illumio

Re-Thinking Cybersecurity

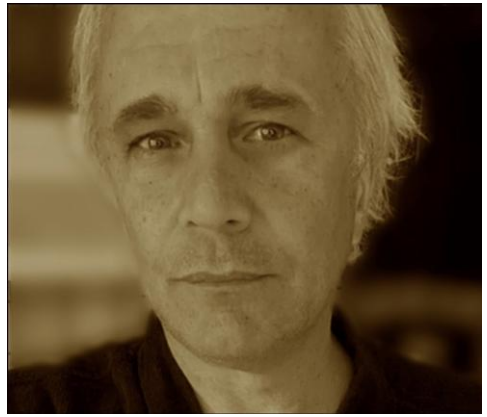
Christer Swartz
Director, Industry Solutions
Illumio

My Background

- I was born at a small startup called Cisco: we had 50 employees, globally.
- I lived for some years in the Caribbean, networking the Bermuda Triangle.
- I lived here in Zurich and worked for Swisscom, designing their MPLS backbone.
- I worked for Netflix, when we created our Internet video-streaming service.
- I worked for Microsoft for some years, networking their global Data Centers.
- I worked for Nokia for some years in Berlin, Germany, evolving their global network.
- I worked for Palo Alto Networks for many years, trying to prevent security breaches.
- I now work for Illumio, where we assume a breach, and focus on surviving & isolating it.
  - The theme across that background has been: **Build it first, then secure it later.**
  - This is why security is a big challenge today: it was never a priority in the beginning.

Cisco

Now



Money spent on Cybersecurity in 2024, globally

$215 Billion

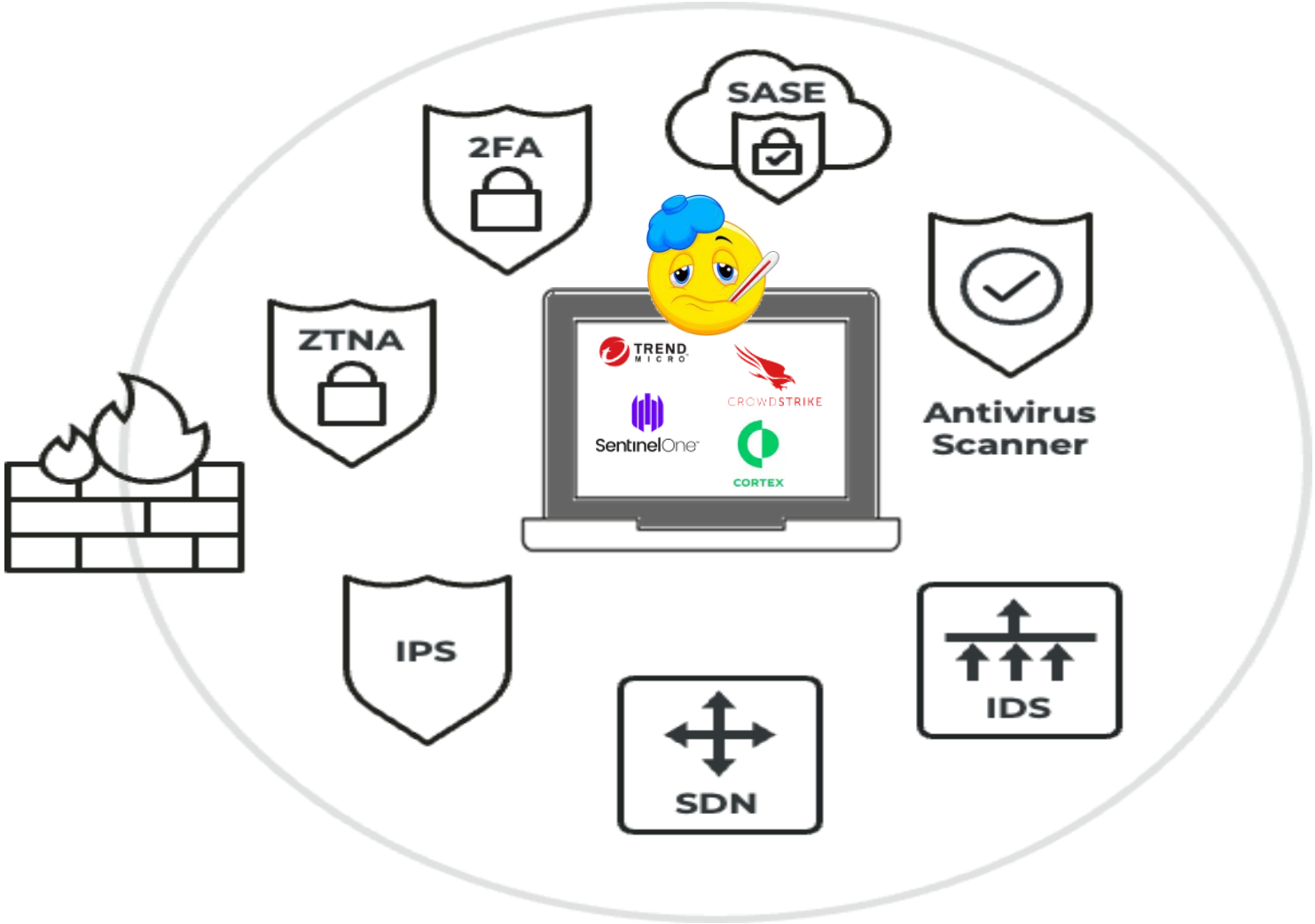
Global Cybersecurity incidents from 2023 to 2024:

Increase of 75%

Global Cybersecurity reported incidents, every day:

2,200

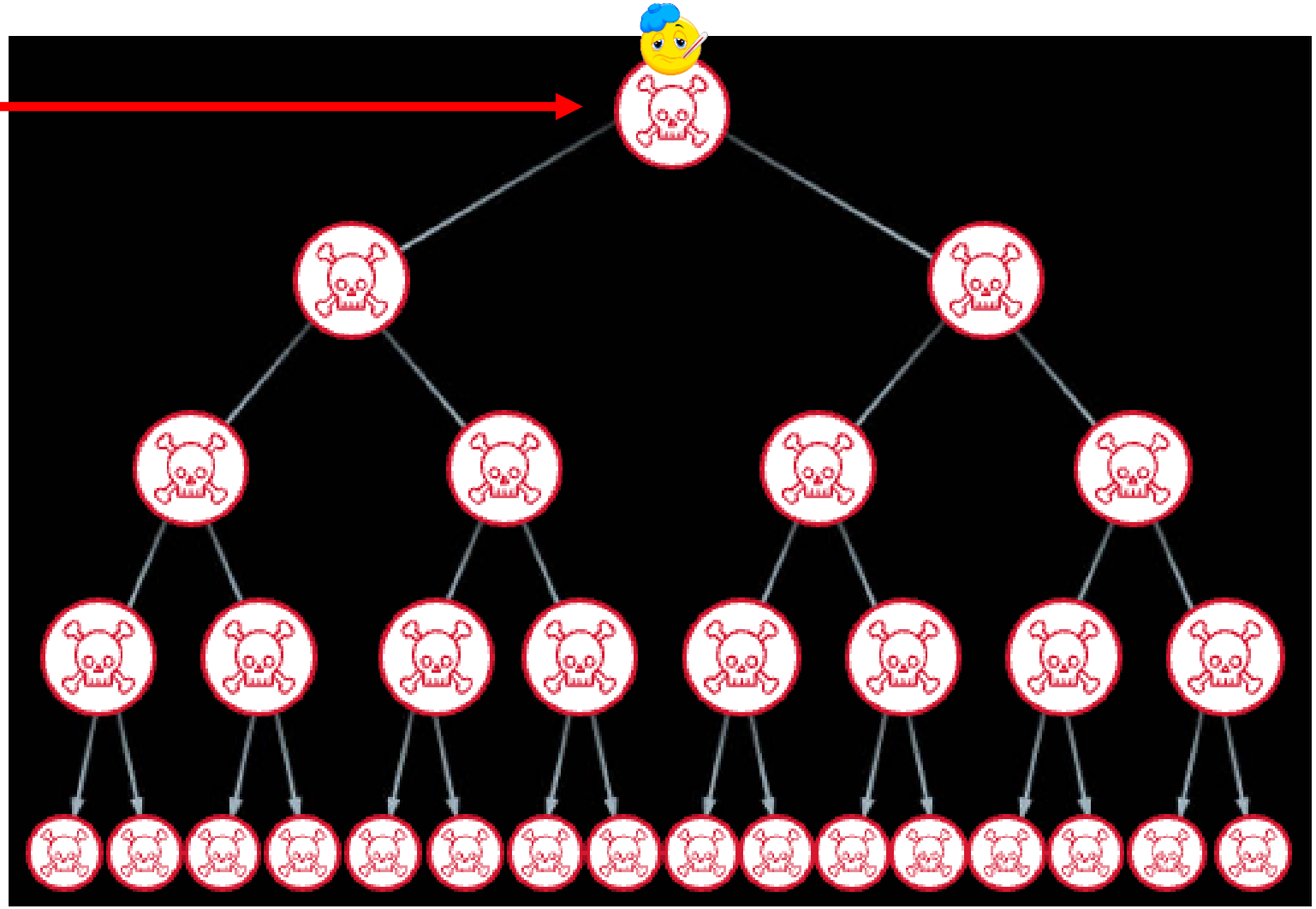
Current Approach: Protect the health of resources



Firewalls

Problem: By the time a threat is found, it has already spread

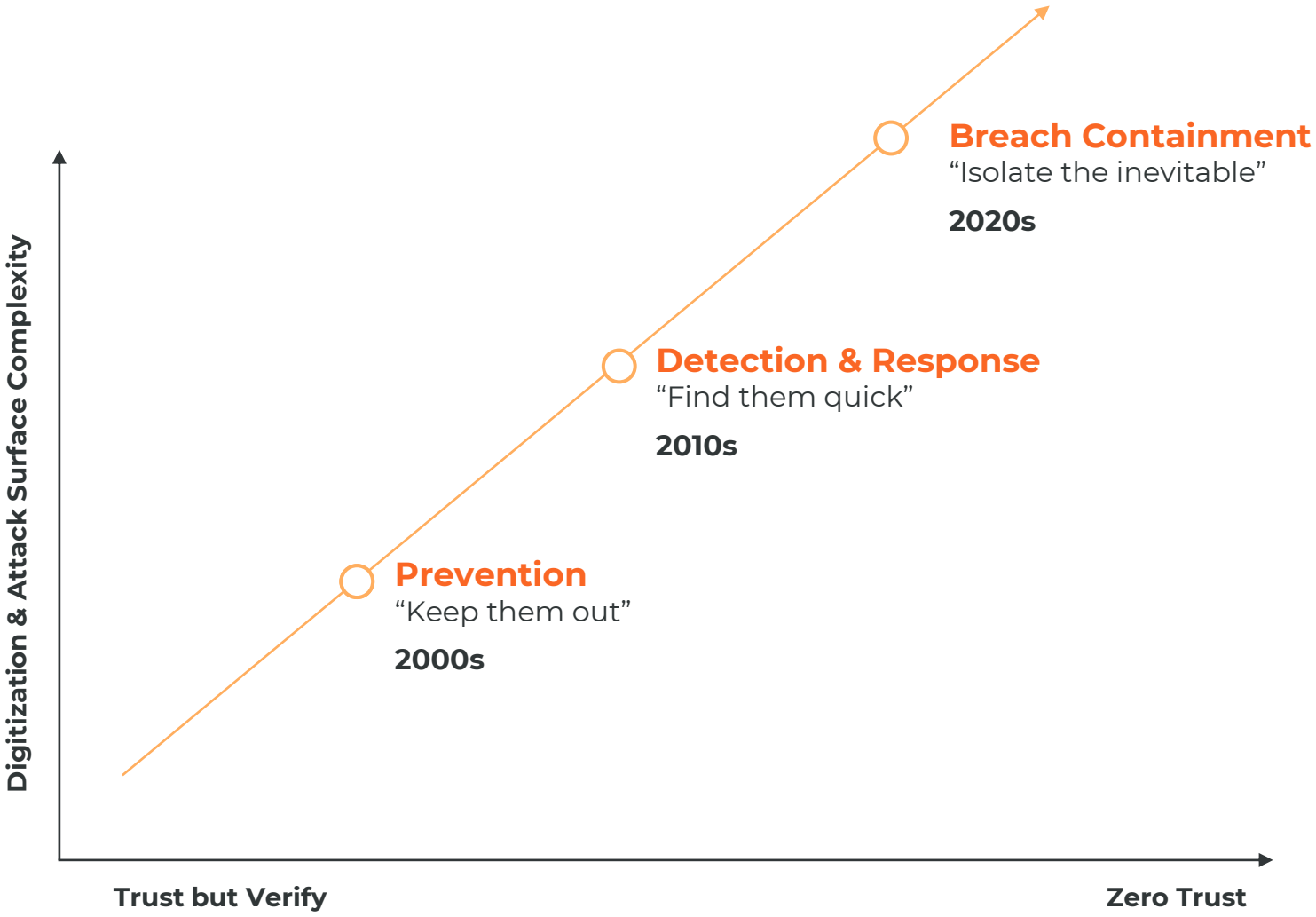
Threat-Hunting Tool Discovery



The 3 Security Mindsets

It's time to face reality:

100% of us will be breached.



illumio

All Threats have only 2 ways to move

#1: Humans: The weakest link in any security architecture.

Human behavior cannot be enforced.

No amount of training will prevent humans from clicking on links, and accidentally downloading threats.

#2: Open ports between workloads, in listen mode:

Your OS has many open ports, in listen-mode.

All threats use open ports to propagate across workloads.

- MacOS: 13 TCP ports open:

```
christer.swartz@KQHQ9YKG6R ~ % lsof -PiTCP -sTCP:LISTEN
COMMAND     PID            USER   FD   TYPE             DEVICE SIZE/OFF NODE NAME
rapportd    625 christer.swartz    3u   IPv4 0x4fe82624610fc935      0t0  TCP *:55342 (LISTEN)
rapportd    625 christer.swartz    4u   IPv6 0x4fe8262462689cdd      0t0  TCP *:55342 (LISTEN)
ControlCe   664 christer.swartz   17u   IPv4 0x4fe82624611393c5      0t0  TCP *:7000 (LISTEN)
ControlCe   664 christer.swartz   18u   IPv6 0x4fe82624610b815d      0t0  TCP *:7000 (LISTEN)
ControlCe   664 christer.swartz   19u   IPv4 0x4fe8262461139e55      0t0  TCP *:5000 (LISTEN)
ControlCe   664 christer.swartz   20u   IPv6 0x4fe82624610b883d      0t0  TCP *:5000 (LISTEN)
inSync     1248 christer.swartz   10u   IPv4 0x4fe82624627f1e55      0t0  TCP localhost:7010 (LISTEN)
inSync     1248 christer.swartz   19u   IPv4 0x4fe826246278f415      0t0  TCP localhost:50788 (LISTEN)
inSync     1248 christer.swartz   23u   IPv4 0x4fe82624628d7ea5      0t0  TCP localhost:50793 (LISTEN)
inSyncUpg  1249 christer.swartz    7u   IPv4 0x4fe826246250fea5      0t0  TCP localhost:50110 (LISTEN)
figma_age  1265 christer.swartz    3u   IPv4 0x4fe826246112a985      0t0  TCP localhost:44960 (LISTEN)
figma_age  1265 christer.swartz   10u   IPv4 0x4fe826246112b415      0t0  TCP localhost:44950 (LISTEN)
Microsoft 88950 christer.swartz   15u   IPv6 0x4fe82624610b65dd      0t0  TCP localhost:42050 (LISTEN)
```

- CentOS Linux: 13 TCP ports open.

- Windows 10 has 10 TCP ports open.

All threats share one thing in common:
They all want to spread.

All malware uses open ports to spread its payload to neighboring workloads.
This is true for the most sophisticated hacker, and for the curious teenager.

Sophisticated AI-generated Ransomware

State-sponsored threat-actor

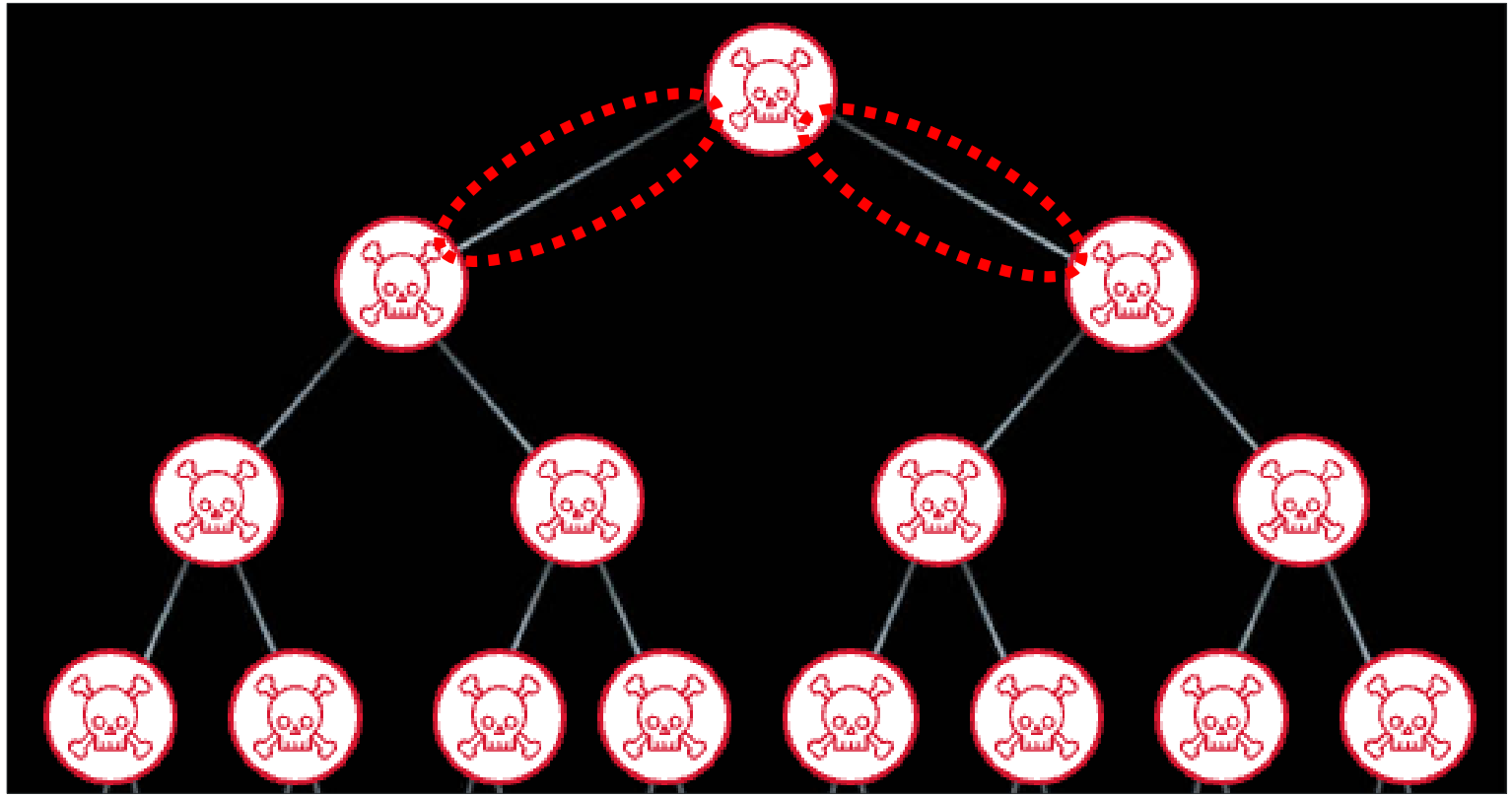
Simple Non-AI Ransomware

Opportunistic teenager (my son)

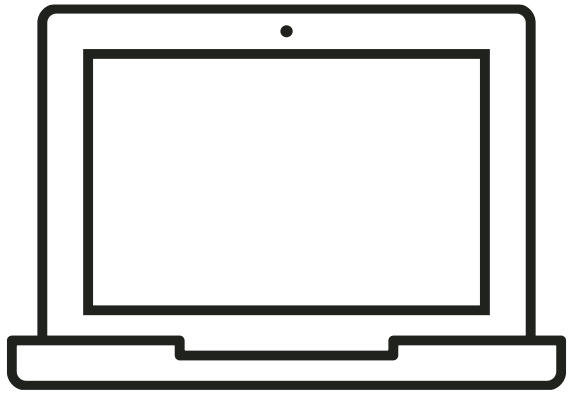
What is more critical? The Workload or the Segment?

100% of threats rely on the Segment to spread. Zero Trust needs to begin at the Segment.

This includes the upcoming AI-generated apocalypse that everyone is afraid of.



Threats can be detected via monitoring Segment behavior



Open DNS port. Base-line behavior:

~ 500 bytes per query.
- Sporadic.
- Activity during expected hours.

Open HTTPS port. Base-line behavior:

~ Asymmetric.
- Sporadic.
- KB outbound, MB inbound.

Example of abnormal behavior:

- 10 Gig of sustained traffic outbound over either port.
- Destination to known malicious IP's.
- Activity during idle hours.

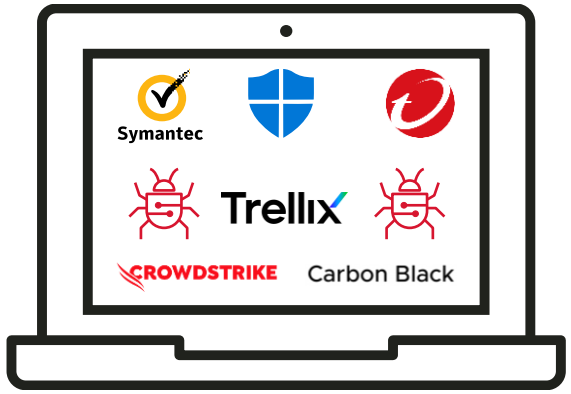
We know this is a problem, without waiting for a threat-hunting tool to detect it.
We can take action immediately.

Security has 2 distinct options

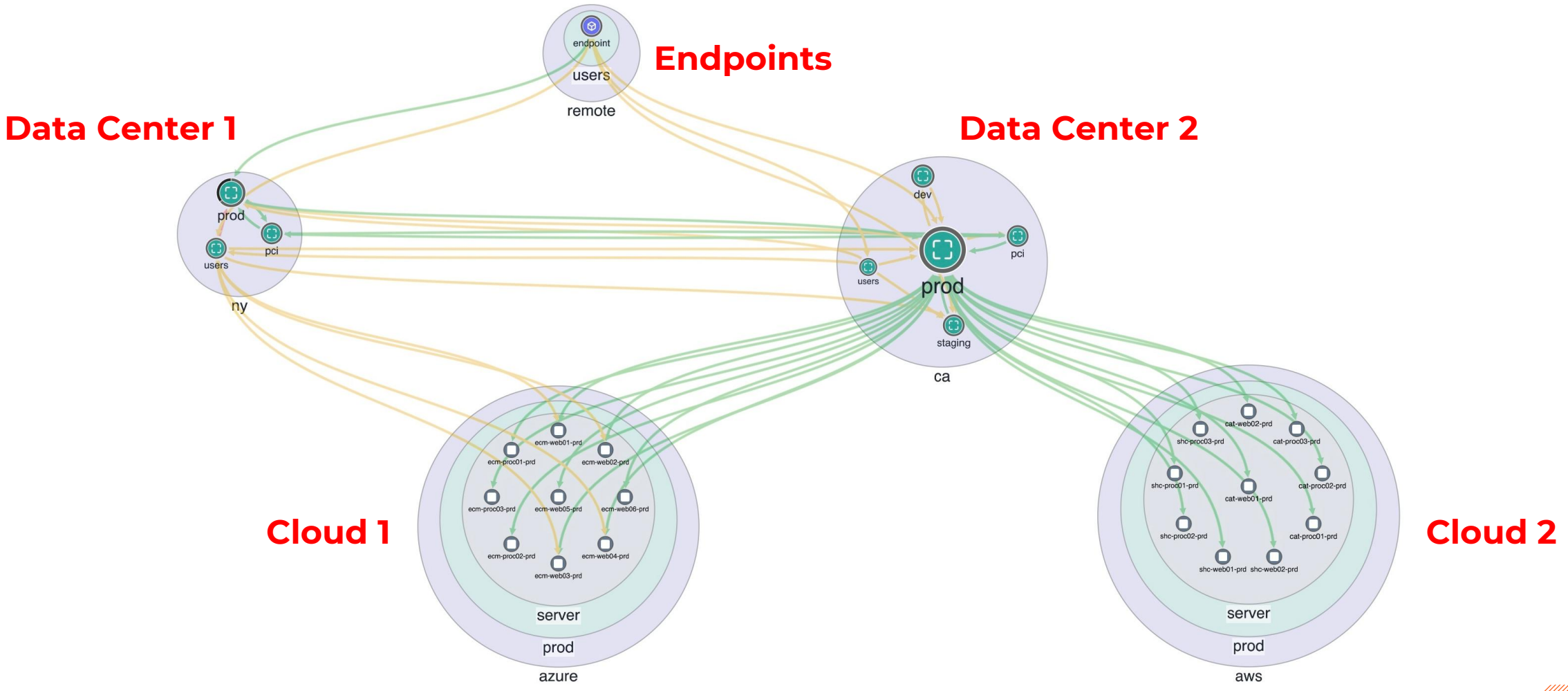
Protect the Workload?

or...

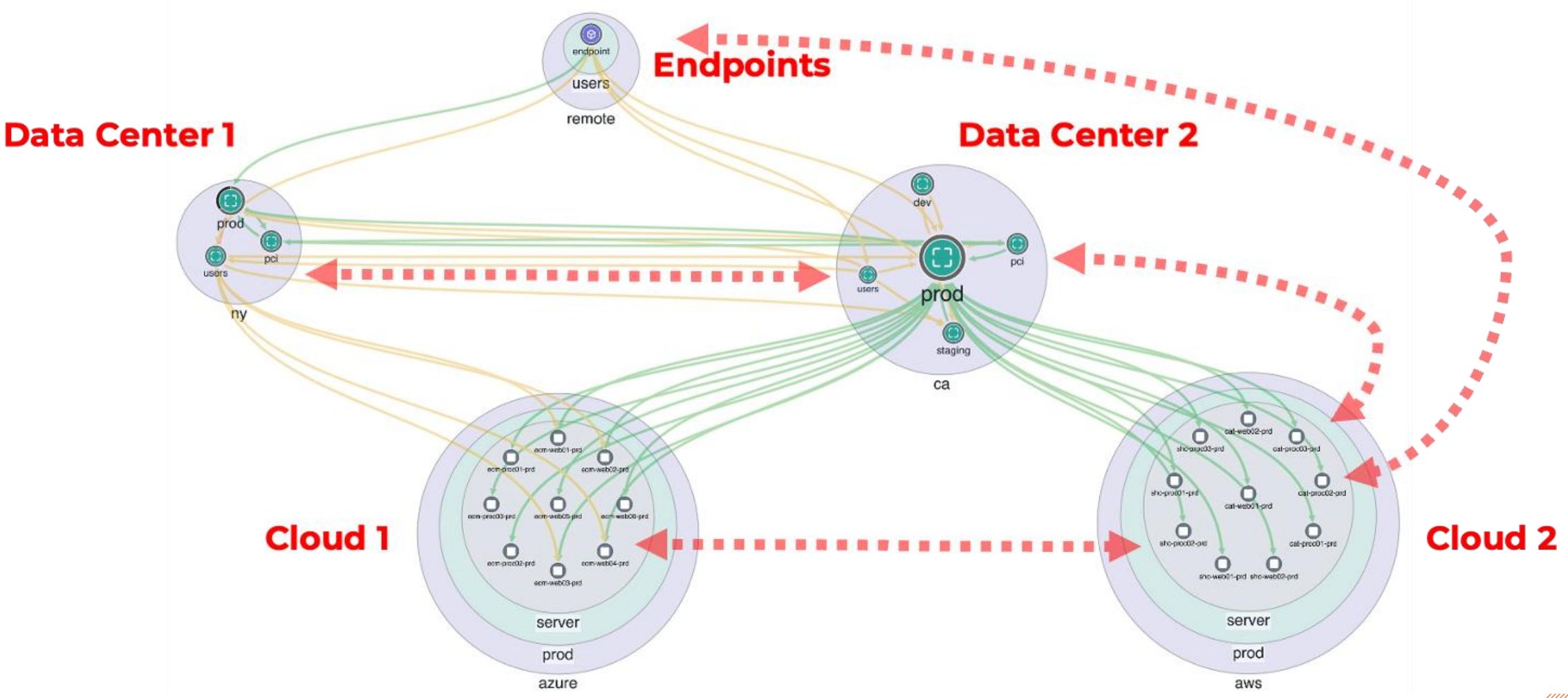
Sacrifice the Workload?



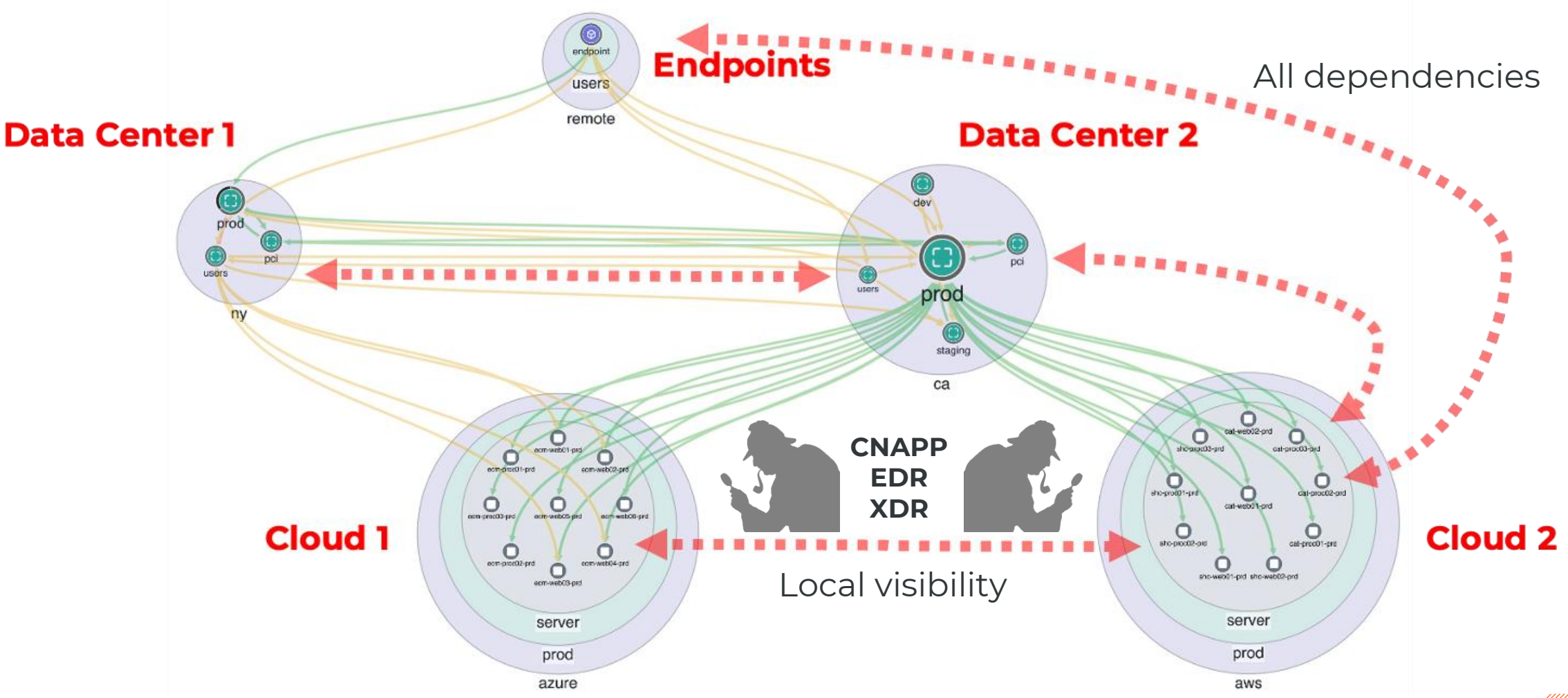
Visibility, into everywhere your data can live



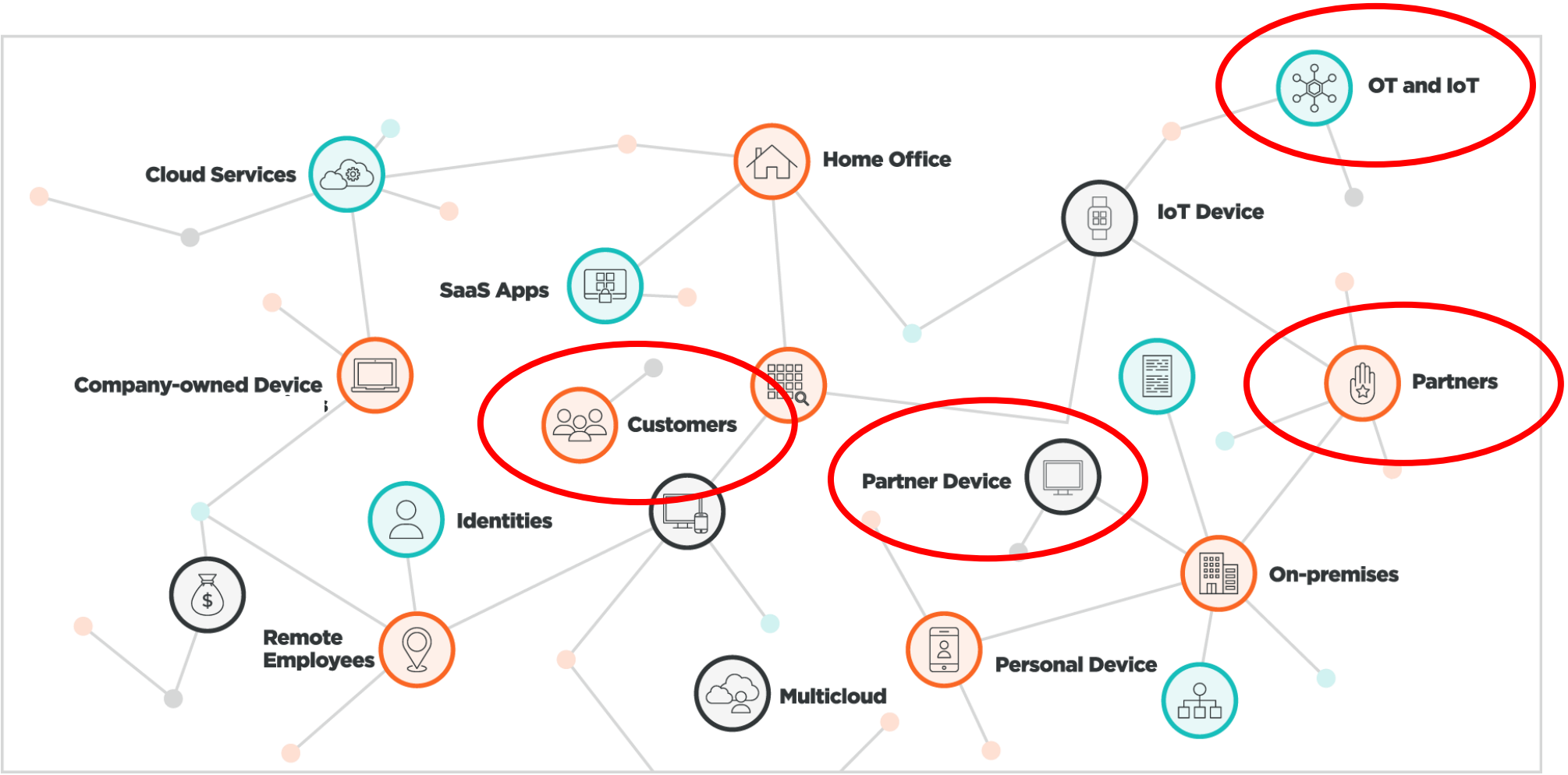
Visibility of all application dependencies, everywhere



CNAPP: Cloud visibility, but not Data Center or Endpoint

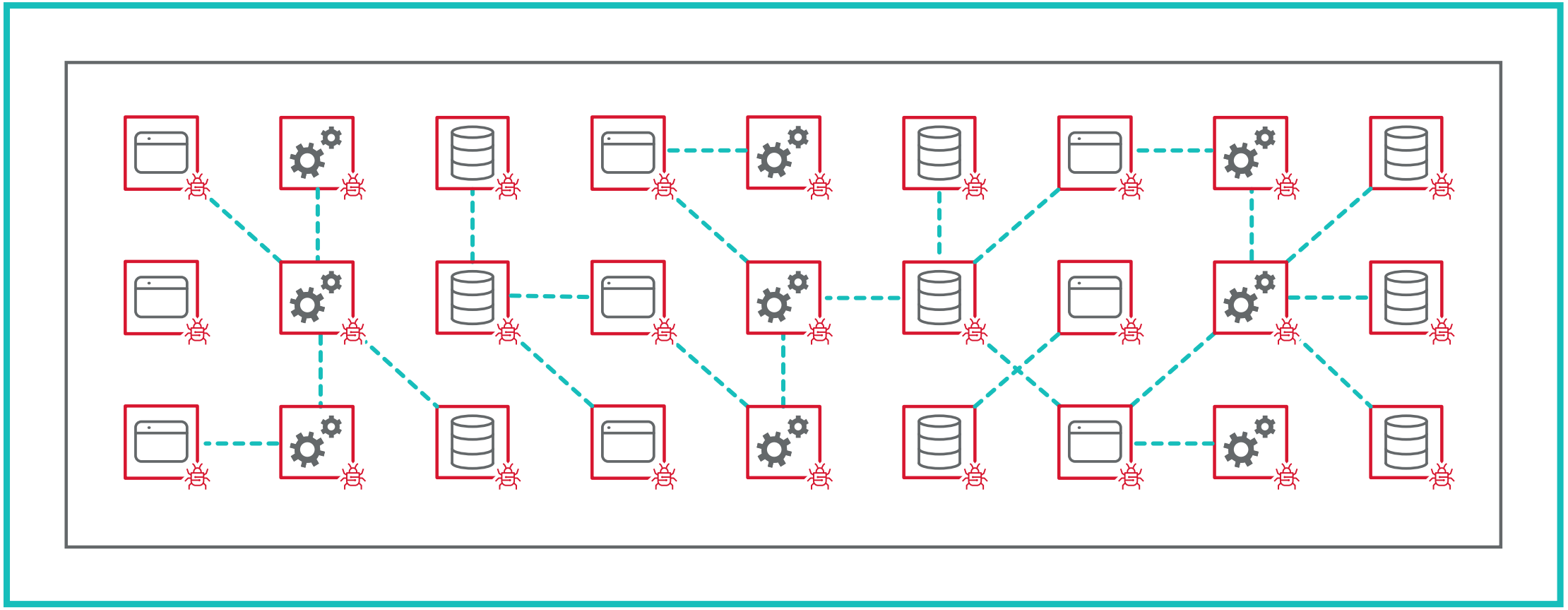


Reality Check: Not all entry points are under your control

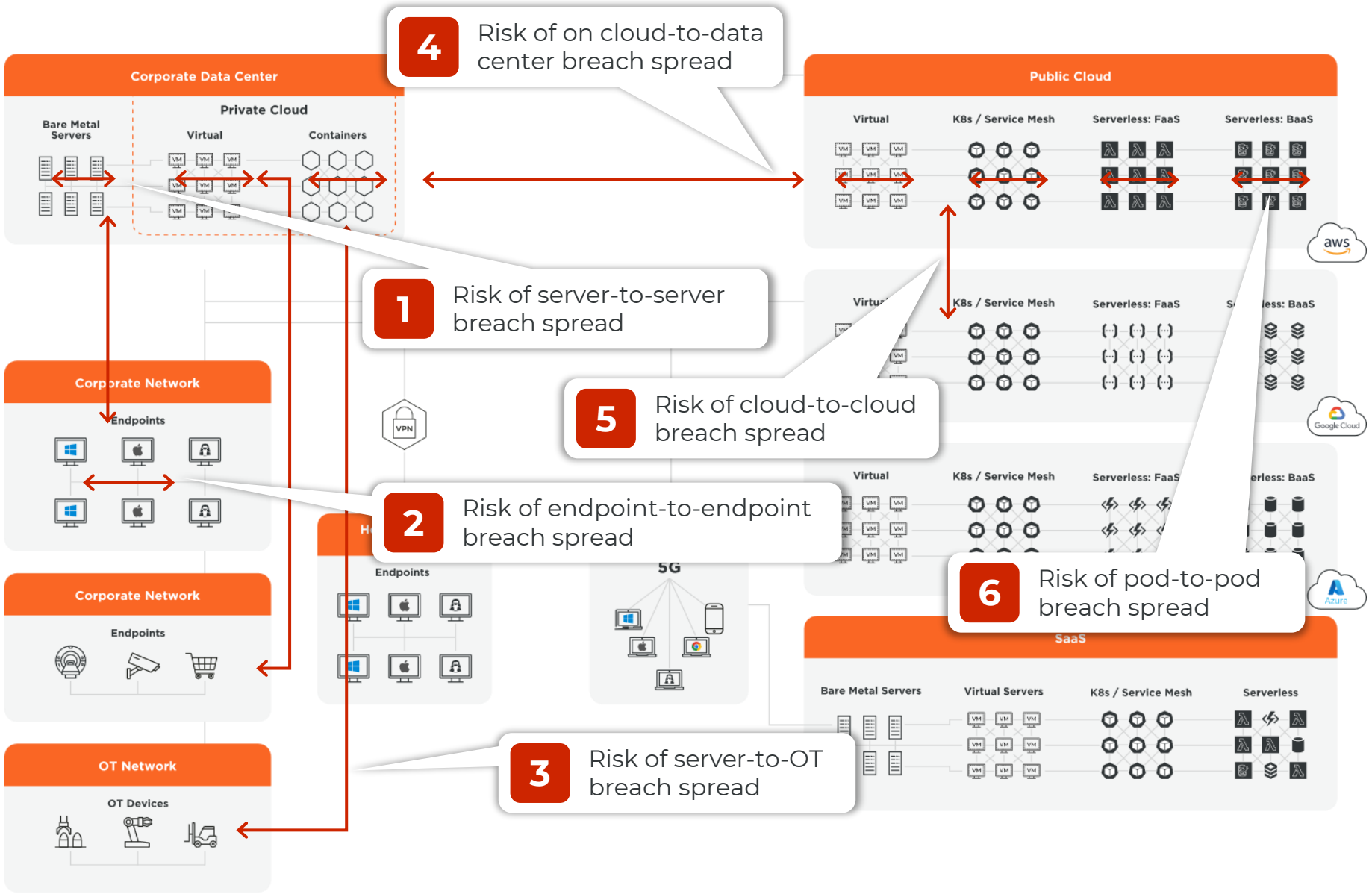


Open ports, in listening mode, are like unlocked doors

Examples: RDP, SMB, SSH, DNS, NetBIOS, LDAP



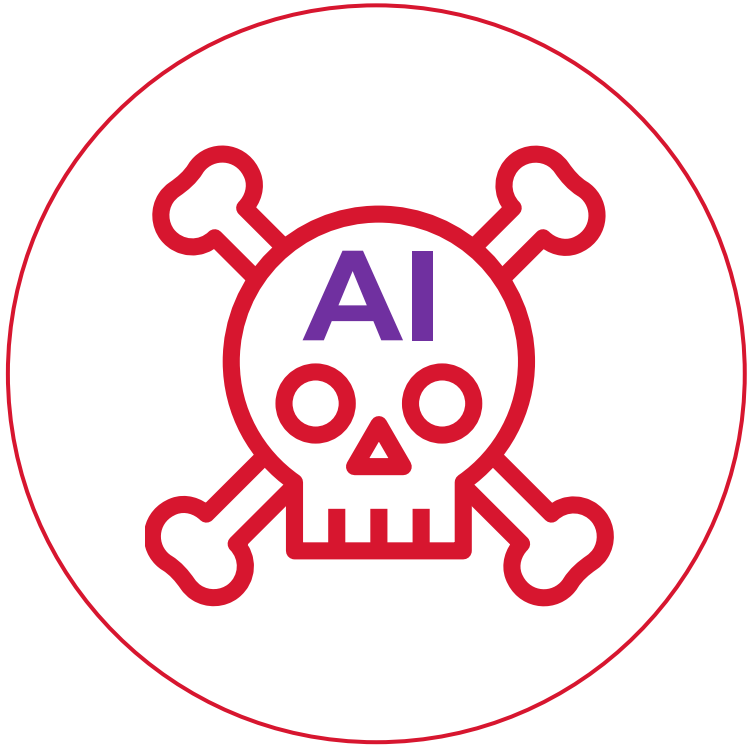
With limited visibility, threat actors have many entry points to choose from.



Future-Proof against AI-Generated Malware

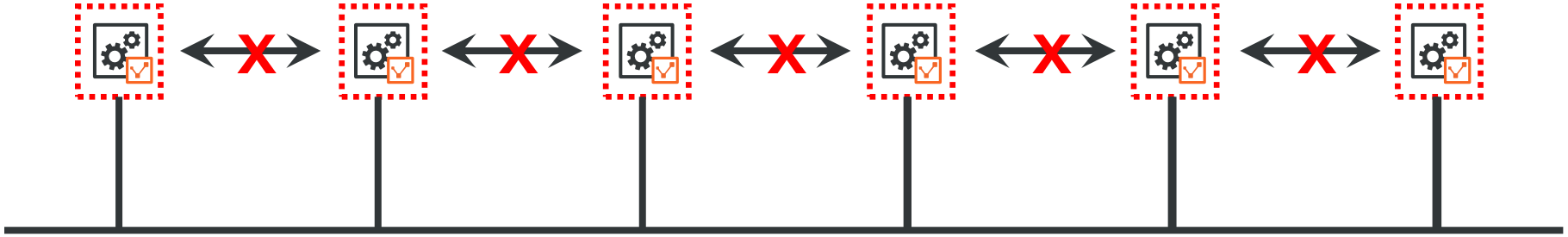
We can predict one detail of all current & future threats with confidence**:**

It will want to spread.



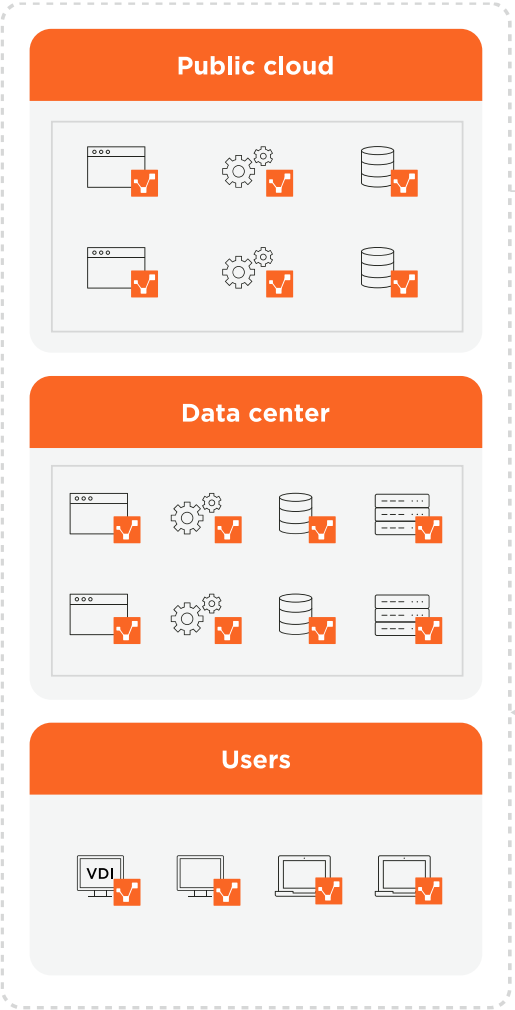
Zero Trust = Every workload a dedicated trust-boundary

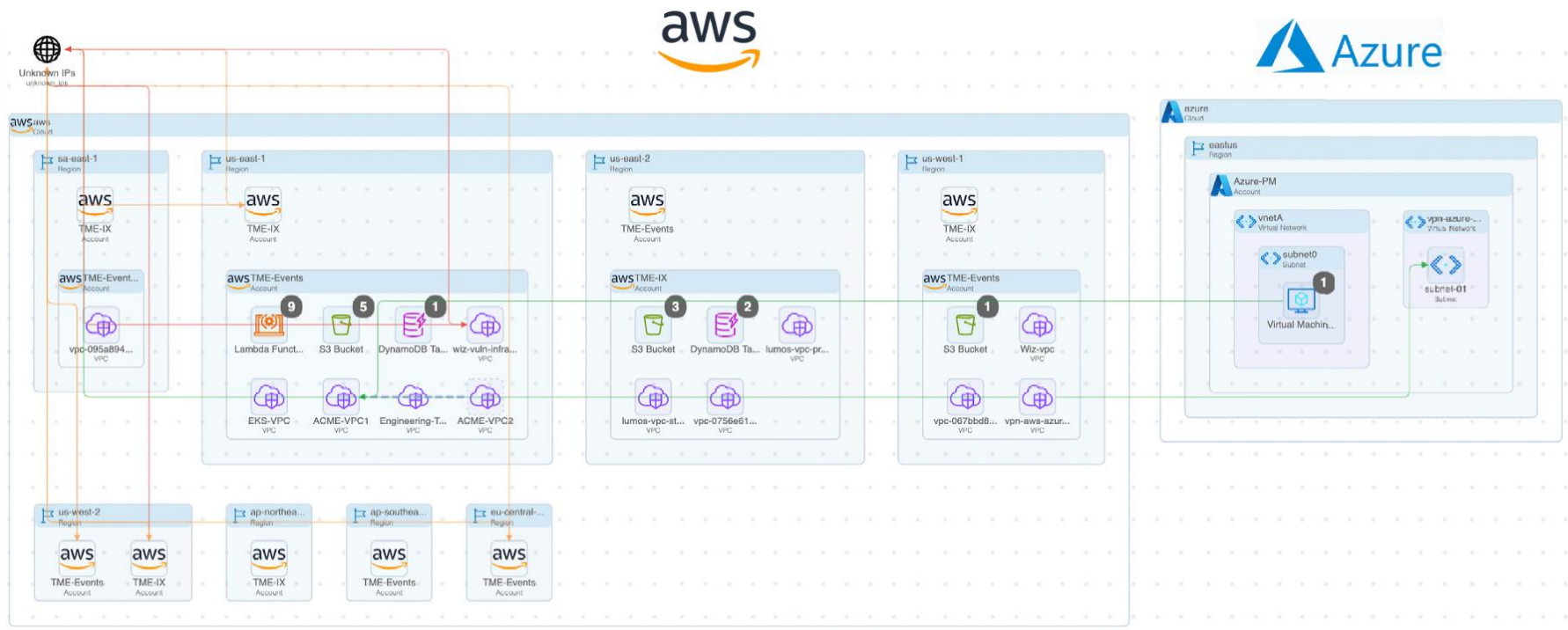
Every workload is a segment, even on a flat network.



Flat Network

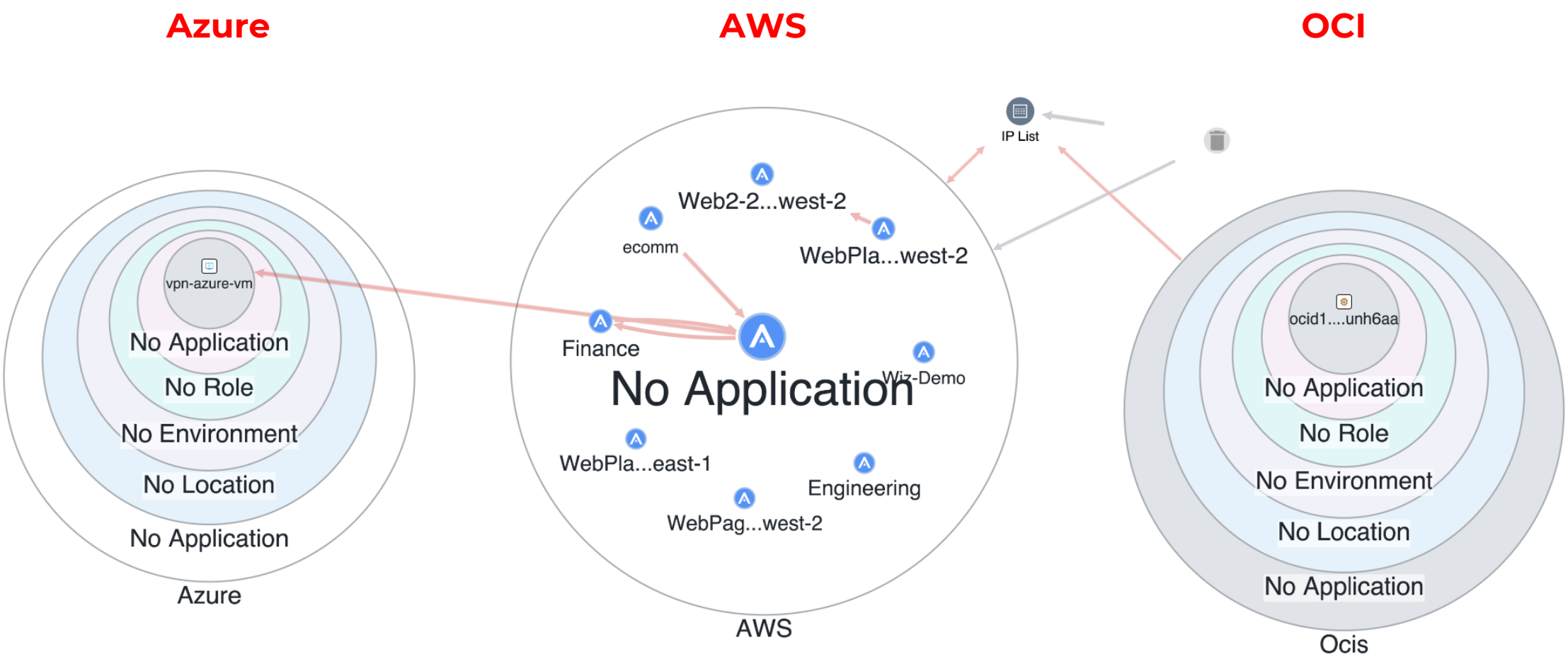
Visibility: Everywhere your Data can live





illumio

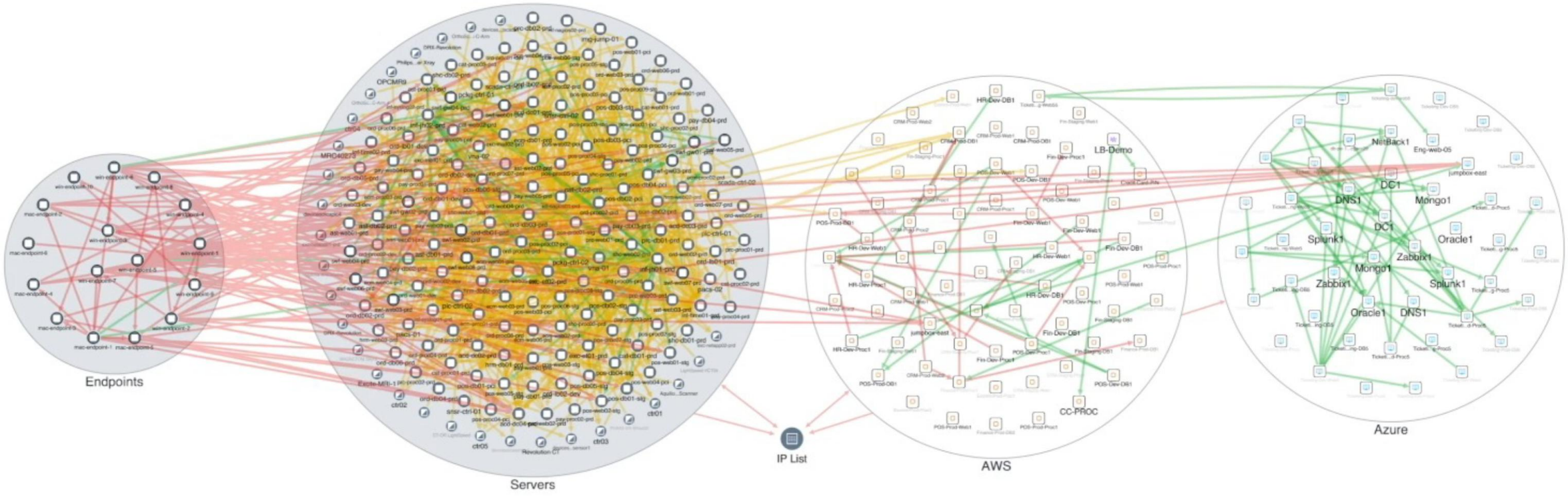
Visibility within and between Clouds, agnostic to Cloud-native tools



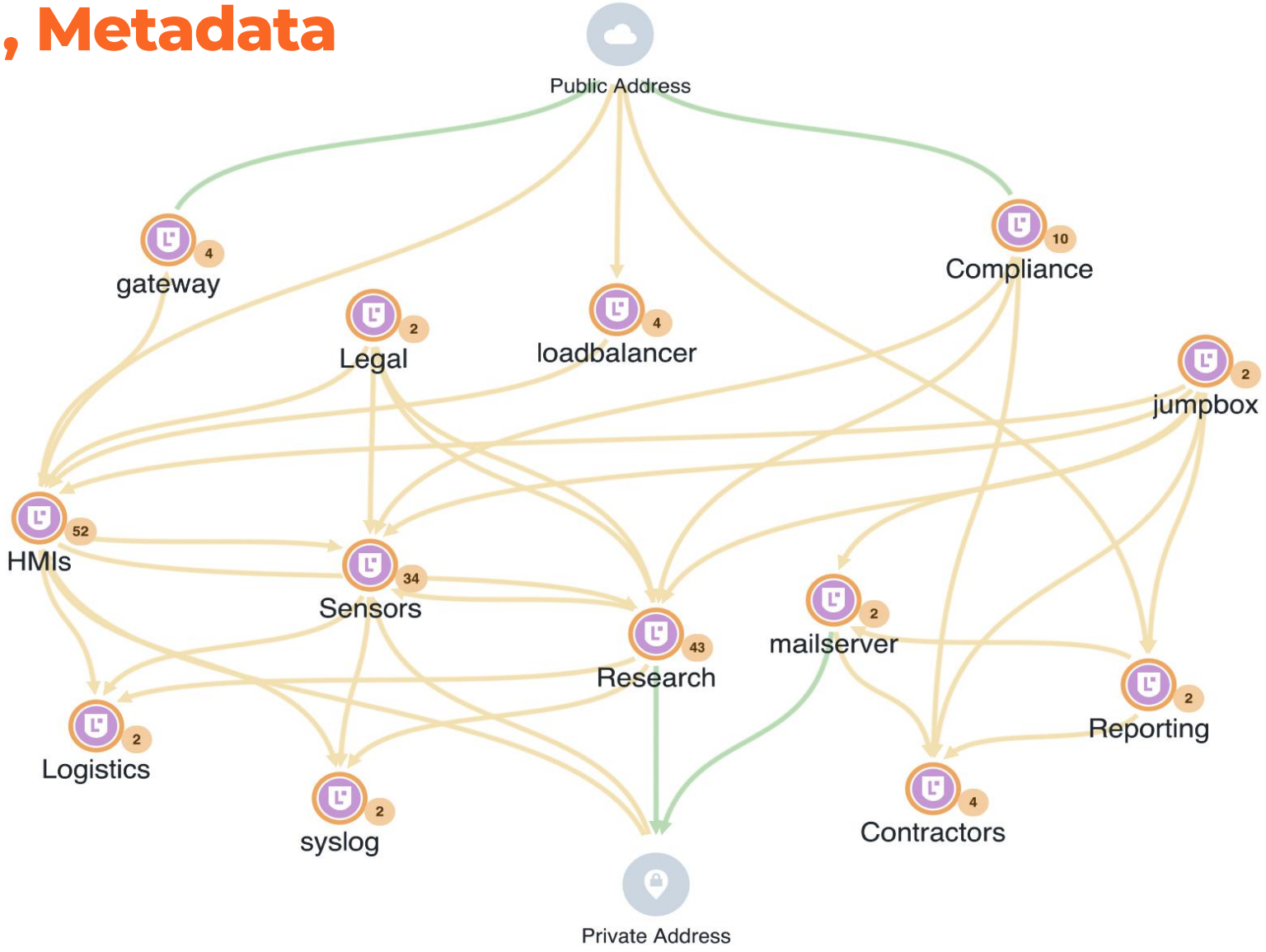
illumio

100% visibility, with *no dependency on security appliances*

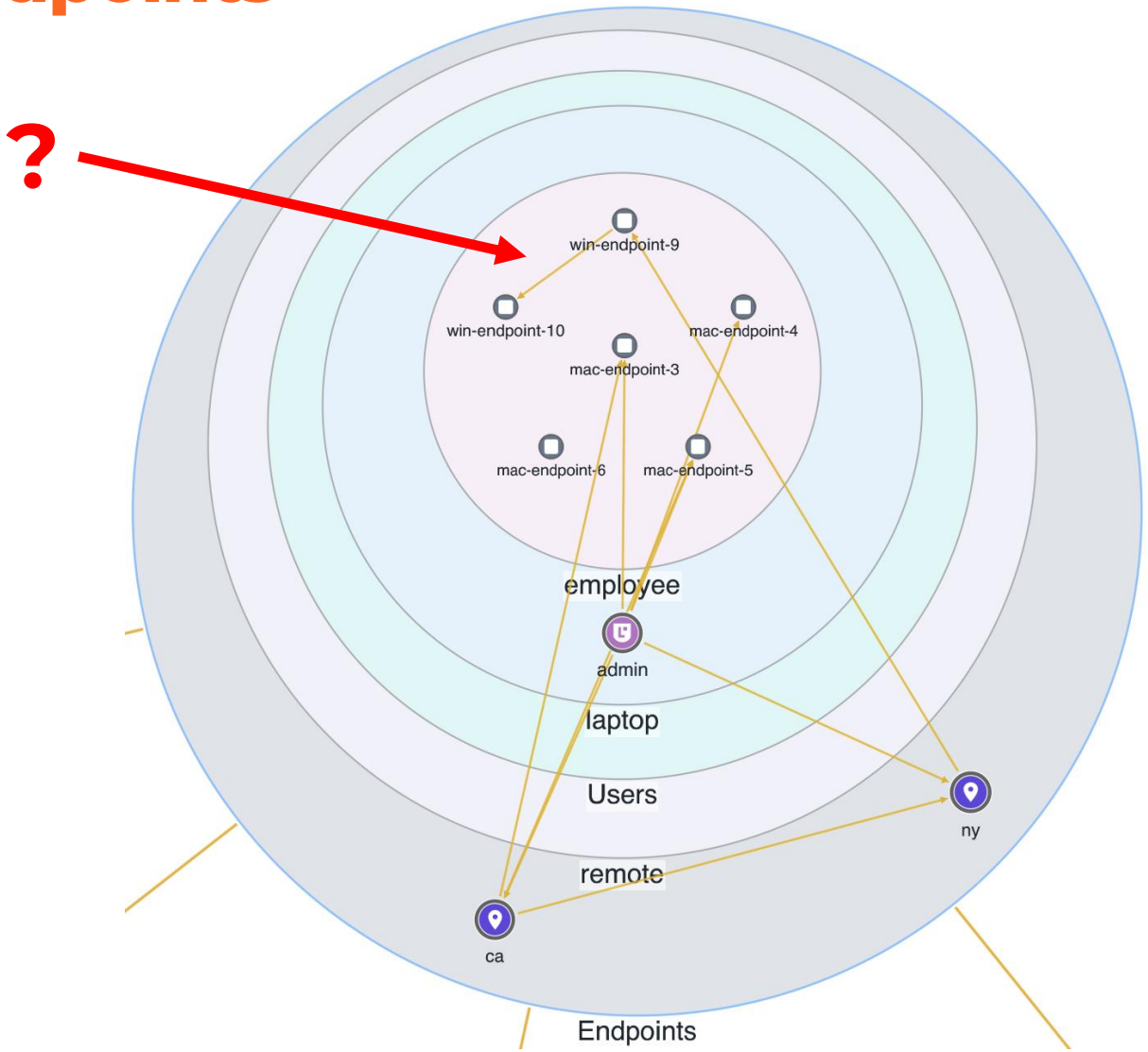
Endpoints **Data Center** **AWS** **Azure**



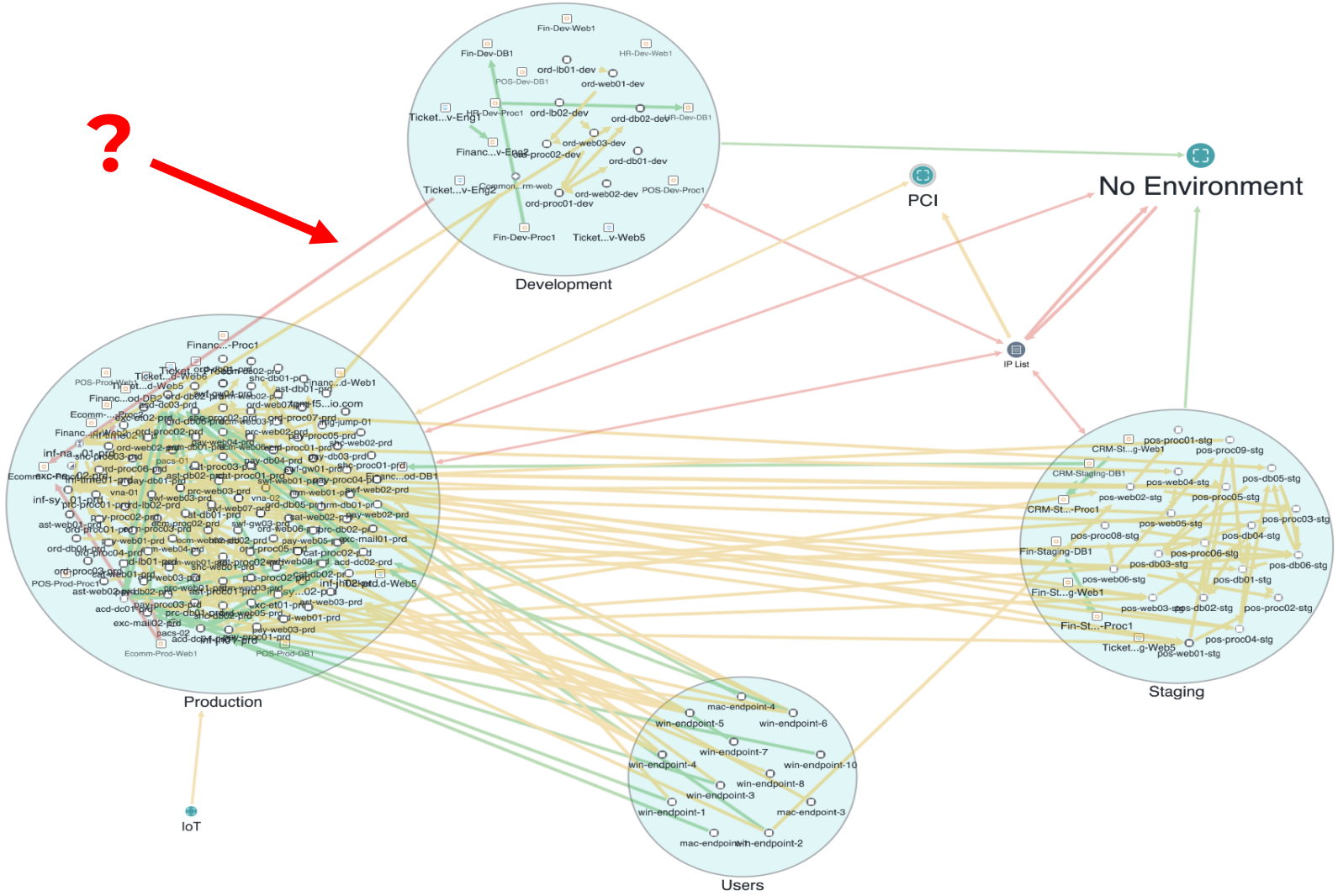
Labeling, Metadata



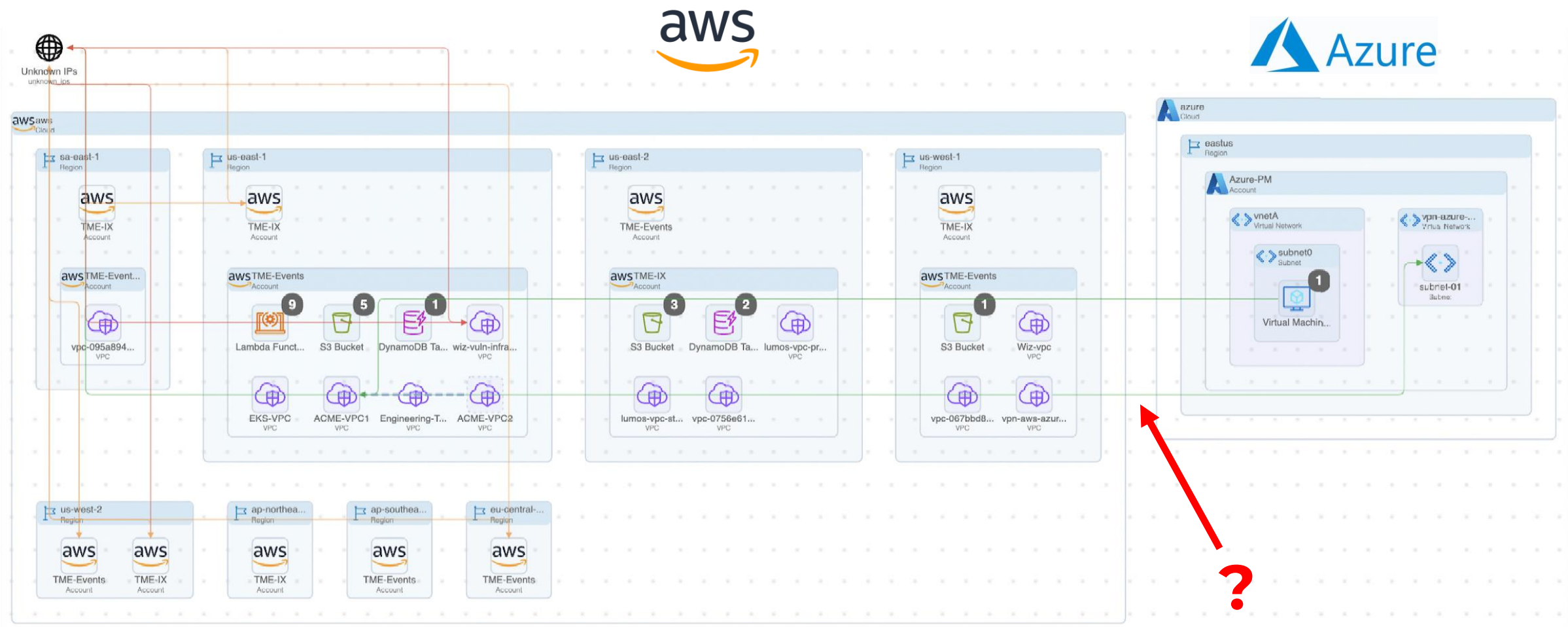
Visibility: Endpoints



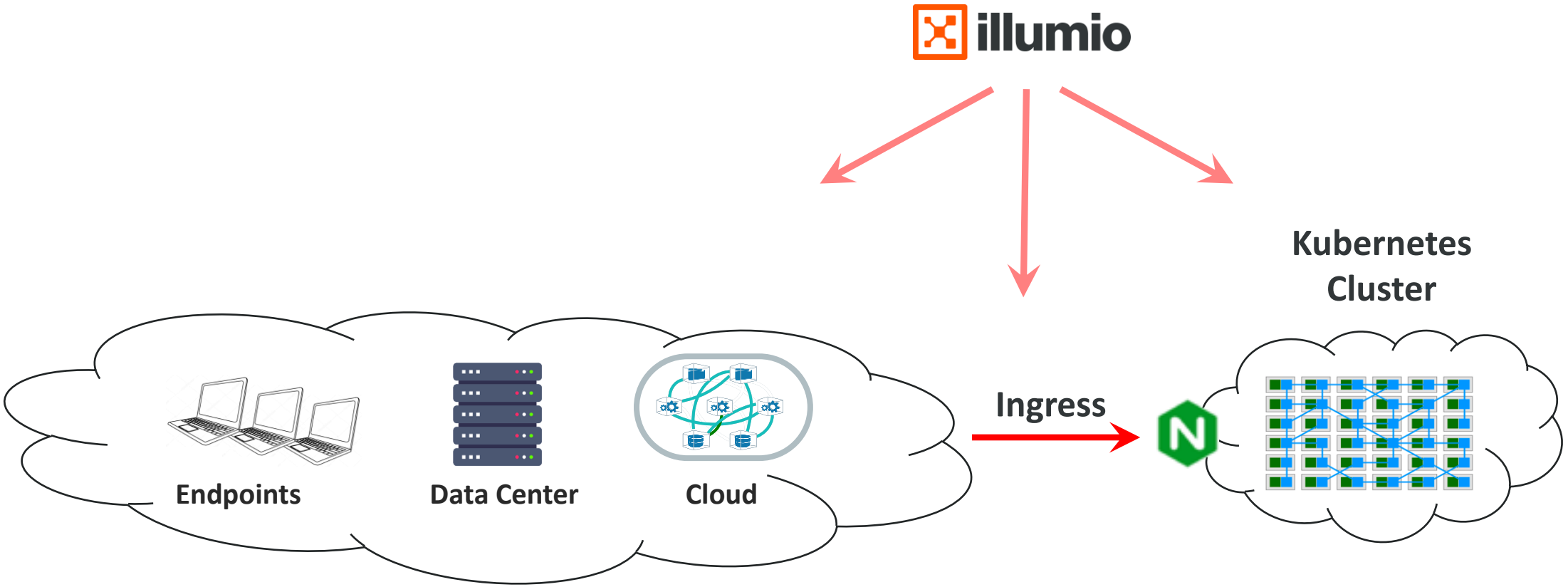
Visibility: Data Center



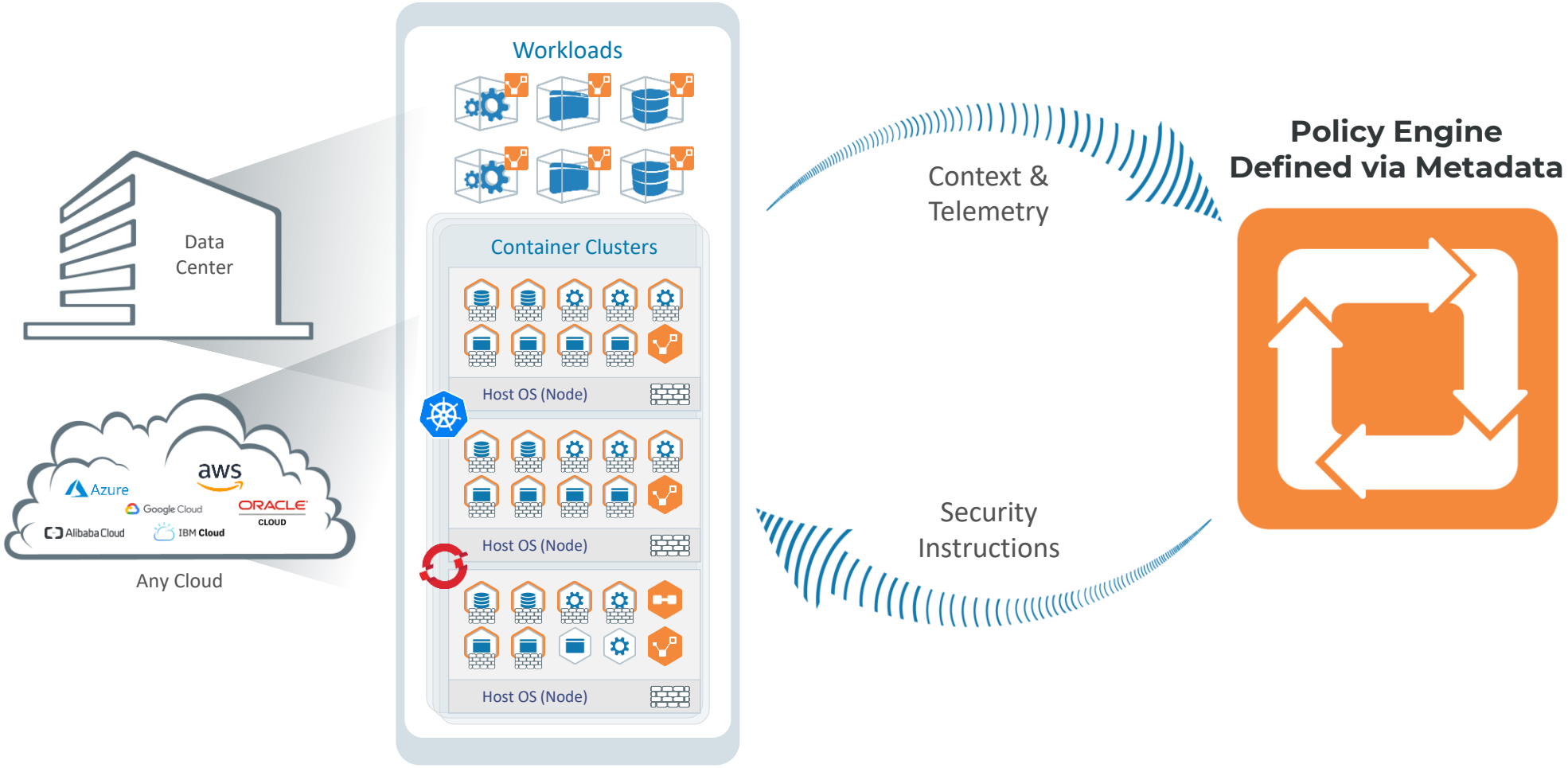
Visibility: Cloud



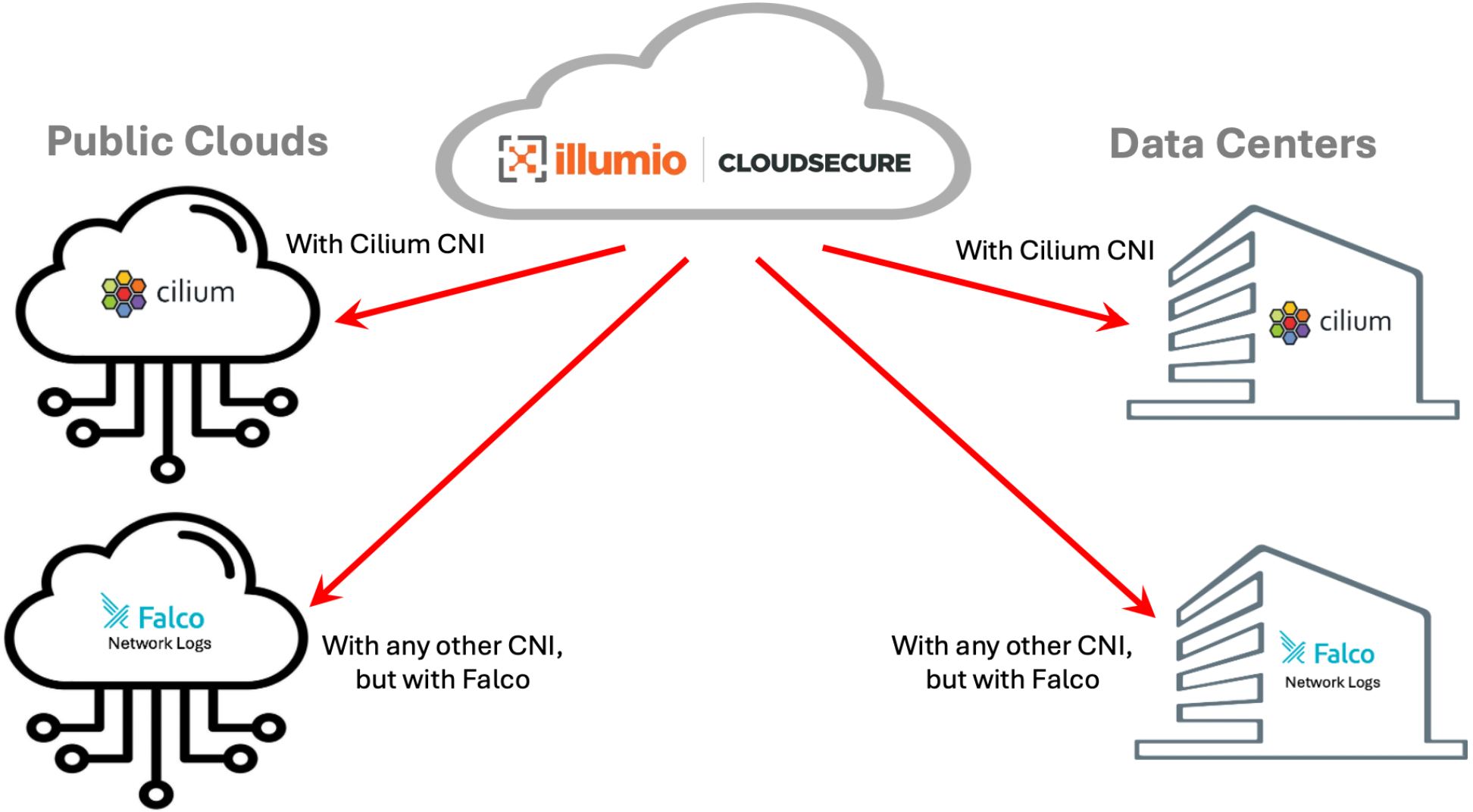
Kubernetes: Seeing traffic that rarely touches the wire



Kubernetes: Agent-based



Kubernetes: Agentless



AI vs. AI

AI-threats require AI-security tools, since AI is faster than any human can respond.

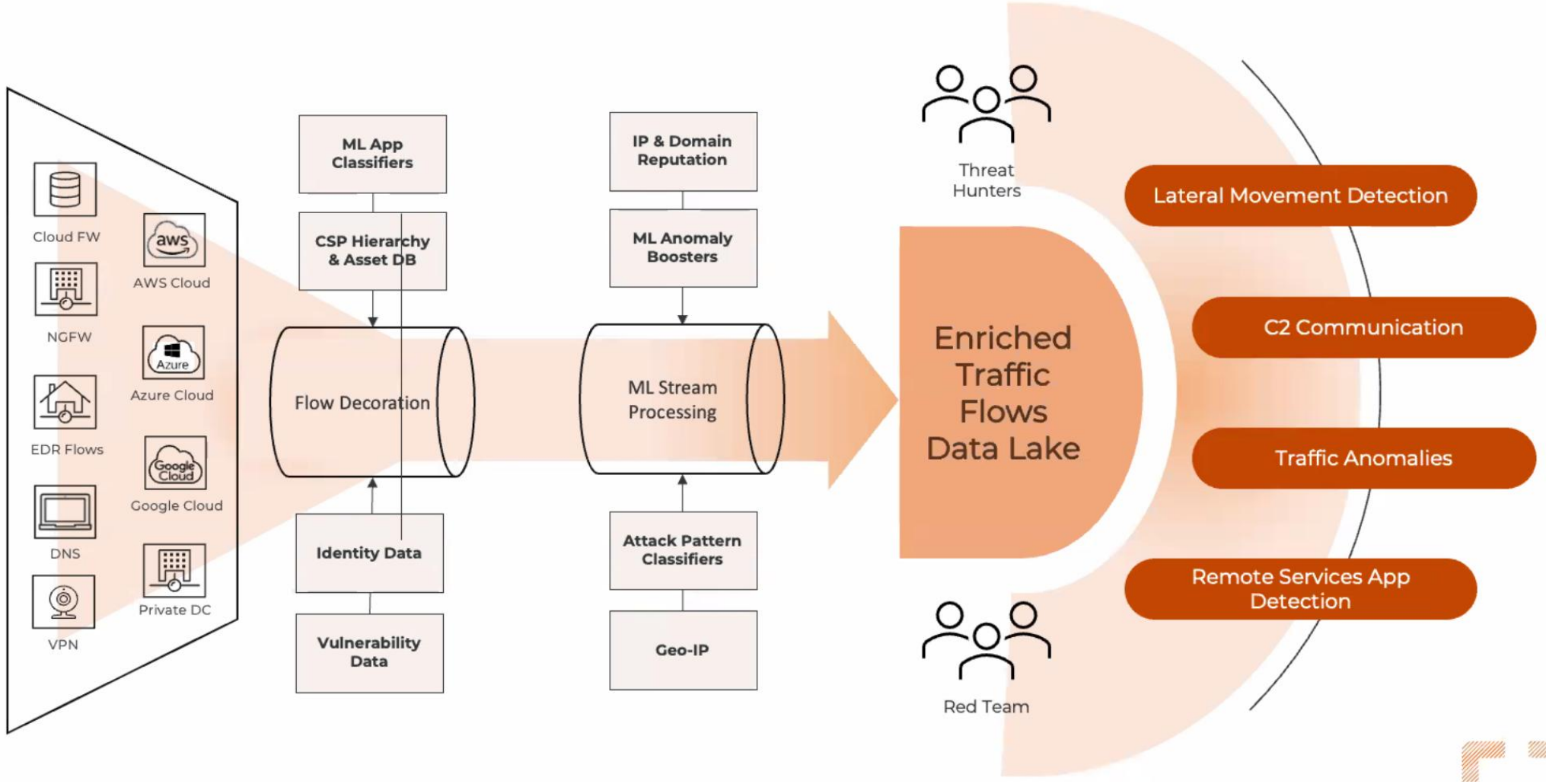
- **Illumio uses AI Tools to automate visibility:**

  - AI Labeling: Auto-label workloads based on traffic patterns observed.
  - Virtual Assistant:: AI interface to ask & respond to natural-language queries.

- **Automation tools, for instant Policy changes:**

  - Threat-hunting tools, such as Wiz, will notify Illumio of compromised workloads, *even if they have not yet begun to spread*.
  - Vulnerability Scanners, such as Tenable, will notify Illumio of at-risk ports used by Zero Day malware.
  - SOAR platforms such as Splunk & Palo Alto Cortex can automate Illumio Policy changes, without human action.
  - Illumio integrates with ZTNA platforms, such as Netskope, to dynamically notify them of workload label changes.

AI/ML Enabled Data Lake



A security Data Lake can surface trends that are hard to find

Datacenter Traffic
Datacenter Traffic to Risky Ports
Last Synced:
13 seconds ago

Cloud Configurations
Internet Exposed EC2 Instances
Last Synced:
3 minutes ago

External Talkers
Azure Tenant to AWS External IP Traffic
Last Synced:
26 minutes ago

Cloud Configurations
Traffic Blindspots
Last Synced:
3 minutes ago

Cross Talkers
Cross Cloud Traffic
Last Synced:
26 minutes ago

External Talkers
Region to Malicious IP Traffic
Last Synced:
26 minutes ago

Cloud Configurations
Unprotected Resources
Last Synced:
3 minutes ago

External Talkers
Account to External Geo Traffic
Last Synced:
26 minutes ago

Example: Cross-Cloud Traffic

External Talkers
Account to External Cloud Traffic
Last Synced: 37 minutes ago

External Talkers
Tenant to External Cloud Traffic
Last Synced: 37 minutes ago

External Talkers
Azure Tenant to AWS External IP Traffic
Last Synced: 37 minutes ago

Cross Talkers
Cross Cloud Traffic
Last Synced: 37 minutes ago

Cross Talkers
Cross Region Traffic
Last Synced: 37 minutes ago

Cross Talkers
Cross Account Traffic
Last Synced: 37 minutes ago

Cross Talkers
Cross Tenant Traffic
Last Synced: 37 minutes ago

Cross Cloud Traffic from Last 24 hours: Jan 24, 2025, 17:36 - Jan 25, 2025, 17:36 compared to Previous period: Jan 23, 2025, 17:36 - Jan 24, 2025, 17:36

Export

Customize columns | 50 per page | 1 – 2 of 2 Total

Traffic Status	Source	Destination	Flows	Bytes
Allowed Traffic	AWS	Azure	72 ↓ 0%	1.23 MB ↓ 1.8%
Allowed Traffic	Azure	AWS	72 ↓ 0%	624.38 KB ↓ 0%

Example: Unprotected Resources

Talkers
Cloud Traffic
Synced:
minutes ago

Cross Talkers
Cross Region Traffic
Last Synced:
39 minutes ago

Cross Talkers
Cross Account Traffic
Last Synced:
39 minutes ago

Cross Talkers
Cross Tenant Traffic
Last Synced:
39 minutes ago

Cloud Configurations
Cross Talking Peering Connections
Last Synced:
3 minutes ago

Cloud Configurations
Traffic Blindspots
Last Synced:
3 minutes ago

Cloud Configurations
Unprotected Resources
Last Synced:
3 minutes ago

Cloud Configurations
Internet Exposed EC2 Instances
Last Synced:
3 minutes ago

Unprotected Resources

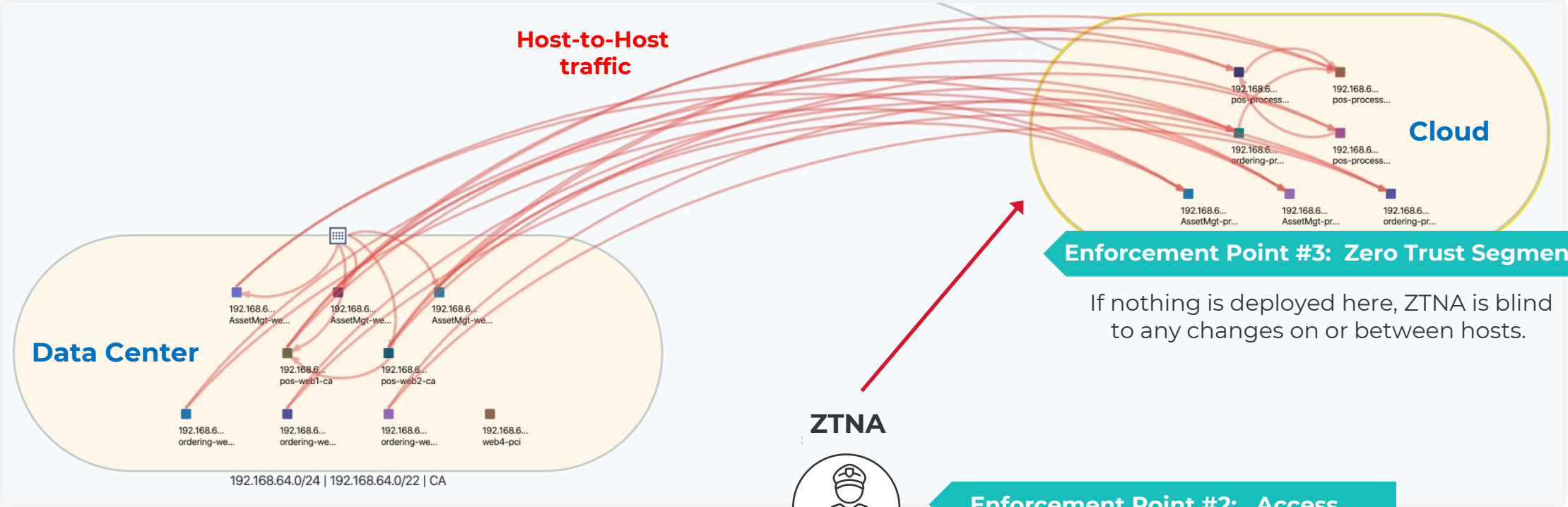
Custom | 50 per page | 1 – 40 of 40 Total

Resource	Resource State	Category	Account ID	Region	Labels	Cloud Tags	Security Controls
dev Virtual Machine	Succeeded	Compute	azure-se13	westus3	Compute ComputeVirtualMachines	Not available	Not available
dev-ven Virtual Machine	Succeeded	Compute	azure-se13	westus3	Compute ComputeVirtualMachines	Not available	Not available

Example: Vulnerable Resources

ZTNA + Identity + ZTS = Zero Trust

ZTNA enforces access into a Hybrid-Cloud, but it *lacks host-to-host visibility & enforcement inside Cloud*



Enforcement Point #3: Zero Trust Segmentation

If nothing is deployed here, ZTNA is blind to any changes on or between hosts.

ZTNA

Enforcement Point #2: Access

Examples: Netskope, Appgate, ZScaler

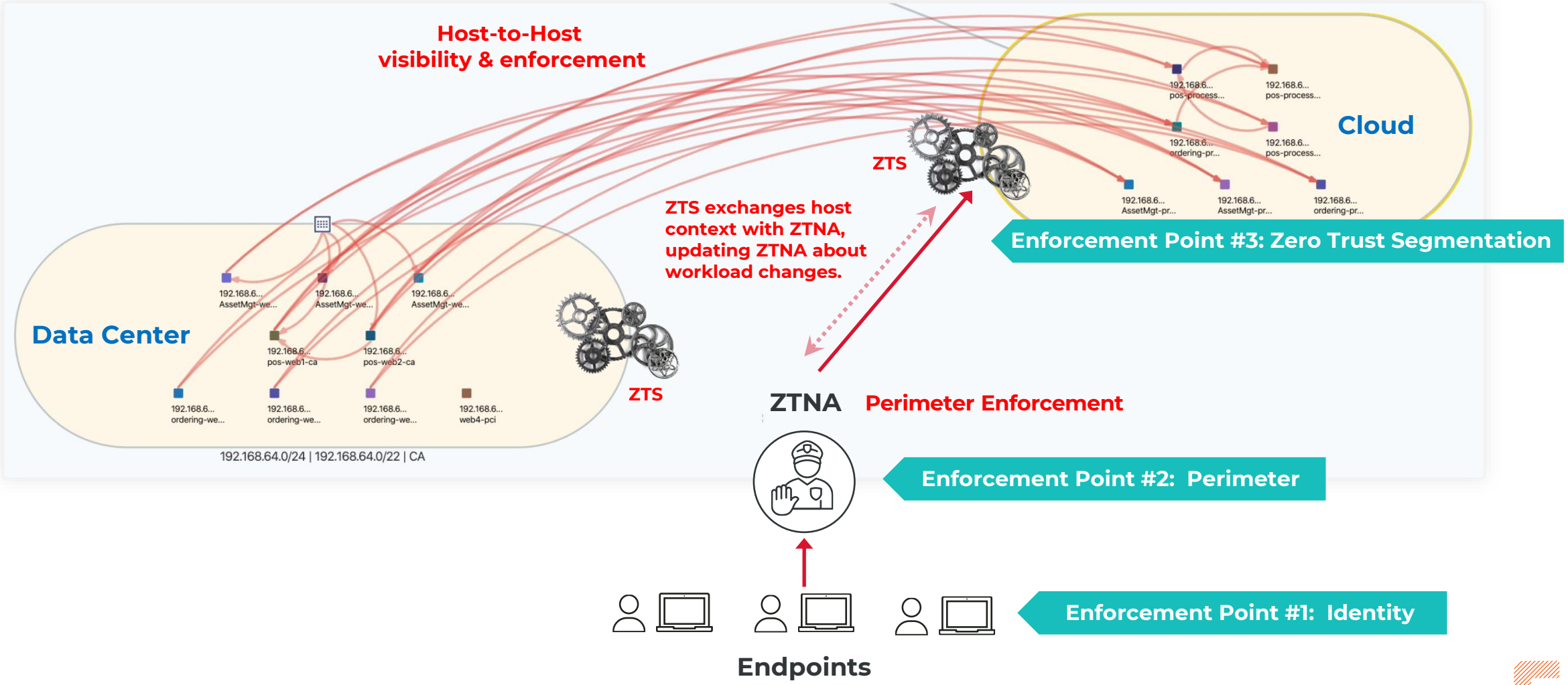
Endpoints

Enforcement Point #1: Identity

MFA, Biometrics, etc.

Visibility across all workloads, not just at Cloud perimeter

Perimeter Access (ZTNA) + ZTS (across both Cloud & Data Center) = Zero Trust



Illumio ZTS Platform: Zero Trust Segmentation everywhere

Illumio CloudSecure

Complete visibility into cloud traffic flows & proactively discover vulnerabilities across your entire environment

- Assess application behavior based on what did and what can happen
- Recommend & automate Zero Trust security policies

Illumio Core

- Real-time actionable insights into applications & cybersecurity risks
- Enhance compliance & business agility with automated security enforcement
- Fast & secure Zero Trust Segmentation, at scale

Coverage:
- Physical servers
- VMs running any hypervisor or cloud.
- Kubernetes, OpenShift

Illumio Endpoint

- Prevent lateral movement to isolate ransomware & malware to a single endpoint
- Visibility regardless of where users are – on the network or at home
- A proven allowlist-based policy model that brings Zero Trust to the endpoint

Coverage:
- Laptops
- VDIs
- Workstations

illumio

illumio

Q & A