

Segmentation Untangled

Streamlining Hybrid Data Center Security

Jamey Heary
Cisco Chief Security Architect, DSE



Zero Trust Use Cases



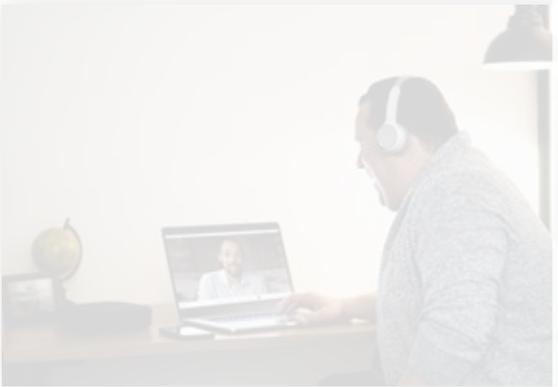
Admin
Access

Remote
Worker

On-Premise

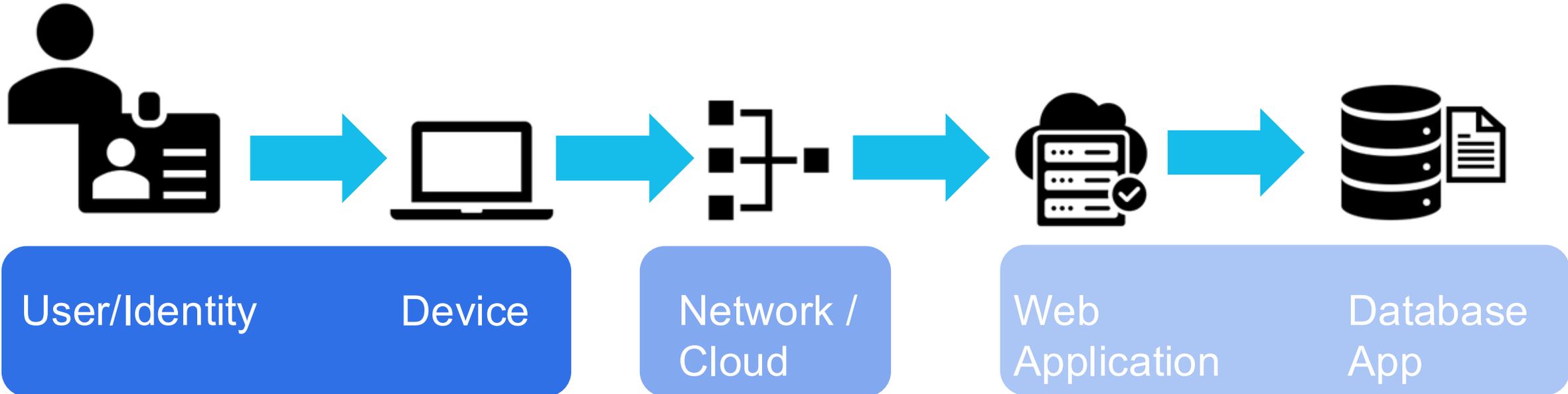
Application to
Application

Application to
Model



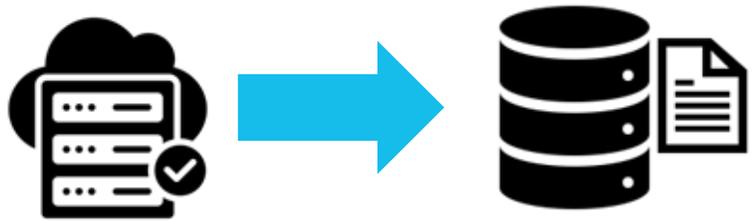
Zero Trust End to End

User to App, App to App



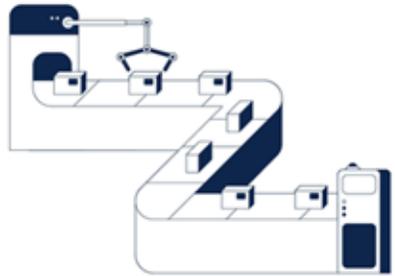
Zero Trust App to App/Service

Is it this Simple?



Web Application Database App

Zero Trust Use Case Detailed Examples

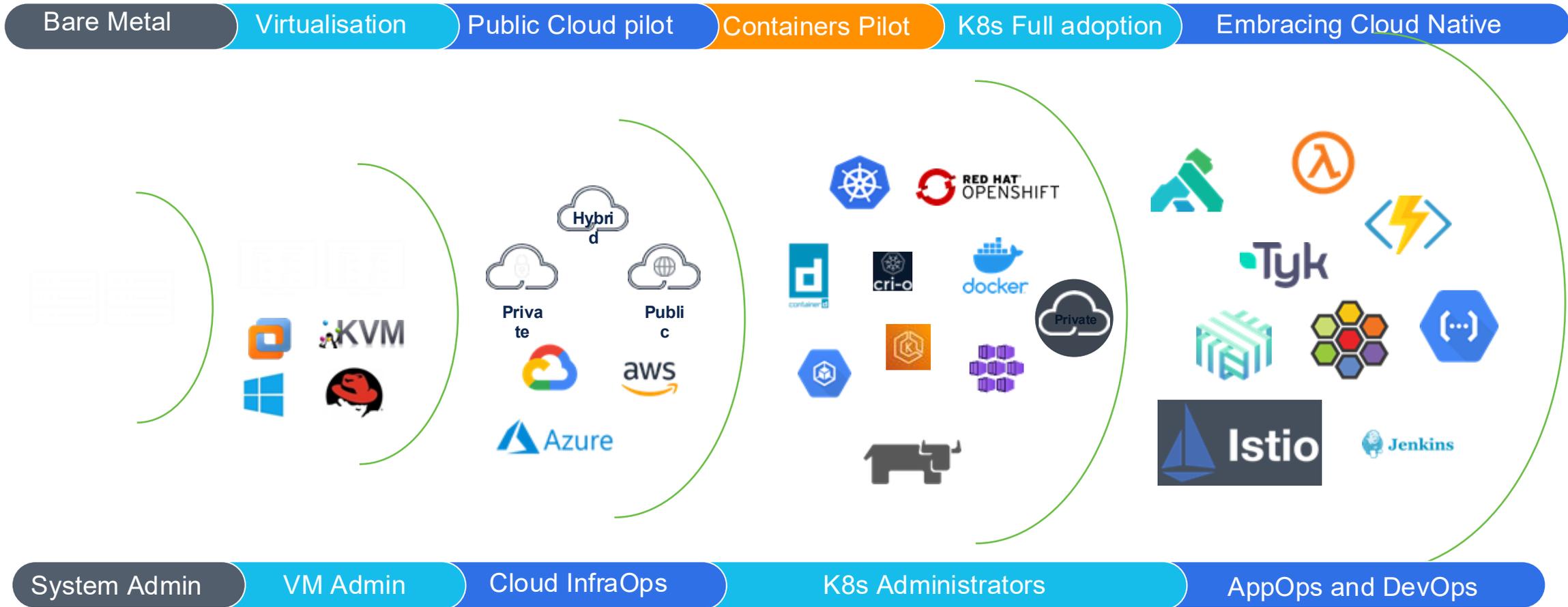


App-to-App

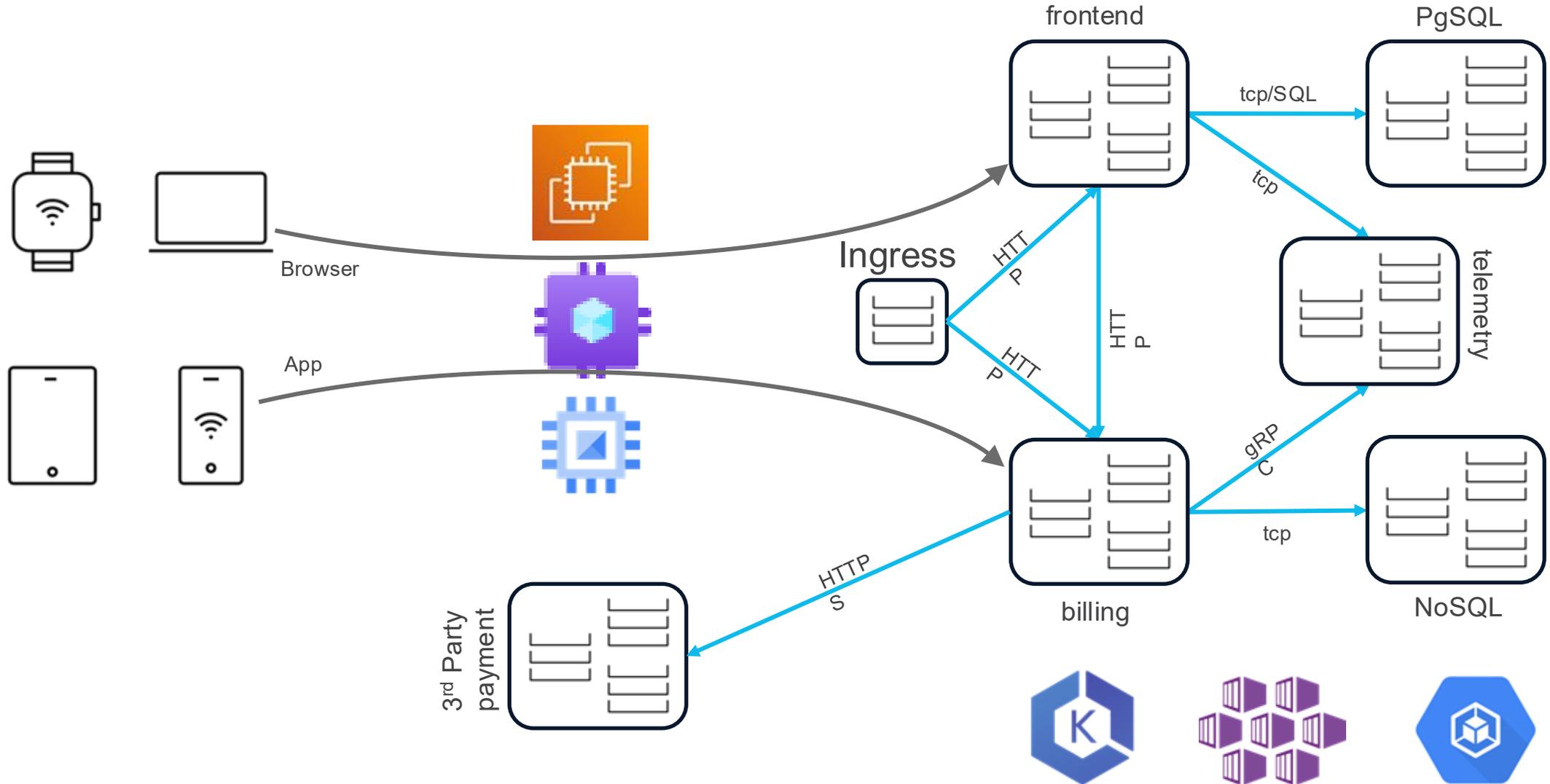


- App-to-App Inter multi-cloud
- App to app intra zone
- App to Internet
- App to API/public app SaaS
- Apps to/with GenAI Model

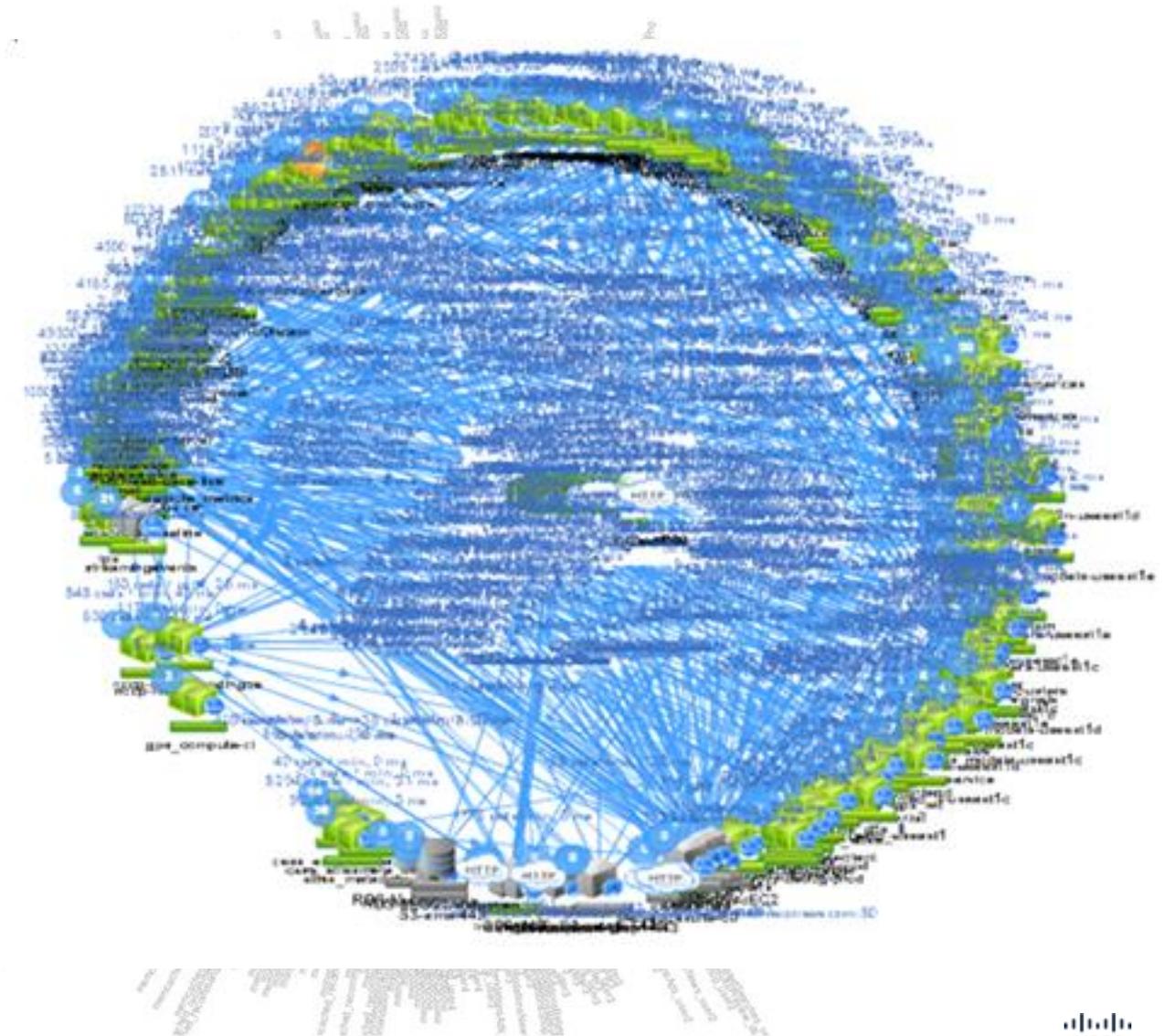
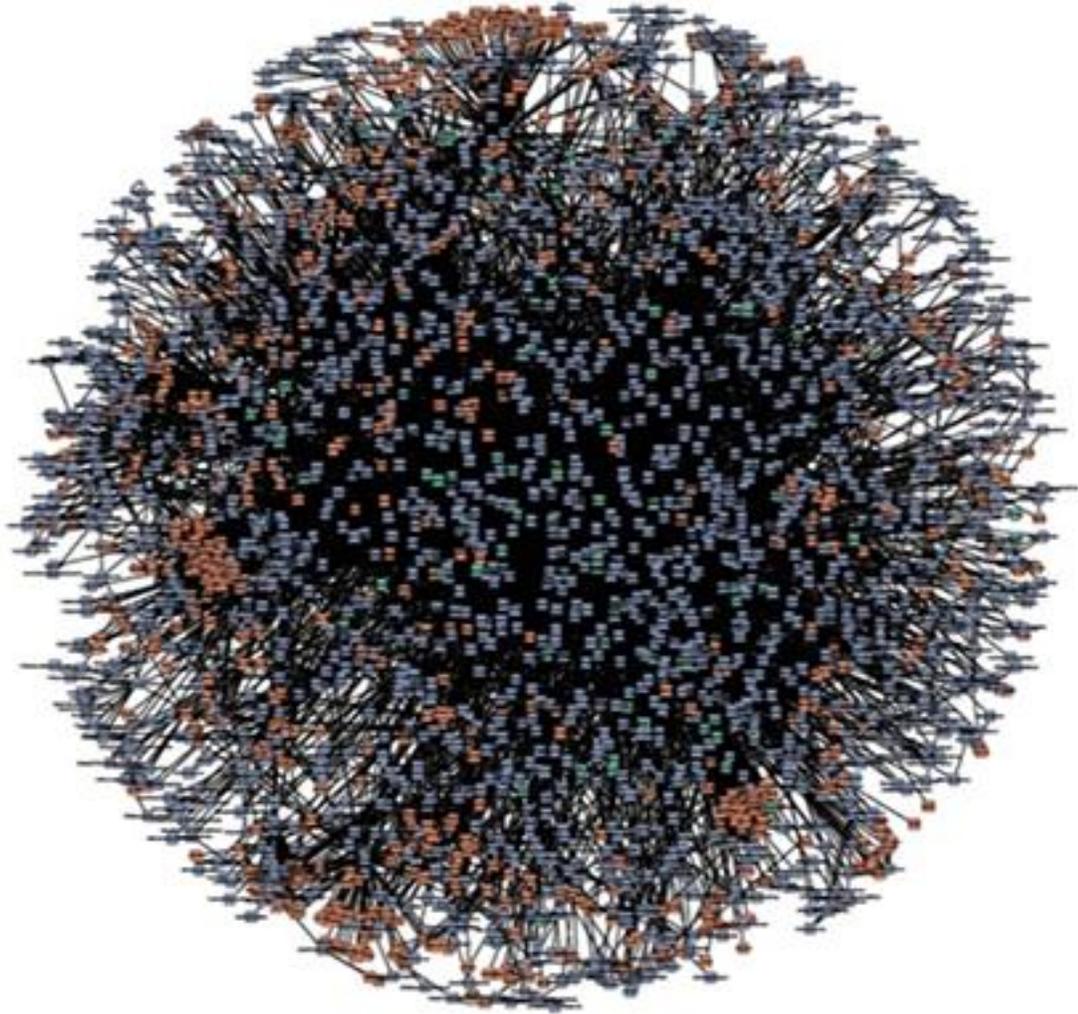
Application workloads evolution



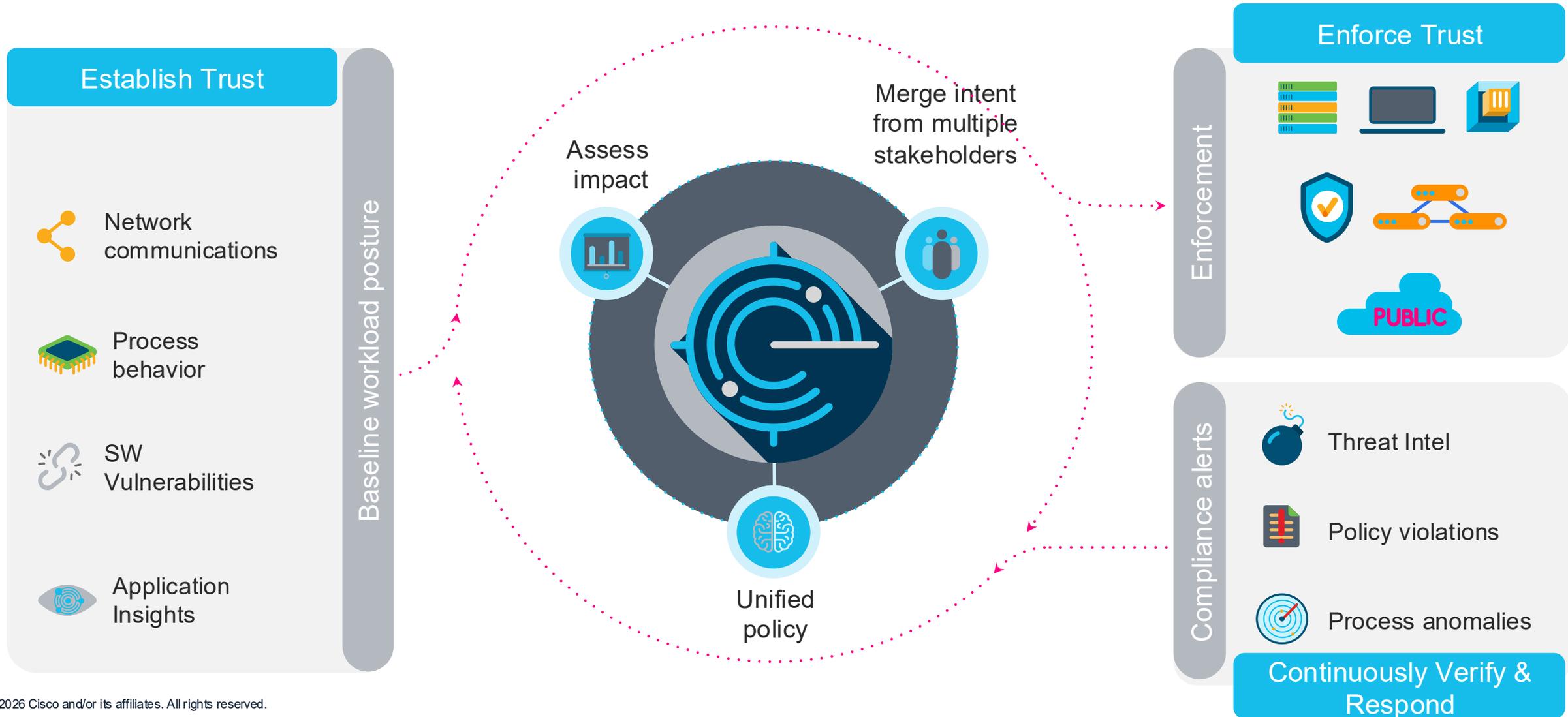
Simple Modern Application



Their dream is your nightmare



Achieving Zero Trust for Modern Applications



Hybrid Cloud Zero Trust Segmentation

Defense in Depth via Hybrid Mesh of enforcement points

Edge Firewall



Secure Firewall



Multicloud Defense

Macro-Segmentation



ACI



Secure Firewall



Secure Workload



Micro-Segmentation



Secure Workload



tetragon

Hypershield



cilium

Unified Segmentation

Perimeter Defense

- Ingress & Egress Security
- Threat inspection at the data center or cloud edge.

Zones

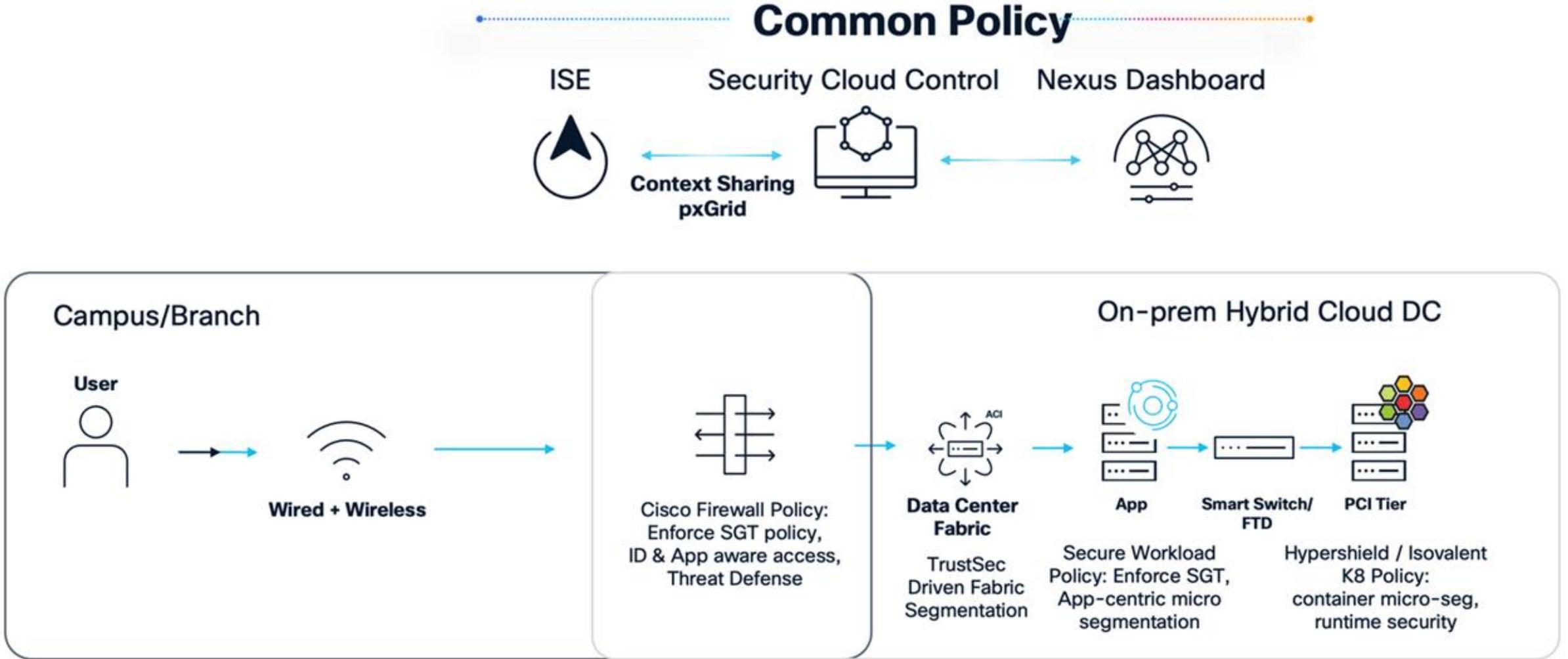
- Segment zones within your data center and cloud.
- Supplementary coverage for workloads without agents.

App Segmentation

- Zero trust micro-segmentation enforcement at the workload
- Automated policy discovery and compliance

Hybrid Cloud Security

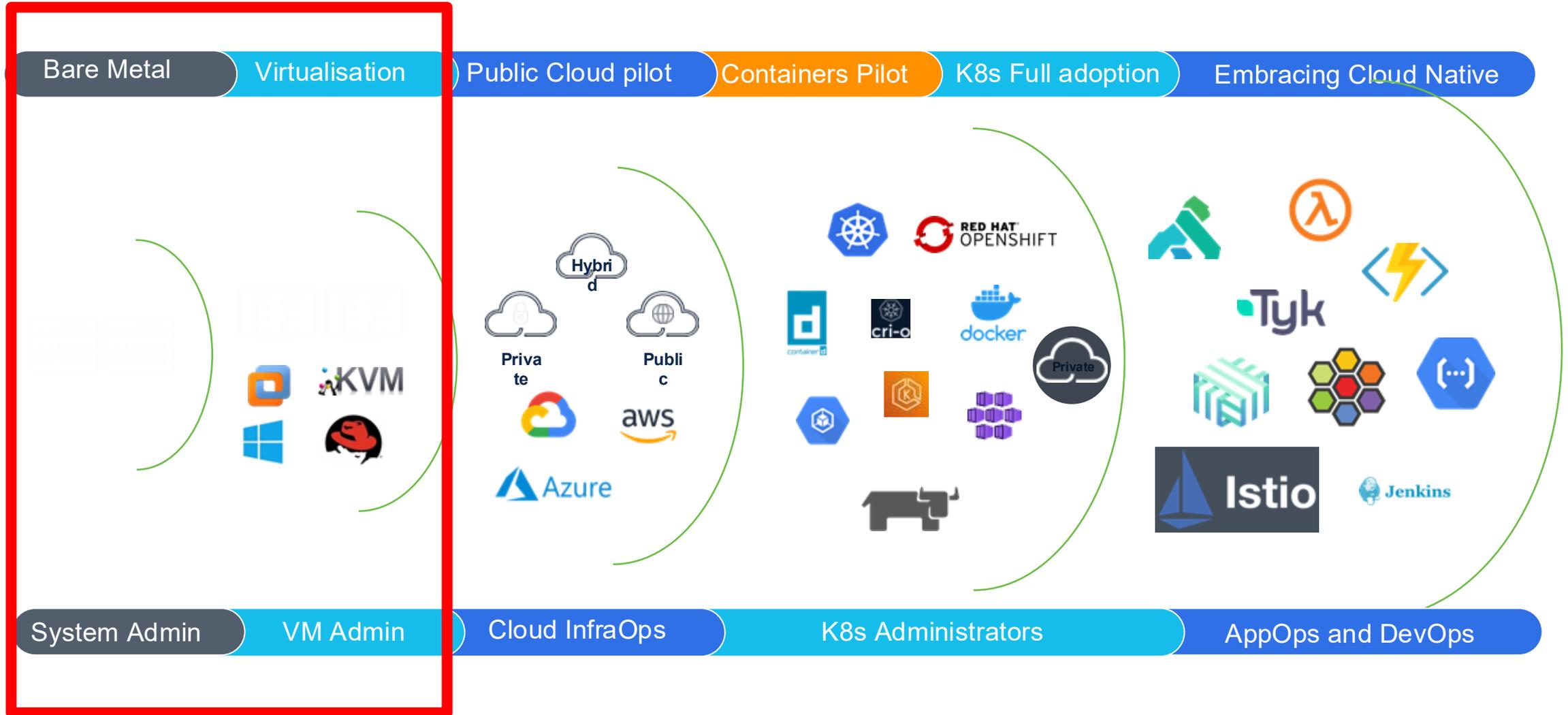
Zero Trust



Common Security Operations (Splunk / XDR)

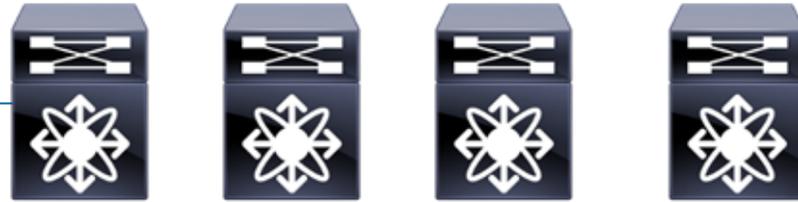
Common Data Center Operations

Application workloads evolution



Enforce Trust in the DC with Cisco ACI

Spine Nodes



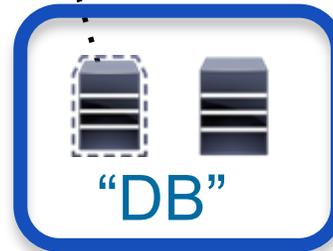
Leaf Nodes



Service Producers

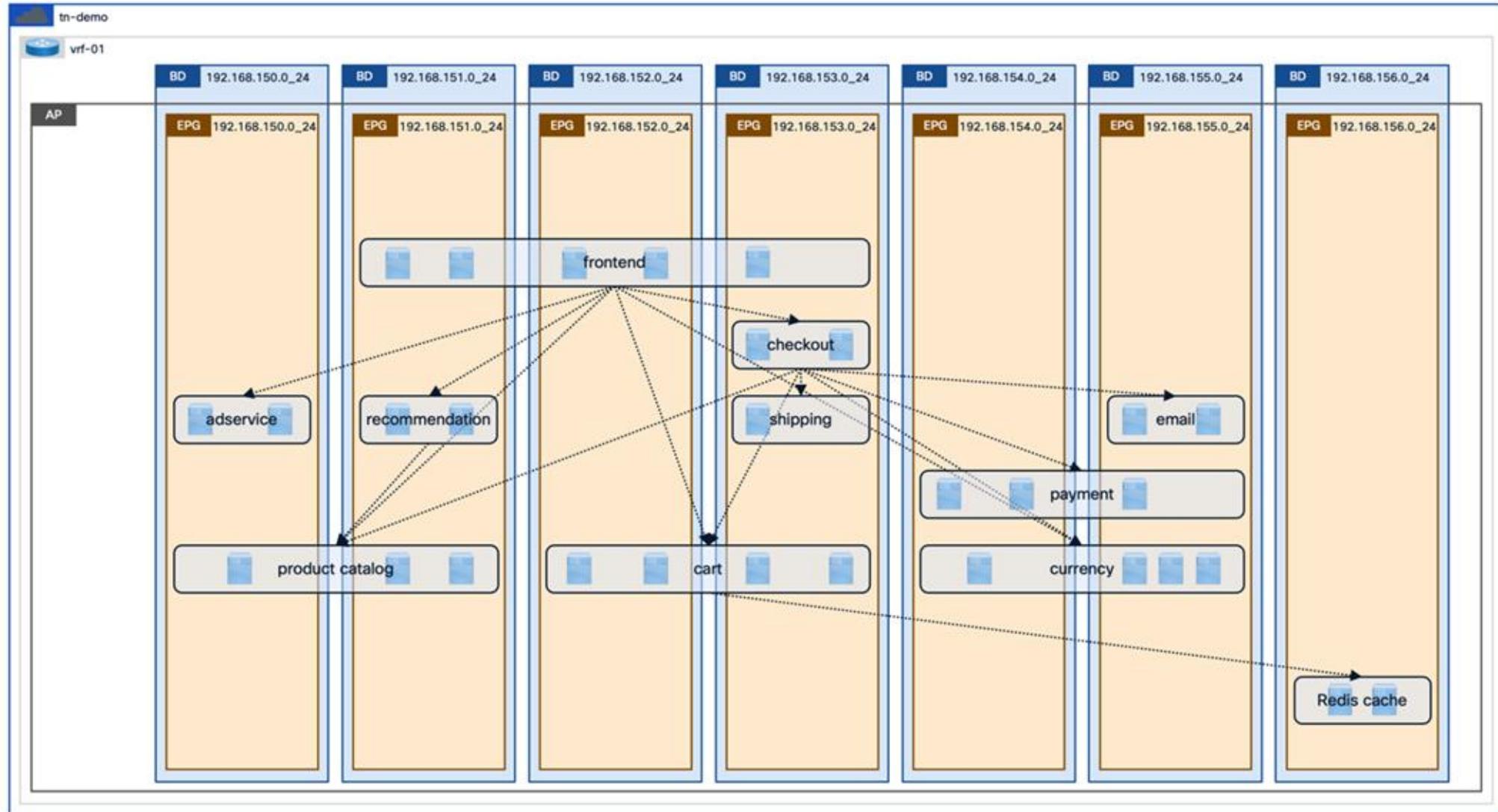


APIC Controller

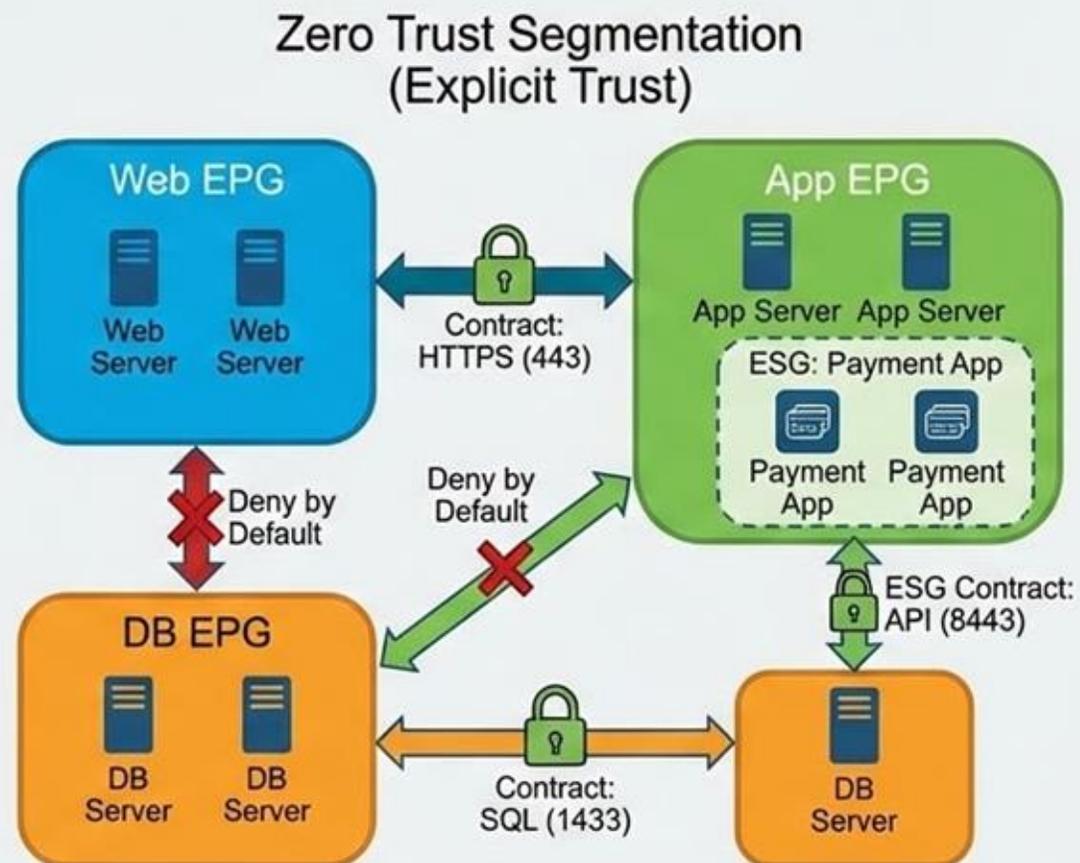
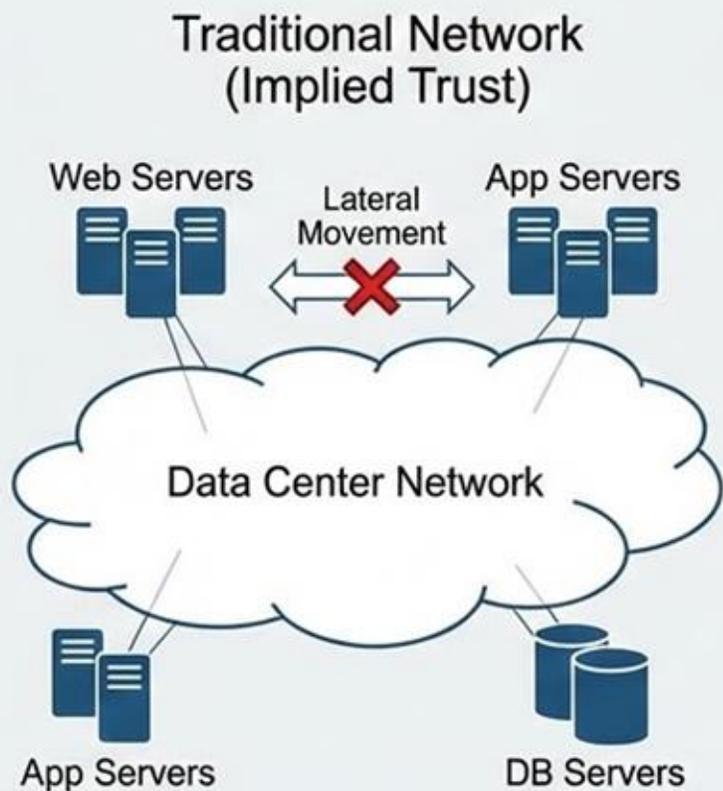


Service Consumers

Is subnet the right way to establish trust groups?



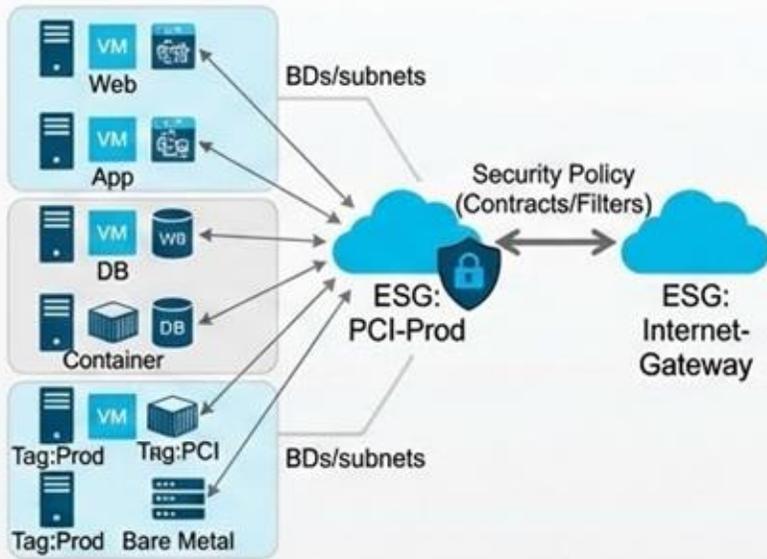
Zero Trust Segmentation in the Data Center: EPGs, ESGs, and Contracts



EPG = Endpoint Group (Logical Grouping)
ESG = Endpoint Security Group (Micro-segmentation)
Contract = Policy (Allowed Traffic Only)

Endpoint Security Groups (ESGs) vs. Endpoint Groups (EPGs) in Cisco ACI

How ESG Works



- Logical grouping for security, independent of network topology (BDs, VRFs).
- Membership defined by attributes (tags, VM labels, OS type, etc.).
- Enforces security policies (contracts) based on these logical groupings.
- Enables fine-grained micro-segmentation.

Differences from EPG

Feature	EPG vs. ESG	
Grouping Basis:	EPG: Network-centric (Subnet/VLAN/IP).	ESG: Attribute-centric (Tags, Labels, Identity).
Network Dependency:	EPG: Tightly coupled to BD & VRF.	ESG: Network-agnostic, decoupled from BD.
Segmentation Level:	EPG: Coarse-grained (Network Segment).	ESG: Fine-grained (Micro-segmentation).
Policy Scope:	EPG: Intra-EPG communication allowed by default (unless isolated).	ESG: Strict policy enforcement, zero trust model.

Why Use ESG instead of EPG



Decouple Security from Network: Define security policies without constraints of network addressing or topology changes.



Simplify Dynamic Environments: Ideal for containers, cloud, and highly dynamic workloads where IPs change frequently.

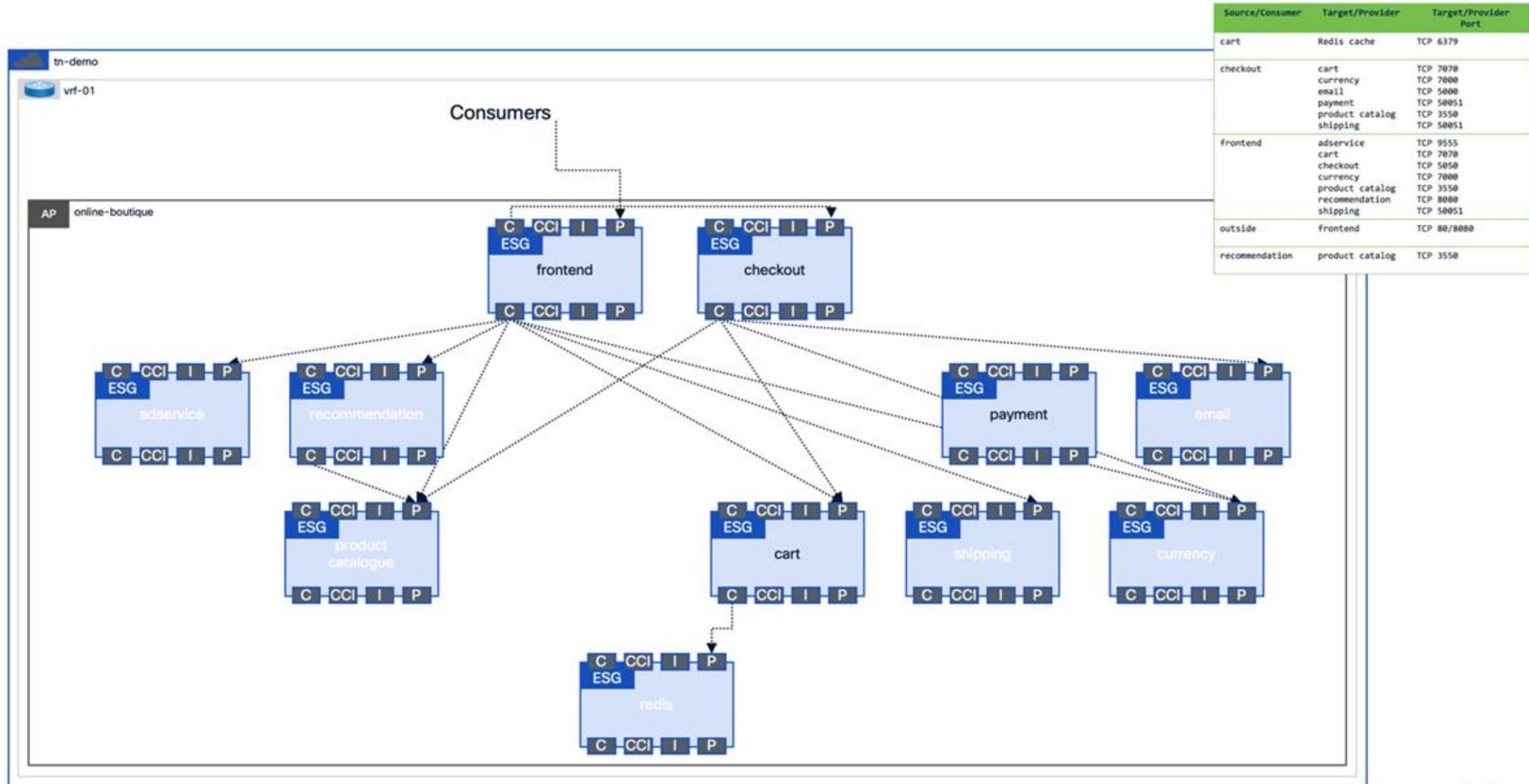


Granular Micro-Segmentation: Achieve zero trust by grouping workloads based on business function and security posture, not just location.



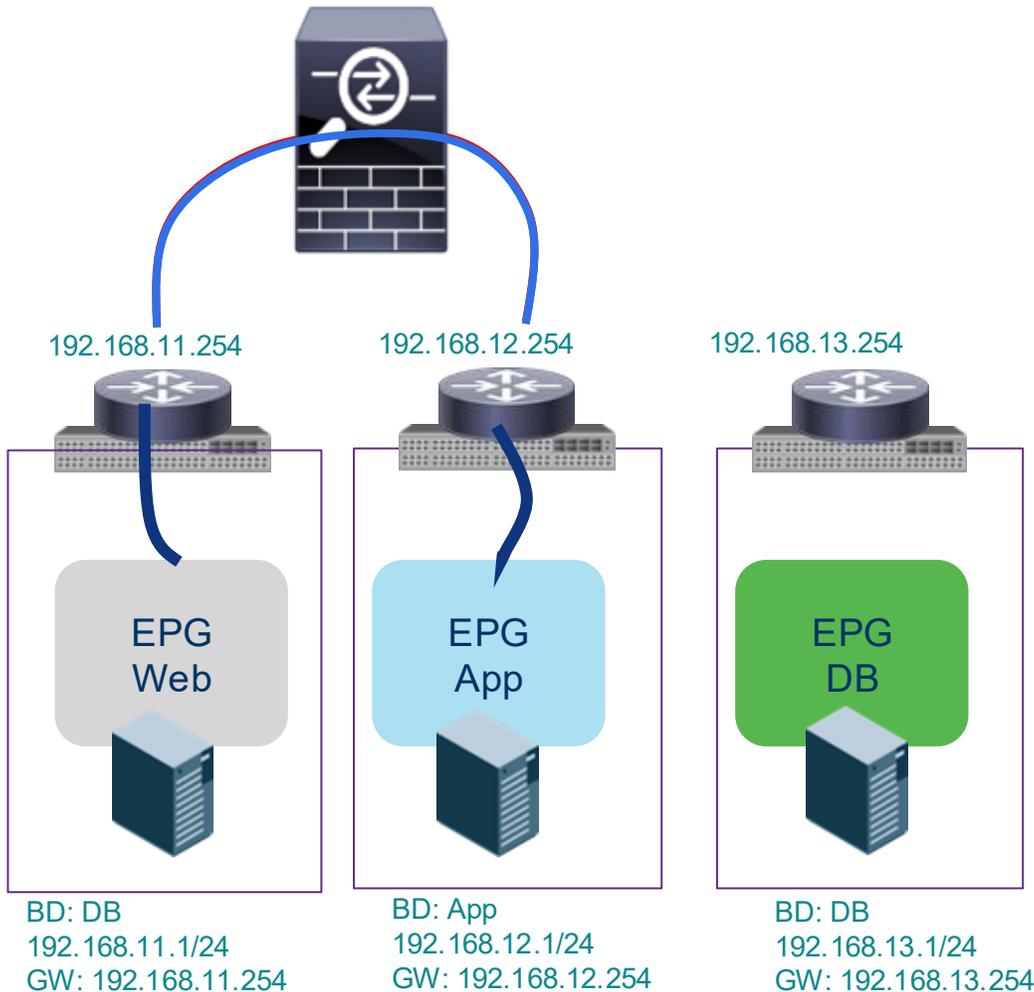
Unified Policy Model: Apply consistent security policies across different infrastructure types (on-prem, cloud, hybrid) using attributes.

Network agnostic endpoint security groups (ESGs)

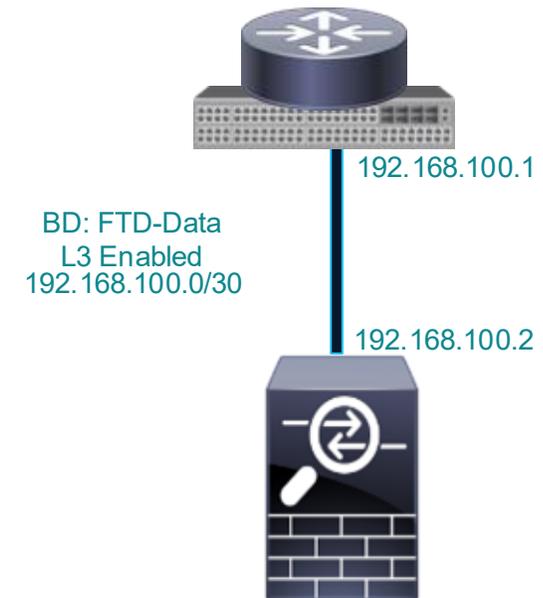


Policy Based Redirect to insert security services like NGFW

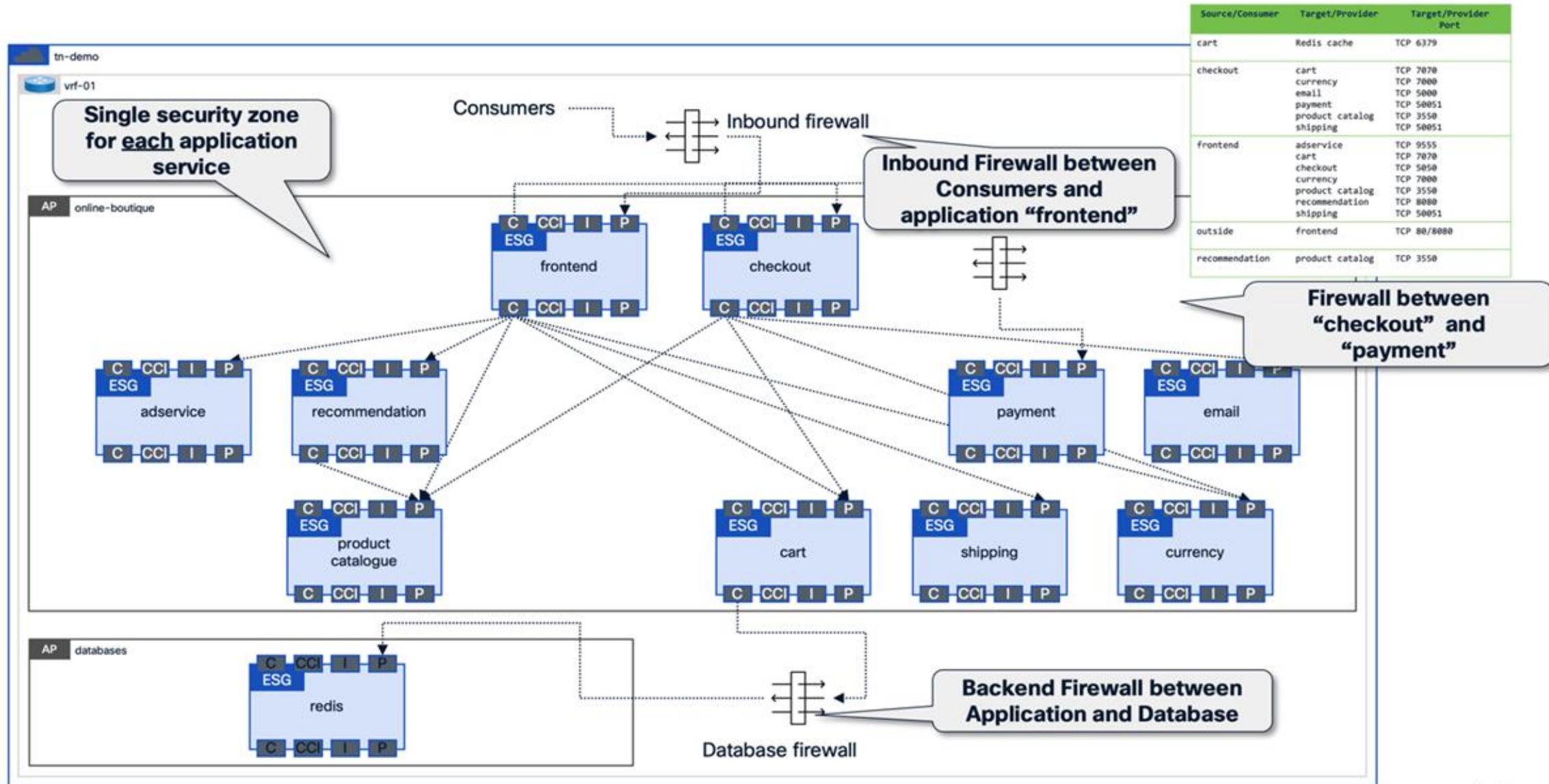
With PBR Service Graph



PBR redirects the traffic matching the **contract(s)** to the **Security Service**



Complement ACI Contracts with Firewalls



Establish Trust - FTD/ASA can leverage SGTs

Action: Block Time Range: None

Zones Networks VLAN Tags Users Applications Ports URLs **Dynamic Attributes** Inspection Logging Comments

Available Attributes ↻

Q Search by name or value

Security Group Tag

- Employees
- Guests
- Network_Services
- PCI_Servers
- Point_of_Sale_Systems**
- Production_Servers
- Production_Users
- Quarantined_Systems

Add to Source

Add to Destination

Selected Source Attributes (1)

- Security Group Tags
- Developers

Add a Location IP Address Add

Selected Destination Attributes (2)

- Security Group Tags
- PCI_Servers
- Point_of_Sale_Systems

i Attributes of the same type (for example, SGT) match the rule if any attribute is matched. Attributes of different types match the rule only if all attributes are matched. [More info](#)

Establish Trust - FMC Learns EPGs/ESGs

APIC (aci-dev-01)

System | **Tenants** | Fabric

ALL TENANTS | Add Tenant | Tenant Search: name o

fgandola

- Quick Start
- fgandola
 - Application Profiles
 - applications
 - Application EPGs
 - uSeg EPGs
 - Endpoint Security Groups
 - ALL_EPGs
 - development
 - production
 - firewalls
 - Application EPGs
 - ftd-HA-link
 - ftd-mgmt
 - uSeg EPGs
 - Endpoint Security Groups
 - network-segments
 - Networking
 - Contracts
 - Policies
 - Services
 - Security

Secure Firewall Management Center

Objects / Object Management

Overview | Analysis | Policies | Devices | **Objects** | Integration | Deploy

Dynamic Objects

Name	Description	Number of Mapped IPs
APIC_DEMO_APPLICATIONS_ESG-DEMO-APP		1
APIC_DEMO_NETWORK-SEGMENTS_192.168.150.X_24		1
APIC_FGANDOLA_APPLICATIONS_ESG-ALL_EPGS		2
APIC_FGANDOLA_APPLICATIONS_ESG-DEVELOPMENT		1
APIC_FGANDOLA_APPLICATIONS_ESG-PRODUCTION		1
APIC_FGANDOLA_FIREWALLS_FTD-HA-LINK		1
APIC_FGANDOLA_FIREWALLS_FTD-MGMT		4
APIC_FGANDOLA_NETWORK-SEGMENTS_192.168.151....		1
APIC_FGANDOLA_NETWORK-SEGMENTS_192.168.152....		2
APIC_FGANDOLA_NETWORK-SEGMENTS_192.168.153....		1

APIC_FGANDOLA_FIREWALLS_FTD-MGMT

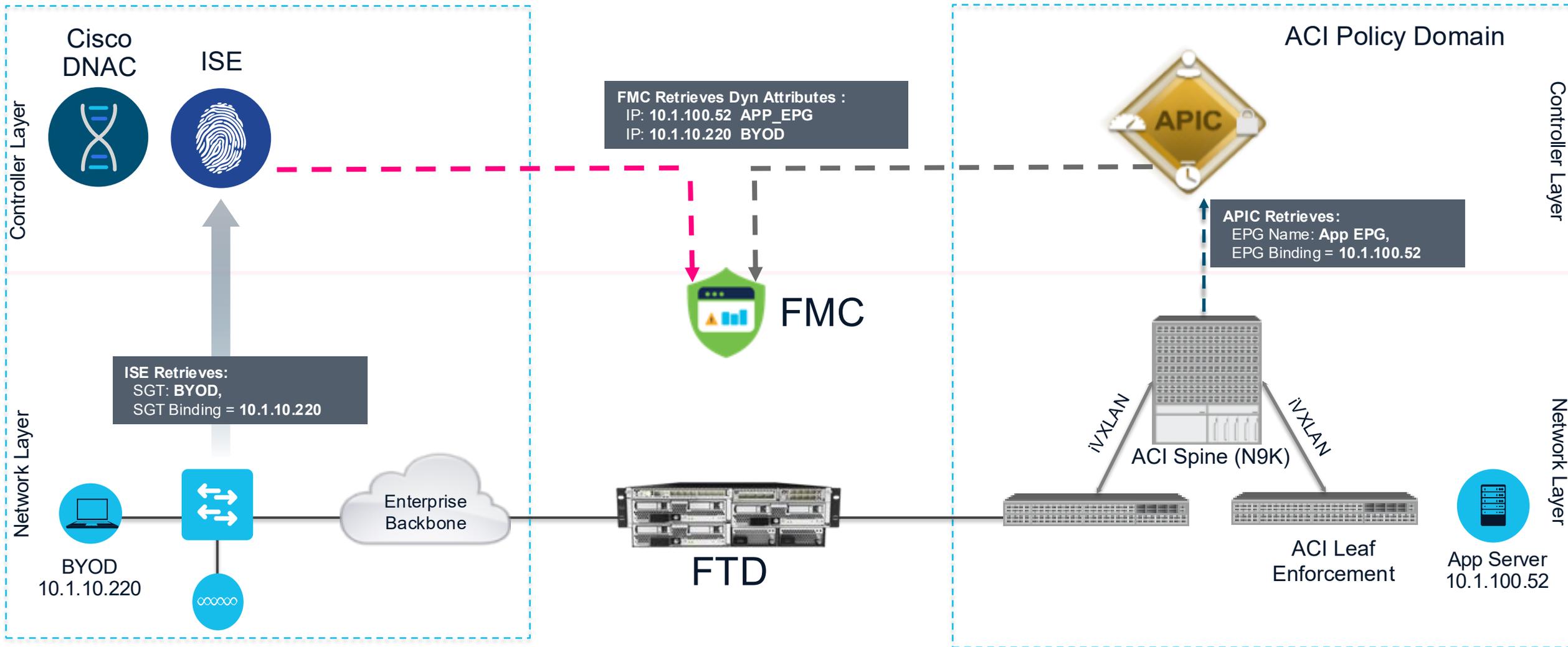
Mapped IPs

- 10.237.100.22
- 10.237.100.23
- 10.237.100.24
- 10.237.100.25

4 Mapped IPs

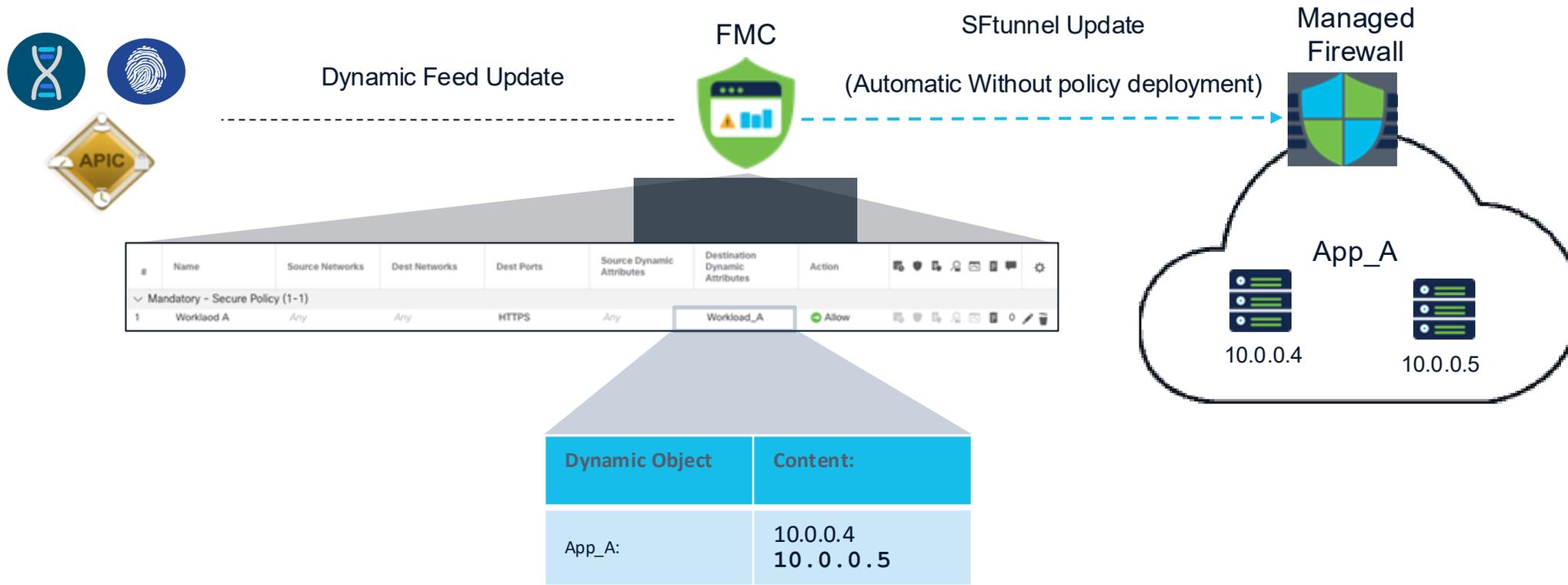
Download OK

Use dynamic attributes to enforce trust

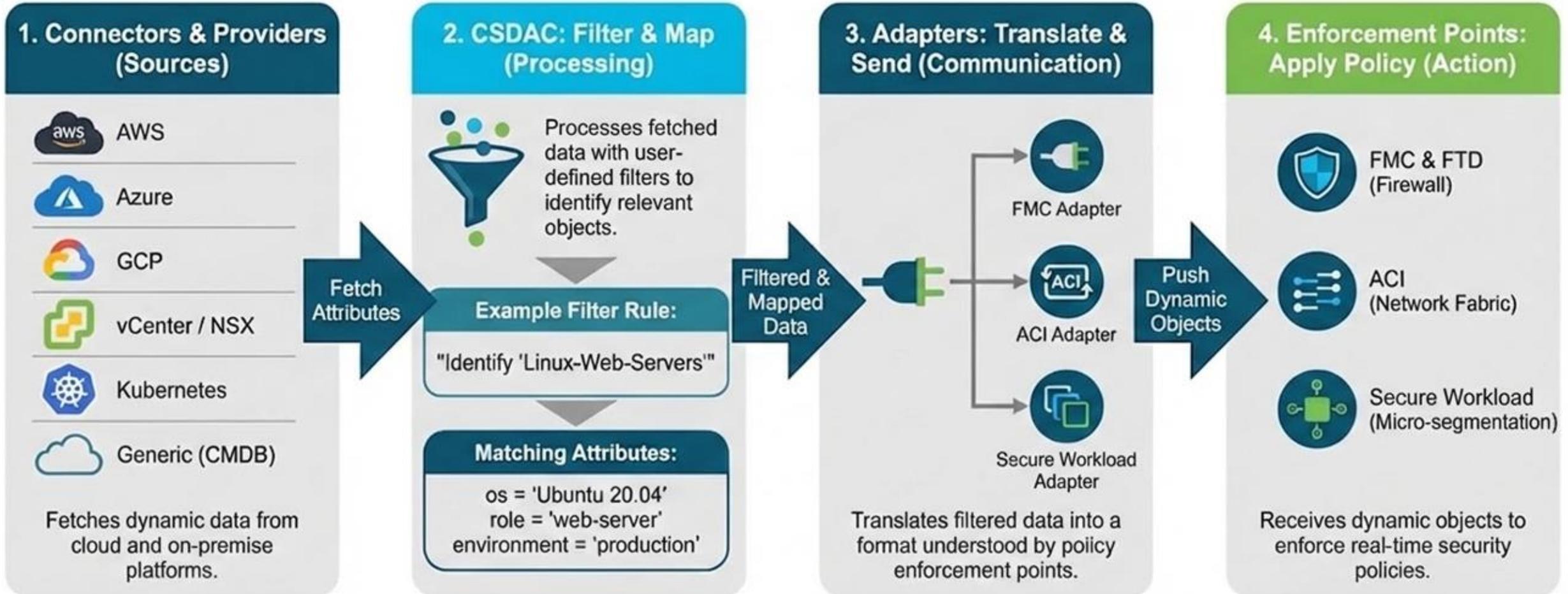


Dynamic Objects in Action

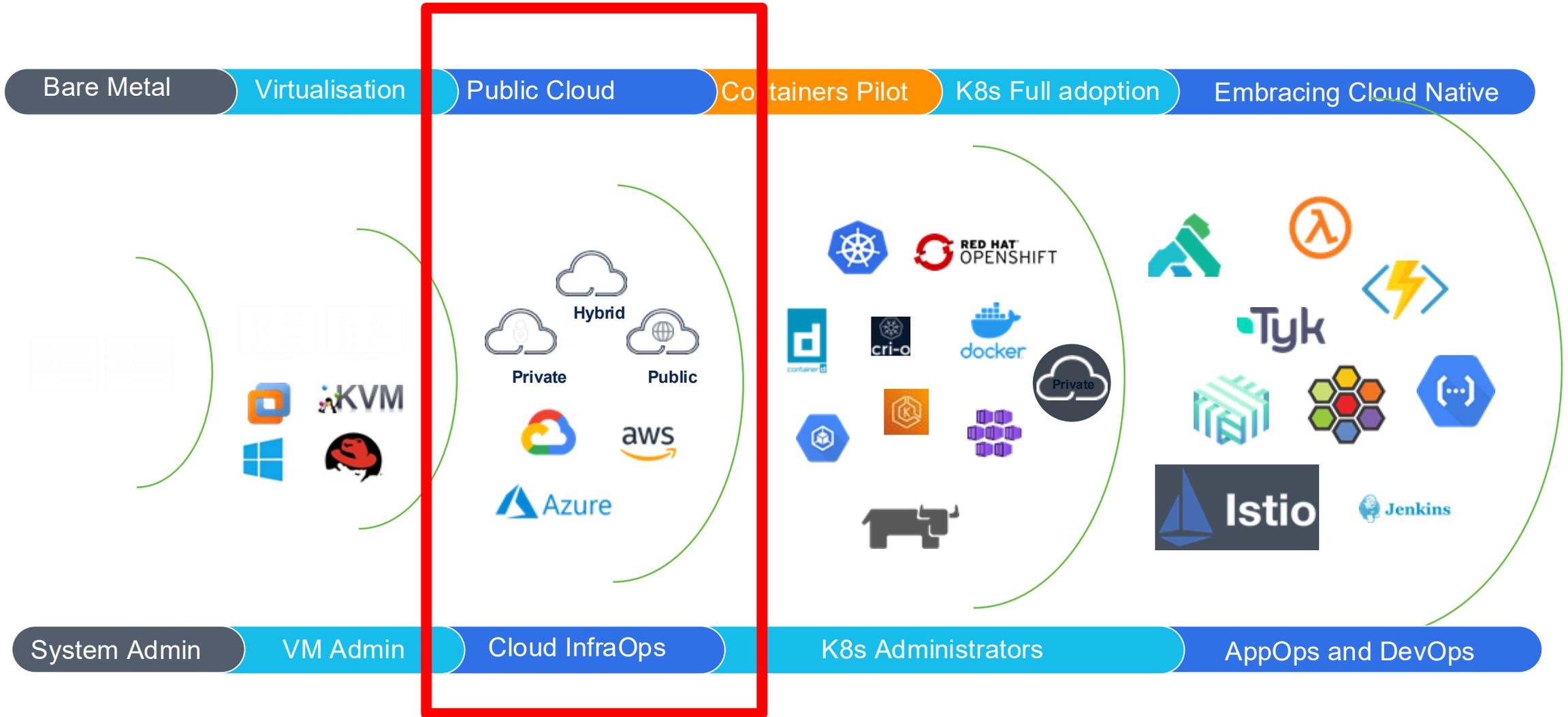
Automatic Without policy re-deployment



Cisco Dynamic Attributes Connector (CDAC): Workflow & Example

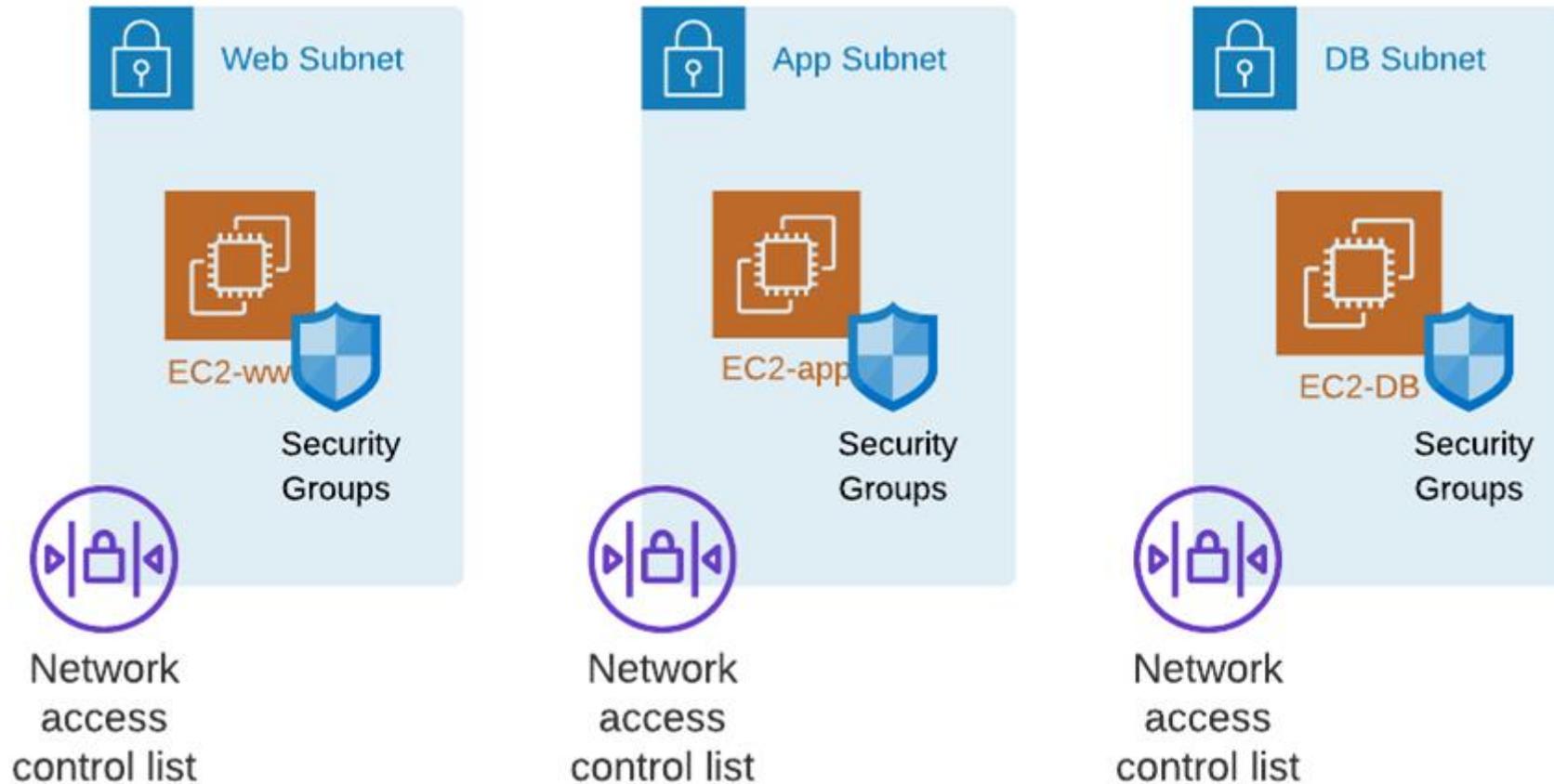


Application workloads evolution

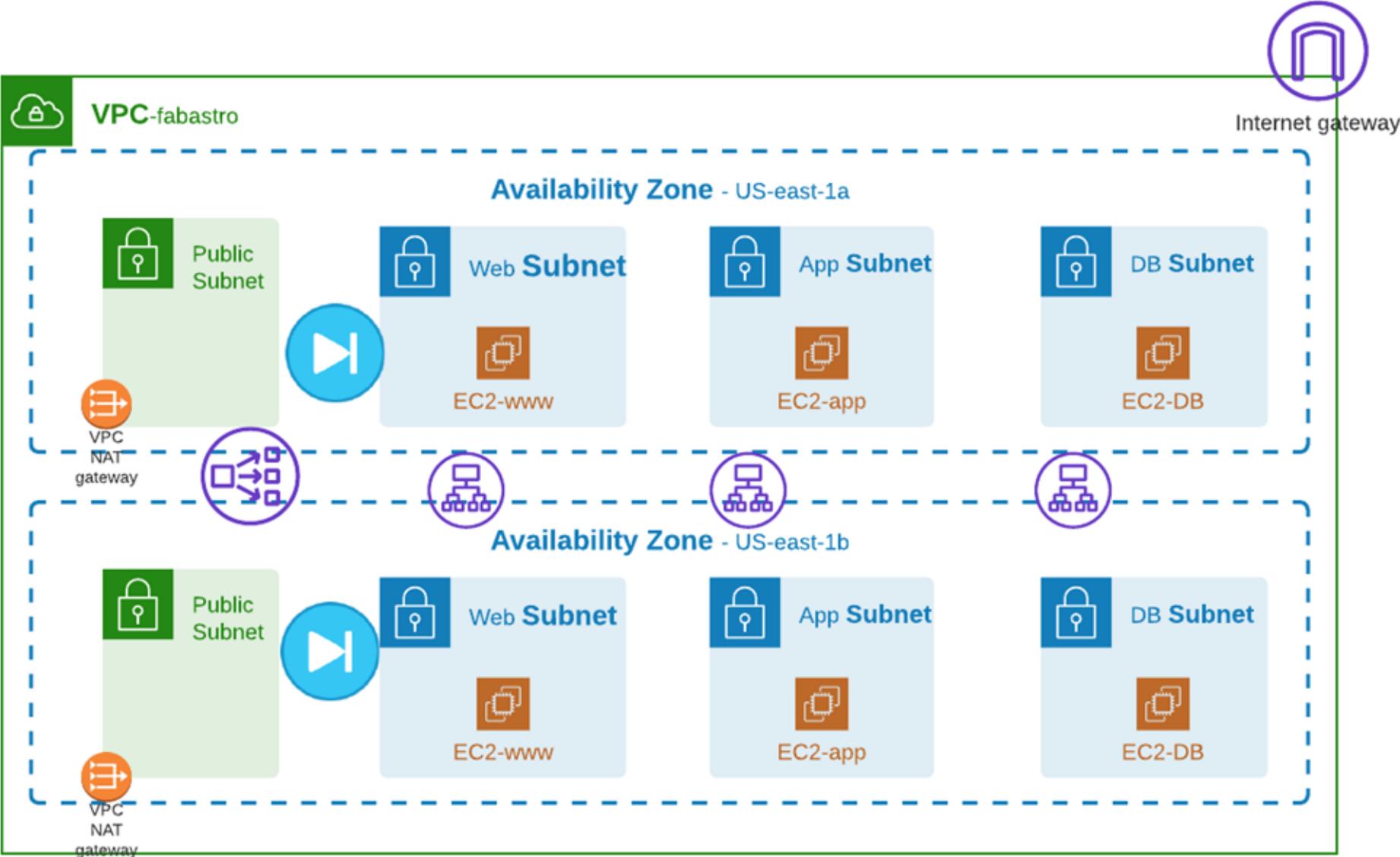


Macrosegmentation in the Cloud

Security Groups and Network Access list



Firewall insertion with HA in front of the "Application" VPC



Multi-Cloud Security configuration complexity

What do we need to configure?

Security VPCs

VPC and DNS Flow Log capture

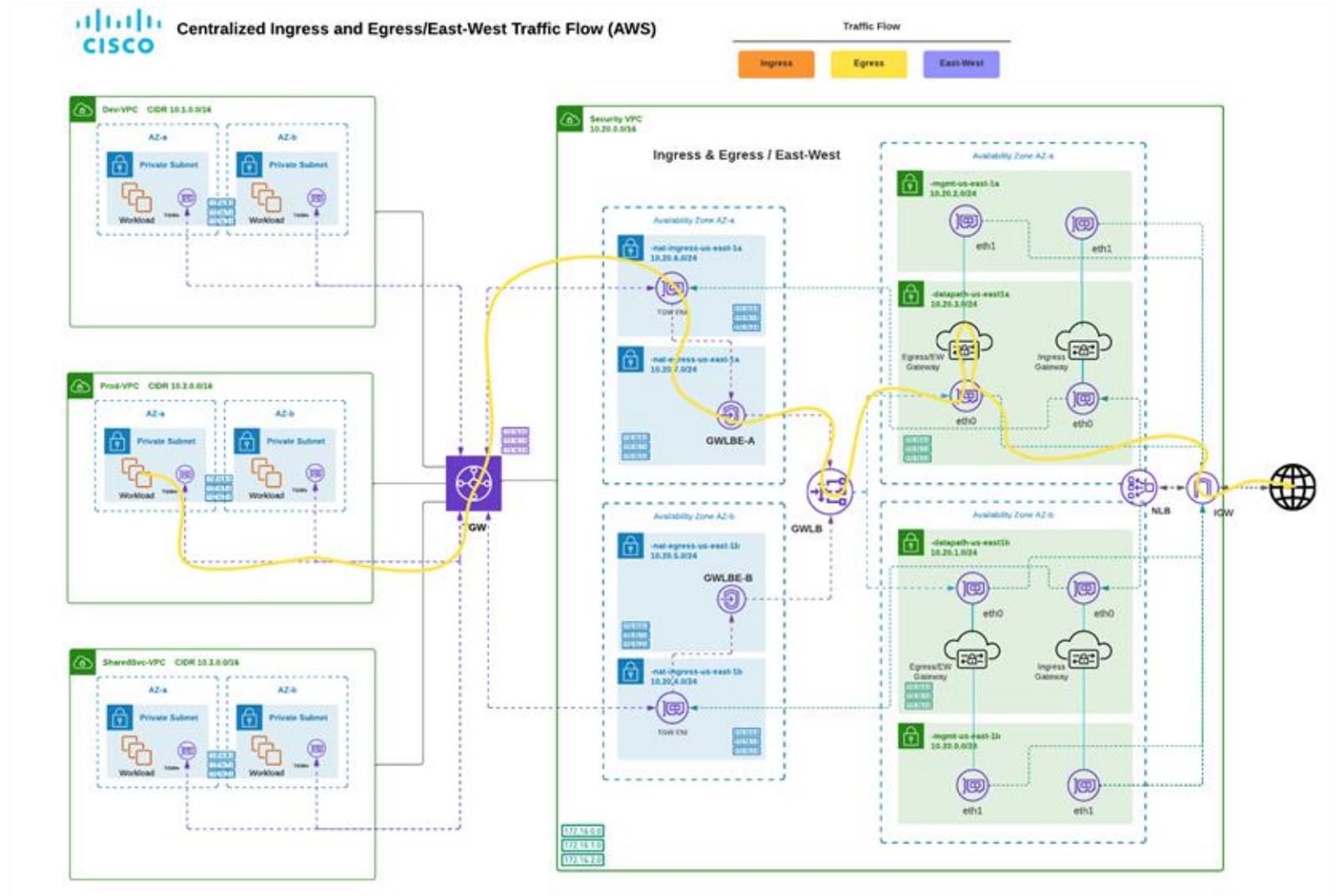
Network Load Balancer

Gateway Load Balancers

Firewalls Gateways
(Deployment, Insertion, Autoscaling)

AWS Transit Gateways
(New or existing, TGW attachment)

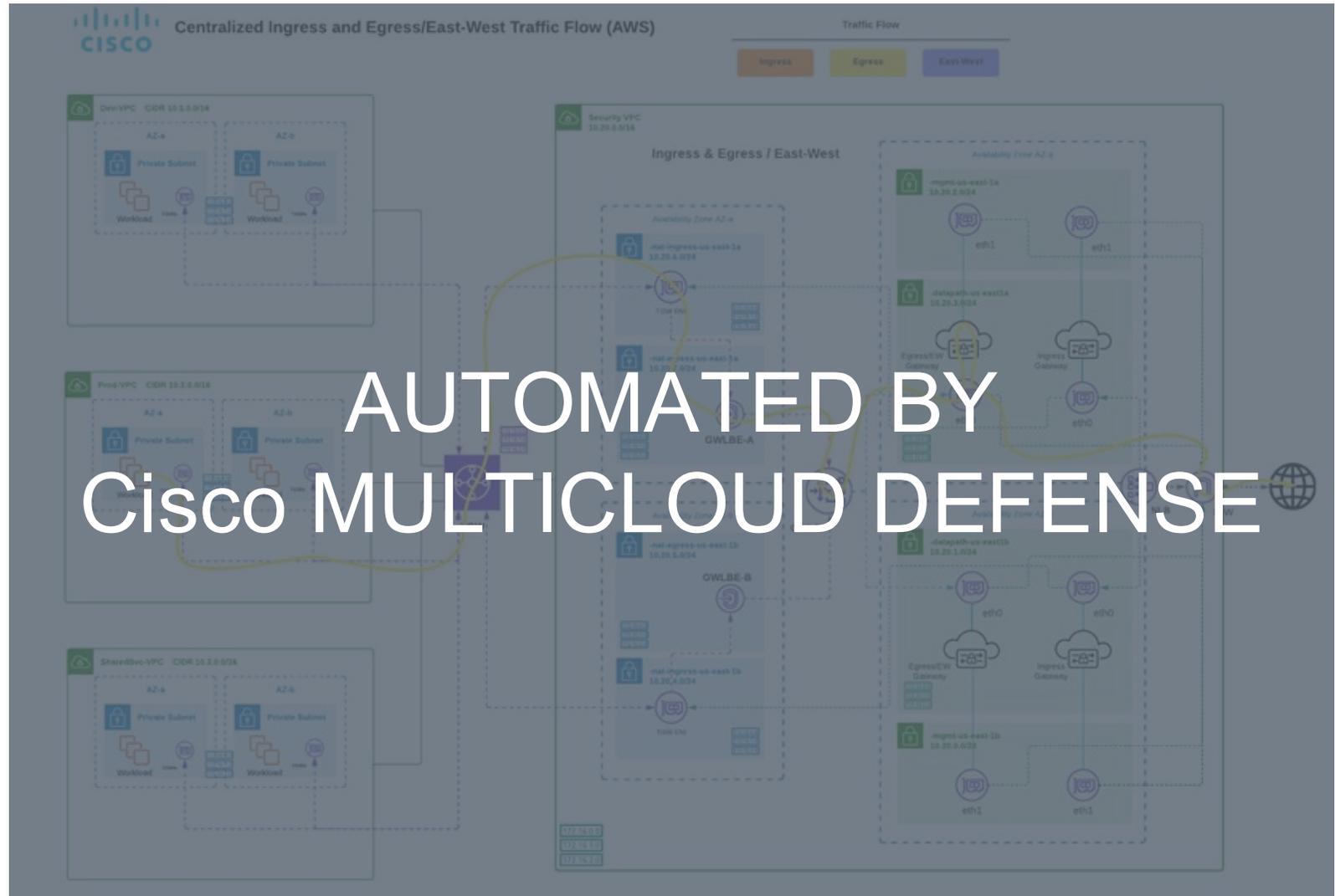
VPC subnet routing to TGW



Cisco Multicloud Defense automates orchestration

What do we need to
configure?

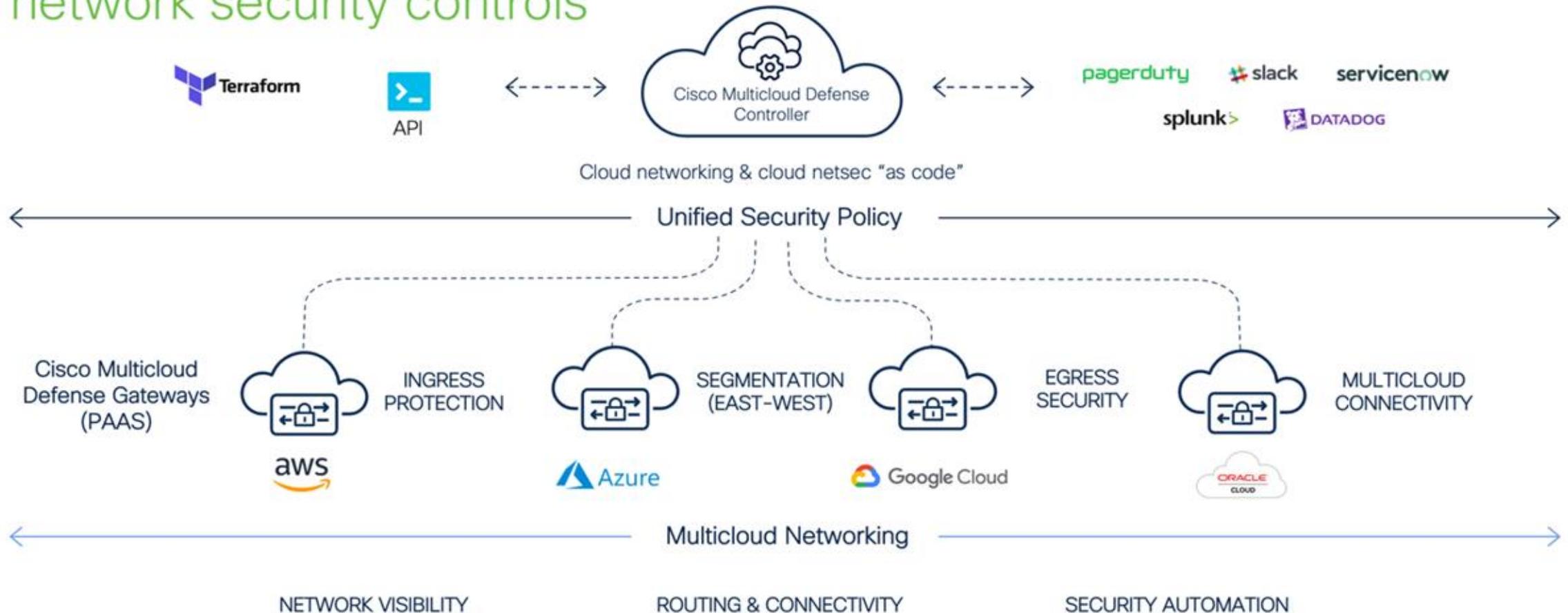
AUTOMATED
BY
MULTICLOUD
DEFENSE



AUTOMATED BY
Cisco MULTICLOUD DEFENSE

Cisco Multicloud Defense

Combining multicloud networking, automation, and cloud-native network security controls



Use cases

FTDv Use Case

↑ Ingress protection



Why Critical?



Stop inbound threats for web and non-web apps

Security Drivers



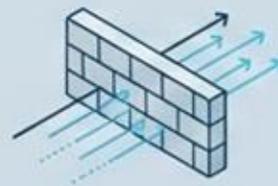
- Supply Chain Vulnerabilities
- Library Exploits (Log4Shell)
- Compliance

Security Controls



- WAF
- IDS / IPS
- Geo IP
- Malicious IP
- Antivirus

↓ Egress security



Why Critical?



Block Command & Control, Botnets, Data Exfiltration

Security Drivers



- Zero Days
- C2, Ransomware
- Compliance

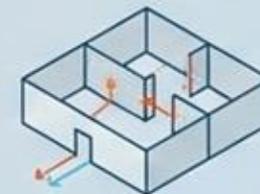
Security Controls



- FQDN Filtering
- URL Filtering
- DLP
- IPS / IDS
- Antivirus



Segmentation



Why Critical?



Mitigate Lateral Movement

Security Drivers



- Zero Trust / Least Privilege
- Data Protection
- Compliance

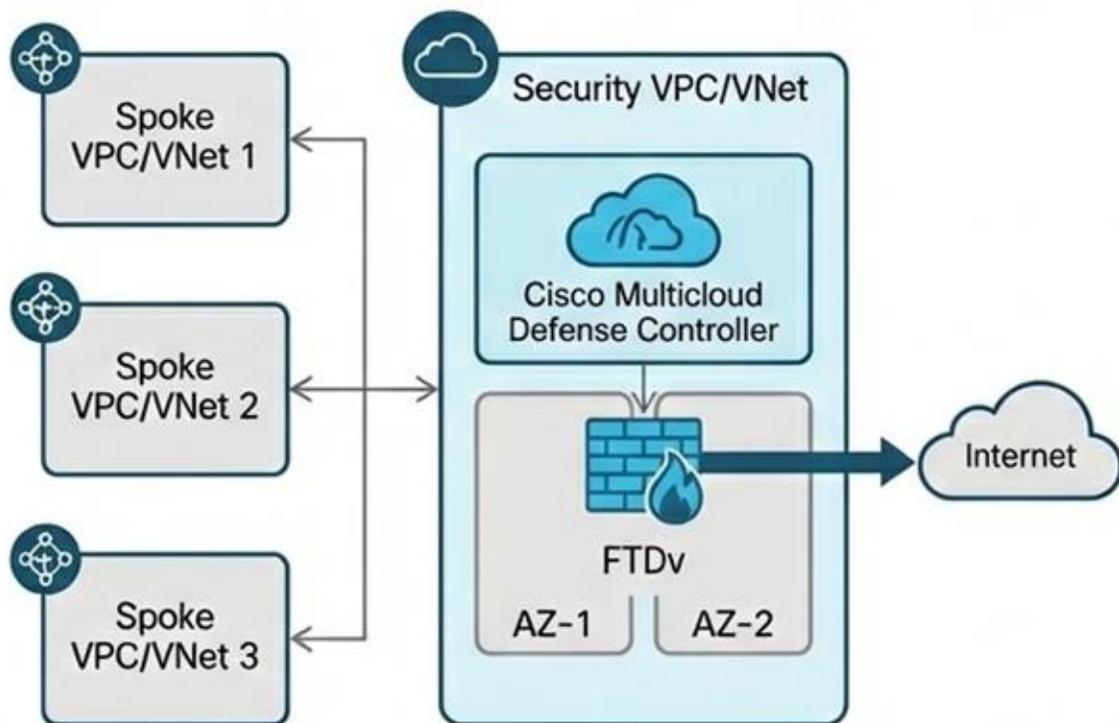
Security Controls



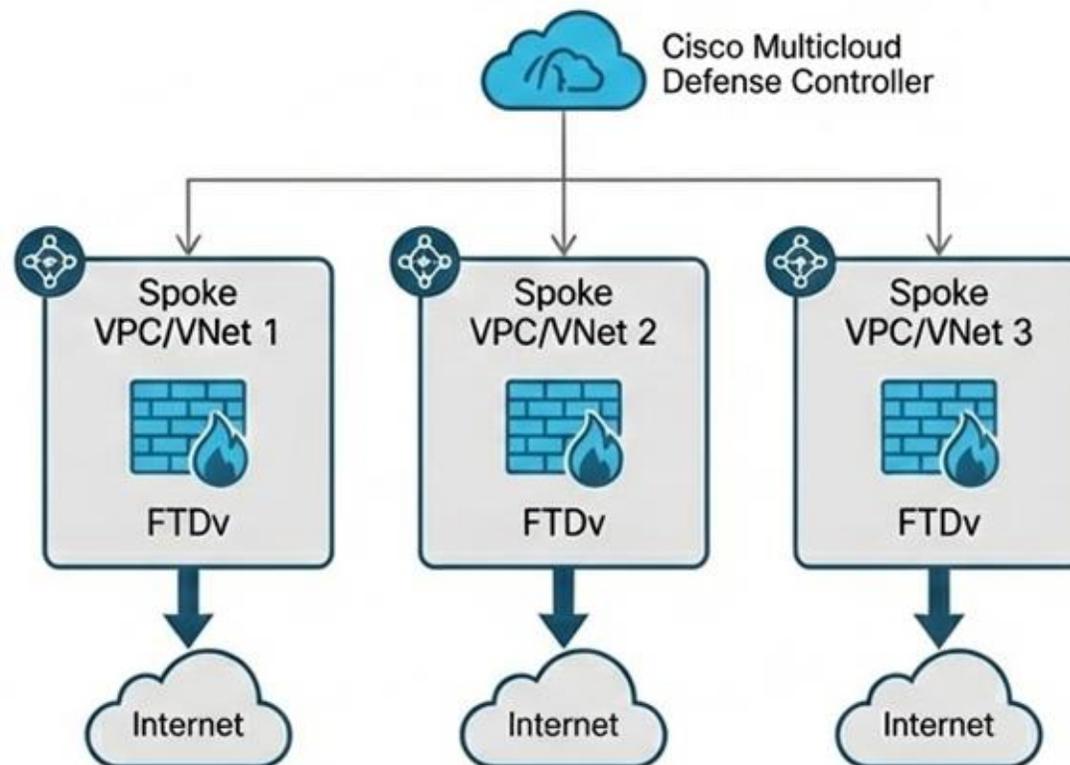
- Cloud-native Identity
- IPS / IDS
- Antivirus

Egress Security Deployment Models

Centralized Security Model



Distributed Security Model



Simple Setup Process

The screenshot shows the Cisco Multicloud Defense Easy Setup interface. The browser address bar displays `prod1.mcd.eu.cdo.cisco.com/easysetup`. The page header includes the Cisco logo, the text "Multicloud Defense", and a user profile for "Admin: dstoeckm@cis...". A navigation menu contains "Dashboard", "Discover", "Investigate", "Manage", "Report", and "Administration".

Setup

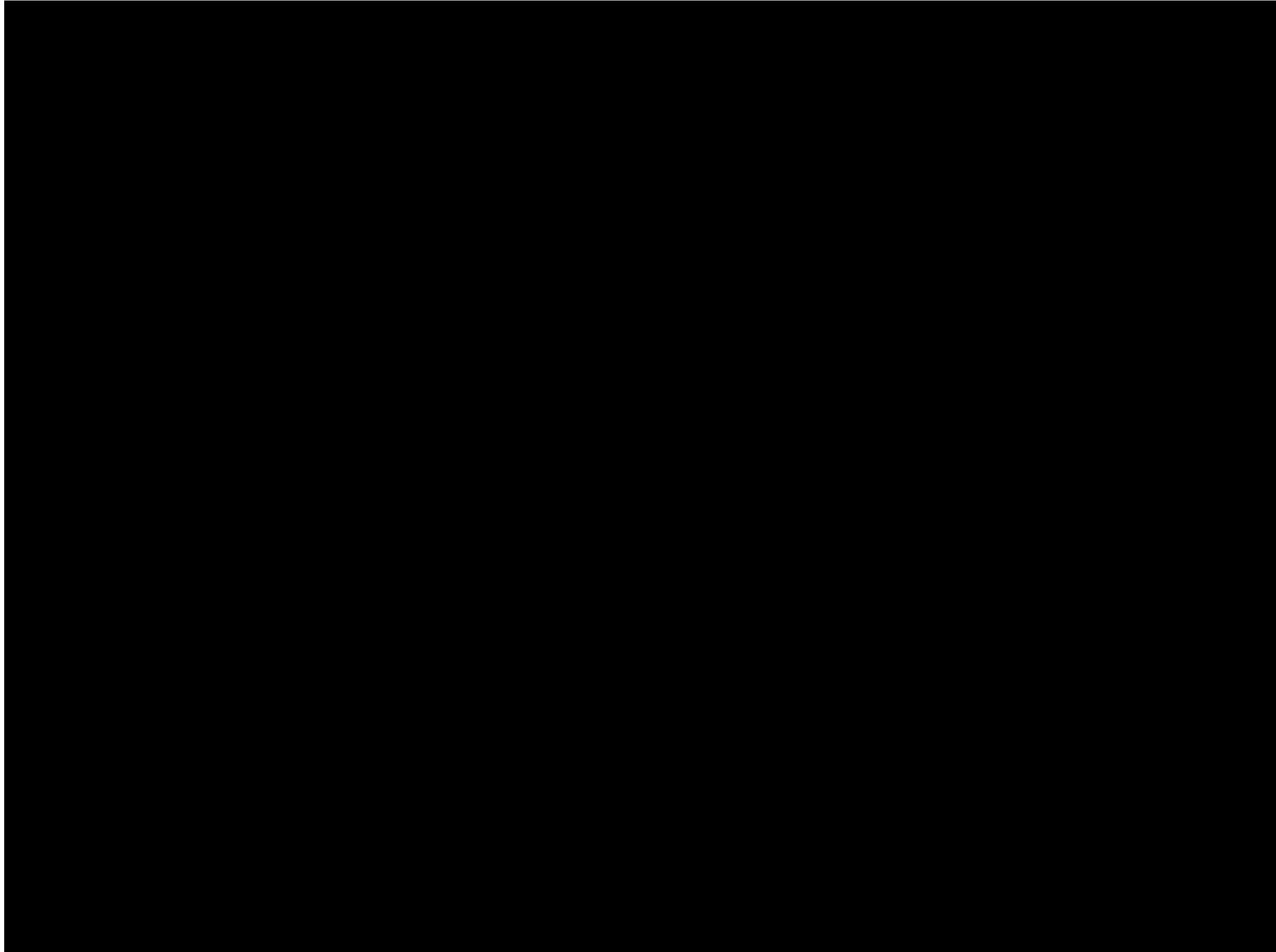
Multicloud Defence secures your applications in minutes by orchestrating the deployment of all security components. Let's begin securing your application by following 3 simple steps.

- Step 1: Connect Account**
Icon: Cloud with checkmark.
Description: Connect a cloud account with the Multicloud Defense Controller.
Button: [Connect Account](#)
- Step 2: Enable Traffic Visibility**
Icon: Globe with crossed lines.
Description: Enable traffic visibility on specific VPCs to allow for more insight into the traffic in and out of your account.
Button: [Enable Visibility](#)
- Step 3: Secure Your Account**
Icon: Padlock.
Description: Setup a Service VPC and Multicloud Defense Gateway to secure your Account.
Button: [Secure Account](#)

Left Sidebar:

- Favorites**
Pinned navigation items will go here
- Setup**
- Security Policies**
 - Rule Sets
 - Addresses
 - Services
 - Certificates
 - FQDNs
- Profiles**
 - Decryption
 - IPS/IDS
 - Data Loss Prevention
 - Anti Malware
 - WAF
 - Layer 7 DOS
 - URL Filtering
 - FQDN Filtering
 - Malicious IPs
 - Packet Capture
 - Log Forwarding

MCD Setup Demo



Cisco Secure Firewall Threat Defense Virtual

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
Microsoft Azure
Google Cloud Platform

Virtual firewall performance-based licensing from 100Mbps up to 16 Gbps

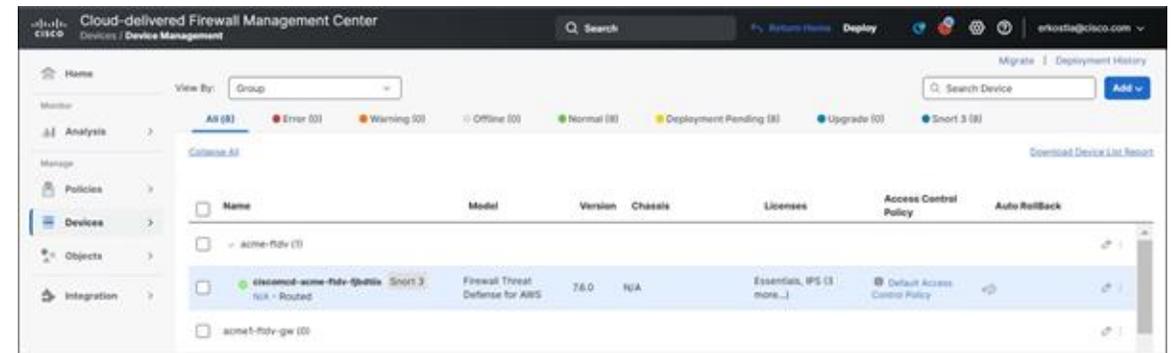
FTDv5 (100Mbps), FTDv10 (1 Gbps), FTDv20 (3 Gbps), FTDv30 (5 Gbps), FTDv50 (10 Gbps), and FTDv100 (16 Gbps)

Cloud Leadership

- Clustering & Auto Scaling
- Integration with cloud native services & infrastructure
- Accelerated Networking
- Smart & Tiered Licensing
- Dynamic Policy
- Quickstarts, Infrastructure as Code and Automation
- Gateway Load balancer integration
- Snapshots

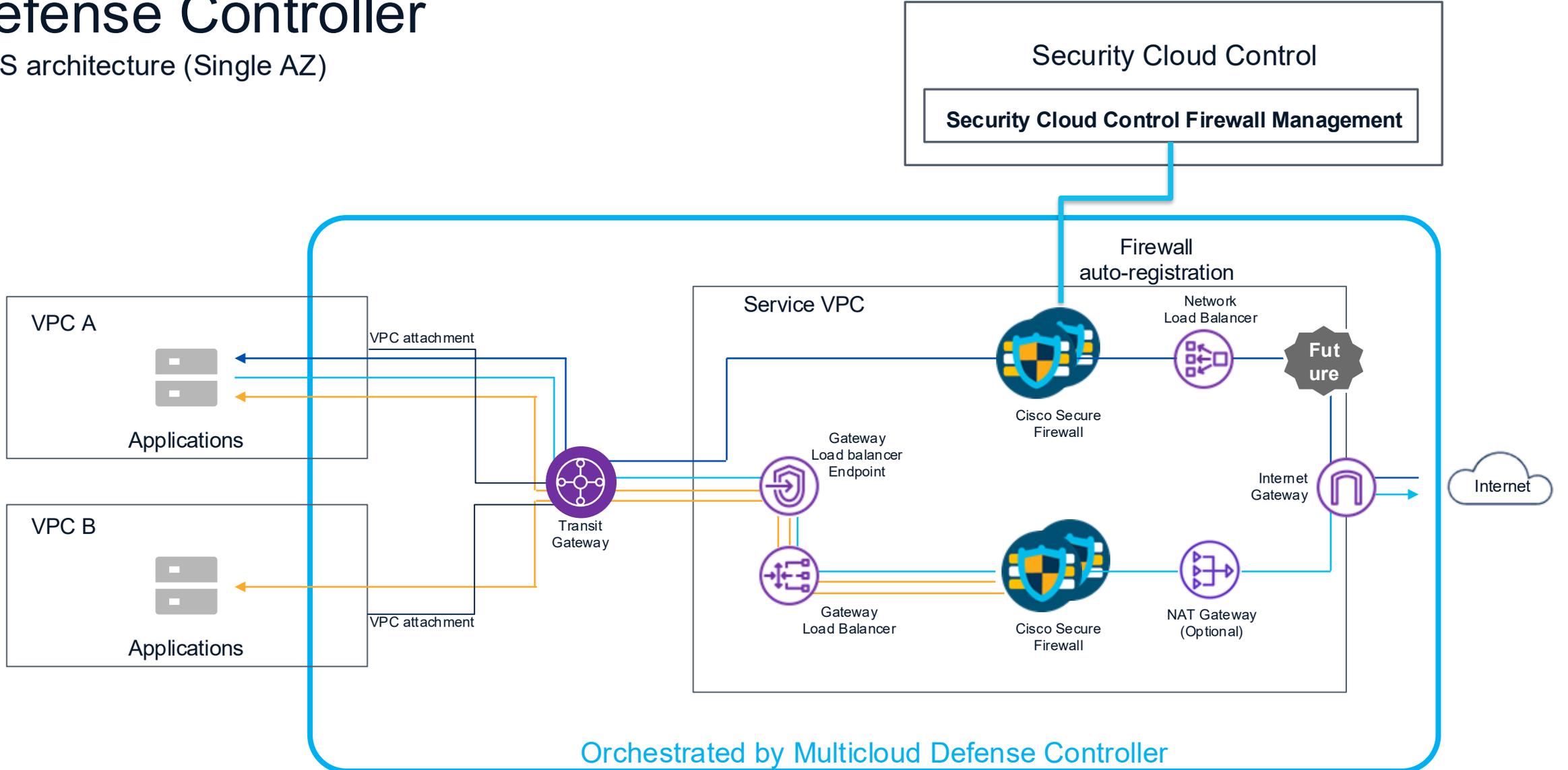
Cisco Firewall Threat Defense Virtual orchestrated by Multicloud Defense Controller

- Simplifies Secure Firewall (FTDv) deployment
 - Deploy one or more firewalls, along with load balancers
 - Configures all necessary routing
 - Identical workflow for all public cloud providers
- Simplifies Secure Firewall (FTDv) operations
 - Automatically scales in or out FTDv's to adjust to load
 - Monitors health of each FTD and replace unhealthy unit
- Performs registration and license management
- Bootstraps FTDv
 - Configure interfaces, device group, platform settings, NAT, and routing
 - Creates all objects on the FMC that are needed for FTDv deployment



Cisco Secure Firewall Virtual Orchestrated by Multicloud Defense Controller

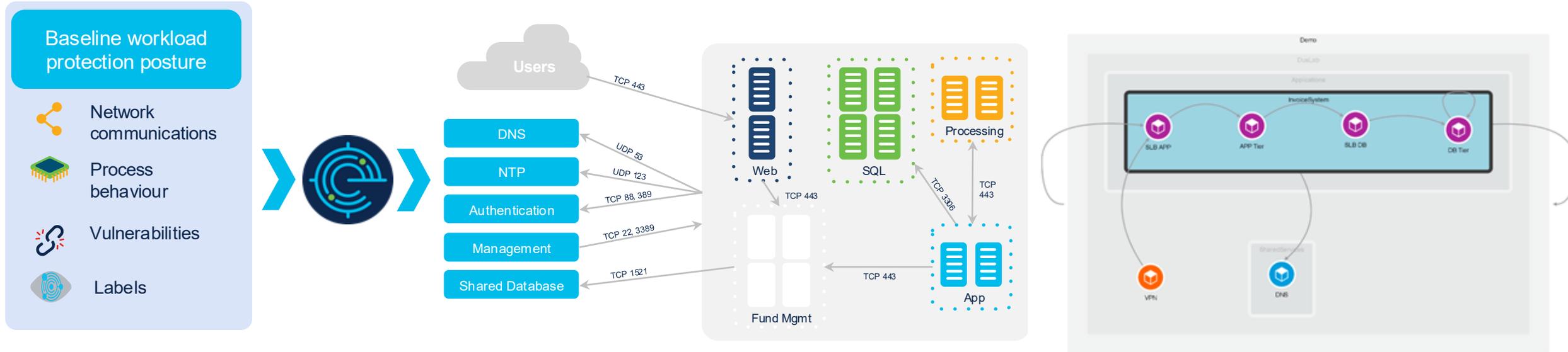
AWS architecture (Single AZ)



Getting closer to Zero Trust with microsegmentation

Establishing Trust with Cisco Secure Workload

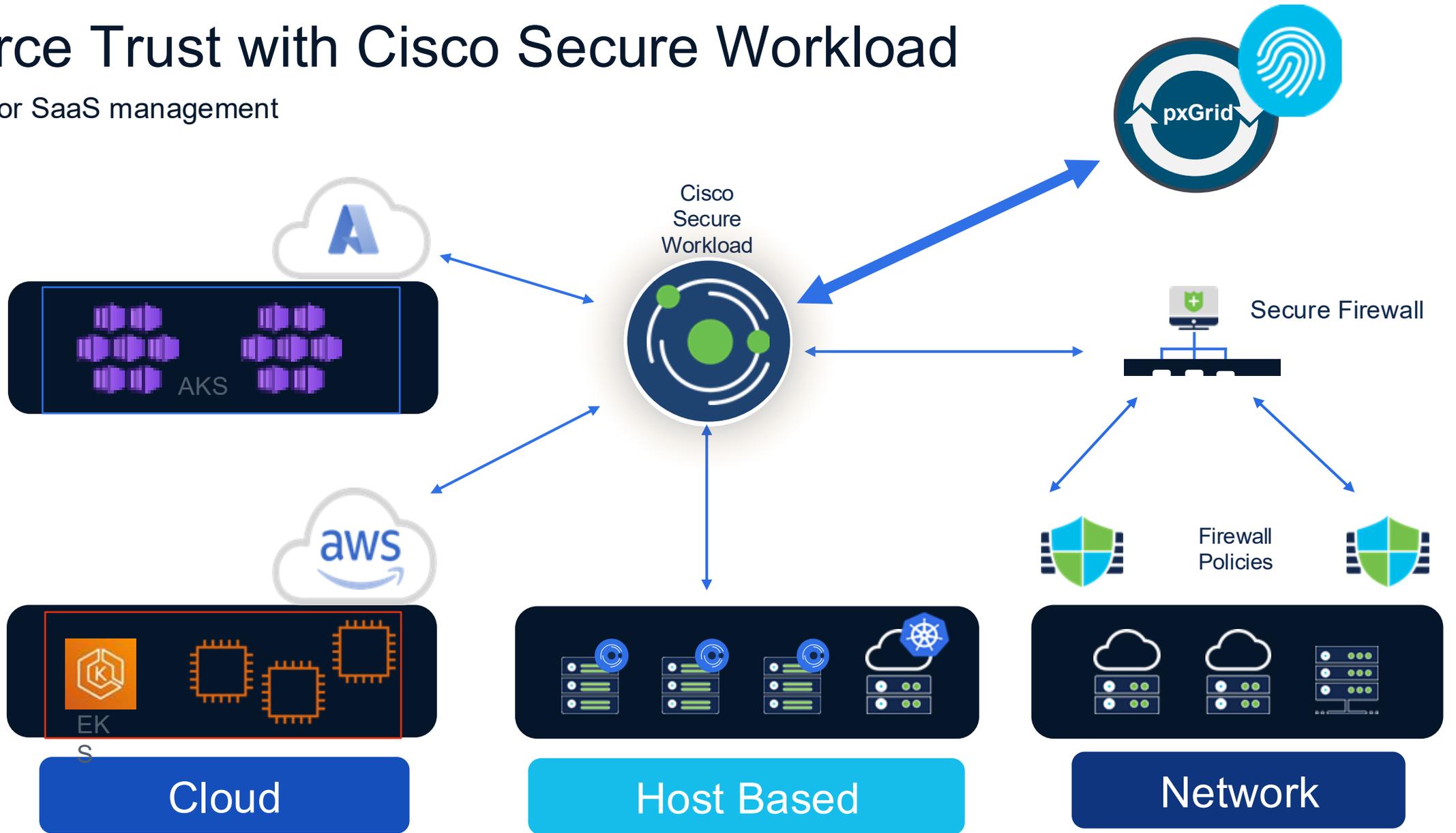
Automated discovery, clustering & policy generation and verification



Rank	Priority	Action	Consumer	Provider	Protocols And Ports
Absolute	100	ALLOW	VPN	SLB APP	TCP : 1936
Default	100	ALLOW	VPN	SLB APP	TCP : 80 (HTTP)
Default	100	ALLOW	SLB DB	DB Tier	TCP : 3306 (MySQL)
Default	100	ALLOW	SLB APP	APP Tier	TCP : 8081
Default	100	ALLOW	Demo : DusLab : Applications : InvoiceSystem	Demo	UDP : 123 (NTP) ...2 more
Default	100	ALLOW	Demo : DusLab : Applications : InvoiceSystem	Demo : DusLab : SharedServices : DNS	UDP : 53 (DNS) ...1 more

Enforce Trust with Cisco Secure Workload

On-prem or SaaS management



CSW Software Appliance



Background

CSW appliance was tightly coupled with Cisco UCS hardware and was not qualified to run on other hardware. Many customers are looking for utilizing existing or non cisco hardware for CSW



What's New

CSW 4.0 will come with software appliance and can run on VMware cluster. The customers can use their existing hardware for VMware cluster and CSW



Benefits

- Reduces CAPEX for micro segmentation adoption.
- Efficient use of hardware and better ROI
- Improved operational efficiency
- Scales to 40,000 workloads

Process and User based policy for Windows & Linux Agents



Background

Process/application-based policies are needed for some environments for better security, this was available on Windows only



What's New

With 4.0 release introduces process based policy for Linux



Benefits

- Granular security policies based on application / process / UID /GID
- Critical application workloads secured from malicious connections

No big fan
of using agents ?

Agentless visibility & enforcement everywhere

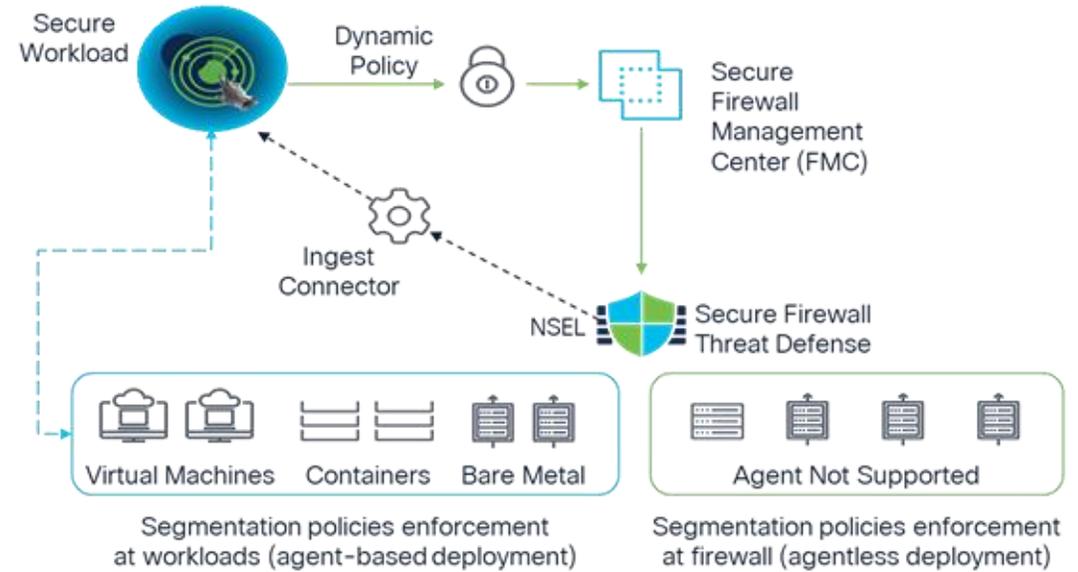
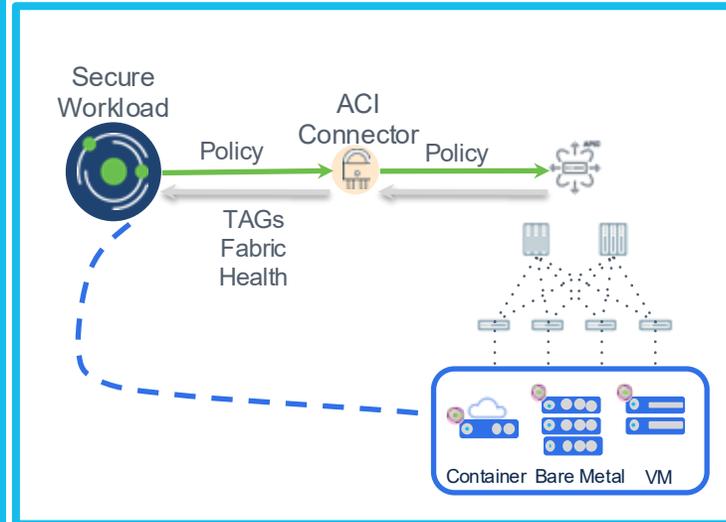


Public Cloud

- Centralized cloud-onboarding & cloud connectors
- Visibility with real-time discovery of workloads and labels & Flow telemetry via VPC/Nets flow-logs
- Enforcement using Security Groups (AWS), Network Security Groups (Azure), Firewall (GCP)

On-prem with ACI

- Realize ACI vision of App Centric deployment
- Automated Policy Lifecycle management

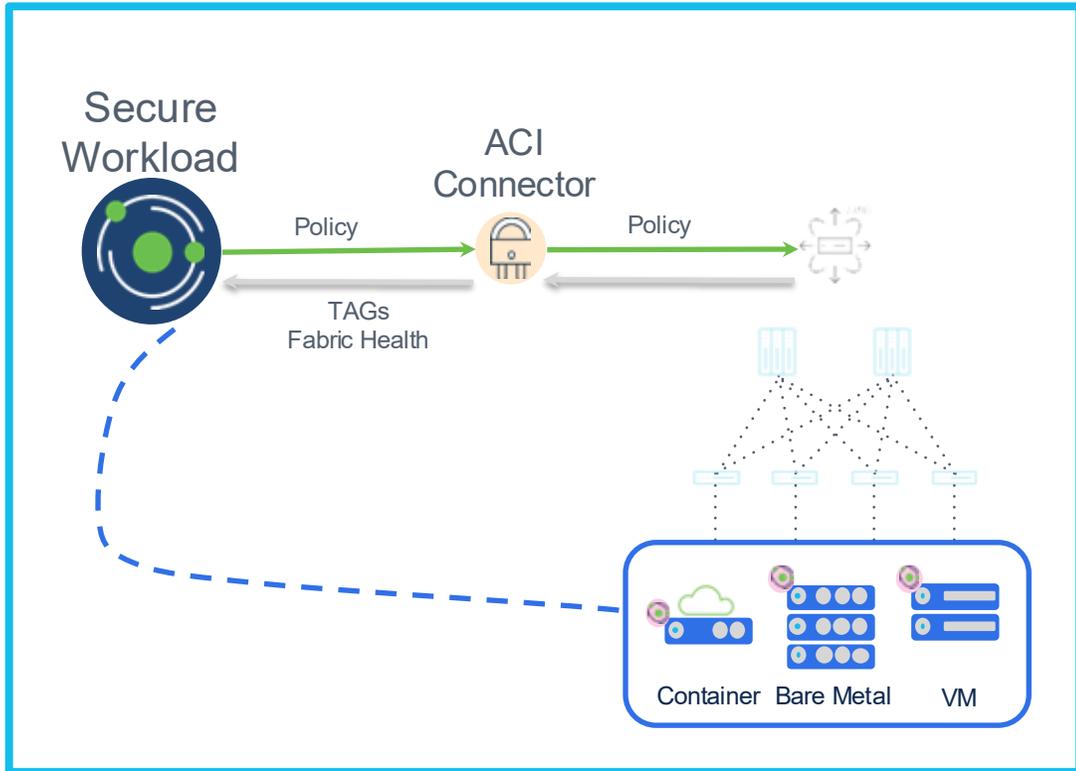


With Firewalls and Switching

- Topology aware policy enforcement
- Support access control policy and dynamic object

Secure Workload – ACI Integration

New in 4.0



 Agentless policy enforcement

 Realize ACI vision of App Centric deployment

 Automated Policy Lifecycle management

 Faster Time to Value

 Foster collaboration between NetOps, App and NetSec team

CSW Policies Pushed to ACI

CISCO APIC admin [Search] [Menu] [Settings] [Help] [Logout]

System **Tenants** Fabric Virtual Networking Admin Operations Integrations

ALL TENANTS | Add Tenant | Tenant Search: name or descr | common | CSWDemo | vinnaga2 | sachenna | raminder01

CSWDemo

- Quick Start
- CSWDemo
 - Application Profiles
 - DemoAPIinfra
 - SecureWorkload-68b8fa52cbf7695cb7dab550**
 - Application EPGs
 - uSeg EPGs
 - Endpoint Security Groups
 - SecureWorkload-ESG-4e55c16b
 - SecureWorkload-ESG-50ebc37d
 - SecureWorkload-ESG-74693396
 - SecureWorkload-ESG-a789dd7
 - SecureWorkload-ESG-e7884366
 - Networking
 - Contracts
 - Policies
 - Services

Application Profile - SecureWorkload-68b8fa52cbf7695cb7dab550

Summary **Topology** Policy Stats Health Faults History

Healthy [Status Icons]

Contract EPG uSeg EPG Any EPG Baremetal VMware Microsoft Red Hat OpenStack Kubernetes Cloud Foundry OpenShift Layer 2 Layer 3 Layer 4-7

Relation Indicators

Configured Operational

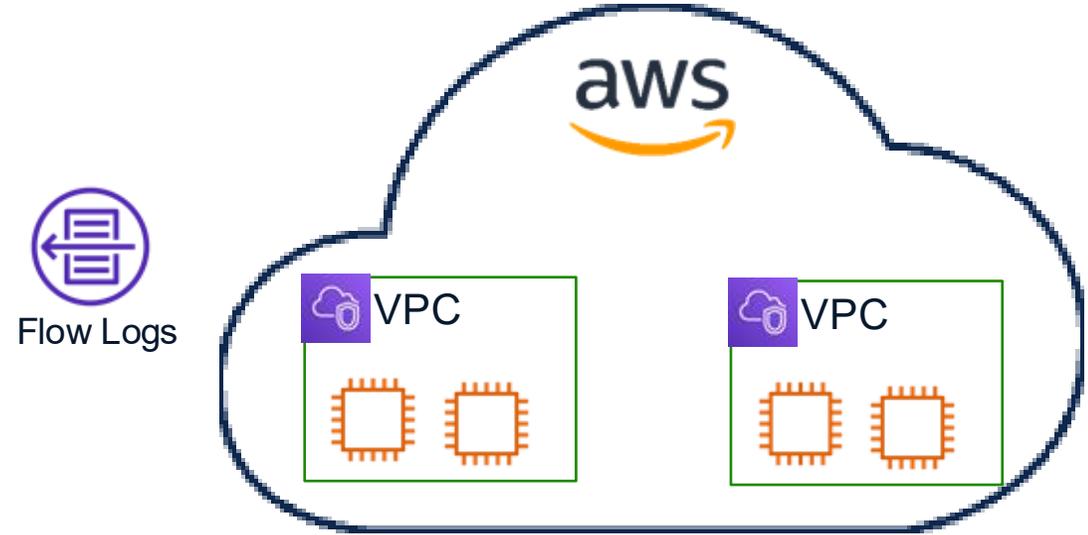
Show All On Click

Show VRF on EPG:

Provider
Consumer
Intra EPG/ESG
Provider (from Master)
Consumer (From Master)
Intra EPG/ESG (from Master)
Master EPG/ESG

Application Profile - SecureWorkload-68b8fa52cbf7695cb7dab550

Cisco Secure Workload Cloud-Based Sources



Edit AWS Connector

Activities Roles and Settings Select VPC

Enabling Segmentation : Enabling segmentation on VPCs will remove existing Security Group(s).

Select the VPCs and fine tune the settings for each VPC

<input type="checkbox"/>	VPC Name	Region	Ingest Flow Logs	Gather Labels	Enable Segmentation
<input checked="" type="checkbox"/>	eucentral-minnie1	eu-central-1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/>	eu-default-vpc	eu-central-1	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/>	▼ vpc-goe2e-eks-enforcement-scale-7	us-east-1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Select kubernetes clusters:

goe2e-eks-enforcement-scale-7

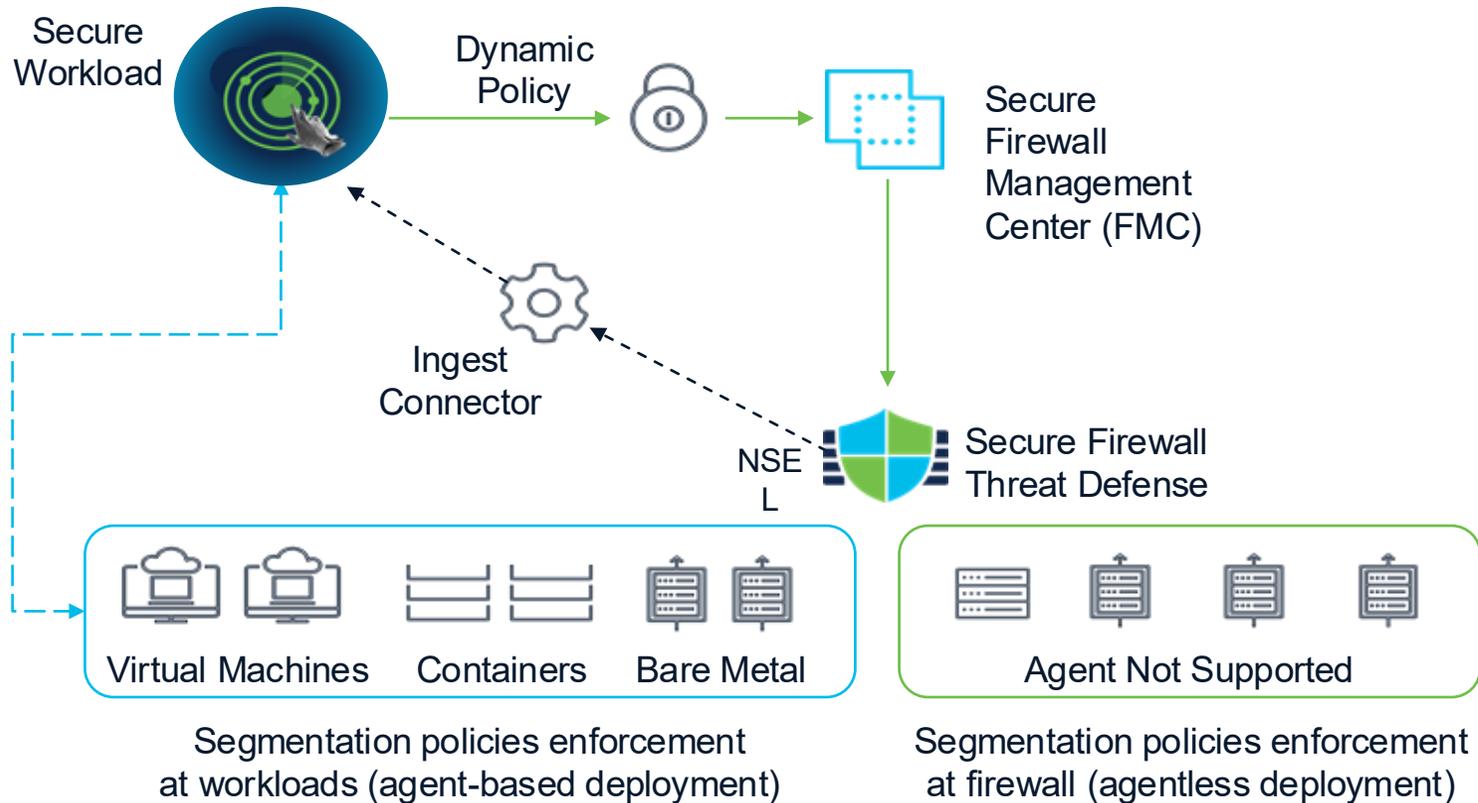
Cancel Back Submit

AWS Connector consolidates:

- VPC flow logs ingestion
- Context gathering (AWS tags and labels)
- AWS cloud-managed Kubernetes orchestration (Kubernetes object labels and annotations)
- Enforcement via cloud native constructs

Secure Workload & Firewall Integration And Enforcement

Firewall Segmentation - Enforce Trust without agents



Defense in depth



Support access control policy and dynamic object



Improved rule ordering



FMC domain awareness



Topology aware policy enforcement



Support deployment across multicloud

Secure Workload Policy Orchestration in FMC

Firepower Management Center
Policies / Access Control / Policy Editor

Overview Analysis Policies Devices Objects AMP Deploy

East-West-Poli

Inserted rules are organized by sections.

Dynamic objects are used to replace IP addresses where applicable.

Different rulesets are scoped by domains.

Rules Security Intelligence HTTP Responses Logging Advanced

Filter by Device Search Rules Show Rule Conflicts Add Category Add Rule

#	Name	Source Networks	Dest Networks	Dest Ports	Source Dynamic Attributes	Destination Dynamic Attributes	Action
Mandatory - East-West-Policy (1-11)							
1	Block log4j	Any	log4j-ubuntu	Any	Any	Any	Block
2	Workload_golden_1	Any	Any	Any	WorkloadObj_collector	Any	Allow
3	Workload_golden_2	Any	Any	TCP (6):5640	Any	WorkloadObj_collector	Allow
4	Workload_golden_3	Any	Any	Any	WorkloadObj_collector	Any	Allow
5	Workload_golden_4	Any	Any	TCP (6):5660	Any	WorkloadObj_collector	Allow
6	Workload_golden_5	Any	Any	Any	WorkloadObj_wss	Any	Allow
7	Workload_golden_6	Any	Any	TCP (6):443	Any	WorkloadObj_wss	Allow
8	Workload_7	Any	Any	TCP (6)	WorkloadObj_Production_!	WorkloadObj_Developmen	Block
9	Workload_8	Any	Any	TCP (6)	WorkloadObj_Vulnerable_v	WorkloadObj_Root_Interne	Block
10	Workload_9	Any	Any	TCP (6)	WorkloadObj_Administrato	WorkloadObj_Root_CSW_!	Allow

Continuously Verify & Respond

Cisco Secure Workload

Workspaces: DC-Access-PCI Compliance (NEW) PRIMARY Version 1 View Version History

Matching Inventories: 42 Policies: 6 Filters: 0 Conversations Provided Services Policy Analysis Enforcement Status Enforcement

Filter Policies ... Run Quick Analysis + Add Policy

Absolute and Default Policies: 3 Catch All: ALLOW Grouped: 1 Ungrouped

DENY and policies for ANY protocol have different behavior in Windows firewalls when compared to Linux. See User Guide for more details.

Rank	Priority	Action	Consumer	Provider	Protocols And Ports
Default	50	DENY	Kill_Switch	Finance Servers	Any
Default	90	DENY	CVE-2021-34480	PCI	Any
Default	90	DENY	Irvine: JerryLin-Lab	CVE 2022-30190	ICMP ...1 more
Default	92	ALLOW	PCI-non-PCI	non-PCI server	ICMP

Filter: CVE 2022-30190

Filter Actions: [edit icon]

Query: Package CVE = 2022-30190

Scope: Irvine:JerryLin-Lab

Restricted: No

Provides Service: No

View Filter Details

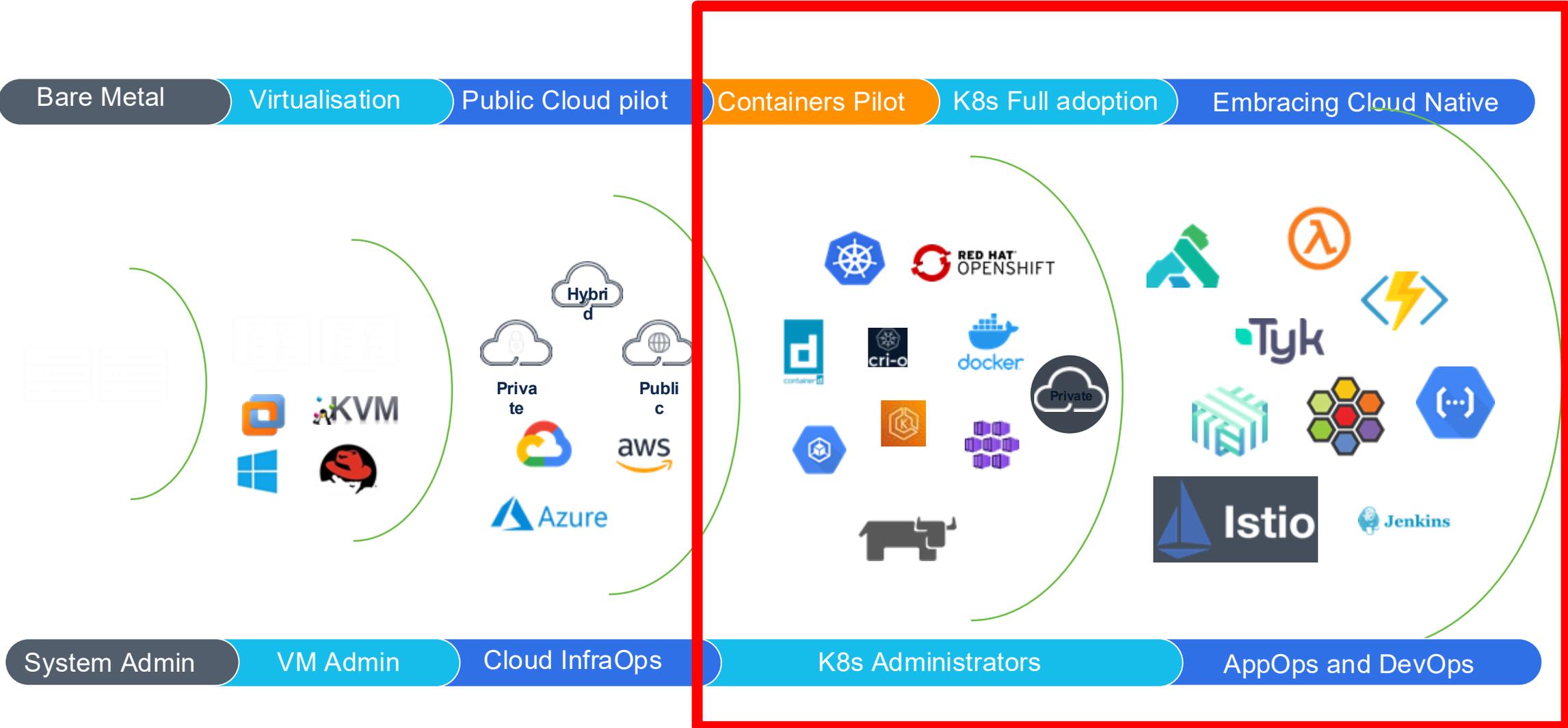
servers identified with CVE 2022-30190

Address	Hostname	OS
10.3.3.111	Win2016-VM4	MSServer2016Standard
192.168.1.241	TomHomeLabDC	MSServer2019Standard
10.2.2.110	W2016-AuthProxy	MSServer2016Standard
10.3.3.110	Win2016-VM3	MSServer2016Standard

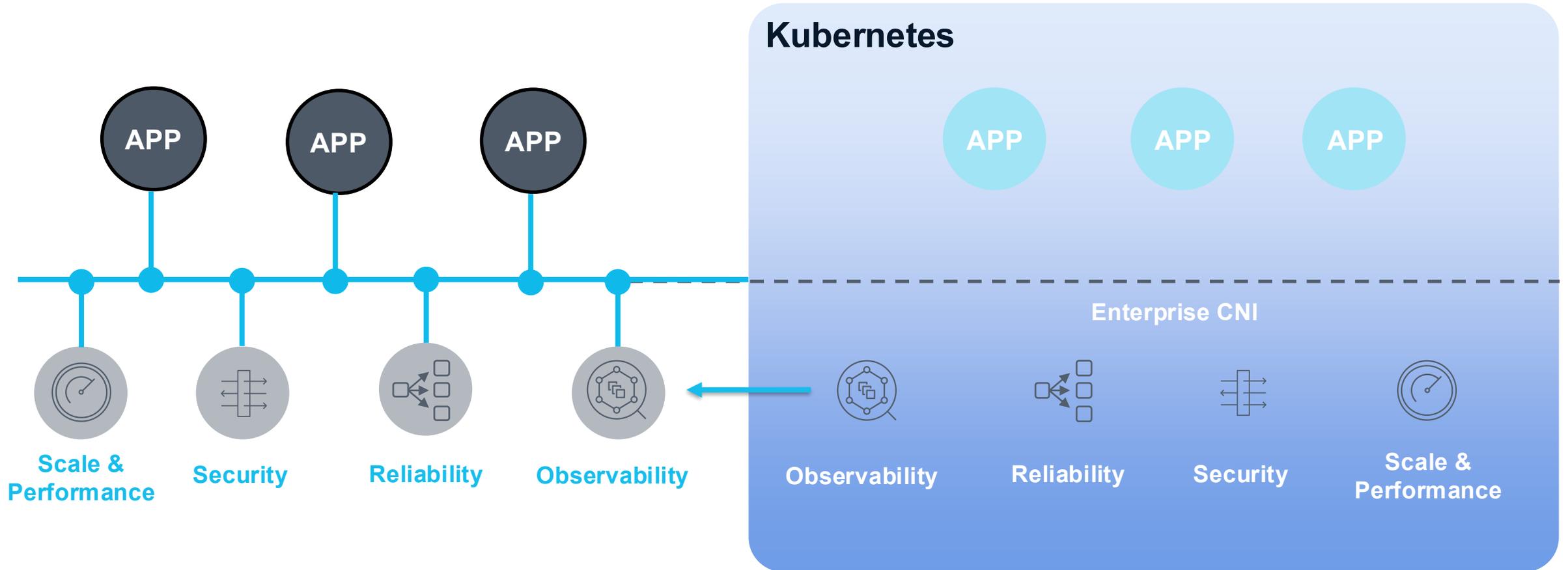
Workloads: 4

IP Addresses: 0

Application workloads evolution



Solution to Regain the Visibility and Control Enterprises Need



From Open-Source Innovator to Enterprise Platform

ISOVALENT
now part of CISCO

The team behind the innovation. The platform for mission-critical environments.



Open-Source Leadership

- Creators and maintainers of Cilium, the leading cloud-native networking project.
- Creators of Tetragon, the eBPF-based runtime security and observability engine.
- Key contributors to the eBPF ecosystem
- Powering technologies trusted by hyperscalers like AWS, Google, and Microsoft.
- Backed by a vibrant open-source community and CNCF ecosystem.

ISOVALENT

now part of CISCO

Enterprise-Ready Platform

- Hardened enterprise platform
- Enterprise features for production use
- Enterprise-grade support and SLAs
- Built-in capabilities for compliance, threat detection, and forensics.
- Trusted by regulated industries and global enterprises.

Isovalent Enterprise Platform



ISOVALENT
**Networking for
Kubernetes**

Enterprise-grade networking, security & observability at scale.

Reliable connectivity and performance with identity-aware network policies and deep traffic observability.



ISOVALENT
**Runtime
Security**

Modern security observability and threat mitigation.

Strengthen security and compliance across any environment while reducing complexity and improving efficiency.



ISOVALENT
**Load
Balancer**

Simplified load balancing across any environment.

Enhance developer productivity with high-performance load balancing that reduces complexity across all environments.



ISOVALENT
**Mesh
Networking**

A universal networking layer across cloud, on-premises, and edge.

Break down networking silos and speed up application delivery and security with a unified network fabric.

Runs anywhere - cloud, on-prem, or bare metal.

The Isovalent Platform is supported across major cloud providers, Kubernetes distributions, VMs, and bare metal, giving you full flexibility without lock-in.



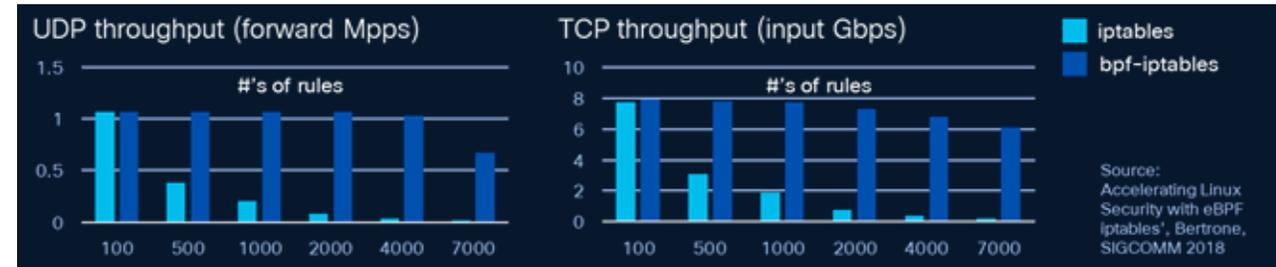
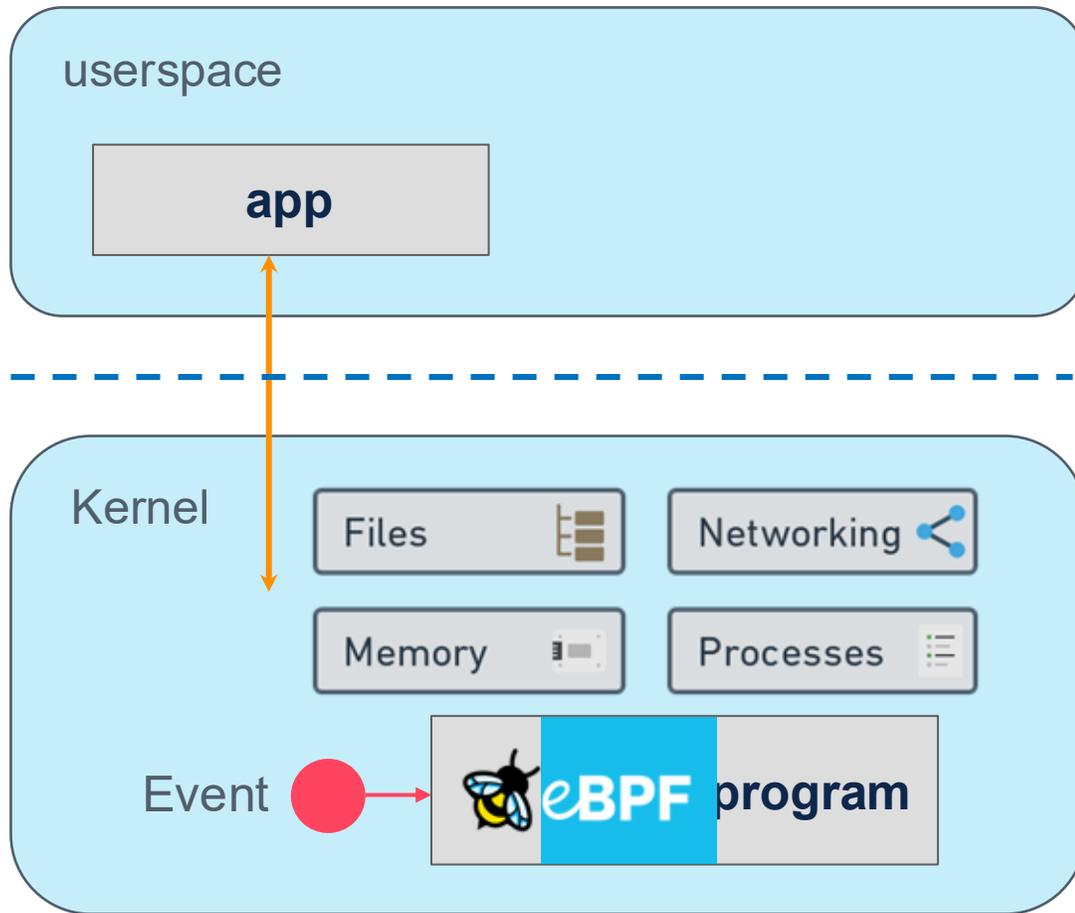
Built on Open Source Standards

Powered by Cilium, Tetragon, and eBPF open source projects created by Isovalent and backed by a strong community. Trusted for performance, scalability, and rapid innovation with minimal vendor lock-in.



eBPF – Extended Berkely Packet Filter

Makes the kernel programmable in a secure and efficient way

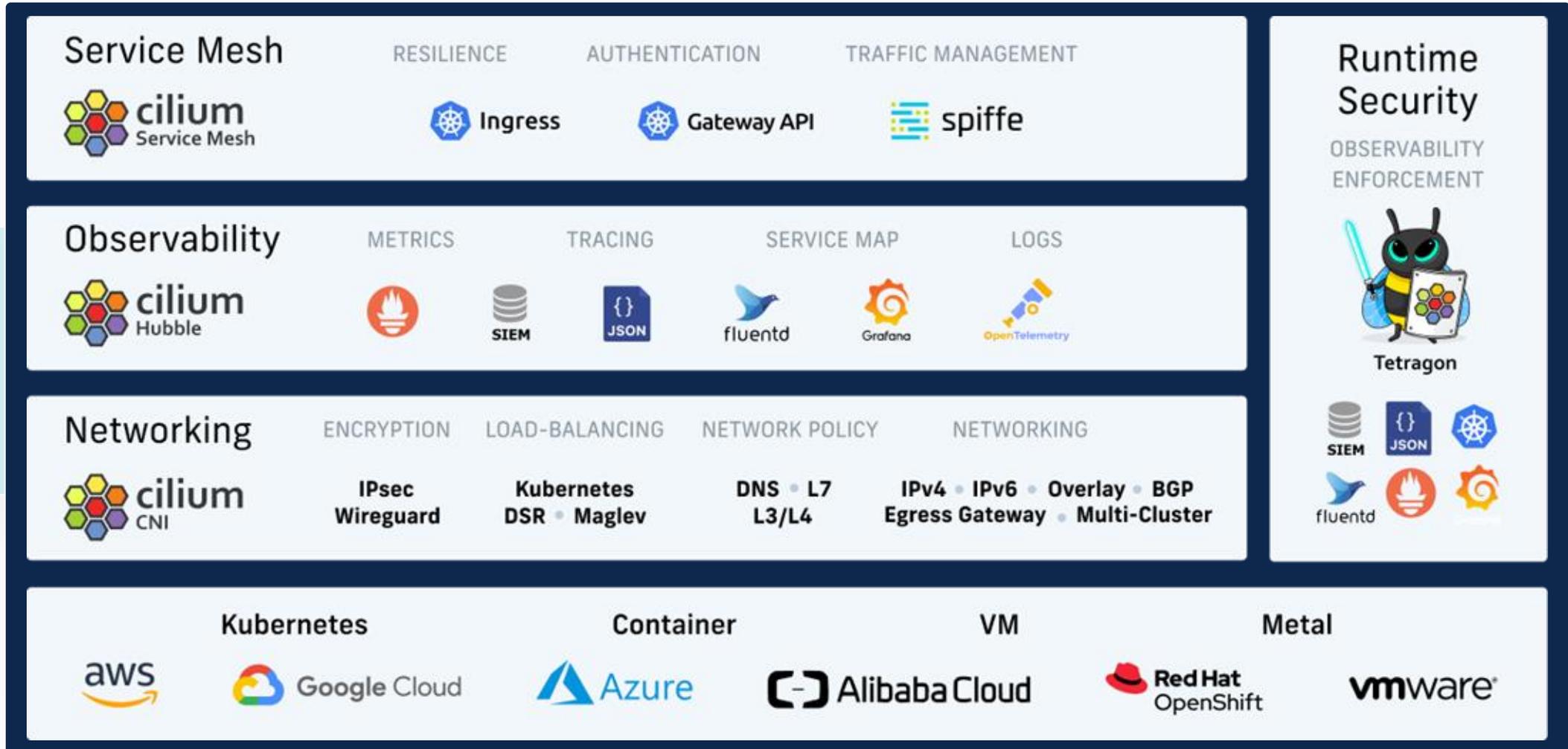


System calls

- eBPF runs in a restricted execution environment
- Before eBPF script is compiled:
 - Verifier ensures things such as memory safety
 - Hardening process (program execution protection, mitigation against spectre, constant blinding, ...)
- eBPF can only access pre-approved kernel functions and data structures

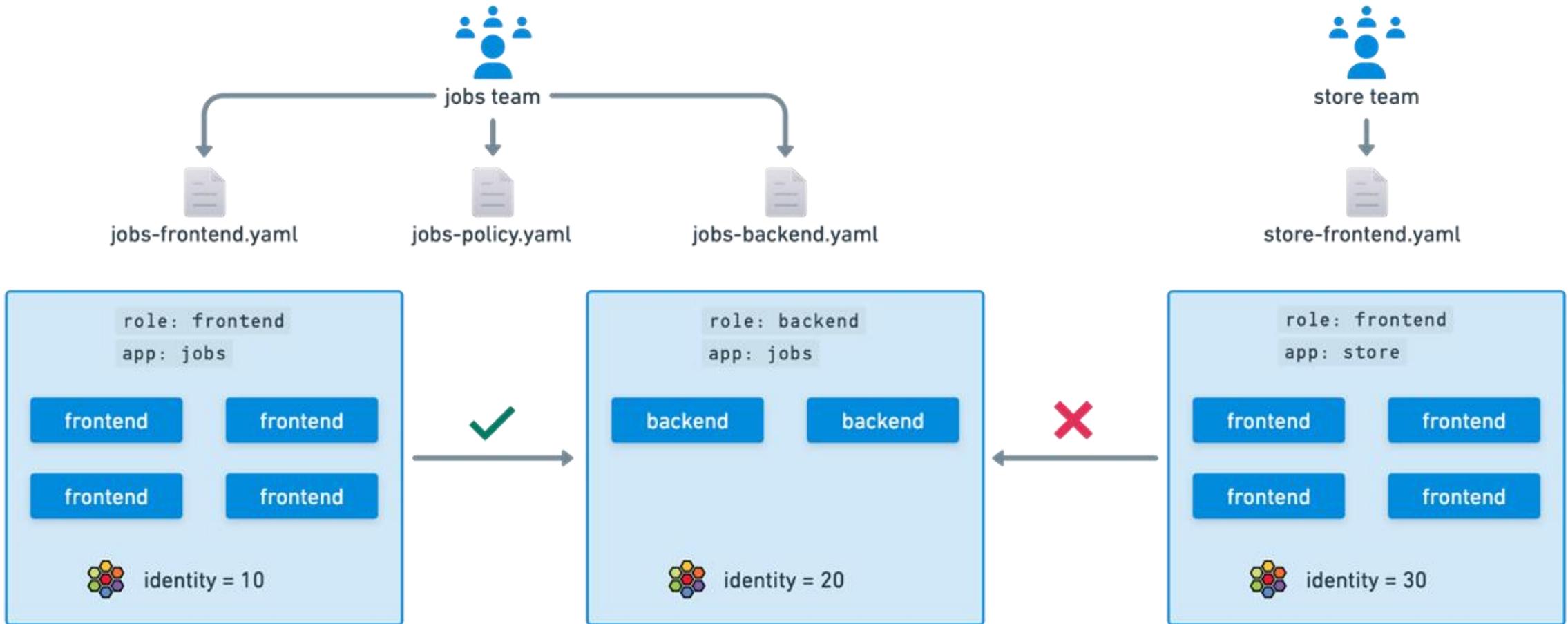
powers many things

Capabilities For Your Cloud Native Journey



Micro-Segmentation

Label based East-West Application or Multi-tenant Security Enforcement



Shaping the future of cloud & cloud native

Observability, Networking & Security with eBPF, Cilium & Tetragon



- Presence in the OS kernel for ultimate efficiency
- Networking & Load Balancing
 - CNI, K8 Service Mesh
- Observability & Security
 - L4-7 traffic, encryption, process, data, file, identity-aware, api-aware

Securing the Application workloads evolution

Cisco Security Cloud Control

Bare Metal

Virtualisation

Public Cloud pilot

Containers Pilot

K8s Full adoption

Embracing Cloud Native



Cisco DC Fabric (ACI, Smart Switches)



Cisco Secure Workload (Agent)



Cisco Secure Firewall



Cisco Secure Workload (Agentless) & Multicloud Defense

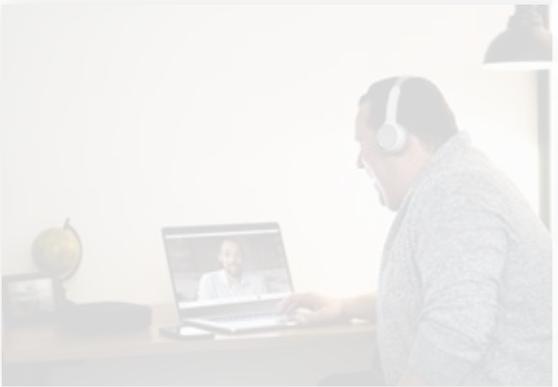
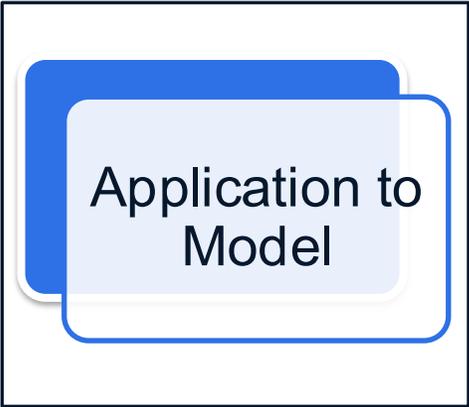
Cisco Secure Workload & Isovalent Enterprise



Hypershield

Cisco Hybrid Mesh Firewall

Zero Trust Use Cases



The Evolution of AI

Rapidly increasing autonomy and capabilities



Agentic AI in Cisco: Automating tasks, reducing friction.

Agents in a Sandbox (Gen AI)

- Creates Output (txt, images..)
- safely generates content and insights in controlled environments with limited access and guardrails

Agents in the real world (Agentic AI)

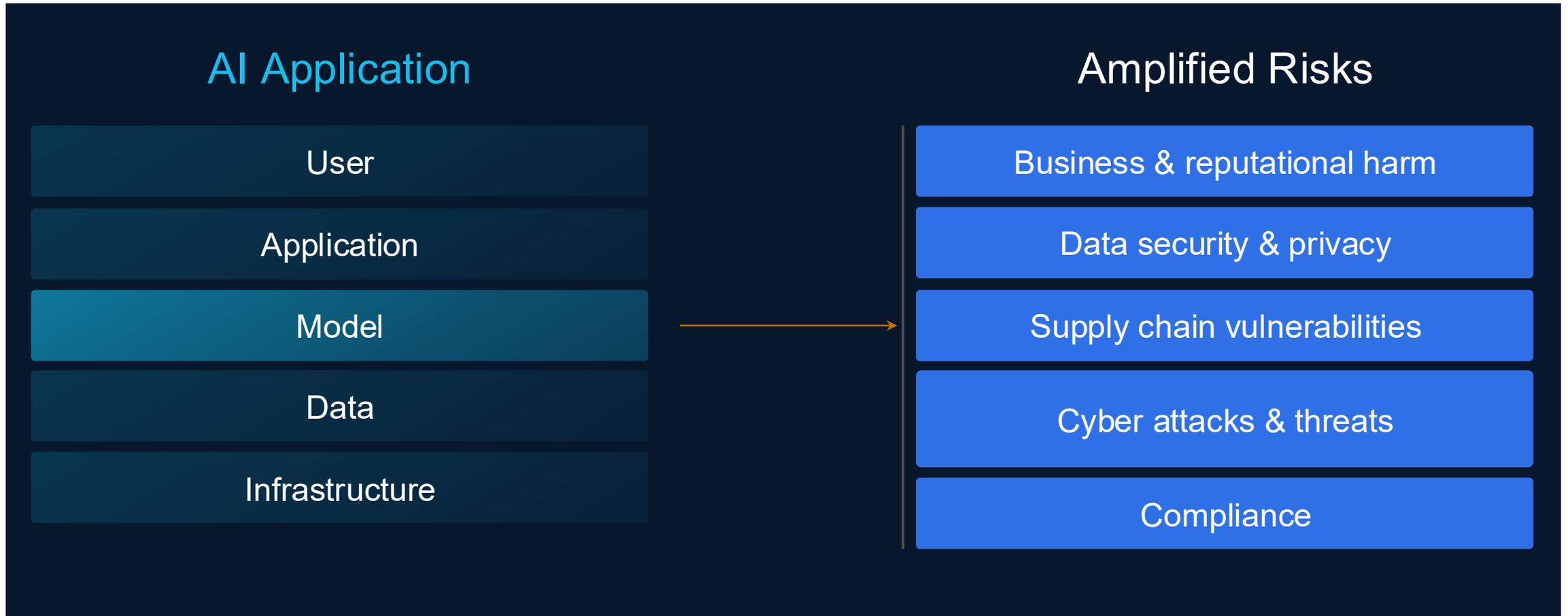
- **Takes Actions like a real user**
- **Agentic AI acts on your behalf. It's AI that can take initiative, interact with systems and data, and complete tasks end-to-end, much like a digital coworker**

Agentic AI is like a model employee – brilliant, tireless, perfect memory, and fully autonomous.

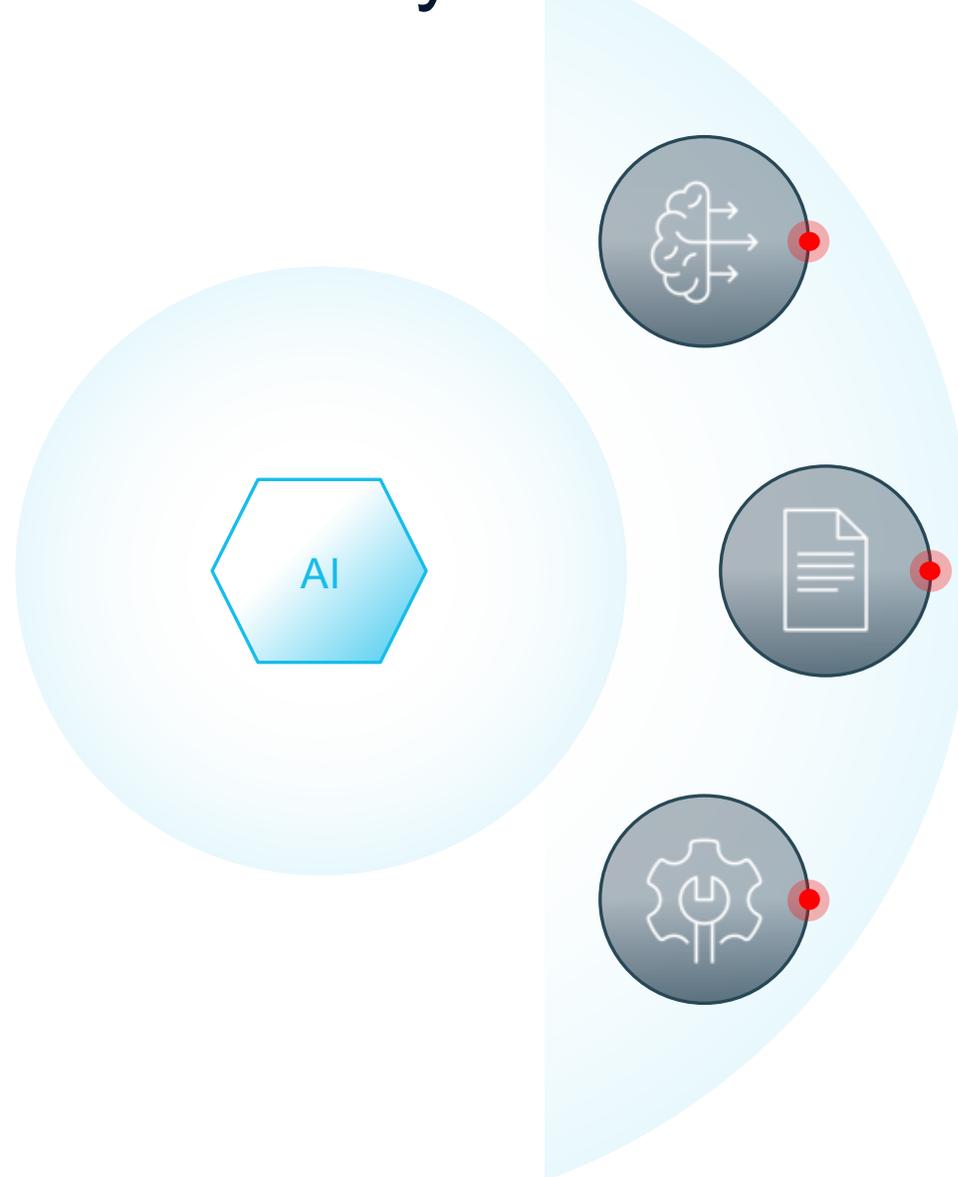
Unfortunately, it's also your least-supervised, immoral, root access user with a knack for outsmarting your defenses!

What's the risk?

AI Applications can be non-deterministic



Third-party AI assets carry risks



Open-source models
1.9M+ on HuggingFace

Risks: Model backdoors & malware

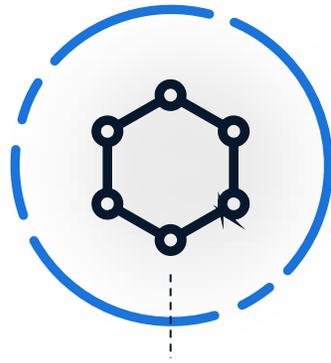
Third-party datasets
450K+ on HuggingFace

Risks: Data poisoning & privacy violations

MCP servers & tools
Thousand across multiple repos

Risks: Tool & server vulnerabilities

Model security is inconsistent



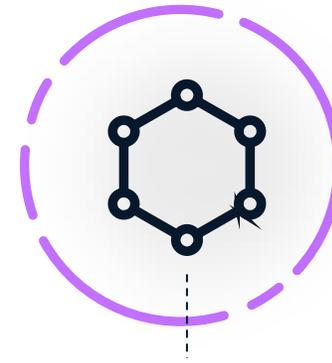
Model A



Model B



Model C

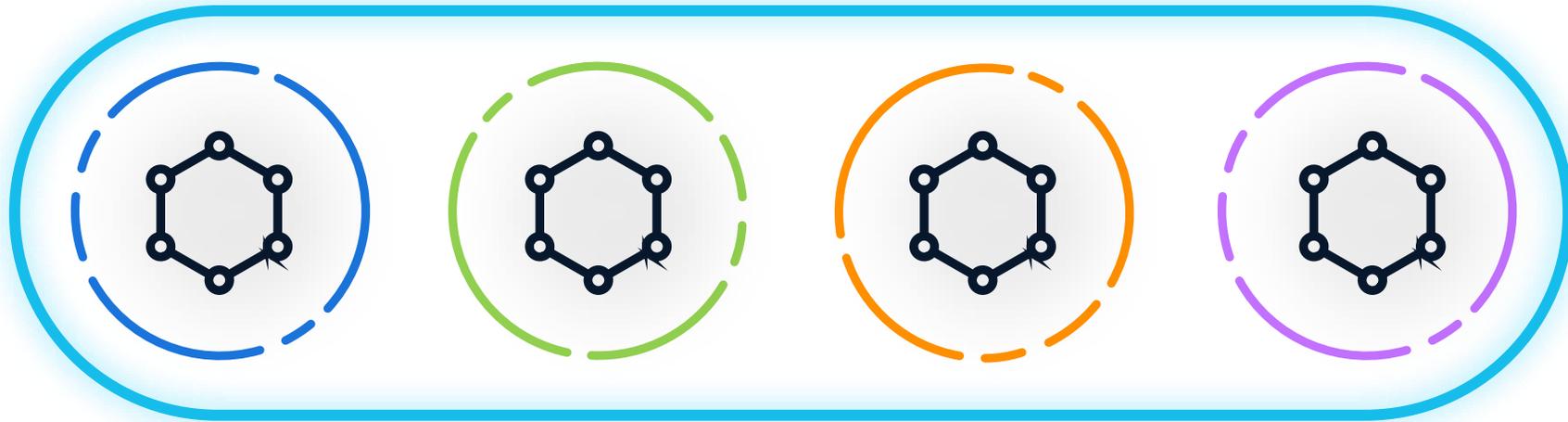


Model D

Built-in guardrails are **different** for each model, optimized for **performance over security**, and **easily broken** when changing the model.

Model security is inconsistent

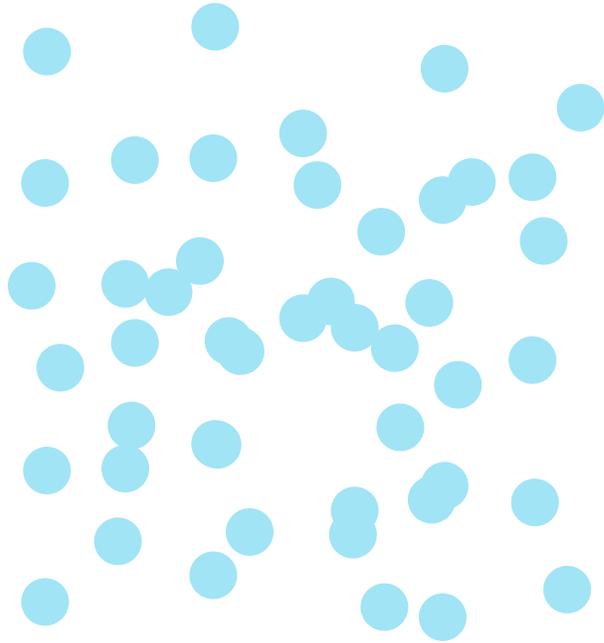
Enterprise Guardrails



Enterprise guardrails provide a **common layer of security** across models, allowing AI teams to focus fully on development.

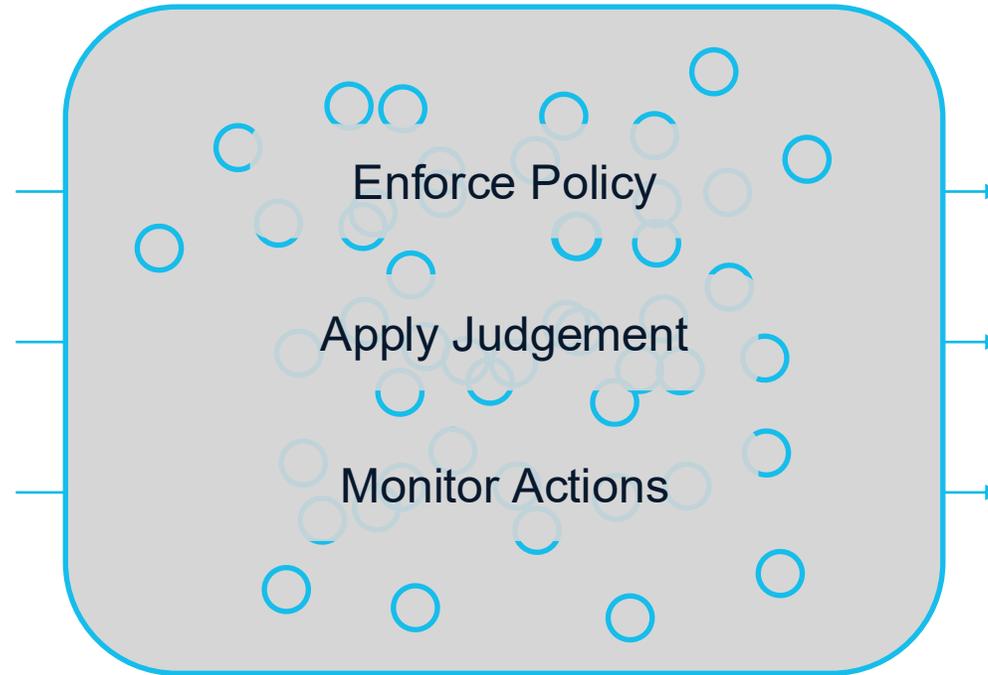
Future: an intelligent layer between agents and resources

Agents



Identify & Authenticate

Zero Trust for Agents



Authorize & Monitor

Resources



Access & Optimize

New Standards for AI Security

The New AI Risk Landscape



Cisco AI Security – Shaping AI Security Standards



- Founding member of MITRE Atlas
- Co-developed the AI Risk Database



- Representing AI Security for National Academies
- Co-organized Hackers on the Hill for Congressional staffers



- Co authored Adversarial AI Taxonomy
- Selected to NIST's AI Safety Institute



- Creating Prompt Injection Taxonomy w/ UK AI Security Institute
- AI Security Hackathon at The National Cyber Security Centre



- Contributors to OWASP Top 10 for LLMs
- Selected as review panelist for Agentic Security initiative



Asia

- Representing AI Safety at APEC Summit in front of South Korean President, Japanese PM
- Partnering with the Japanese Government on AI safety proposal

Cisco's integrated AI security and safety framework

We've started to integrating it into the product – starting with AI Validation

20+ Objectives

The motive or goal behind an attack

Goal Hijacking

Data Privacy Violation

150+ Techniques & Sub-Techniques

A granular understanding of the threats including actions, methods, and variations

Direct Prompt Injection

Multi-Modal Injection Manipulation

Data Exfiltration / Exposure

Instruction Manipulation

Obfuscation

Image-Text Injection

Audio Command Injection

Video Overlay Manipulation

Training Data Exposure

Data Exfiltration via Agent Tooling

5+ Mappings

References to common AI and governance frameworks

OWASP: AAI003:2025, MITRE: AML.T0051.000...

OWASP: AAI003:2025, MITRE: AML.T0051.000...

OWASP: AAI001:2025, NIST: AML.018...

OWASP: AAI001:2025, NIST: AML.018...

OWASP: AAI001:2025, NIST: AML.018...

OWASP: AAI015:2025, MITRE: AML.T0024...

OWASP: AAI015:2025, MITRE: AML.T0086...



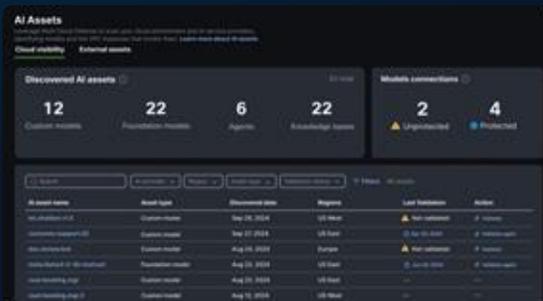
AI Defense: coverage across the AI lifecycle

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.



Protection

AI Runtime Protection

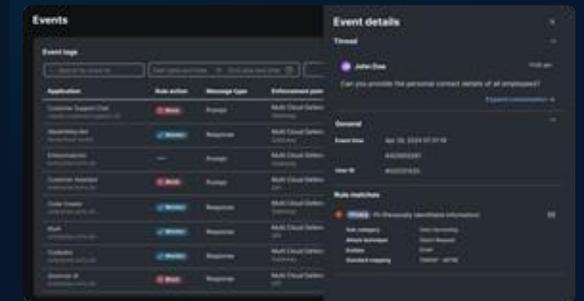
Mitigate threats in real time

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

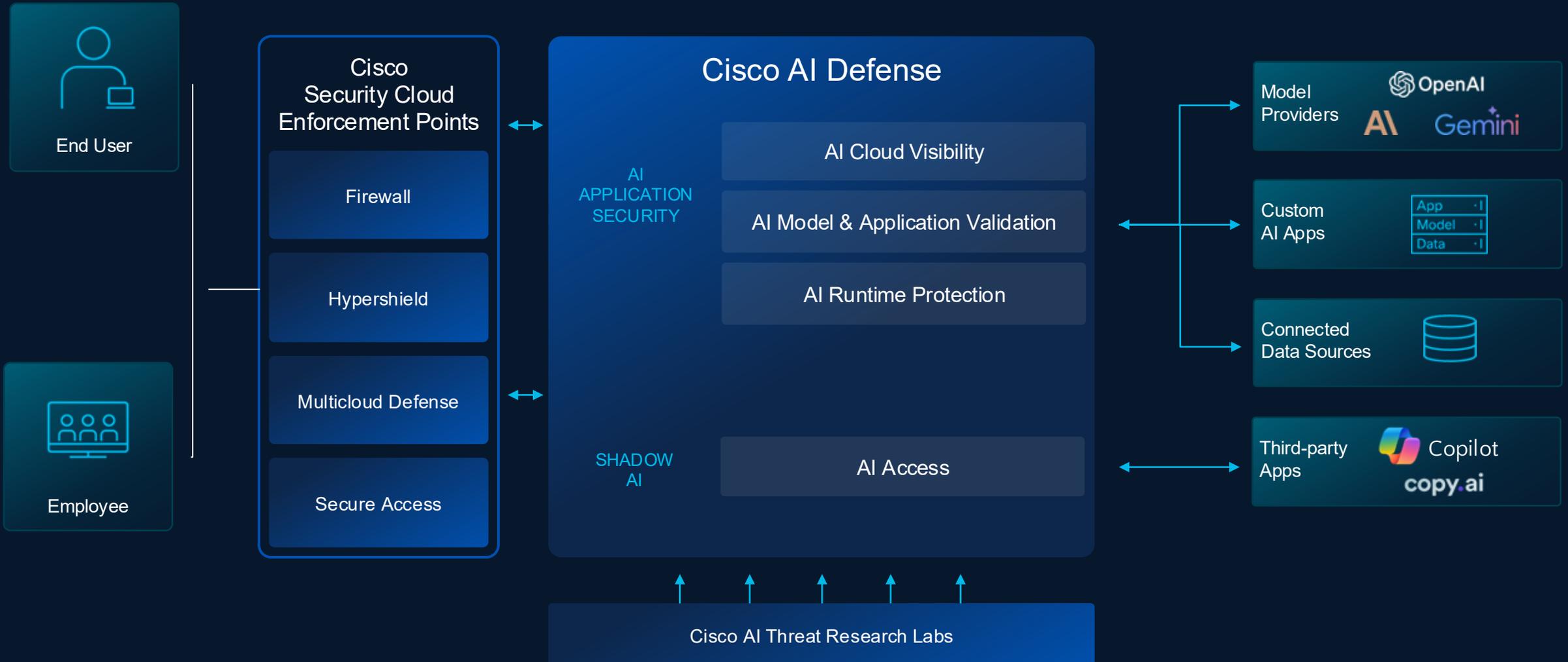
AI Model & App Validation

Detect the vulnerabilities

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



The AI Defense Solution



Discovery: AI Cloud Visibility

- Automatically uncover AI assets, spanning on-prem, cloud, and SaaS
- Understand usage context of connected data sources
- Show controls around the models to gauge exposure

AI Assets
Leverage Multi Cloud Defense to scan your cloud environment and AI service providers, identifying models and the VPC instances that invoke them. [Learn more about AI assets](#)

Cloud visibility External assets

Discovered AI assets 43 total

12	22	6	22
Custom models	Foundational models	Agents	Knowledge bases

Models connections

2	4
⚠️ Unprotected	🔒 Protected

Search [] AI provider [v] Region [v] Asset type [v] Validation status [v] Filters 48 results

AI asset name	Asset type	Discovered date	Regions	Last Validation	Action
int.chatbot.v1.5	Custom model	Sep 29, 2024 02:44:19	US West	⚠️ Not validated	🔗 Validate
customer.support.d2	Custom model	Sep 27, 2024 02:44:19	US East	📅 Apr 29, 2024	🔗 Validate again
doc.review.bot	Custom model	Aug 24, 2024 02:44:19	Europe	⚠️ Not validated	🔗 Validate
meta.llama3-2-3b-instruct	Foundation model	Aug 22, 2024	US East	📅 Jun 29, 2024	🔗 Validate again
cust.booking.mgr	Custom model	Aug 22, 2024	US East	—	—
cust.booking.mgr.2	Custom model	Aug 12, 2024	US West	—	—

Complete Solution for building AI Apps

1

Platform Advantage

Security at the network layer

- Network-level data insights provide full visibility into AI traffic and associated risks
- Fast, low-friction deployment that does not modify the app
- Enforce policies across and within clouds and datacenters

2

AI Model & App Validation

Algorithmic AI red teaming

- Automated assessment of safety and security vulnerabilities
- AI readiness guides bespoke guardrail and enforcement policy
- Automatic integration into CI/CD workflows for seamless, continuous testing

3

Proprietary Model & Data

Purpose-built for AI security

- Team pioneered breakthroughs from algorithmic jailbreaking to the industry's first AI Firewall
- Contribute to (and align with) NIST, MITRE, and OWASP
- Leverage threat intelligence data from Cisco Talos & Cisco AI security research teams

Thank you

