CISCO Connect

Segmentation Untangled: Streamlining Hybrid Data Center Security

Chris Merkel – Solutions Engineer – DC Architecture

Josh Harmacinski – Solutions Engineer – Security

04/07/2026

Agenda

1. DC Segmentation
2. Network Based
3. Service Insertion
4. Agent Based
5. NG DC Security
6. Segmentation Deep Dive

Key Challenges We’re Solving

Fragmented segmentation policy can’t keep up with change

Visibility and security gaps for modern cloud and AI apps

Attackers move faster than patching cycles

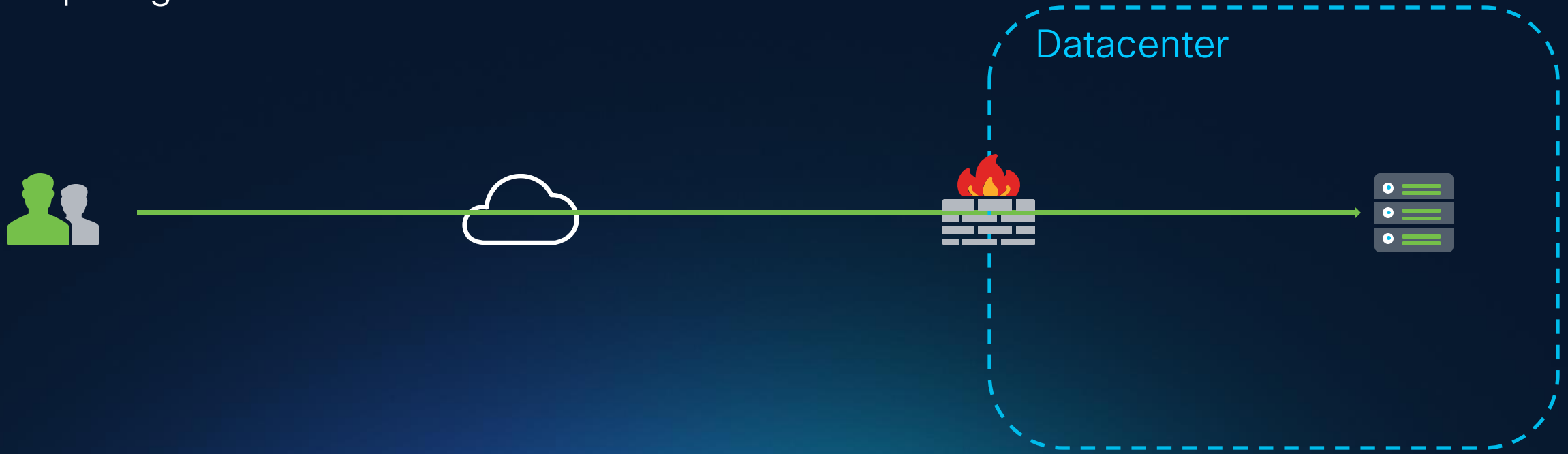
cisco

DC Segmentation

Securing Application Workloads – Threat Landscape

Using Network Security Controls

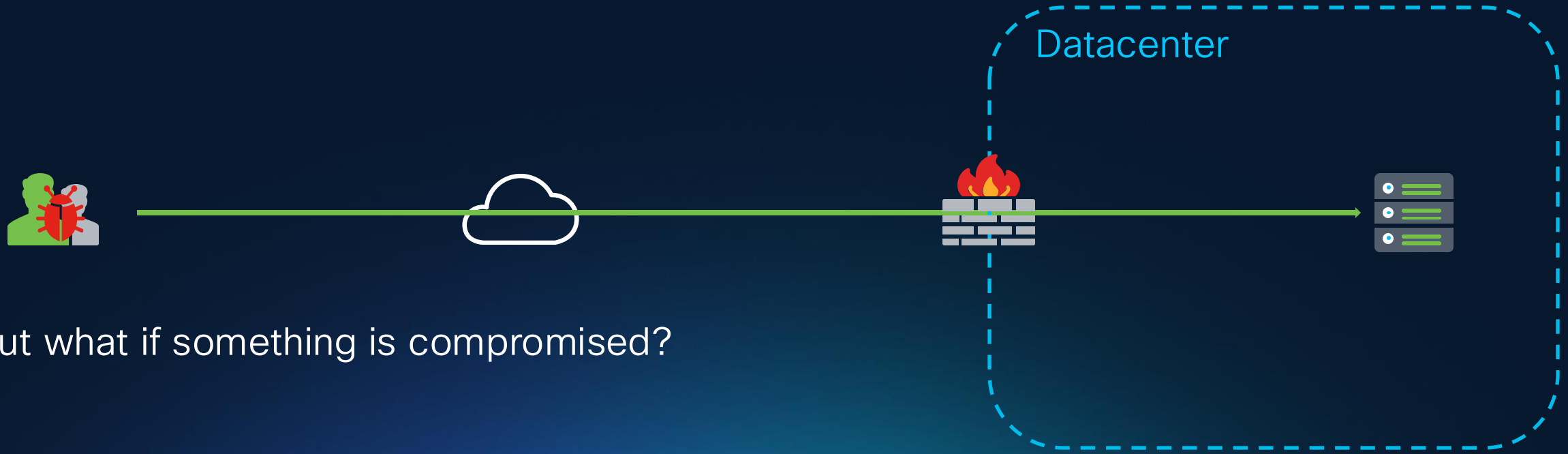
Simple right?



cisco

Securing Application Workloads – Threat Landscape

Using Network Security Controls

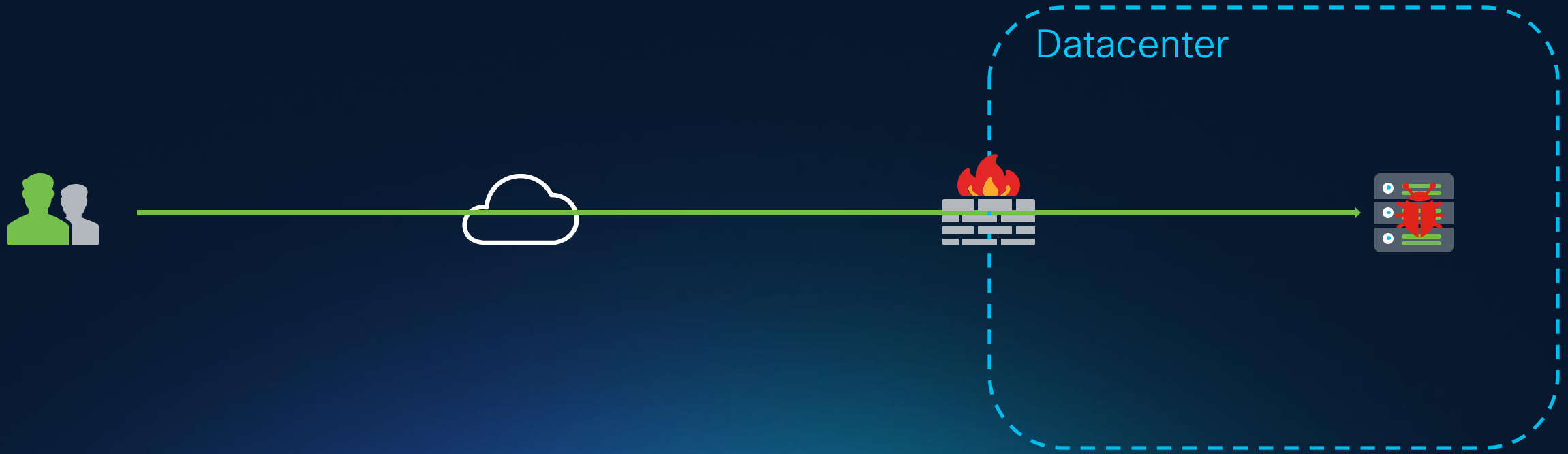


But what if something is compromised?

cisco

Securing Application Workloads – Threat Landscape

Using Network Security Controls

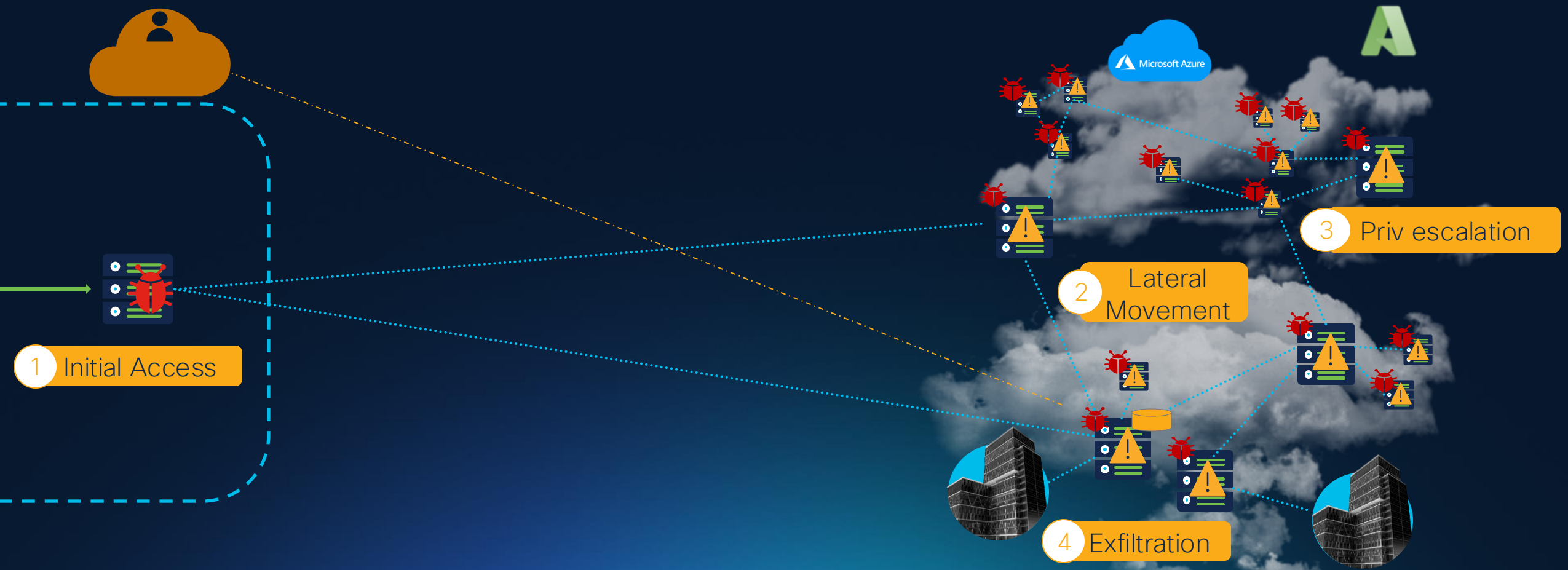


And this is only a part of the story.....

cisco

Securing 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

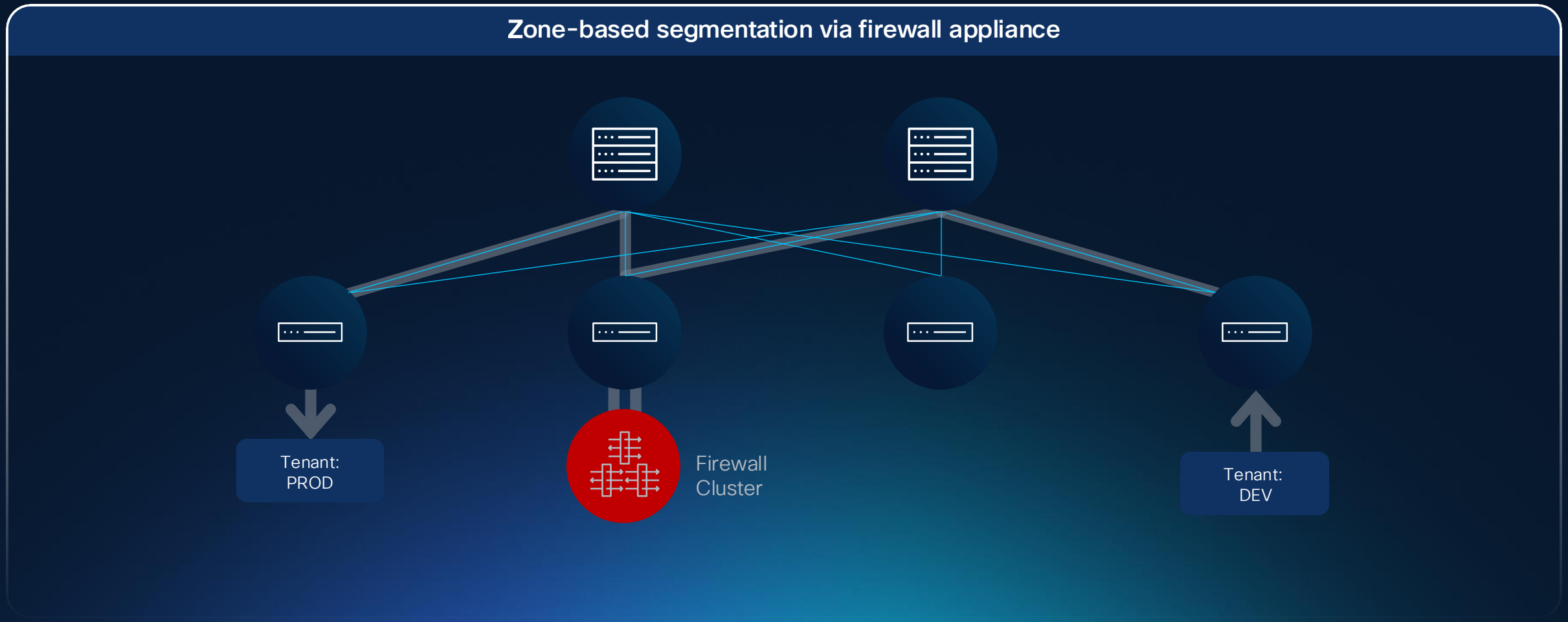
K8s Mainstream adoption

cisco

Segmentation Methods

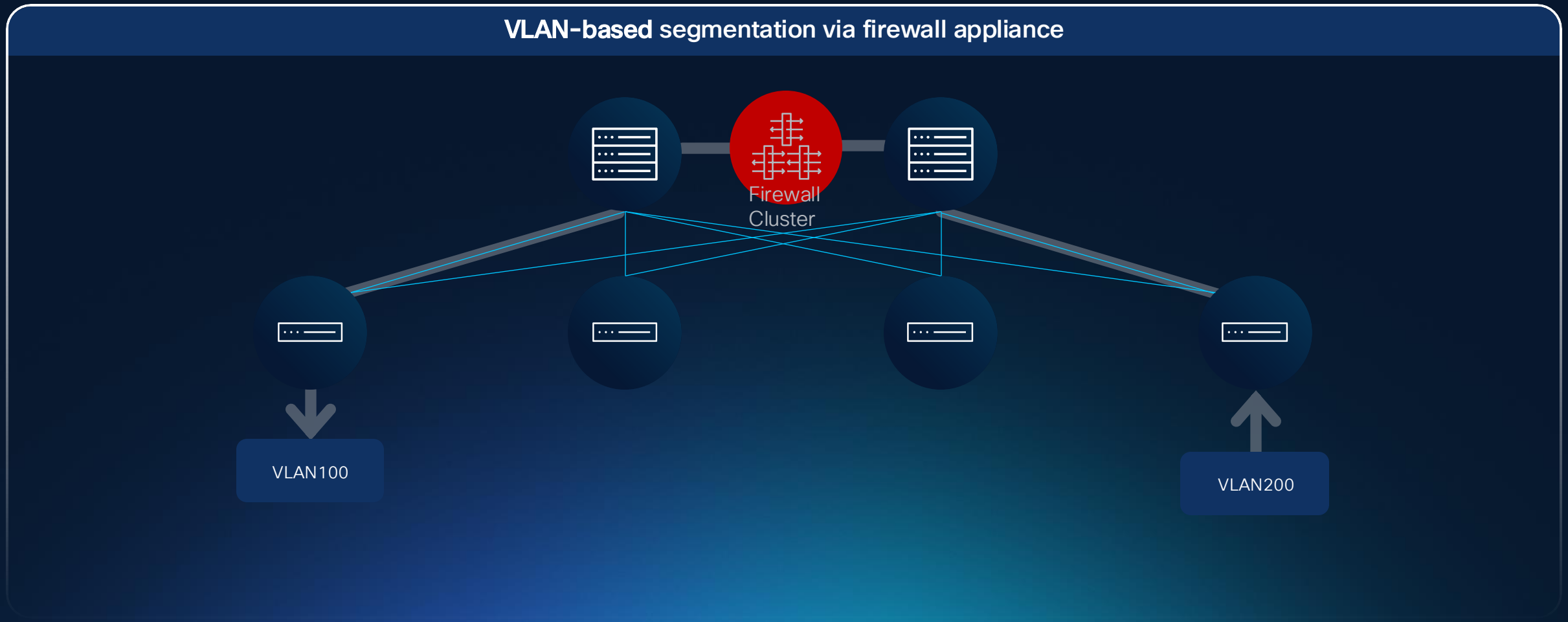
Zone-Based Segmentation

- Routing domains as boundary



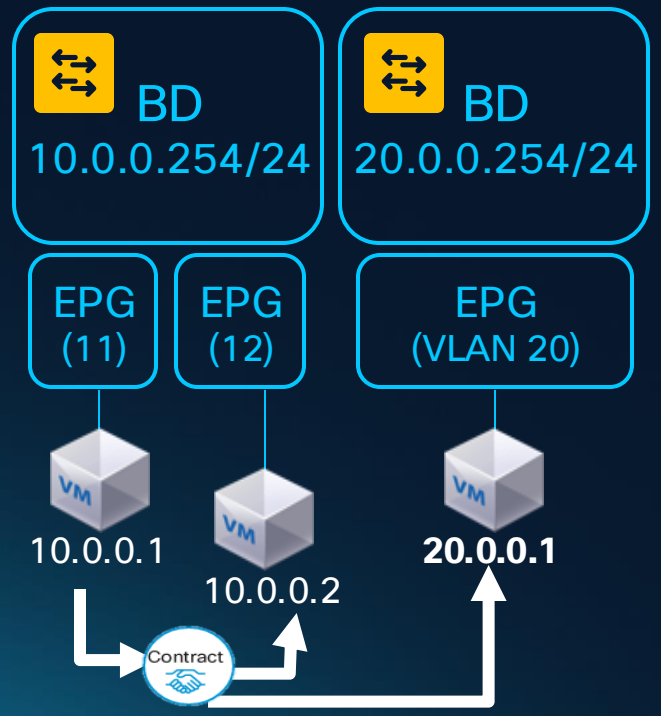
L2 Based Segmentation

- VLAN or VXLAN domain as boundary



Endpoint Groups

- Application Centric
  - Multiple EPGs per BD – drive segmentation deeper into the infrastructure
  - ACI only

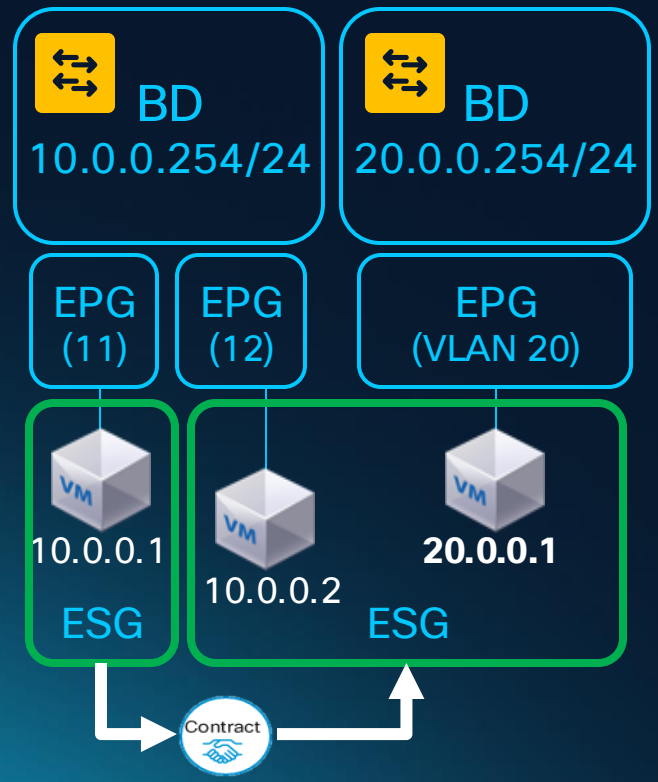


Endpoint Security Groups

Simple and Flexible Security

- Application Centric
  - Security Groups **across bridge domains**
  - ACI and NXOS VXLAN

Flexible endpoint grouping using Security Groups

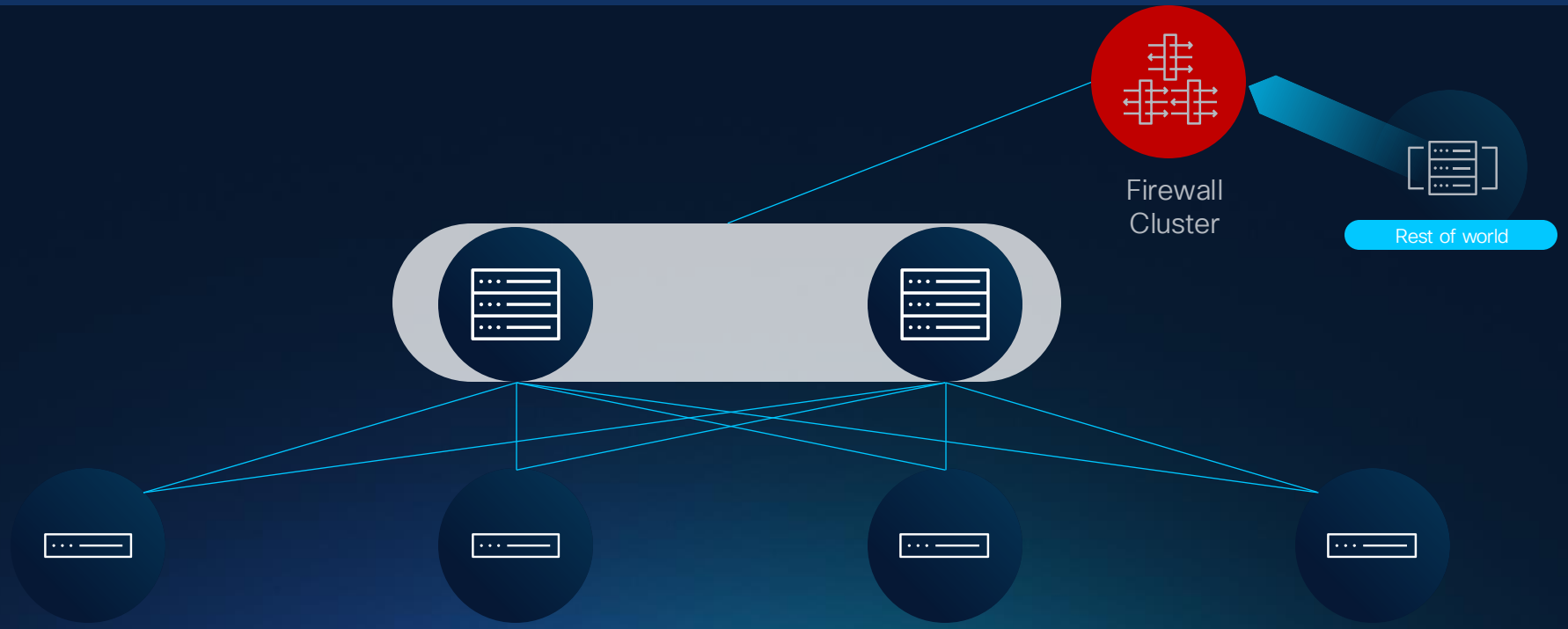


Service Insertion

Enhancing the network security

The DC Front Door Firewall

From: DCI with Border Gateway/Router and Firewall



Challenges

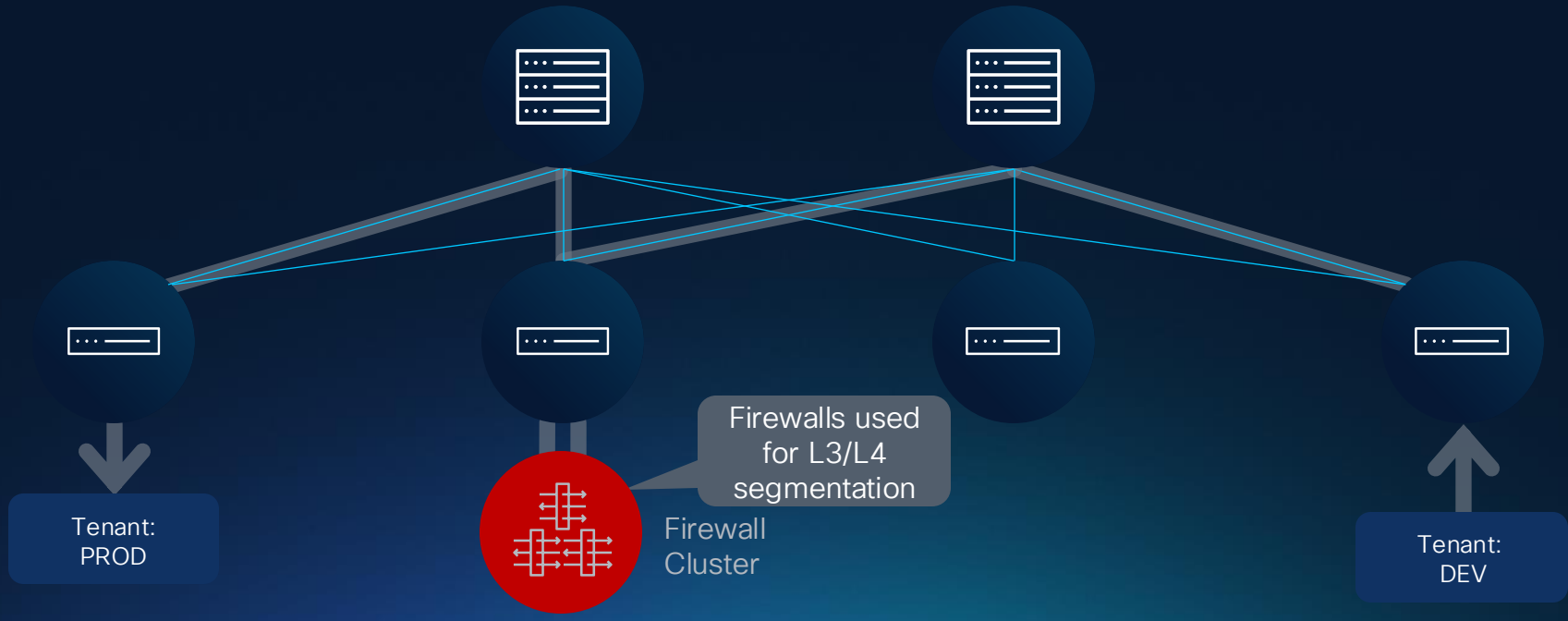
- Firewall only protects traffic coming in. Exploits can easily move laterally once past

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

Zone Based Segmentation

VRF stitching with FW

Zone-based segmentation via firewall appliance



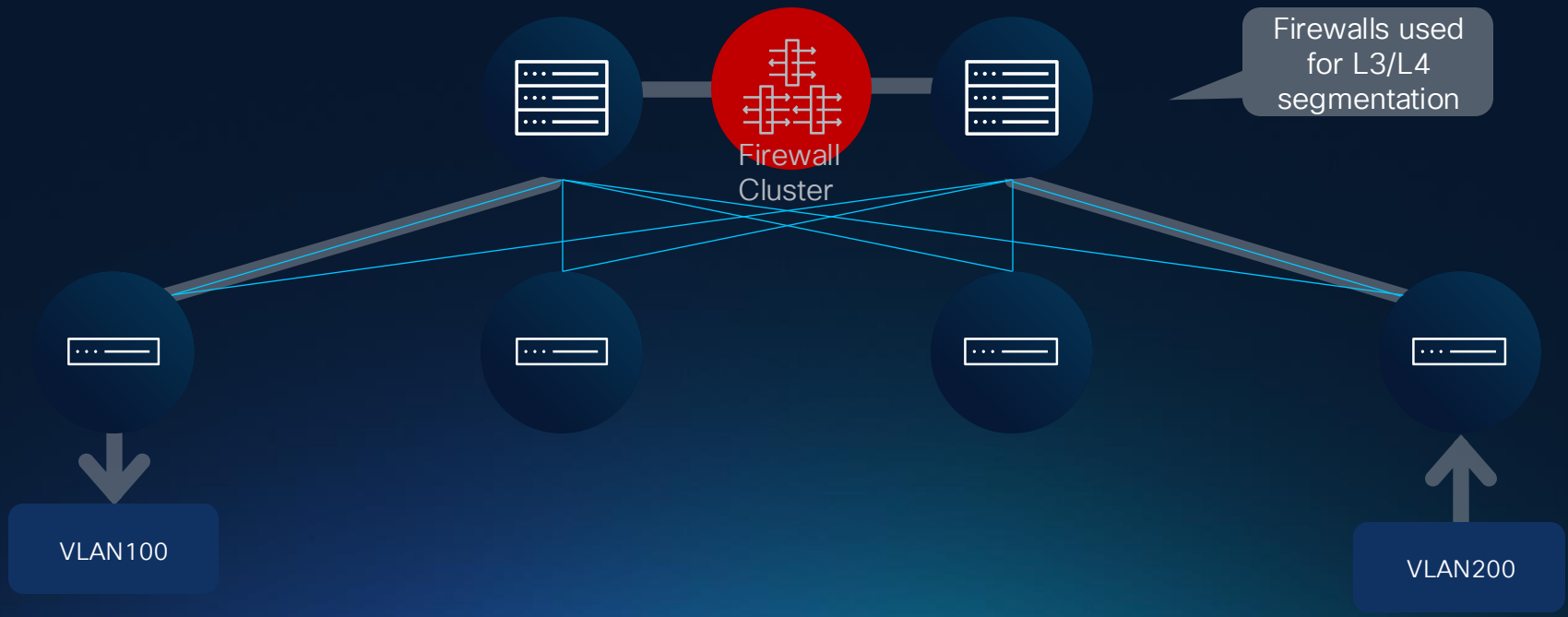
Challenges

- Firewall becomes a router
- Protects between zones but no controls within

VLAN Based Segmentation

Firewall as DG or between hosts and DG

VLAN-based segmentation via firewall appliance

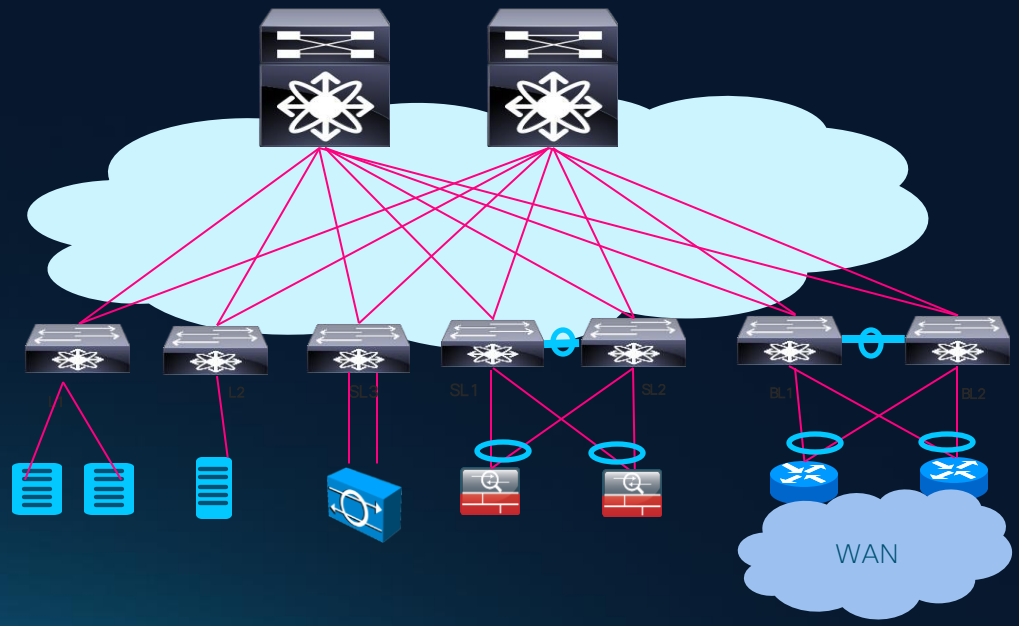


Challenges

- Firewall inspects all inter-VLAN traffic, very expensive
- Installed as either L2 Transparent or L3 Gateway
- No way to omit traffic from inspection

Service Insertion in DC

- Challenges with Service insertion in DC
  - Managing complex traffic rules (lack of flexibility)
  - Service Nodes (Firewall/LB/IPS) are becoming bottle necks
- What is the industry asking?
  - Simplify device onboarding
  - Provide the ability to selective redirect/service chain workflows
  - Leverage network for load-balancing with ability to do selective traffic redirect (omit traffic that FW cannot inspect)

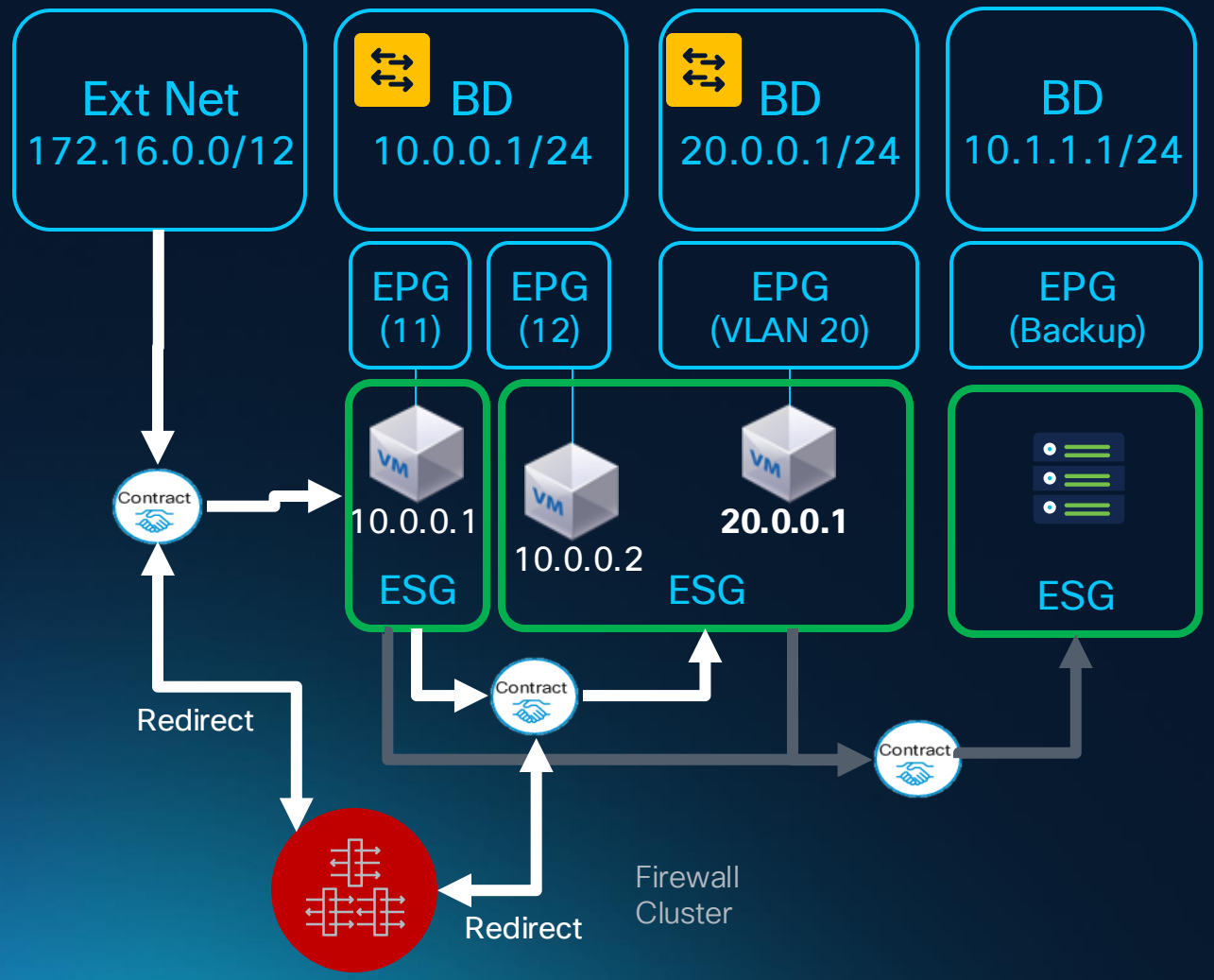


Endpoint Security Groups

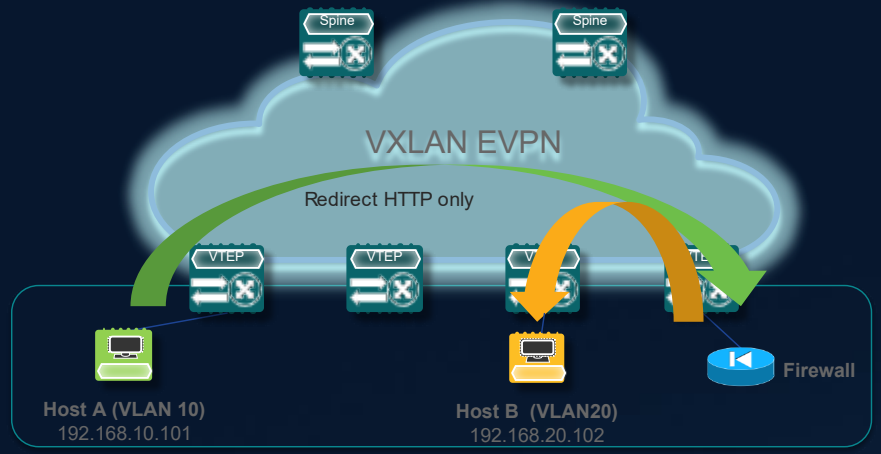
Simple and Flexible Security

- Application Centric
  - Security Groups **across bridge domains**
  - ACI and NXOS VXLAN GPO

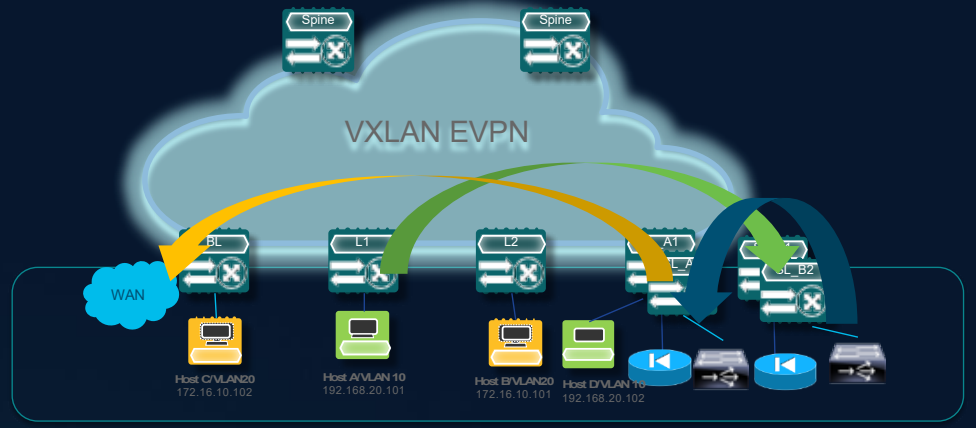
Flexible endpoint grouping using Security Groups



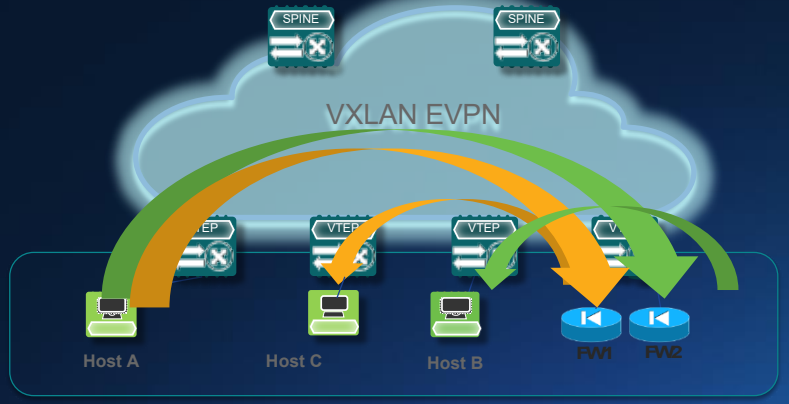
Use Case of Policy Based Redirect



Selective traffic redirection



Selective traffic Service Chaining



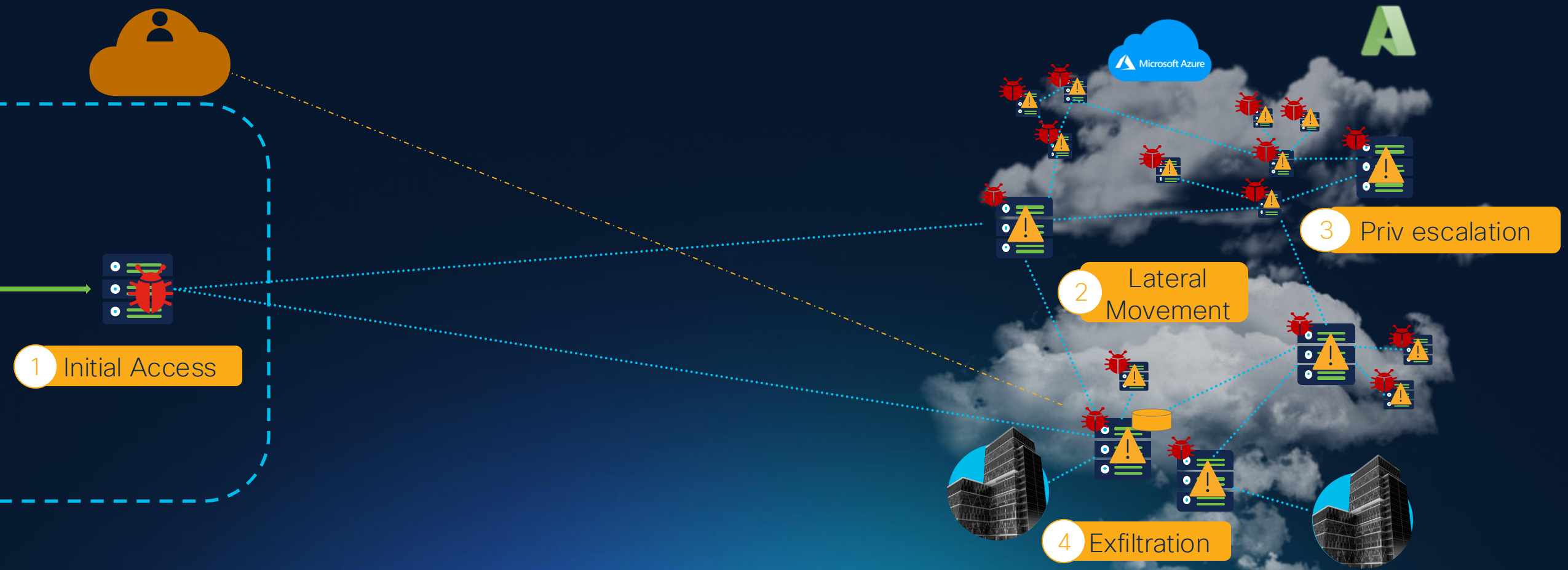
Redirection +Load-balancing

And more..

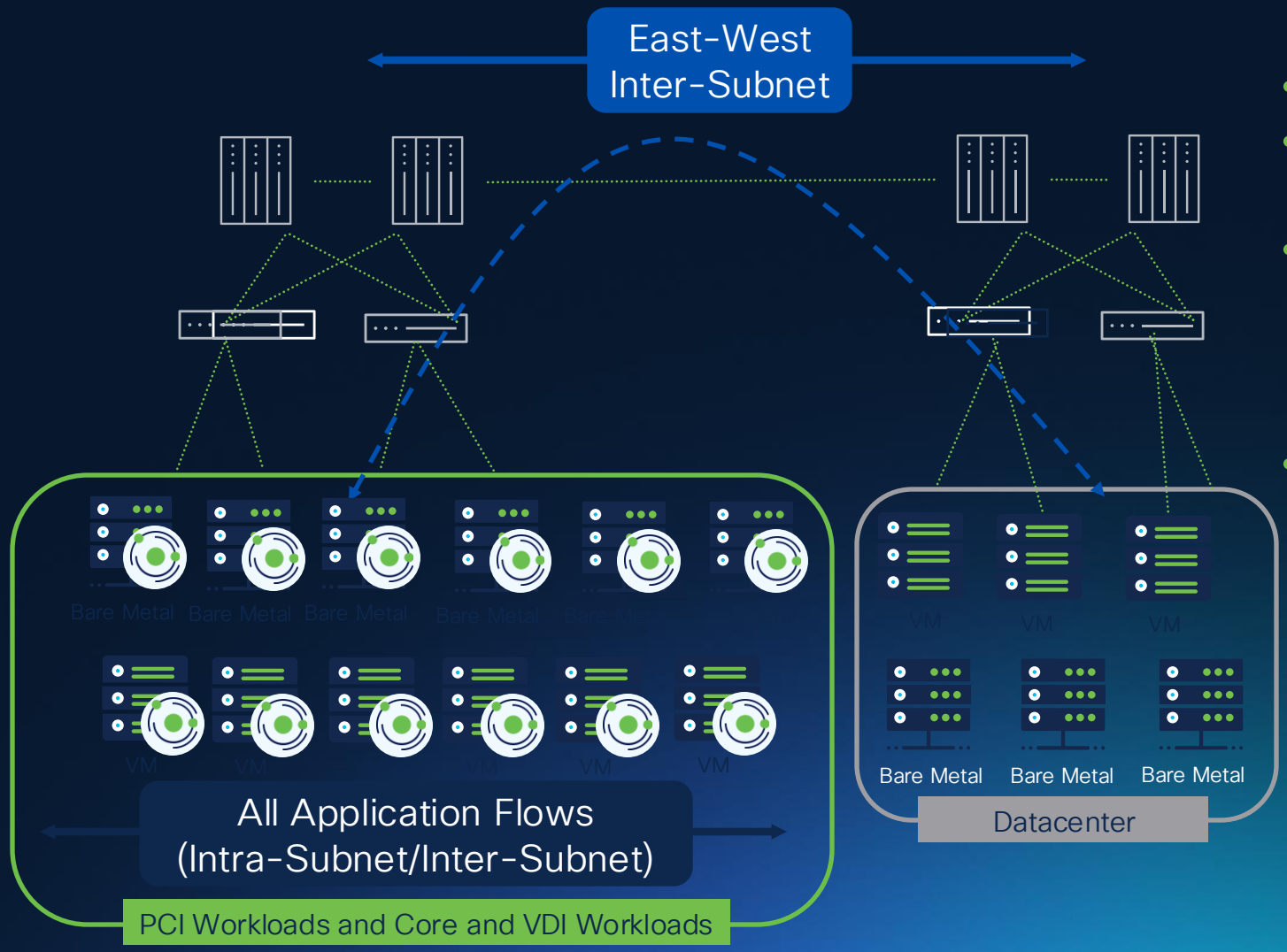
Agent Based

Securing Application Workloads – Threat Landscape

Using Network Security Controls



Workload Segmentation – Agent-Based



Host-Based Agent Segmentation

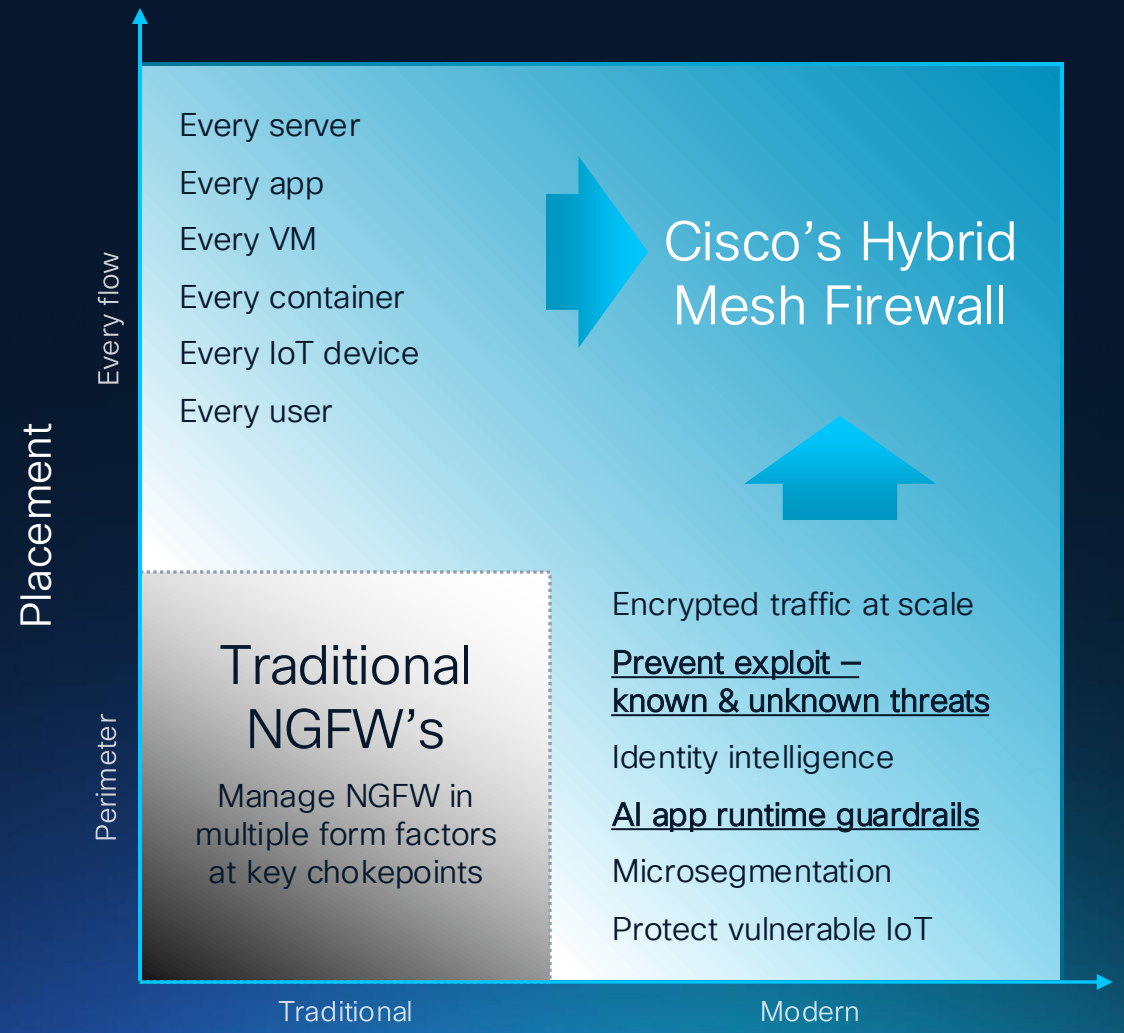
- Ideal for fine-grained segmentation
- In-depth workload visibility
  - Flows/vulnerabilities/processes/users
- Protection at the workload level
  - Intra-App flows (network)
  - Inter-App flows (network)
  - User/Group/Processes
- Suitable for **all personas**
  - Enables delegation of policy controls to **application owners**

What about hosts incompatible with agents?

cisco

Next Generation DC Security

Firewalling Needs to Evolve to Meet Today's Challenges



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

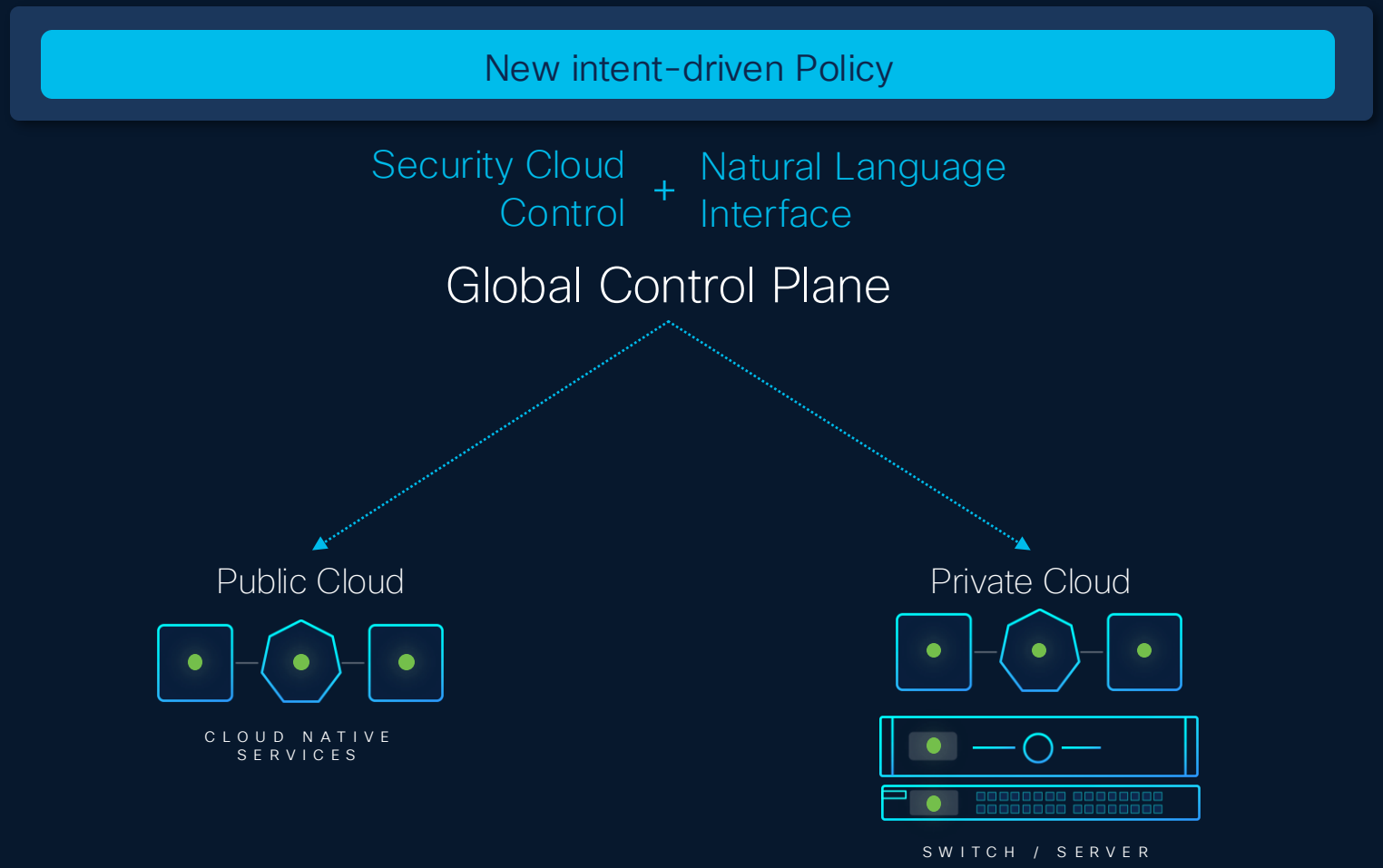
Industry's first multi-vendor intent-based policy

Absorb and optimize existing rules

Change enforcement points, not policy

No rip and replace

Manage Globally and Enforce Locally



Includes

- Unified security management
- Single global policy
- Intelligent placement of shields
- Integrations with cloud/app/infra metadata

Environments

- Kubernetes
- Cloud – Private/Public
- On-prem

Security Infused Into the Data Center Fabric

Cisco N9300 Series Smart Switches

FCS May 2025*

N9324C-SE1U

24-port 100G

- 800G Services Throughput
- Silicon One E100 ASIC + AMD DPUs

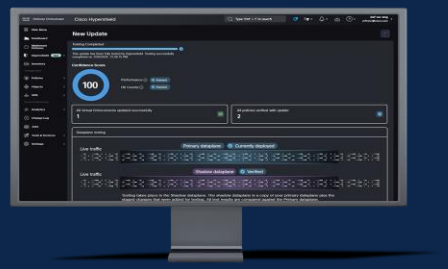
FCS August 2025*

N9348Y2C6D-SE1U

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

- 800G Services Throughput
- Silicon One E100 + AMD DPUs

Cisco Hypershield



Integrated security (license add-on)

- L4 zone-based segmentation
- Intelligent security policy placement
- Self-qualifying policy updates
- Unified with workload/network enforcement, public and private clouds

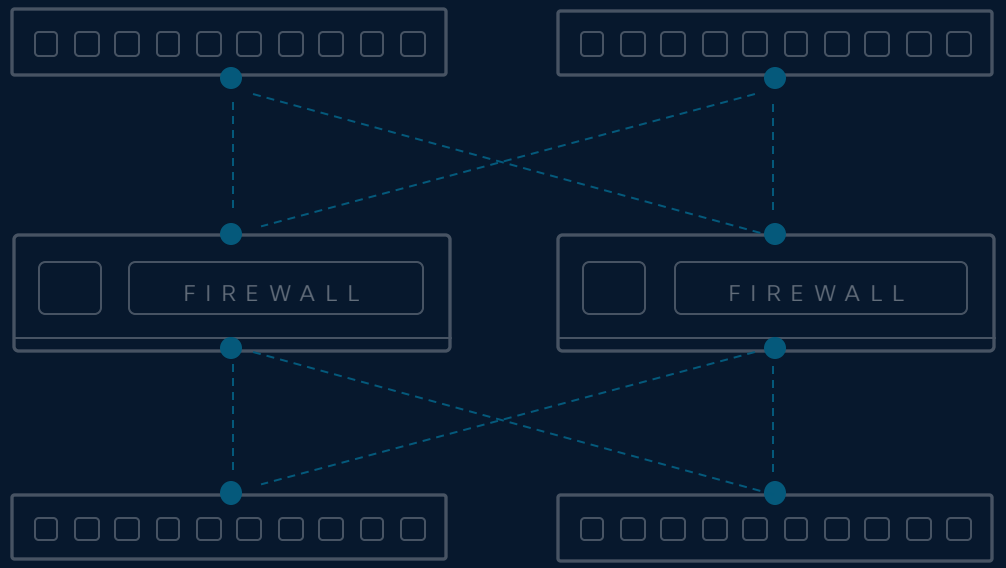
Use cases

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

* GA/FCS timelines for hardware w/ NX-OS
* Hypershield integration with Cisco Smart Switches GA planned for 2HCY2025

Unprecedented ROI

6 boxes



2 boxes

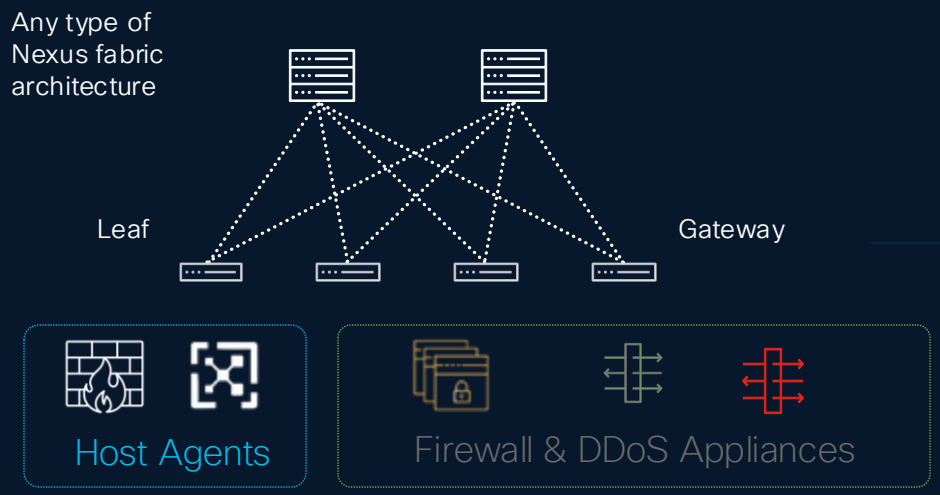
Cisco Smart Switch

Power ↓ Software licenses ↓ Optics ↓ Support contracts ↓ Cables ↓

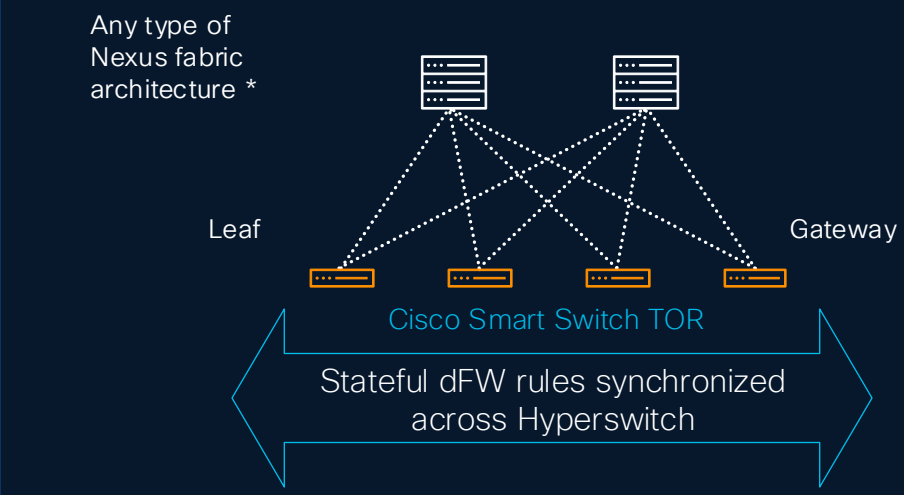
Use Case: Top of Rack

Segmentation & Enforcement

From: DCI with Router and Firewall



To: Pervasive east-west autonomous segmentation



N9348Y2C6D: 25G ToR
N9324C : 100G ToR

Example Customer: Applies to Nexus fabric customers

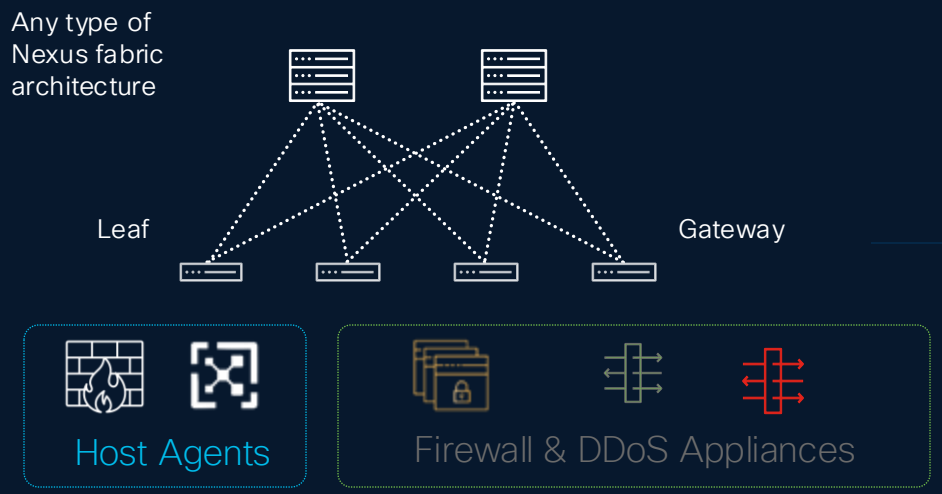
Main Benefits

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

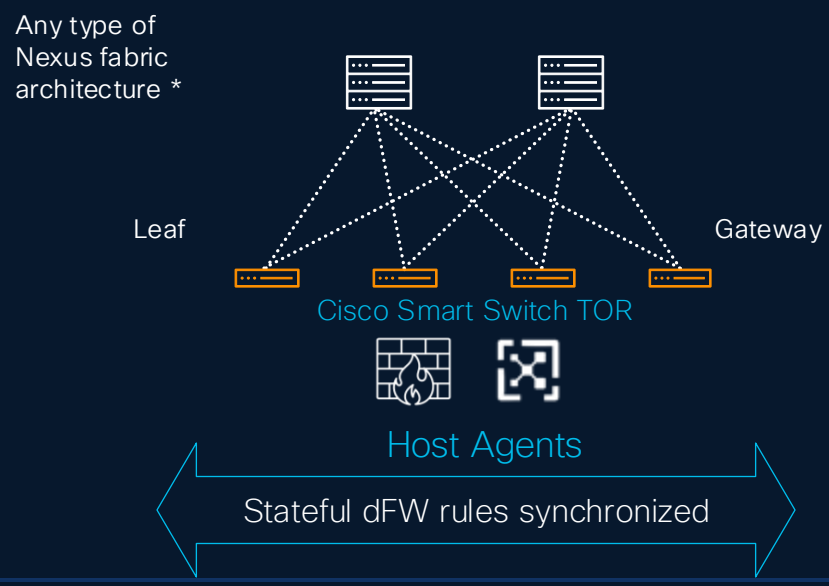
Use Case: Top of Rack and Agents

Segmentation & Enforcement

From: DCI with Router and Firewall



To: Pervasive east-west autonomous segmentation



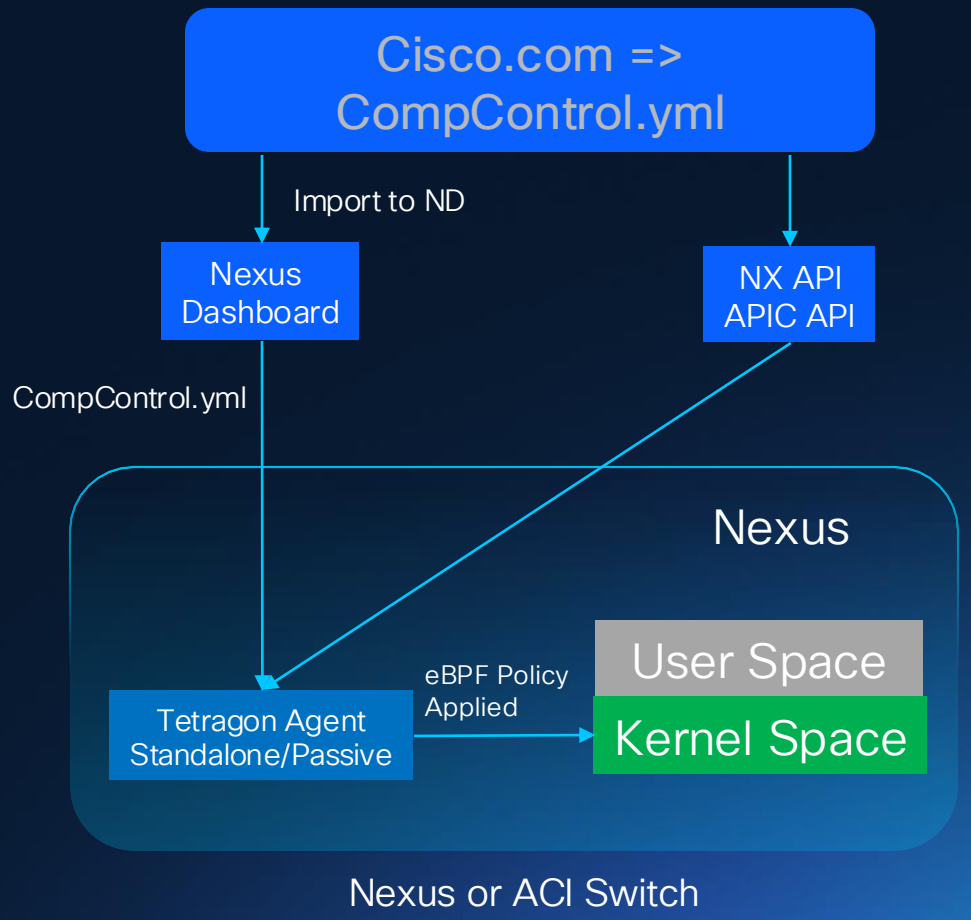
Example Customer: Applies to Nexus fabric customers

Main Benefits

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

Virtual Patching for Nexus and ACI Switches

- PSIRT/CVE Mitigation



Problem:
Customers are facing high OpEx to upgrade 100s of switches for critical PSIRTs/CVEs outside regular maintenance window

Solution:
Provide a virtual patching solution that can mitigate PSIRTs/CVE by patching a live system with compensating controls

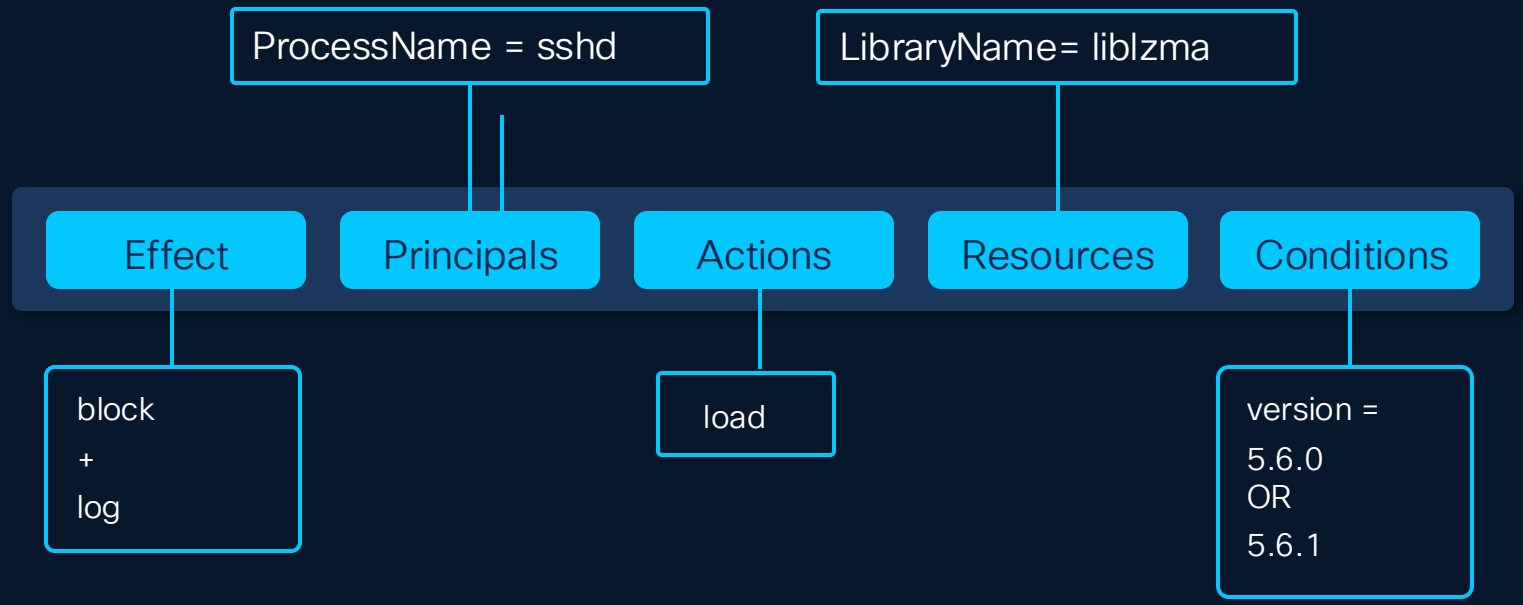
Workflow:

1. All CVE compensating controls (CompControl.yml) are published on cisco.com
2. Tetragon agent is included in NXOS/iNXOS release
3. NX 10.6.1 for demos and GA in NX 10.6.2, ACI 6.2.1 planning
4. Nexus Dashboard, NX-API, or ACI API pushes the compensating controls to Tetragon Agent which applies the eBPF policy to the kernel

XZ Vulnerability Example With eBPF

Natural language:
Do not allow ssh process to load vulnerable XZ library

Hypershield Global Policy:

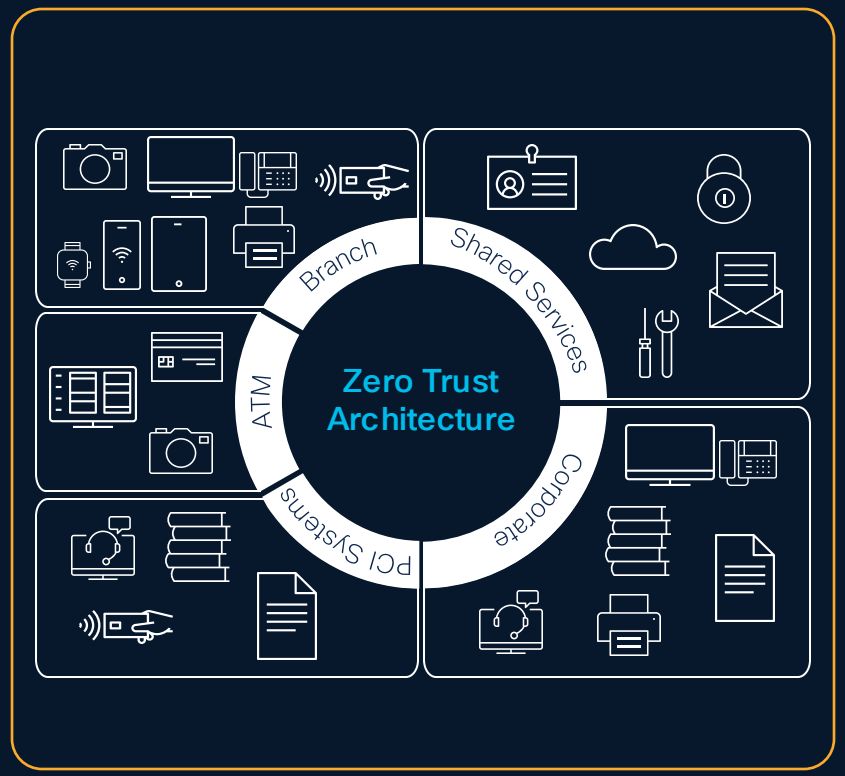


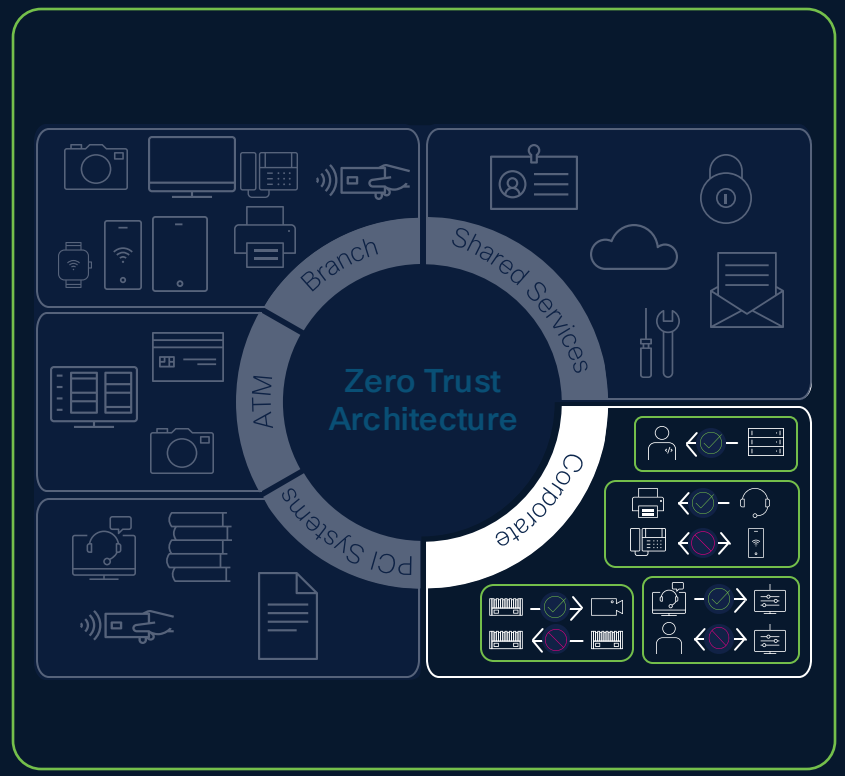
TSA (eBPF policy):

```
selectors:
- matchBinaries:
  - operator: "In"
    values:
    - "/usr/sbin/sshd"
  matchArgs:
  - index: 0
    operator: "Postfix"
    values:
    - "liblzma.so.5.6.0"
    - "liblzma.so.5.6.1"
```

Cisco Secure Workload

Compliance and Reduction of Attack Surface with Microsegmentation





Visibility → Segmentation → Microsegmentation

cisco

Top Segmentation Use Cases

Prevent and block **lateral movement**

Increase operational efficiency by converting NGFWs to **SGT-based SGFWs**

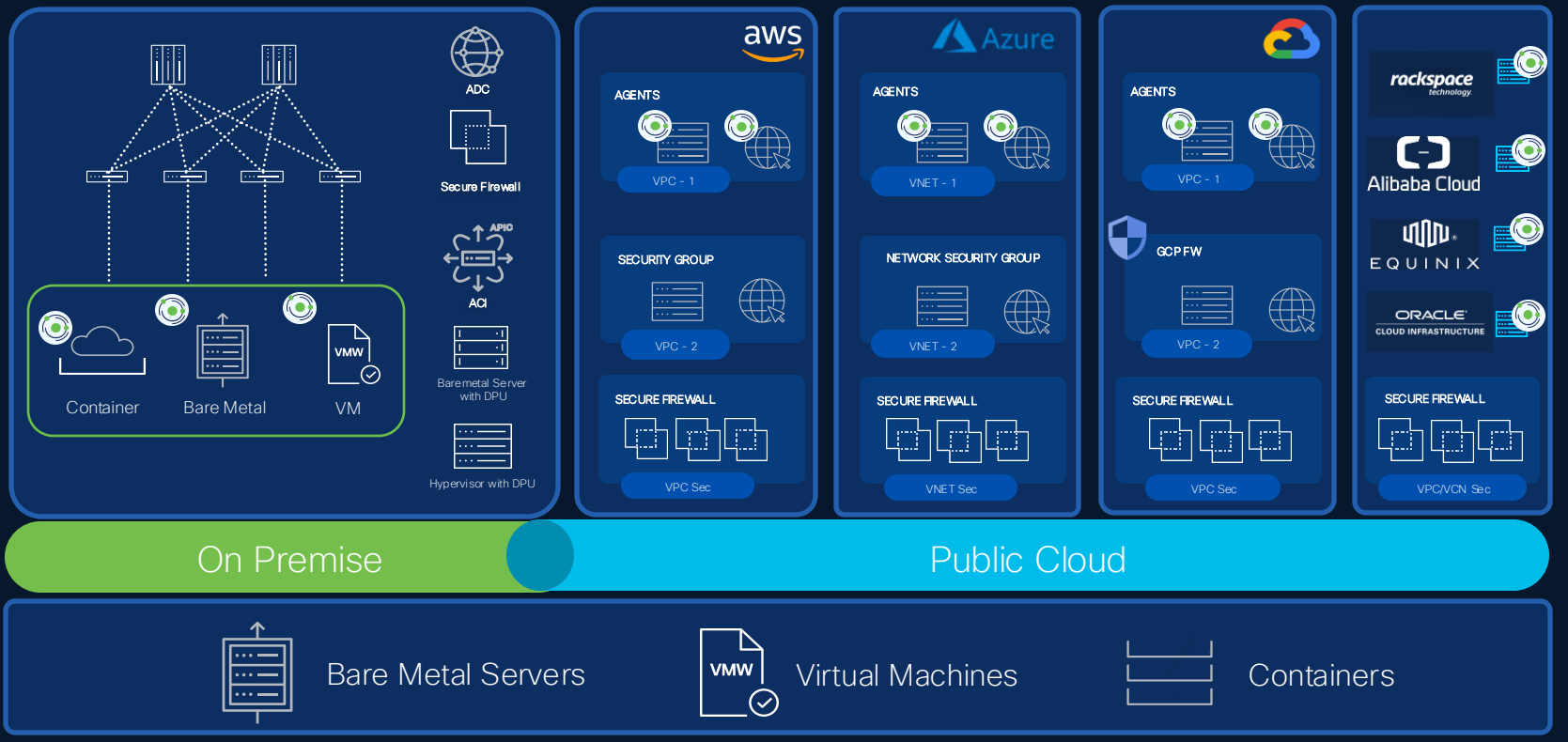
Big Picture

Agent

Consistent microsegmentation from on-premises to the cloud

Agentless

- Anywhere
- Windows Desktop
- Windows Server
- IBM AIX
- Oracle Solaris
- Oracle Linux
- Centos, Rocky, Alma Linux
- Ubuntu, Debian
- SUSE Linux
- RedHat Linux
- Amazon Linux
- OpenShift
- Kubernetes



On Premise

Public Cloud

Bare Metal Servers

Virtual Machines

Containers

- On-Prem
- Loadbalancer (ADC)
- Firewalls
- Data Center Fabric (SDN)
- NVIDIA Smart NIC (DPU)
- AWS, GCP, Azure
- Security Group
- Network Security Group
- Cloud Network Firewall
- Multicloud Defense*

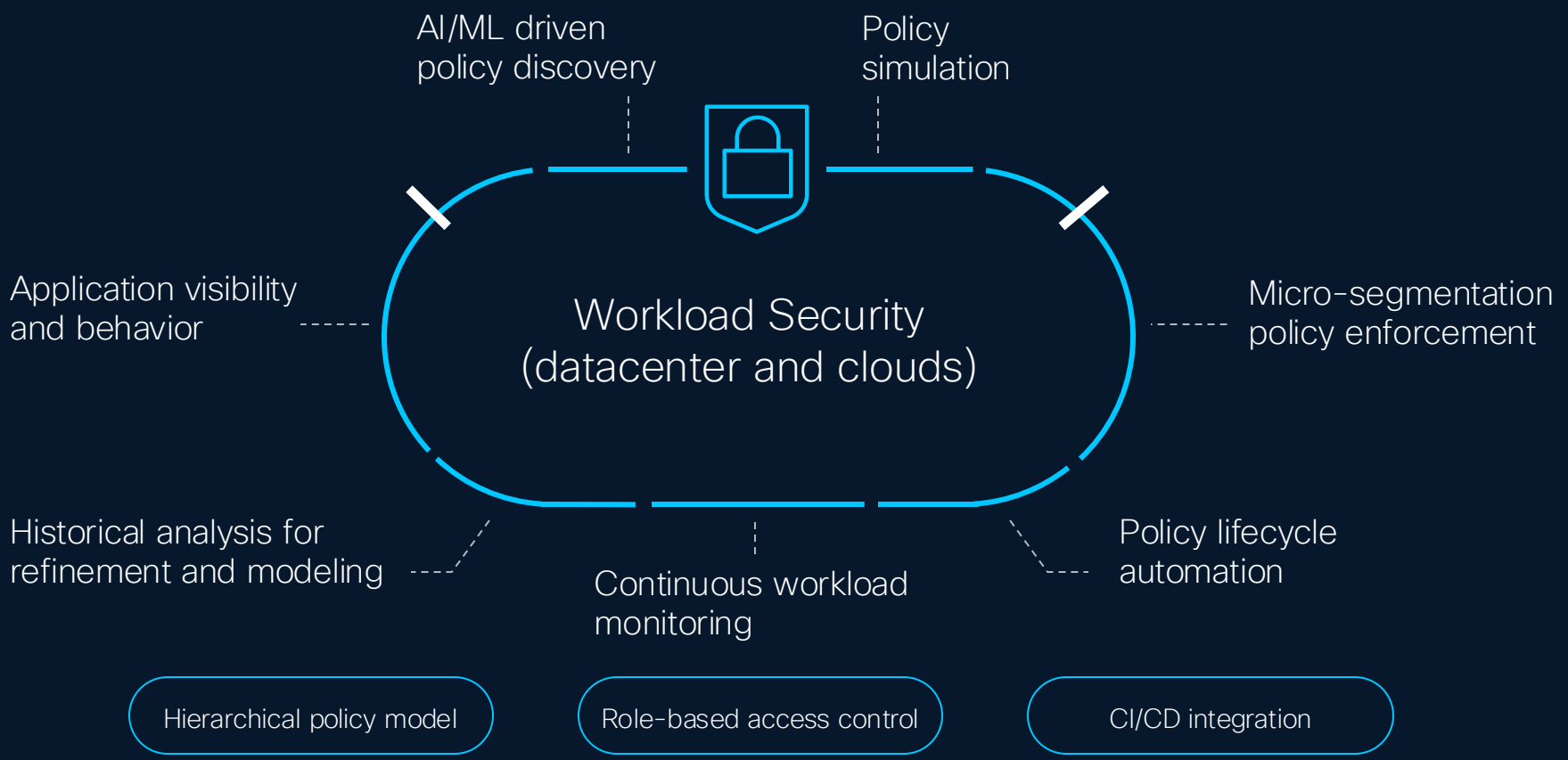
User Identity | Tags and Labels | Vulnerability

Threat Feed | Application Encryption | Domain/FQDN | Cisco Security Risk Score

cisco

* - In Roadmap

Secure Workload



Stop lateral movement

Zero trust microsegmentation protects application workloads across the data center and clouds from one solution

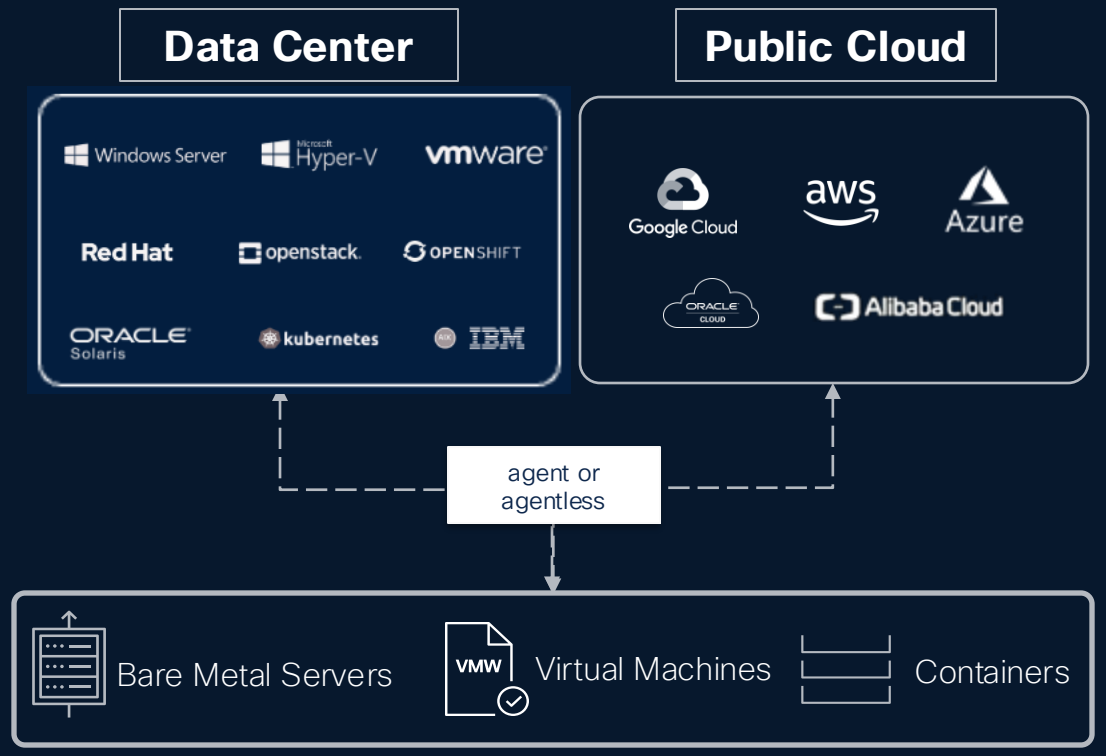
Quickly improve security posture

Understand application behavior and enact best-practice hardening policies such as blocking insecure app to app communications

AI/ML tackles tasks that are beyond human scale

Powerful AI/ML driven policy discovery recommends policies tailored to the unique environment and automation ensures consistency and accuracy

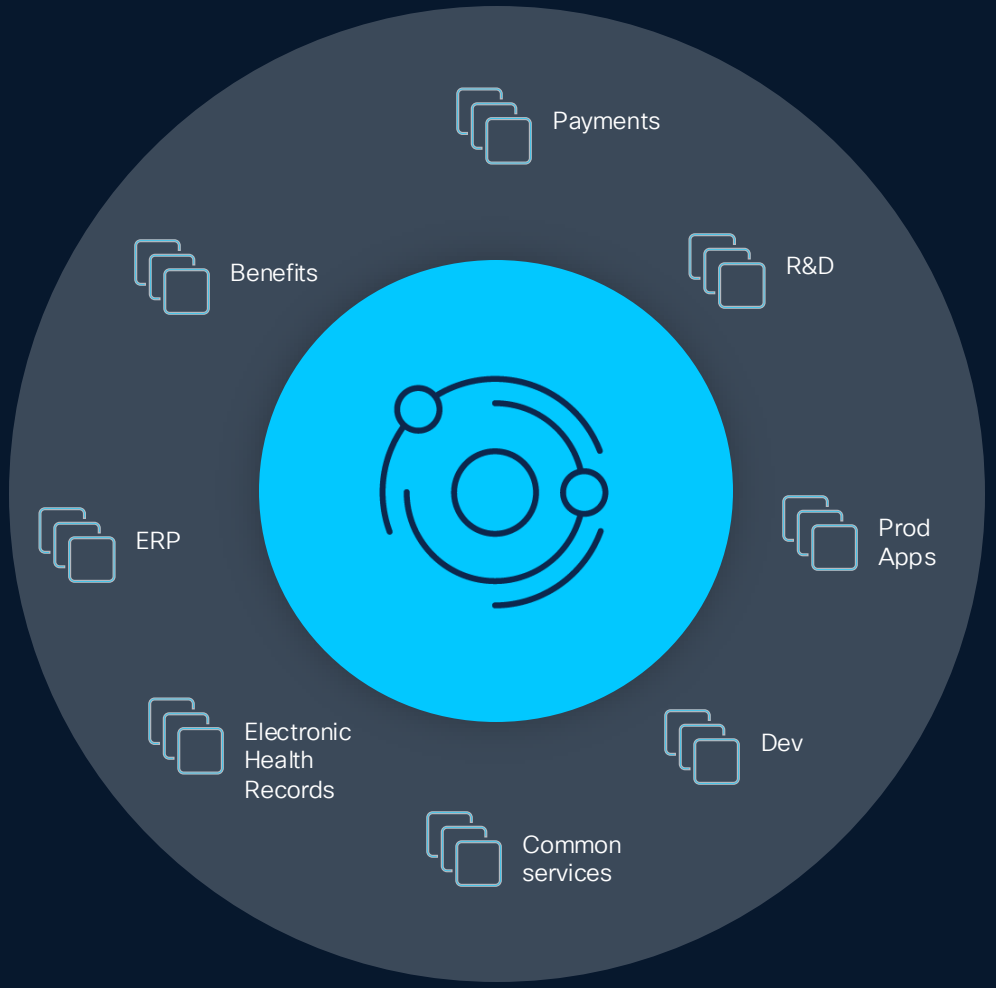
Visibility



- ✓ Discover applications, identify interactions, and understand vulnerabilities
- ✓ Discover applications across on-prem data center, public and private cloud with agents and/or agentless approach
- ✓ Get process-level visibility into Microsoft Windows, Linux, Solaris, AIX, and Container infrastructure
- ✓ Agentless discovery through pre-built integrations with hypervisors, cloud providers, CMDB, IPAM, IDP, DNS, VMM, etc.

cisco

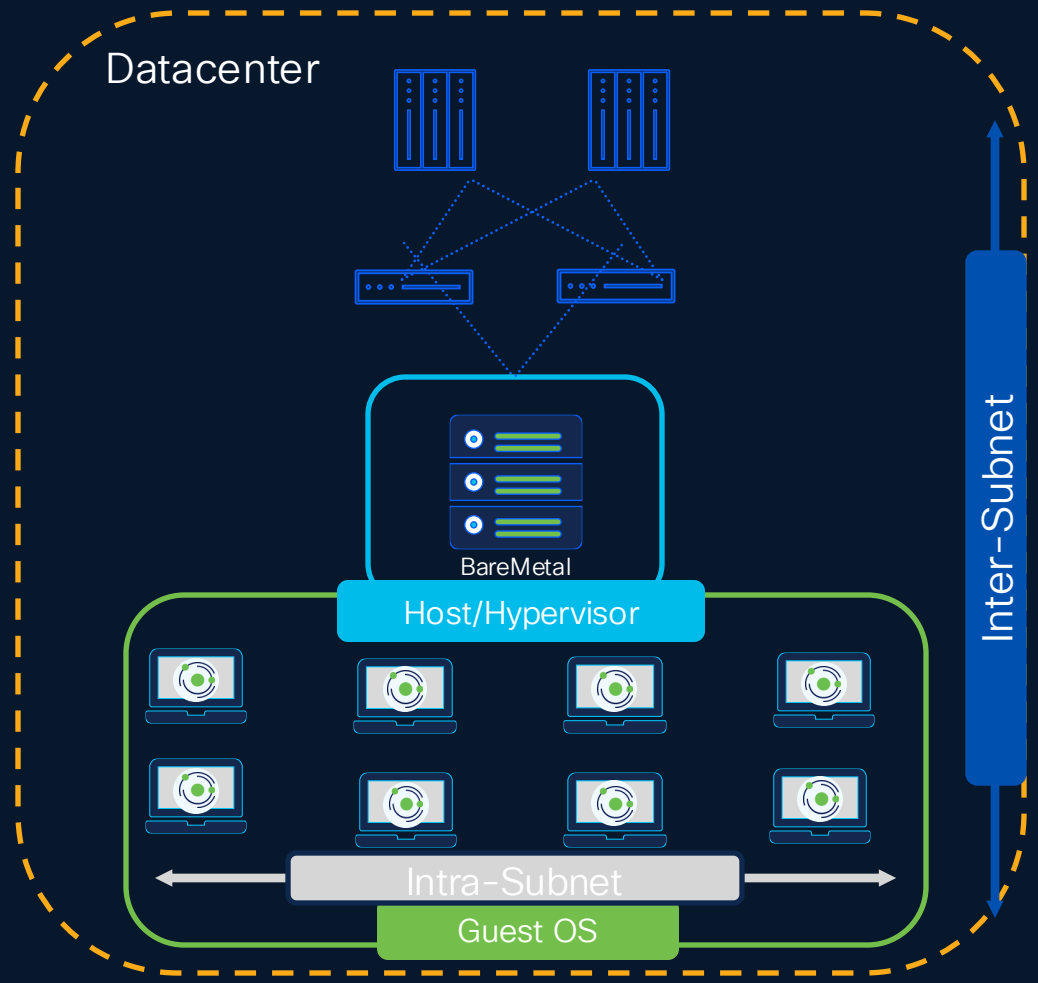
Application Protection



- ✓ Enforce micro-segmentation throughout the network stack: SDN, edge firewall, subnet, application
- ✓ Use vulnerability risk score for access policies to change
- ✓ AI/ML-driven policy review to eliminate stale or overlapping policies
- ✓ Use policy templates to accelerate micro-segmentation aligned with NIST and CISA frameworks

cisco

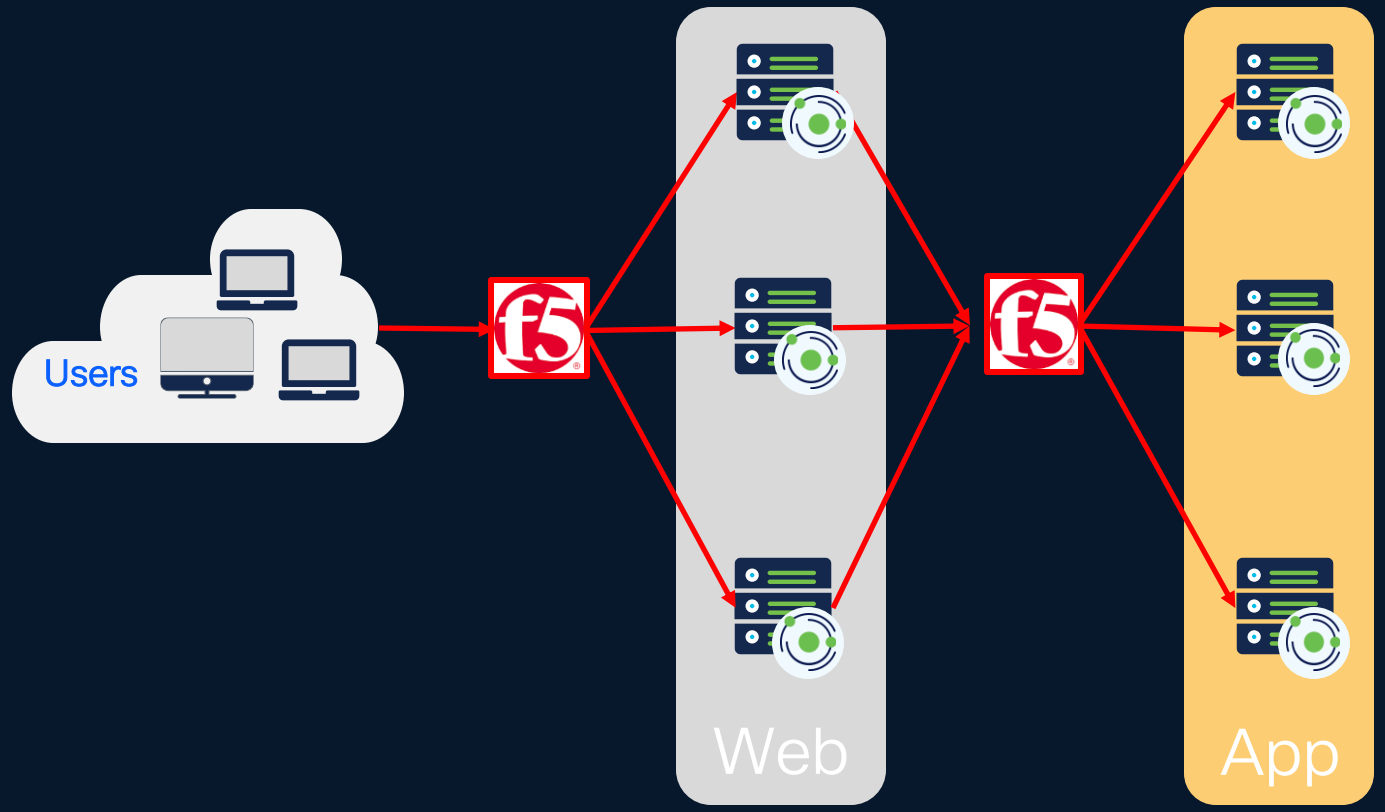
Virtual Desktop Infrastructure Microsegmentation



Host-Based Agent VDI Microsegmentation

- Same agent as for workloads
- Ideal for fine-grained segmentation
  - In-depth endpoint visibility
  - Protection at the VDI user/desktop level
- Suitable for **all personas**

Load-Balancer Services



Load-Balancers Services Protection

- LB services discovery and telemetry
- Provides end-to-end protection
- LB services with agentless integration
  - VIP/SNAT

Cisco on Cisco

webex by CISCO

Key Highlights

- Largest Secure Workload deployment
- Visibility & microsegmentation for VM and containerized workload
- Global hybrid multicloud workload deployment

WebEx Environment

- 200K workloads across 5 production applications
- Workload deployed - AWS, GCP, and On-prem globally
- 180K VMs and 21K Container Node

Use cases

- Visibility and automated policy lifecycle management
- Segmentation and microsegmentation
- Forensics and vulnerability management

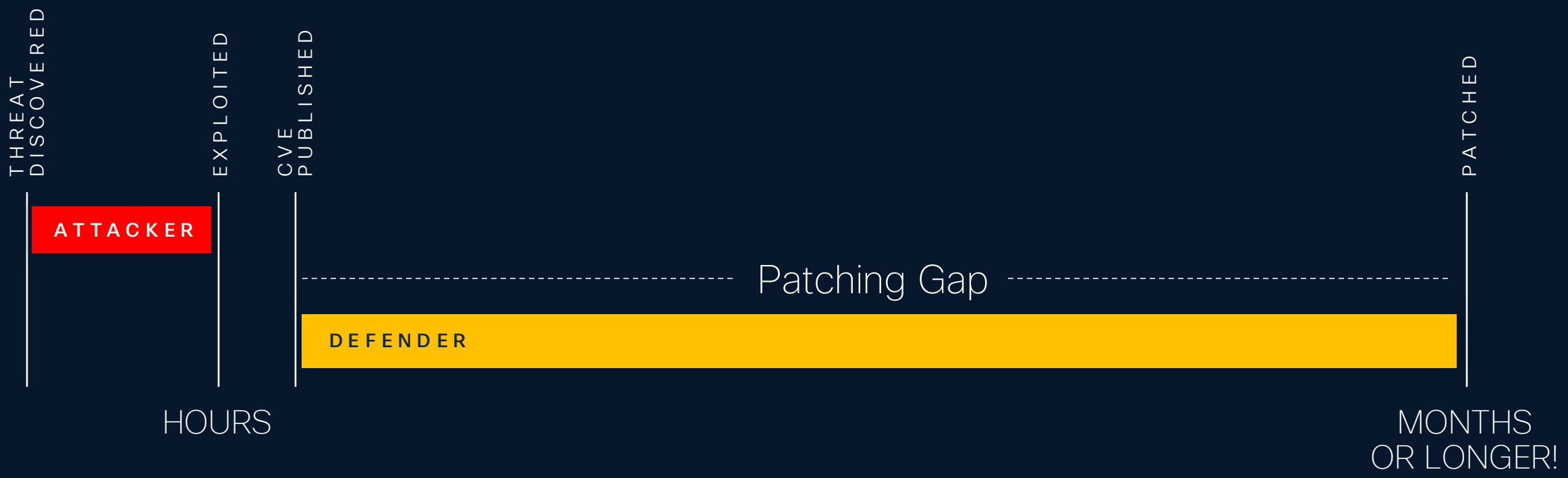
Journey so far and timelines

- P1 Oct 2022: WebEx calling App – 9K workloads (VM)
- P2 Dec 2022: SPLAT and KUBED App – 7K+14K workloads (containers)
- P3 Dec 2023: Scale to 200k workloads

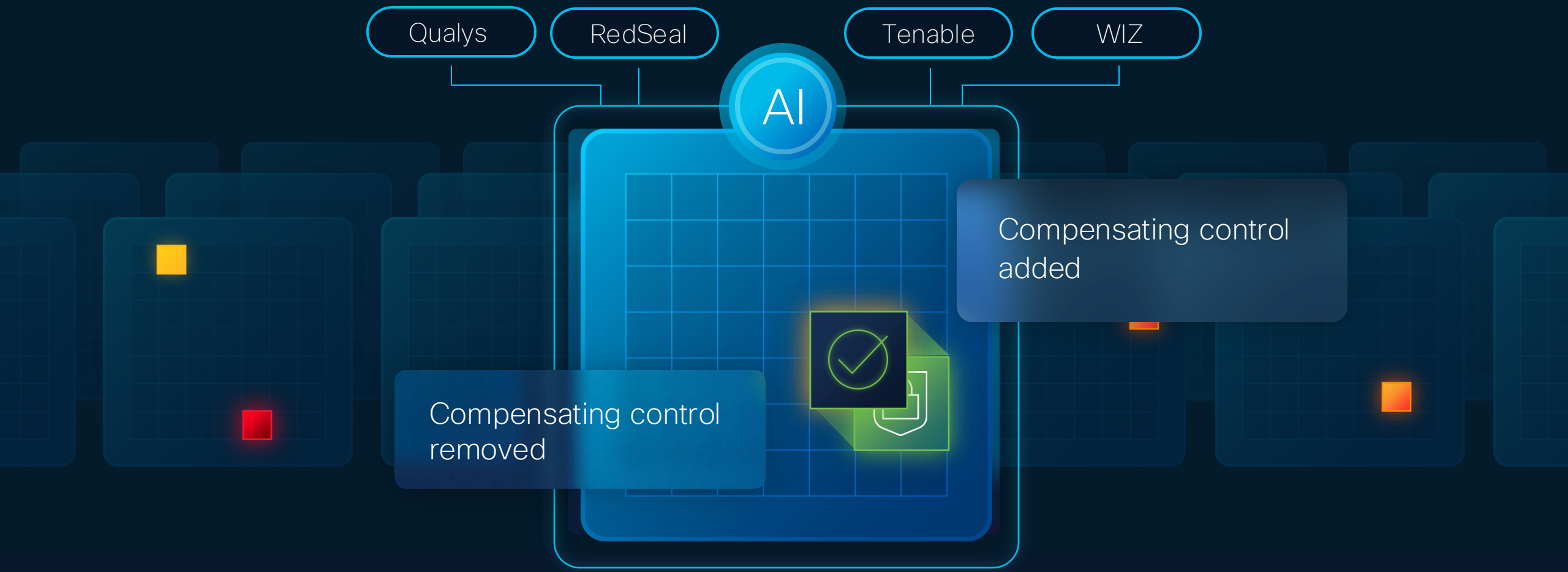
cisco

Hypershield

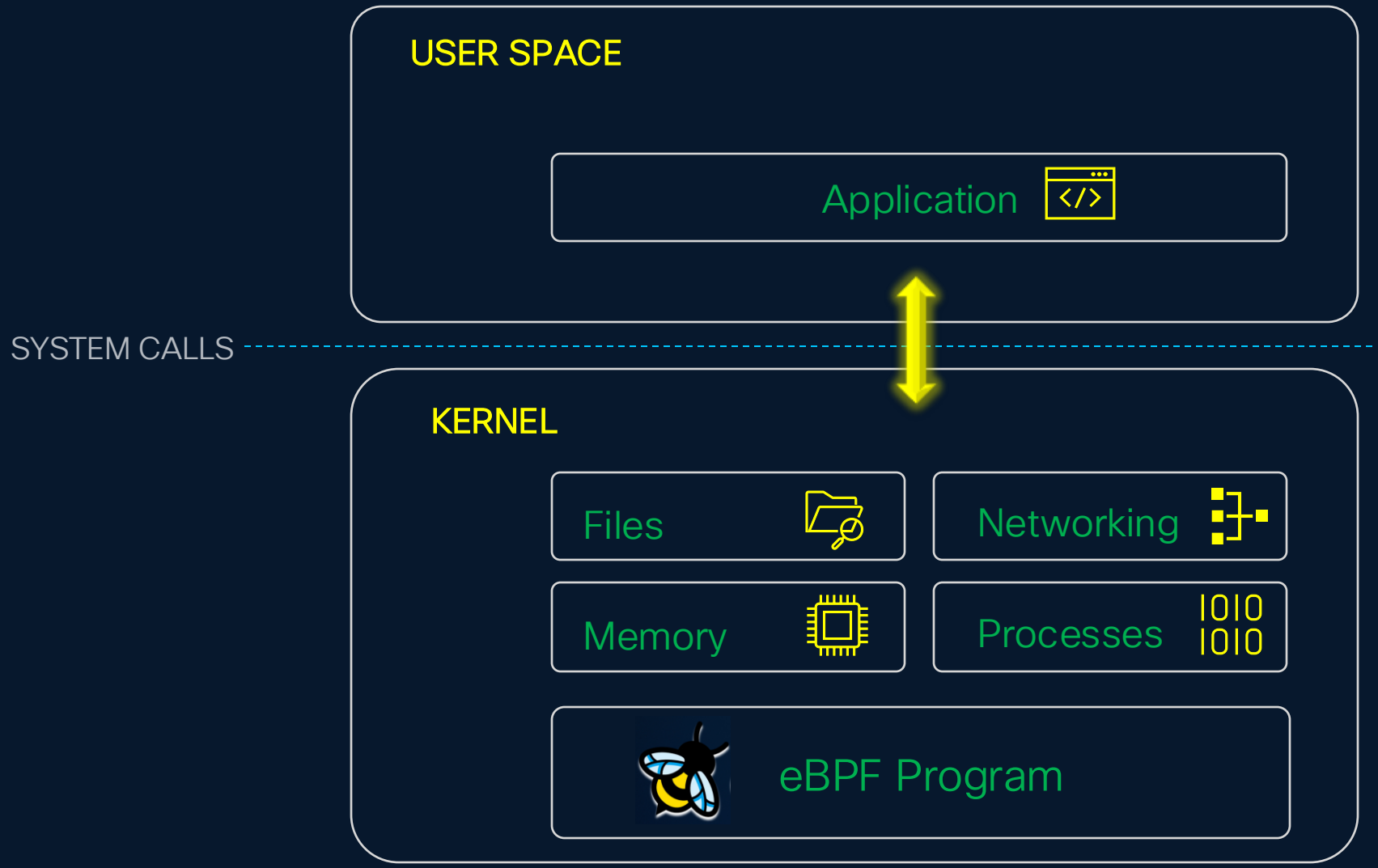
Patching Is Hard



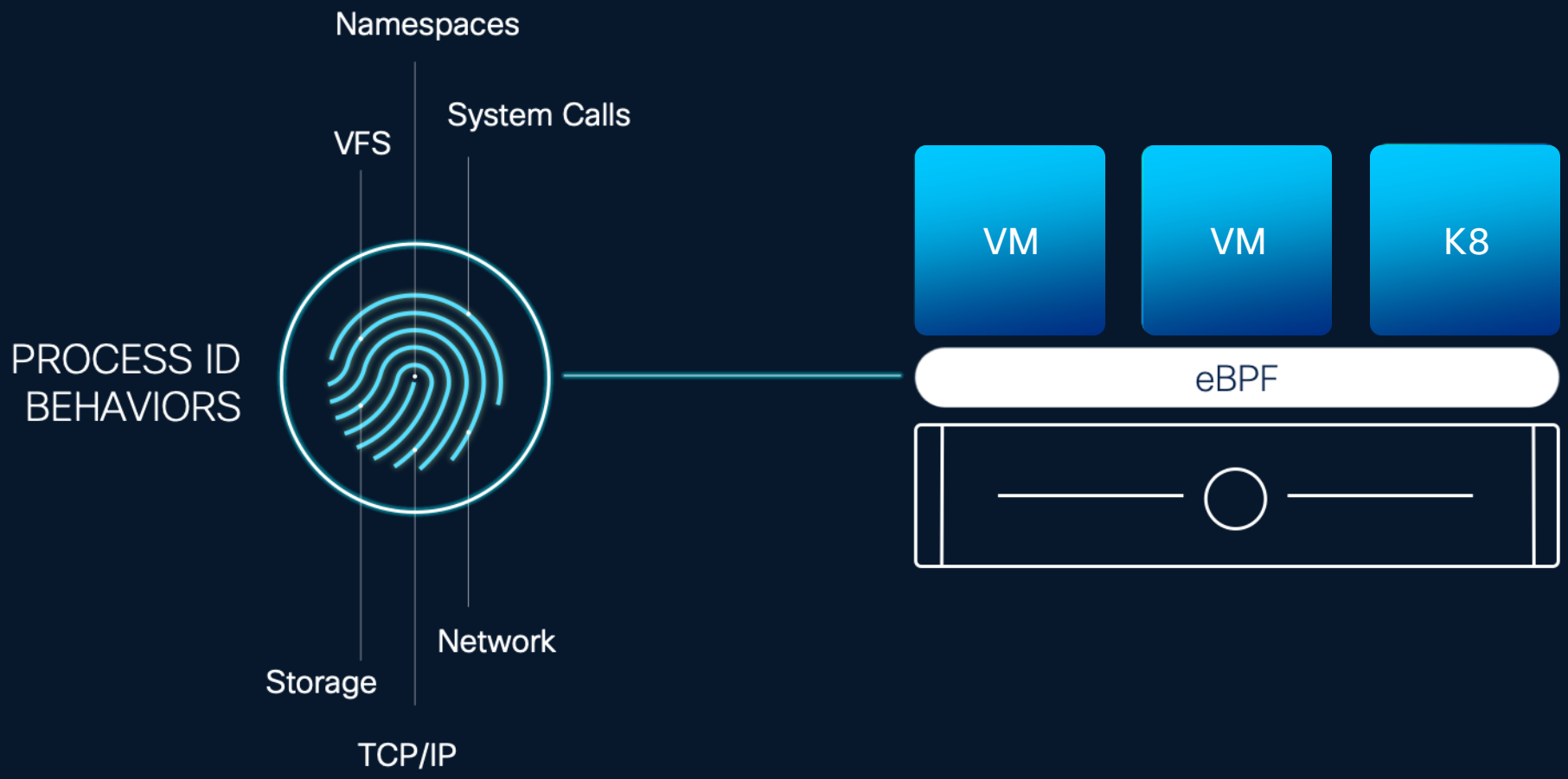
Distributed Exploit Protection



Hypershield Building Blocks – eBPF



eBPF Provides Visibility Deep Into the Workload



We Also Understand Things

OS version | Mac ID | OPSWAT checks | DHCP | Traffic flows | DNS and certificate

Hypershield Building Blocks – eBPF

Source: https://isovalent.com/blog/post/2021-08-ebpf-foundation-announcement/

Customers in Every Industry Use eBPF in Production

Google uses eBPF for security auditing, packet processing, and performance monitoring

Netflix uses eBPF at scale for network insights

Android uses eBPF to monitor network usage, power, and memory profiling

S&P Global uses eBPF through Cilium for networking across multiple clouds and on-prem

Shopify uses eBPF through Falco for intrusion detection

Cloudflare uses eBPF for network security, performance monitoring, and network observability

Recap

1. Many ways to drive security deeper into the DC
2. Complexity varies with method
3. Dynamic service insertion offers flexibility to scale
4. Agents give new levels of ability for supported workload
5. Cisco NG DC security offers common policy for DC workloads regardless of endpoint type

CISCO Connect

Thank you


CISCO