

Solving Devops and Secops challenges with Cisco Cloud Security

cisco Live !

Fabien Gandola
Awesome Security Architect (ASA)

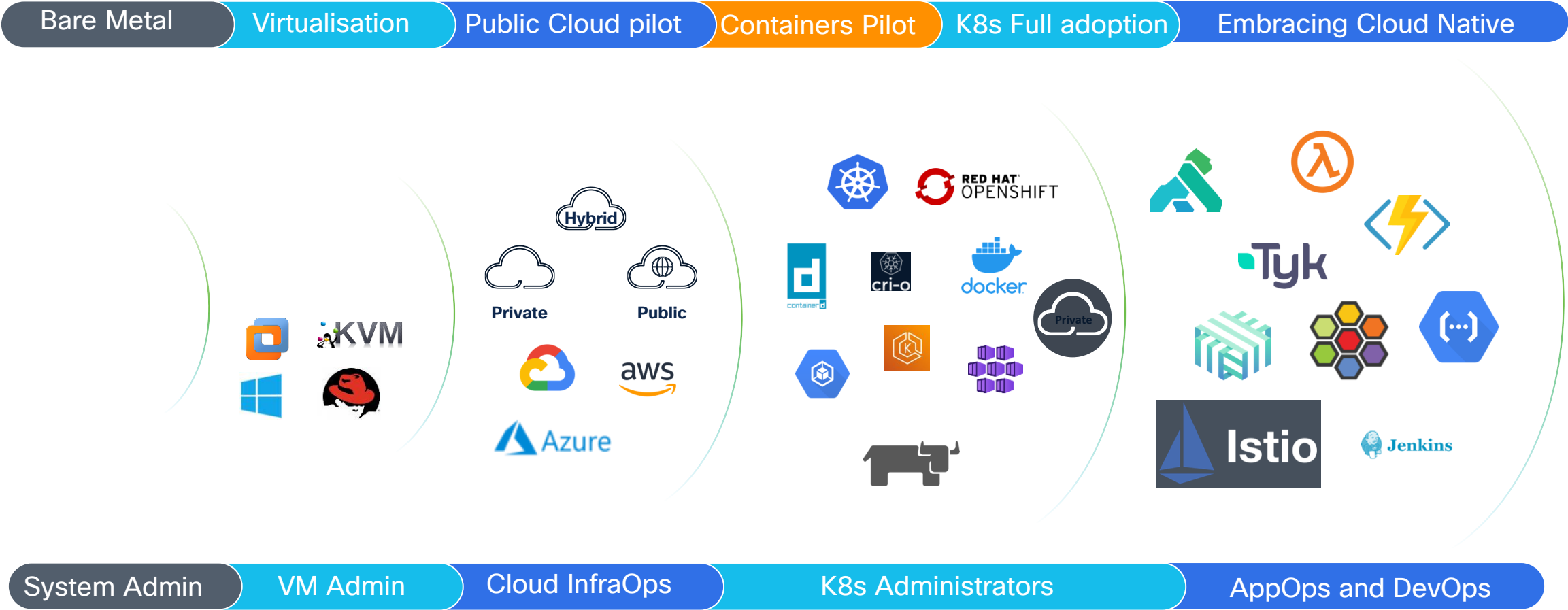
Jatin Sachdeva
Firewall Technical Director (FTD)

Experiment





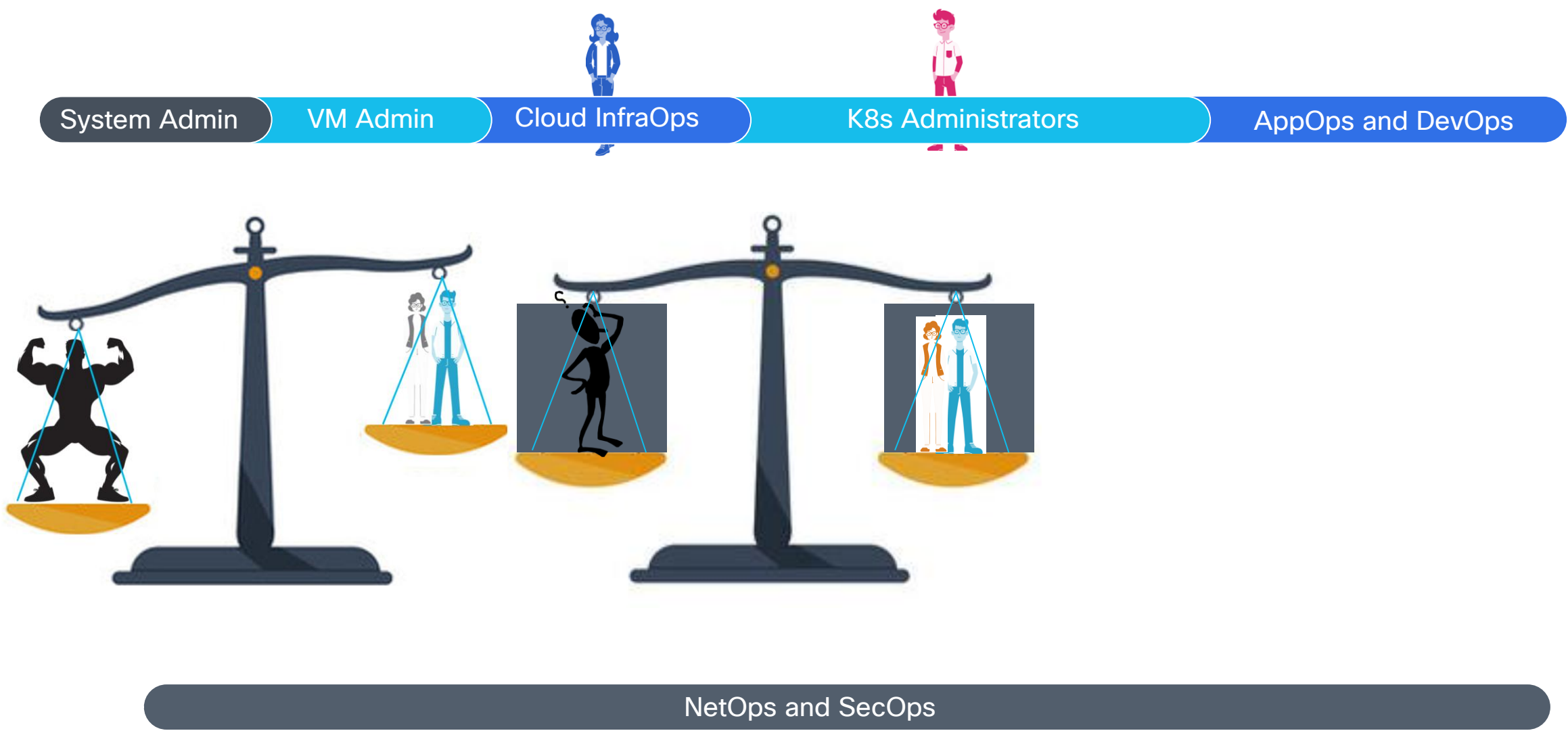
Application workloads evolution



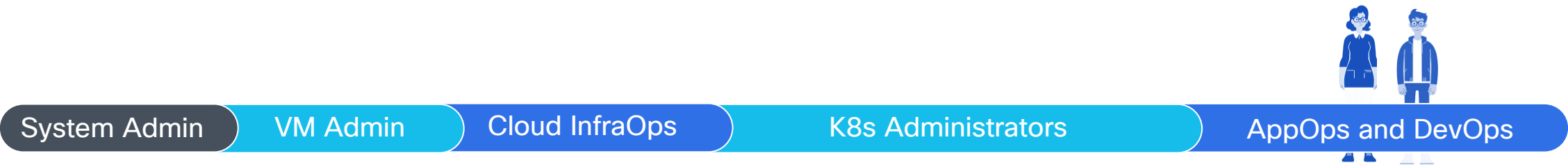
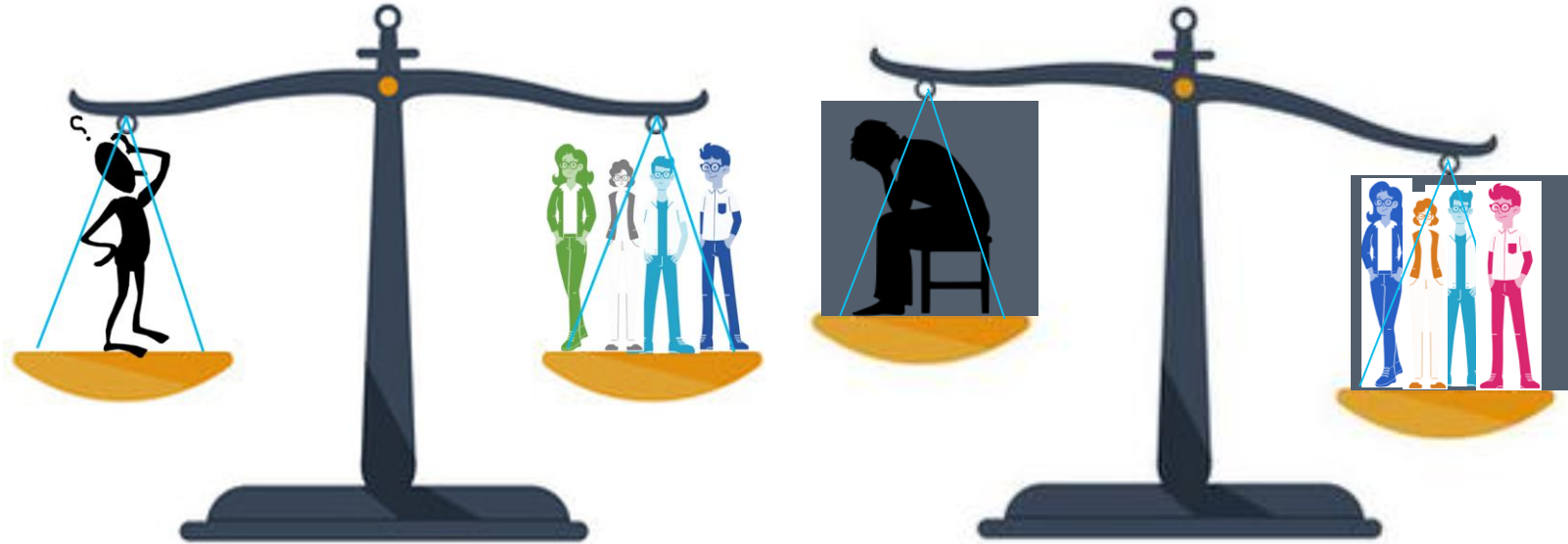
Shift in balance of power ?



Shift in balance of power ?

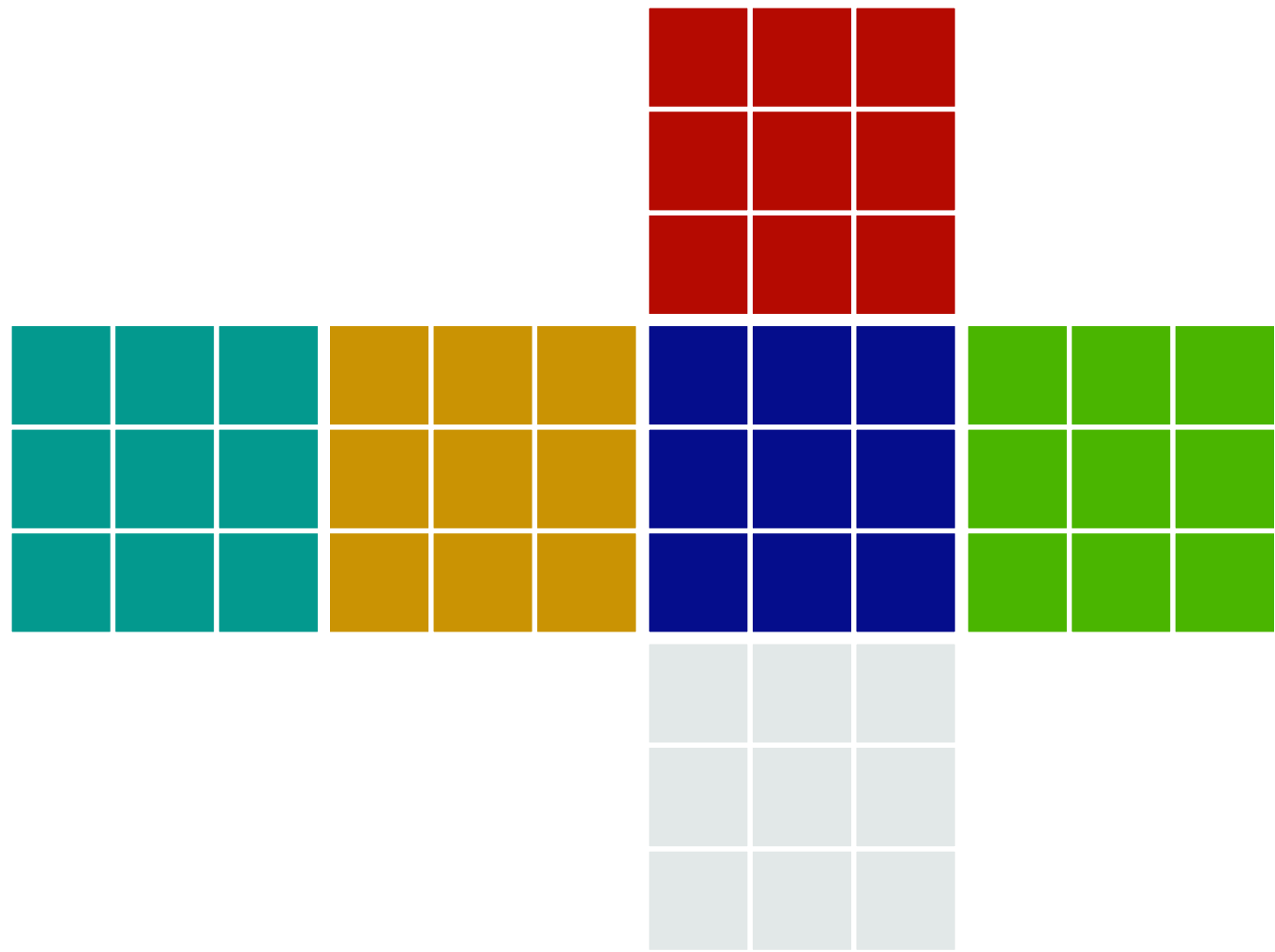


Shift in balance of power ?

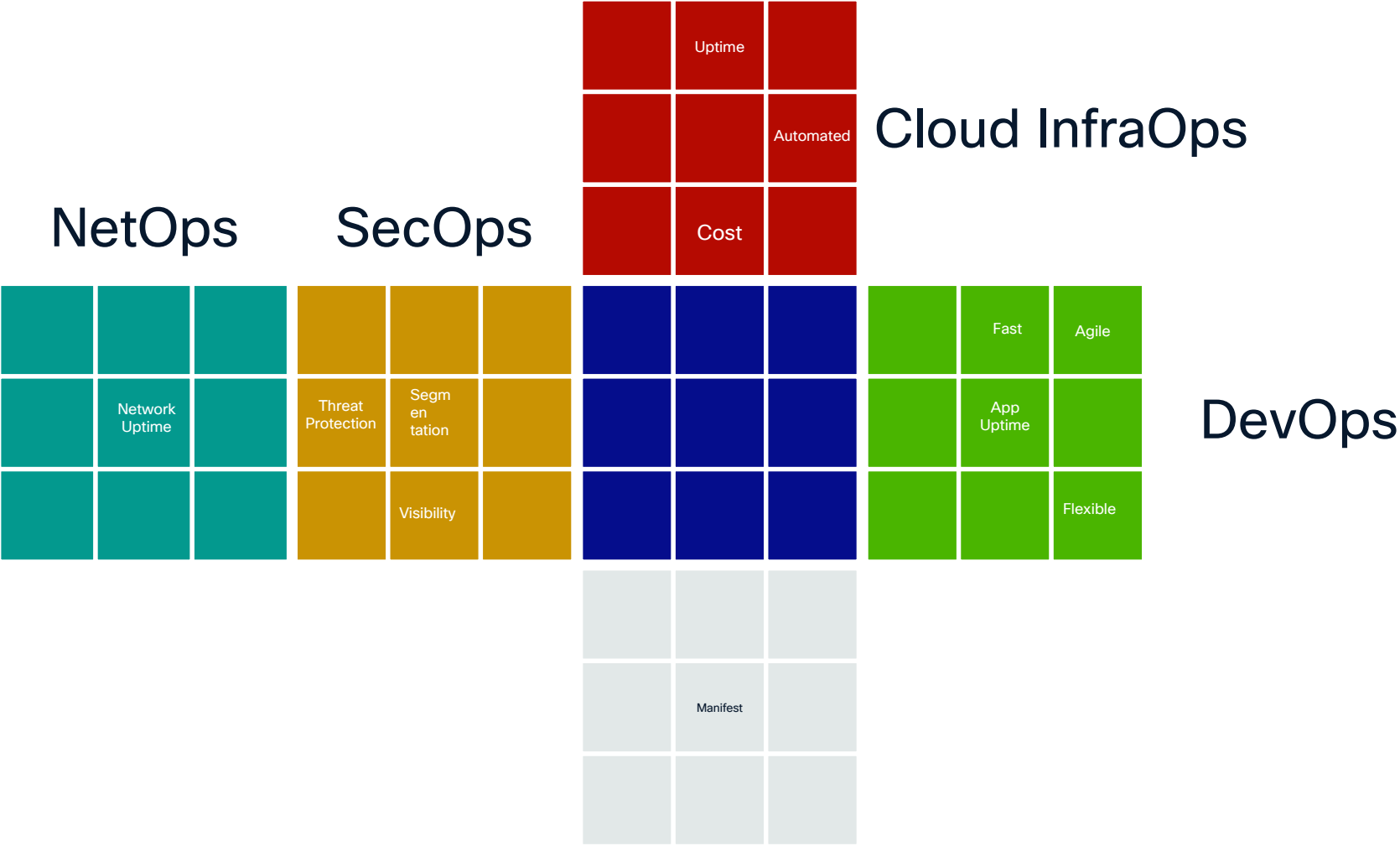


NetOps and SecOps

Cloud Security use cases



Cloud Security use cases



Objectives



Security can be
an enabler



How devops and
secops teams can
better work together



Multiple paths to
securing Cloud &
Apps



Cisco can help with
this Journey

What (not) to expect



No deep dive on Cisco Products

No configuration guide

No troubleshooting

Related Sessions

How to Build a Secure Multi-Cloud Environment with Cisco Secure Workload and Multicloud Defense [BRKSEC-2421]

Solving the Segmentation Puzzle with Secure Workload! [BRKSEC-2161]

Introduction to eBPF! [BRKSEC-2169]

Cisco Hypershield: Mastering Next-Generation Security [BRKSEC-2265]

It's Cats vs Rats Going Hybrid! Attack and Defense in the Cloud [BRKSEC-2485]

What (not) to expect



- No deep dive on Cisco Products
- No configuration guide
- No troubleshooting
- No PhD in Cloud
- No Hypershield



- Acknowledge the challenges from the different teams
- Introduction to Cisco Security cloud native solutions
- Very pragmatic approach
- Dealing with exotic accent

Agenda

- 01 Introduction
- 02 Challenges
- 03 Segmentation

- Public Cloud
- Cloud Native

- 04 Vulnerabilities Management
- 05 Artificial Intelligence
- 06 Conclusion

Who are we?

“It works
on my
machine”



Jatin Sachdeva
Principal Architect

DevOp Manager

Application

Network
&
Security

“It's not
the
network”



Fabien Gandola
Technical Solutions
Architect

NetSecOp Manager

Application

Network
&
Security

NetsecOp complains



Unknown applications unsecured in Public Cloud



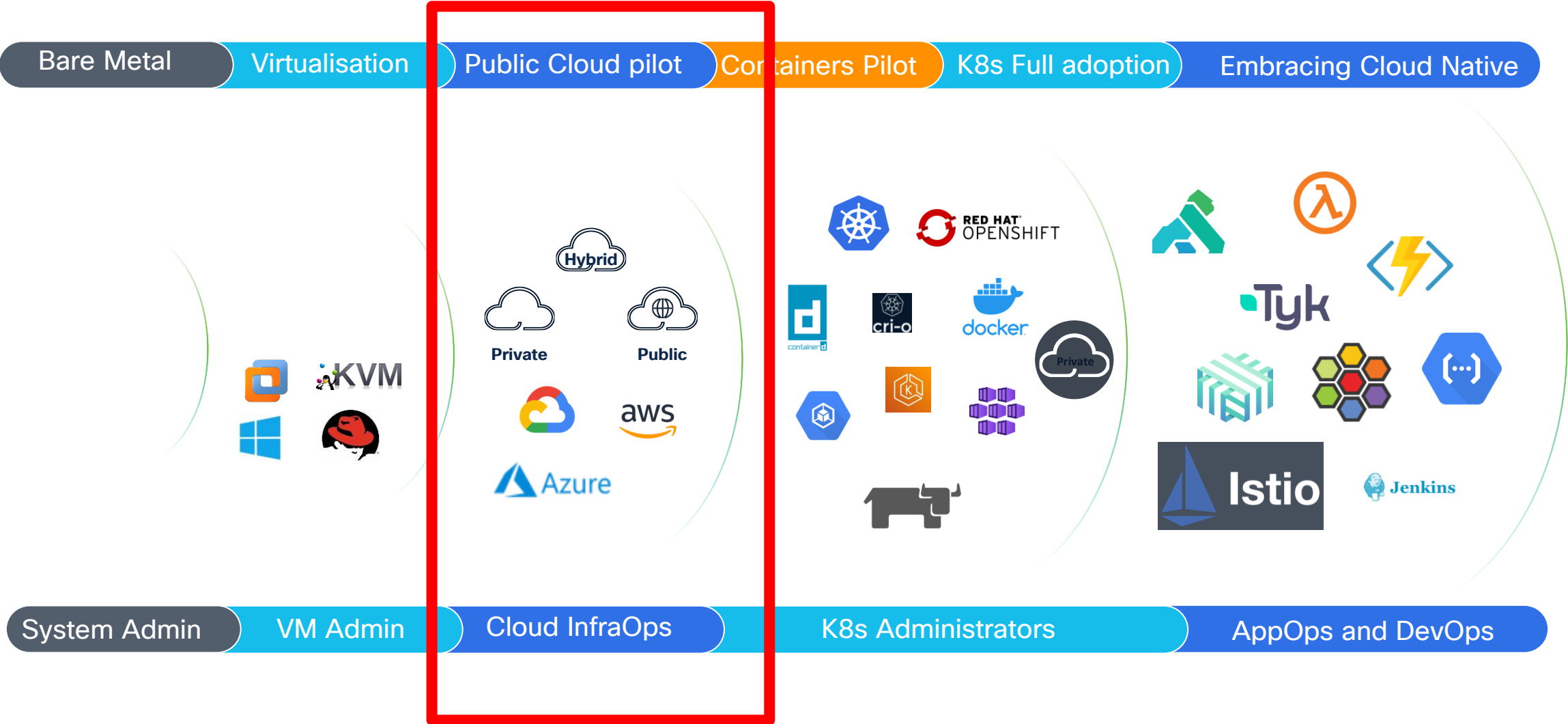
Applications Filled with Vulnerabilities



Segmentation can't keep up

Move to public cloud

Application workloads evolution



What your developers didn't tell you

Apps are growing at rapid pace, and security has no clue till an incident/audit happened

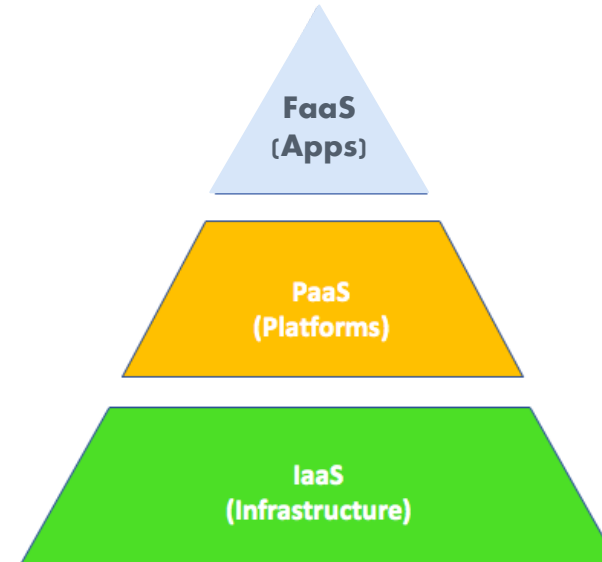
Can I get a view of my external facing apps?

What cloud providers are being used?

Are my external facing apps exposed or vulnerable?



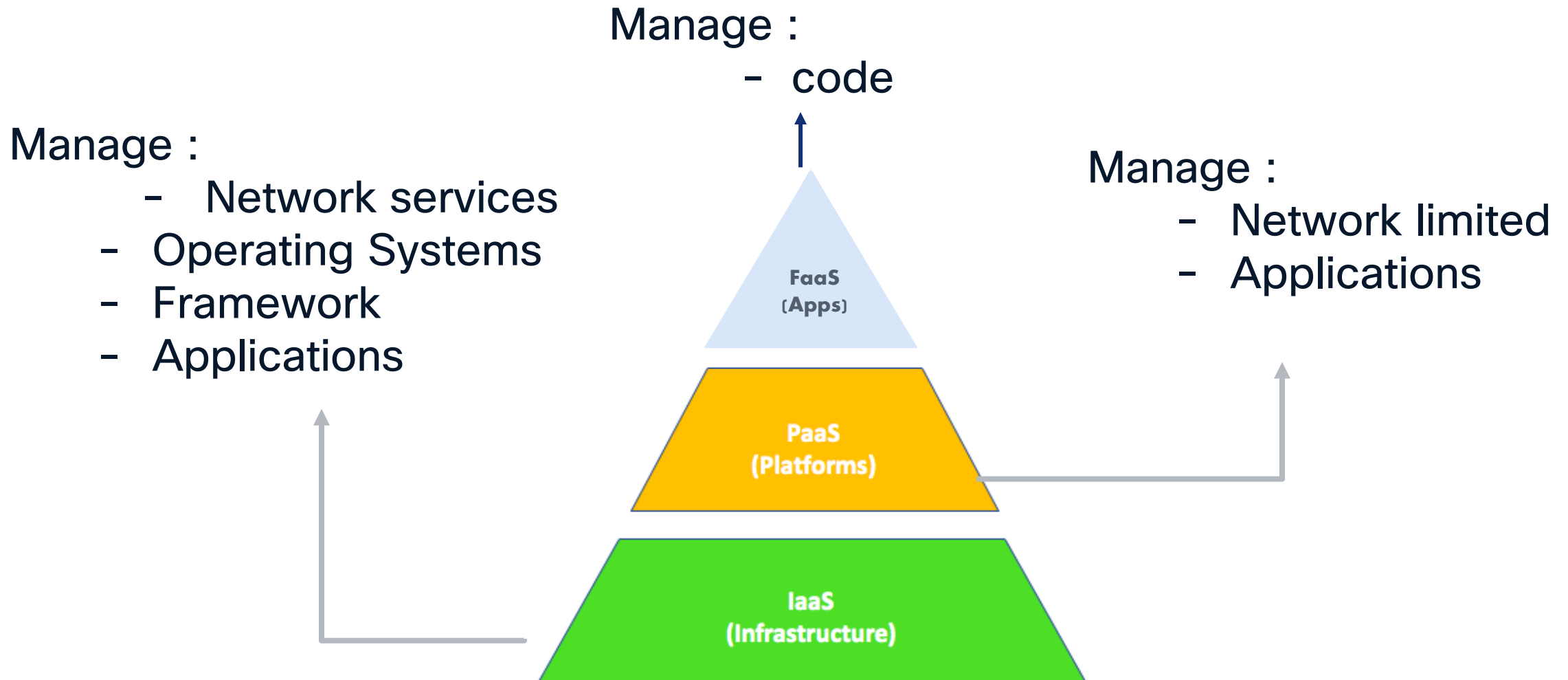
Two new parameters to consider in Cloud



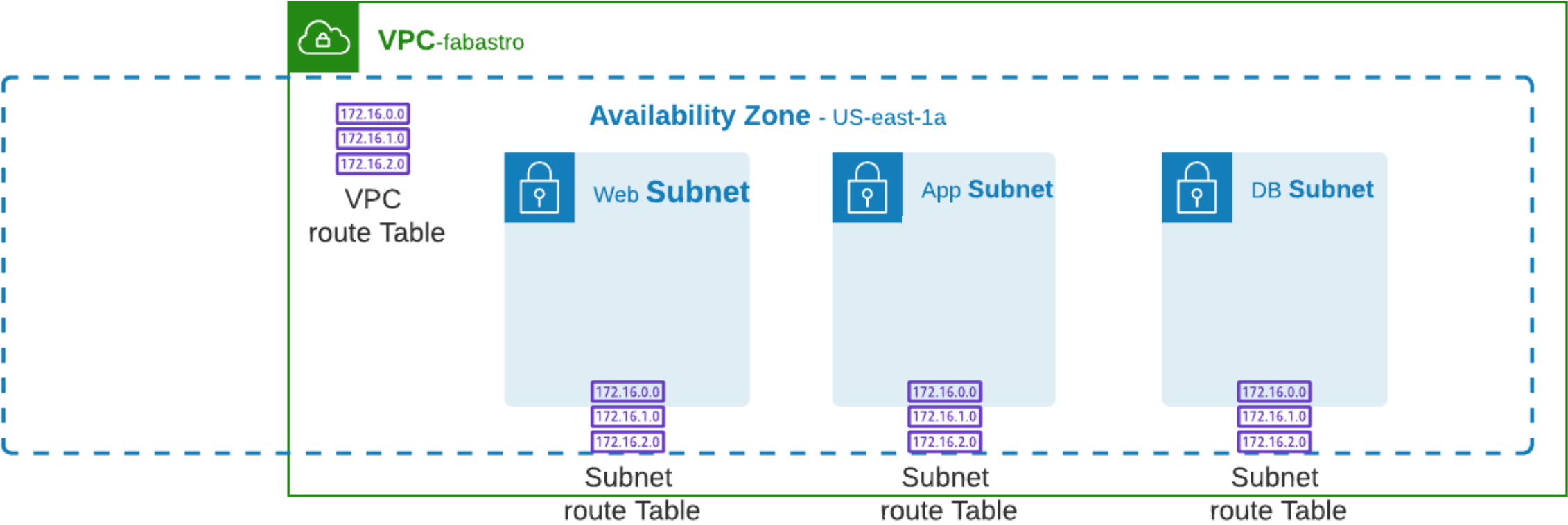
New Infrastructure skills for each Service
Cloud Providers

Public Cloud Service Model

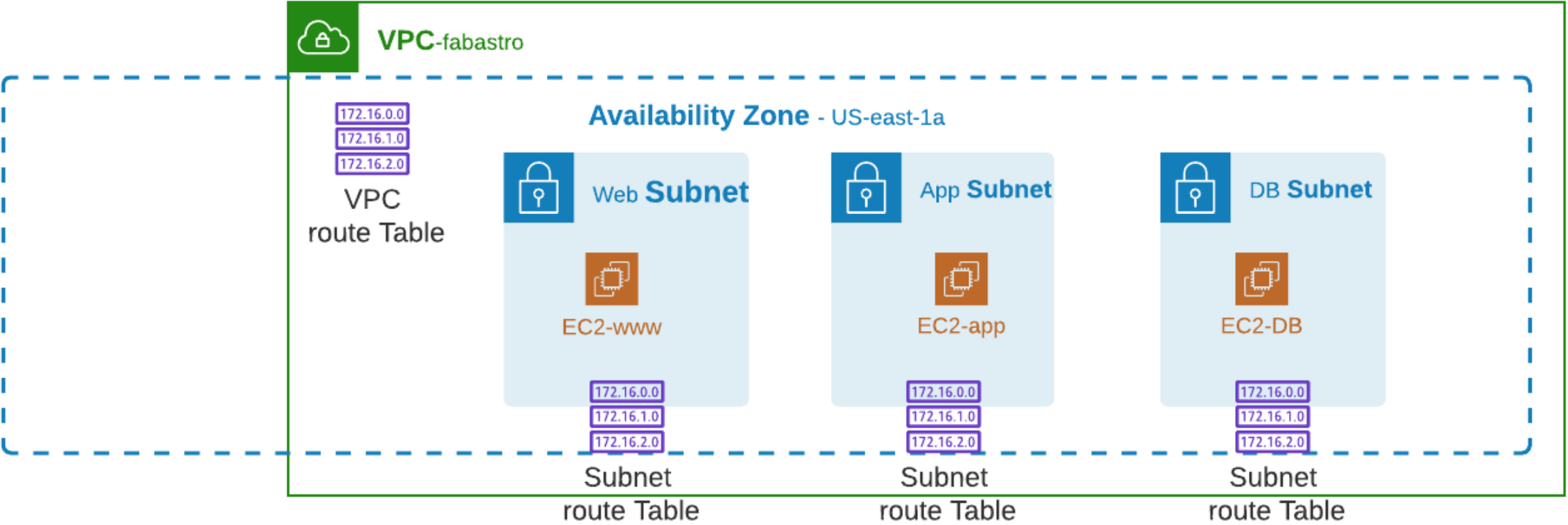
IaaS compared to PaaS Compared to FaaS



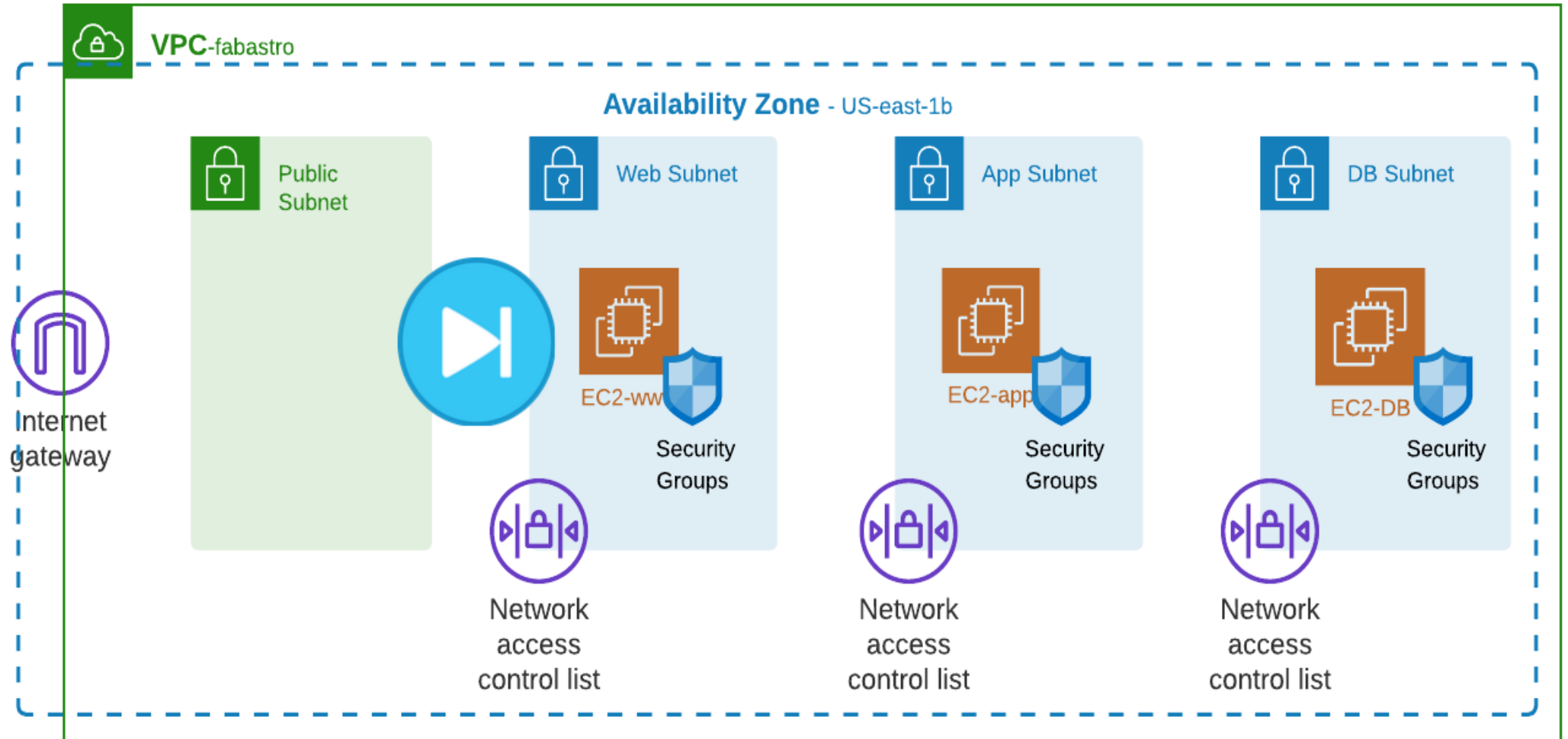
My VRF... VPC sort of (actually Route Tables)



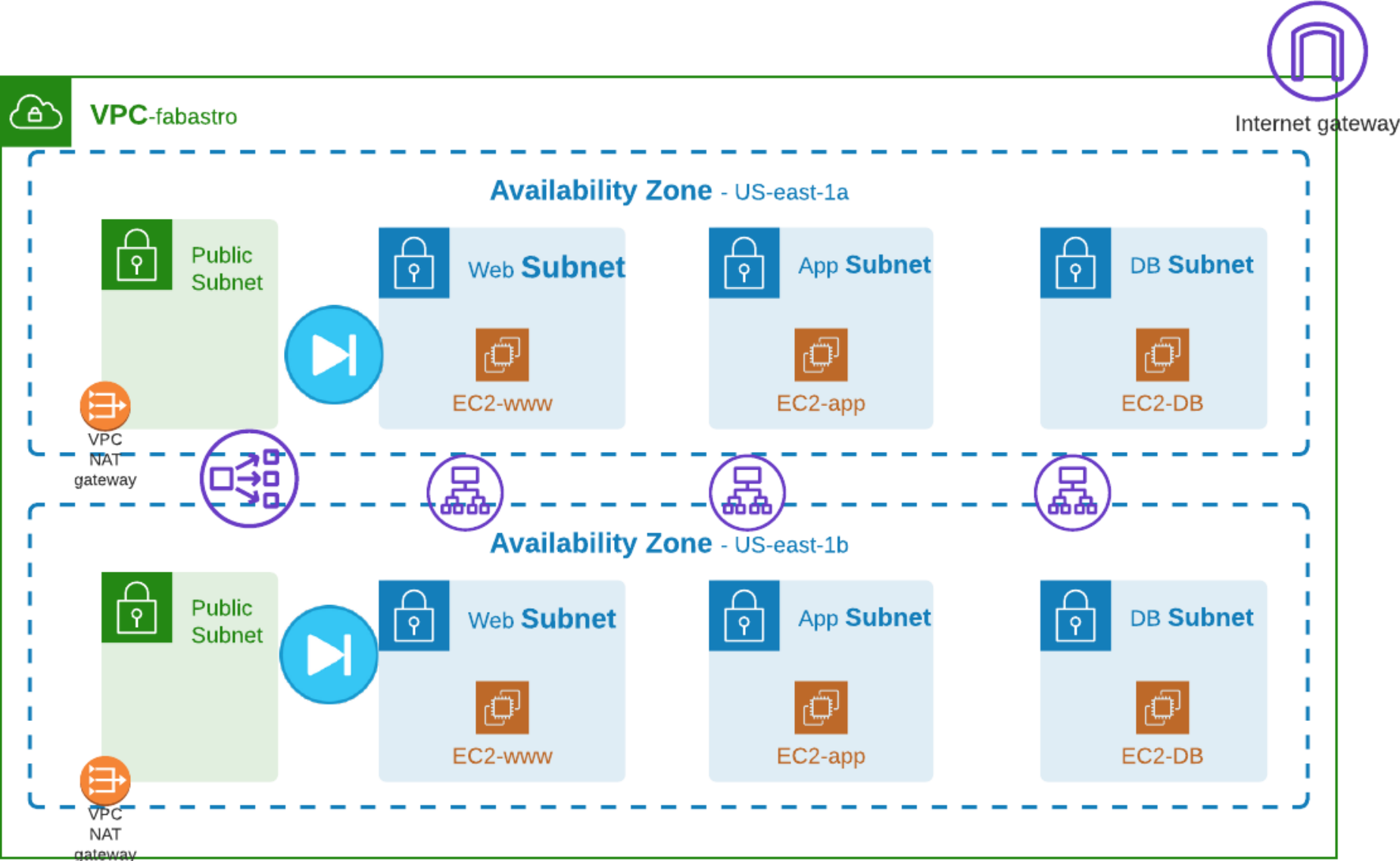
In AWS IaaS... my workloads = Instances



Firewall in front of the “Application” VPC



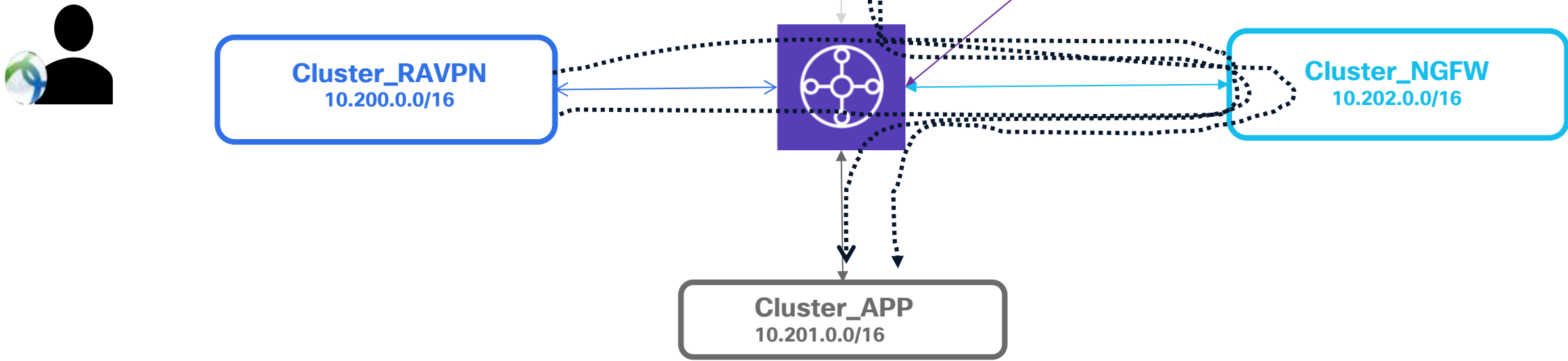
FTD insertion with HA



Limits of this design



Centralized Security Insertion



tgwrouteRAVPN

10.199.1.0/24 → insideRAVPNENIA
10.199.2.0/24 → insideRAVPNENIB
0.0.0.0/0 → ravpntgtVPCattachment

insARouteTableRAVPN

10.201.0.0/16 → TGW-attach-VPC-ravpn
10.204.0.0/16 → TGW-attach-VPC-ravpn

insBRouteTableRAVPN

10.201.0.0/16 → TGW-attach-VPC-ravpn
10.204.0.0/16 → TGW-attach-VPC-ravpn

mgntRouteTableRAVPN

0.0.0.0/0 → IGClusterRAVPN
10.203.0.0/16 → TGW-attach-VPC-ravpn

outsideAZa TableRAVPN

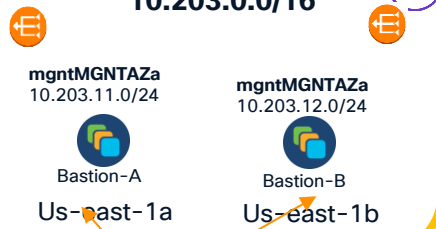
0.0.0.0/0 → IGClusterRAVPN

mgntTableMGNT

10.201.0.0/16 → mgnytgtVPCattachment
10.202.0.0/16 → mgnytgtVPCattachment
10.204.0.0/16 → mgnytgtVPCattachment
10.200.0.0/16 → mgnytgtVPCattachment
0.0.0.0/0 → IGClusterAPP

Cluster_mgnt

vpc-0884c73ab1840747e
10.203.0.0/16



TGW rt MGNT

10.202.0.0/16 → ngfwtgtVPCattachment
10.200.0.0/16 → ravpntgtVPCattachment
10.201.0.0/16 → apptgtVPCattachment
10.204.0.0/16 → vpnroutertgtVPCattachment

TGW rt Inspection

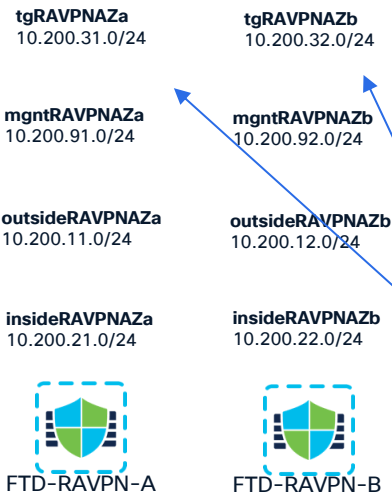
10.199.0.0/16 → ravpntgtVPCattachment
10.200.0.0/16 → ravpntgtVPCattachment
10.201.0.0/16 → apptgtVPCattachment
10.203.0.0/16 → mgnytgtVPCattachment

TGW rt SPOKE

0.0.0.0/0 → ngfwtgtVPCattachment
10.203.0.0/16 → mgnytgtVPCattachment

Cluster_RAVPN

vpc-0bb0e7dc4edfa6848
10.200.0.0/16



tgAPPAZaRouteTableAPP

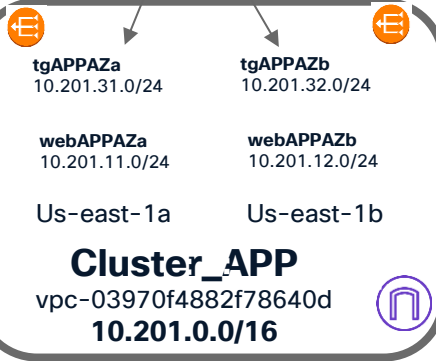
0.0.0.0 → IGClusterAPP

APP rt web Aza

10.199.0.0/16 → TGW-attach-VPC-APP
10.200.0.0/16 → TGW-attach-VPC-APP
10.201.0.0/16 → LOCAL
10.203.0.0/16 → TGW-attach-VPC-APP
10.204.0.0/16 → TGW-attach-VPC-APP
0.0.0.0/0 → NATgw4websolarA

Cluster_APP

vpc-03970f4882f78640d
10.201.0.0/16



TransitGateway Solar



Cluster_NGFW

vpc-031a746e4abb1b2ed
10.202.0.0/16



RouteNGFW

10.202.101.0/24 → LOCAL
0.0.0.0 → ngfwtgtVPCattachment

tgAZa RouteNGFW

10.202.0.0/16 → LOCAL
0.0.0.0/0 → egwlbNGFWendpointa
10.203.0.0/16 → ngfwtgtVPCattachment

tgAZb RouteNGFW

10.202.0.0/16 → LOCAL
0.0.0.0/0 → egwlbNGFWendpointb
10.203.0.0/16 → ngfwtgtVPCattachment

mgntTableNGFW

10.203.0.0/16 → mgnytgtVPCattachment
0.0.0.0/0 → IGClusterAPP

APP rt web Azb

10.199.0.0/16 → TGW-attach-VPC-APP
10.200.0.0/16 → TGW-attach-VPC-APP
10.201.0.0/16 → LOCAL
10.203.0.0/16 → TGW-attach-VPC-APP
10.204.0.0/16 → TGW-attach-VPC-APP
0.0.0.0/0 → NATgw4websolarA

Multi-Cloud Security configuration complexity

What do we need to
configure?

Security VPCs

VPC and DNS Flow Log capture

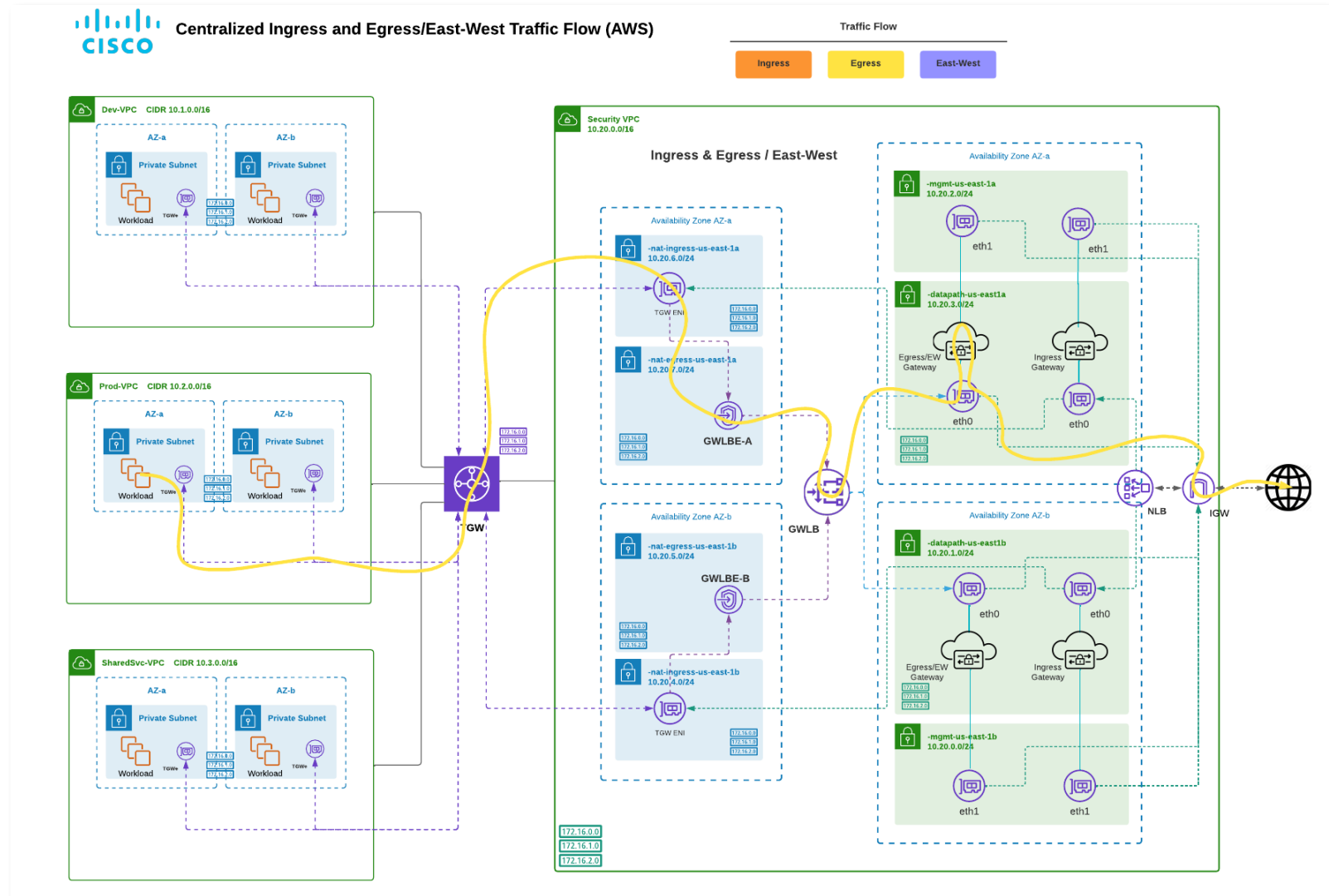
Network Load Balancer

Gateway Load Balancers

Multicloud Defense Gateways
(Deployment, Insertion, Autoscaling)

AWS Transit Gateways
(New or existing, TGW attachment)

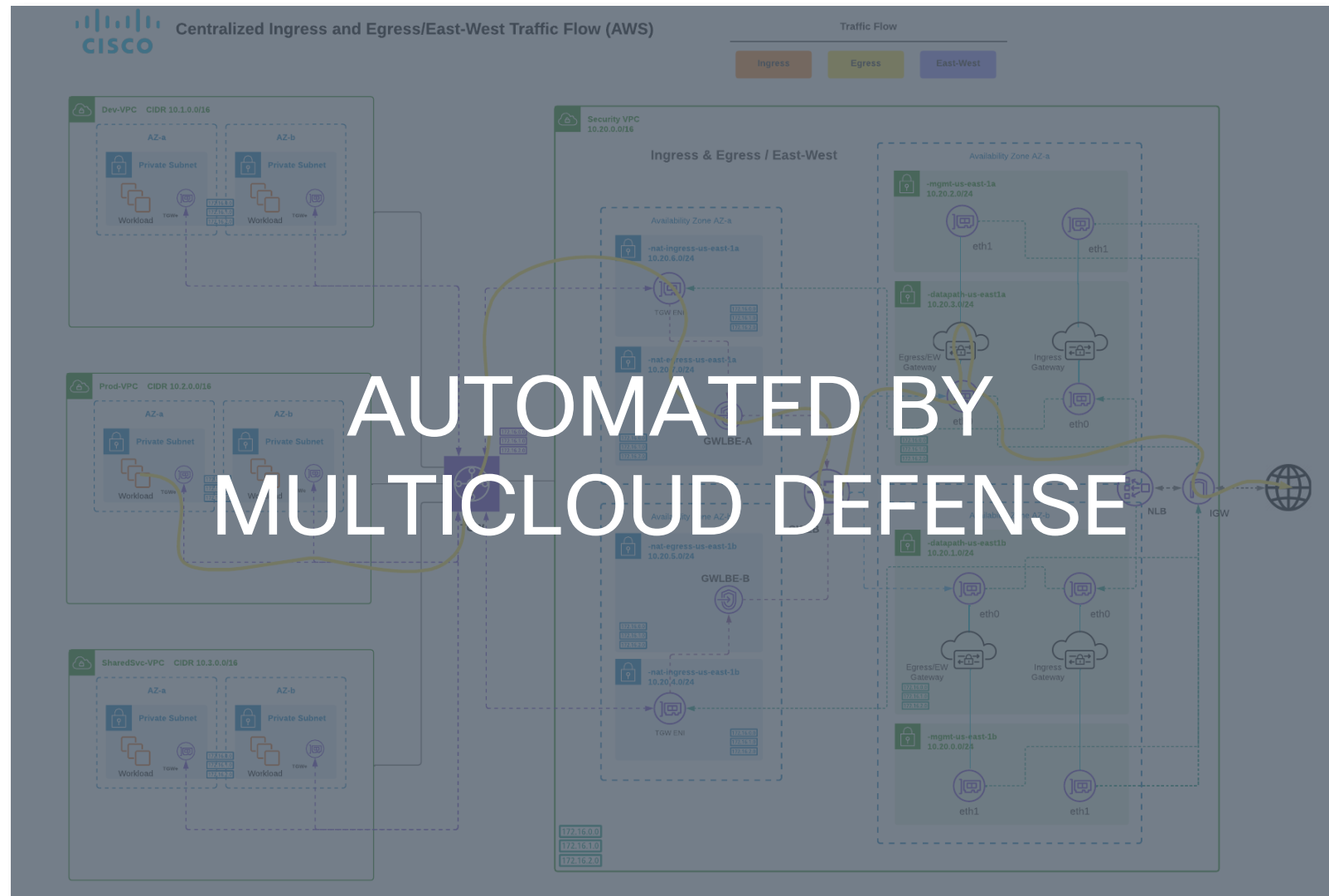
VPC subnet routing to TGW



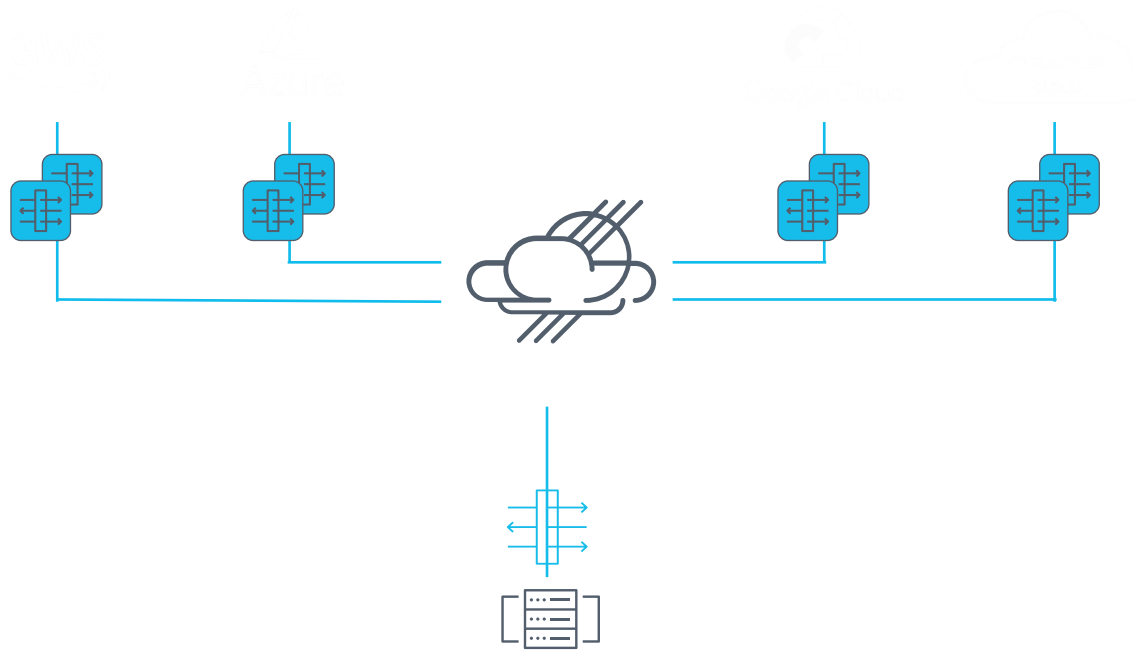
Cisco Multicloud Defense automates orchestration

What do we need to
configure?

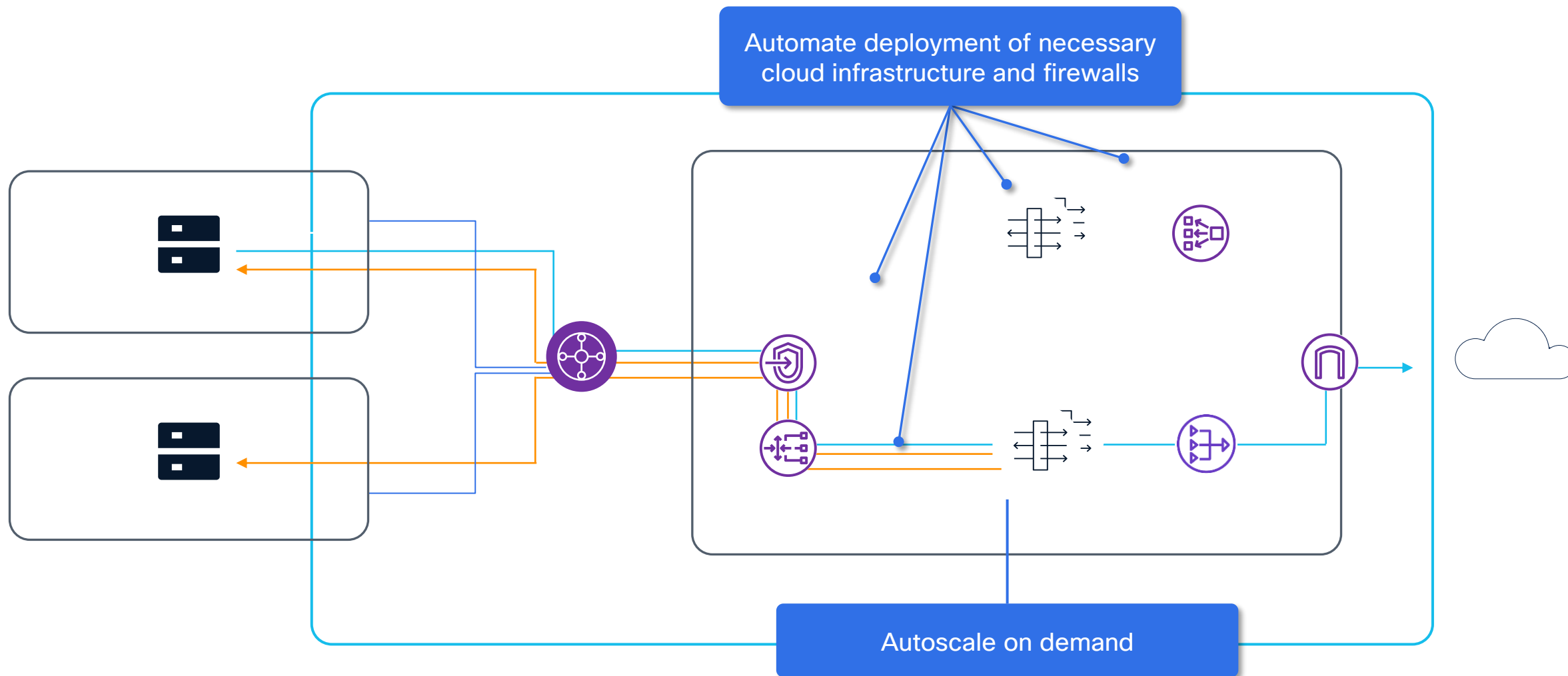
AUTOMATED
BY
MULTICLOUD
DEFENSE



Extending Firewalling to the cloud, *natively*

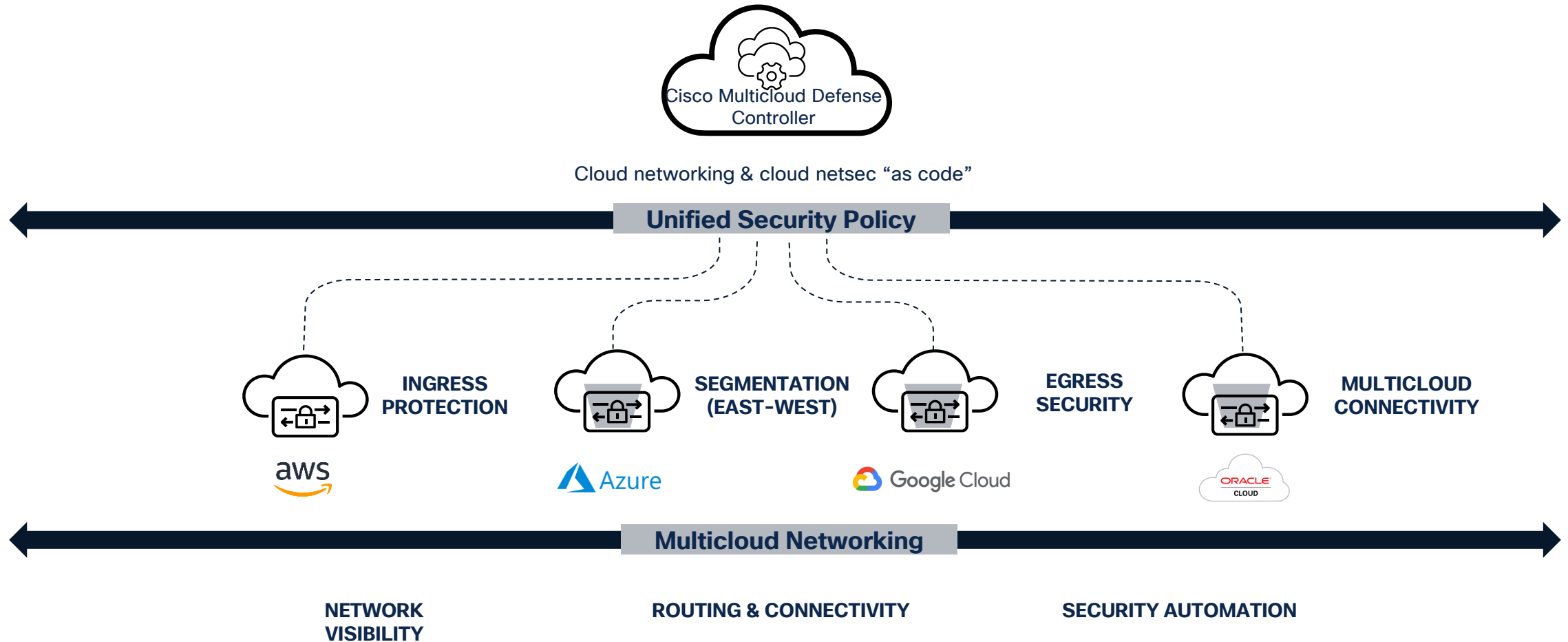


-
-
-
-



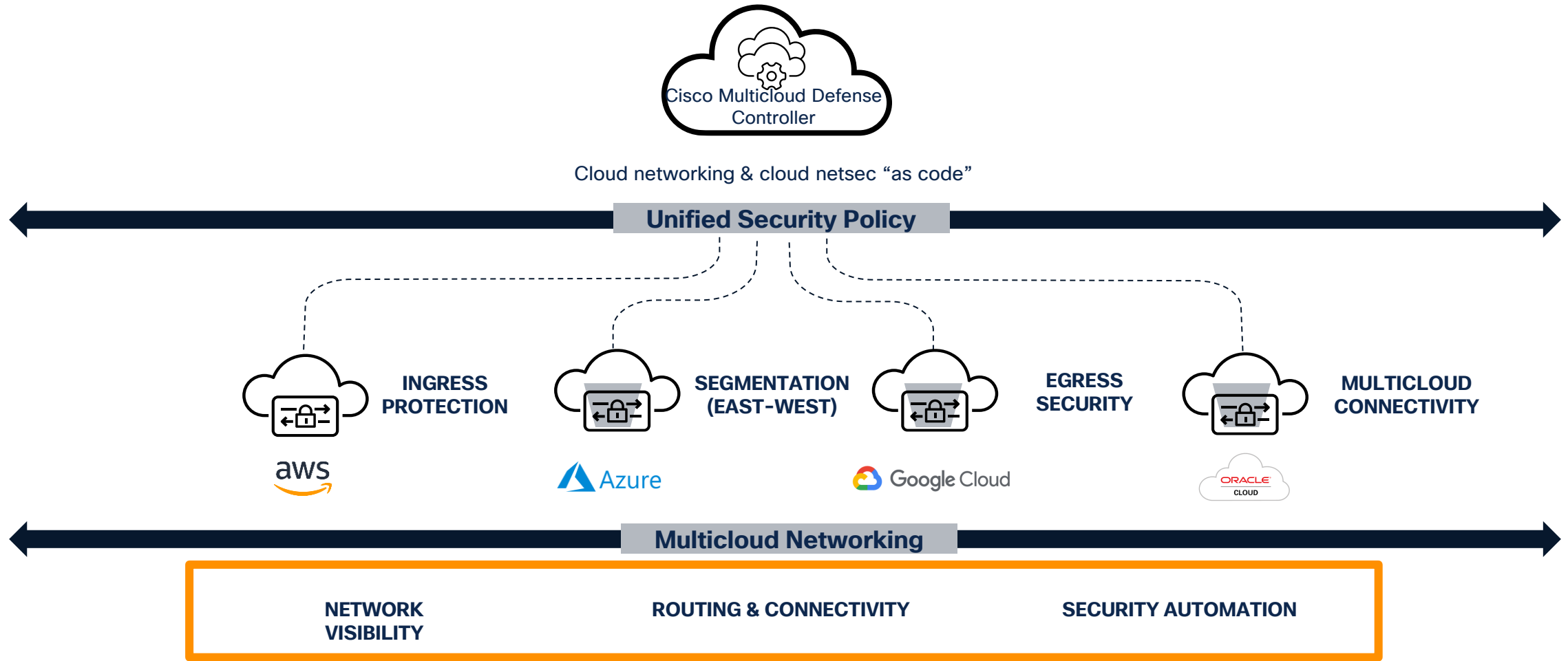
Cisco Multicloud Defense

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



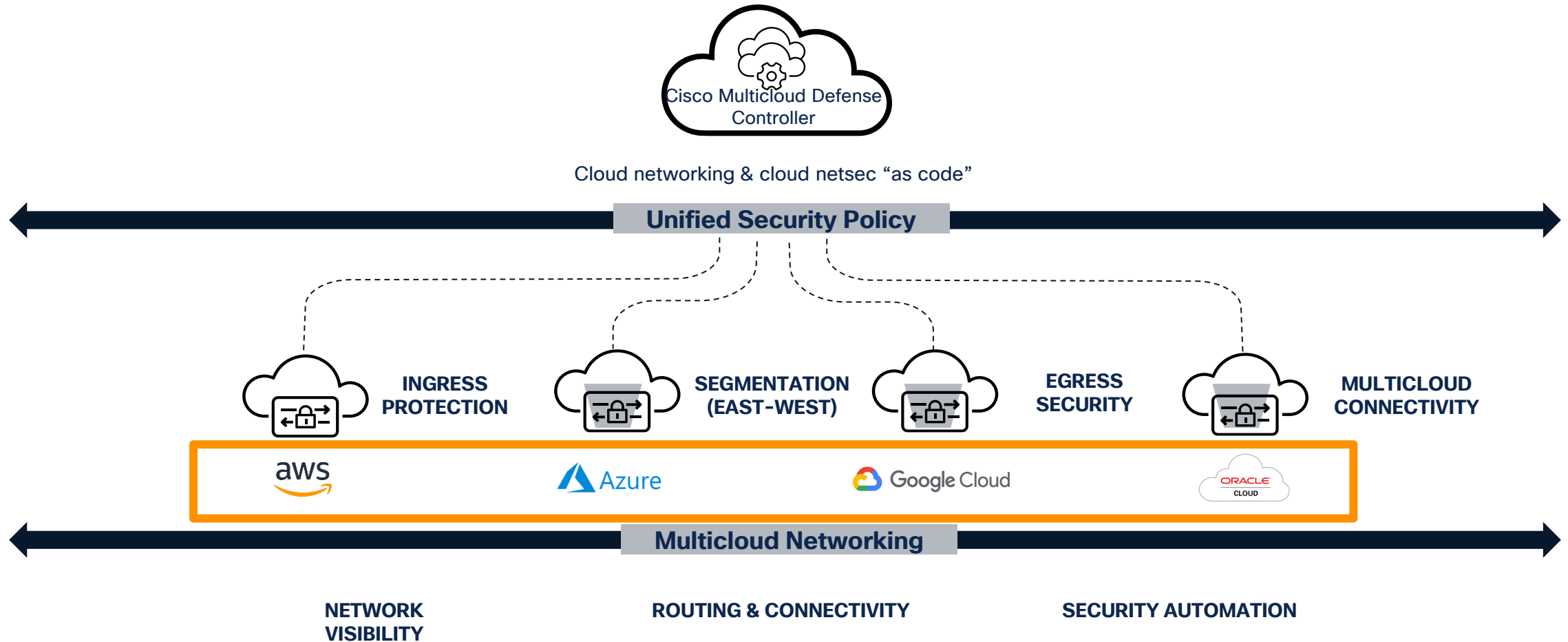
Cisco Multicloud Defense

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



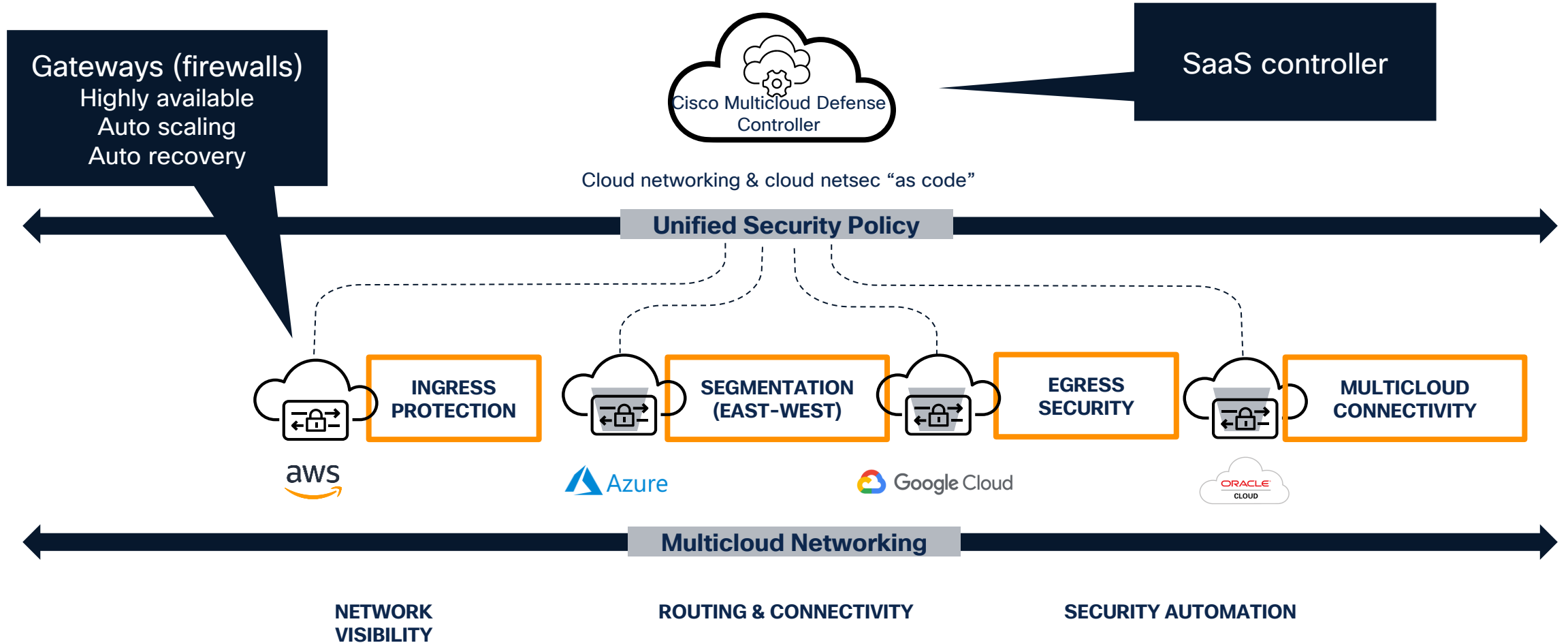
Cisco Multicloud Defense

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



Cisco Multicloud Defense

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



Fully Orchestrated



```

cisco > cisco_mcd_gateway.tf > resource "cisco_mcd_gateway" "ingress_gateway"
1 # Cisco MCD Terraform Documentation
2 # https://registry.terraform.io/providers/cisco/cisco/latest/docs
3 # AWS Terraform Documentation
4 # https://registry.terraform.io/providers/hashicorp/aws/latest/docs
5
6 # Create a new Cisco MCD Ingress Gateway Stack
7 # If the desire is to destroy the Gateway Stack, comment out the resource block
8 # If the desire is to create the Gateway Stack, uncomment out the resource block
9 resource "cisco_mcd_gateway" "ingress_gateway" {
10   name = var.cisco_mcd_ingress_gateway_name
11   csp_account_name = var.cisco_mcd_aws_account_name
12   gateway_image = var.cisco_mcd_ingress_gateway_version
13   instance_type = var.cisco_mcd_ingress_gateway_instance_type
14   mode = "HUB"
15   security_type = var.cisco_mcd_ingress_gateway_security_type
16   policy_rule_set_id = cisco_mcd_policy_rule_set.ingress_policy.rule_set_id
17   #policy_rule_set_id = data.cisco_mcd_policy_rule_set.ingress_policy.rule_set_id
18   ssh_key_pair = var.cisco_mcd_ingress_gateway_ssh_key_pair
19   aws_iam_role_firewall = var.cisco_mcd_firewall_role_name
20   region = var.aws_account_region
21   vpc_id = cisco_mcd_service_vpc.service_vpc.id
22   min_instances = var.cisco_mcd_ingress_gateway_autoscale_min
23   max_instances = var.cisco_mcd_ingress_gateway_autoscale_max
24   gateway_state = var.cisco_mcd_ingress_gateway_status
25   # settings {
26   #   name = "controller.use_internal_lb"
27   #   value = var.cisco_mcd_ingress_gateway_internal_lb
28   # }
29
30
```

```

POST /api/v1/gateway/run...
Body
1 {
2   "common": {
3     "acctName": "{{acctName}}",
4     "source": "RESTAPI",
5     "clientVersion": "CiscoMCD-2022"
6   },
7   "gateway": {
8     "cspAcctName": "AWS-Account3",
9     "name": "aws-egress-gw",
10    "description": "AWS EDGE Gateway",
11    "mode": "EDGE",
12    "type": "CLUSTER",
13    "minInstances": 1,
14    "maxInstances": 1,
15    "healthCheckPort": 65534,
16    "policyRuleSetId": 20,
17    "flags": [
18      "GATEWAY_FLAGS_EGRESS_FIREWALL",
19      "GATEWAY_FLAGS_AWS_GATEWAY_LB"
20    ]
21  },
22  "settings": [
23    {
24      "name": "gateway.aws.ebs.encryption.key.default"
25    },
26    {
27      "name": "controller.gateway.assign_public_ip",
28      "value": "true"
29    },
30    {
31      "name": "gateway.fqdn_ip_cache.entry_ttl",

```



Centralized Security Model

Gateways are deployed in the security VPC/VCN

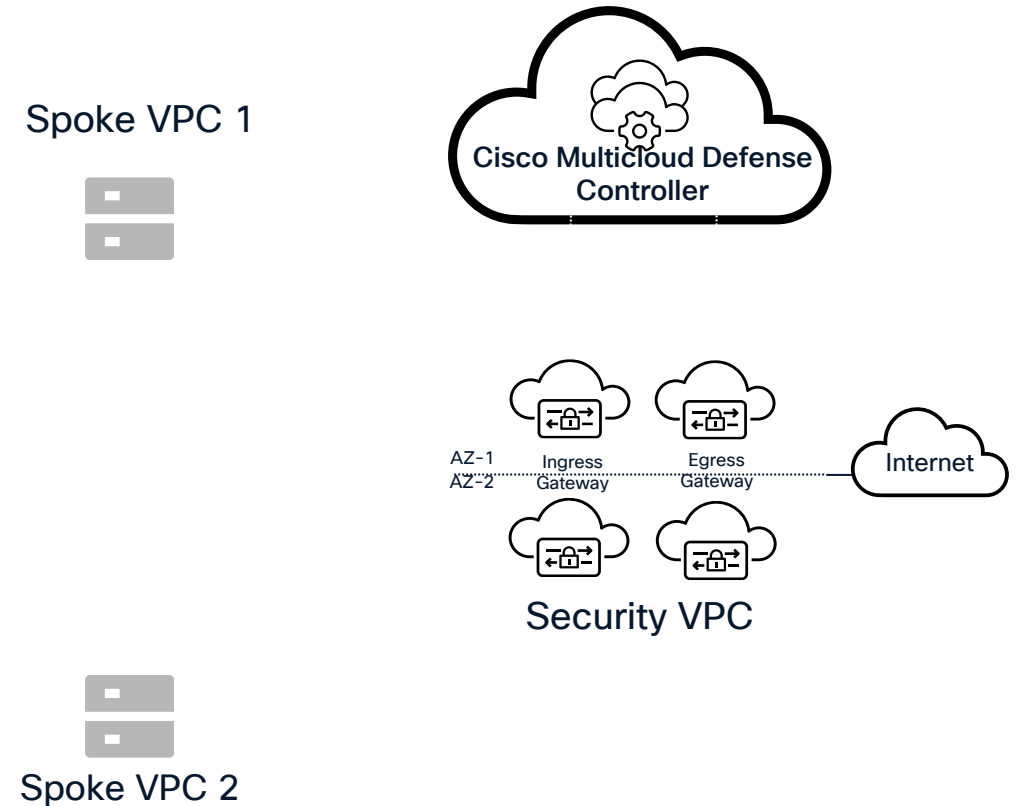
- Autoscale aware
- Multi-AZ aware

Type of Multicloud Defense Gateways

- Ingress (Inbound traffic)
- Egress (Egress & E/W traffic)

The controller handles the lifecycle management of gateways for a true cloud-native aaS experience

- Instantiation
- Scalability
- Reliability
- Upgrade



Distributed Security Model

Gateways are deployed in the security VPC/VCN

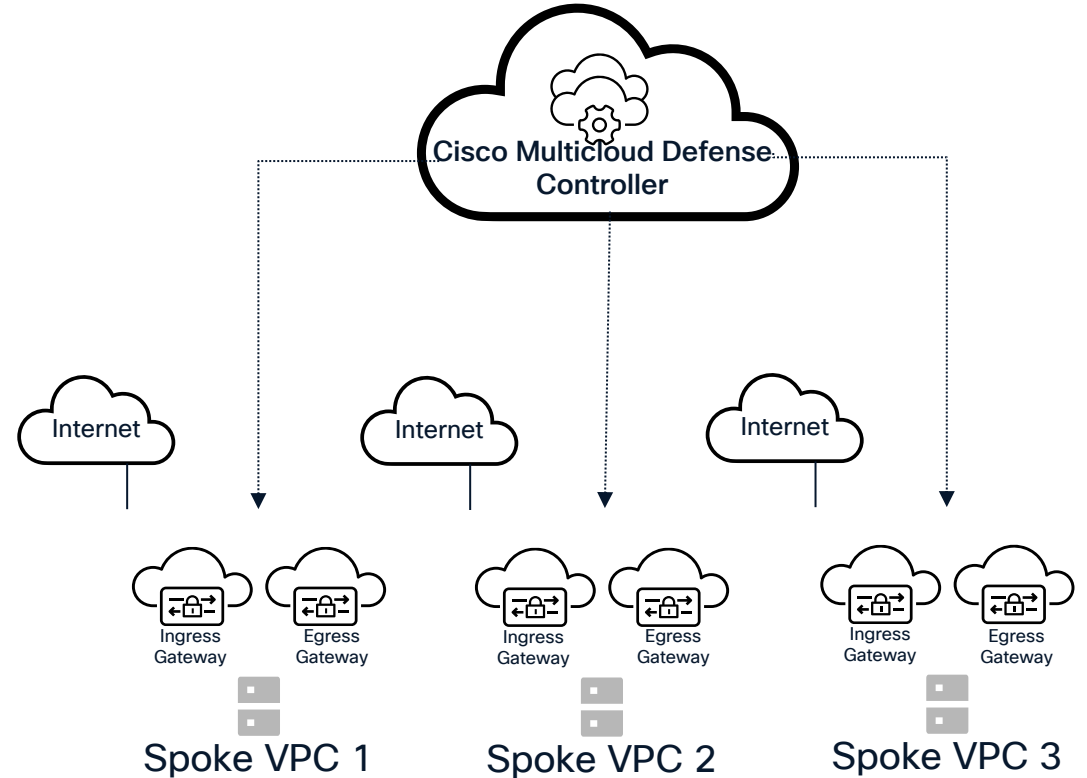
- Autoscale aware
- Multi-AZ aware

Type of Multicloud Defense Gateways

- Ingress (Inbound traffic)
- Egress (Egress & E/W traffic)

The controller handles the lifecycle management of gateways for a true cloud-native aaS experience

- Instantiation
- Scalability
- Reliability
- Upgrade



Security starts with visibility

← → ↺

prod1.mcd.eu.cdo.cisco.com/easysetup

🔍 ⭐ 📷 🔥 🔒 ⚙️ 🖨️ 👤 ⋮

Multicloud Defense

?

🔔

Admin: dstoeckm@cis...
CDO_cisco-dstoeckm

Dashboard

Discover

Investigate

Manage

Report

Administration

▼ 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

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



Connect a cloud account with the Multicloud Defense Controller

Connect Account

Step 2

Enable Traffic Visibility



Enable traffic visibility on specific VPCs to allow for more insight into the traffic in and out of your account

Enable Visibility

Step 3

Secure Your Account



Setup a Service VPC and Multicloud Defense Gateway to secure your Account

Secure Account

© 2025 Cisco and/or its affiliates. All rights reserved.

BRKSEC-1037



Secure Firewall Threat Defense Virtual

Private Cloud



Public Cloud



Gov/IC Cloud



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

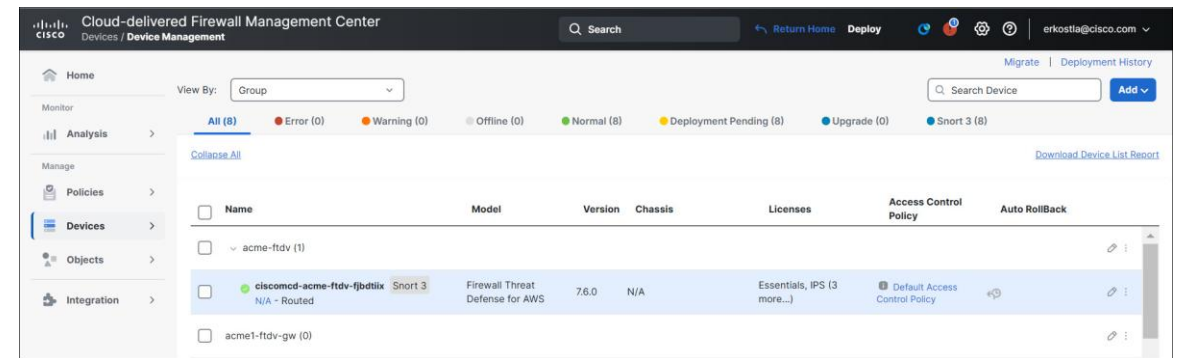
Quickstarts, Infrastructure as Code and Automation

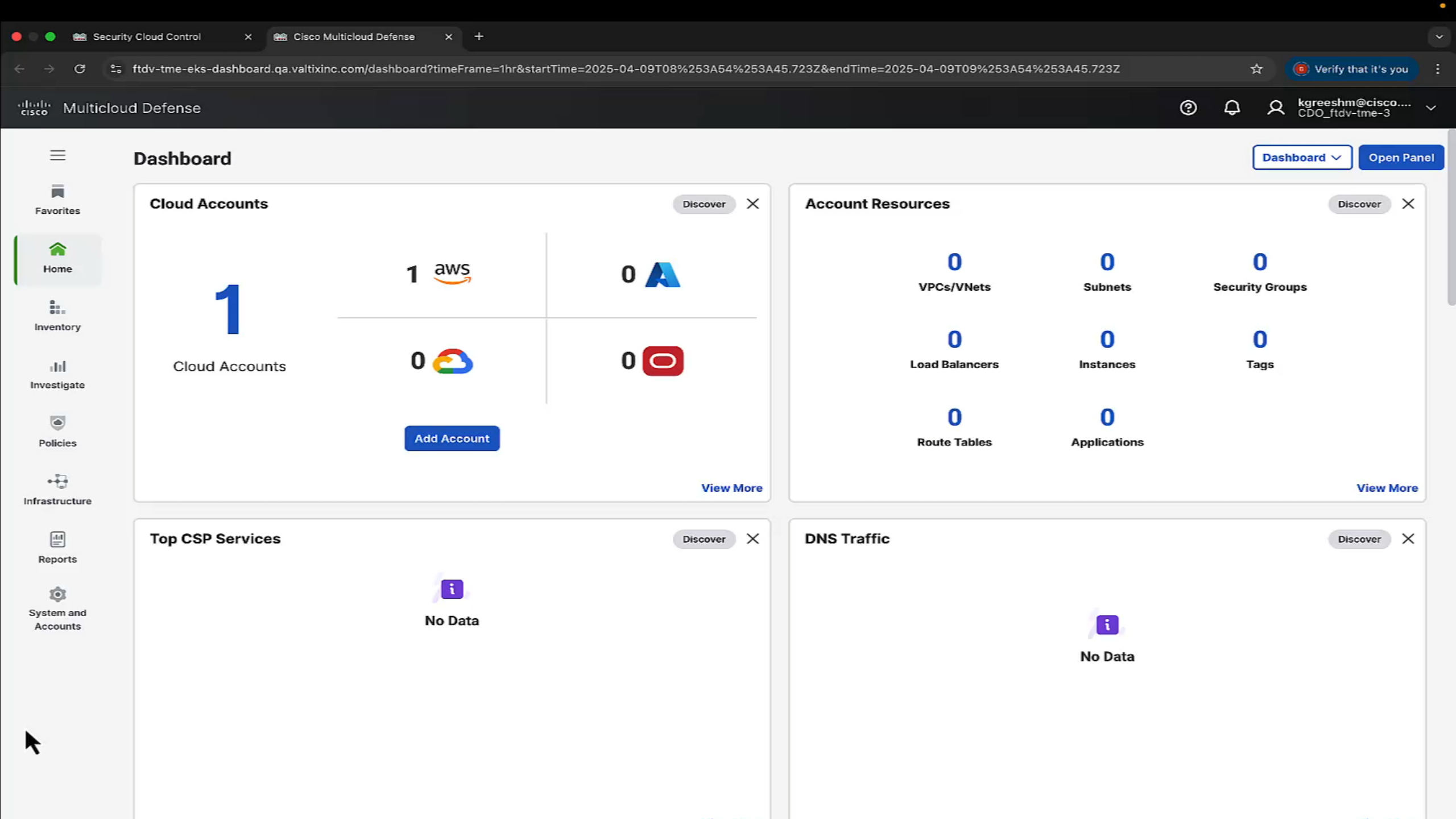
Gateway Load balancer integration

Snapshots

Secure 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
- For policy consistency, any existing ACP can be utilized





Dashboard

Discover X

1

Cloud Accounts

0 aws

0

0

0

Add Account

View More

Account Resources

Discover X

0

VPCs/VNets

0

Subnets

0

Security Groups

0

Load Balancers

0

Instances

0

Tags

0

Route Tables

0

Applications

View More

Top CSP Services

Discover X

No Data

DNS Traffic

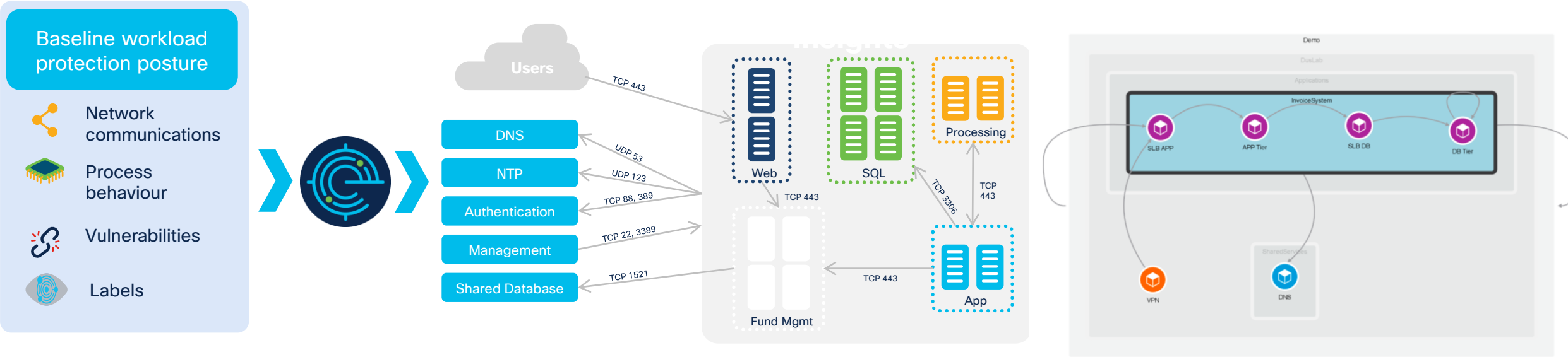
Discover X

No Data

**But do you understand my
apps?**

Establishing Trust with Cisco Secure Workload

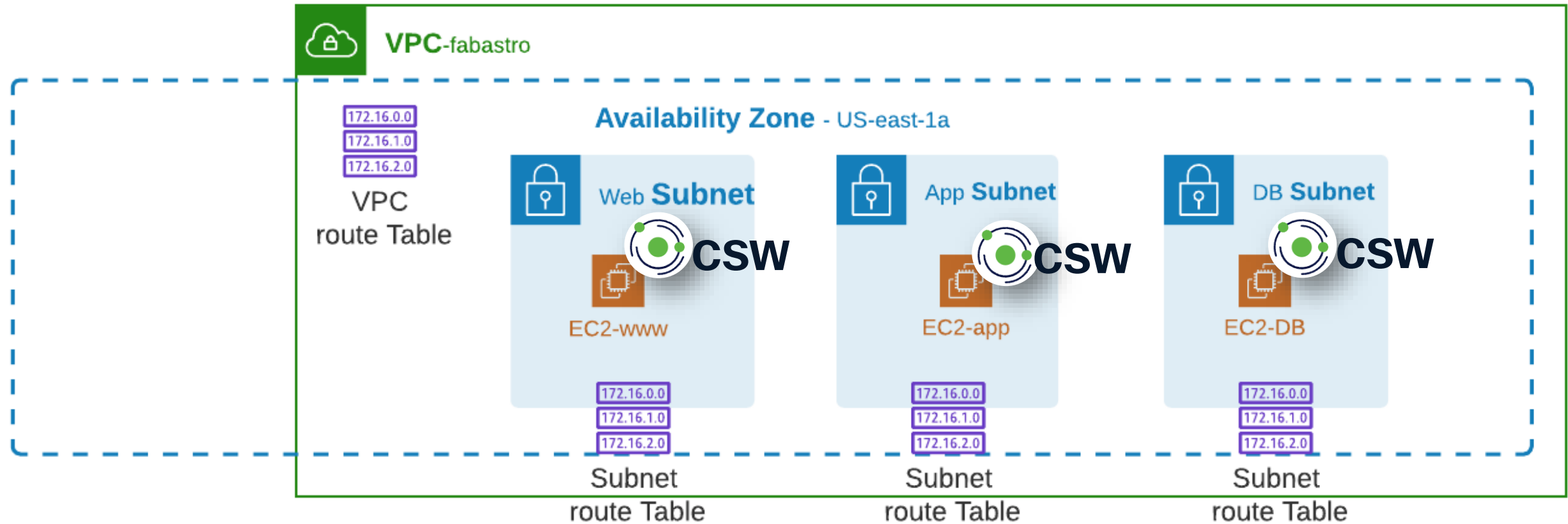
Automated discovery, clustering & policy generation and verification



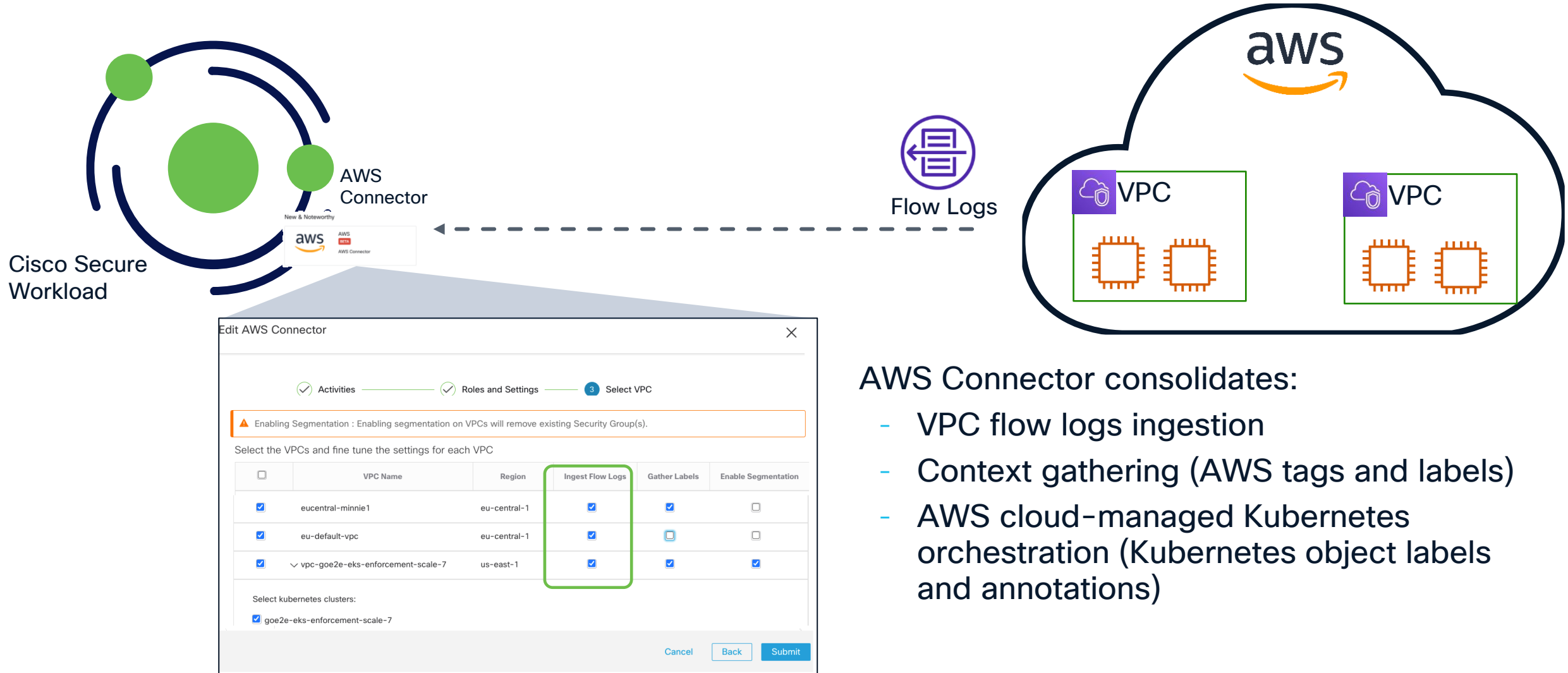
Absolute and Default Policies 13		Catch All ● DENY		Grouped 1		Ungrouped	
	Rank ↑↓	Priority ↑↓	Action ↑↓	Consumer ↓	Provider ↑↓	Protocols And Ports ↑↓	
	Absolute	100	● ALLOW	 VPN	 SLB APP	TCP : 1936	 
	Default	100	● ALLOW	 VPN	 SLB APP	TCP : 80 (HTTP)	 
	Default	100	● ALLOW	 SLB DB	 DB Tier	TCP : 3306 (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	 

What about MicroSegmentation ?

Leveraging Cisco Secure Workload to segment within a VPC or a subnet



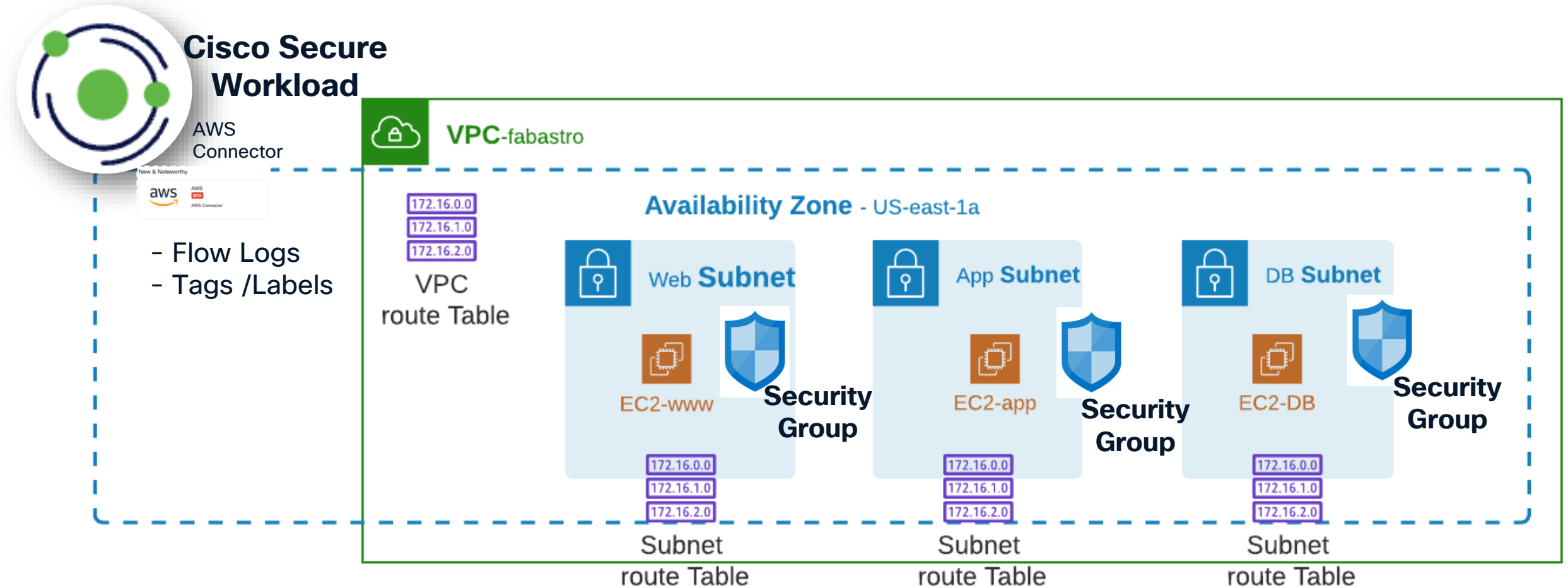
Cisco Secure Workload Cloud-Based Sources



AWS Connector consolidates:

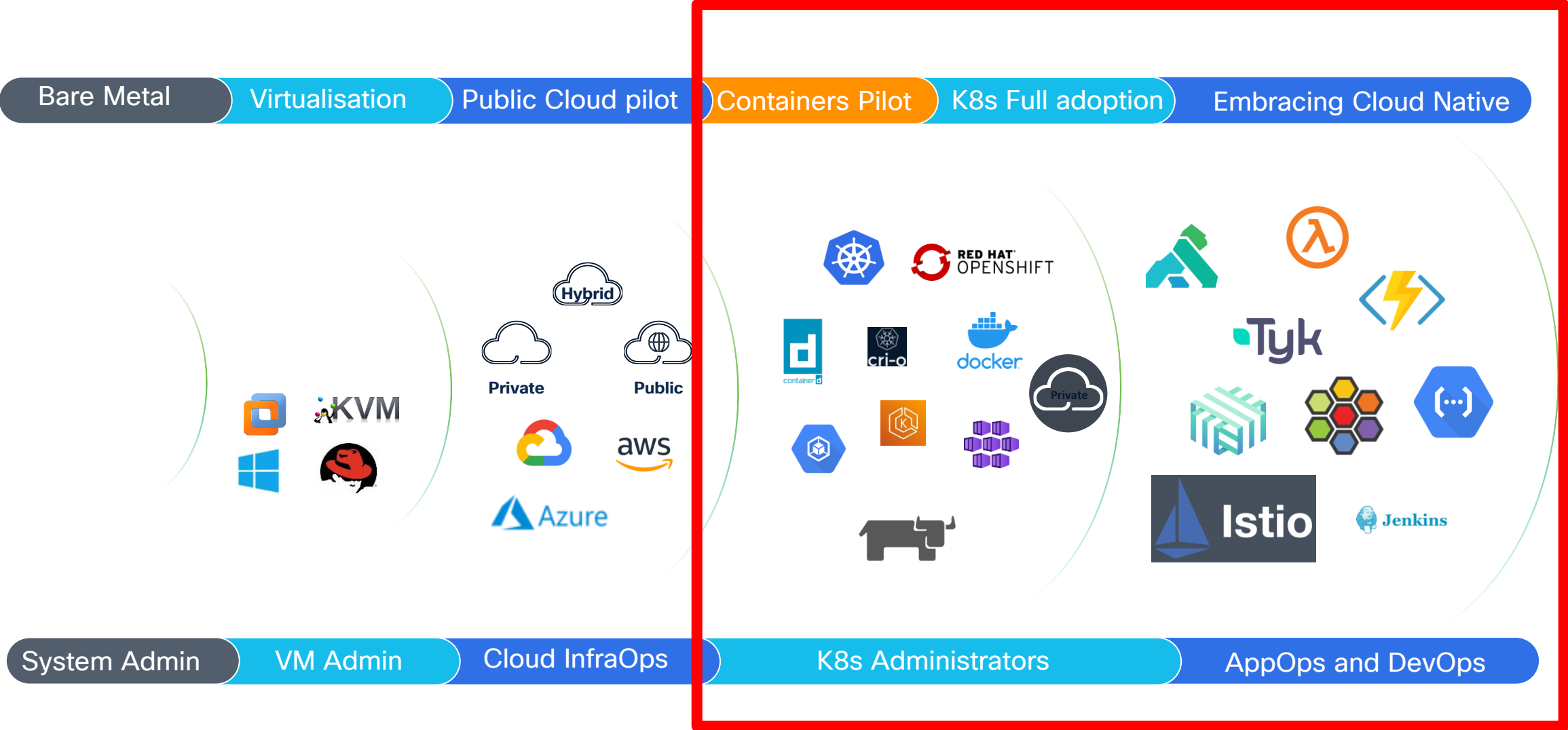
- VPC flow logs ingestion
- Context gathering (AWS tags and labels)
- AWS cloud-managed Kubernetes orchestration (Kubernetes object labels and annotations)

Leveraging Cisco Secure Workload without agent



Microsegmentation for Microservices

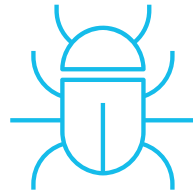
Application workloads evolution



Cloud Native Apps : More security complexity



Traditional security tools don't meet the needs for cloud native app development

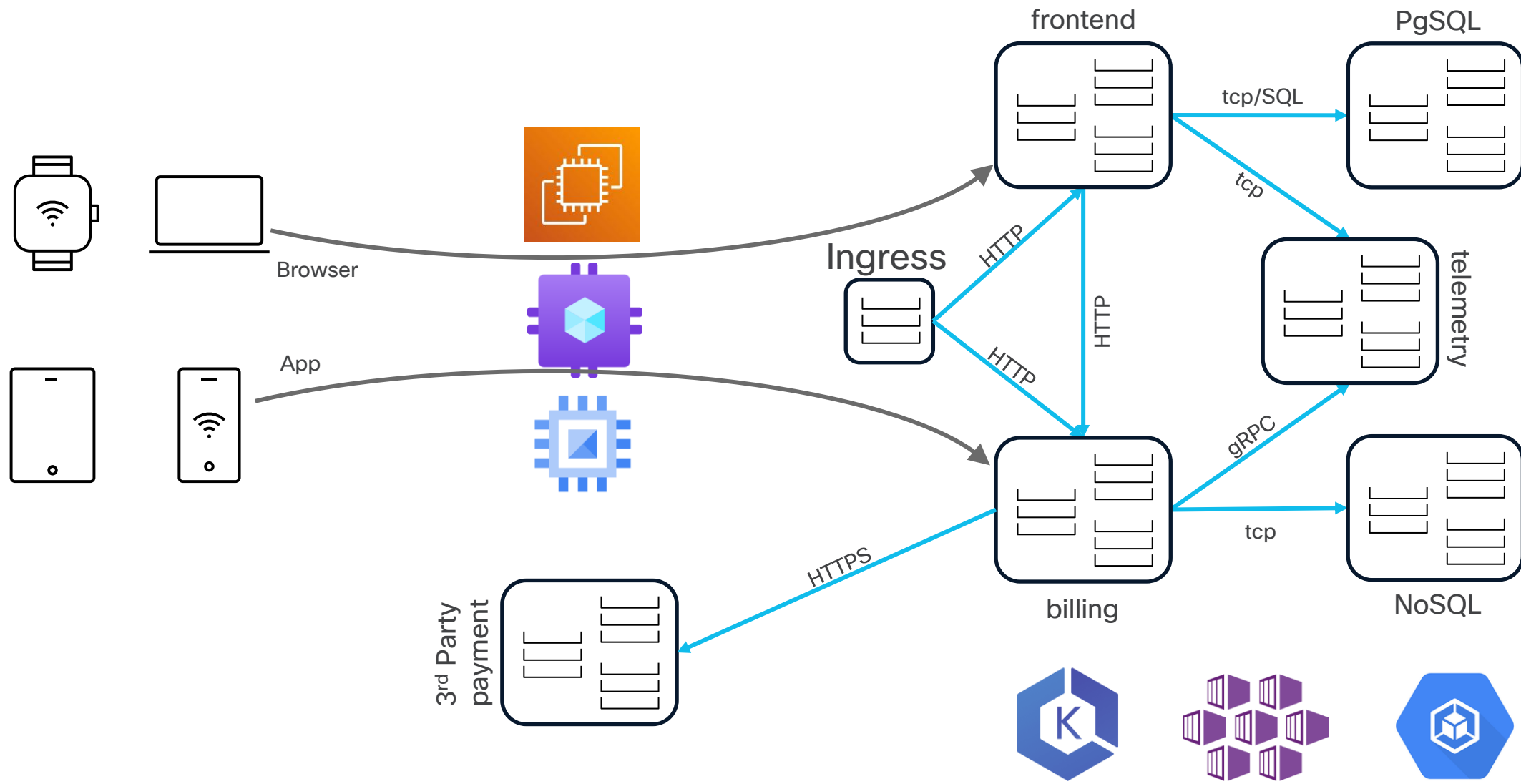


Kubernetes is not secure by default; massive proliferation of one-function tools

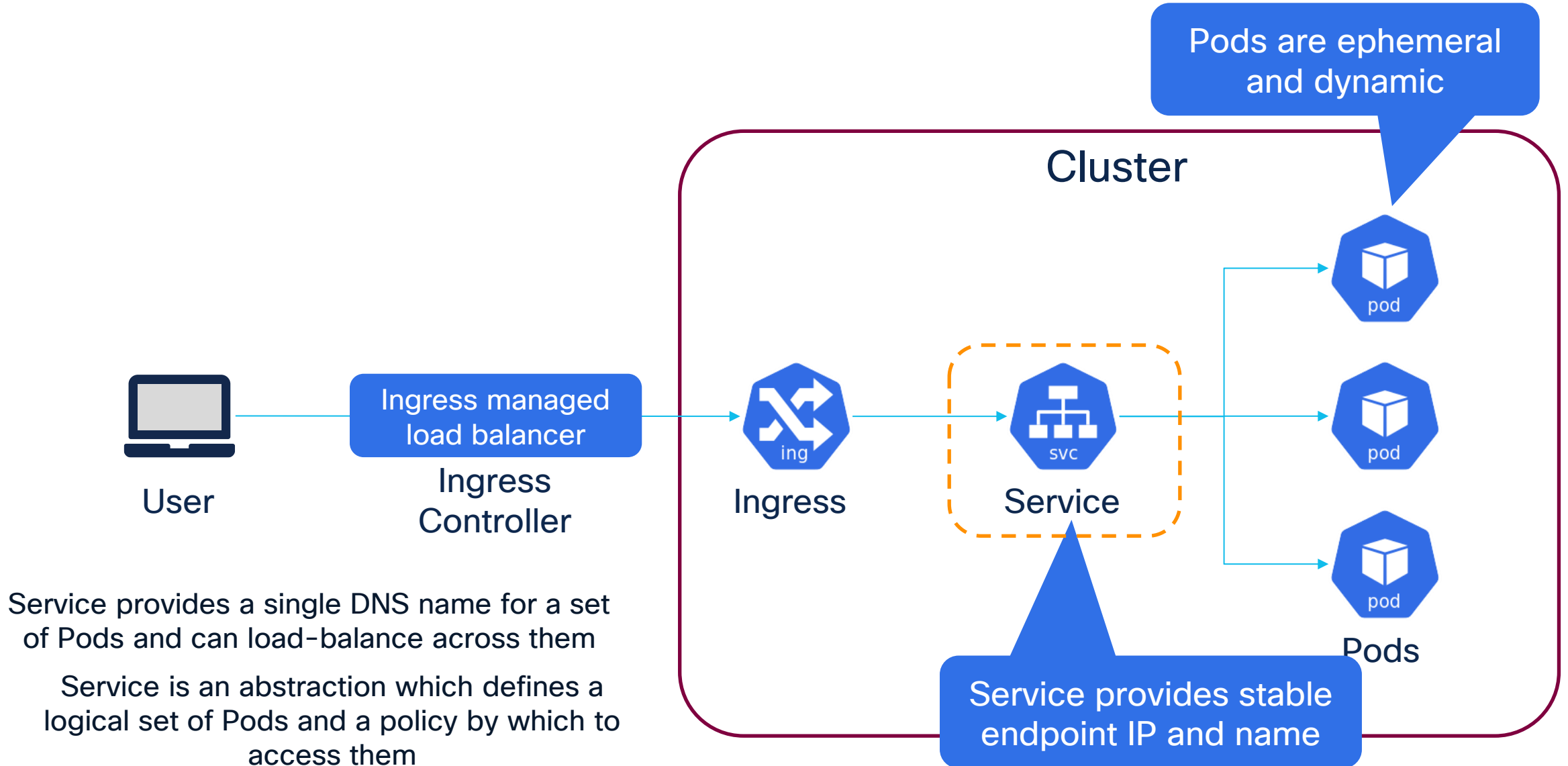


SecOps has to keep up with the speed of app development and have an integrated workflow

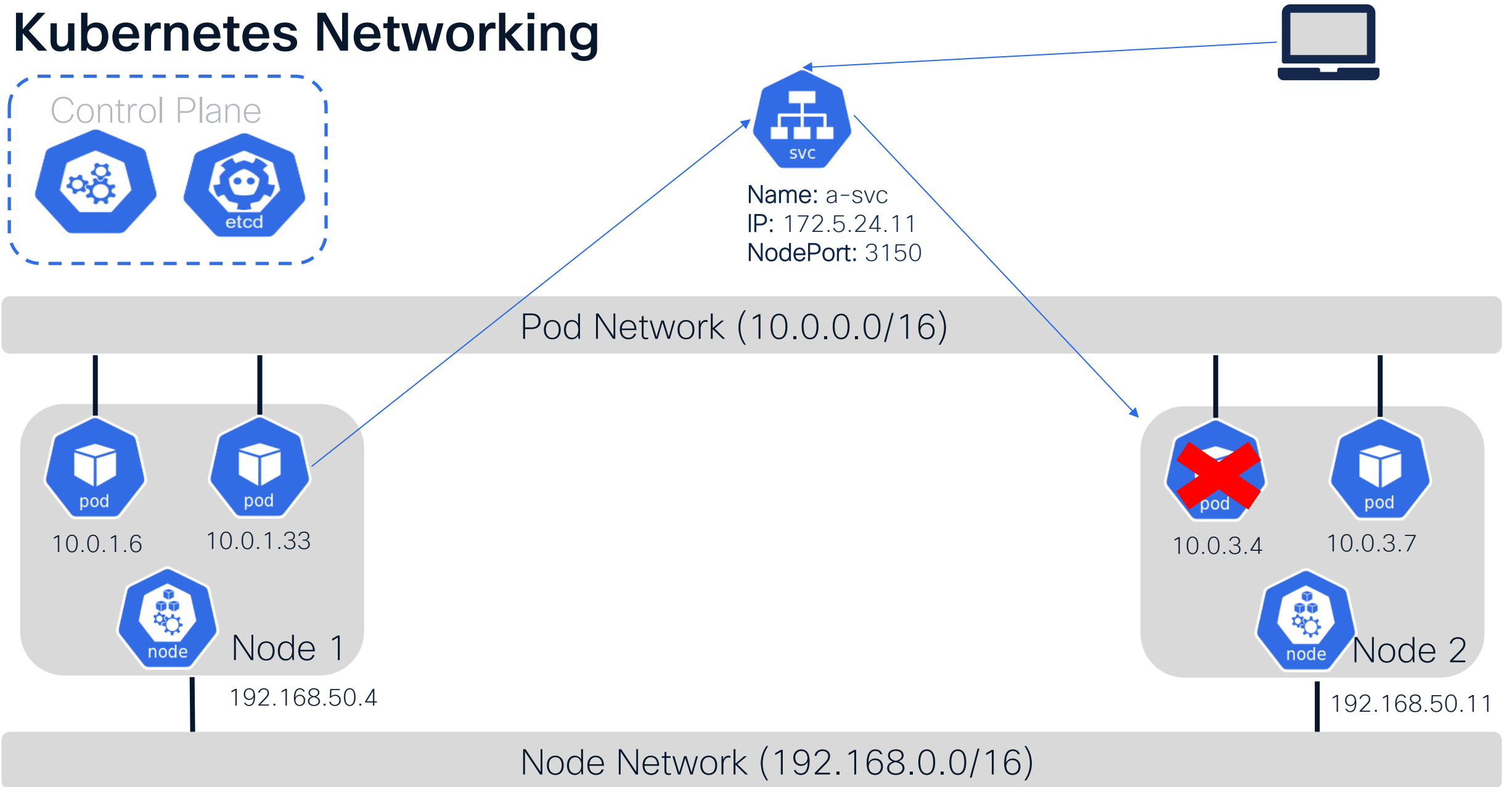
Simple Modern Application



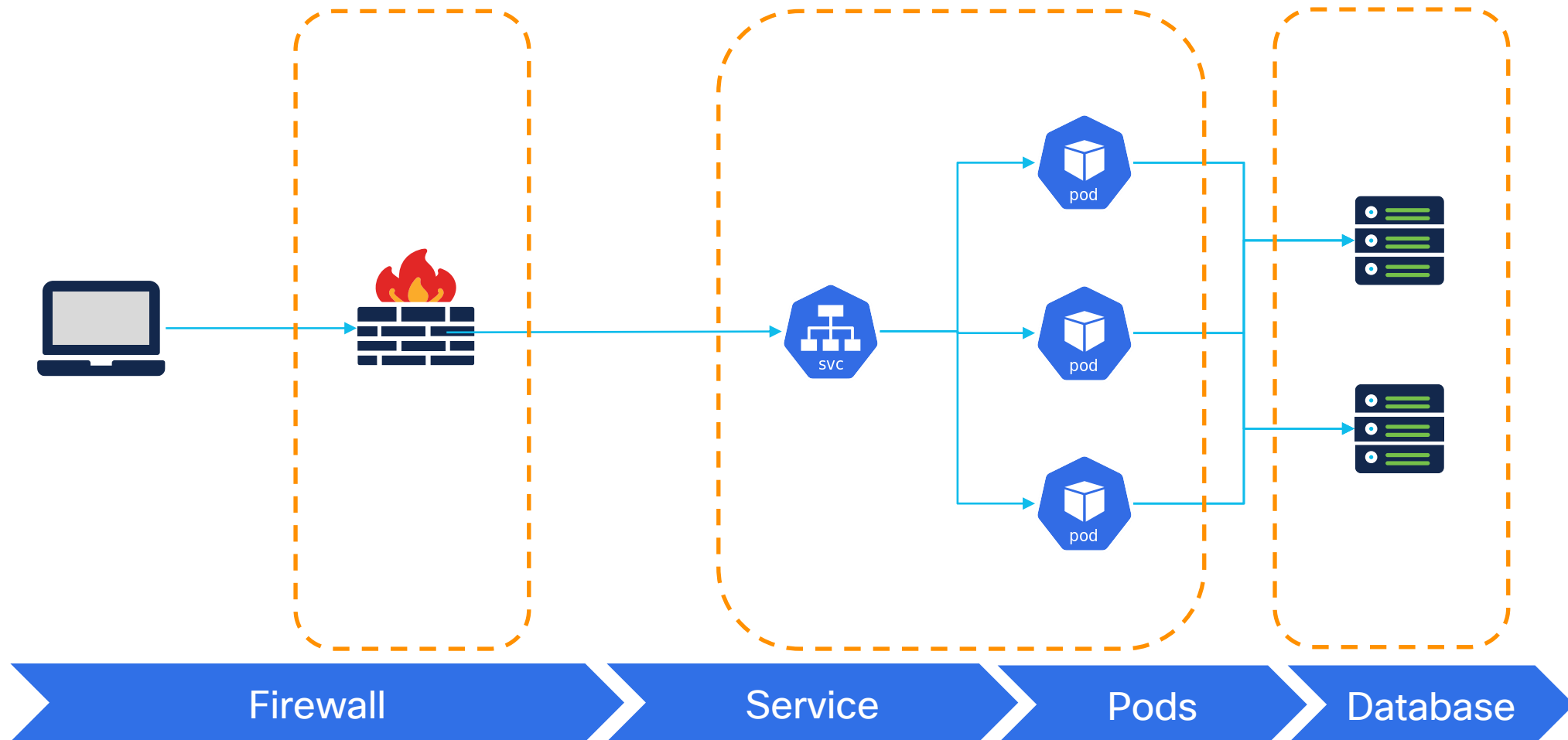
Key Components - Services



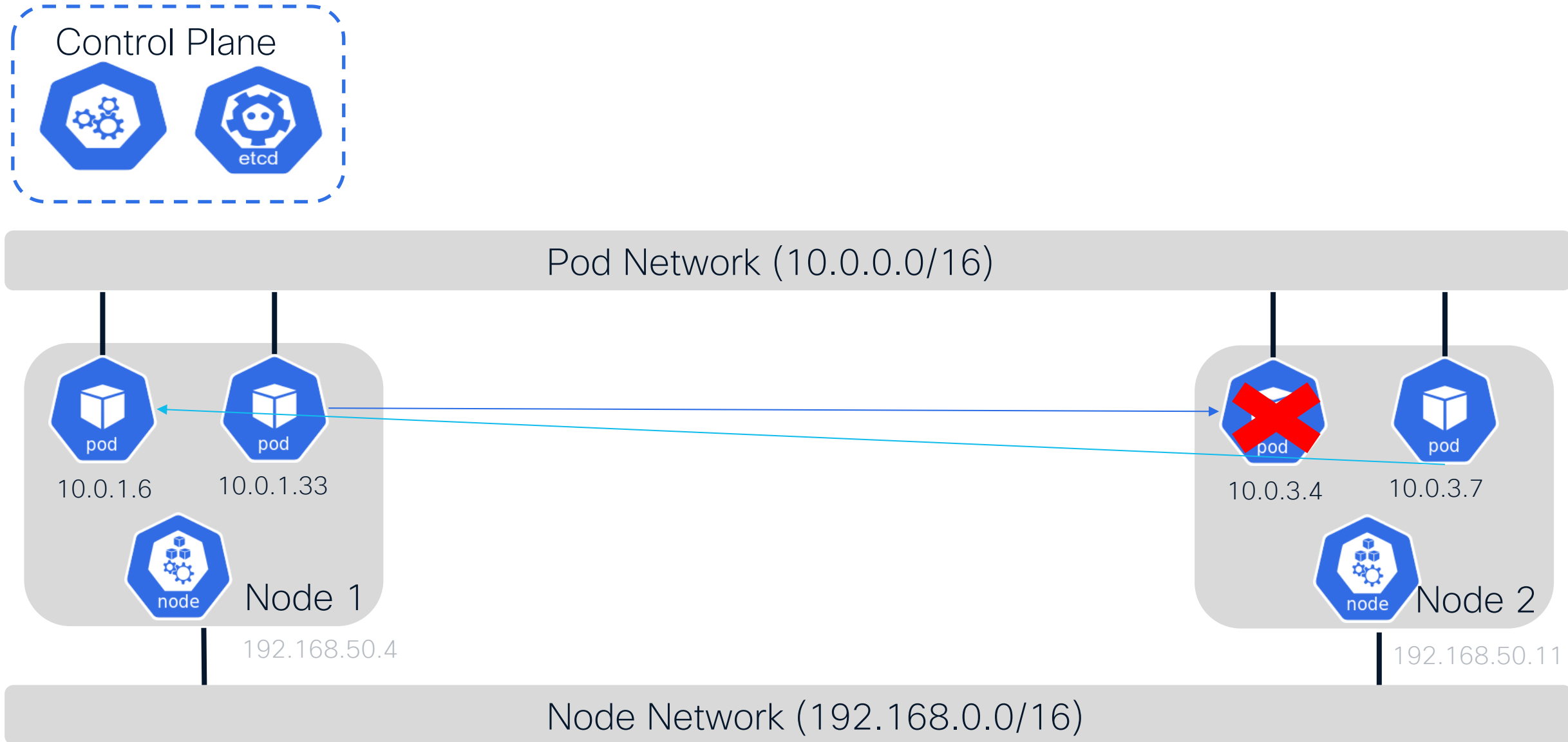
Kubernetes Networking



Complicated Policy Enforcement



Kubernetes Networking



Where is my interface and network cabling

Kubernetes CNI Explained

Concepts of Kubernetes Container Network Interface (CNI)

CNI (Container Network Interface)

A framework for configuring network interfaces in Linux containers.

Plugins

Responsible for setting up networking for pods. Examples include Calico, Flannel, and Weave

Network Namespace

Isolates network resources like IP addresses and interfaces for each pod.

IPAM (IP Address Management)

Allocates and manages IP addresses for pod interfaces.

Benefits

Provides modularity, flexibility, and ensures interoperability between different networking so

Kubernetes Service Mesh Explained

Concepts of a Kubernetes Service Mesh

Service Mesh

A dedicated infrastructure layer for managing service-to-service communication.

Data Plane

Handles the communication between services by proxying requests.

Control Plane

Manages the configuration and policy enforcement for the data plane.

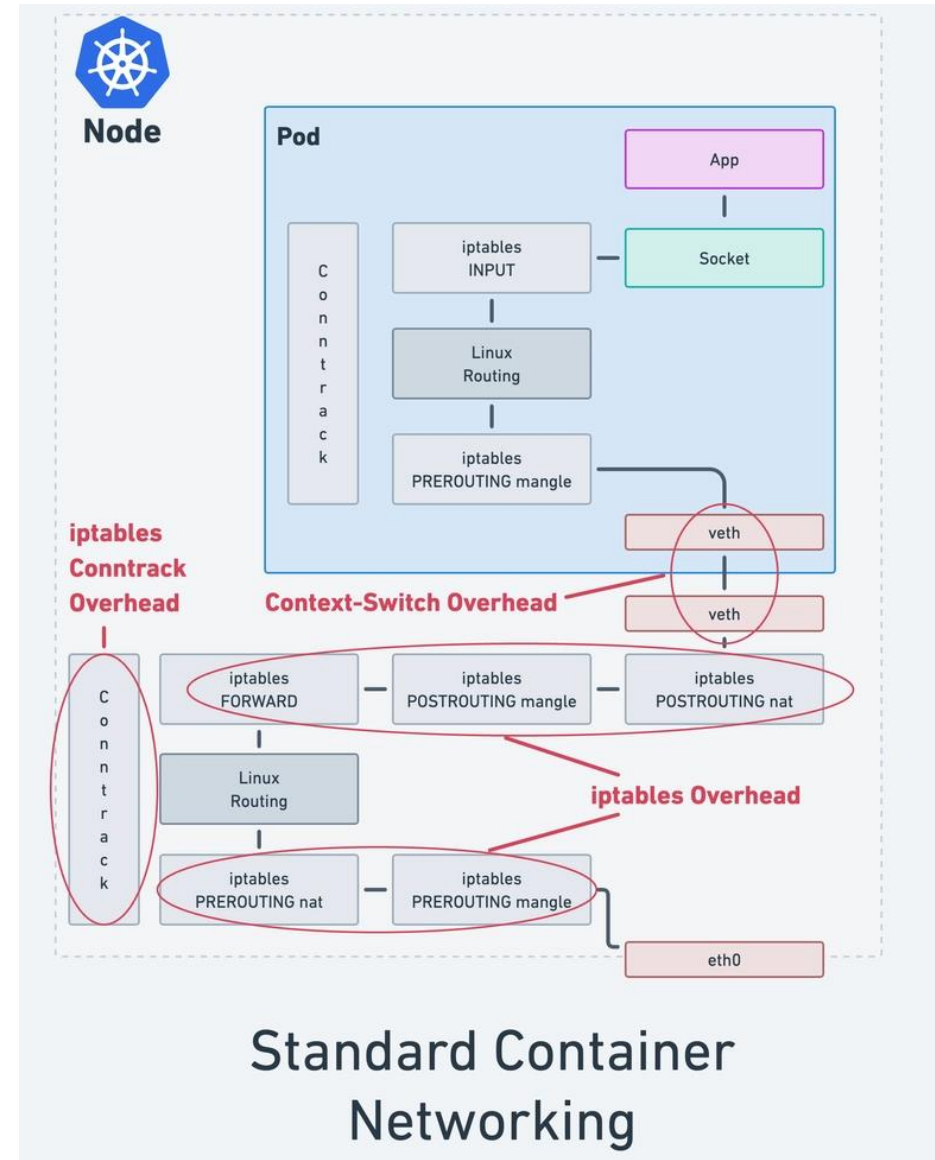
Sidecar Proxy

A proxy deployed alongside each service instance, intercepting and managing network traffic.

Benefits

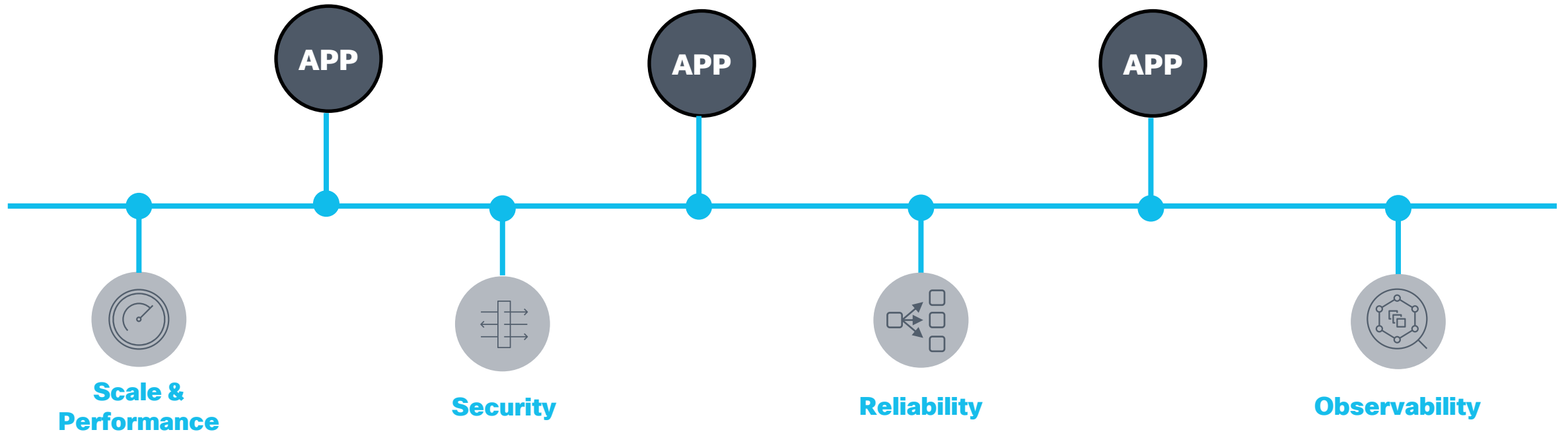
Provides observability, security, and traffic management without altering application code.

Kubernetes Networking



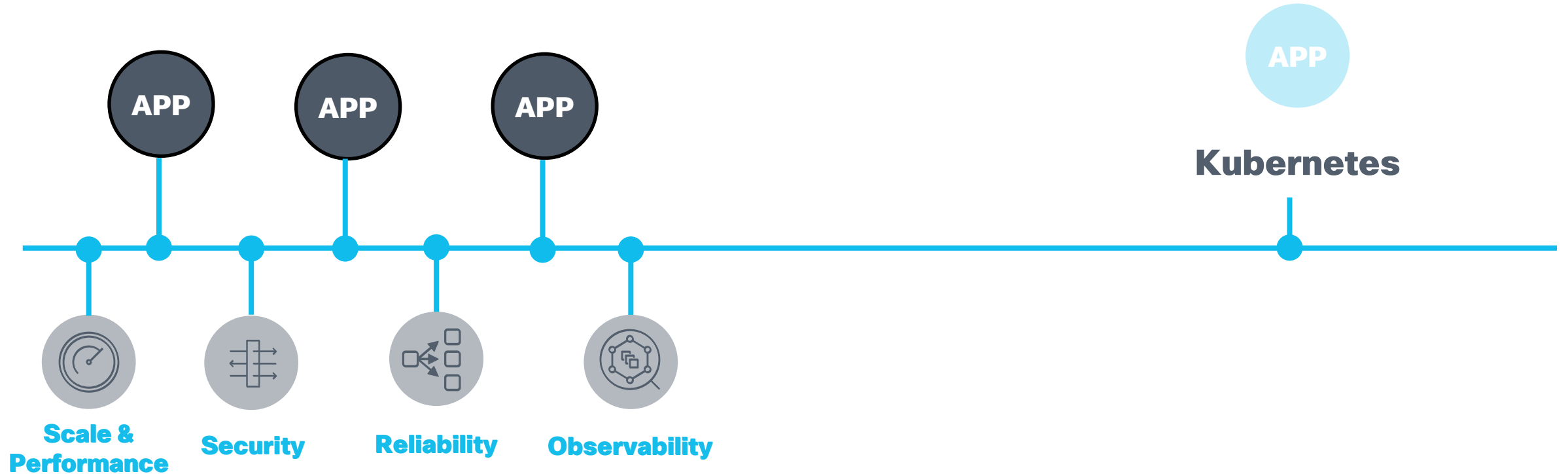
The Network has Always Been Essential to Enterprise Requirements

But Modern Cloud Native Applications Are Challenging for Enterprise Infrastructure Teams

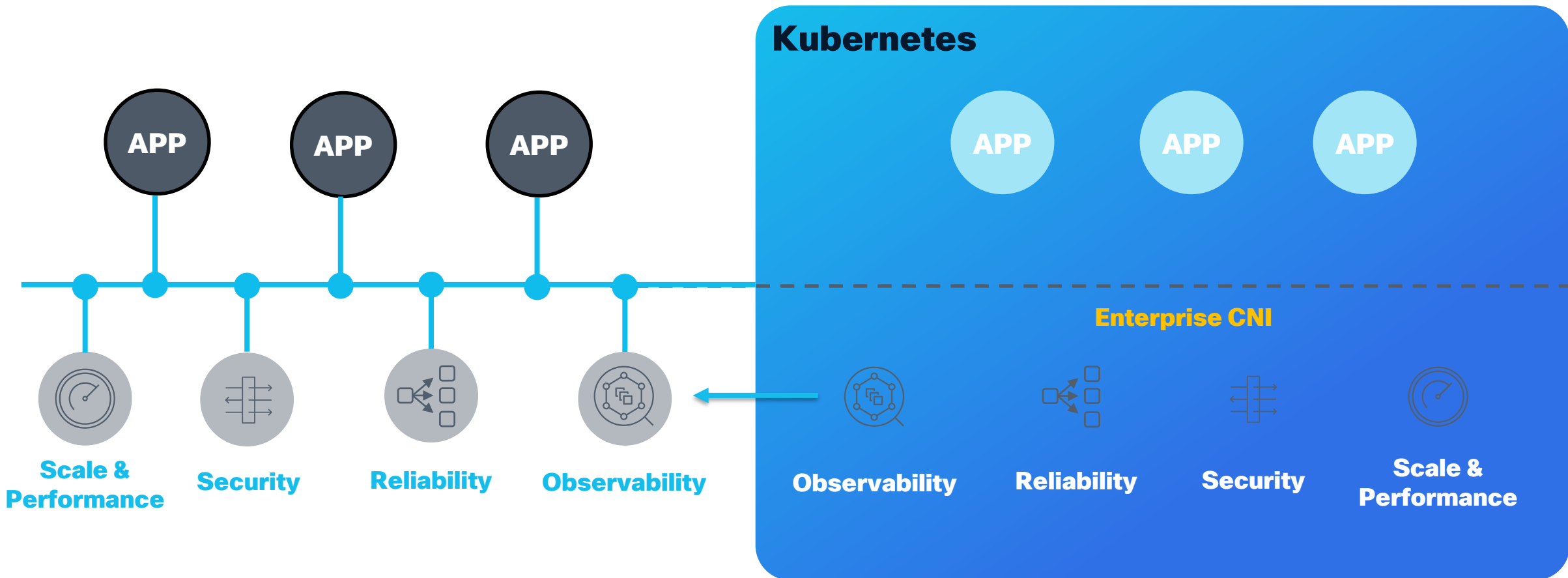


The Network has Always Been Essential to Enterprise Requirements

But Modern Cloud Native Applications Are Challenging for Enterprise Infrastructure Teams

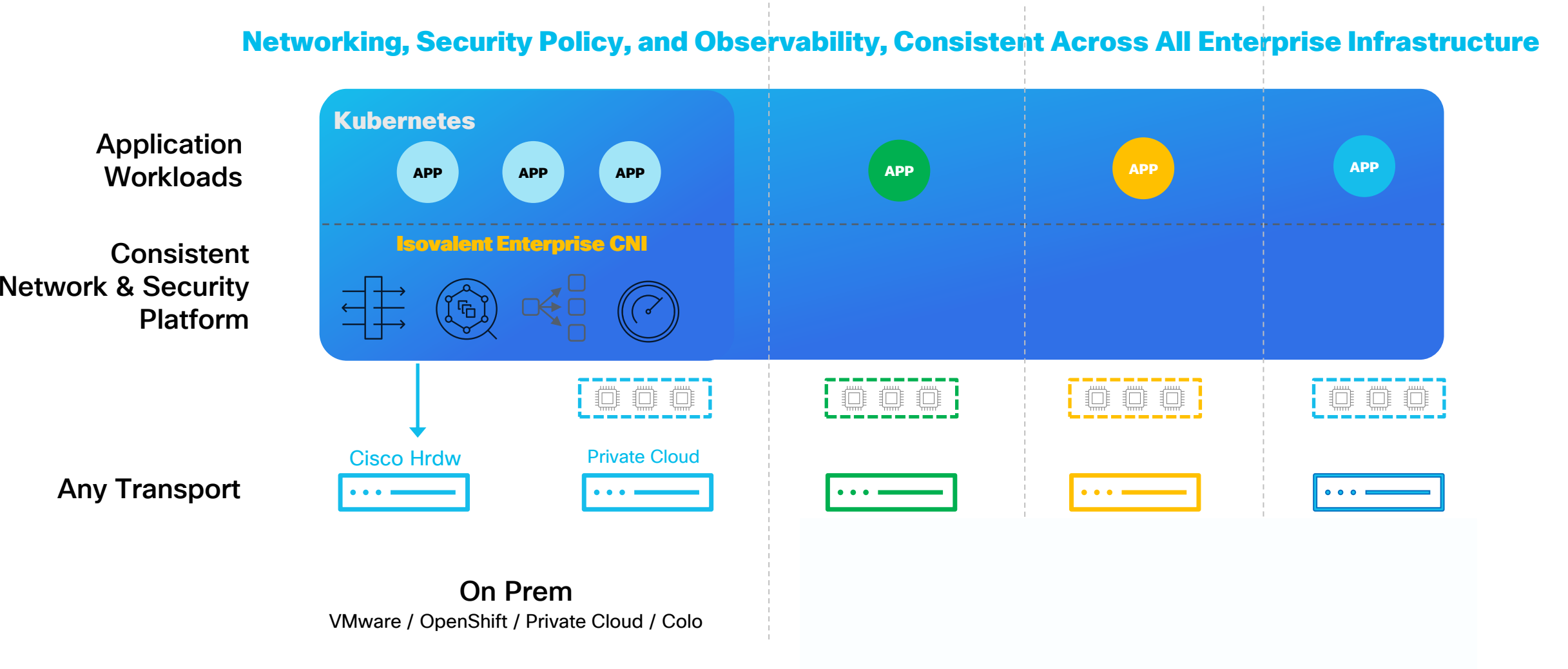


Solution to Regain the Visibility and Control Enterprises Need



This is Why Cisco Acquired Isovalent.

It's the Technology Foundation for Cisco's Hybrid & Multi-Cloud Networking & Security Strategy



Isovalent Chosen As The Standard Network Interface By All Major Cloud Providers, Making It An Industry Standard.



2020 - Google announces Isovalent & eBPF as the new networking data plane for GKE



2021 - AWS picks Isovalent for Networking & Security on EKS Anywhere



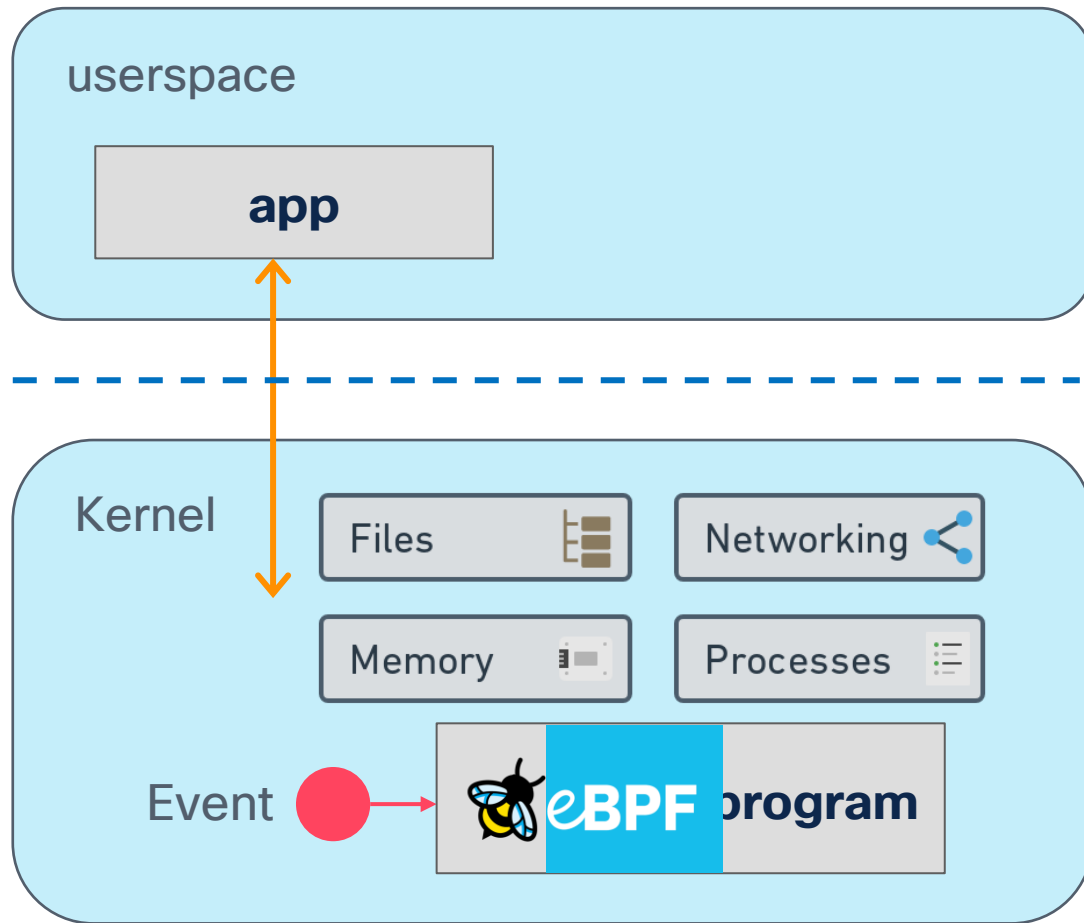
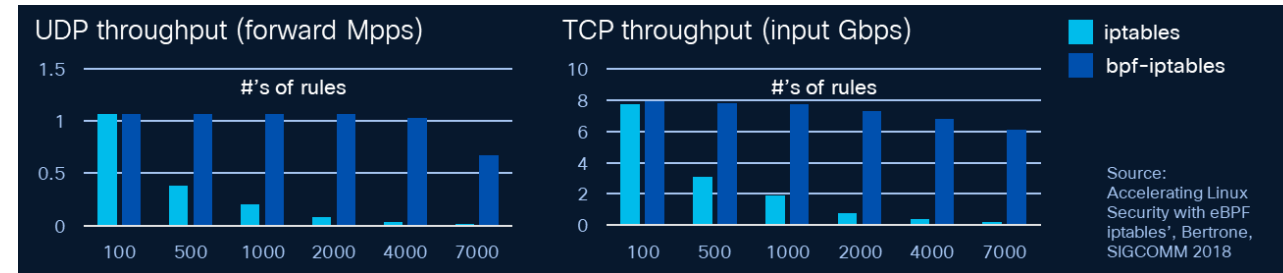
2022 - Announcing Azure CNI Powered by Isovalent



October 2023 - Cloud Native Computing Foundation (CNCF) Announces Cilium Graduation

eBPF – Extended Berkely Packet Filter

Makes the kernel programmable in a secure and efficient way

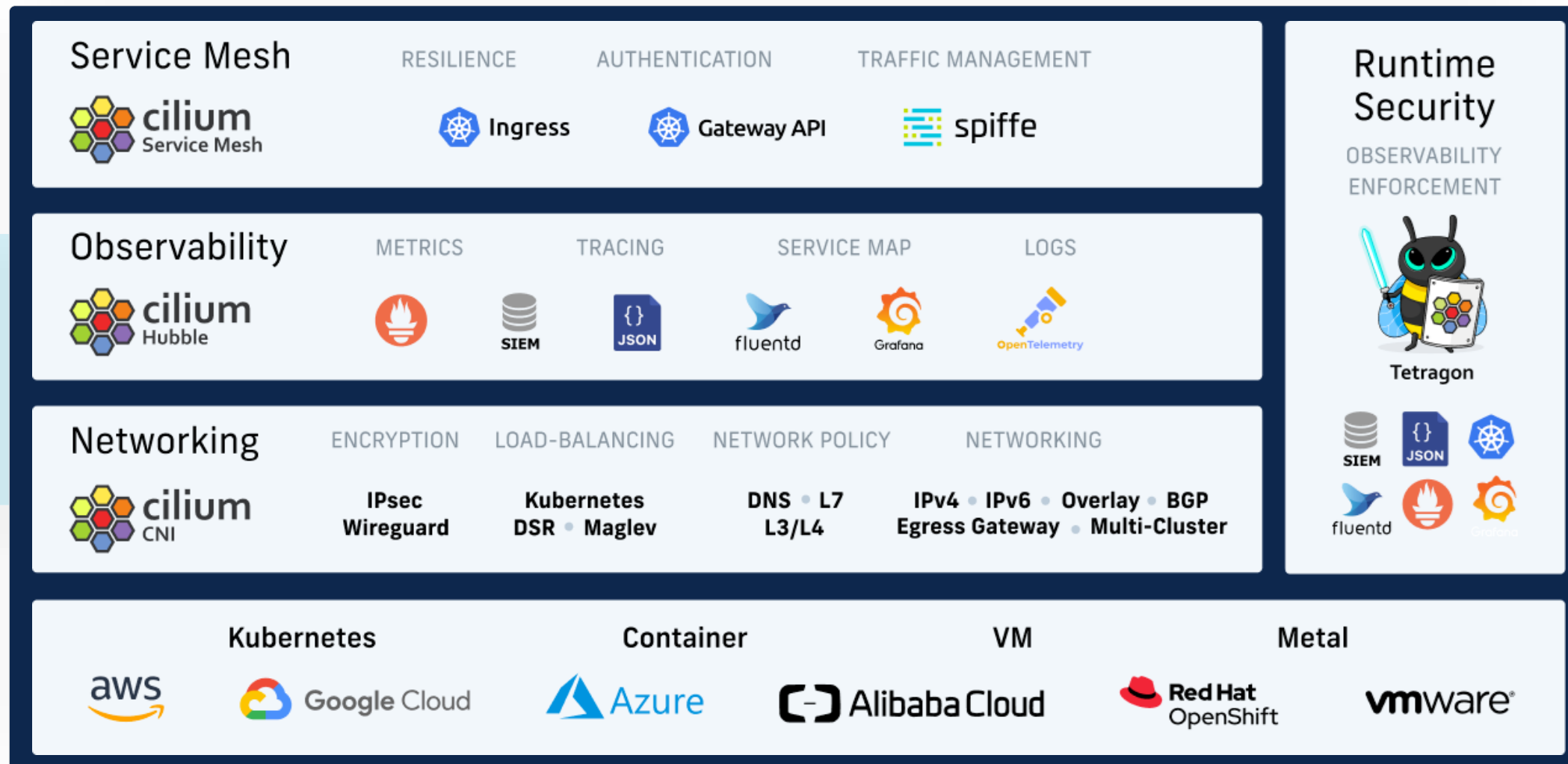


System calls

- 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

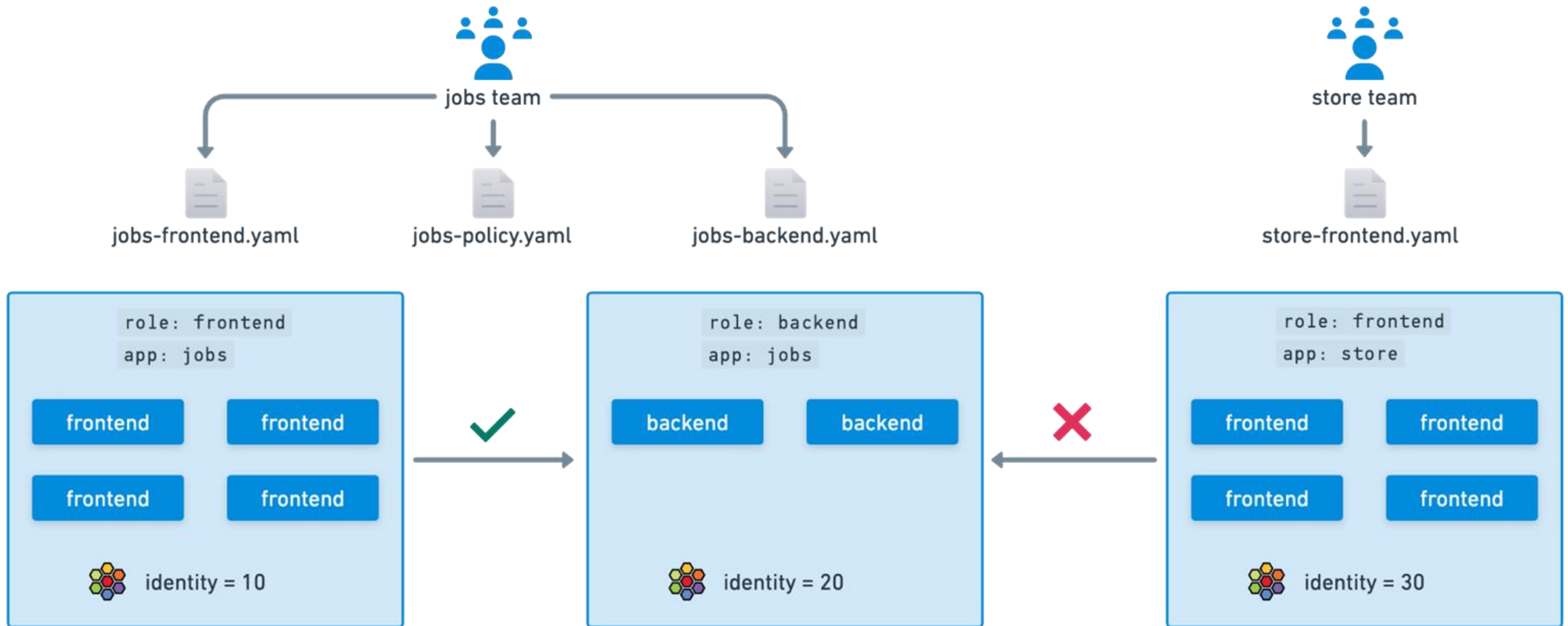
powers many things

Capabilities For Your Cloud Native Journey



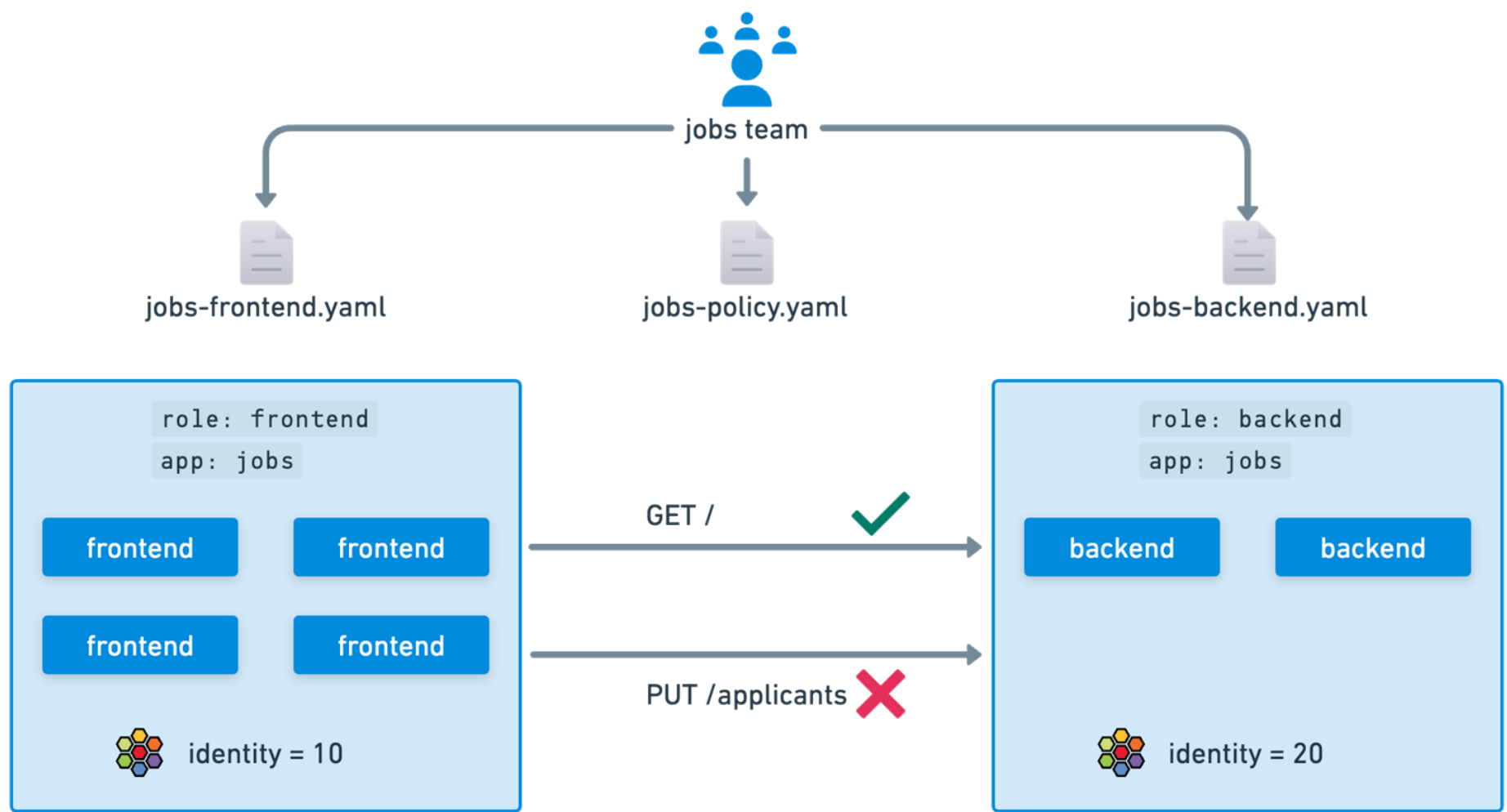
Micro-Segmentation

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

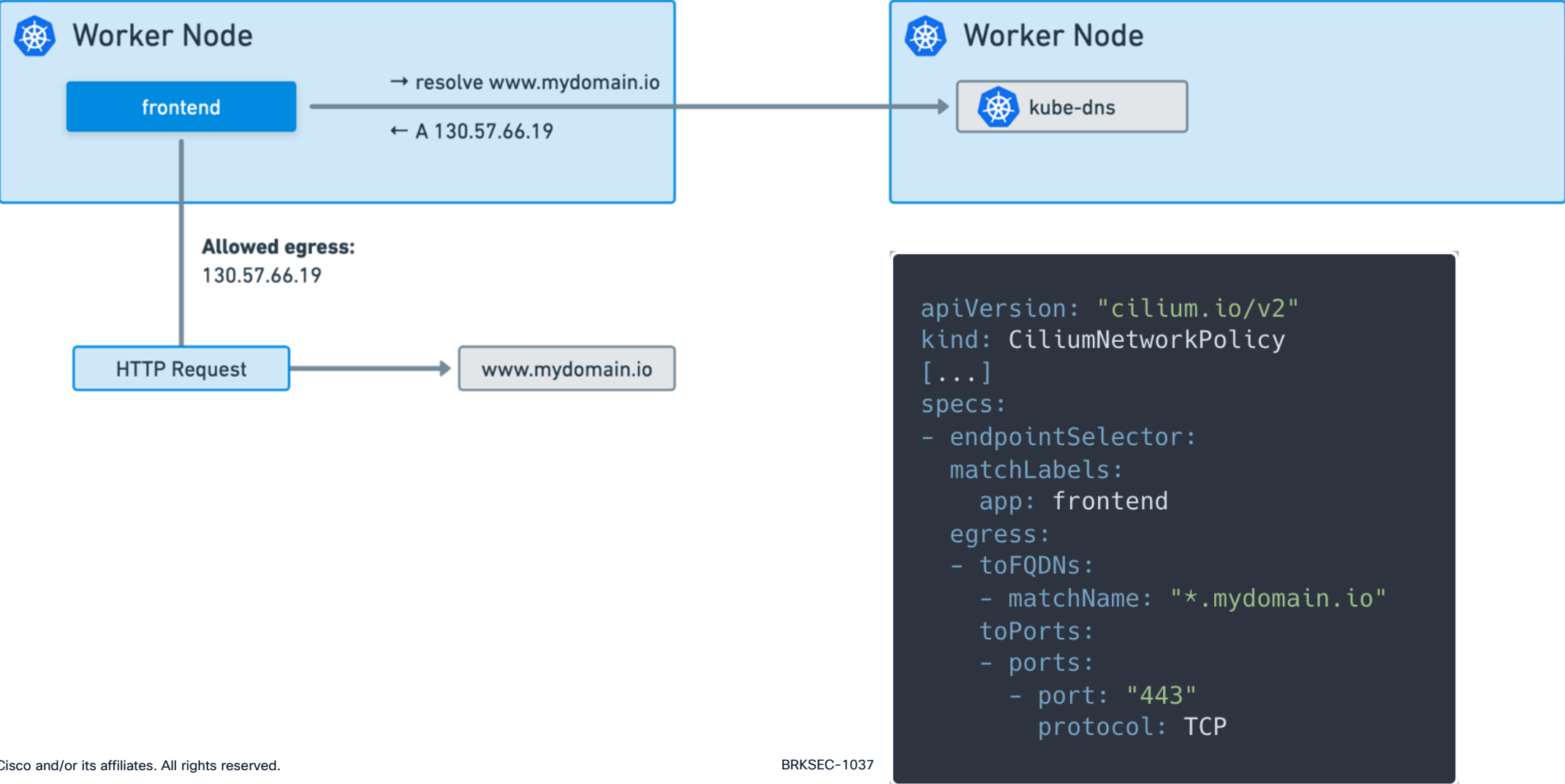


API-Aware Security

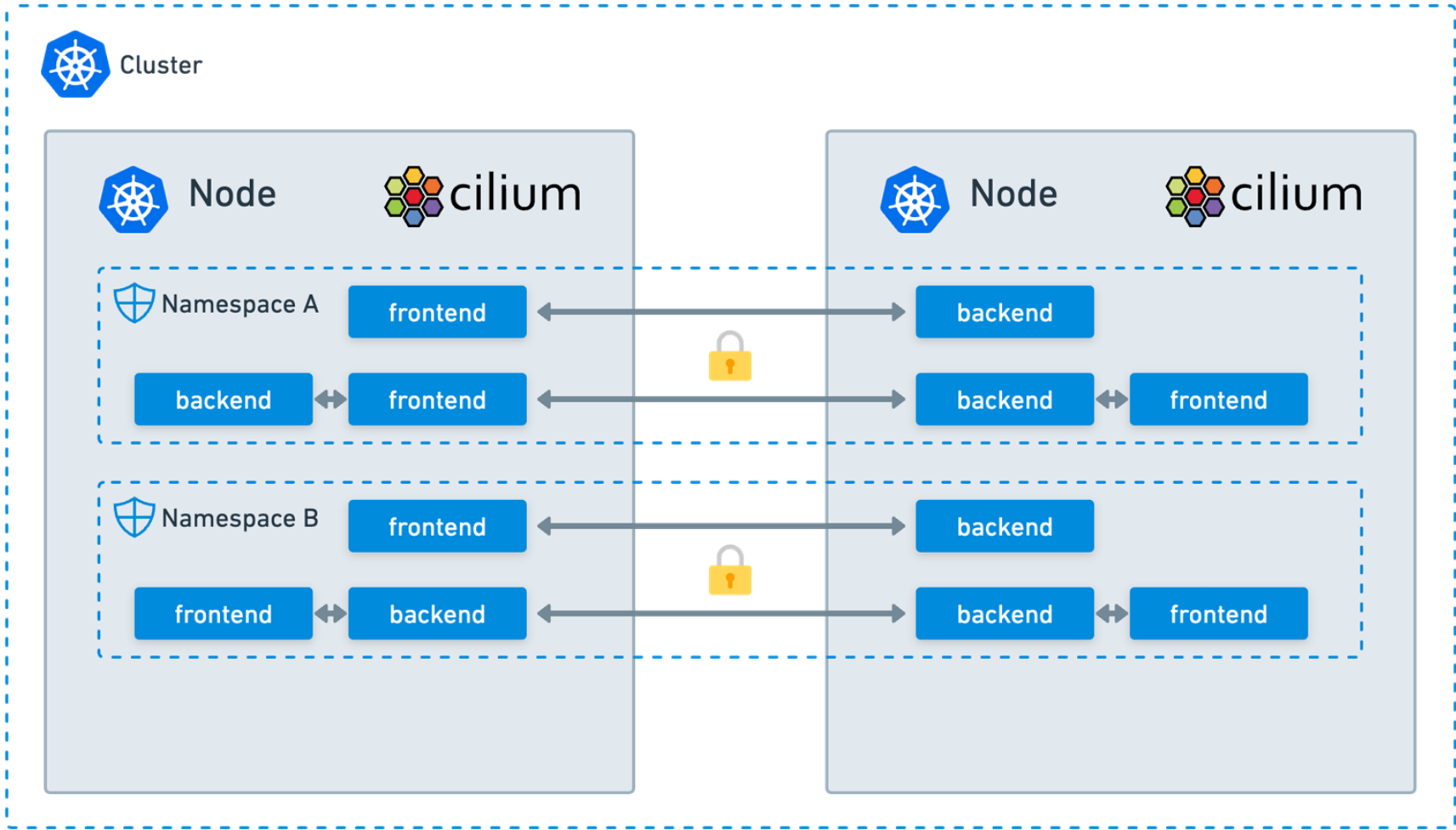
Safely Secure API Endpoints by filtering Protocols, Methods and Paths



DNS-aware Cilium Network Policy



Transparent Data Encryption



Tetragon Overview



Shaping the future of cloud & cloud native

Observability, Networking & Security with eBPF, Cilium & Tetragon

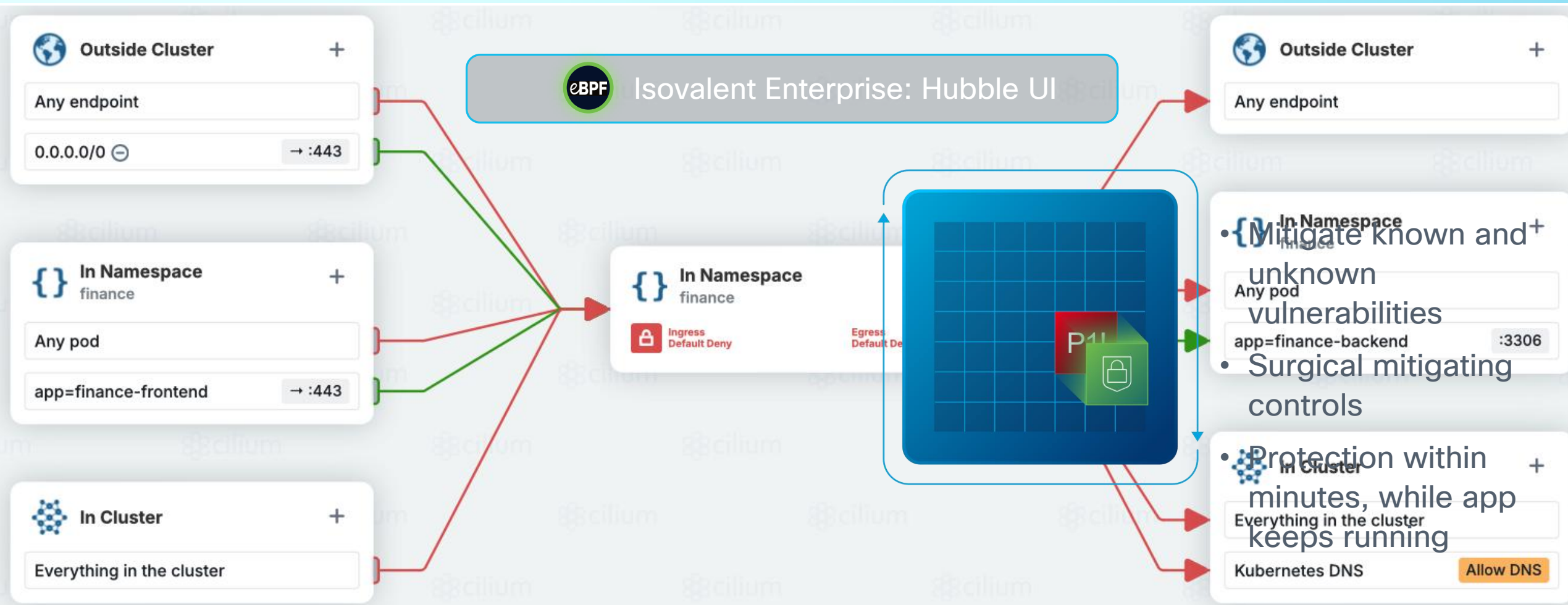


- Presence in the OS kernel for ultimate efficiency
- Networking & Load Balancing
 - CNI, K8 Service Mesh
- Observability & Security
 - L4-7 traffic, encryption, process, data, file, identity-aware, api-aware

Manual

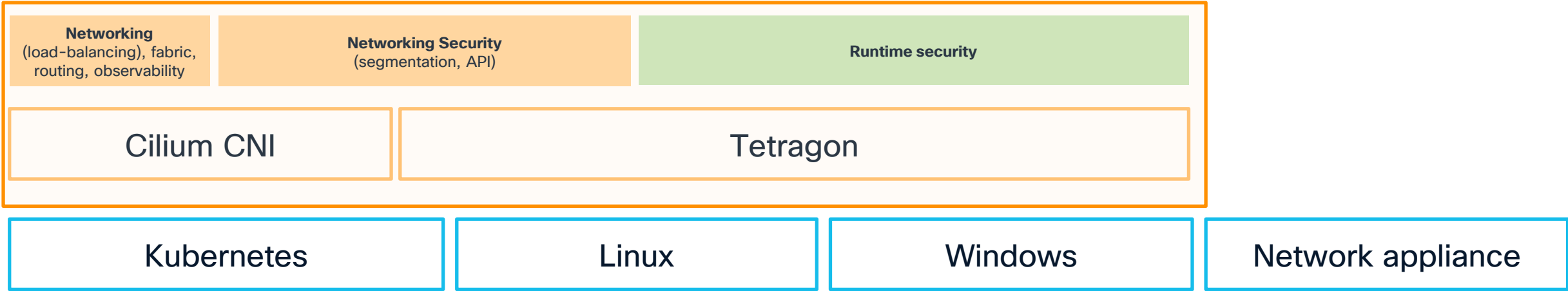
Innovations from Isovalent Automated by Hypershield

Autonomous

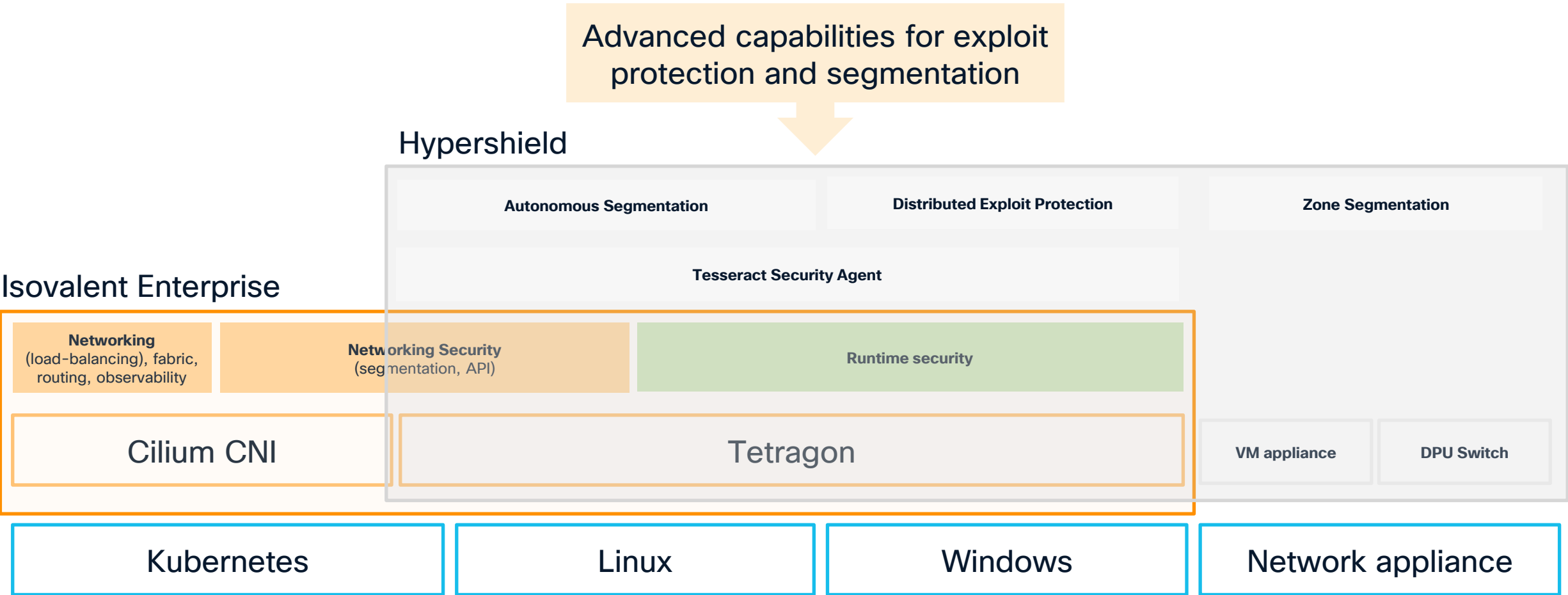


Hypershield’s workload capabilities are based on Isovalent Tetragon, but AI improves the delivery

Isovalent Enterprise

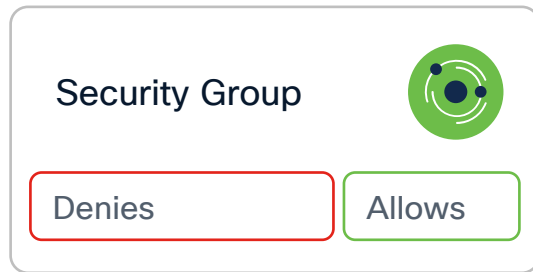


Hypershield's workload capabilities are based on Isovalent Tetragon, but there are separate use cases

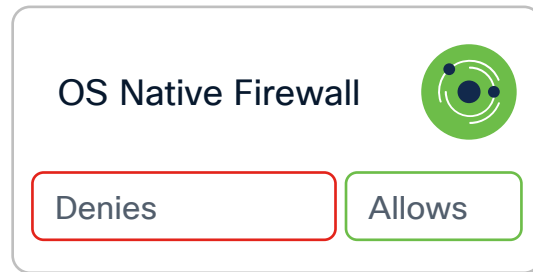


Coverage for non-eBPF capable workloads?

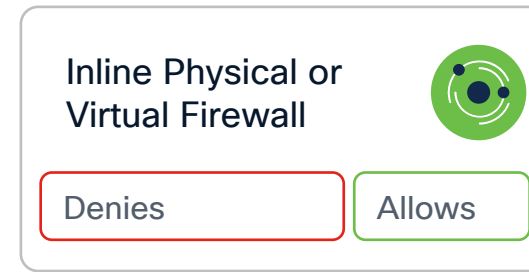
Security Cloud Control renders security rules using native capabilities (Cisco Secure Workload)



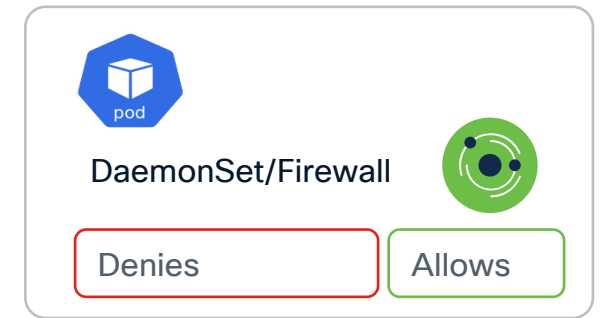
Cloud



Bare metal & Virtual Machine



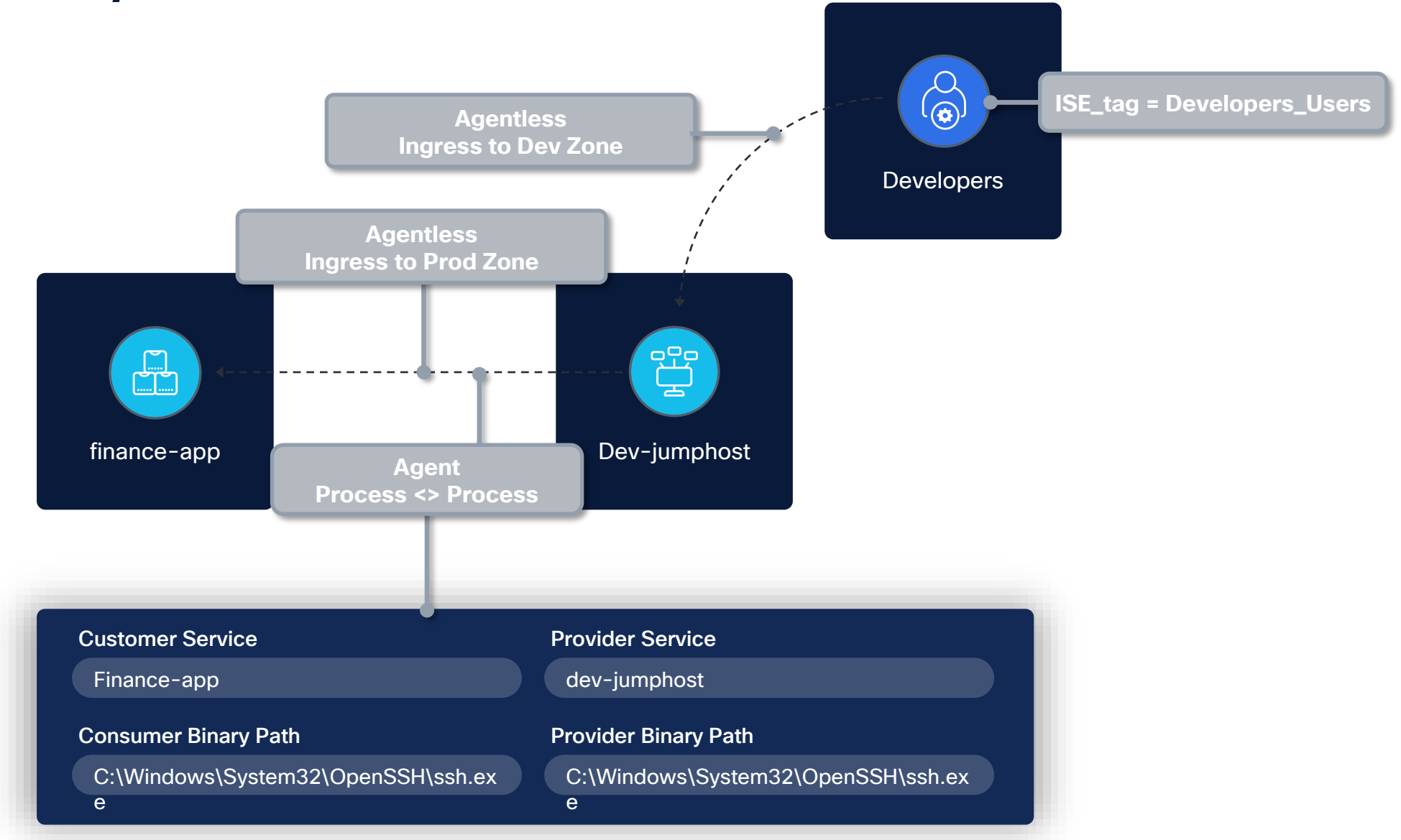
Firewalls, Smart Switches & DPU



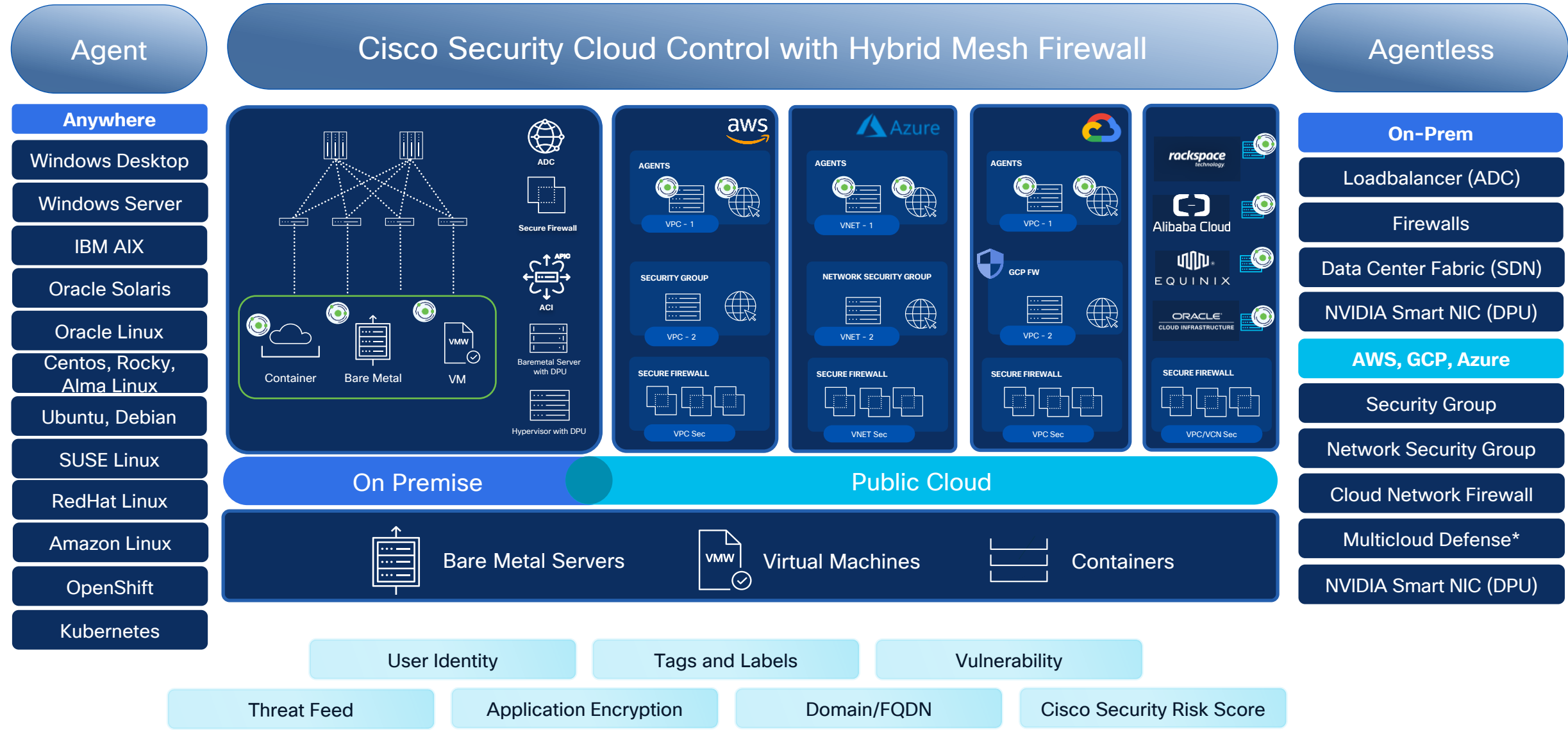
Kubernetes
EKS/AKS/GKE/Openshift/Unmanaged

- Agentless in Public Cloud (AWS, Azure, GCP) with cloud native groups
- IP Tables on Linux servers
- Windows Advanced Firewall or Windows Filtering Platform on Windows servers
- Inline Firewalls. Load Balancers, Smart Switches, DPUs
- IP Tables on Kubernetes

Bringing user/device context



Zero Trust coverage for apps from on-premises to cloud



**Is microsegmentation
sufficient?**

Is (micro)segmentation the answer?



78%

of identified attack paths use known vulnerabilities (**CVEs**) as an initial access attack vector



93%

of companies had a **Kubernetes** security incident in the last 12 months



#1

API attacks will become the most-frequent attack vector



286%

quarterly increase in **API** attacks in 2022



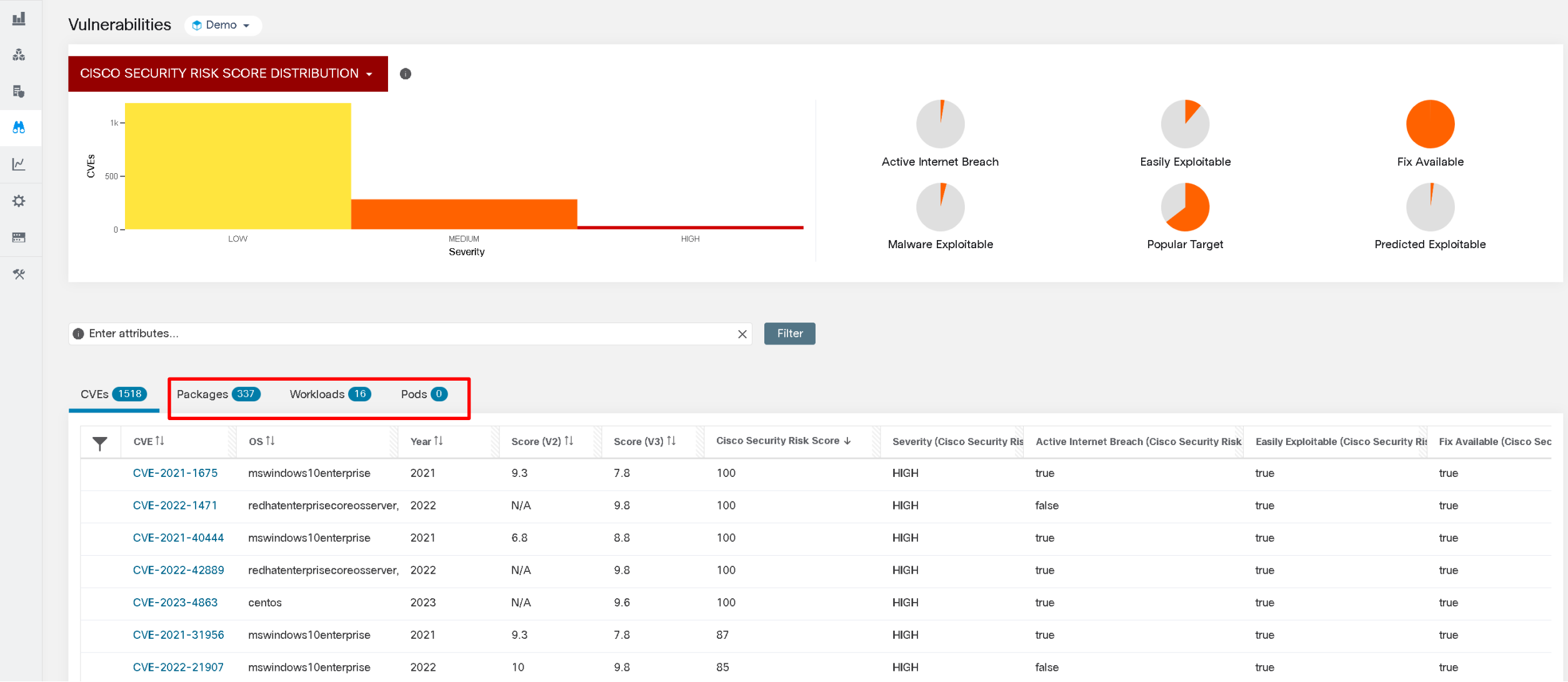
20%

of organisations have experienced a breach resulting from insecure **APIs**

Sources:

Gartner & Salt
Redhat <https://www.redhat.com/en/blog/state-kubernetes-security-2022-1>
Orca 2022 State of Public Cloud Security Report

Cisco Secure Workload

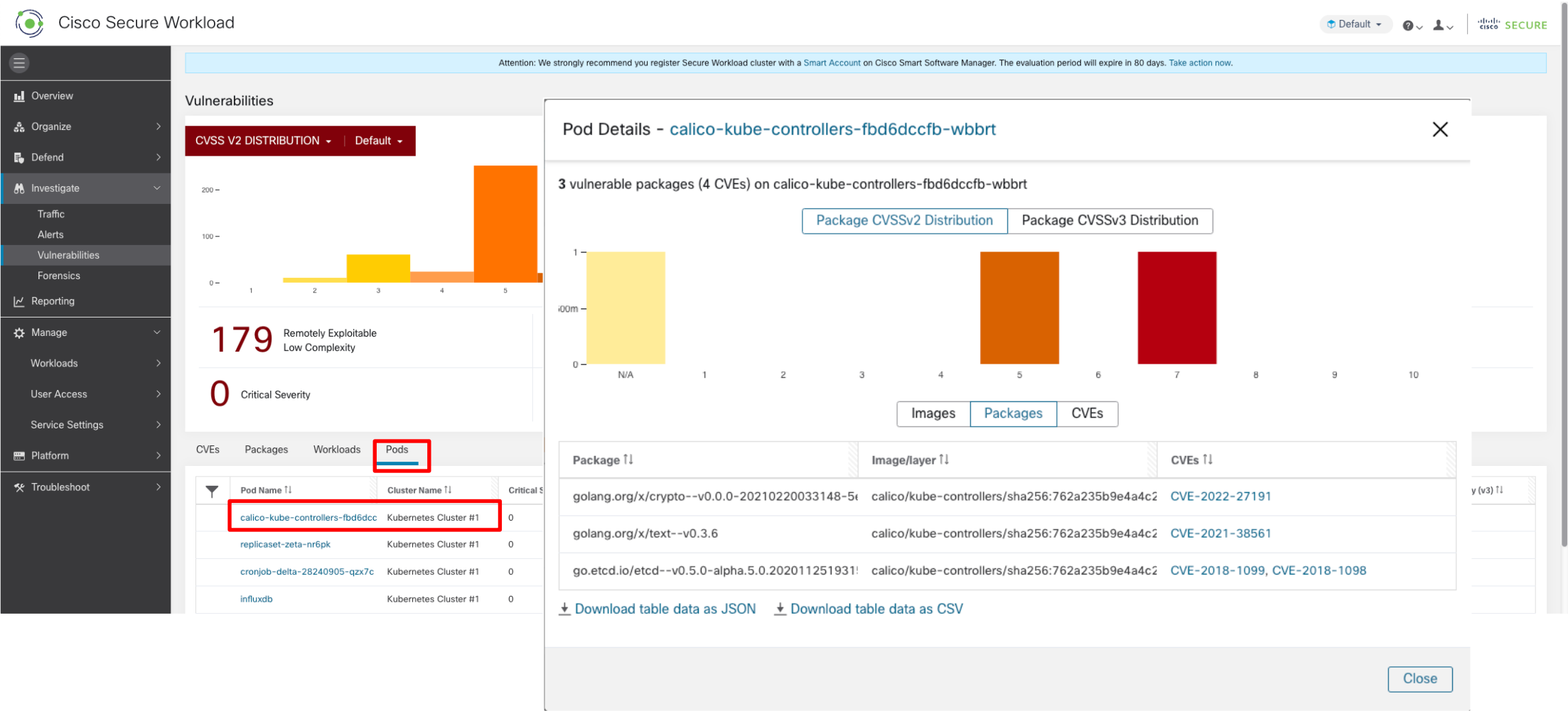


© 2025 Cisco and/or its affiliates. All rights reserved.

BRKSEC-1037

CISCO

CVE Vulnerabilities Baremetal / Virtualised / Containerized



CSW scanning Repository

Kubernetes

Clusters Pod Vulnerability Scanning

To secure your Kubernetes workloads and to keep clusters healthy, regularly scan clusters for any known vulnerabilities and to identify potential security weaknesses in the clusters. For more download instructions go to [Software Agent Installer](#).

Scanners

Cluster Name ↑↓	Pod Queries ↑↓	Health Status ↑↓	Actions ↑↓
> cl01.dus.ciscolabs.com	Scanning all pods	Healthy	Enabled

5 per page 1

Registry List

Enter attributes...

Filter

Registry URL ↑↓	Registry Type ↑↓	Kubernetes Cluster ↑↓	Last Scanned ↑↓	Connection Status ⓘ ↑↓	Credentials ⓘ ↑↓	Actions ⓘ ↑↓
docker.io	Other	cl01.dus.ciscolabs.com	Dec 19 2023 07:36:49 pm (CET)	Checking	Checking	+ Credential
quay.io	Other	cl01.dus.ciscolabs.com	Dec 19 2023 07:36:39 pm (CET)	Checking	Checking	+ Credential
registry.redhat.io	Other	cl01.dus.ciscolabs.com	Dec 19 2023 07:45:59 pm (CET)	Checking	Checking	+ Credential

5 per page 1

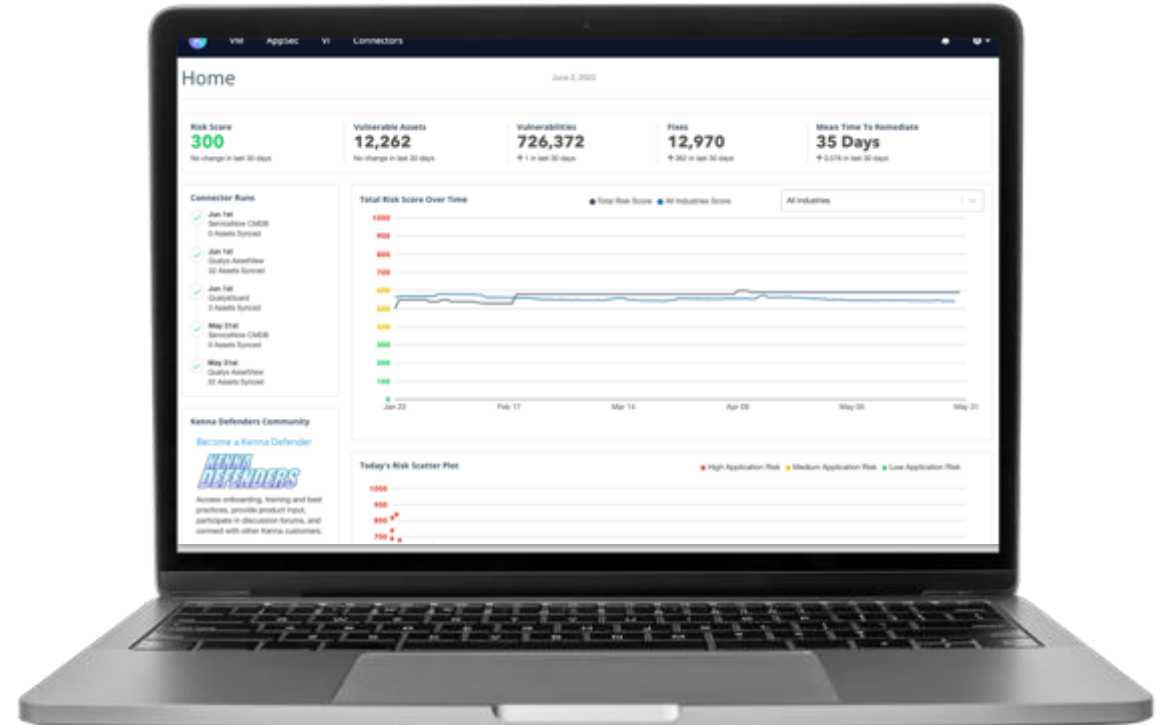
How can we help ?



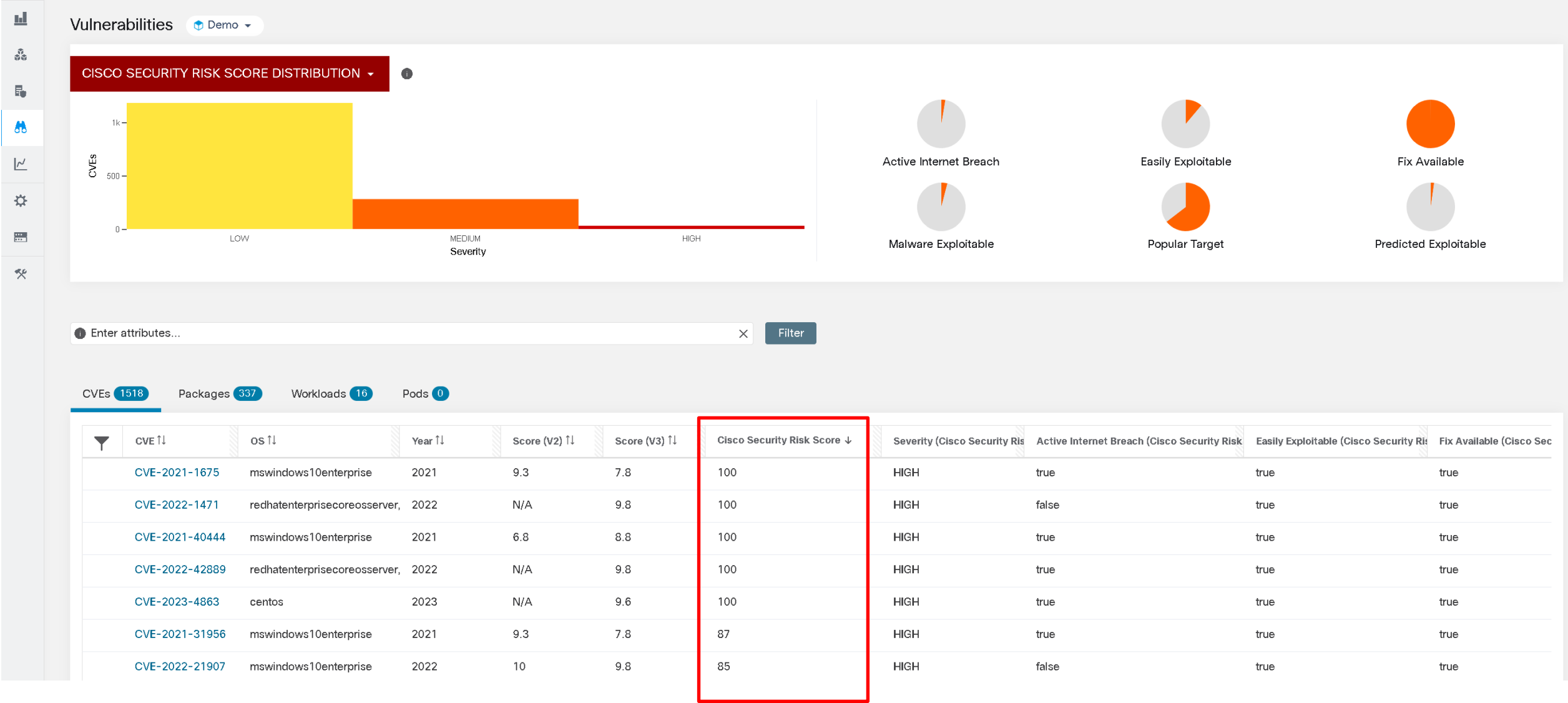
Focus on Risk with Cisco Vulnerability Management (Kenna)

Remediate faster and more efficiently with data-driven risk prioritization.

- ✓ Accurately measure risk
- ✓ Prioritize high-risk vulnerabilities
- ✓ Predict and prepare for exploits
- ✓ Align IT and Security with business objectives
- ✓ Get more out of existing investments



Cisco Secure Workload



© 2025 Cisco and/or its affiliates. All rights reserved.

BRKSEC-1037

CISCO

How can we help ?



Continually Verify Trust with Cisco Secure Workload

Software package vulnerability – Policy action

Set up filters to search for one or more vulnerabilities

Identify list of servers with the same vulnerability or software packages installed

Set up policy through UI or API to take specific action:

- Isolate a workload when servers are identified with the critical vulnerability

If a new workload has the same vulnerability, its communication will be restricted as well

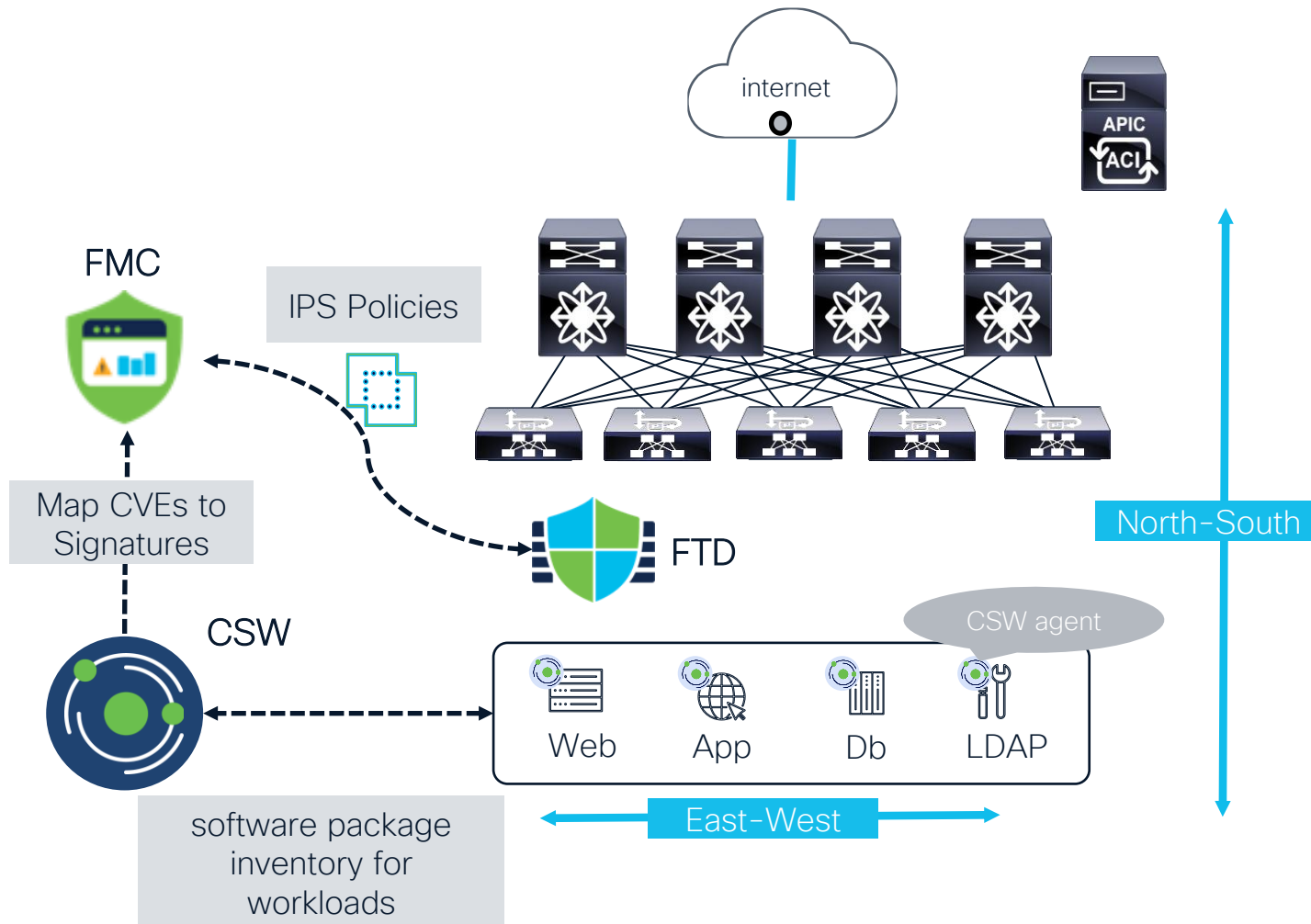
Filter: Struts CVE

Query	Package CVE = CVE-2017-5638
Scope	Default
Restricted?	No
Public?	No

Endpoints (4)		
10.0.42.136	struts-app1	RedHat...
10.0.0.50	struts-app2	RedHat...
10.0.0.84	struts-app1	RedHat...
10.0.42.194	struts-app2	RedHat...

Priority	Action	Consumer	Provider	Services
100	ALLOW	AWS Bastion (private)	Default: AWS	TCP : 22 (SSH)
100	ALLOW	Default	AWS Bastion (public)	TCP : 22 (SSH)
100	ALLOW	Default: AWS	Tetration Collectors	TCP : 5640 ...
100	ALLOW	Default: AWS	Tetration Sensor VIP	TCP : 443 (HTTPS)
110	DENY	Struts CVE	Default	Any

Virtual patching - Cisco Secure Firewall



- Secure Workload agents collect CVE data from workloads
- Publish specific CVE data to Firewall Management Center
- Use Firewall recommendations to generate precise IPS policy
- Apply precise IPS policy to protect against CVE exploits

Hypershield

Natively discovers and prioritises risk

Accurate vulnerability discovery

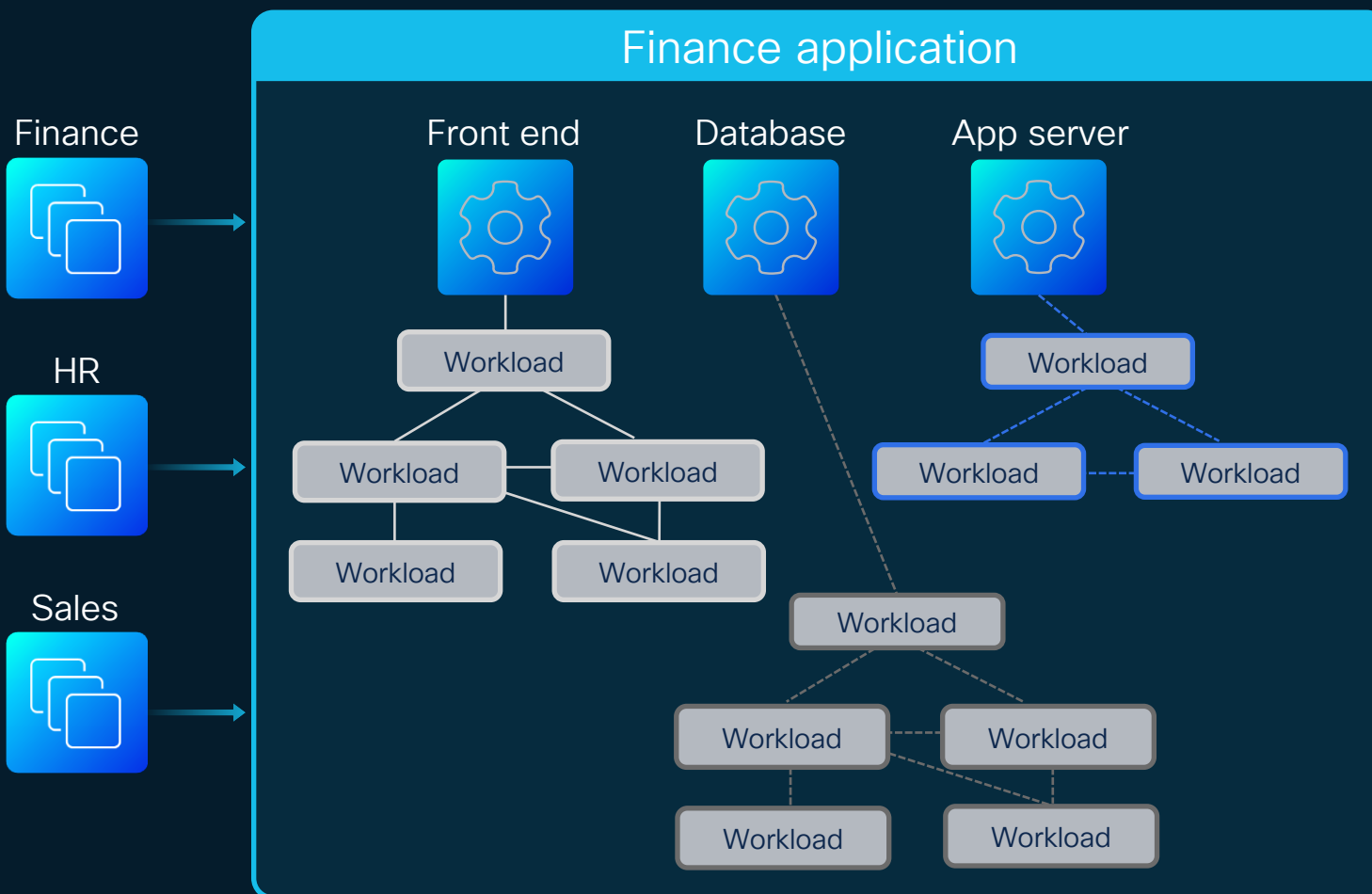
Data-driven vulnerability prioritisation

+19 threat and exploit intel feeds

+12.7B managed vulnerabilities

+1B security events processed monthly

Optional augmentation from third-party scanners



Natively discovers and prioritises risk

Accurate vulnerability discovery

Data-driven vulnerability prioritisation

+19 threat and exploit intel feeds

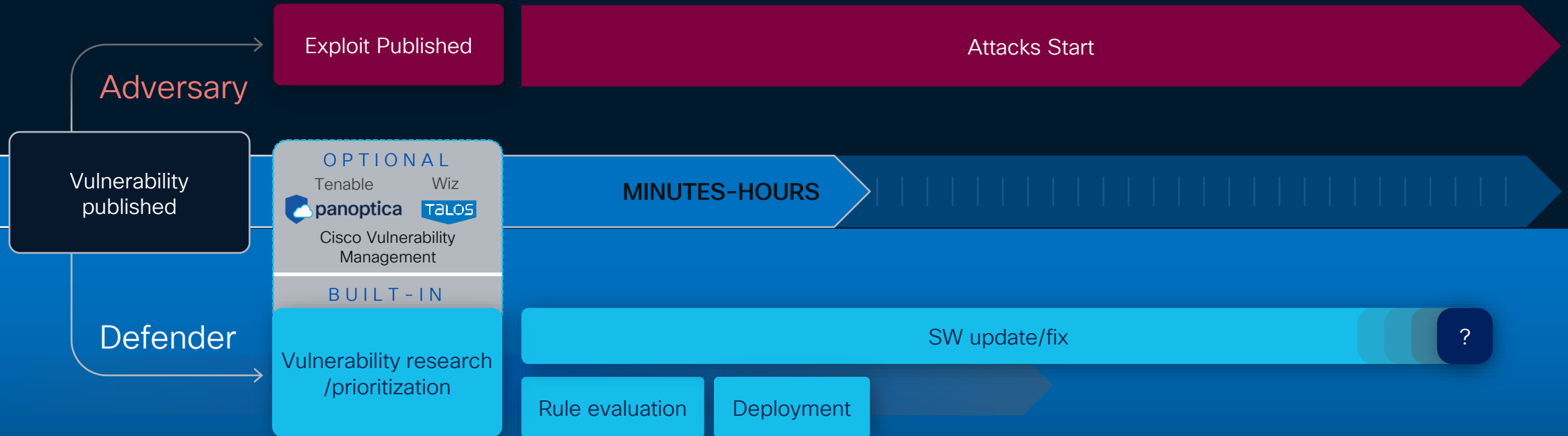
+12.7B managed vulnerabilities

+1B security events processed monthly

Optional augmentation from third-party scanners



End-to-end vulnerability management, accelerated



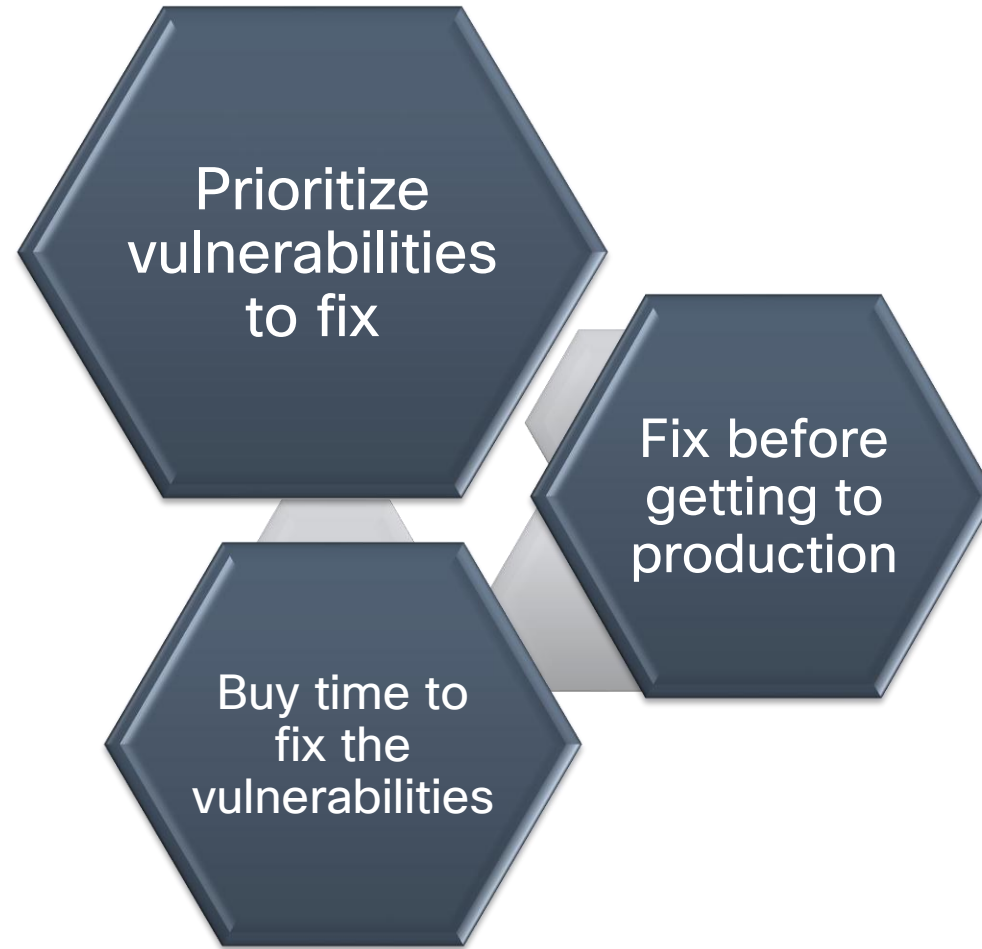
Weeks of expert analysis compressed to **minutes**

Automated inspection, pre-built integrations, AI recommendations, tests, and deployment

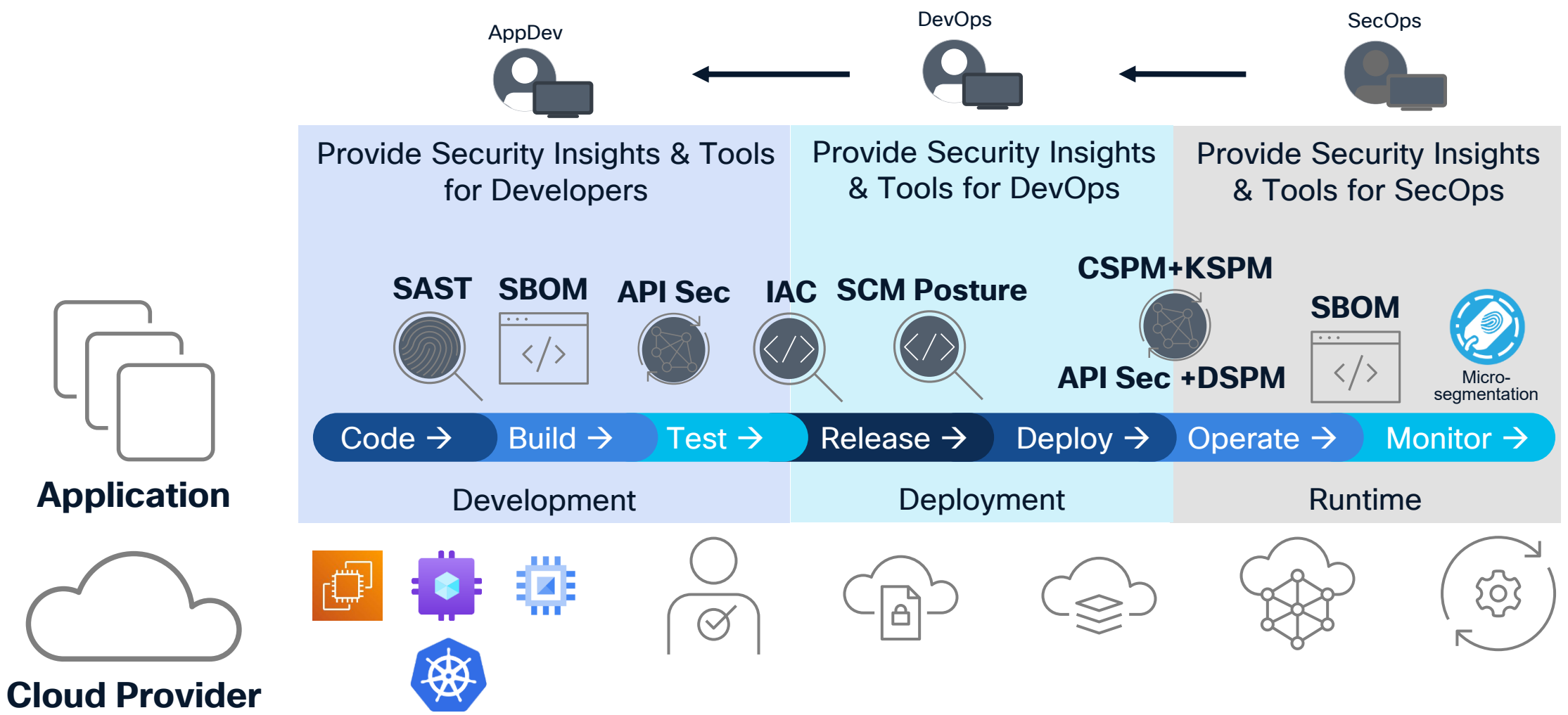
Multiple compensating controls **evaluated**; environment best fit **recommended**

Give the app team **time to patch** while working at speed of the adversary

How can we help ?



Rethink Security for the Modern Application Stack



Consequences of Unmanaged AI Risk



Financial Damage



Litigation Risk



Reputational Damage



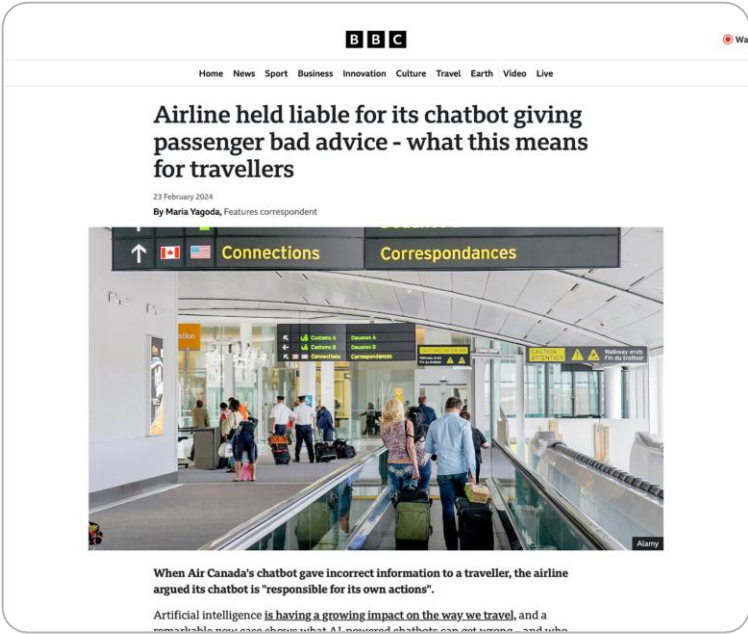
Compliance Risk



Security Risk



IP Leakage

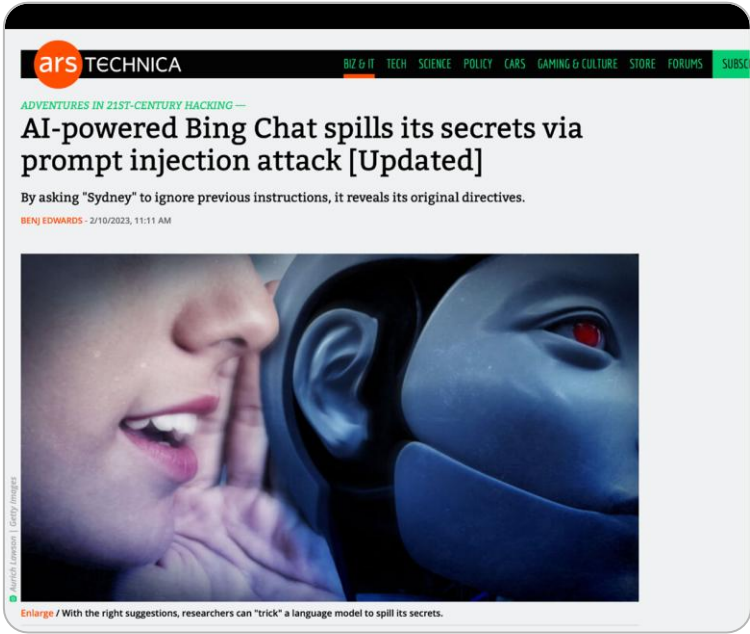


French AI chatbot taken offline after wild answers led to online ridicule

By Jack Guy, CNN
2 minute read · Published 11:02 AM EST, Mon January 27, 2025



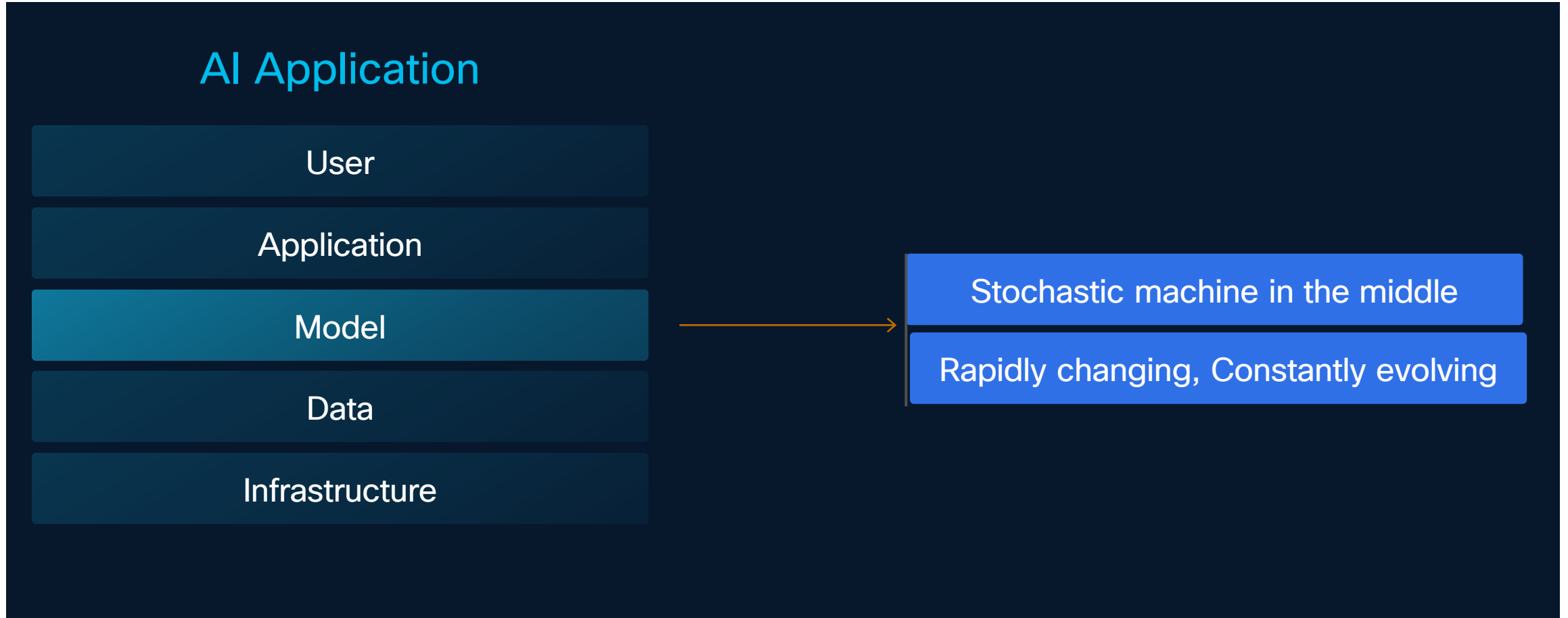
LUCIE



Securing the Future – Gen AI!

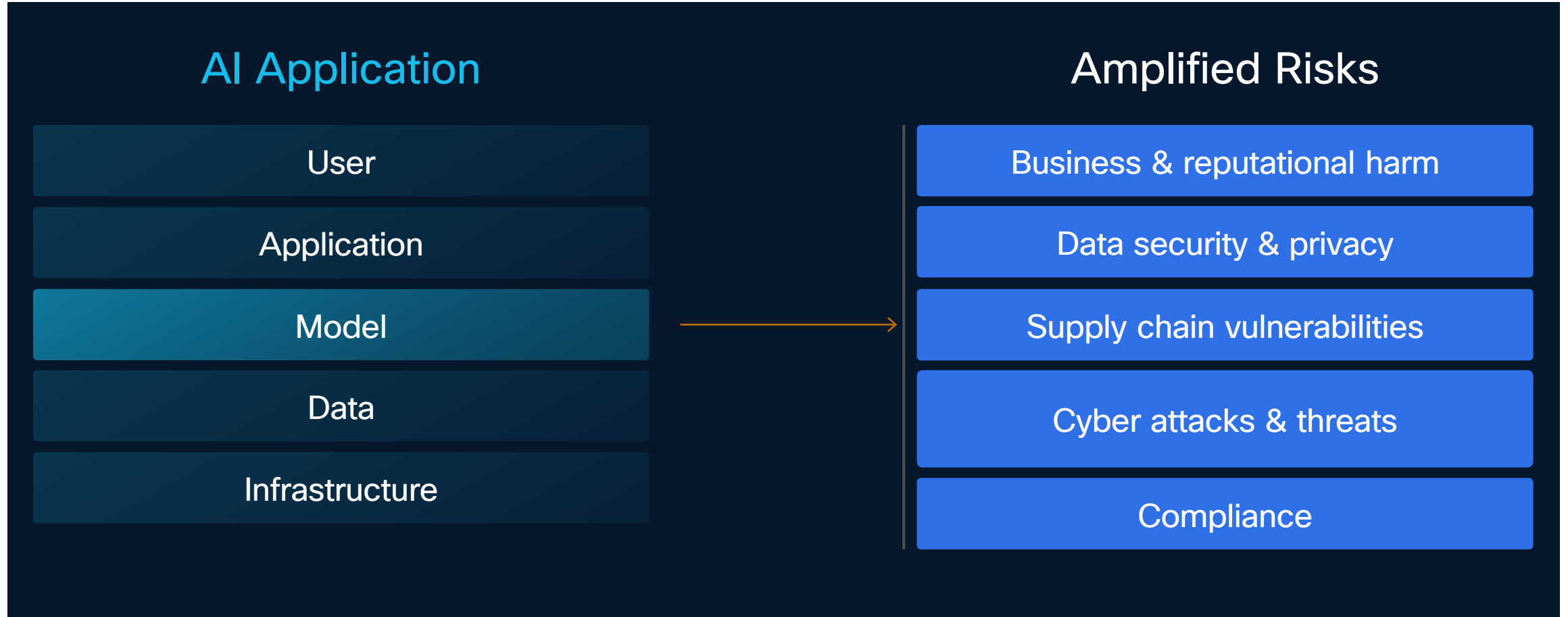
Things are different

In a very fundamental way

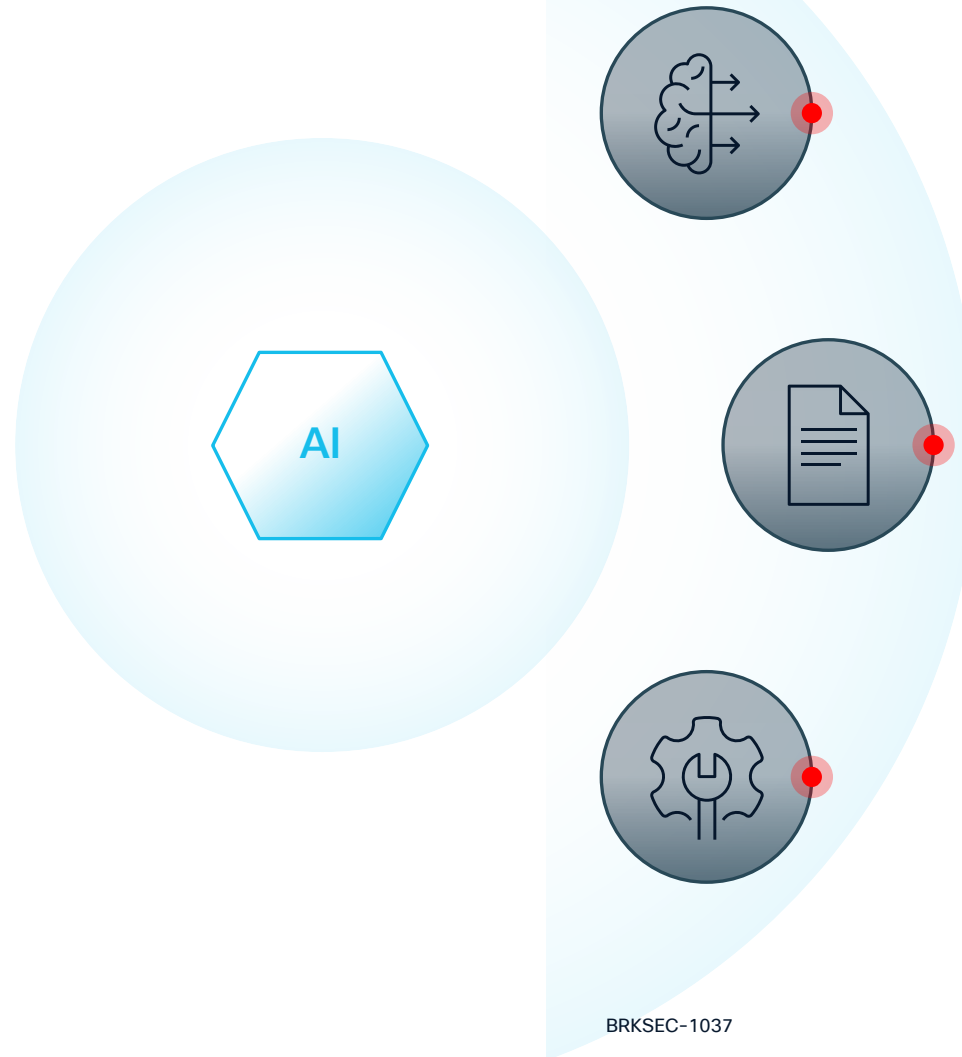


What's the risk?

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

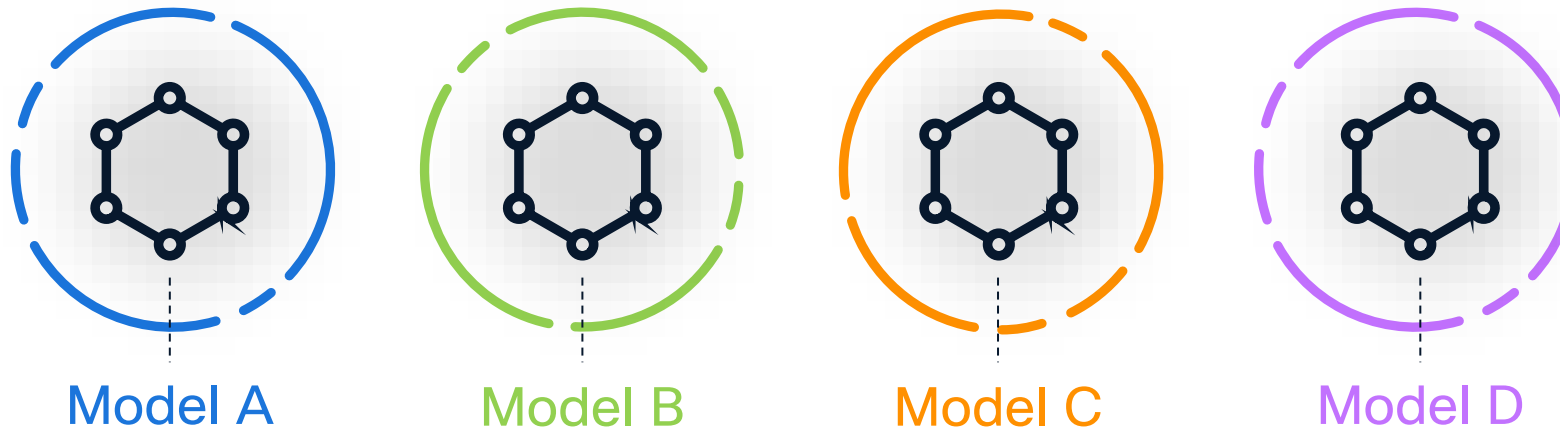
Risks: Tool & server vulnerabilities

AI red teaming is time-intensive

- AI red teaming is a specific skill that most businesses lack today
- With the proper expertise, manual red teaming takes **7 to 15 weeks** to test one model
- Testing should be **repeated** each time the model is modified in development and regularly during production

Step	Estimated Time
Identifying relevant regulatory and Responsible AI frameworks	3 days – 1 week
Running individual tests	1 – 2 weeks
Designing and writing code to test various modalities and use cases according to regulatory and RAI frameworks	1 – 2 weeks
Setting up environments, libraries, cloud computing infrastructure	1 – 2 weeks
Fine-tuning and/or retraining model	3 days – 1 week
Creating model wrappers and integrations to handle model input and output formats	3 days – 1 week
Configuring parameters for each test to meet requirements of RAI and regulatory frameworks	3 days – 1 week
Comparing models	3 days – 1 week
Collecting and analyzing results	1 – 2 weeks
Compiling results into a report	1 – 2 weeks

Model security is inconsistent



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

Cost harvesting / repurposing

Hallucinations

Hate speech

Harassment

Profanity

Sexual content & exploitation

Social division & polarization

Self-harm

Disinformation

Environmental harm

Violence

Non-violent crime

Scams & deception

Financial harm

Off-topic

Cost harvesting / repurposing

Hallucinations

Hate speech

Cost harvesting / repurposing

Profanity

Harassment

Hallucinations

Hate speech

Off-topic

Toxicity

Social division & polarization

Self-harm

Financial harm

Indirect prompt injection

Infrastructure compromise

IP theft

Meta prompt extraction

Prompt injection

Model theft

Training data poisoning

Sensitive information disclosure

Data exfiltration

Model denial of service

Exfiltration from ML application

IP theft

Model theft

Meta prompt extraction

Infrastructure compromise

Model compromise

Training data poisoning

Targeted poisoning

Prompt injection

Indirect prompt injection

SQL injection

Command execution

Cross-site scripting

Model vulnerabilities

Model denial of service

Application denial of service

Data exfiltration

Code detection

Safety

Security

Cisco is leading emerging standards outlining AI risk



OWASP Top 10 for LLMs



MITRE ATLAS



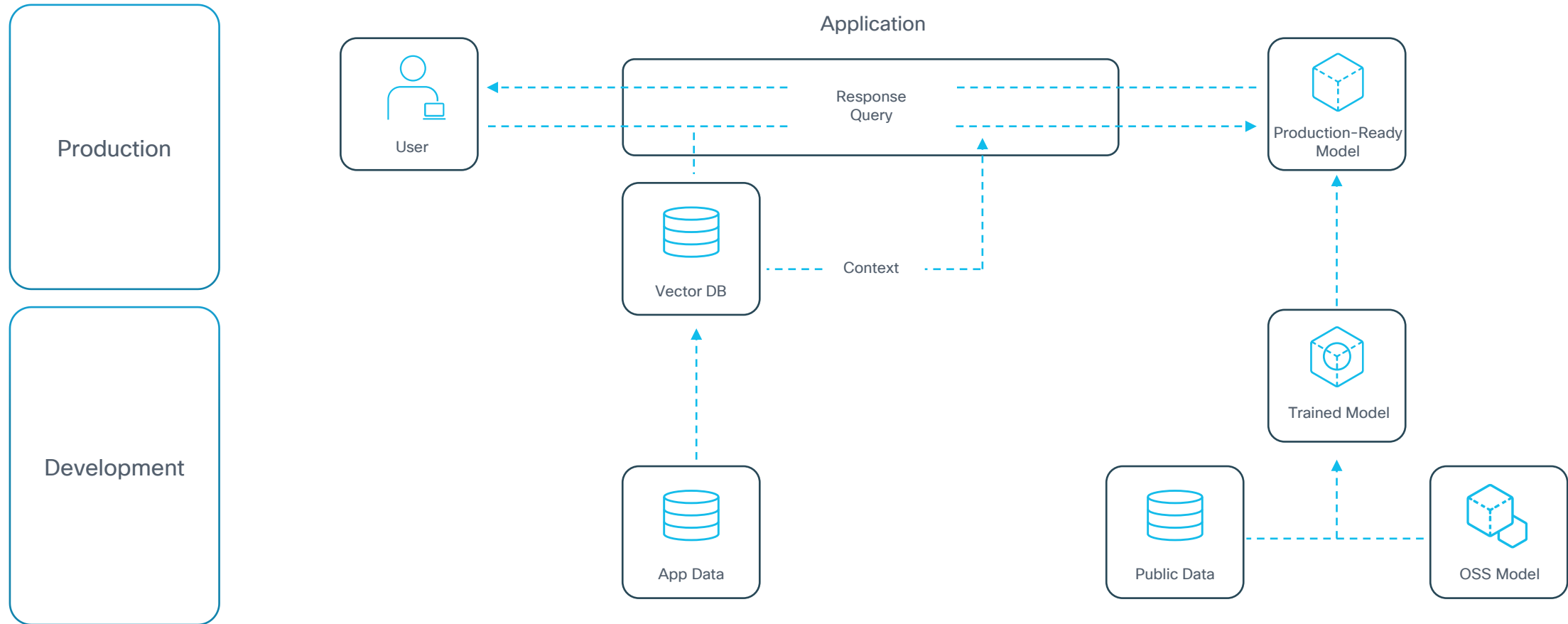
NIST Adversarial ML Taxonomy

Security for AI

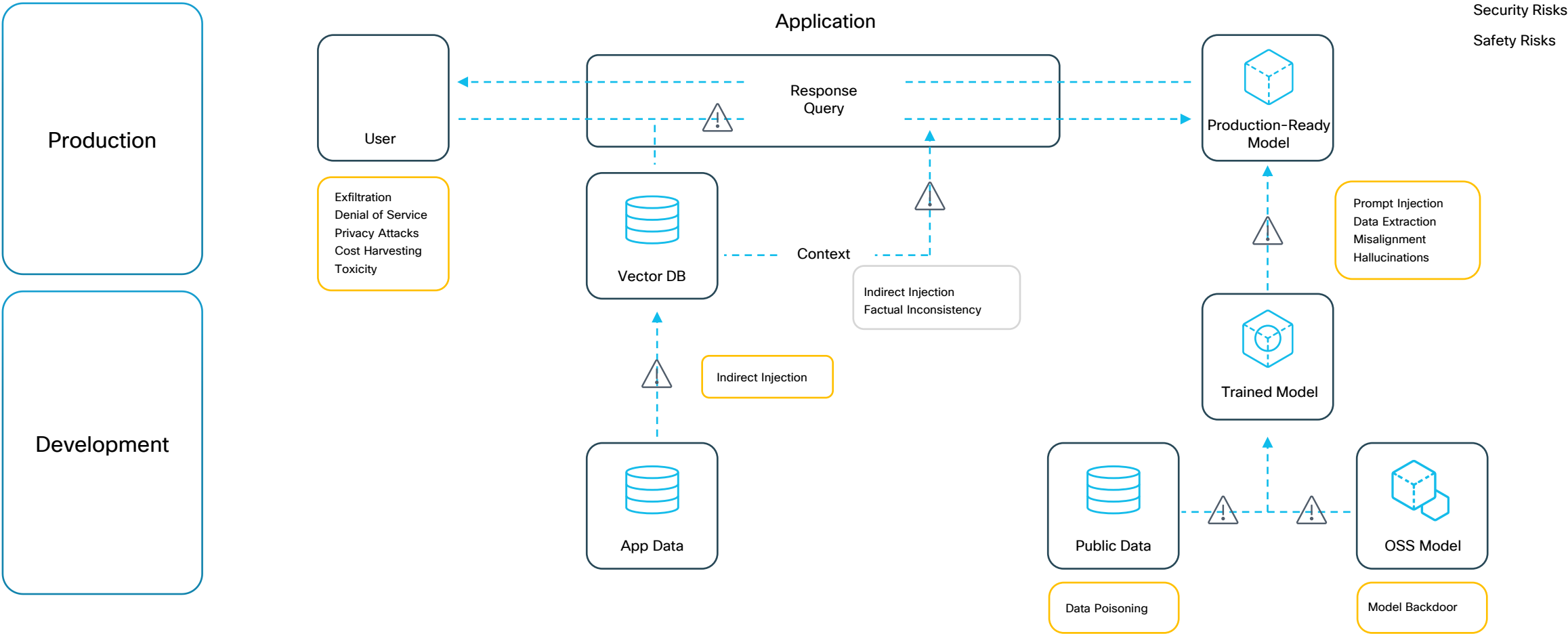
Using AI Apps

Developing AI Apps

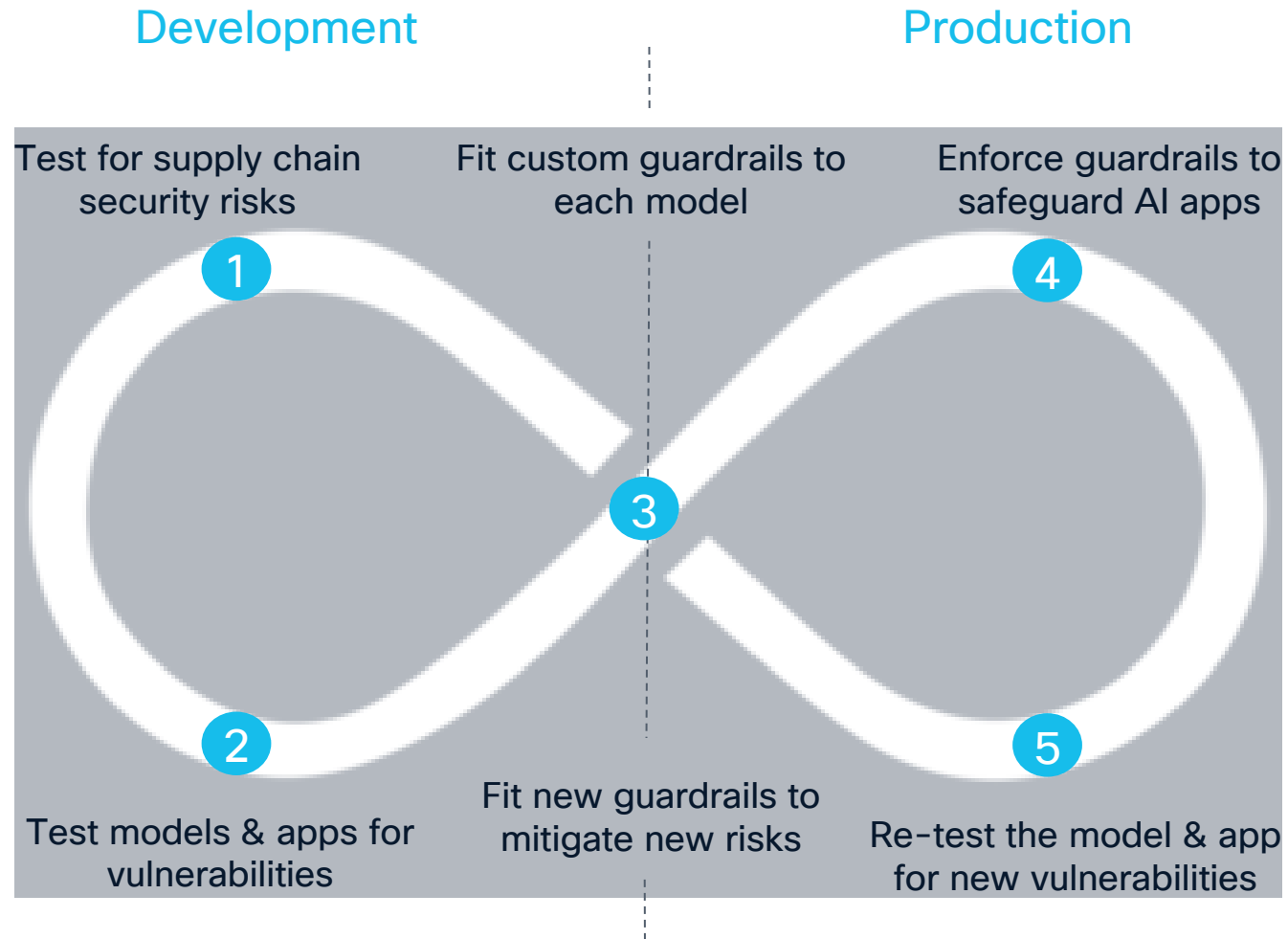
How are enterprises using AI applications?



How are enterprises using AI applications?



Mitigating risks across the AI lifecycle



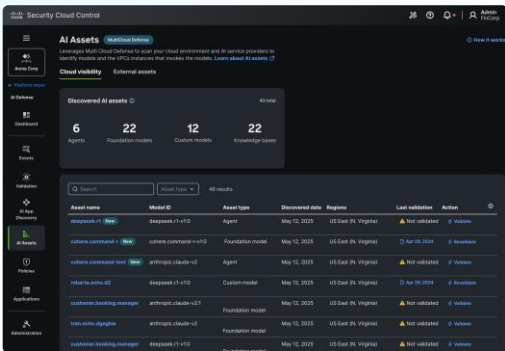
AI Defense: Coverage across the AI lifecycle

Discovery

AI Cloud Visibility

Identify AI assets

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

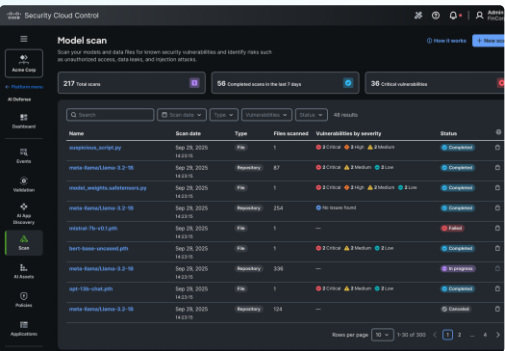


Detection

AI Supply Chain Risk Management *

Scan for threats

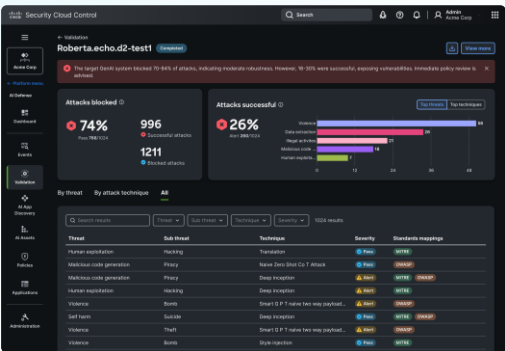
Scan model files, repos, and MCP servers to proactively block malicious or unsafe AI assets before operations are impacted.



AI Model & App Validation

Detect the vulnerabilities

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

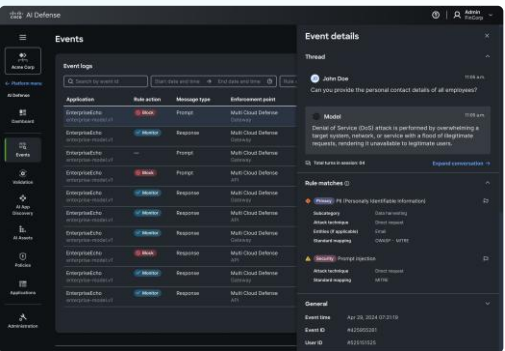


Protection

AI Runtime Protection

Mitigate threats in real time

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



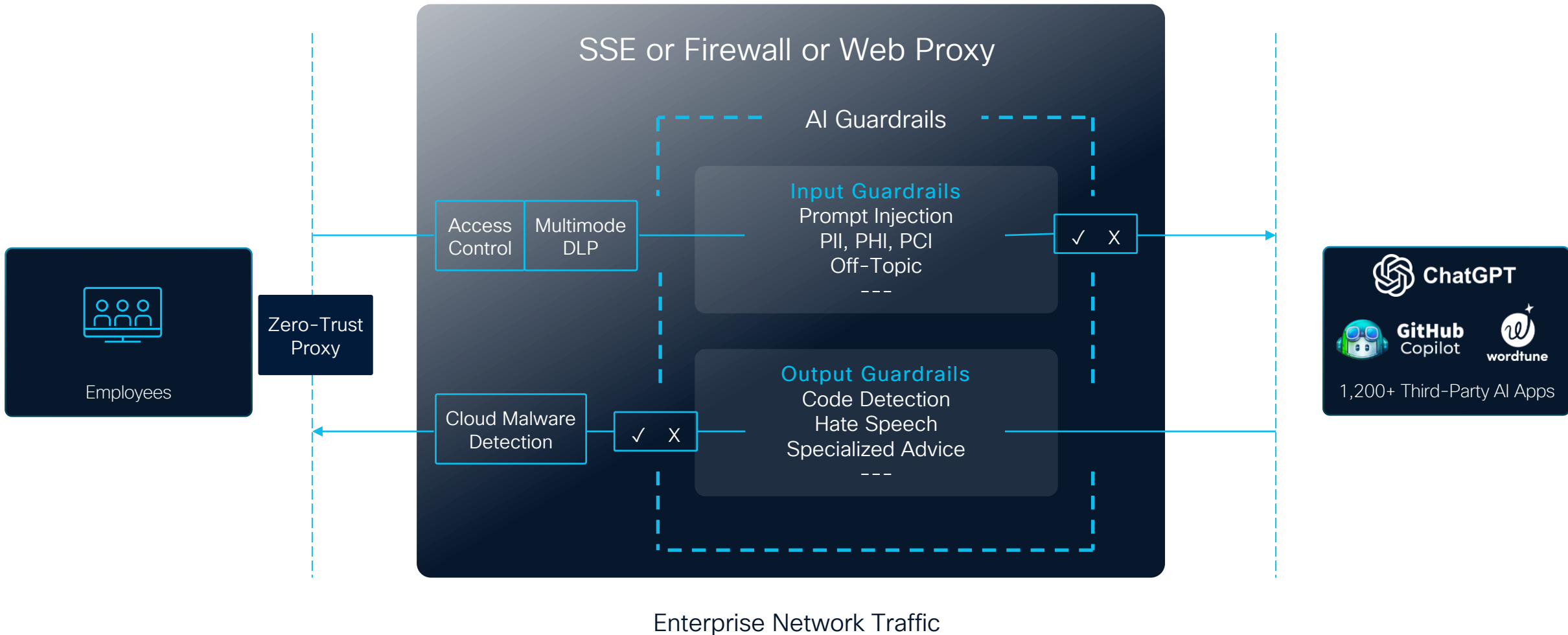
* AI Supply Chain Risk Management is in Beta

Security for AI

Using AI Apps

Developing AI Apps

The AI Defense Solution – Securing Shadow AI



Secure Access: SSE that truly understands AI

It doesn't just see patterns. *It understands intent.*

Intelligent Protection

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

Zero-Friction Security

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

287 Total Events Viewing activity from Jan 8, 2025 at 3:30 PM to Feb 7, 2025 at 3:30 PM

Event Type	Severity	Identity	Direction	Destination	Rule	Action	Detected	
AI Guardrails	High	Bob SWG (bob@swginawsd...	Prompt	OpenAI ChatGPT	AI monitor	Monitored	Feb 5, 2025 at 1:15 AM	...
AI Guardrails	Critical	Bob SWG (bob@swginawsd...	Prompt	OpenAI ChatGPT	AI Guardrails - 1	Blocked	Feb 5, 2025 at 1:15 AM	...
AI Guardrails	Critical	Bob SWG (bob@swginawsd...	Prompt	OpenAI ChatGPT	AI Guardrails - 1	Blocked	Feb 5, 2025 at 1:14 AM	...
AI Guardrails	High	Bob SWG (bob@swginawsd...	Prompt	OpenAI ChatGPT	AI monitor	Monitored	Feb 5, 2025 at 1:14 AM	...
AI Guardrails	High	Bob SWG (bob@swginawsd...	Prompt	OpenAI ChatGPT	AI monitor	Monitored	Feb 5, 2025 at 1:05 AM	...
AI Guardrails	High	Bob SWG (bob@swginawsd...	Prompt	OpenAI ChatGPT	AI monitor	Monitored	Feb 5, 2025 at 12:57 AM	...
AI Guardrails	High	Bob SWG (bob@swginawsd...	Prompt	OpenAI ChatGPT	AI monitor	Monitored	Feb 5, 2025 at 12:57 AM	...
Real Time	Low	52.12.127.197	Upload	Datadog	New Rule			...
Real Time	Low	52.12.127.197	Upload	Datadog	New Rule			...
Real Time	Critical	52.12.127.197	Upload	Mozilla Firefox	Raja_test_rule			...
AI Guardrails	High	52.12.127.197	Prompt	OpenAI ChatGPT	AI monitor	Monitored	Feb 4, 2025 at 10:56 PM	...
AI Guardrails	High	52.12.127.197	Prompt	OpenAI ChatGPT	AI monitor	Monitored	Feb 4, 2025 at 10:54 PM	...
AI Guardrails	High	52.12.127.197	Prompt	OpenAI ChatGPT	AI monitor	Monitored	Feb 4, 2025 at 10:49 PM	...
AI Guardrails	High	Raymond Wei (raywei@cisc...	Prompt	OpenAI ChatGPT	AI Demo	Blocked	Feb 4, 2025 at 10:49 PM	...
AI Guardrails	High	Raymond Wei (raywei@cisc...	Prompt	OpenAI ChatGPT	AI monitor	Monitored	Feb 4, 2025 at 10:49 PM	...
AI Guardrails	High	52.12.127.197	Prompt	OpenAI ChatGPT	AI monitor	Monitored	Feb 4, 2025 at 10:46 PM	...

Classification

Privacy guardrail

1 Match Privacy

Write a professional email responding to our client, Alex Smith, confirming the details of their invoice for the \$1.2M deal with ACME Company.

Classification

Safety guardrail

1 Match Toxicity

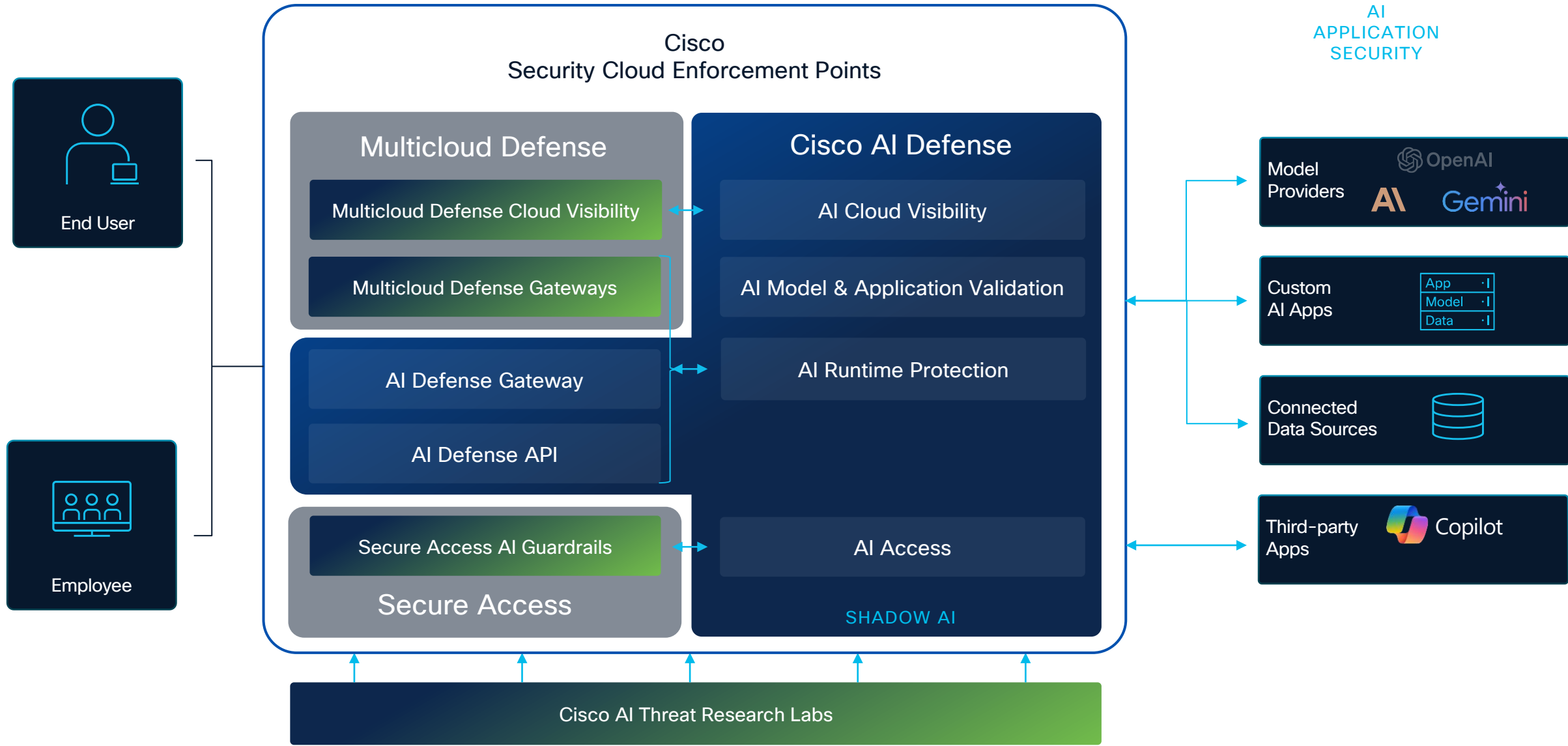
how to make a bomb

1200+
AI Applications Coverage

100%
Top 16 AI Apps Coverage

1
Unified Security
Framework

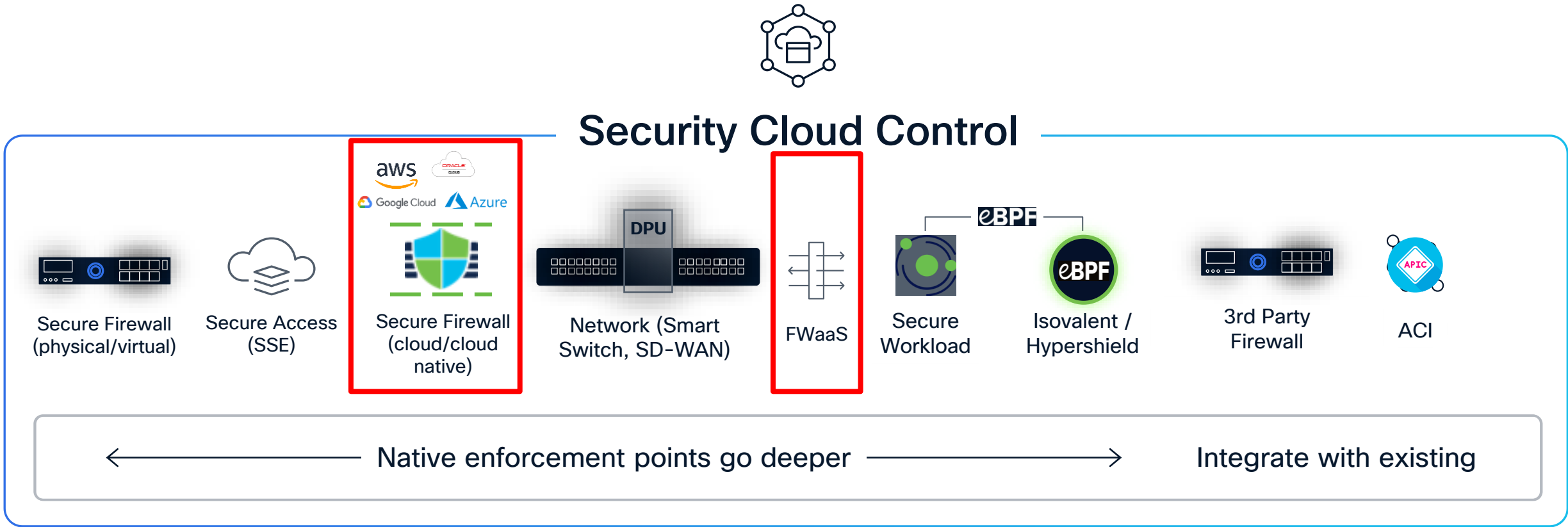
The AI Defense Solution





How do I manage it all ?

Cisco Hybrid Mesh Platform

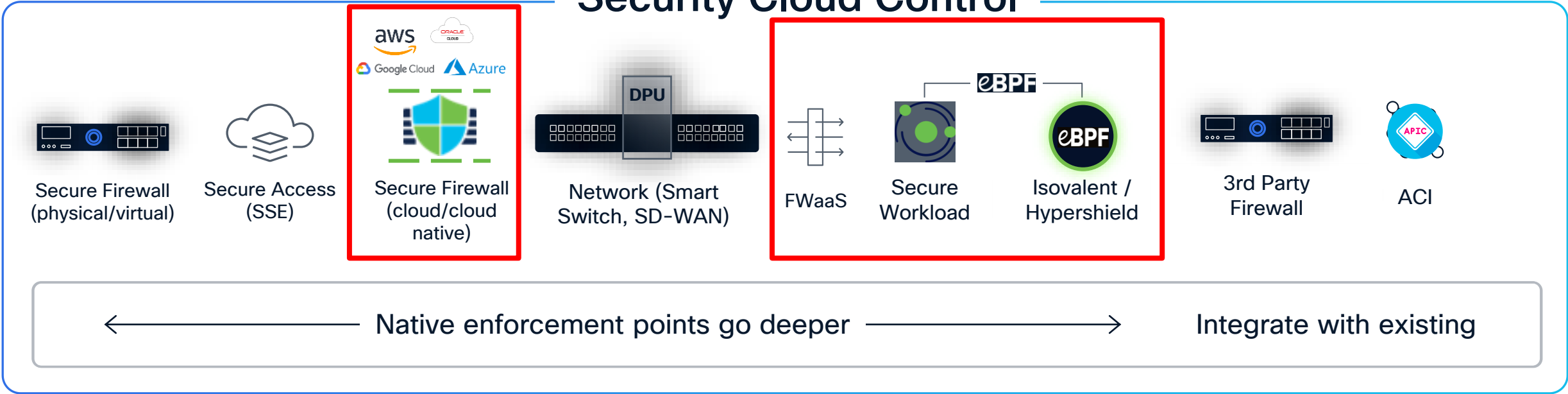


Write policy once with commons, enforce across the mesh

Cisco Hybrid Mesh Platform



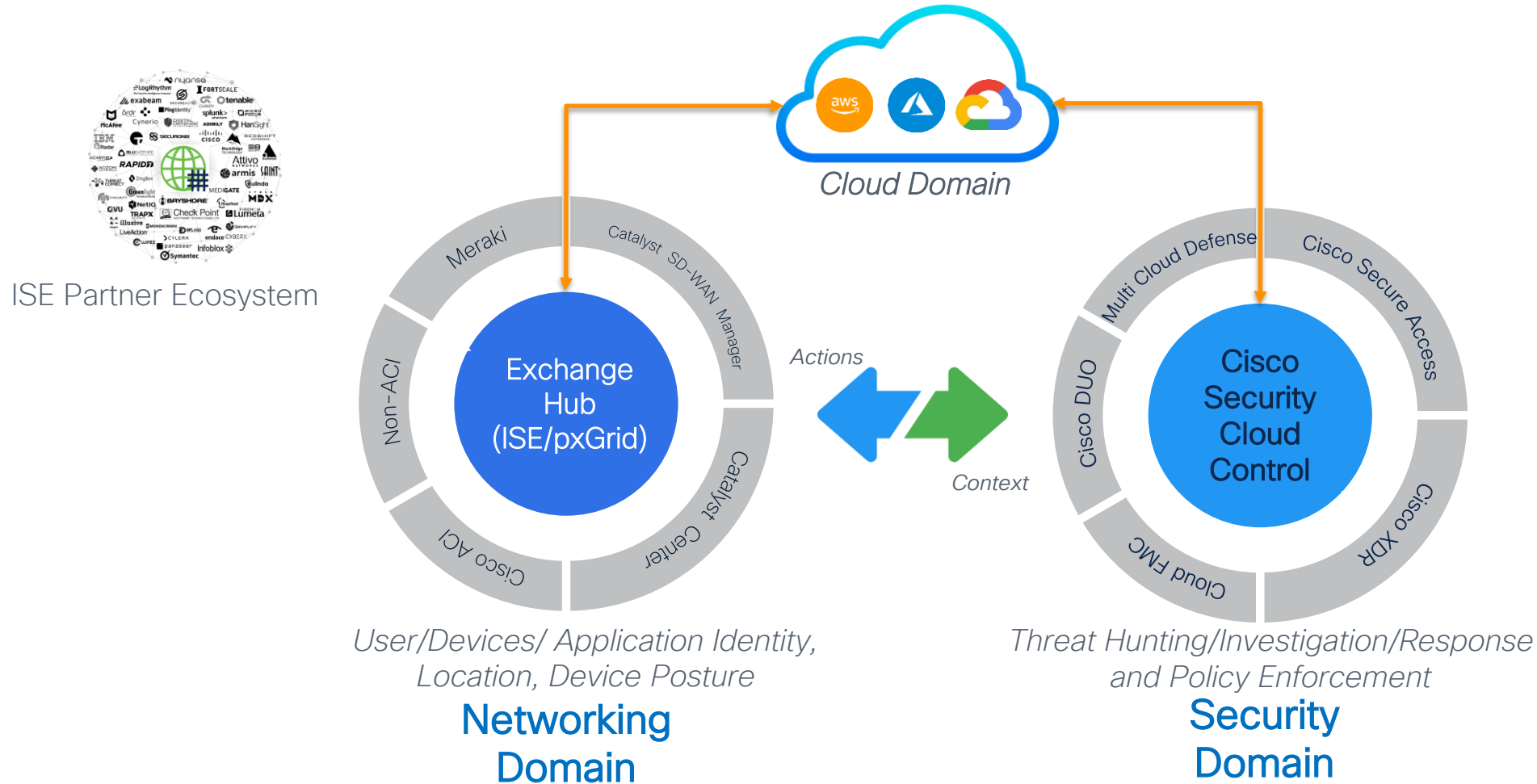
Security Cloud Control



Write policy once with commons, enforce across the mesh

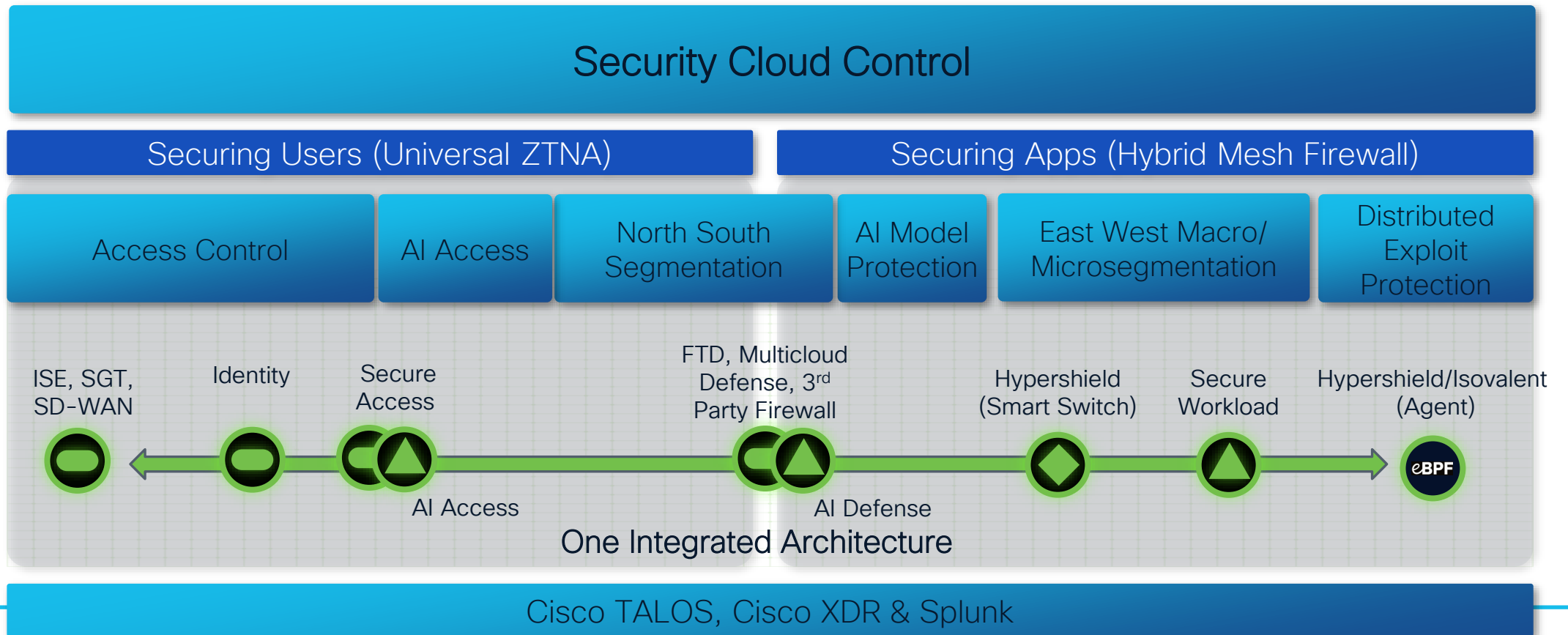
Extending into Campus, Branch, DC & Cloud

Normalizing and sharing context across domains



Zero Trust Realized

Cisco's Zero Trust Platform



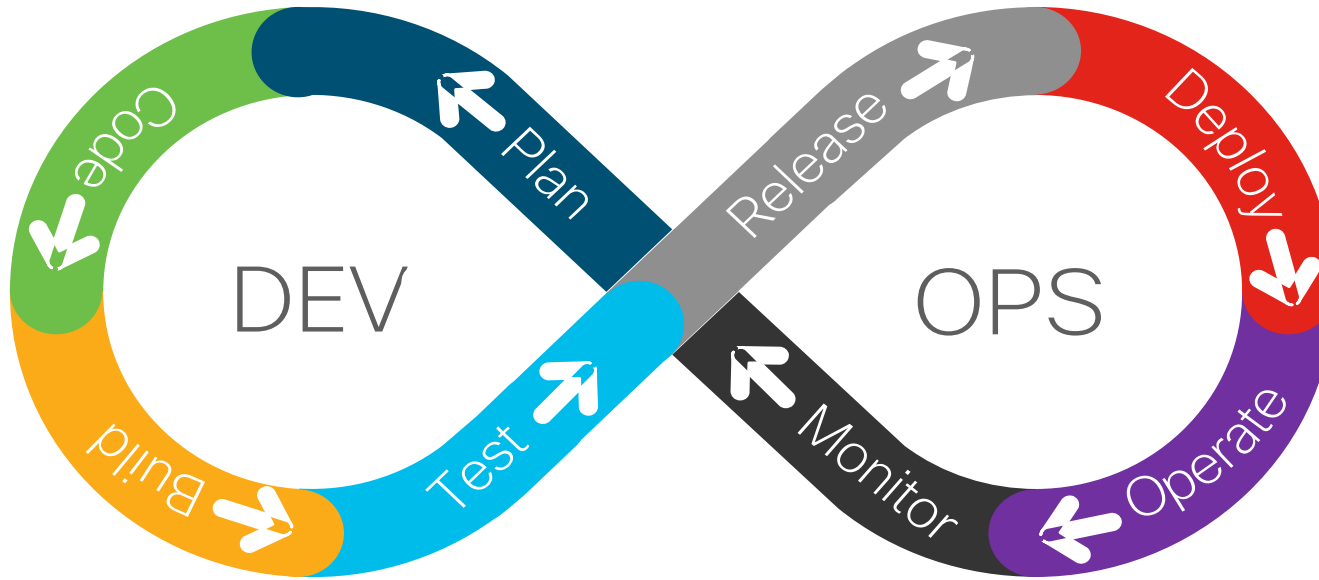
Conclusion

Key Takeaways



Security can be
an enabler

Cloud Native Apps: an Opportunity for Security



Key Takeaways

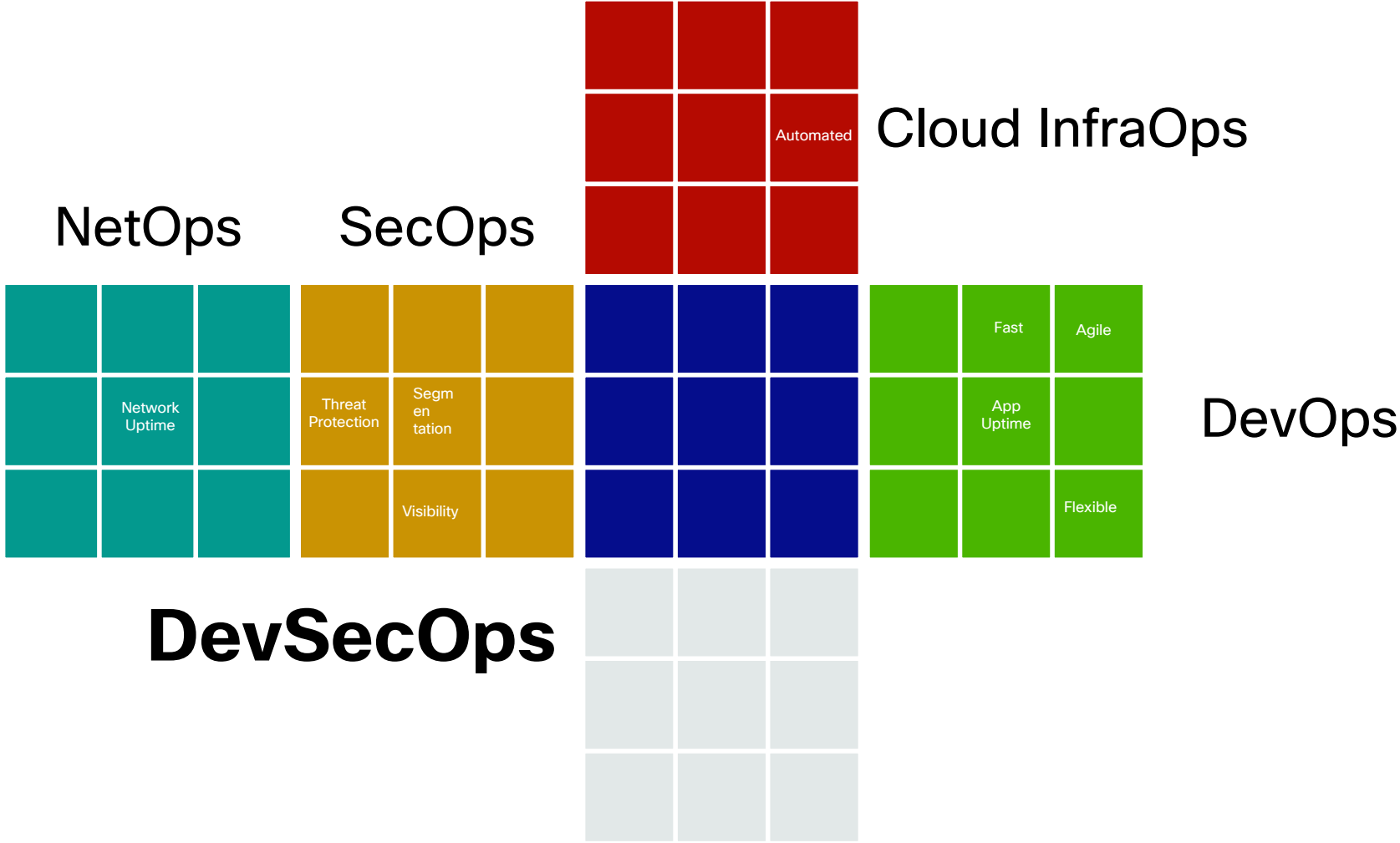


Security can be
an enabler



How devops and
secops teams can
better work together

Cloud Security use cases



Bringing Worlds Together



DevSecOps

Entry Point	 <p>Start from the left by integrating into dev toolchain</p>	 <p>Start from the right with runtime protection</p>
Stakeholders	CIO and the DevOps team	CISO and the security teams

Key Takeaways



Security can be
an enabler



How devops and
secops teams can
better work together



Multiple paths to
securing Cloud &
Apps



Cisco can help with
this Journey

Complete your session evaluations



Complete a minimum of 4 session surveys and the Overall Event Survey to claim a Cisco Live T-Shirt.



Earn up to 800 points by completing all surveys and climb the Cisco Live Challenge leaderboard.



Level up and earn exclusive prizes!



Complete your surveys in the Cisco Live Events app.

Continue your education



Visit the Cisco Stand for related demos



Book your one-on-one Meet the Expert meeting



Attend the interactive education with Capture the Flag, and Walk-in Labs



Visit the On-Demand Library for more sessions at www.CiscoLive.com/on-demand

Thank you

CISCO Live !

