End-to-End Micro-Segmentation & Agent Security Part 2:

Extending Zero Trust into the Data Center

Chase Abrams

Jacob Schneider

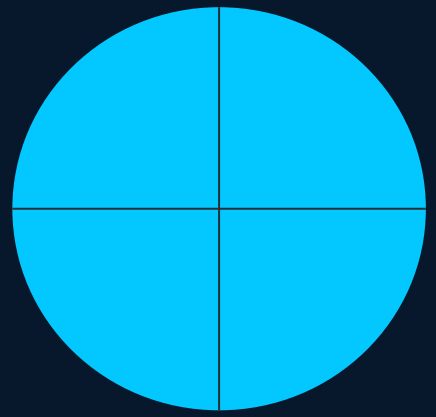
October 15, 2025

Part 1 - Recap

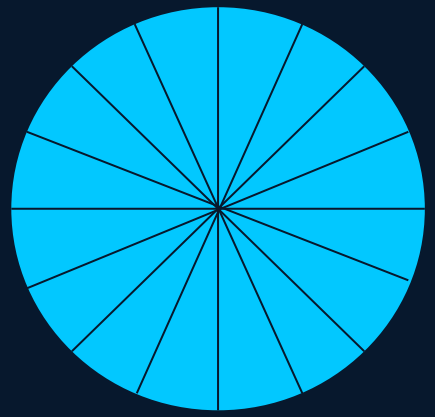
What is Segmentation?

“ Segmentation is the practice of dividing a larger system into smaller, isolated parts to improve control, security, and performance.” - CIRCUIT (a.k.a BridgeIT).

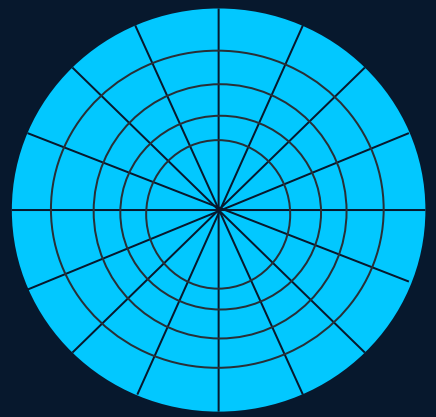
No Segmentation



Macro Segmentation

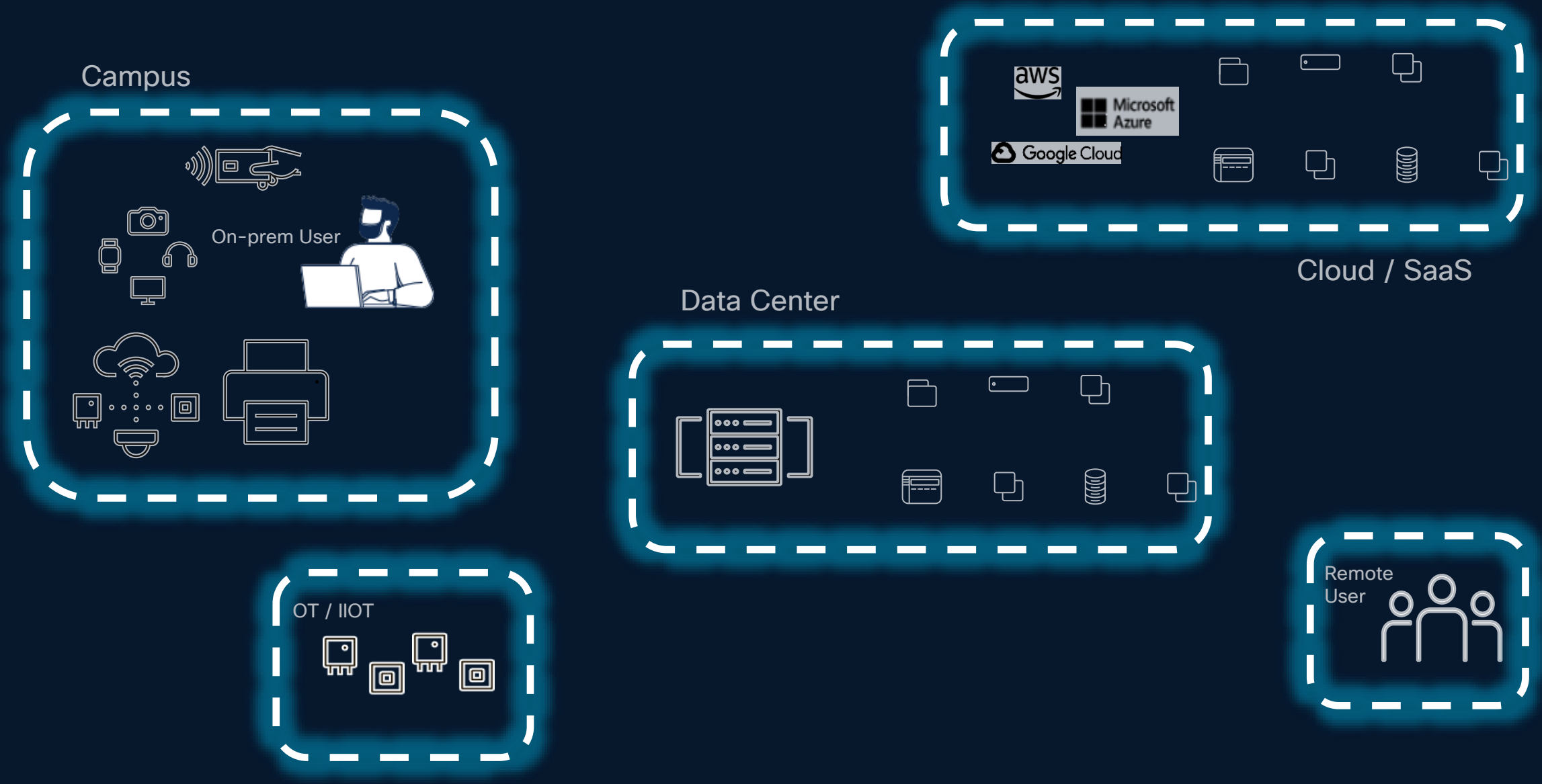


Micro Segmentation



Nano Segmentation??

Segmentation Domains



Segmentation is a solution, but it is complex.

Cisco is dedicated to solving customers' needs

People, process and technology

Scale, speed and granularity

Customers need flexibility and choice to address unique scenarios

Why it matters to our customers

- App modernization and multicloud adoption
- Ransomware threat – contain lateral movement
- Meet compliance requirement
- Automation at scale
- Visibility

Cisco innovations

1998	2008	2014	2016	2022	2023	2024
VRF, PVLAN	Cisco TrustSec (SGT)	Cisco ACI and VXLAN – EVPN	Cisco Secure Workload (Tetration)	Cisco Multicloud Defense (Valtix)	Cisco Secure Access	Cisco HyperShield

Cisco intent-based access in the Campus

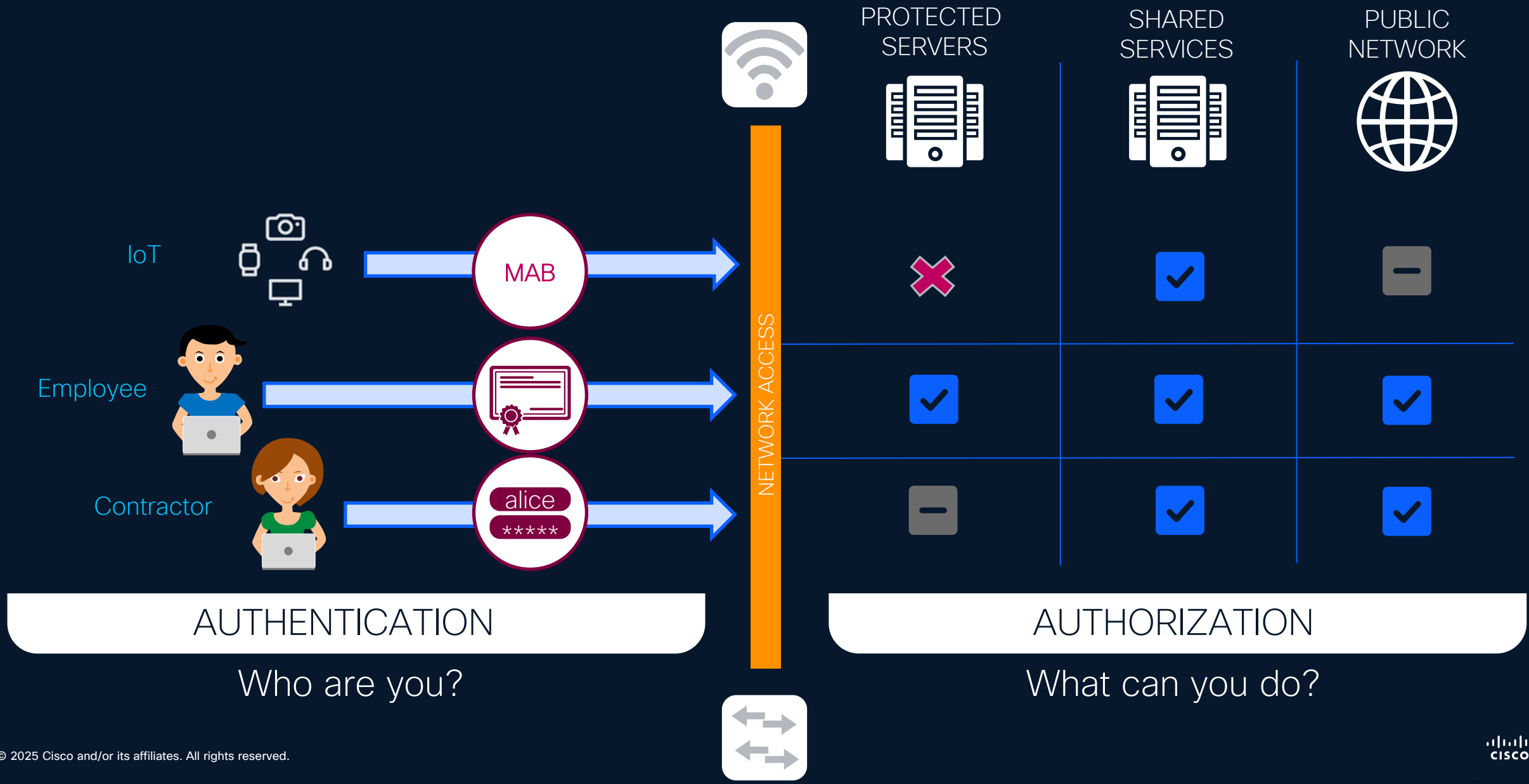
Cisco's campus intent-based access that lets you:

See
Users, endpoints and applications

Secure
By controlling network access and segmentation

Share
Context with partners for enhanced operations

Authentication and Authorization



Why Customers Buy ISE

Device Administration	TACACS+ Allows for secure, identity-based access to the network devices	https://cs.co/ise-tacacs
Secure Access	Secure wired, wireless, or VPN access using industry standard protocols RADIUS and 802.1X	https://cs.co/ise-wired
Guest Access	Choose from Hotspot, Self-Registered Guest, and Sponsored Guest access options	https://cs.co/ise-guest
Asset Visibility	Use the probes in ISE and Cisco devices to classify endpoints and authorize them	https://cs.co/ise-profiling
Compliance & Posture	Use agentless posture, Cisco Secure Client, MDM, or EMM to check endpoints' posture	https://cs.co/ise-posture
Context Exchange	Integrate applications and vendors with ISE for endpoint identity, context, and automated Enforcement	https://cs.co/ise-pxgrid
Segmentation	Group-based Policy with Security Group Tags (SGT) and Security Group ACLs (SGACL) instead of VLAN/ACLs	https://cs.co/segmentation-resources
Cisco Catalyst Center	ISE integrates with Catalyst Center to automate the network fabric and policies using SDA	https://cs.co/ise-ccc
EMM/MDM	Endpoint Management is required for provisioning endpoints with certificates and controls for secure network access	https://cs.co/ise-mdm
Threat Containment	Use Threat Analysis tools to grade an endpoint's threat score and automatically quarantine it if	https://cs.co/ise-tcnac

Segmentation Beyond the Campus

Zero Trust Realized

Cisco's Zero Trust Platform

Security Cloud Control

Securing Users (Universal ZTNA)

Securing Apps (Hybrid Mesh Firewall)

Access Control

AI Access

North South Segmentation

AI Model Protection

East West Macro/ Microsegmentation

Distributed Exploit Protection

One Integrated Architecture

Cisco TALOS, Cisco XDR & Splunk

End-to-end protections

North-South

Secure Firewall

East-West

Secure Firewall
Secure Workload

Microsegmentation

Hypershield
Secure Workload

Perimeter Protection

Threat inspection at the data center or cloud edge

Visibility into internet, branch, and campus

Zones

Segment zones within your data center and cloud

Supplementary coverage for workloads with or without agents

Zero Trust

Zero trust micro-segmentation enforcement at the workload

Automated policy discovery and compliance

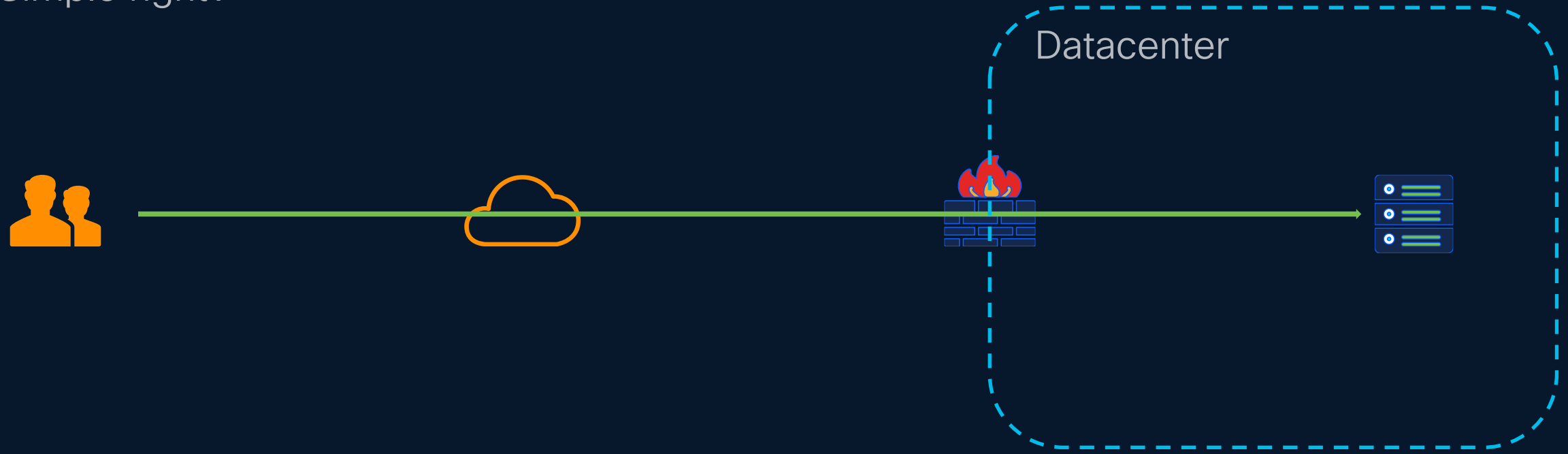
Closer to application

Application Microsegmentation

Securing Application Workloads – Threat Landscape

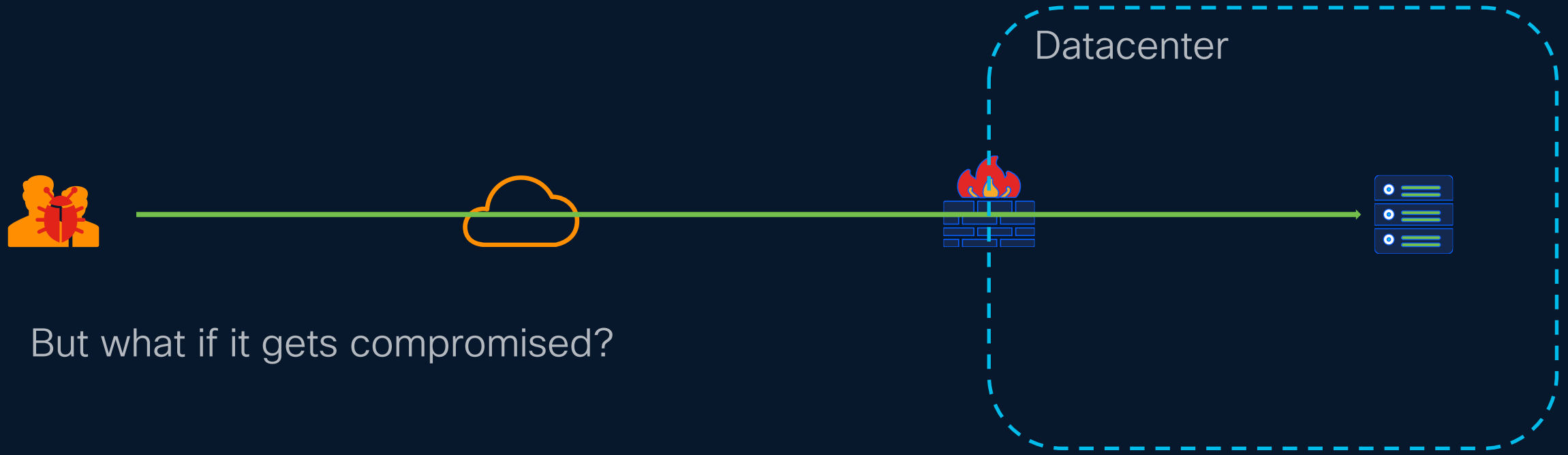
Using Network Security Controls

Simple right?



Securing Application Workloads – Threat Landscape

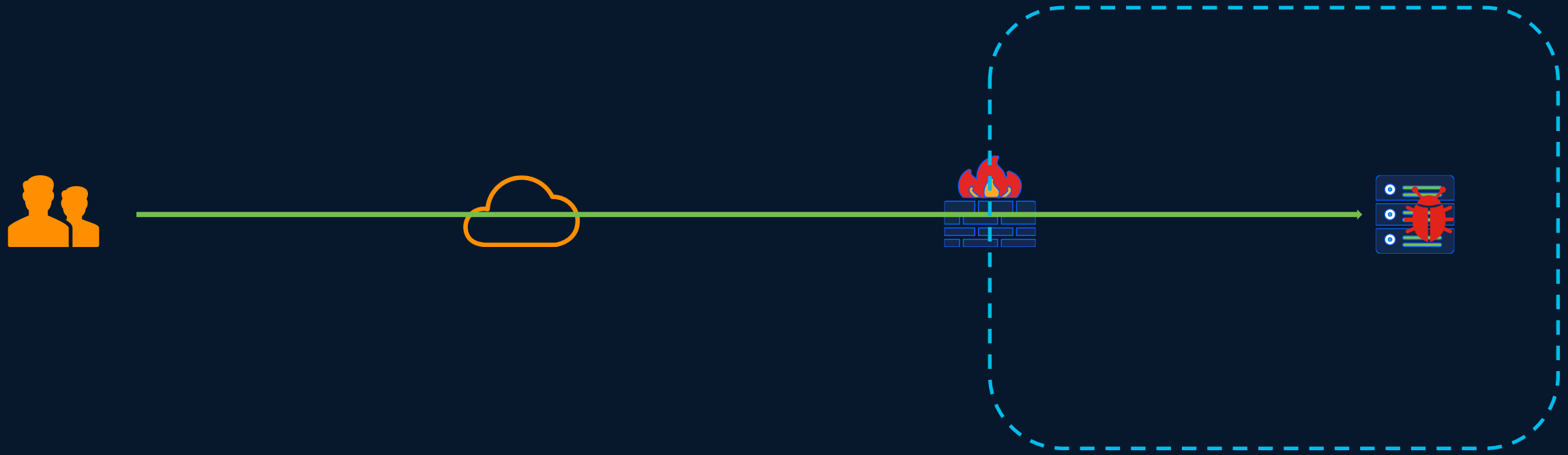
Using Network Security Controls



But what if it gets compromised?

Securing Application Workloads – Threat Landscape

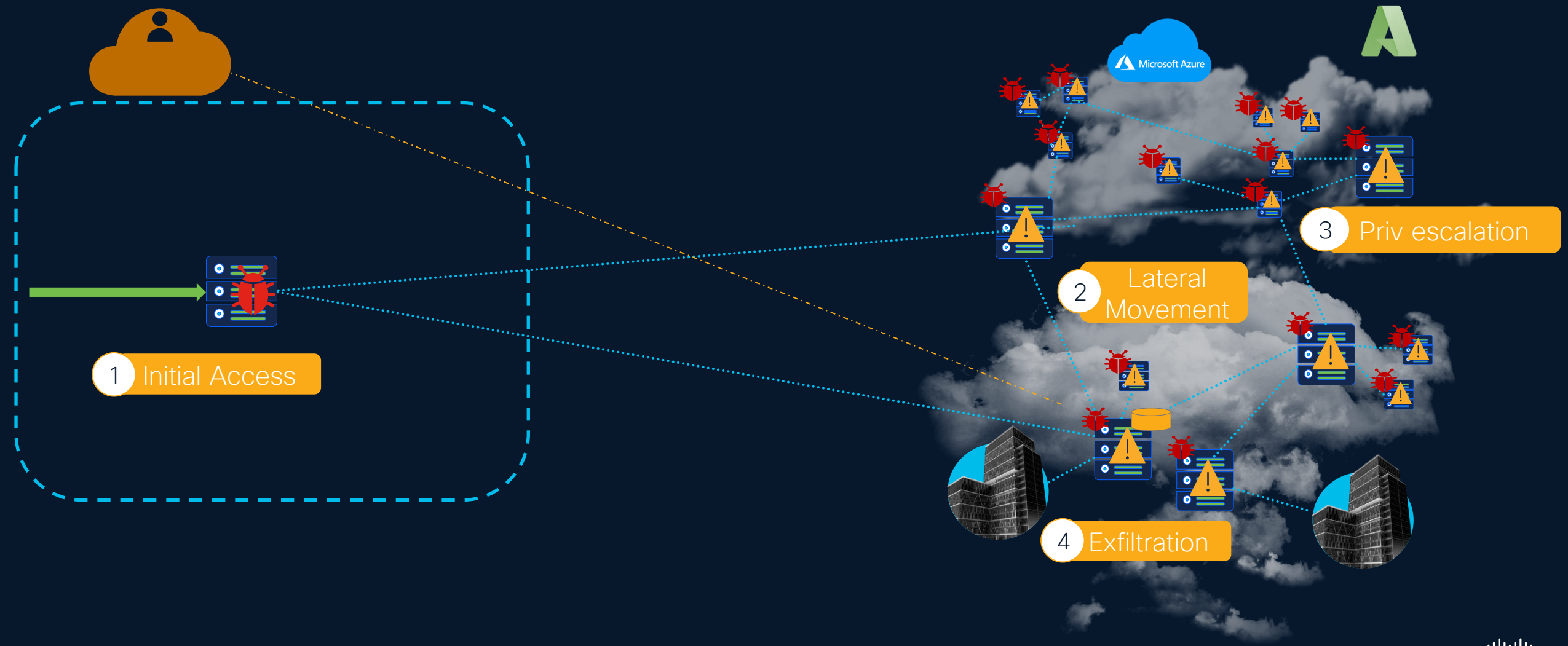
Using Network Security Controls



And this is only a part of the story.....

Securing Application Workloads – Threat Landscape

Using Network Security Controls



Application Workload Evolution

Workload Security is Getting More Complex!

Virtual Machine

Maturing of containers

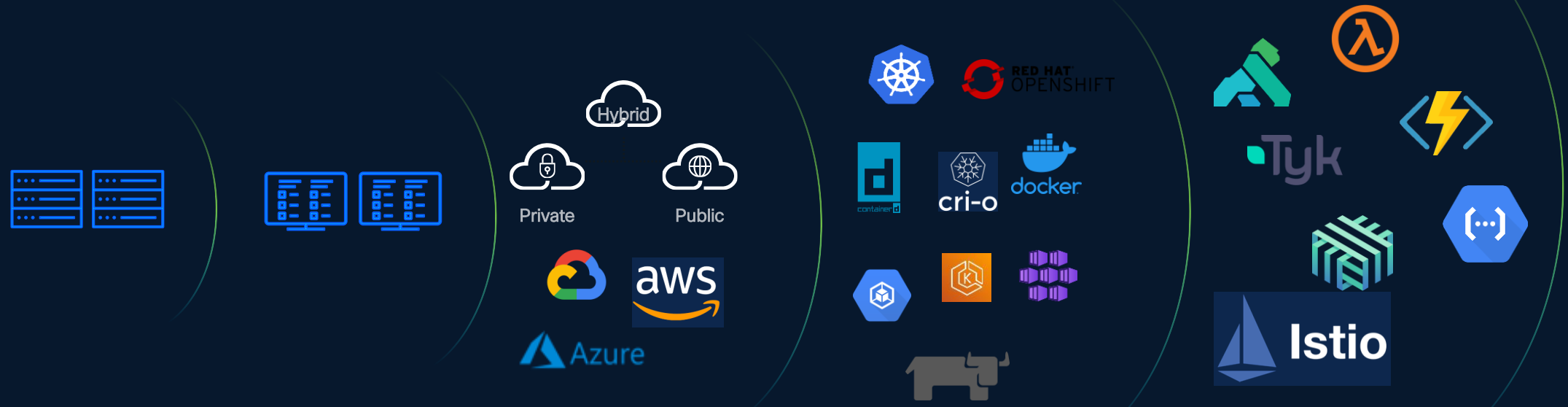
Serverless and more...

Before 2006 | 2006 | 2014 | 2016 | 2021 | 2022

Bare Metal

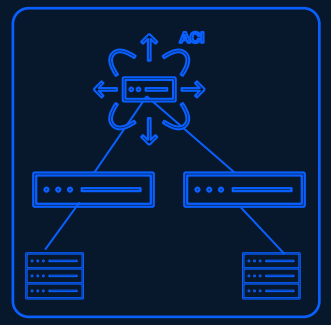
Public Cloud

K8s Mainstream adoption



But… what is an application workload?

Network Engineer

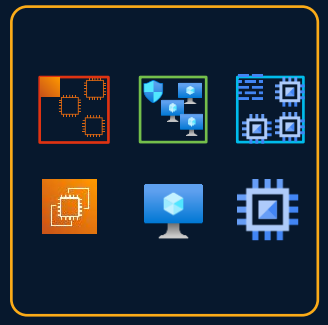


- Vlans/VRF
- Subnets
- Contracts

Firewall Engineer

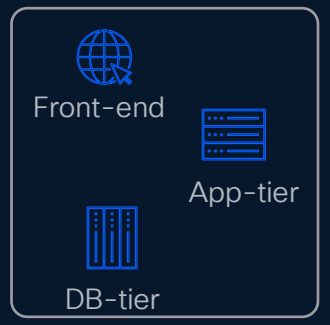
- Zones
- Subnets
- ACLs

Cloud Engineer



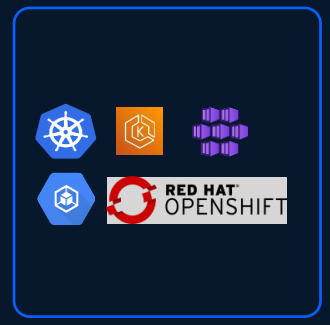
- VPC
- Subnets
- Security Groups

Application Owners



- Service
- Application
- Workload

Cloud-Native Engineer



- Namespace
- Service
- CNI

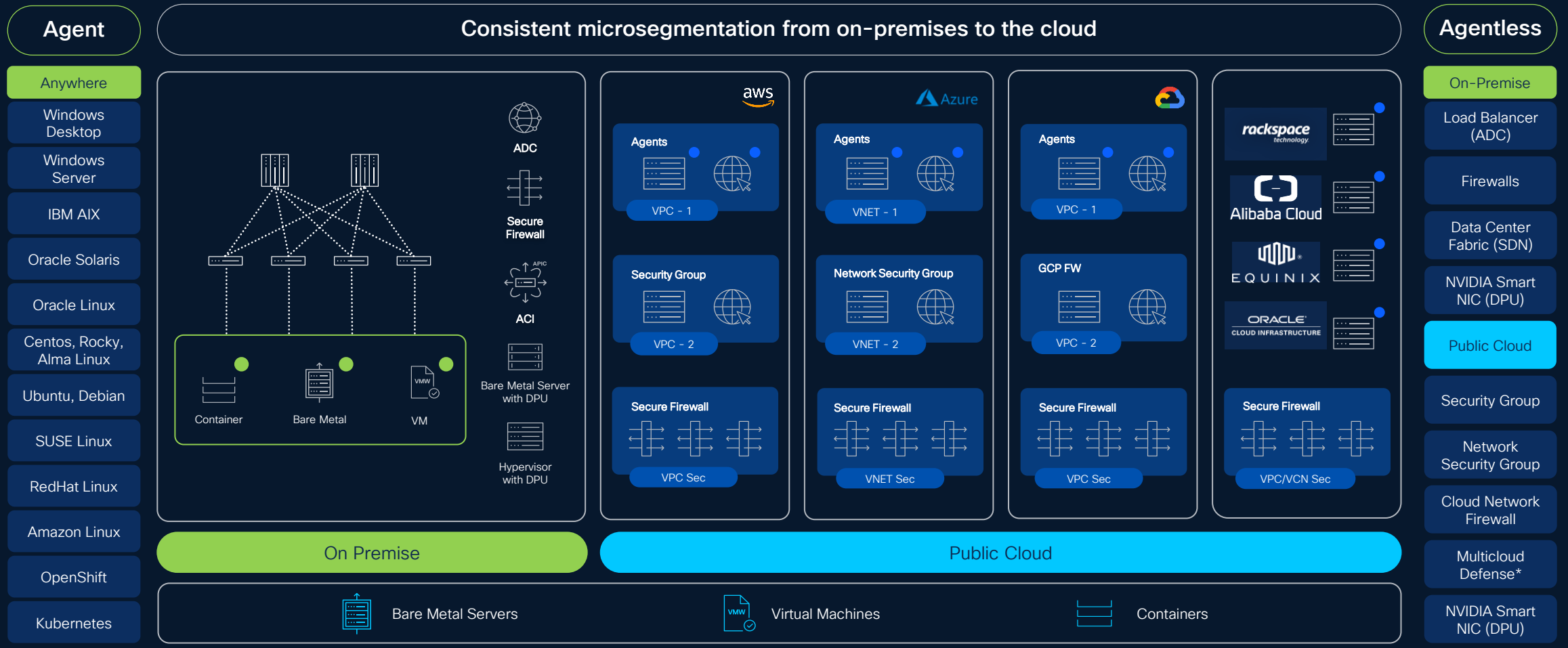
Segmentation and Policy Control Challenges

Organizational Challenges

Multiple teams, organizations and environments

Inconsistent islands of policy controls across environments

Big picture for Applications – Let's take a step back



* - In Roadmap

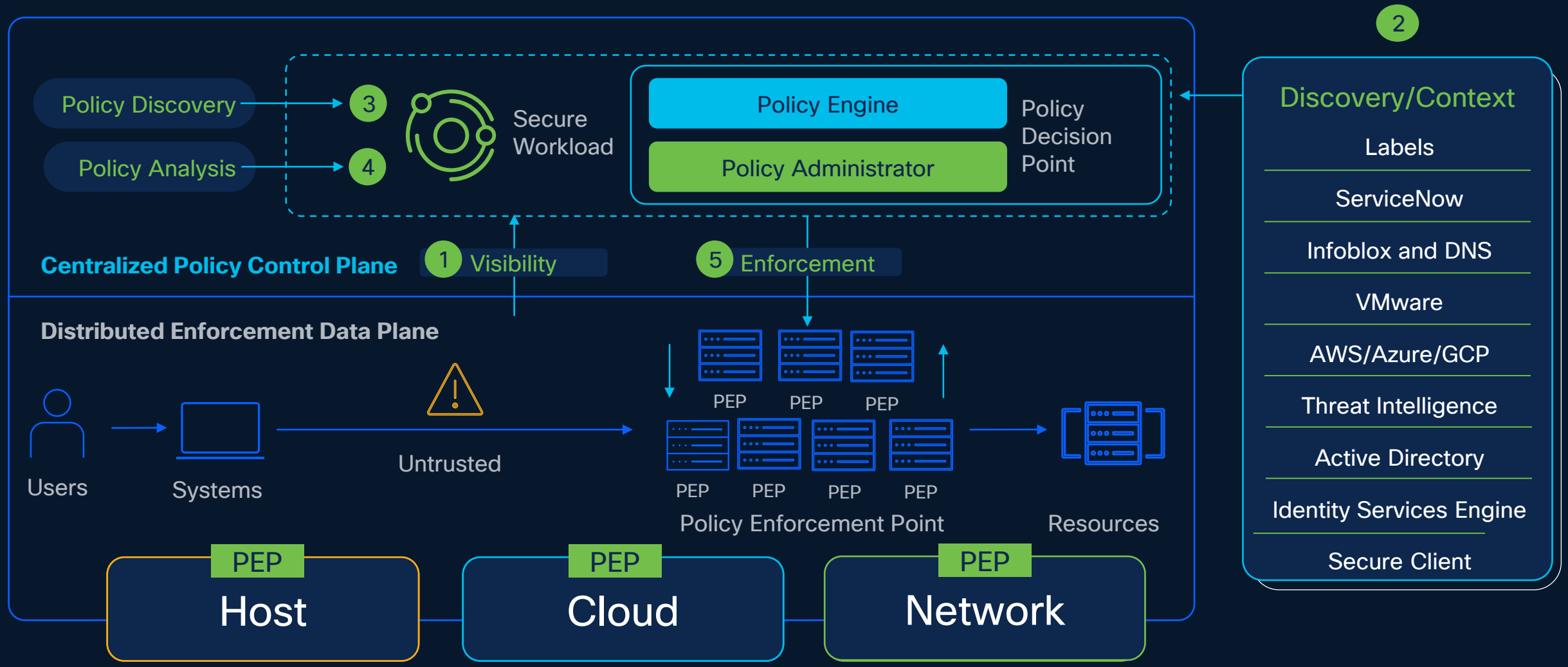
Secure Workload Use-Cases

Microsegmentation

Behavioral detection and protection

Vulnerability detection and protection

Secure Workload – Zero Trust Segmentation



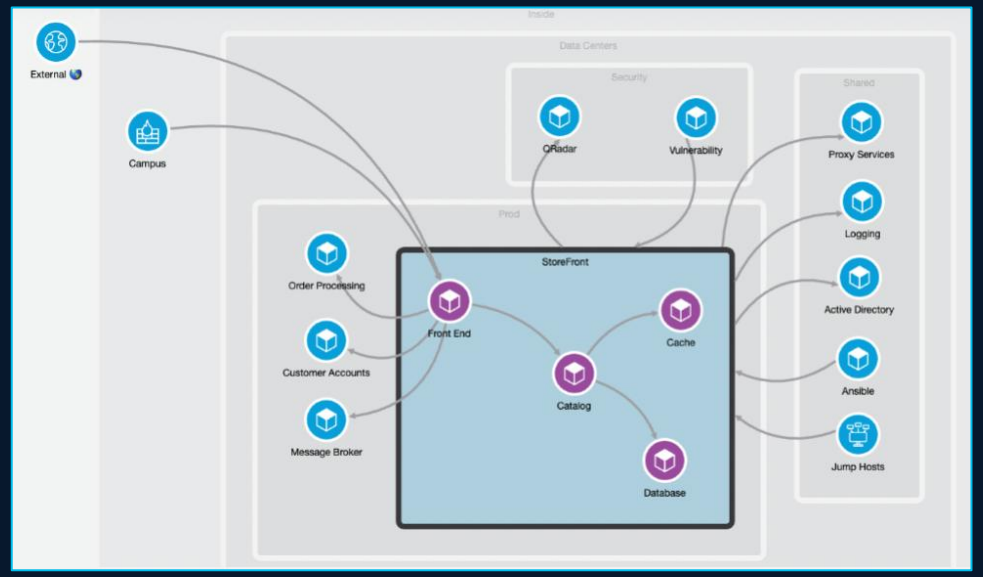
cisco

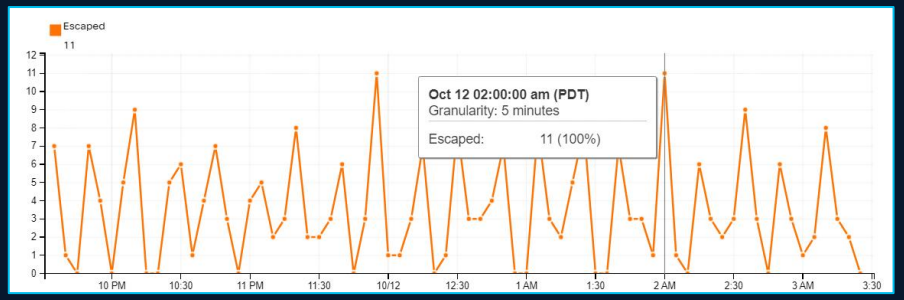
Cisco

Policy Discovery and Policy Analysis (AI)

Automatically generated policy based on application behavior

- A key challenge with the microsegmentation journey is managing the policy lifecycle
- ADM (Application Dependency Mapping) is fundamental in the journey
- Using an application dependency map as a blueprint, Secure Workload automatically generates the microsegmentation policy
- Policy Deviations can be easily identified and corrected before enforcement with Policy Analysis



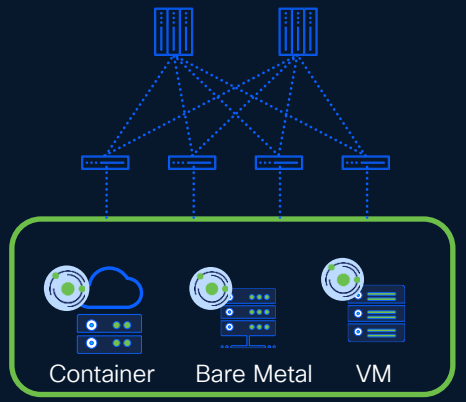


Microsegmentation Approach Evaluation

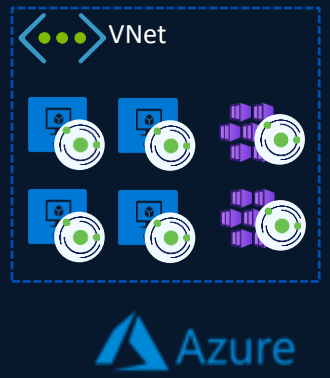
	Agent	Agentless
Pros	• Network Abstraction • In-depth visibility and protection • Flexible segmentation	• Less organizational dependencies • Leverage existing infrastructure • Faster time to deploy
Cons	• Organizational dependencies • OS dependency (legacy) • Agent fatigue	• Network/CSP infrastructure dependency • Segmentation granularity/scalability • Only network-flows visibility

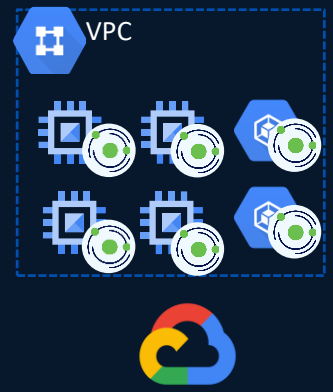
Host-Based Agent

Visibility and Enforcement



On-Prem





Any Location

Establish Policy Guardrails with Policies for your Application Workloads

Host-Based Agent - Features

Protect the workloads – at the workload level!

Lightweight

- Doesn't sit on Datapath
- Minimal resource footprint
- Easy to install

Configurable

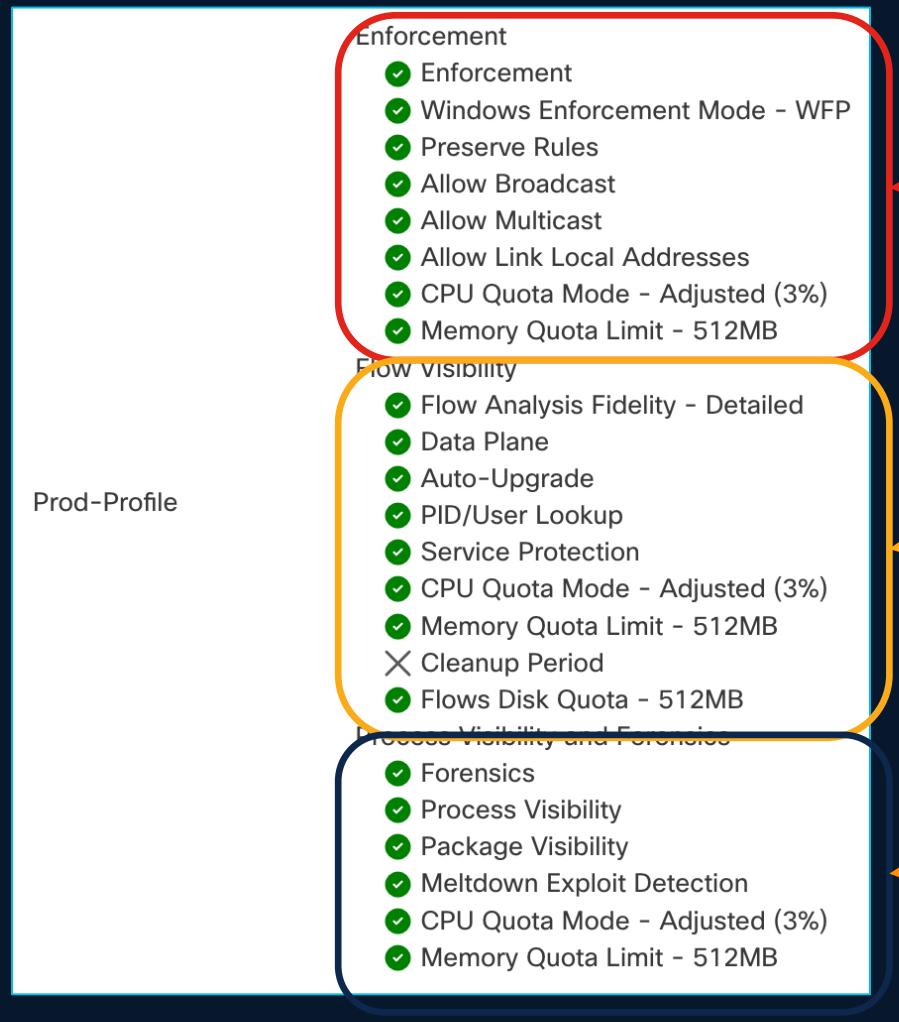
- Flow Visibility
- Packages/Process visibility
- Forensics
- Enforcement

Resilient

- Centralized upgrade
- Easy migration
- Protected communications

Host-Based Agent - Features

Protect the workloads – at the workload level!



Enforcement Features

Flow Telemetry and Operability Features

Process Visibility, Vulnerability and Behavioral Features

Network-Based Agentless

Protect the workloads – at the network level!

Visibility

- Common telemetry protocols
- ERSPAN
- Flow-Stitching

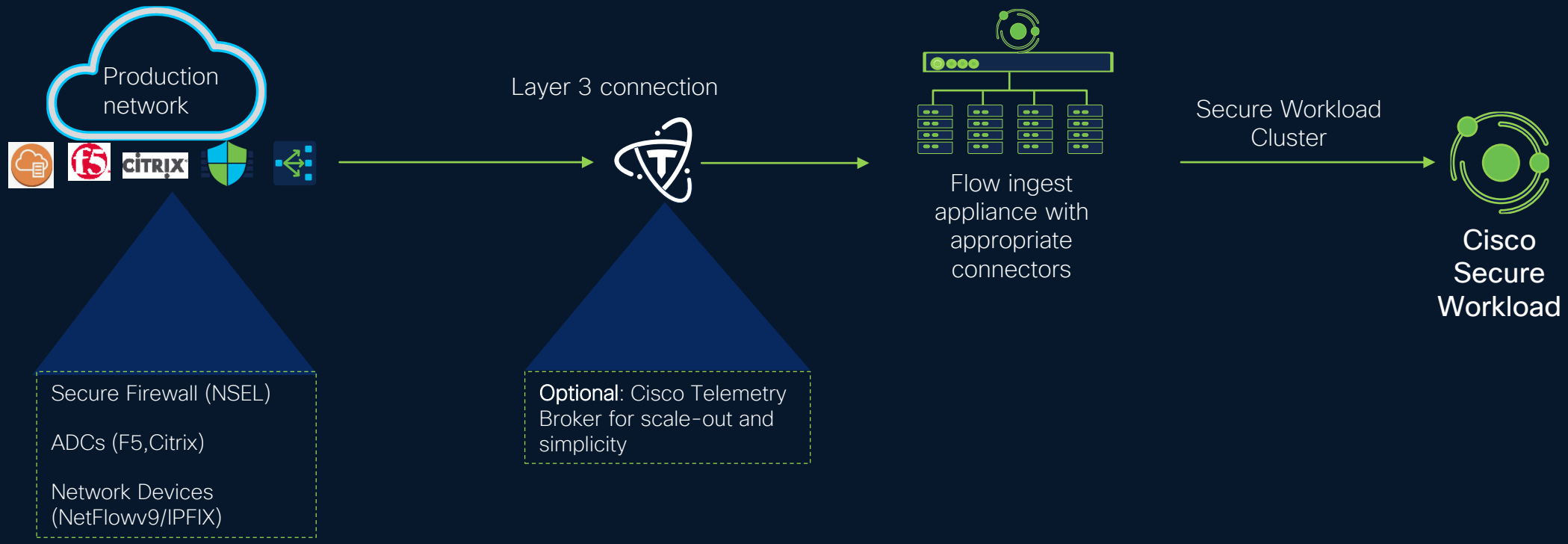
Enforcement

- Secure Firewall
- Load-Balancers

Scalability

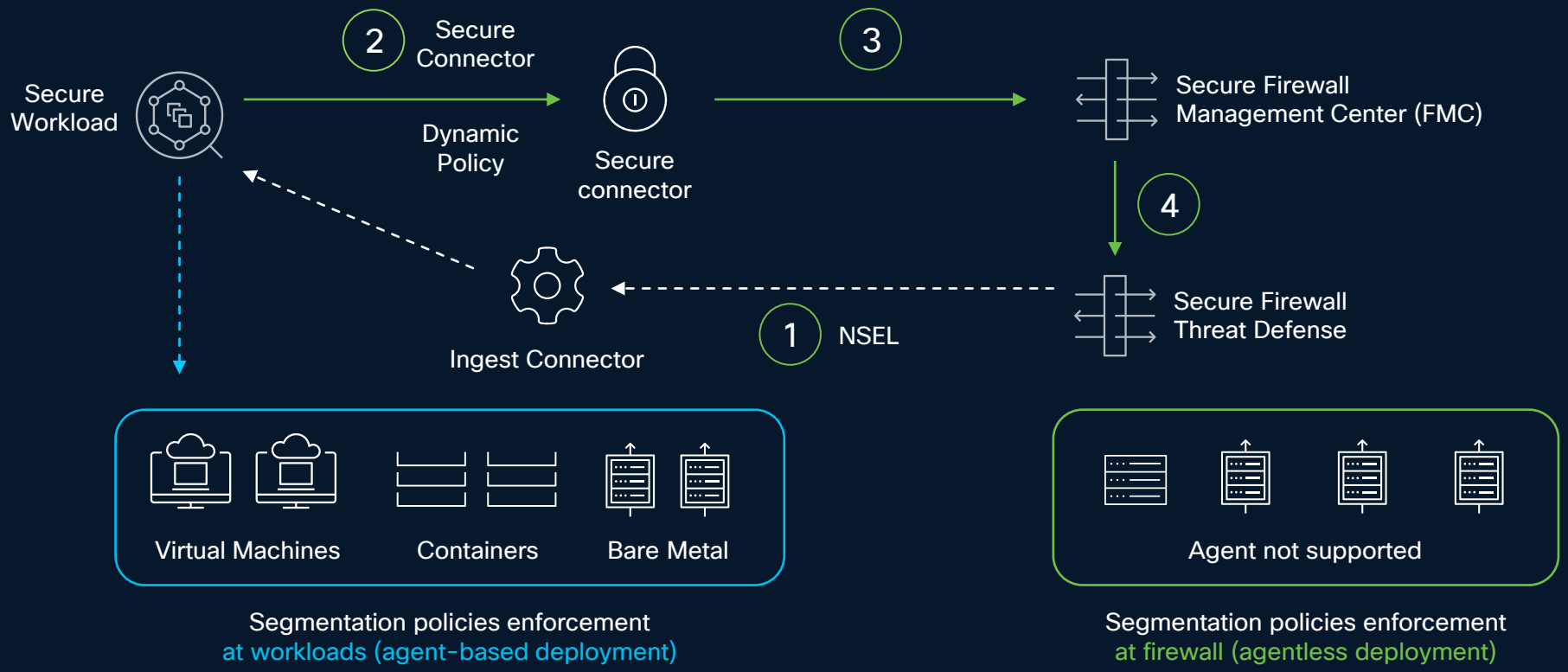
- Ingest Appliance
- Up to 135k fps per appliance

Network-Based Agentless



Agentless - CSW-FMC integration and enforcement

Defense-in-depth use case



Benefits

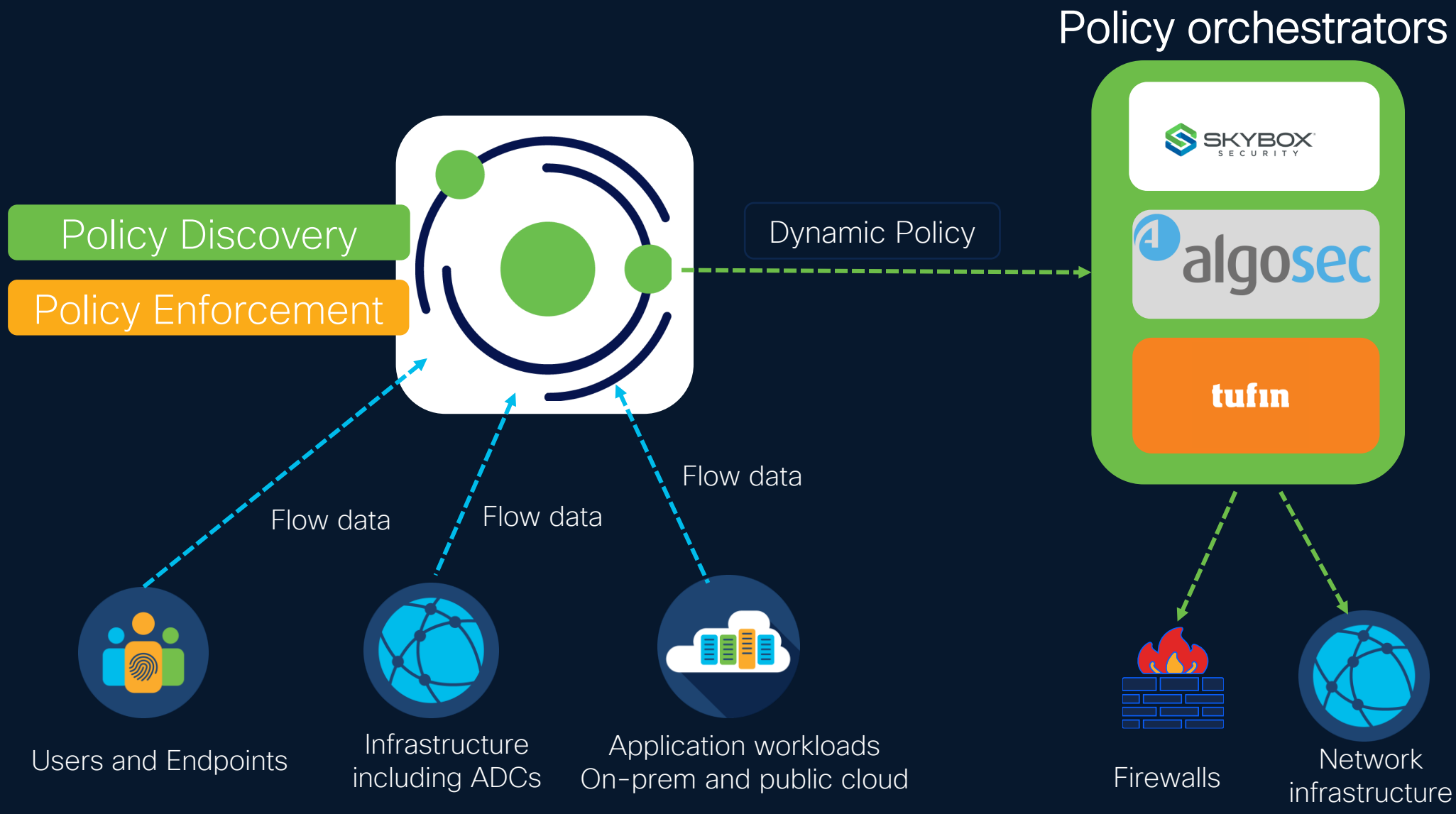
- Faster time to value
- Agentless visibility & policy enforcement
- Flexible and scalable policy enforcement
- Reduce exposure to the known vulnerabilities

Cloud Service Provider Agentless - Features

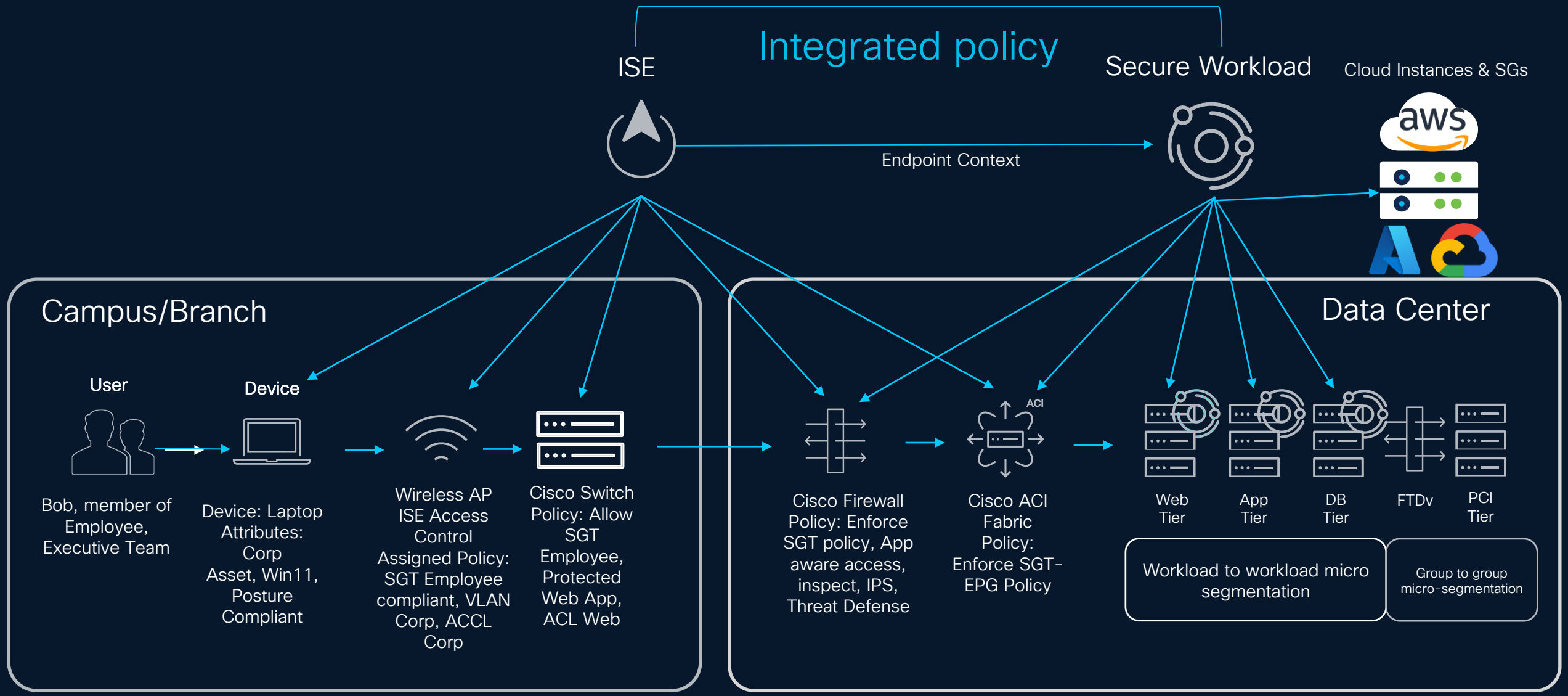
Protect the workloads – at the workload level!

- Centralized cloud-onboarding experience
  - Cloud connectors
  - Single point of management
- Visibility
  - Near real-time discovery of workloads and labels
  - Flow telemetry via VPC/VNets flow-logs
- Enforcement
  - Security Groups (AWS)
  - Network Security Groups (Azure)
  - Firewall (GCP)

Integration with 3rd party policy managers



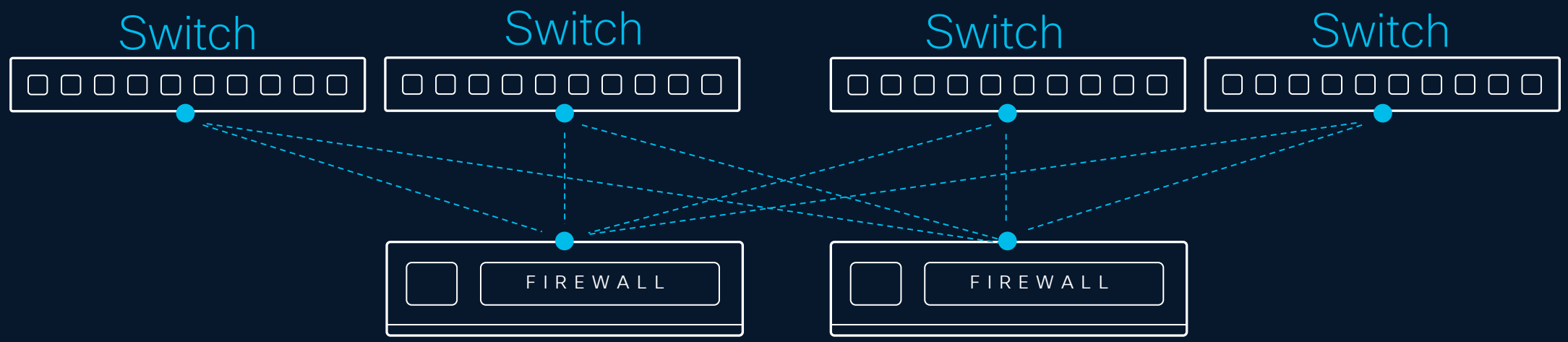
Cisco's Zero Trust Segmentation Strategy



Zone Segmentation

Deploying firewalls for zone segmentation is expensive

While you utilize only a fraction of the firewall capabilities



Power

Software licenses

Optics

Support contracts

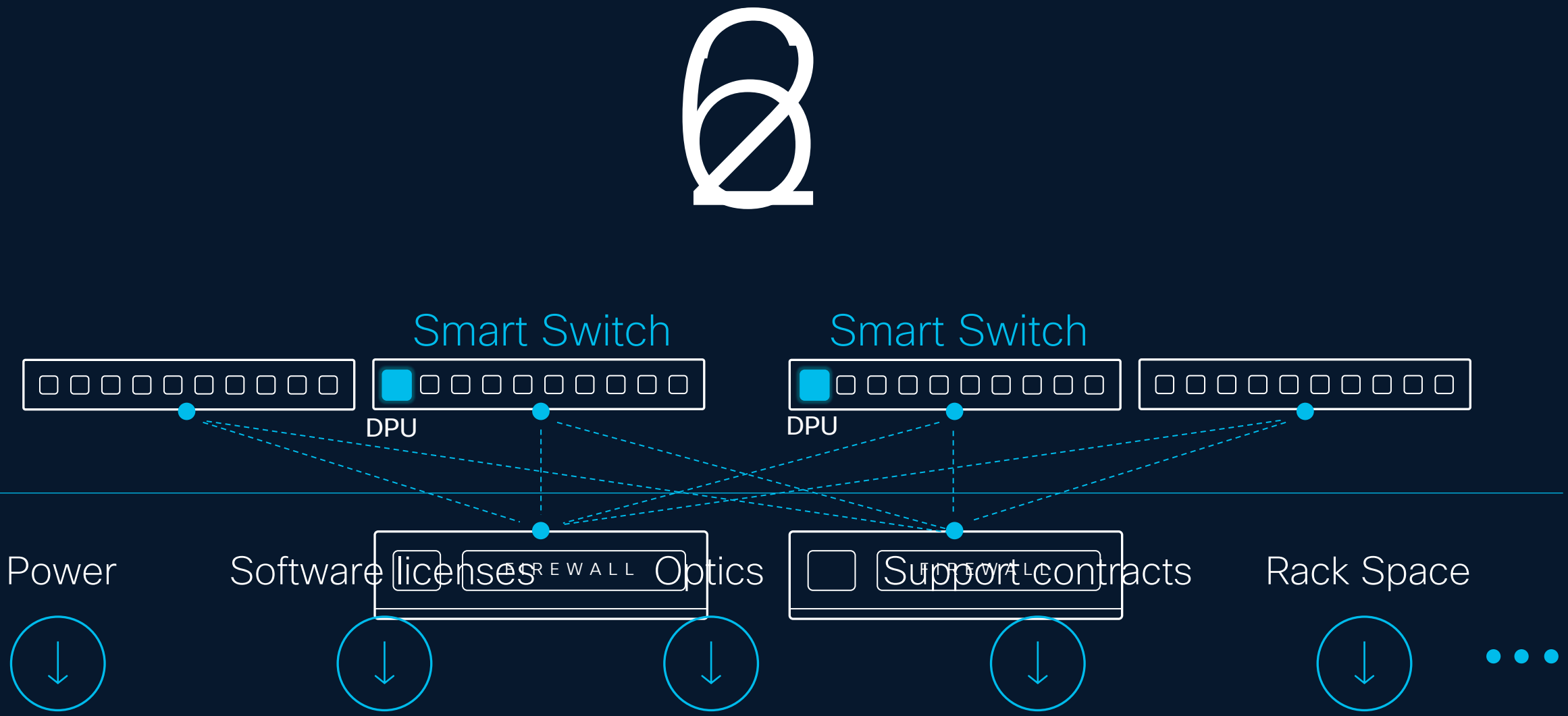
Rack Space

Introducing Cisco Smart Switch

Network + Security
in one switch

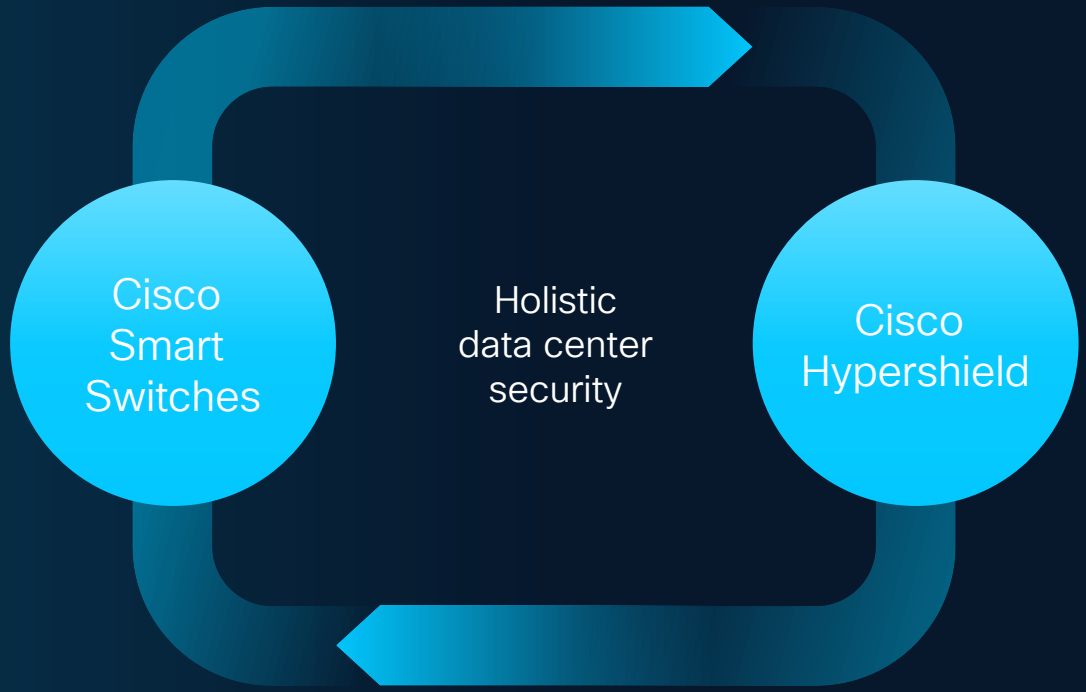
Separate workflows and
separate data flows for
networking and security

Up to 84% TCO savings



Security infused into the data center fabric

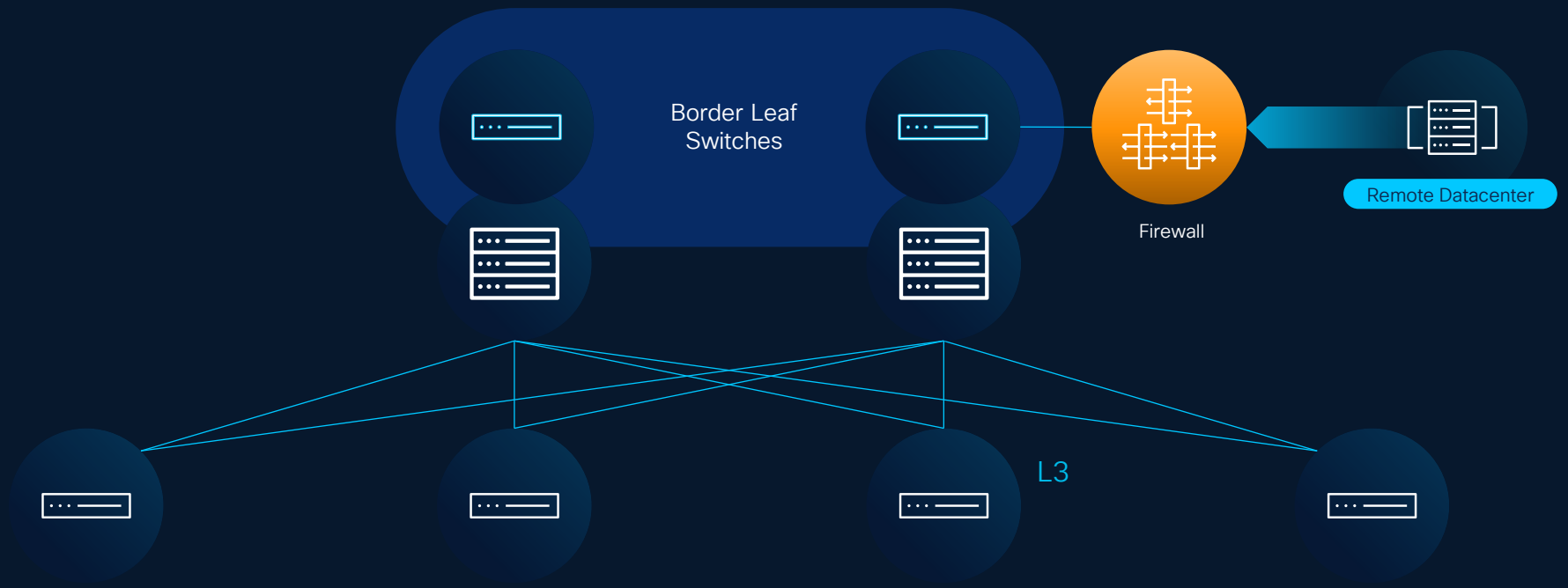
Use cases



- Cloud Edge
- Zone-based segmentation
- Data Center Interconnect (DCI)
- Top of Rack Segmentation & Enforcement

Use Case #3: Data Center Interconnect (DCI)

From: DCI with Border Gateway/Router and Firewall



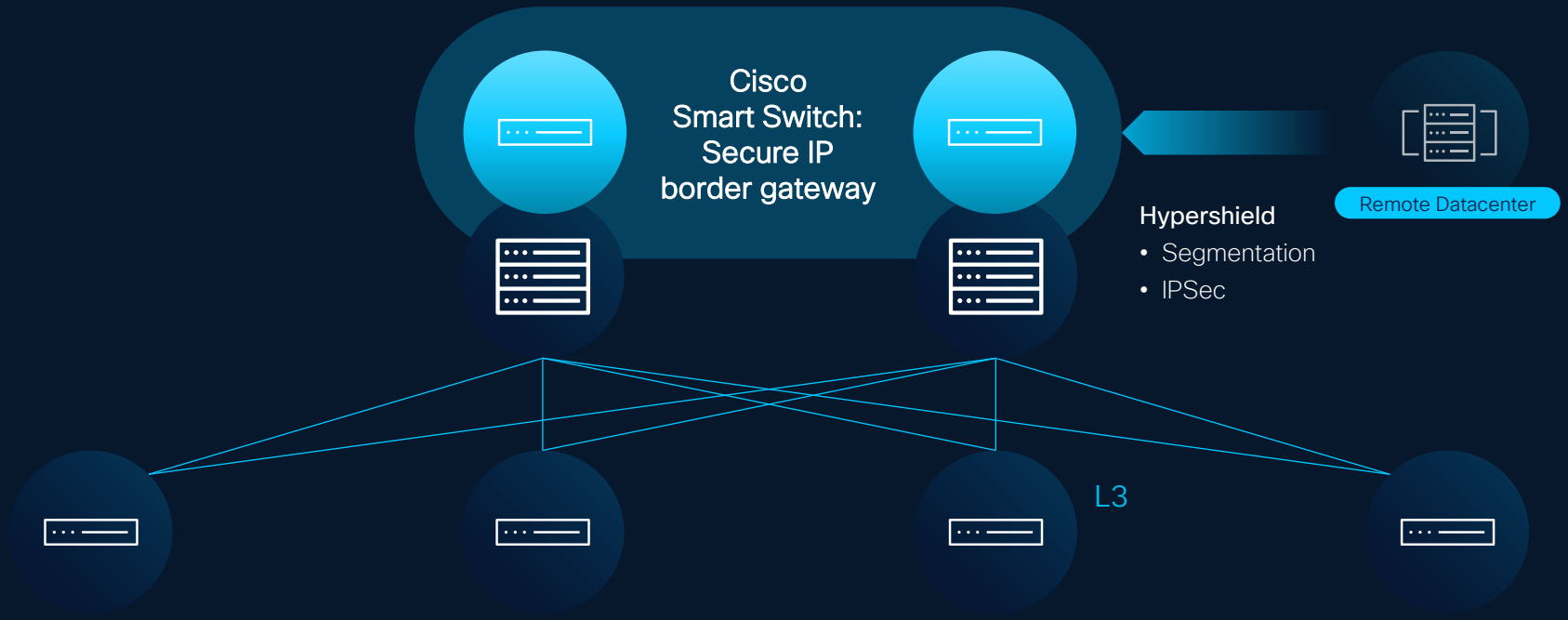
Challenges

- Expensive firewall appliances
- Scale-up firewall without scale out option

Conceptual representation only
(actual design varies, e.g. dark fabric)

Use Case #3: Data Center Interconnect (DCI)

To: DCI with Cisco Smart Switches

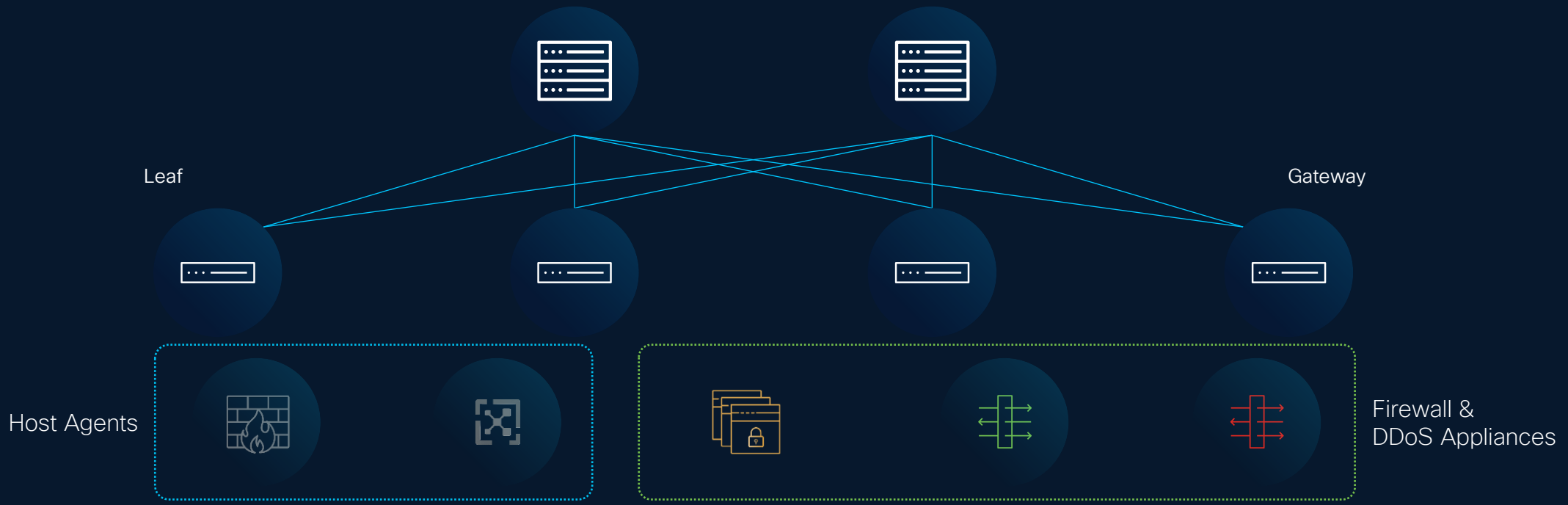


Main Benefits

- Converged network & security into Hypershield services switches / Border Gateway
- Consistent security policy for cross DC connectivity, including L4 segmentation & IPSec encryption
- Common Network and Security visibility in Nexus Dashboard and Cisco Security Cloud Control
- Lossless HA and stateful failover for Active/Active firewall

Use Case #4: Top of Rack Segmentation & Enforcement

From: DCI with Router and Firewall

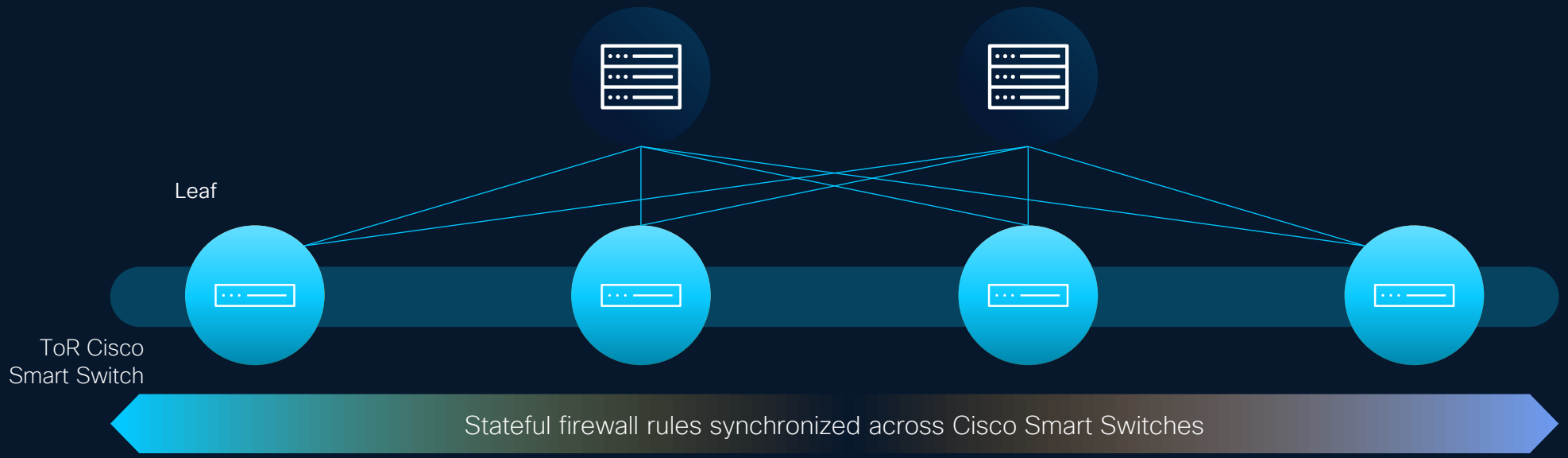


Challenges

- Multiple, disparate solutions – increased risk of error, inconsistent enforcement, & security breaches
- Point solutions hinder implementing holistic zero trust

Use Case #4: Top of Rack Segmentation & Enforcement

To: Pervasive East-West autonomous segmentation

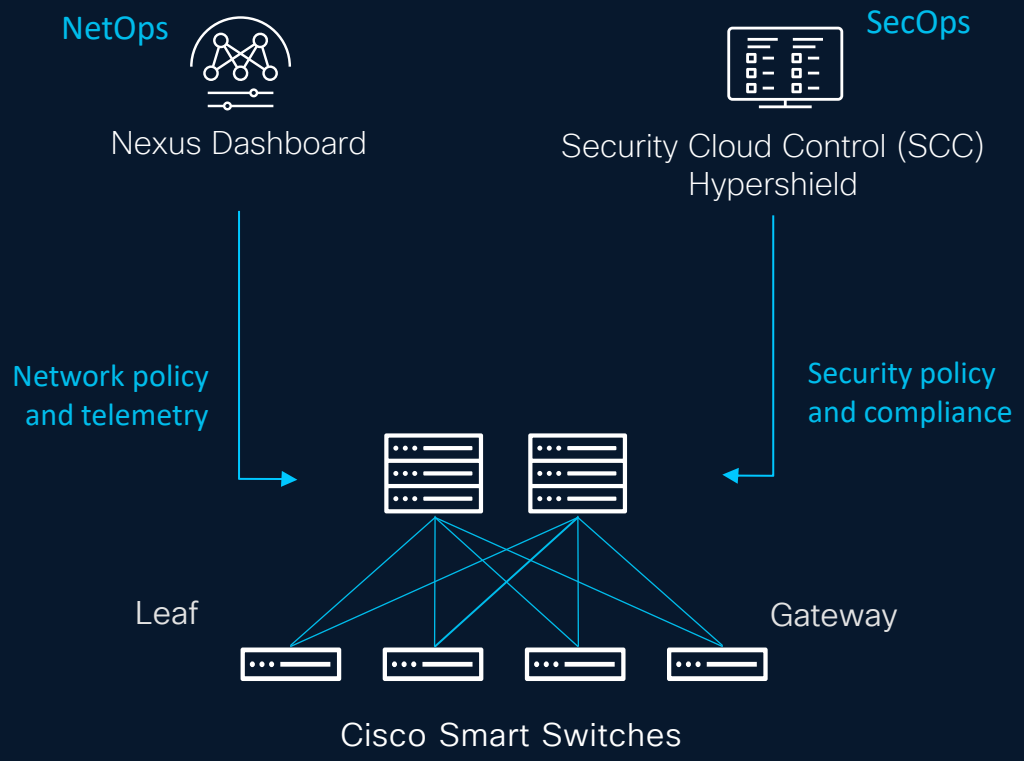


25G or 100G ToR

Main Benefits

- Distributed stateful segmentation and L4 enforcement in every port
- Policy testing before deploy and firewall load updates
- Simple redirect policy (e.g. vrf or vlan) from network to within the switch
- Agentless | supports all workloads | Lower TCO

Network and security workflows delivered within a single solution



Orchestration workflows and lifecycle

- Persona-driven NetOps and SecOps workflows and dashboards
- Common troubleshooting workflows supported by context sharing between network and security controllers
- Observability of network analytics, security policy and compliance

NetOps and SecOps continue to have separate workflows to ensure network connectivity while implementing strong security

Cisco Data Center Switch + Hypershield
Best of Breed Platforms for DC Services

Cisco N9300 Series Smart Switch *(1H 2025)*

24-port 100G

- 800G Stateful Services Throughput
- 4.8T Silicon One + AMD DPUs
- 1 RU

Cisco N9300 Series Smart Switch (2H 2025)

48-port 25G, 6-port 400G, 2-port 100G)

- 800G Stateful Services Throughput
- 4.8T Silicon One + AMD DPUs
- 1 RU

Smart switch fits easily into the broader security fabric

HYBRID MESH FIREWALL

Secure Firewall | Secure Workload | Cilium | Hypershield | Smart Switch/ Server | 3rd Party Firewall

L7 Threat Protection | AI Model Protection | Segmentation | Exploit Protection