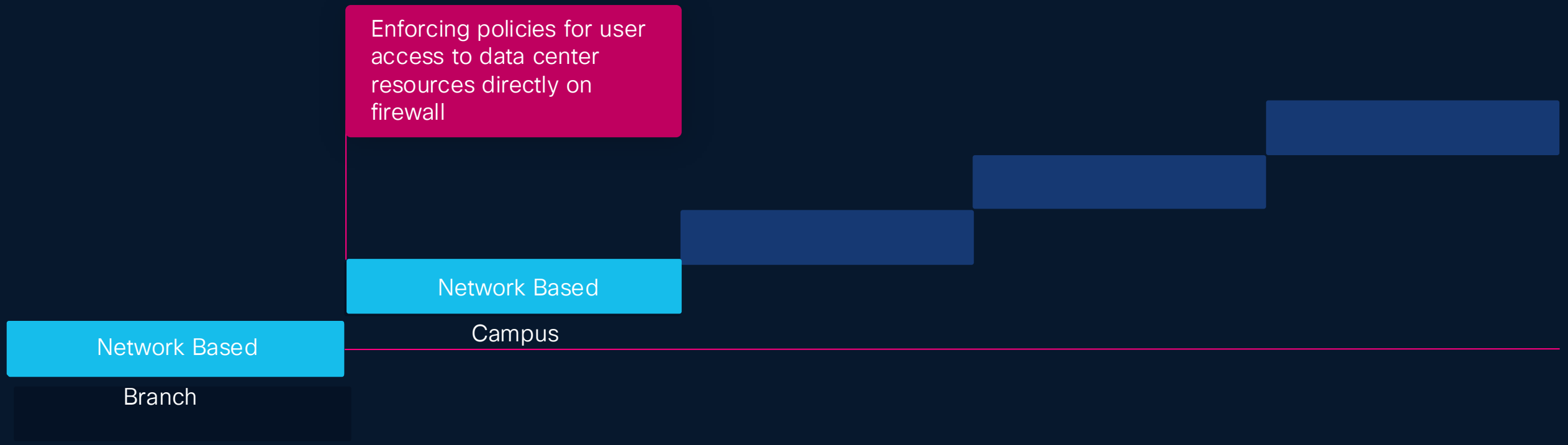
**Architecture Layout**

- **Security Cloud Control** – Unified plane for firewall policy control and visibility management
- **User** – Emulate Malware threat that can be detected and user can be quarantined
- **Internet** – The boundary of Internet (untrusted zone) and the data center (protected zone)
- **Firewall** – The security defense for the campus
- **SD-WAN** – WAN connectivity offering improved application aware policies and enhanced security
- **Switching** – Enforce VLAN segregation and form part of the trustsec architecture
- **ISE** – The network access control and Security Group Tag policy implementation

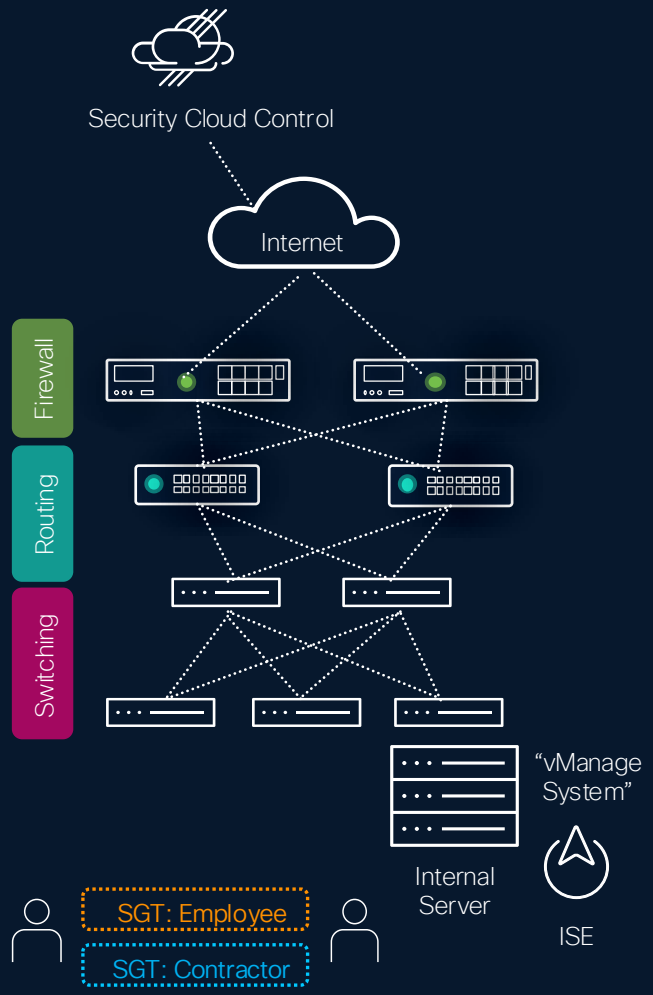
**Scenarios**

- **SGT Propagation Focus**– An employee gets onboarded on the network upon getting authenticated , an IP and an SGT tag gets assigned based on the role of the employee. Also a contractor comes in to fix the IoT devices at multiple branches and connects to LAN network, ISE assigns a Contractor SGT for the connection, ISE policy only allows the contractor to only access IoT device and internet access. Administrator restricted the contractor access at the DC Hub Firewall enforces policy to only allow internet access and will block access if they try to access Intranet server.

# End-to-End Segmentation



# Campus Segmentation Reference Architecture




## Objective

This architecture simulates a real-world enterprise campus environment designed to showcase the capabilities of Cisco Secure Firewall with Cisco ISE in providing a zero-trust segmentation architecture.

It demonstrates how the firewall inspects and controls both inbound threats from external sources and outbound data flows, ensuring secure communication within the enterprise and to external networks while preventing unauthorized access and data exfiltration.

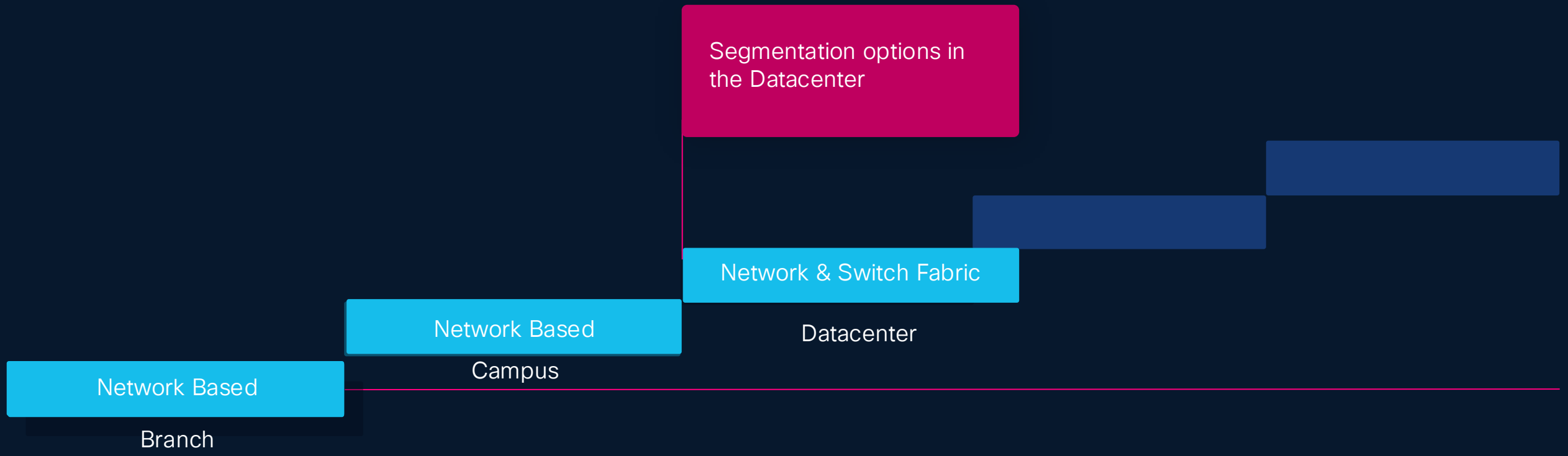
## Architecture Layout

- **Security Cloud Control** – Unified plane for firewall policy control and visibility management
- **User** – Emulate Malware threat that can be detected and user can be quarantined
- **Internet** – The boundary of Internet (untrusted zone) and the data center (protected zone)
- **Firewall** – The security defense for the campus
- **Routing** – Support traffic redirection between firewall and internal enterprise environment
- **Switching** – Enforce VLAN segregation and form part of the trustsec architecture
- **ISE** – The network access control and Security Group Tag policy implementation

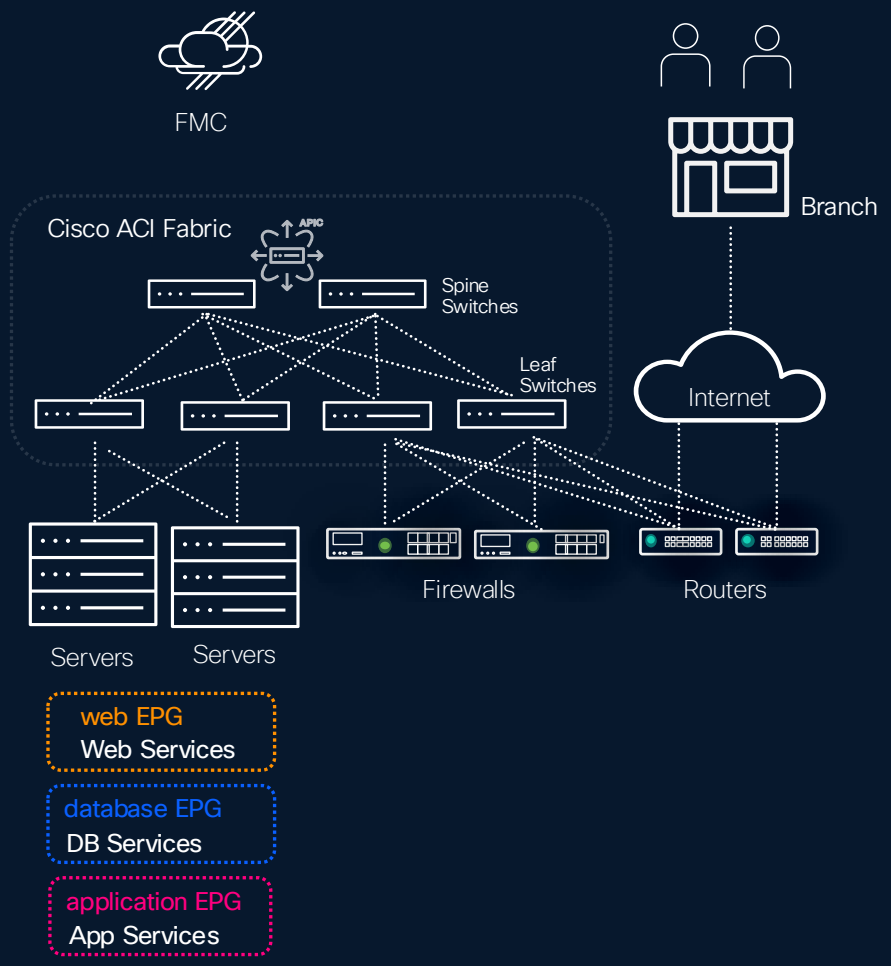
## Scenarios

- **Rapid Threat Containment** – This demo uses the firewall to trigger an IPS rule on malicious traffic from sales user to the intranet server. The firewall send notification to ISE of this event. ISE assigns the "Quarantines System" SGT. Subsequent traffic is blocked at the firewall on the TAG.
- **Context Aware Access**– Contractor connects to LAN network, they get redirected to a guest portal hosted by ISE, ISE authenticates the guest. contractor user is assigned "Contractor" SGT, policy only allows internet access. Firewall enforces policy to only allow internet access and will block access if they try to access vManage system.

# End-to-End Segmentation



# Datacenter Segmentation Reference Architecture




## Objective

This architecture simulates a real-world Datacenter environment designed to showcase the capabilities of Cisco Secure Firewall with Cisco ACI in providing a zero-trust segmentation architecture.

It demonstrates how the firewall inspects both north-south and east-west communication within a data center that is architected around Cisco ACI fabric.

## Architecture Layout

- **Security Cloud Control** – Unified plane for firewall policy control and visibility management
- **Firewall** – the security defense for the data center communications
- **Cisco ACI Fabric** – Enforce segmentation with End Point Groups to create a zero-trust architecture, this includes a control plane function called APIC and for data plane there a Nexus switches
- **Routing** – WAN routers at both DC and branch location
- **Users** – Different types of users, Contractor and Employee

## Scenarios

- **Rapid Threat Containment** – This demo uses the firewall to trigger an IPS rule on malicious traffic being downloaded to servers connected to the ACI fabric. The firewall learns the EPG information from the APIC integration and can configure policies based on the EPGs. The intrusion event is generated and sent to FMC revealing information about infected host. The event is configured to trigger remediation module for APIC that uses NB API to contain the infected host in ACI fabric. APIC quickly quarantines the infected “App server” into an isolated “quarantined” EPG.

# L4 Switch Fabric Segmentation

Nexus Smart Switch + Hypershield

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

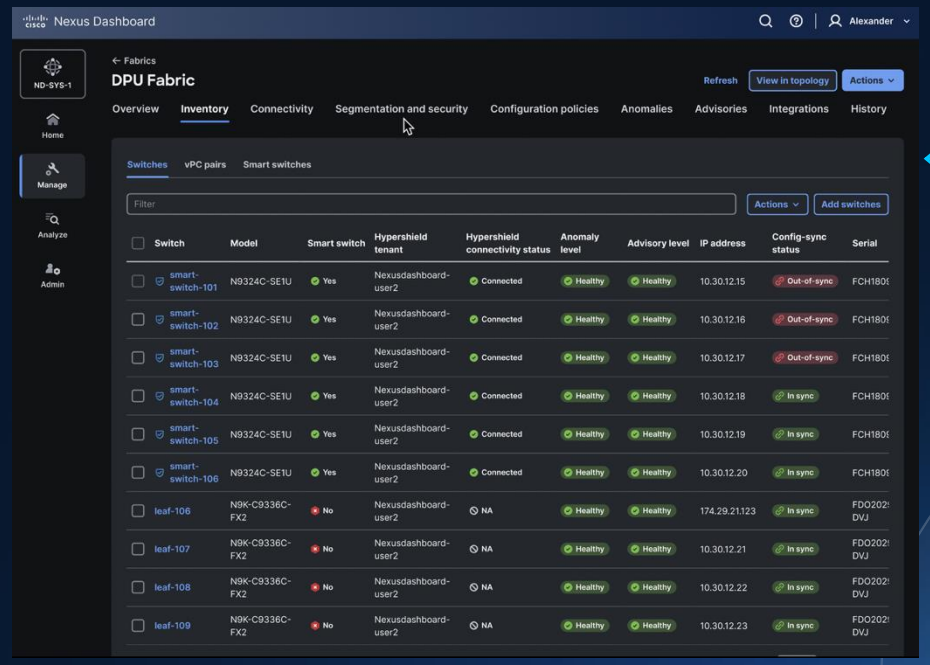
AMD PENSANDO

- 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

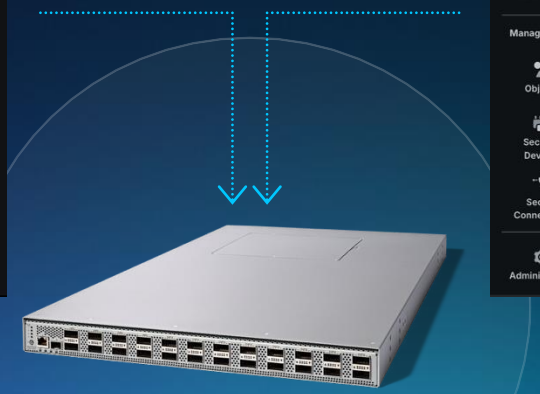
Large-Scale NAT | IPSEC Encryption | Distributed Firewall | Event-Based Telemetry | DoS Protection

# Separate workflows for NetOps and SecOps

## Nexus Dashboard

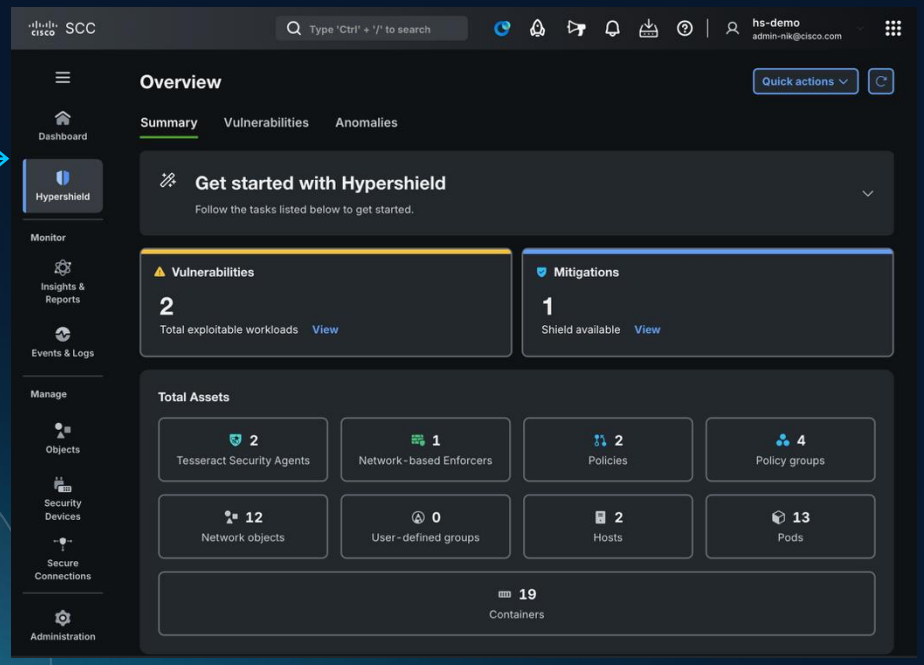



Context sharing for troubleshooting*

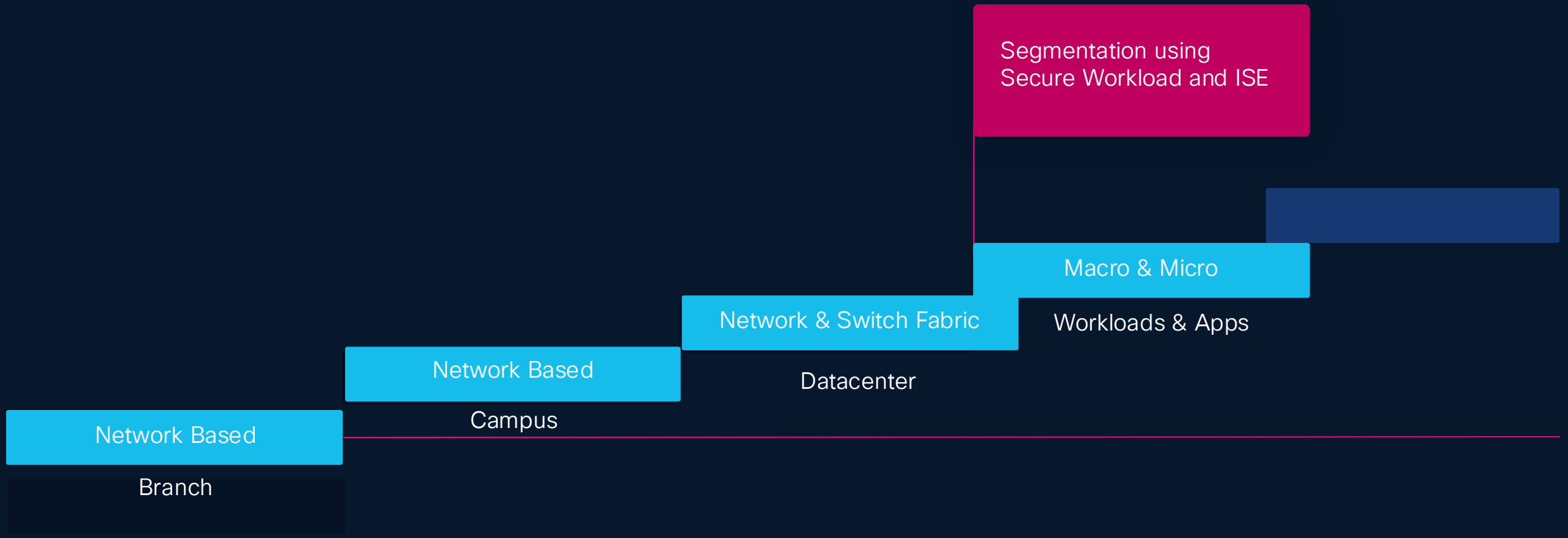


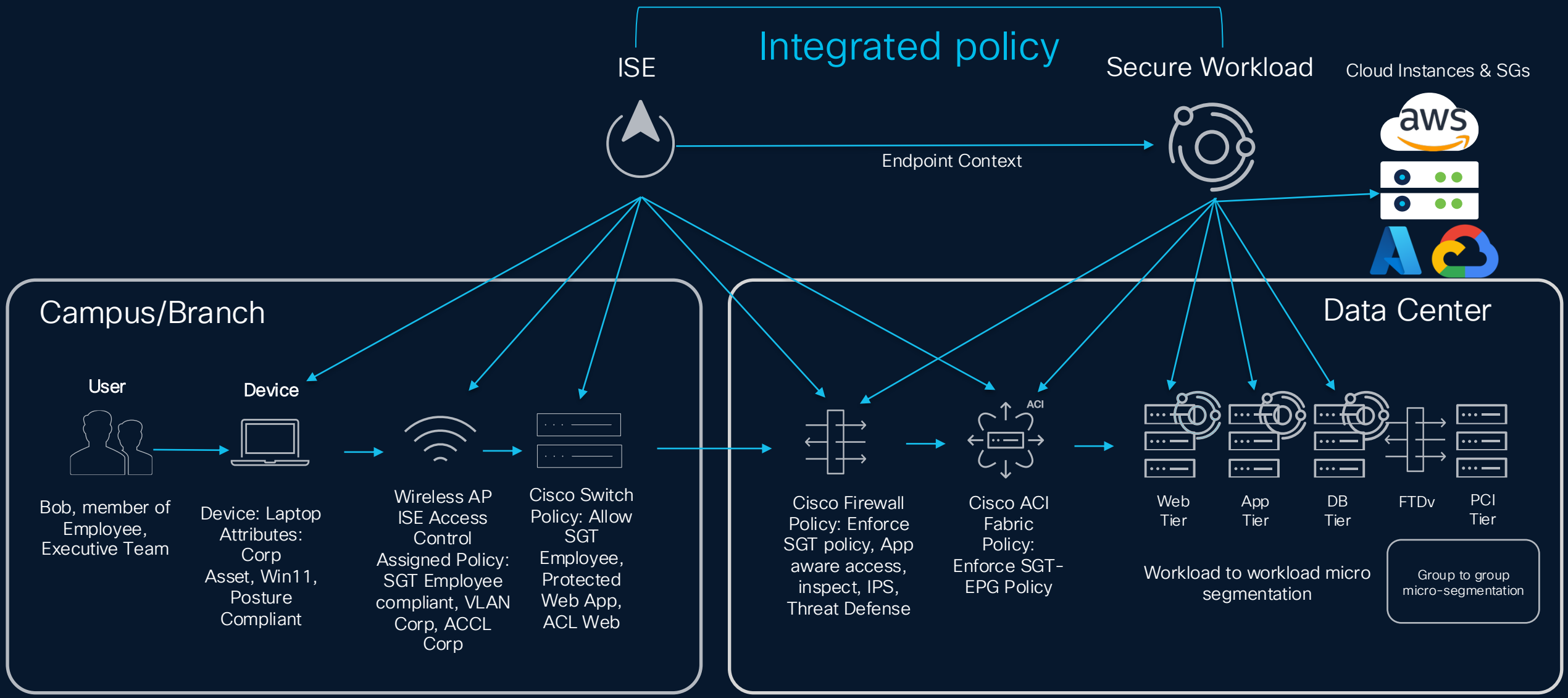
Smart Switch

## Security Cloud Control

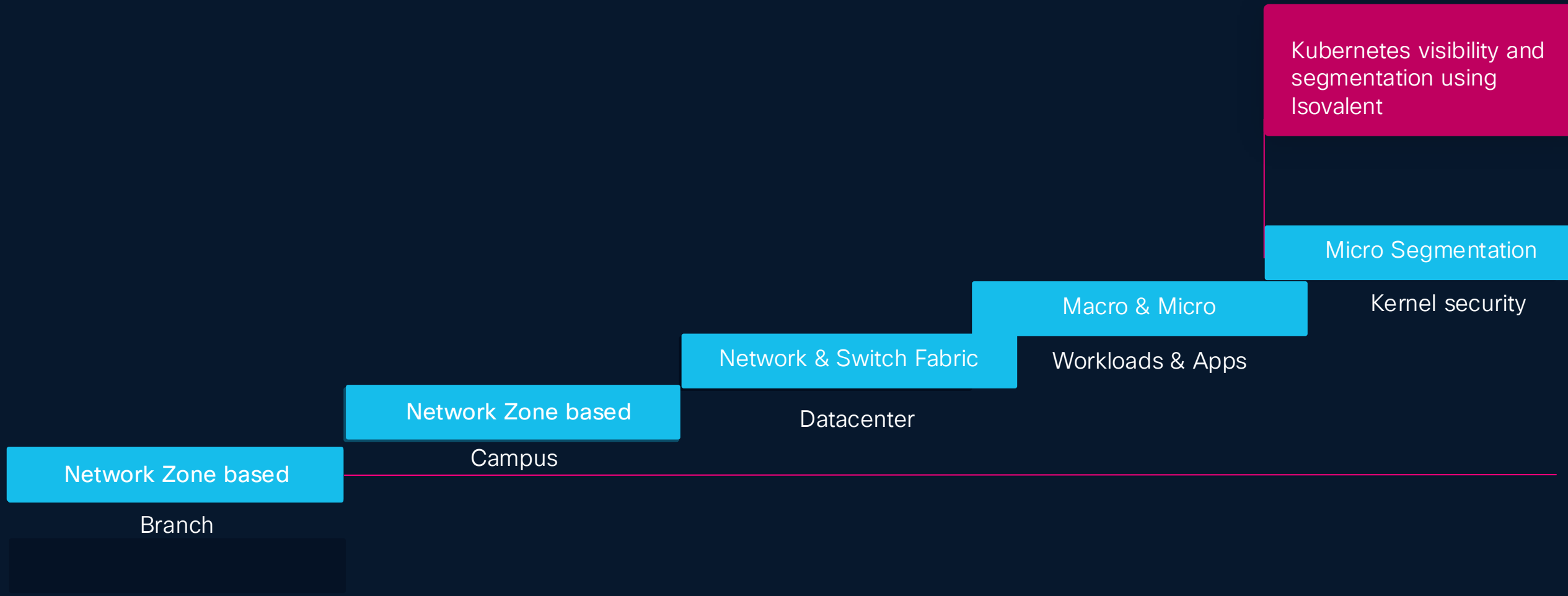


# End-to-End segmentation





# End-to-End Segmentation

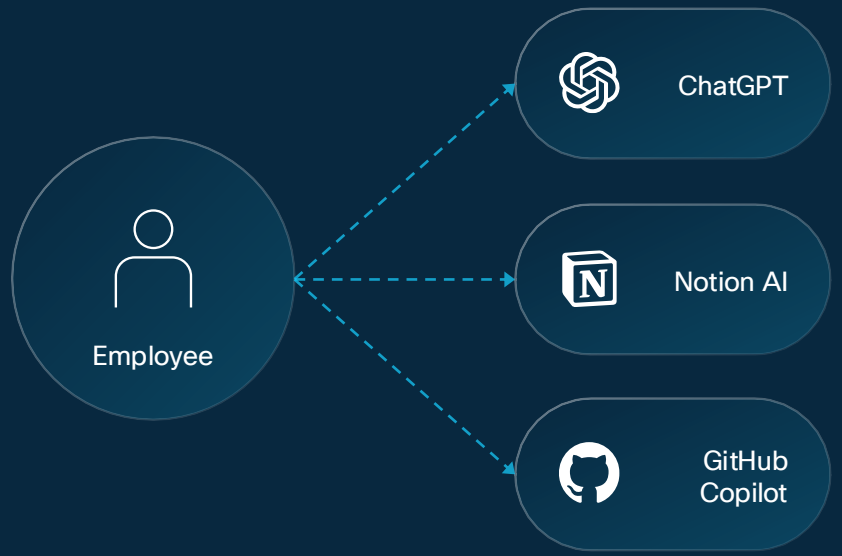


# AI Model Security

# Two distinct areas of AI risk

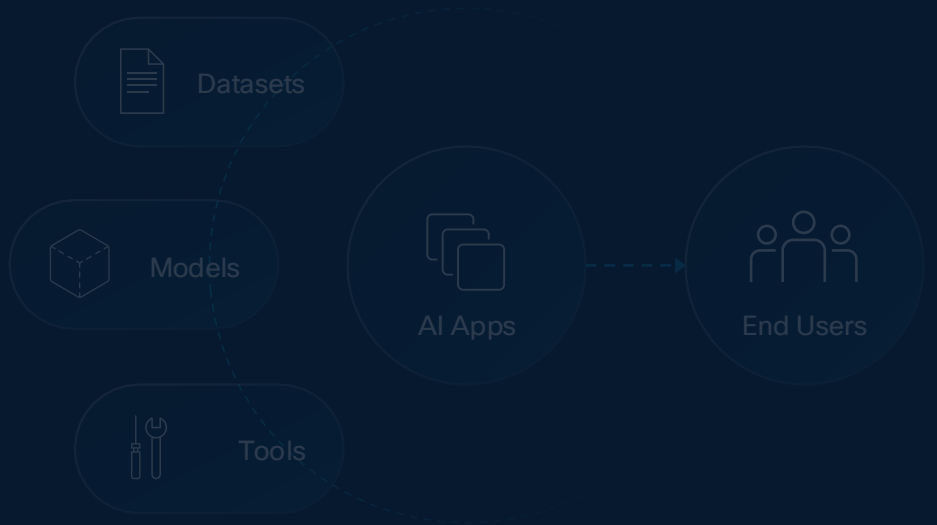
## Third-Party AI Tools

Manage employee use of **third-party AI tools**, preventing data leakage and other business risks, with Cisco Secure Access.




## First-Party AI Applications

Enable end-to-end secure development of **first-party AI applications** across your business with Cisco AI Defense.



# Secure Access: SSE that truly understands AI

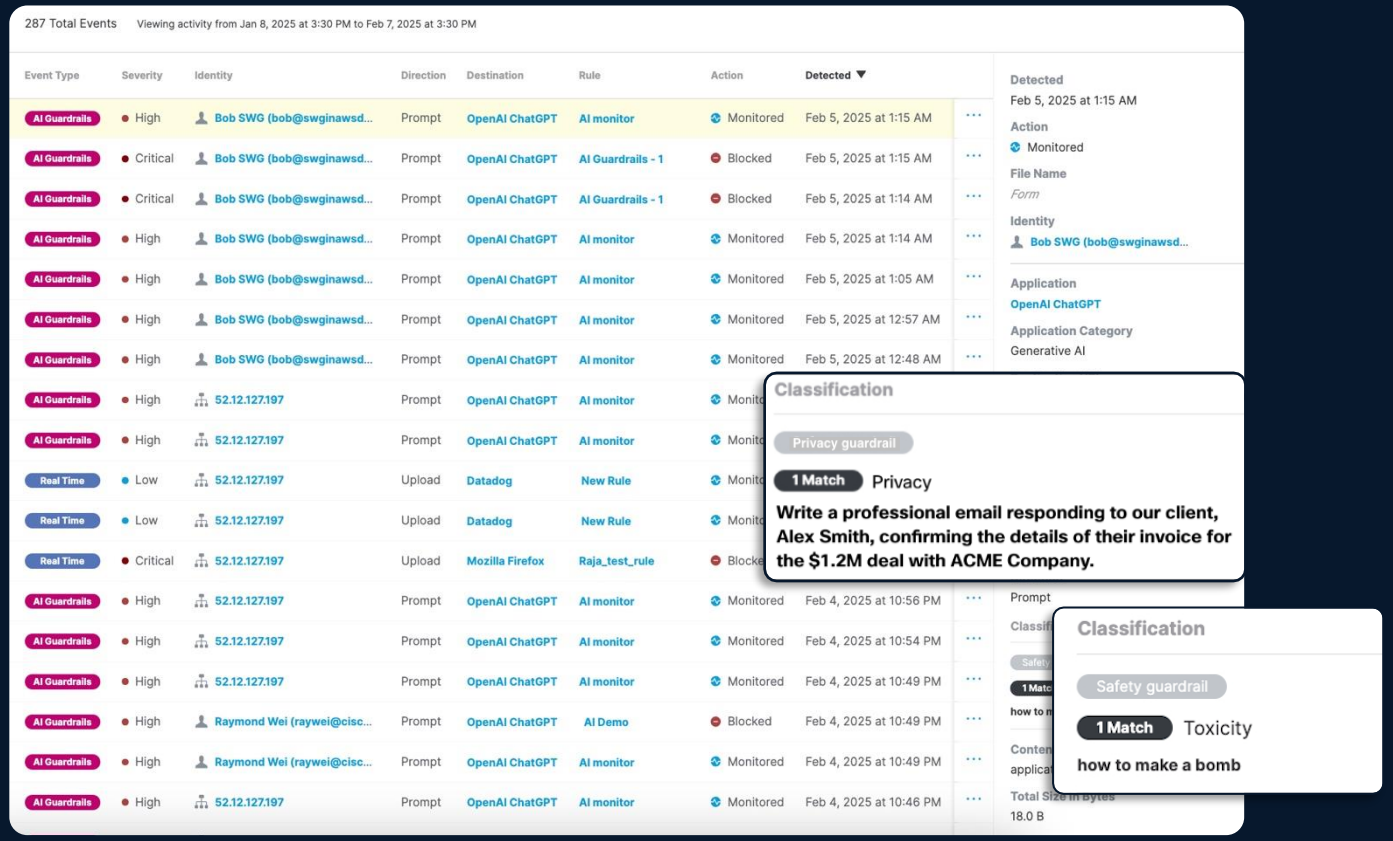
Powered by AI Defense models to *understand intent*

## Intelligent Protection

- Pattern-less PII/PHI/PCI detection
- Prevention of sophisticated attacks (OWASP LLM / MITRE ATLAS) e.g., prompt injection
- Intent-based toxicity detection

## Zero-Friction Security

- Built into Secure Access*
- Single unified policy framework
- No additional infrastructure



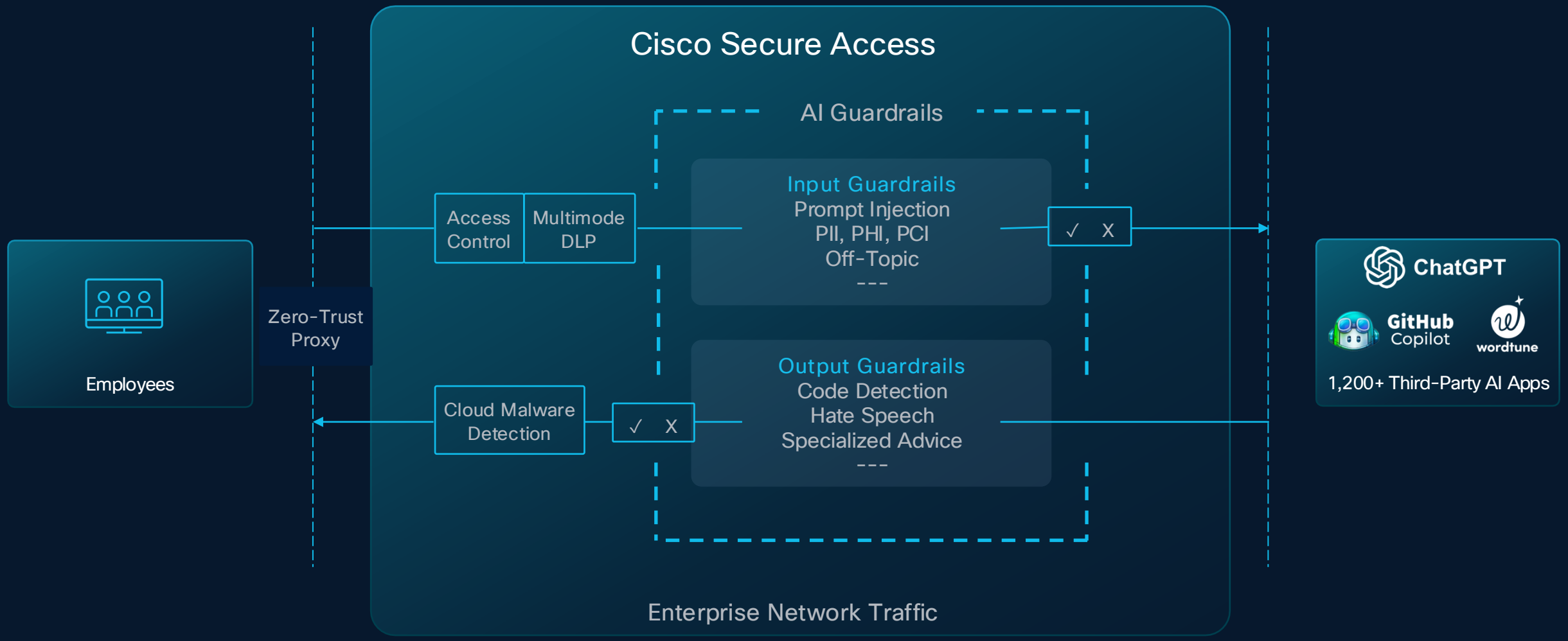

1200+
AI Applications Coverage

100%
Top 16 AI Apps Coverage

1
Unified Security Framework

(*) included in Secure Access Advantage

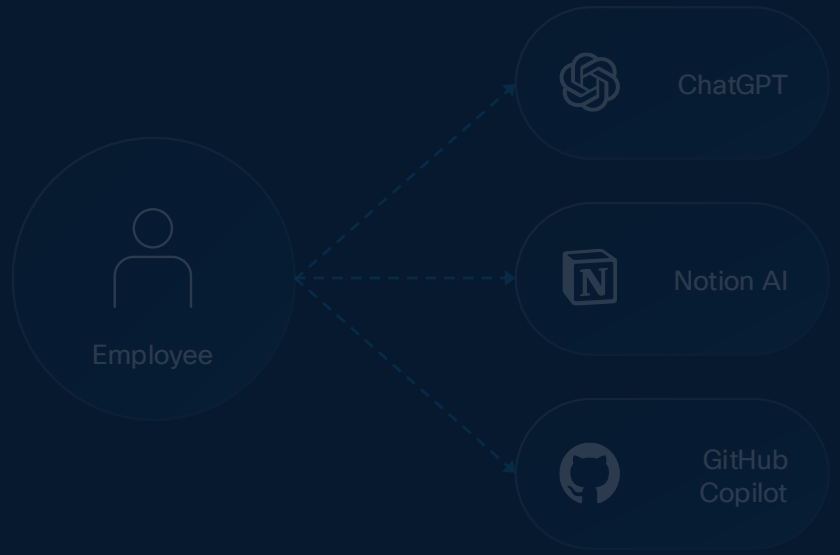
# Protecting usage of third-party AI apps



# Two distinct areas of AI risk

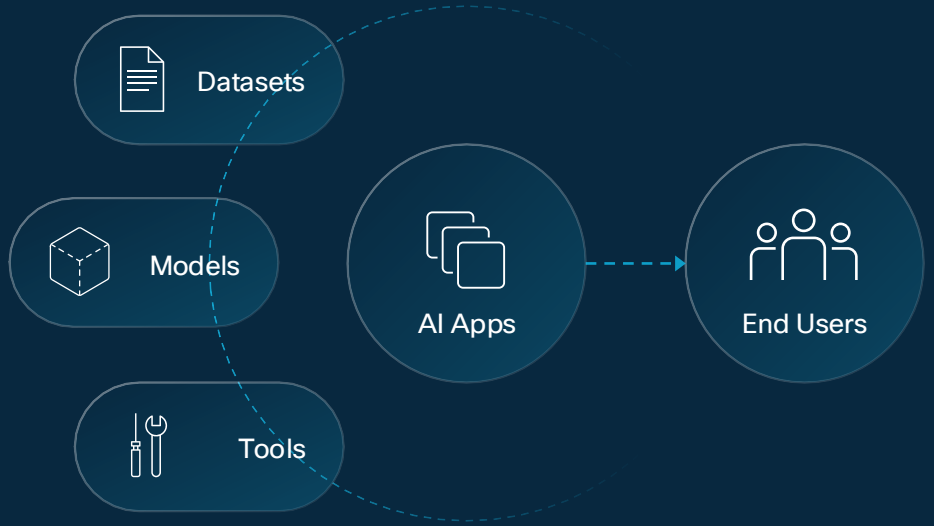
## Third-Party AI Tools

Manage employee use of **third-party AI tools**, preventing data leakage and other business risks, with Cisco Secure Access.




## First-Party AI Applications

Enable end-to-end secure development of **first-party AI applications** across your business with Cisco AI Defense.



# A three-step framework for developing secure AI applications

## Discovery

Uncover AI assets including models, agents, and datasets

## Detection

Test for AI risk, vulnerabilities, and susceptibility to attack

## Protection

Define guardrails that secure data and defend against runtime threats

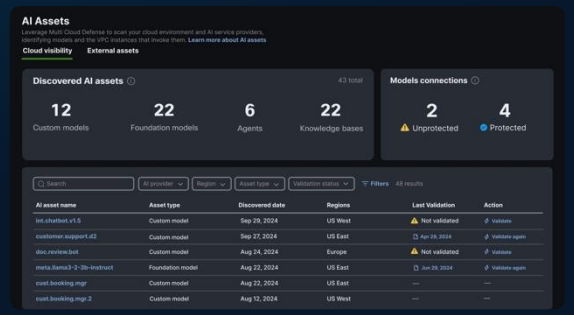
# AI Defense: coverage across the AI lifecycle

*Discovery*

## AI Cloud Visibility

### Identify AI assets

Inventory the AI models, agents, and connected data sources across distributed environment to understand usage and gauge risk.

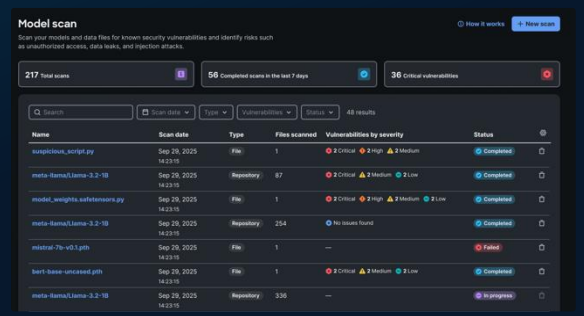



*Detection*

## AI Supply Chain Risk Management

### Scan for threats

Scan model files, repos, and MCP servers to proactively block malicious or unsafe AI assets before operations are impacted.




## AI Model & App Validation

### Detect the vulnerabilities

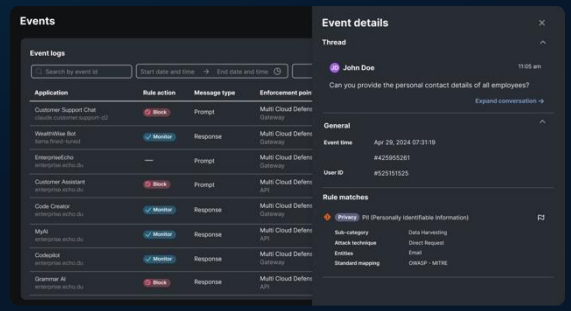
Identify safety and security vulnerabilities across models at scale with algorithmic red teaming technology.


*Protection*

## AI Runtime Protection

### Mitigate threats in real time

Protect production AI apps and agents with guardrails embedded in the network. Block attacks and harmful responses in real time.



# Key Takeaways

Cisco Tech Day
Denver

# Thank you!


CISCO