CISCO Engage | Tech Day

SEC3 - Deciphering Hybrid Mesh Firewall

Mark Stephens – Cyber Security Solutions Engineer

Oct 2, 2025

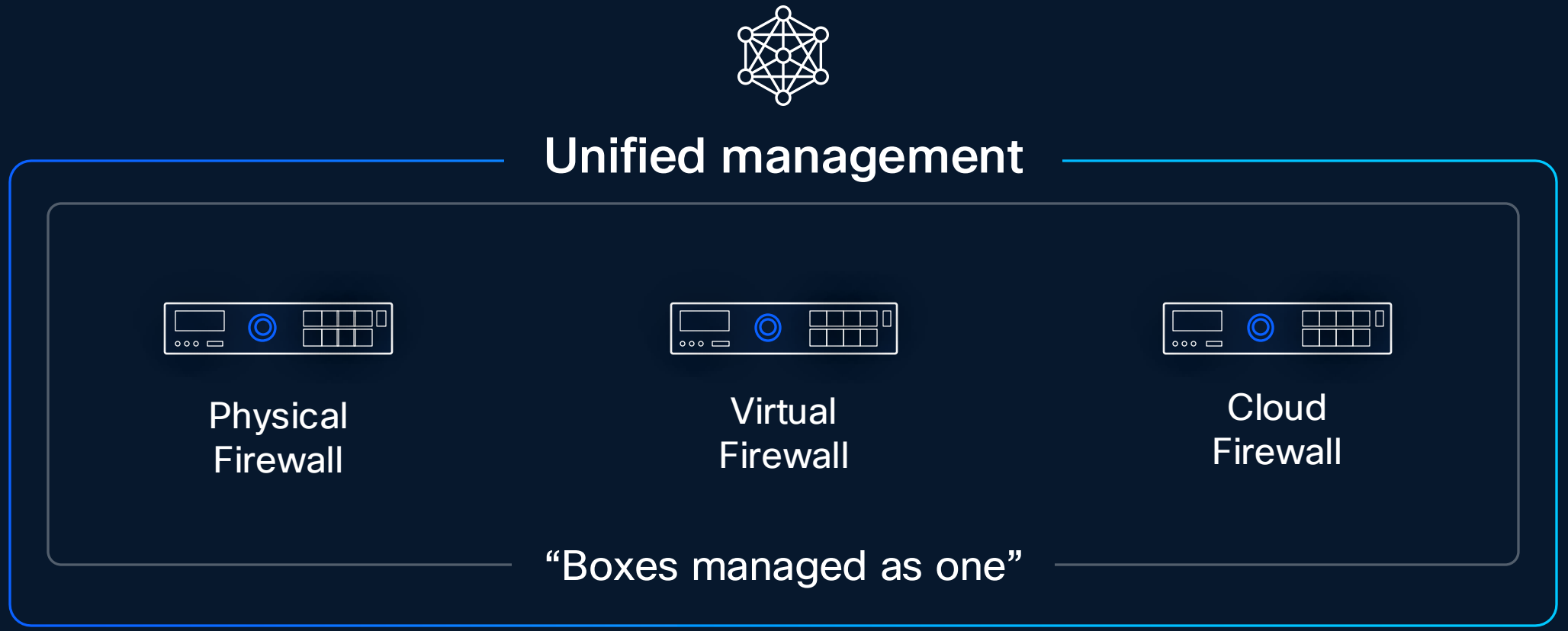
Agenda

1. What is HMF?
2. Firewall Innovations
3. Customer use cases
4. HMF Value Proposition

From Firewall to Firewalling

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

Basic definition of Hybrid Mesh Firewall is limited



Cisco Hybrid Mesh Firewall goes broader and deeper

Security Cloud Control

Native enforcement points go deeper

Integrate with existing

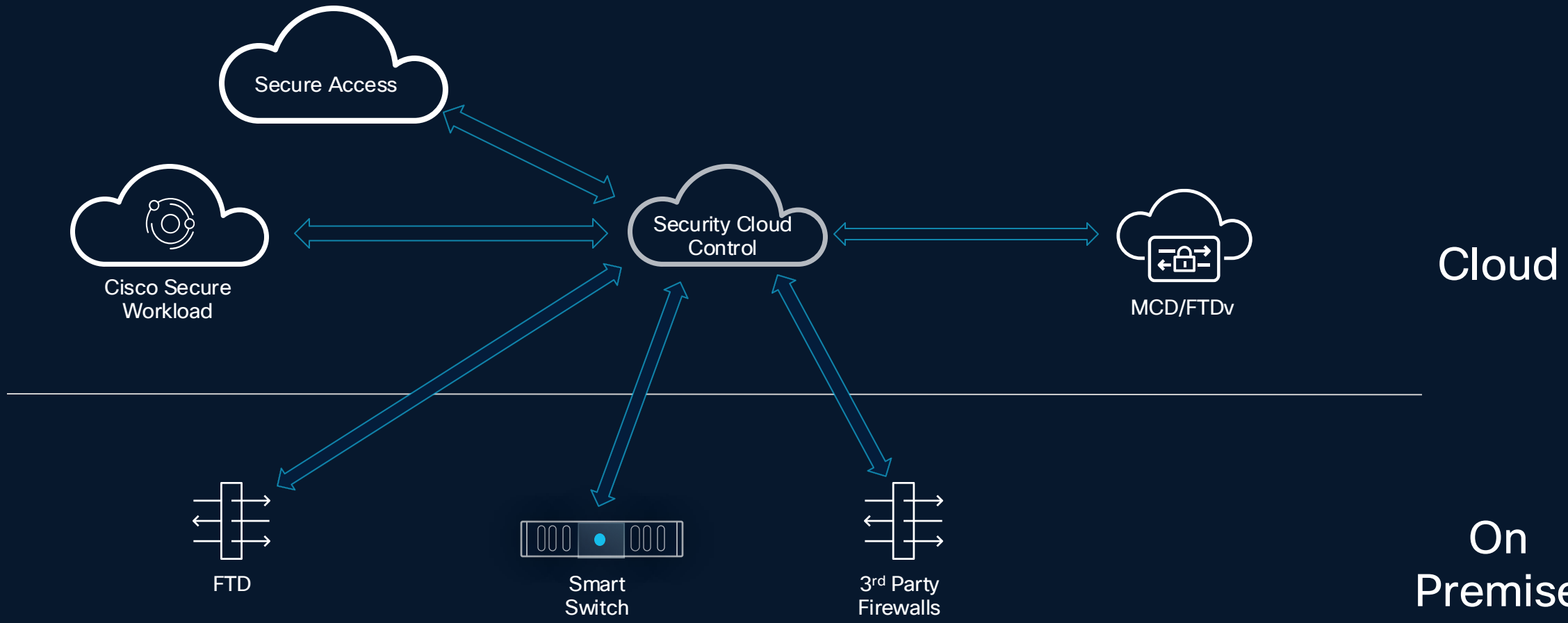
Write policy once, enforce across the mesh

cisco

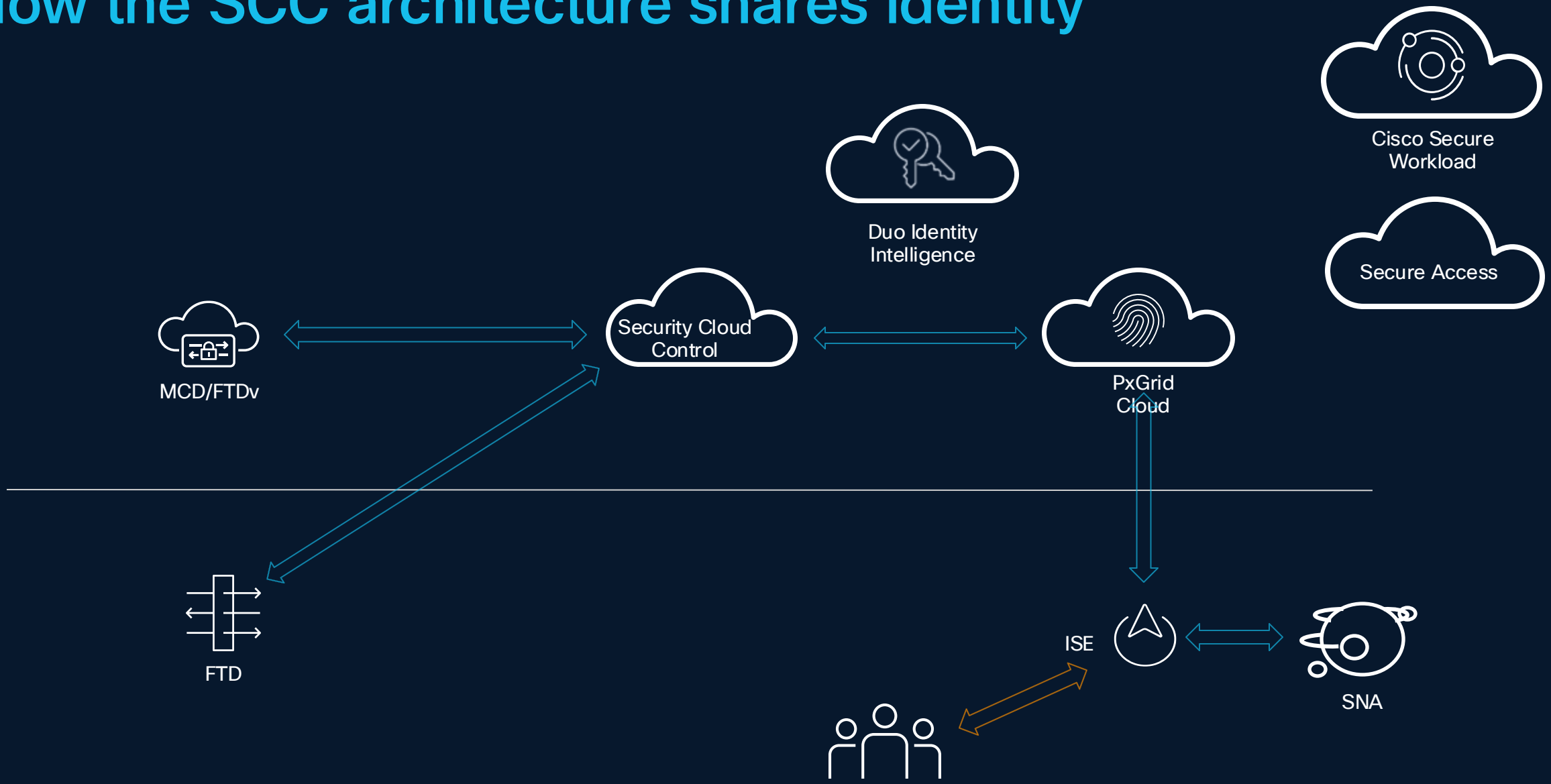
Customer projects we can solve **today**

- Network Segmentation
- Kubernetes Security
- Microsegmentation
- AI Security
- Threat Detection & Exploit Protection

How SCC architecture connects to many PEPs



How the SCC architecture shares identity



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

Unified AI Assistant:
Simplify policy administration **by up to 70%**

cisco

NEW

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

Demo:
Security Cloud Control and Mesh Policy Engine

Something for the network security team

Cisco Firewall price-performance leadership

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 400 Gbps*

*For two rack units (RUs)

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

cisco

Unique capabilities unmatched in the market

Early detection of threats in encryption

Cisco Encrypted Visibility Engine

Detect inline zero-day threats

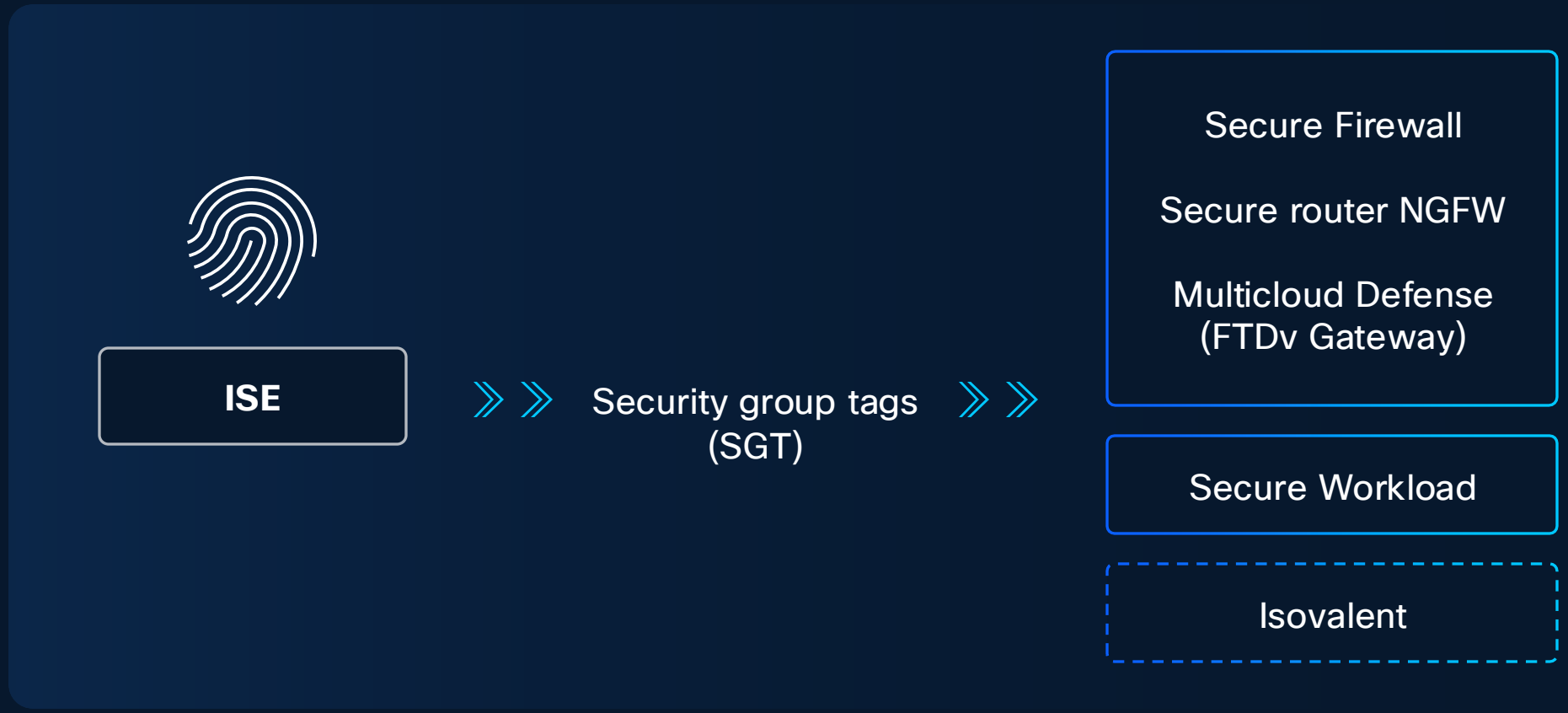
SnortML + Talos

Intelligent segmentation

Native integration with ISE, Secure Workload, and Smart Switch

cisco

Our unique differentiator: Common classification across all Network and Security enforcement points



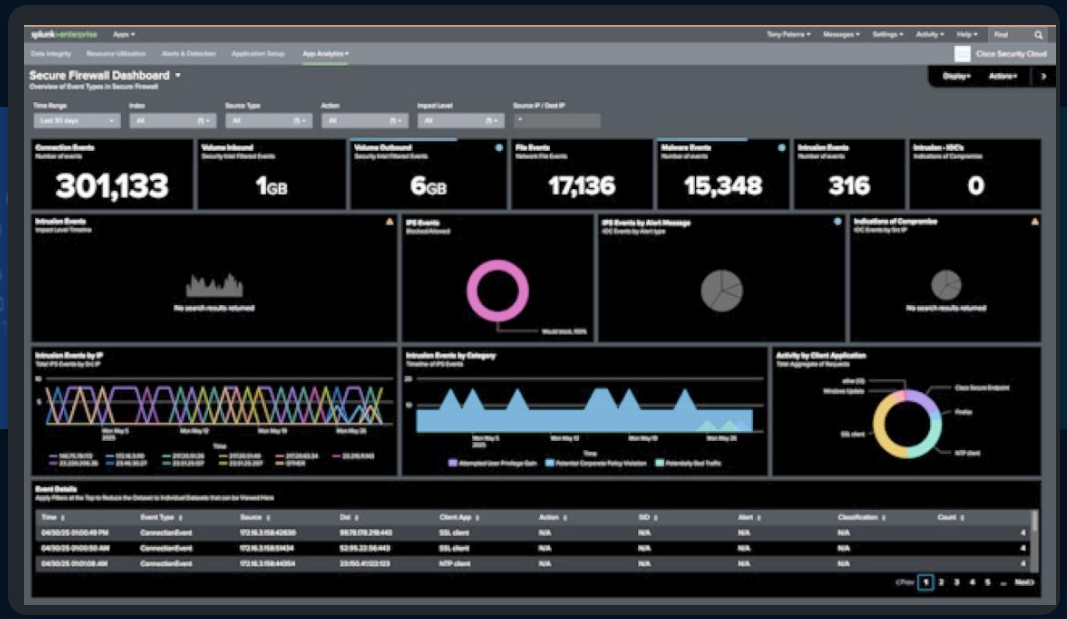
NEW

Security Insight, on Us

Firewall logs free in Splunk

Free log management*

AVAILABLE AUG 2025



New detections | Automated response

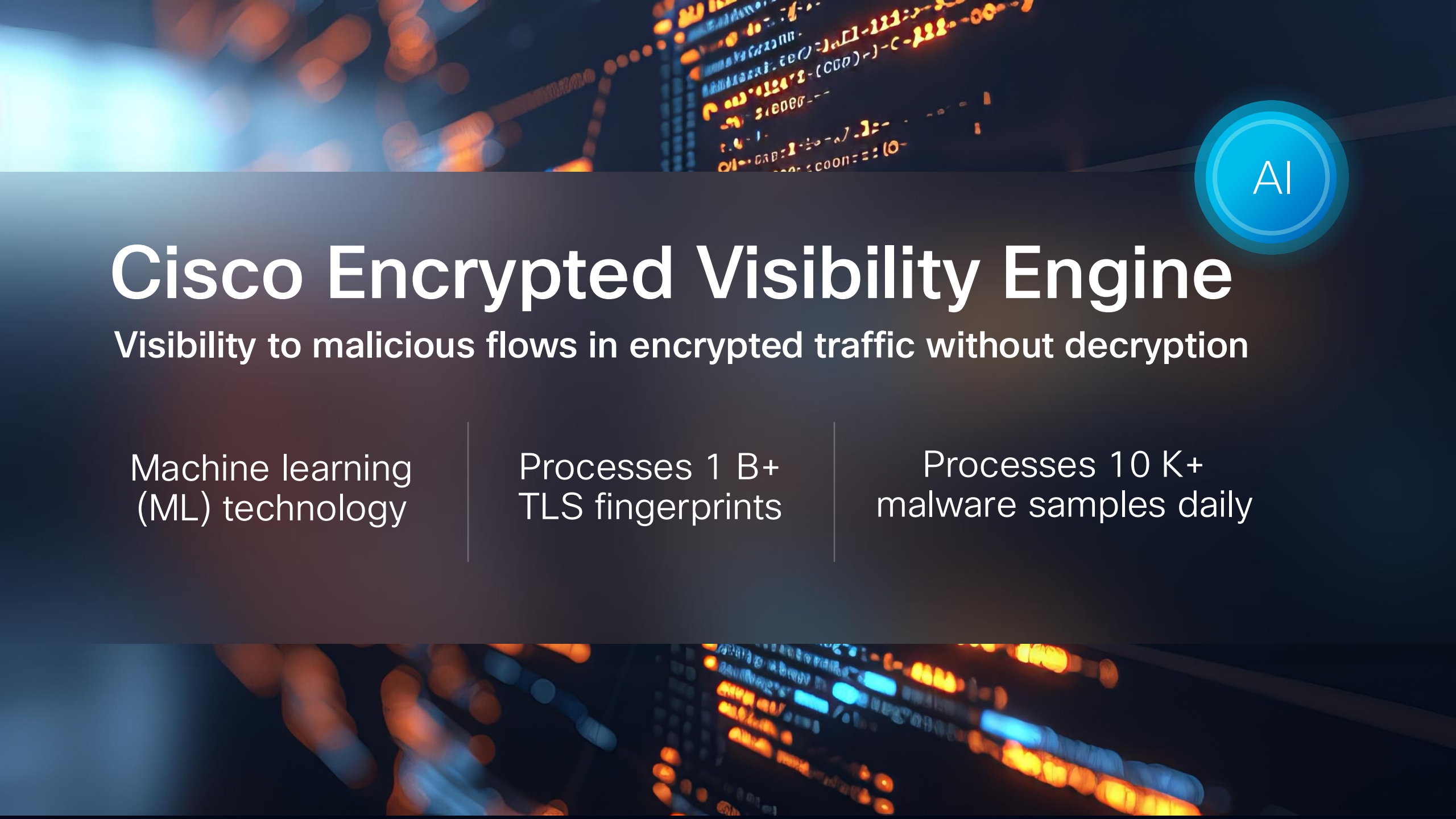
*With active Firewall Threat Defense subscription, some limits and constraints apply

AVAILABLE NOW

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

Firewall operator care abouts:
“How do I do decryption?”



Cisco Encrypted Visibility Engine

Visibility to malicious flows in encrypted traffic without decryption

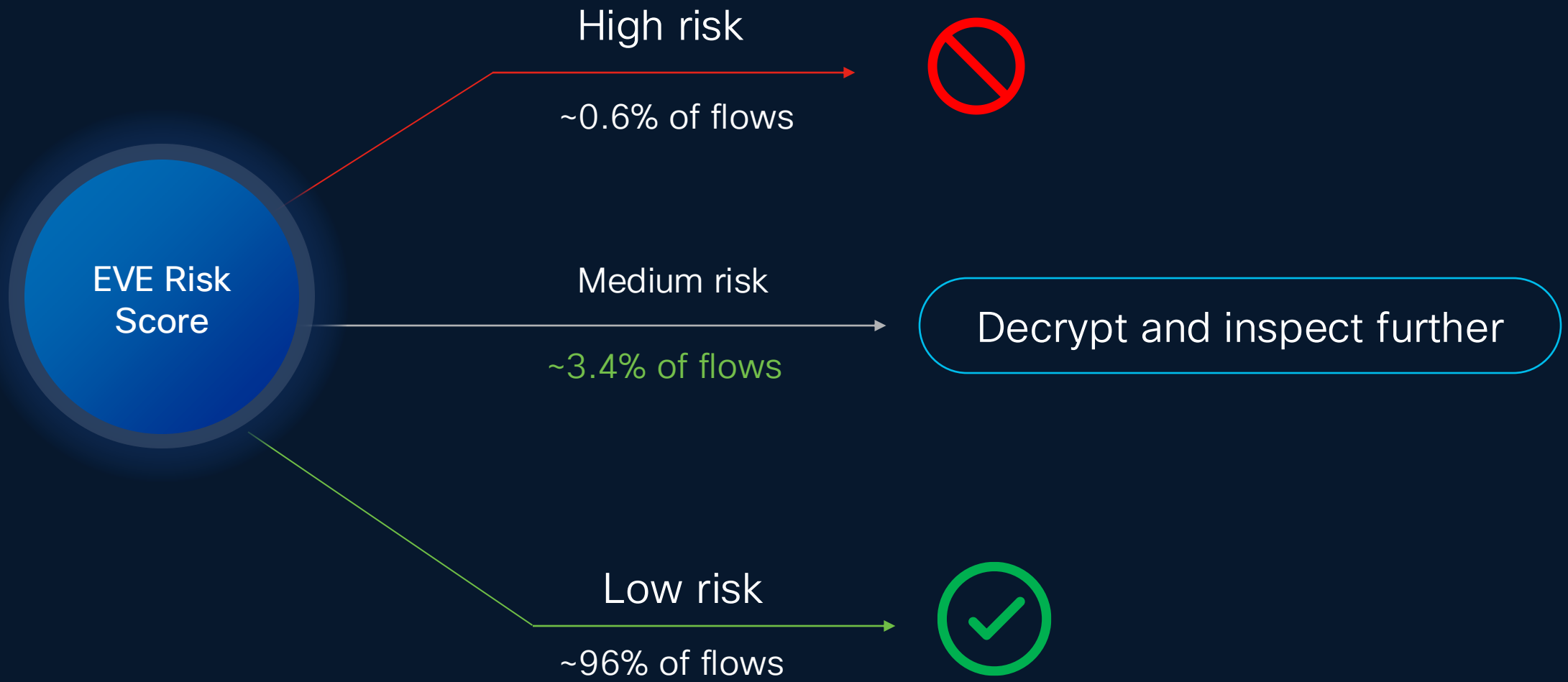
Machine learning (ML) technology

Processes 1 B+ TLS fingerprints

Processes 10 K+ malware samples daily

Cisco Encrypted Visibility Engine (EVE)
Cisco Differentiator

Risk-based intelligent decryption, **powered** by Cisco Encrypted Visibility Engine



Demo:
NGFW Decryption EVE

Organization
acme-netsec
Home

Products
Firewall
Hypershield
Multicloud Defense

Platform services
Favorites
Security Devices
Shared Objects
Platform Management

Home

Set default homepage

Top Insights & Alerts

32 Active Insights

All Insights

High Traffic Caused by Elephant Flow

Data source:

AIOps has detected high traffic on the firewall caused by 1 flow, potentially leading to performance duress in Snort cores.

97d ago Details

RAVPN Forecast - Maximum Sessions Nearing Limit

Data source:

AIOps has forecasted that the number of RAVPN sessions will reach capacity in '9' days

176d ago Details

Best practices and recommendations

Data source: NGFWTG

AIOps has detected 5 needs review checks.

6d ago Details

Multicloud Defense

Multicloud Defense

Account Resources

93 VPCS/ VNets	208 Security Groups	124 Route Tables	289 Subnets
151 Instances	33 Load Balancers	0 Tags	33 Applications

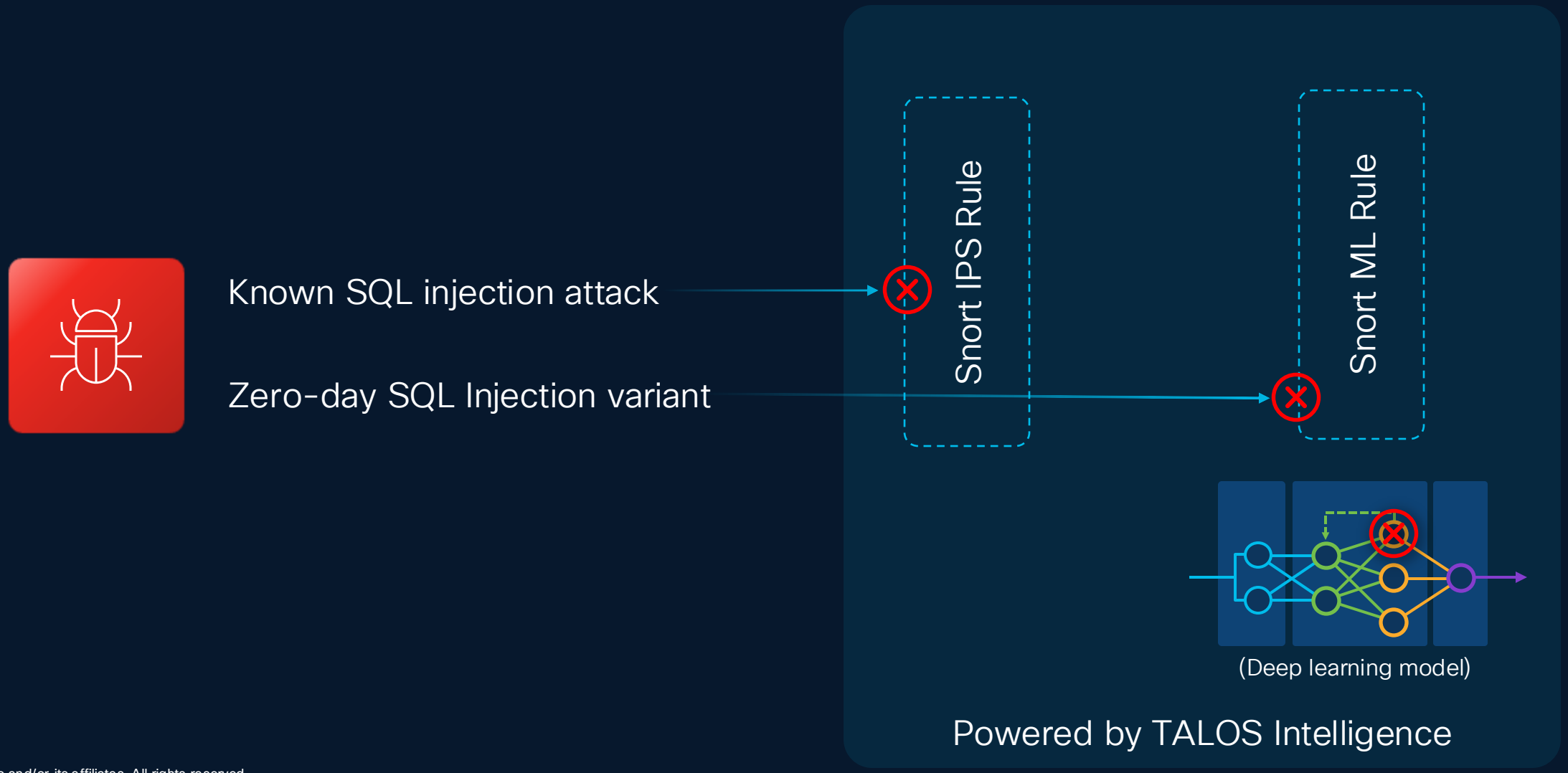
Security Considerations

33 Applications not protected	80 VPCs/VNets not protected	0 Service VPC/VNets without Gateways

Firewall Operator Care-Abouts: “I Need to Block 0-Day Threats!”

The Leading IDPS, Now with Zero-Day Protection

Snort ML extends IDPS protection to unknown variants of common attacks



Customer Use Cases

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

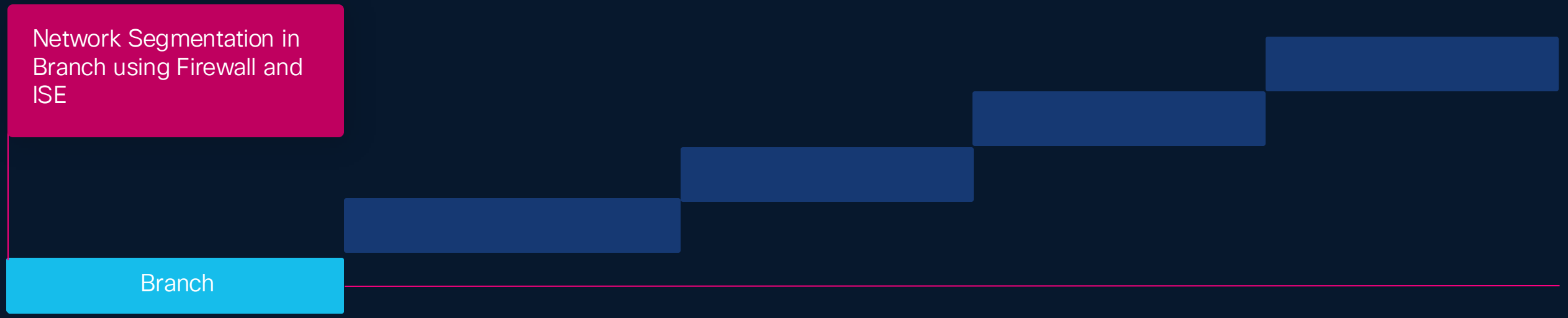
Macro & Micro Segmentation
Reduce risk by enforcing least-privilege access across networks and applications. Cisco strengthens this with AI-driven security that adapts to application behavior, ensuring protection without sacrificing agility.

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.

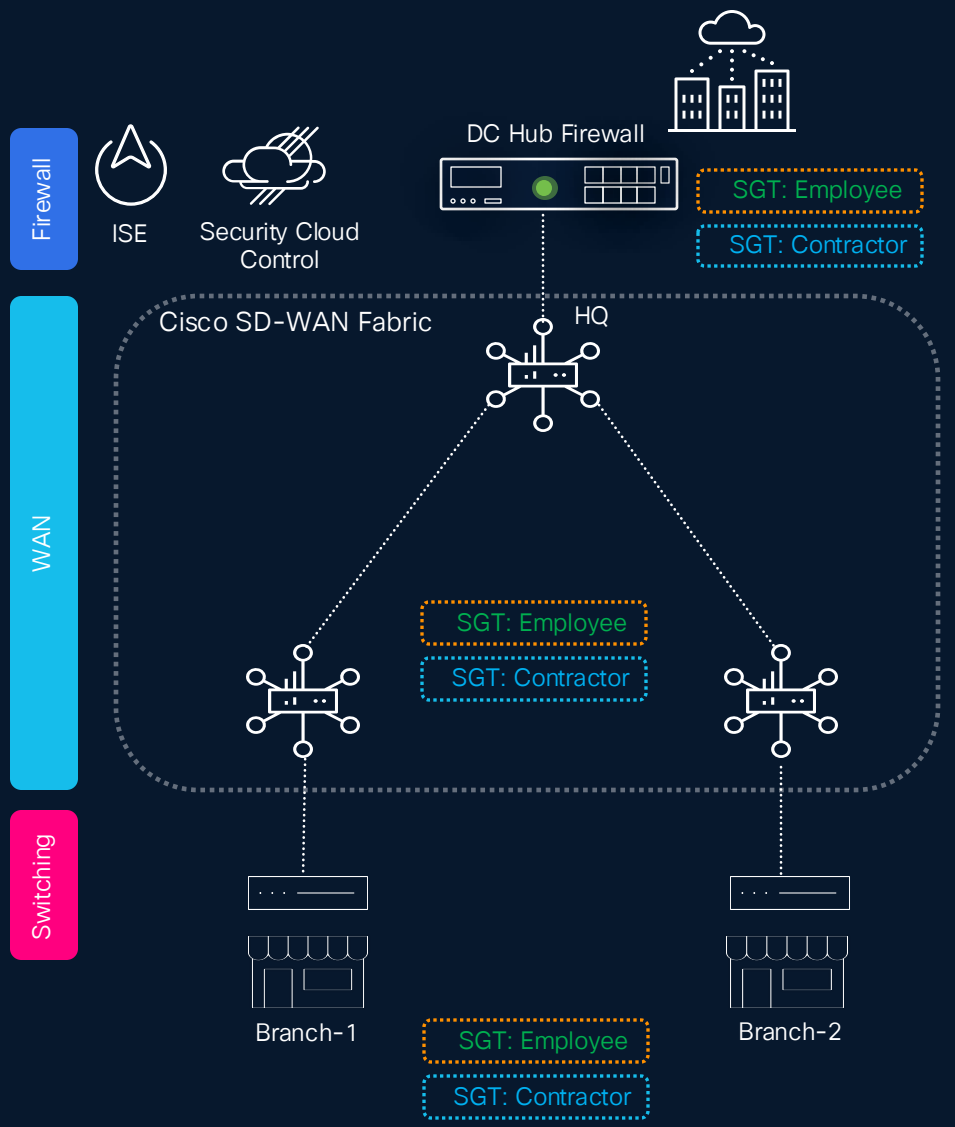
DC Edge - Perimeter Firewall
Safeguard north-south traffic by blocking external threats, securing critical DC workloads, enforcing least-privilege access, supporting compliance, and ensuring uninterrupted business operations.

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.

End-to-End Segmentation



Branch Segmentation Architecture



Customer Problems

Protect data and applications from attacks by
Stopping Lateral Movement
Enforcing Least-Privilege access and
Regulatory compliance

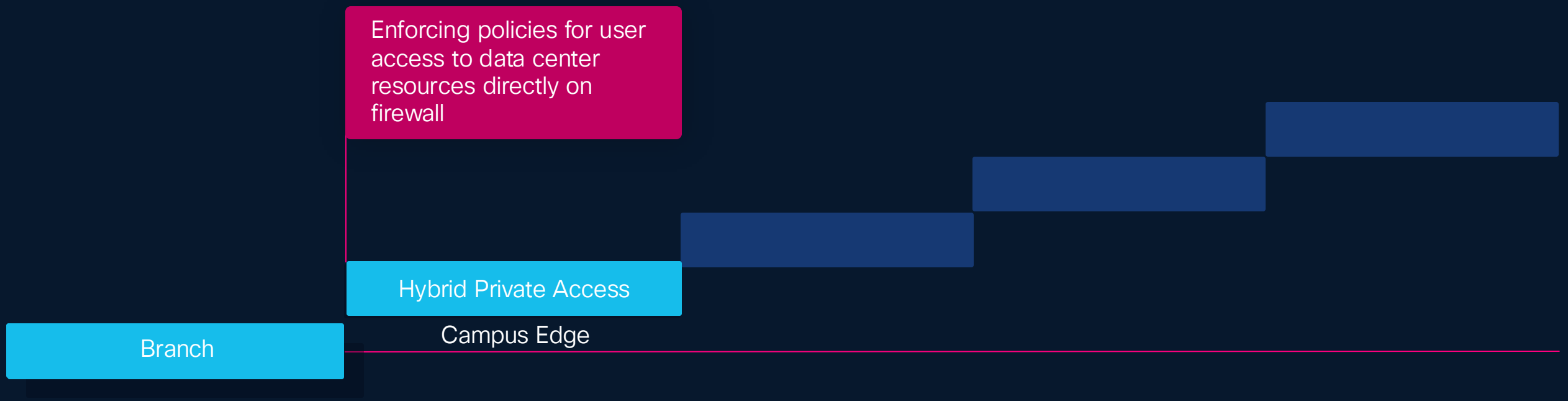
Cisco Solutions

Security Cloud Control
Secure Firewall
Identity Services Engine (ISE)
Catalyst Routers and Switches
SD WAN

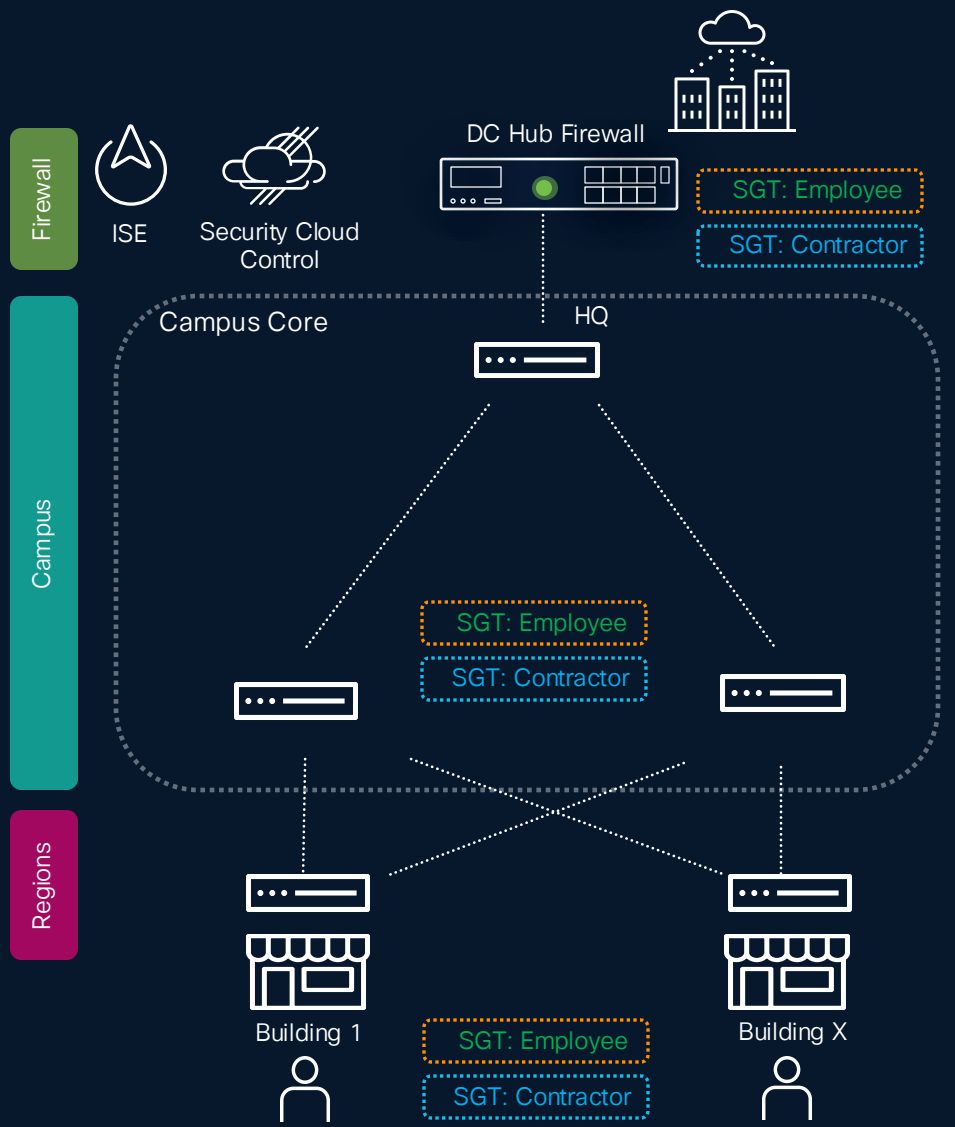
Customer Outcomes

Stronger security posture
Faster incident response and containment
Simplified security operations and improved compliance

End-to-End Segmentation



Campus Segmentation Architecture



Customer Problems

Protect data and applications from attacks by
Stopping Lateral Movement
Enforcing Least-Privilege access and
Regulatory compliance

Cisco Solutions

Security Cloud Control
Secure Firewall
Identity Services Engine (ISE)
Catalyst Routers and Switches

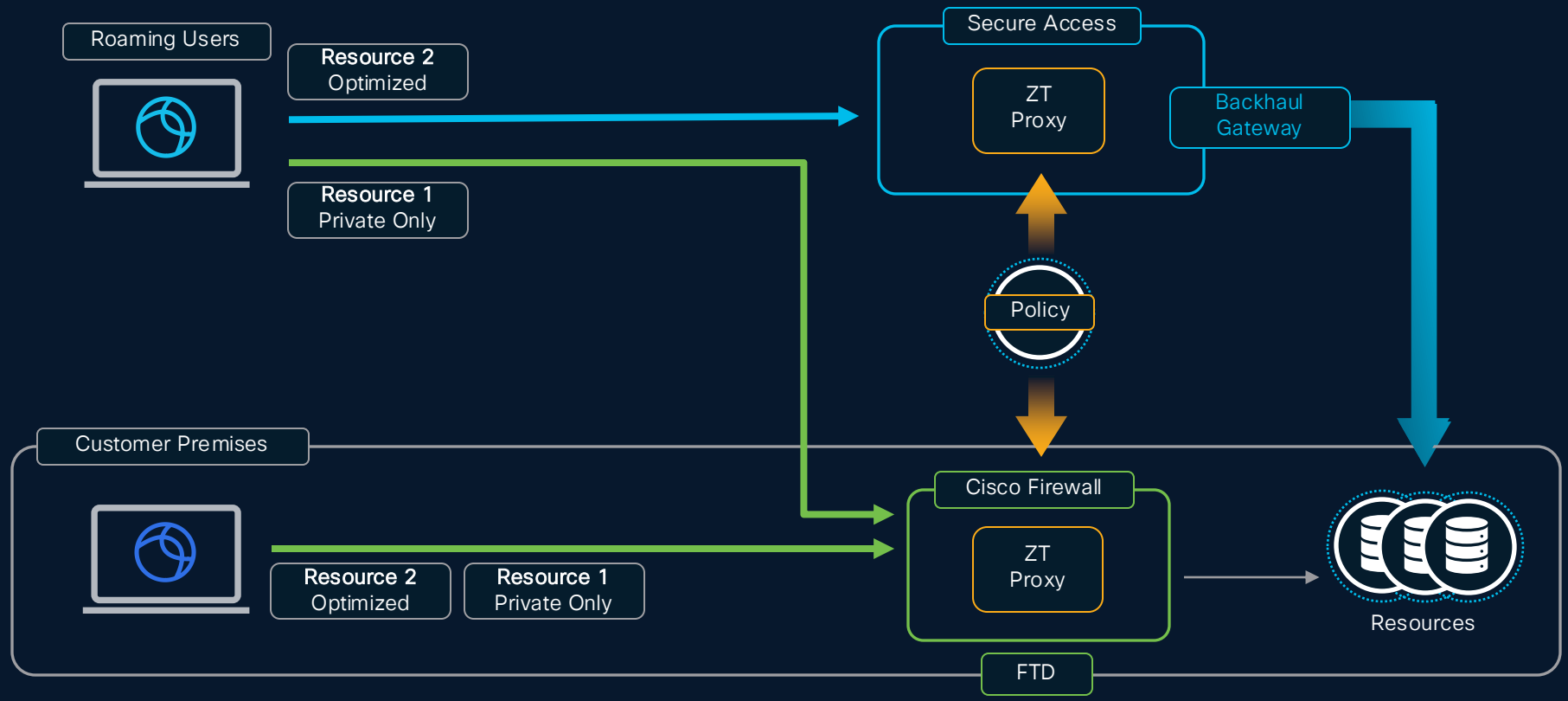
Customer Outcomes

Stronger security posture
Faster incident response and containment
Simplified security operations and improved compliance

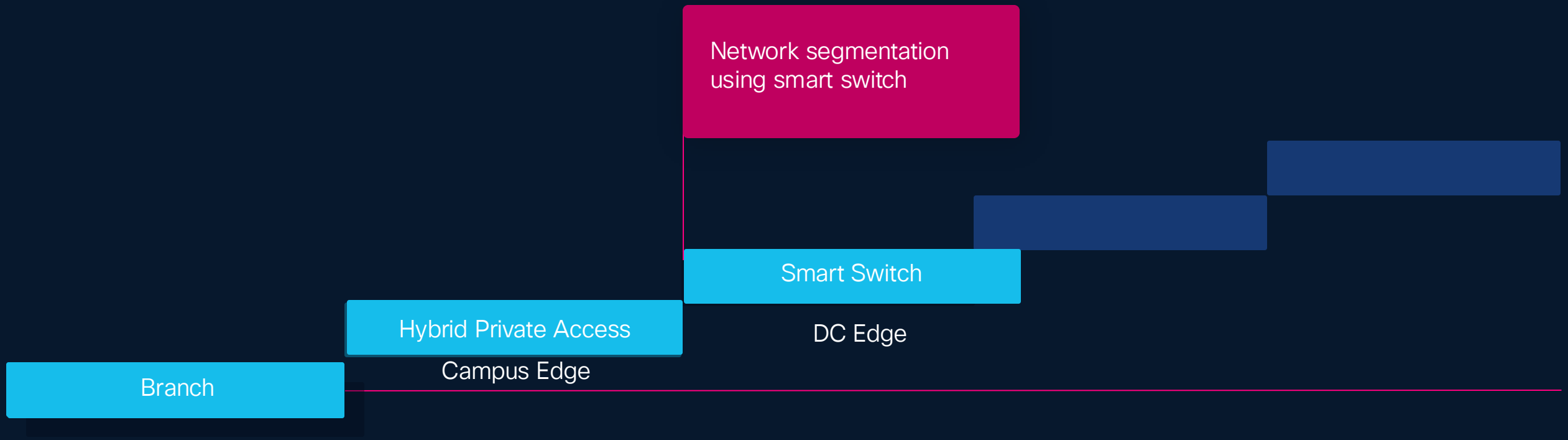
Hybrid Private Access

- Single Policy, Distributed Enforcement

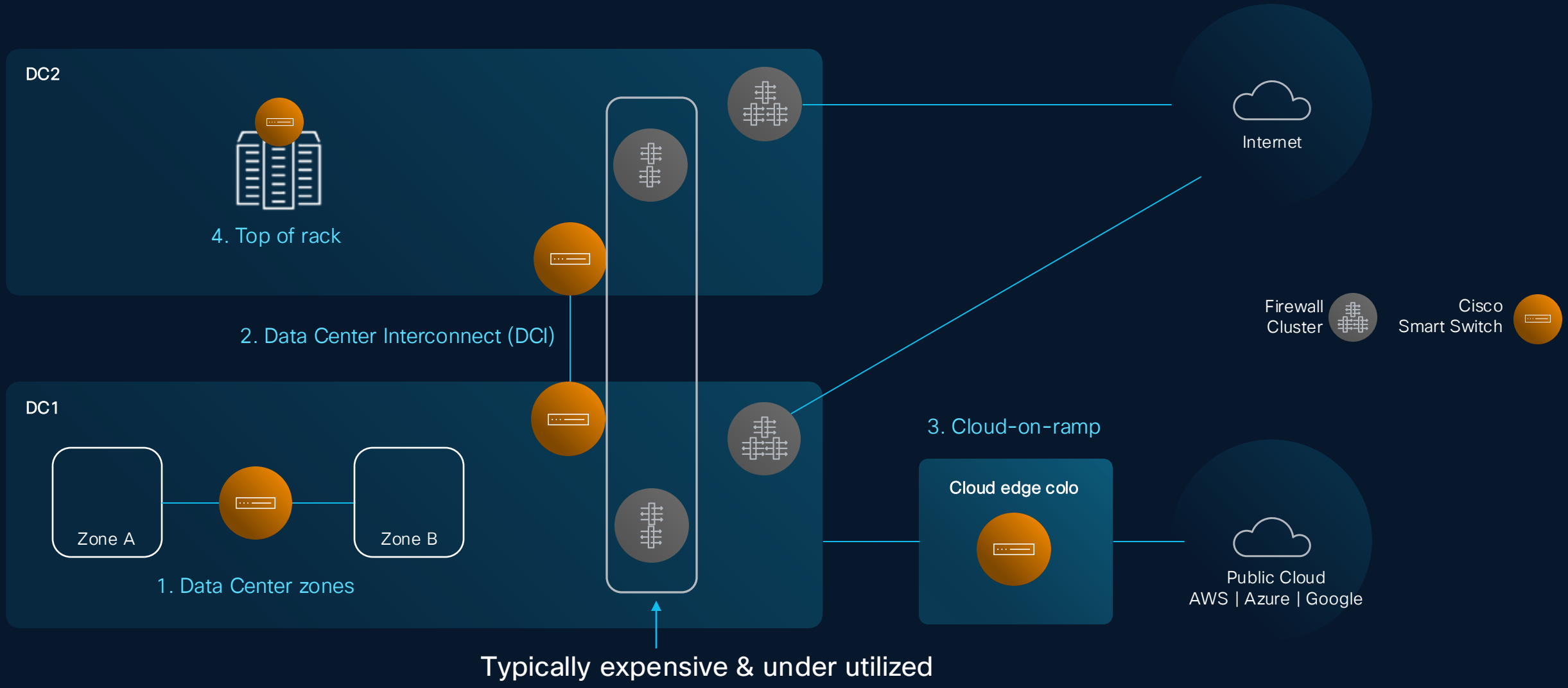
- Same experience in office and remote
- Resilient with Failover to on-prem firewall
- No sensitive traffic through cloud access



End-to-End Segmentation



Security Use Cases with Cisco Smart Switches



Cisco Smart Switches Integrated with Hypershield Security

Ultra Ethernet Consortium

Cisco N9300 Series Smart Switches

Shipping

N9324C-SE1U

24-port 100G

800G Services Throughput

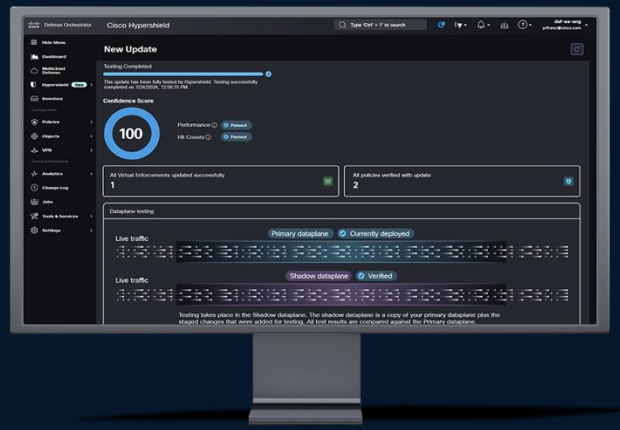
Orderable

N9348Y2C6D-SE1U

48-port 1G/10G/25G, 6-port 400G, 2-port 100G

800G Services Throughput

Cisco Hypershield



Use Cases

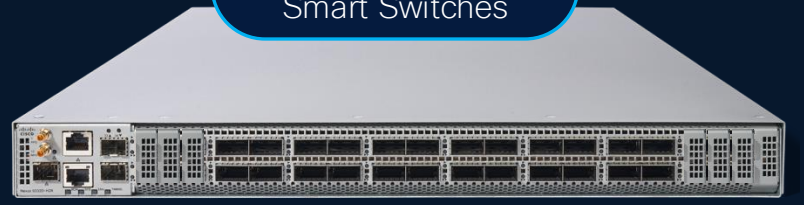
- Top of Rack segmentation and enforcement
- Cloud Edge
- Zone-based segmentation

cisco

Nexus Smart Switch

Unmatched Flexibility, Performance, and Efficiency

Cisco
Smart Switches



Cisco Nexus 9300 Services Accelerated Switch

Networking

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

Hypershield

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

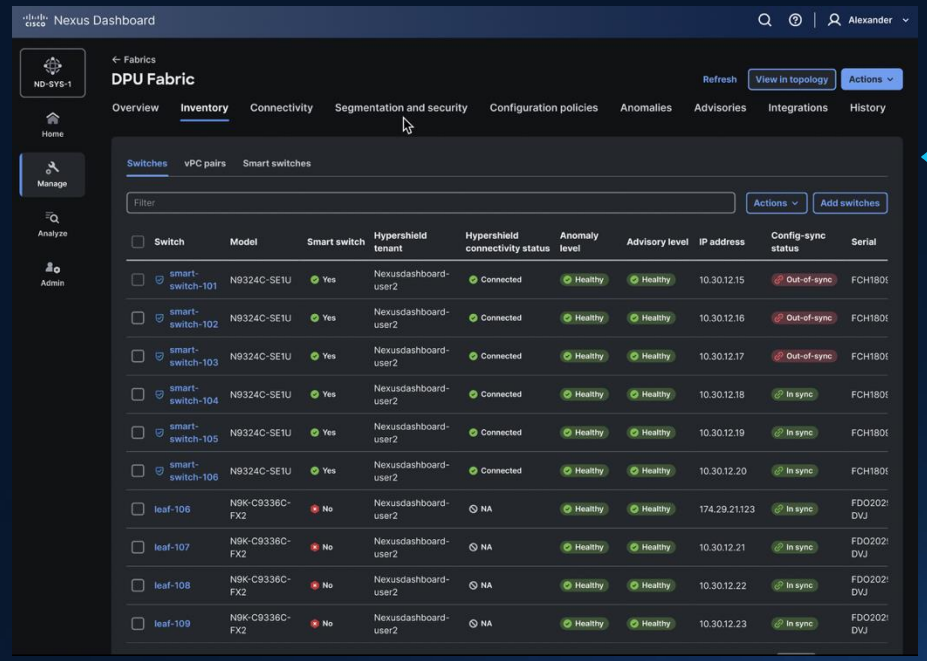
Distributed Security

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

Future Use Cases

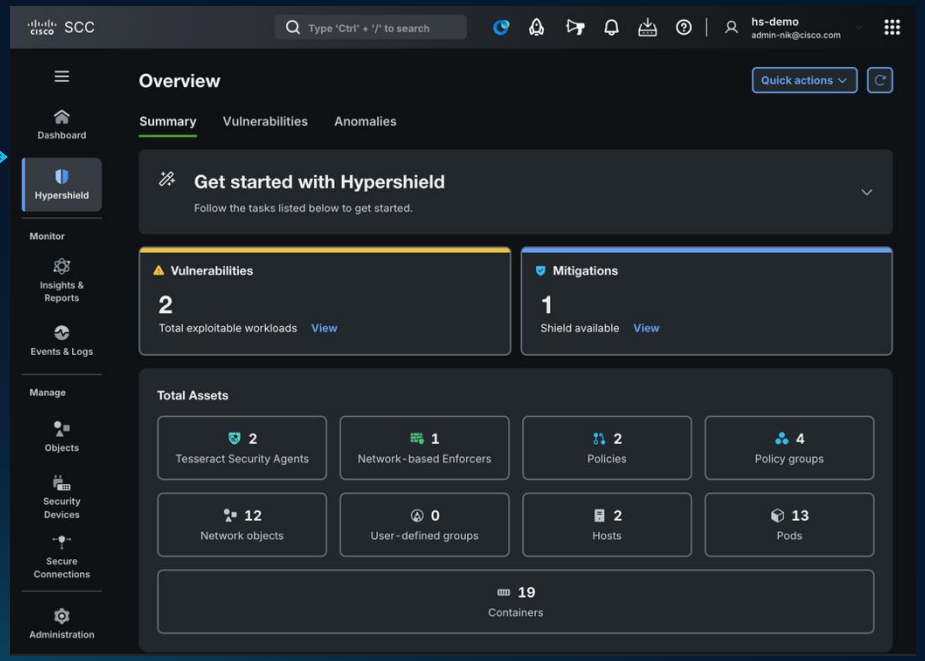
Separate Workflows for NetOps and SecOps

Nexus Dashboard



Context sharing for troubleshooting

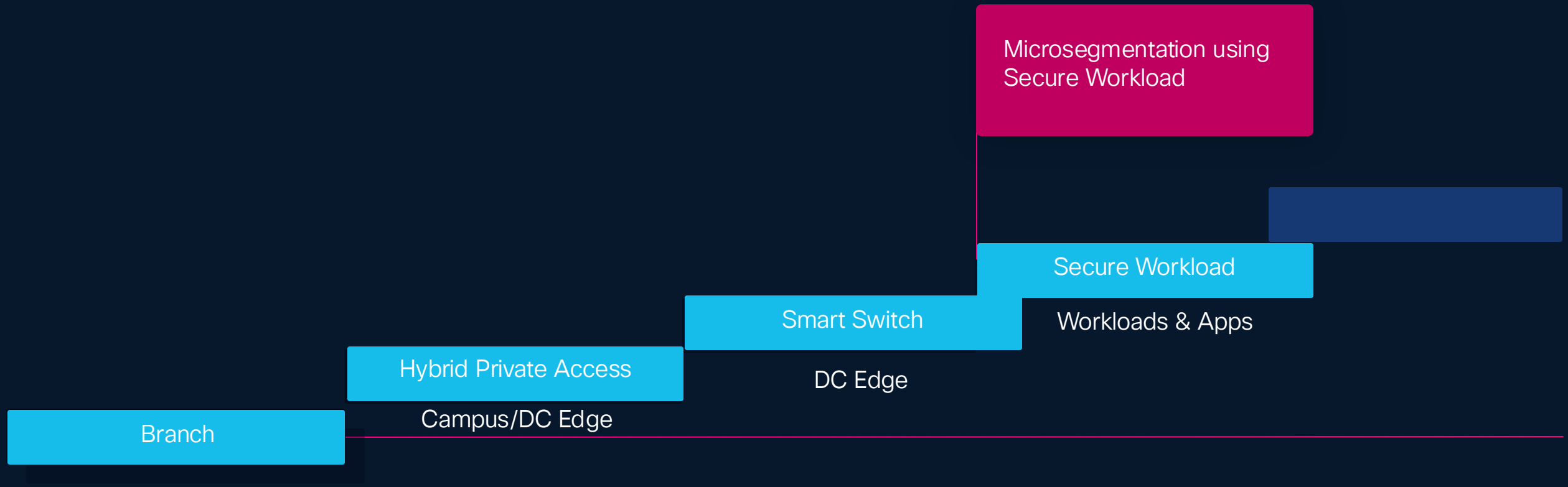
Security Cloud Control



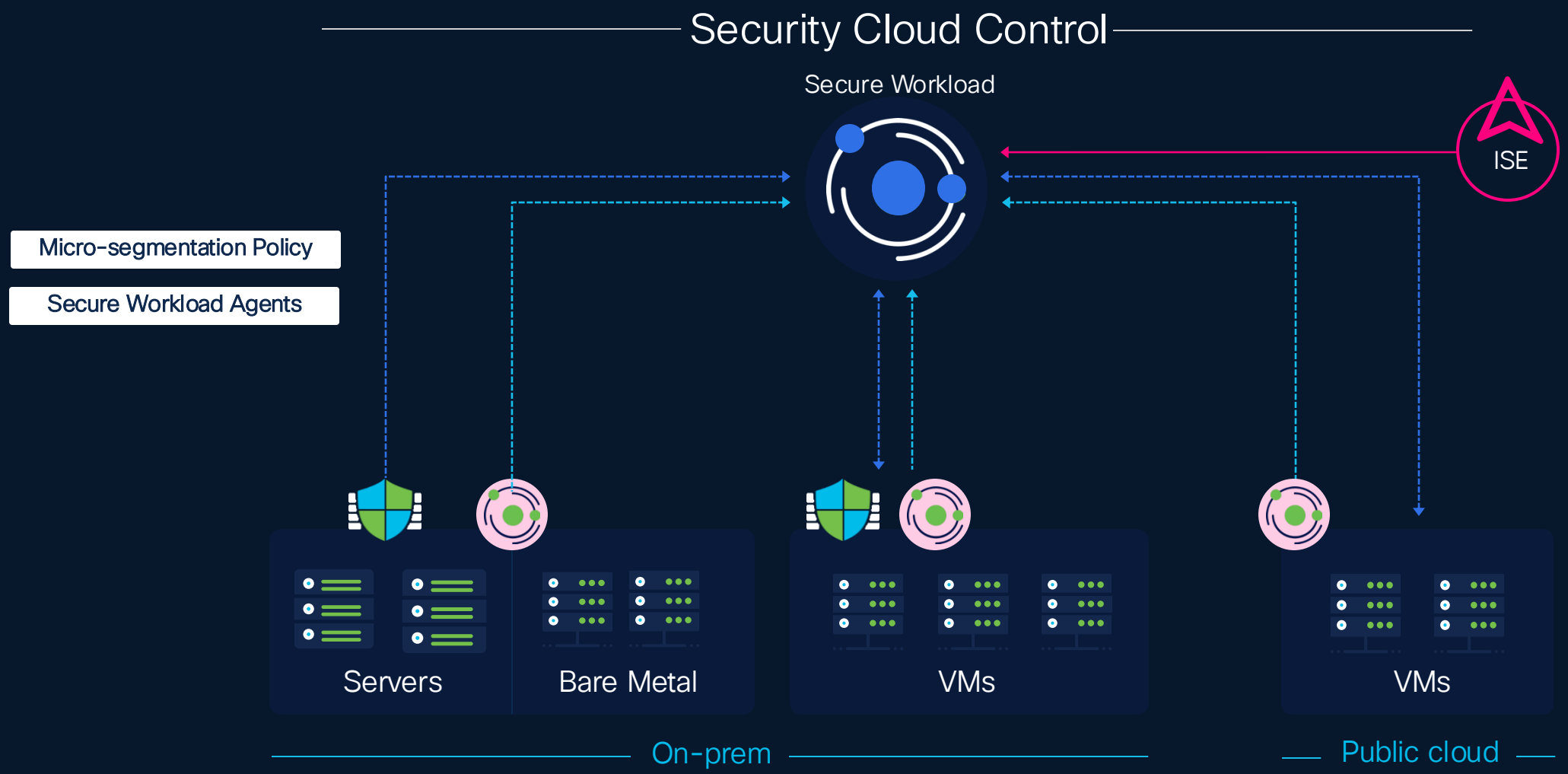
Smart Switch

Demo:
Smart Switch Segmentation

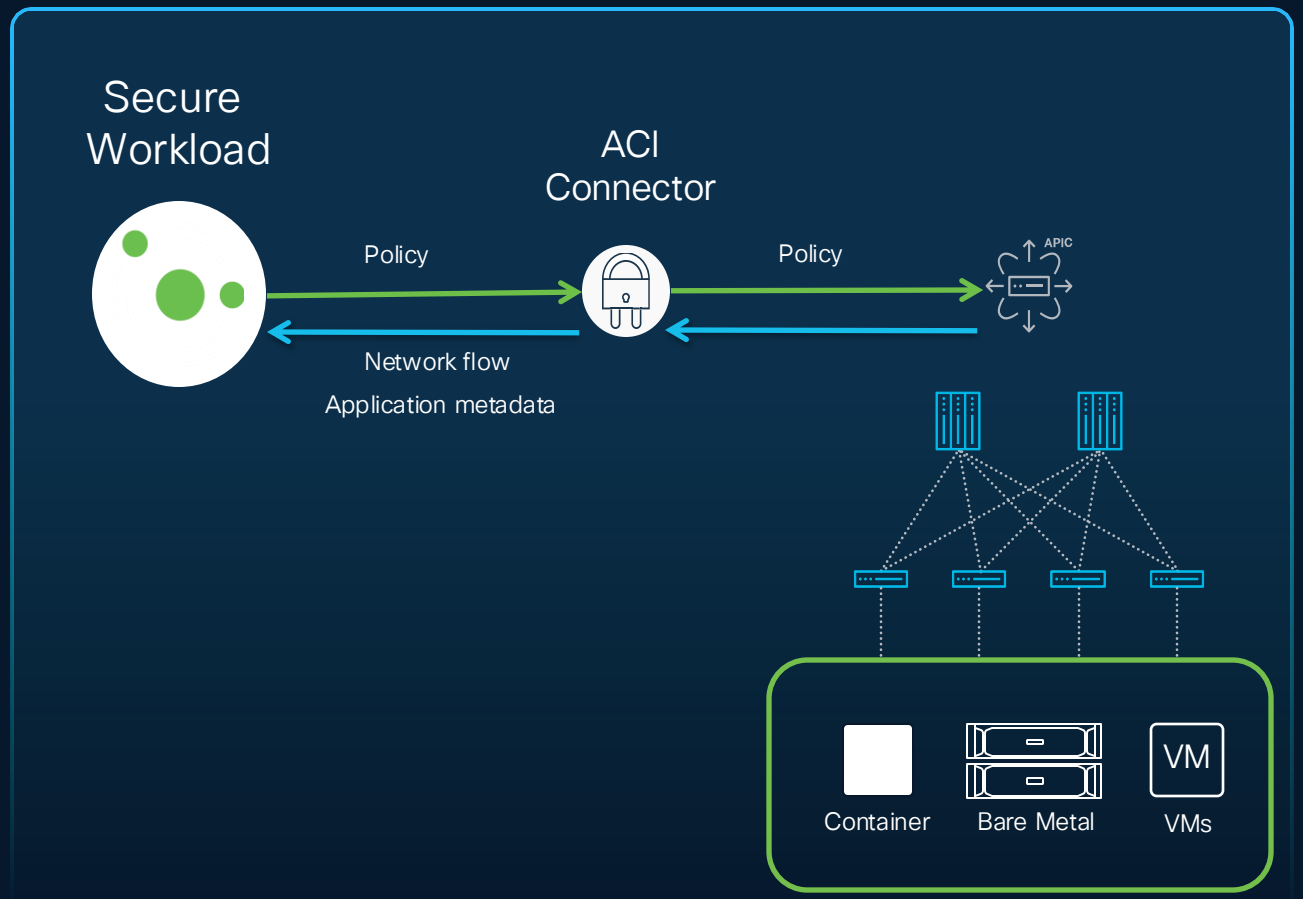
End-to-End segmentation



Micro-segmentation with Secure Workload

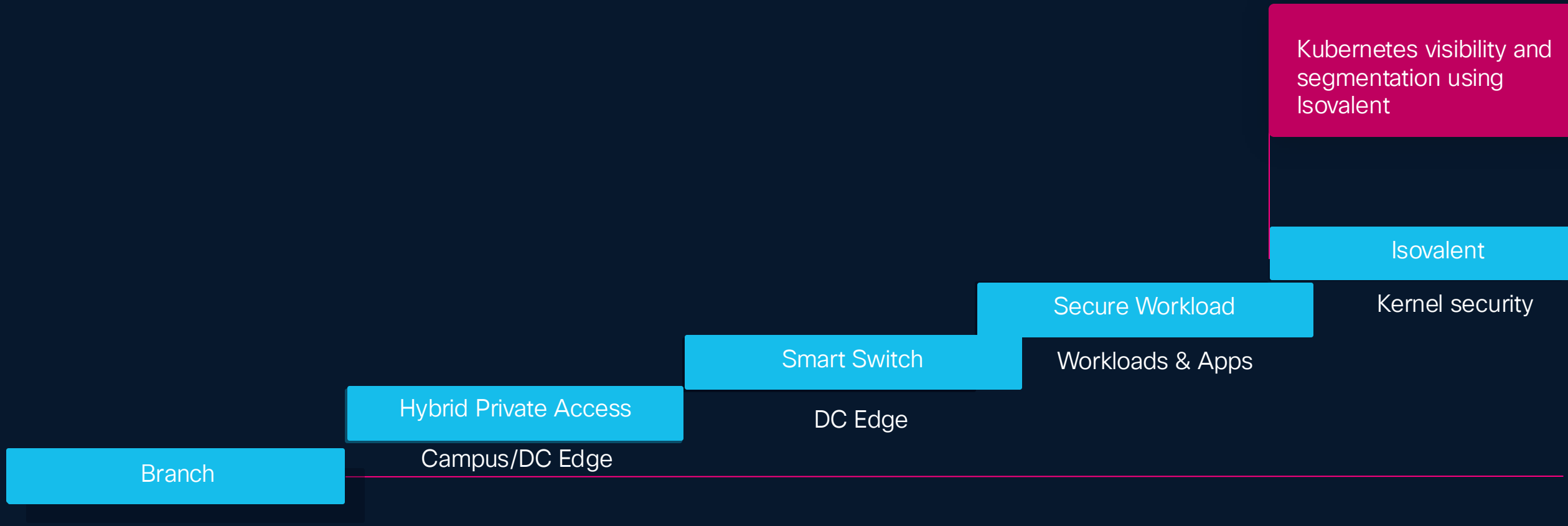


Automate Segmentation Policies for Cisco ACI



- Deep visibility with AI/ML into application dependencies
- Achieve application centric deployment of security
- Automate policy lifecycle management
- Zero friction to adoption
- Agentless policy enforcement for segmentation

End-to-End Segmentation



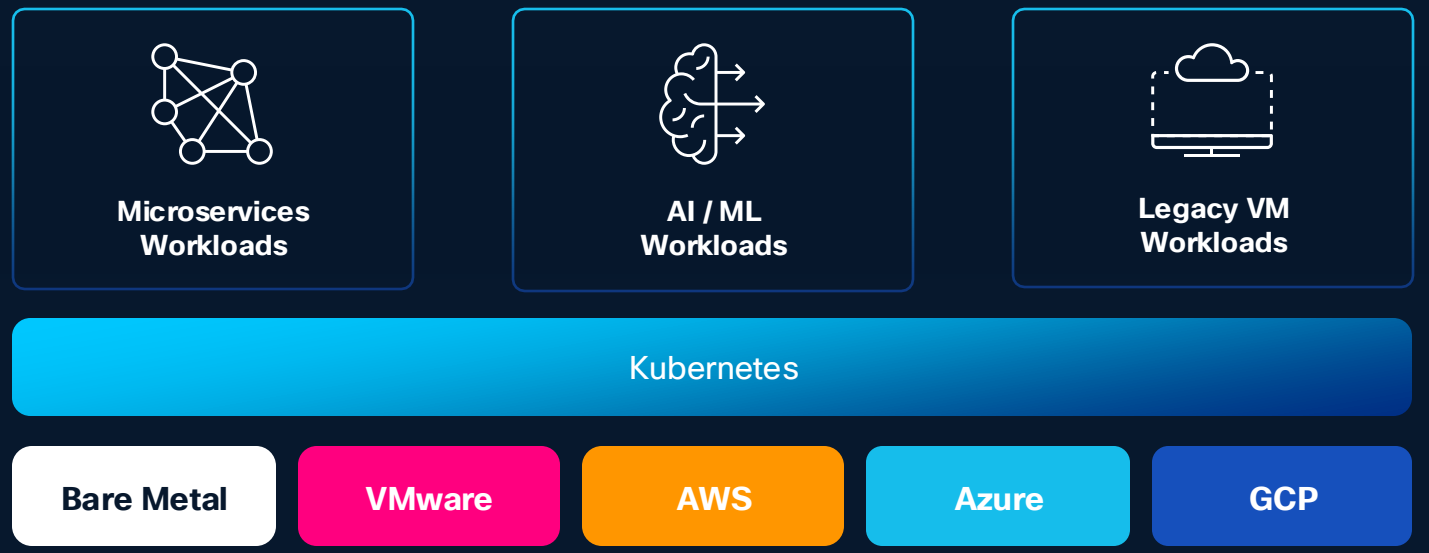
Kubernetes Challenges Traditional Networking and Security Approaches

Challenges

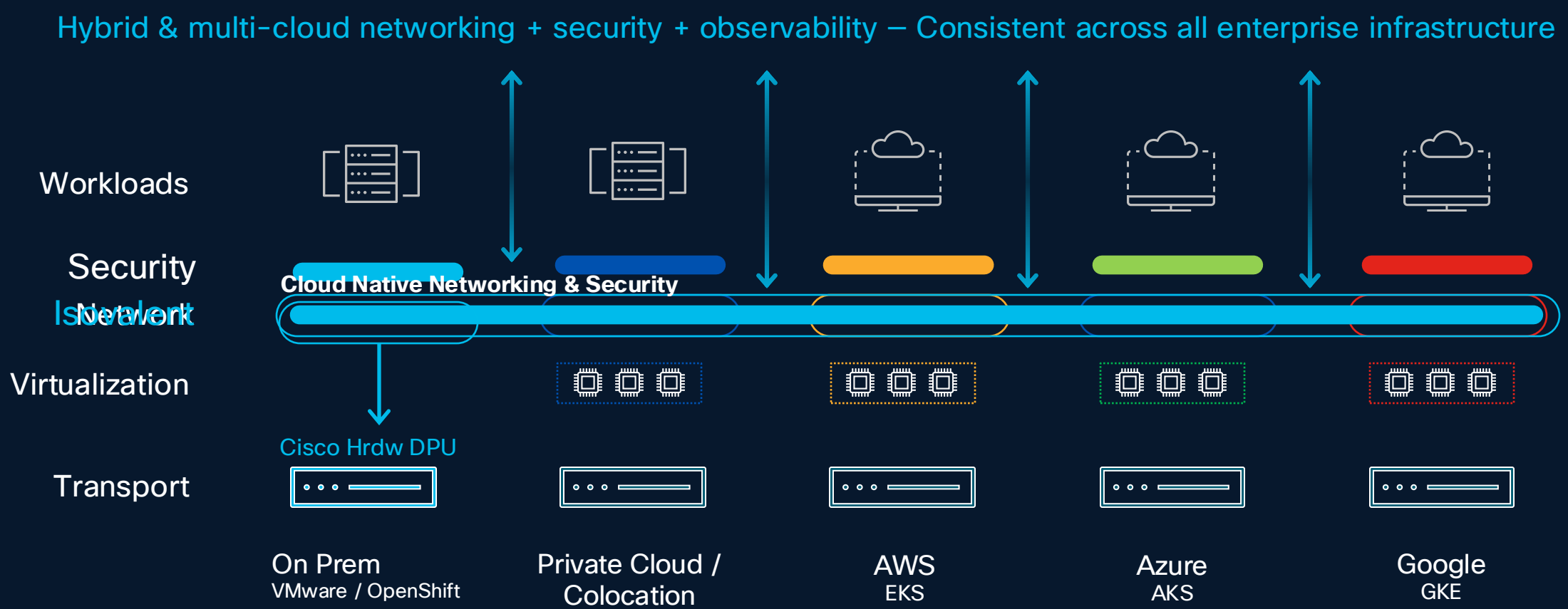
- Nothing is fixed (IPs, hosts, workloads)
- Existing tooling doesn't work
  (firewalls, IP tooling, load balancers, observability)
- Reliability and Observability is a challenge

"My Kubernetes cluster is a black box, but this is where the apps are being built..."

– NetSec lead (financial customer)



Isovalent brings network tooling to Kubernetes



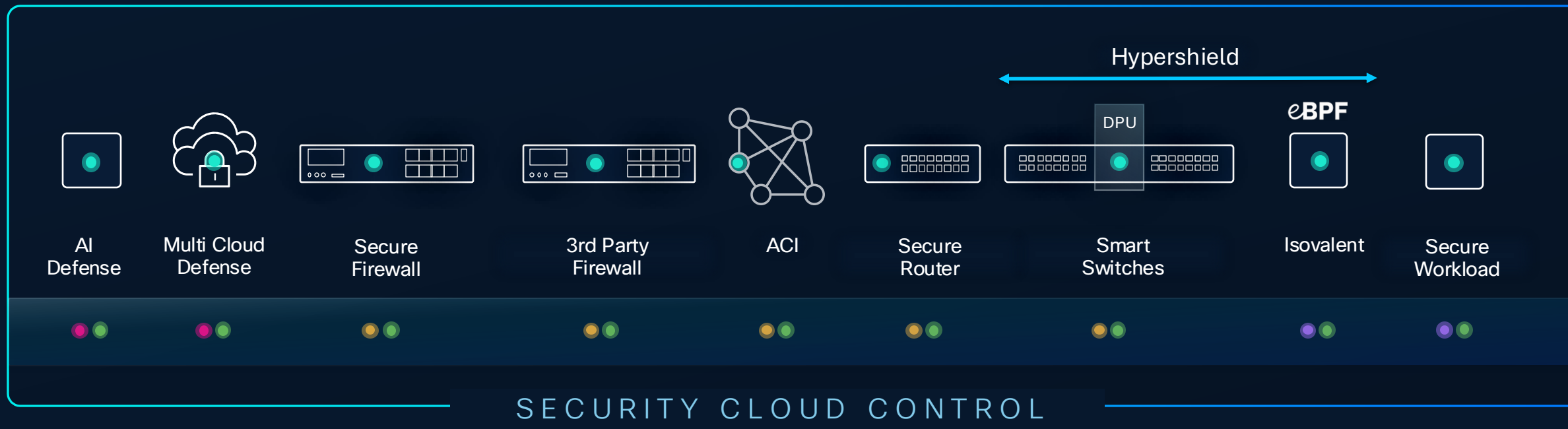
Demo:
Visibility into Kubernetes Clusters

Hybrid Mesh Firewall:
The customer value proposition

Cisco Hybrid Mesh Firewall

CUSTOMER SECURITY OUTCOMES

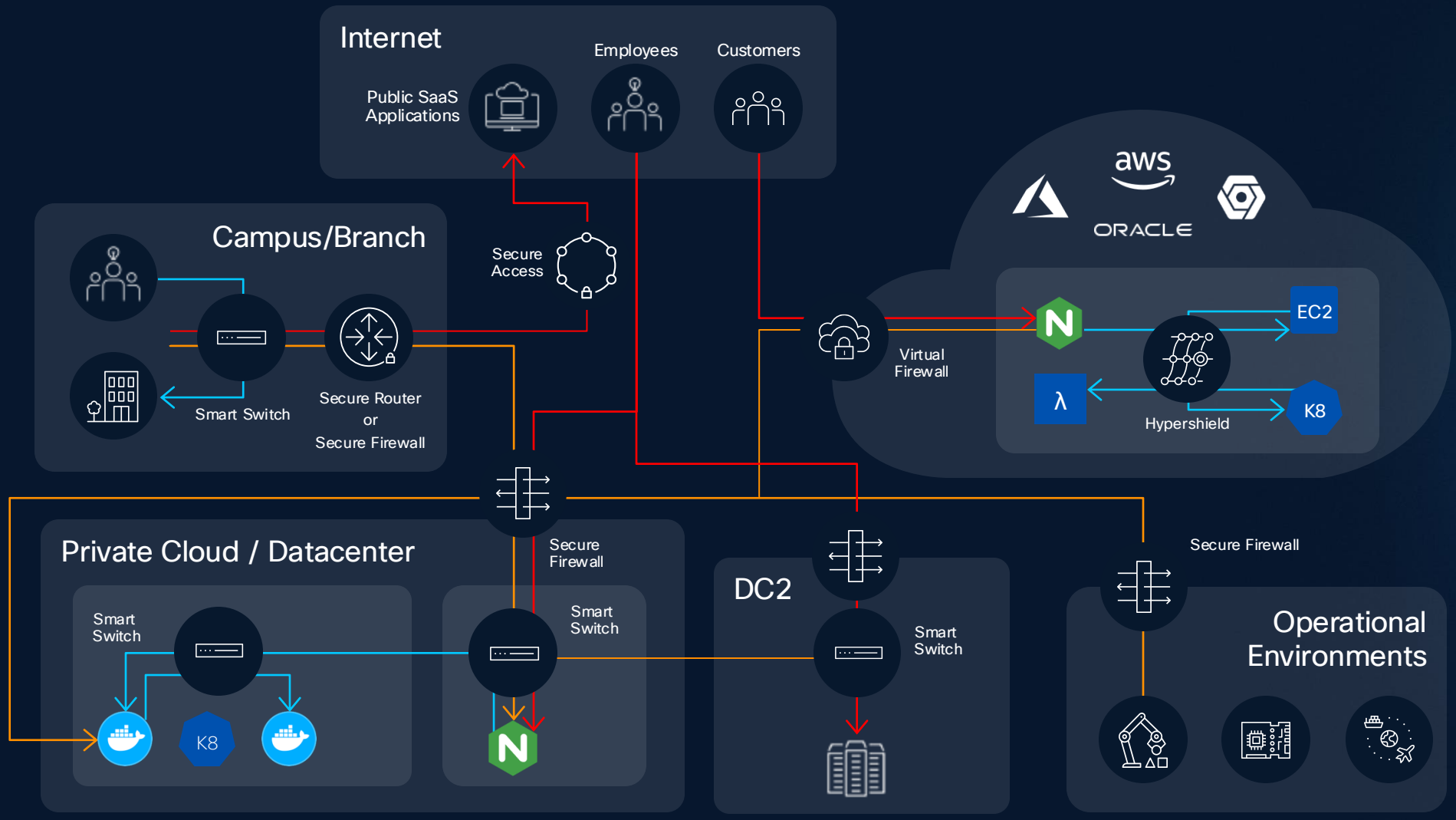
Network Segmentation | Macro & Micro Segmentation | Threat Detection & Exploit Protection | AI Security



SECURITY CLOUD CONTROL

Write policy once, enforce across the mesh

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

cisco

Thank you


CISCO