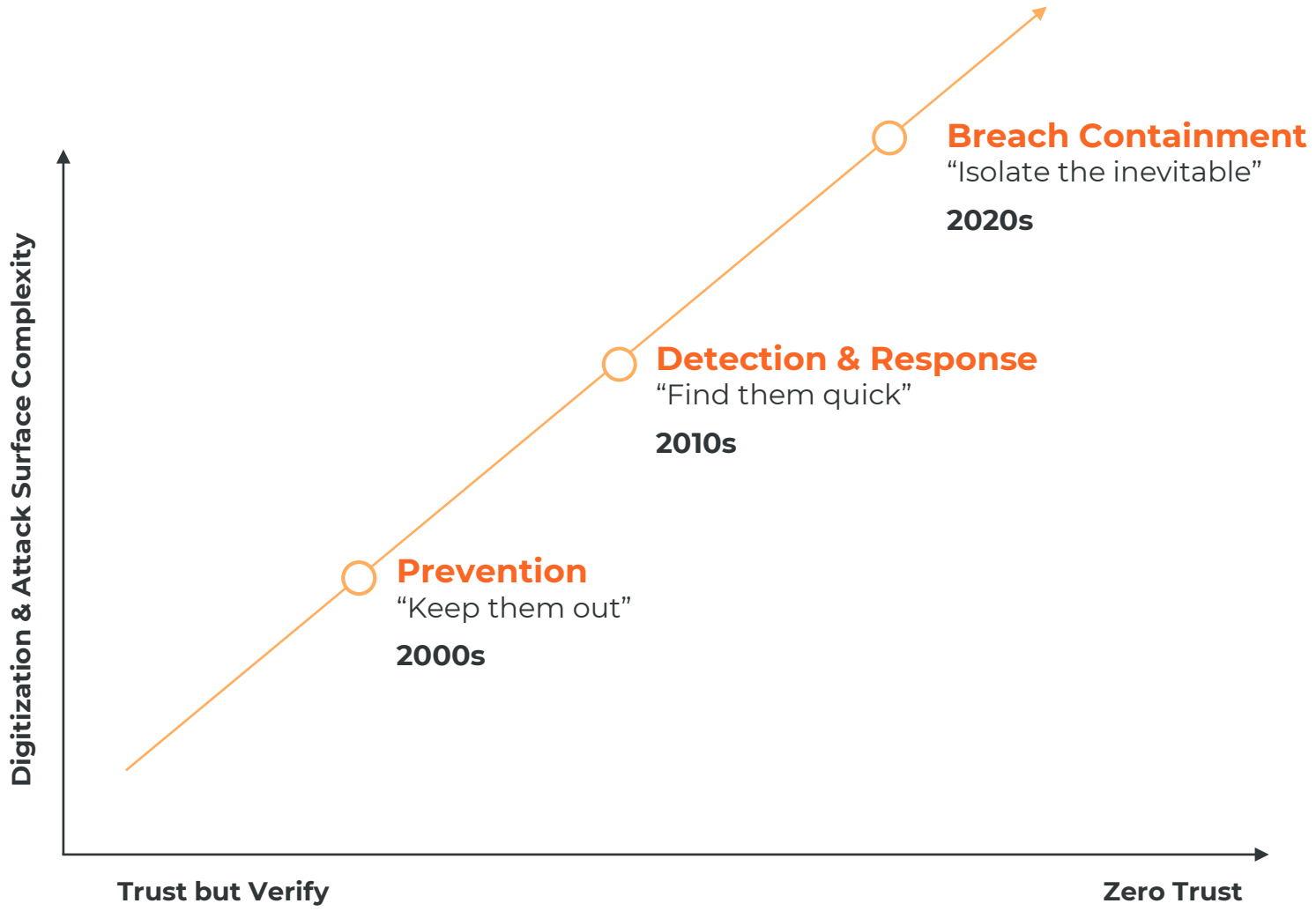
# Re-Thinking Cybersecurity

Christer Swartz
Director, Industry Solutions
Illumio

# The 3 Security Mindsets

**It's time to face reality:**

**100% of us will be breached.**



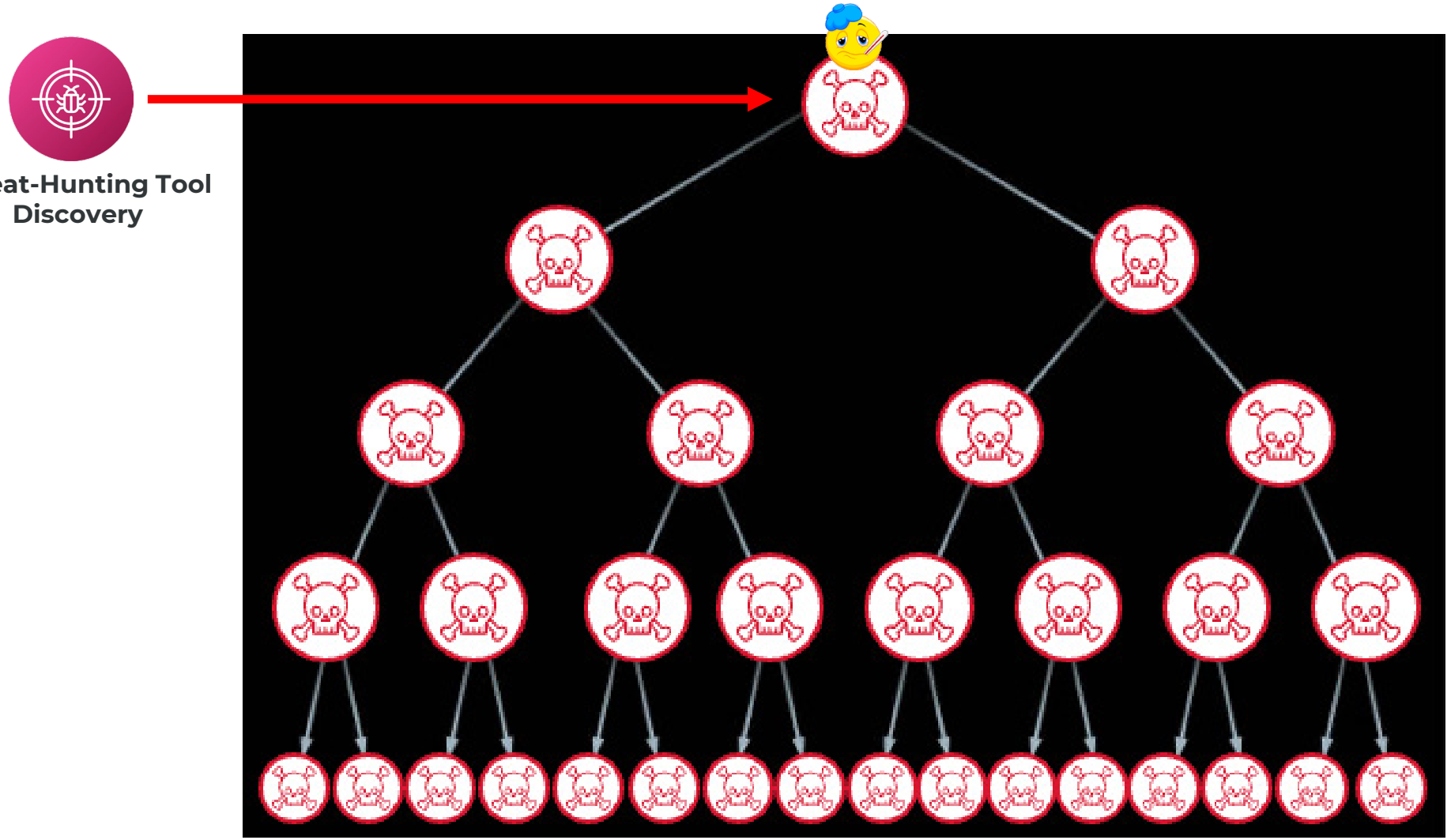
## Money spent on Cybersecurity in 2024, globally

# $215 Billion

**Global Cybersecurity incidents from 2023 to 2024:**
**Increase of 75%** 

**Global Cybersecurity reported incidents, every day:**
**2,200**

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



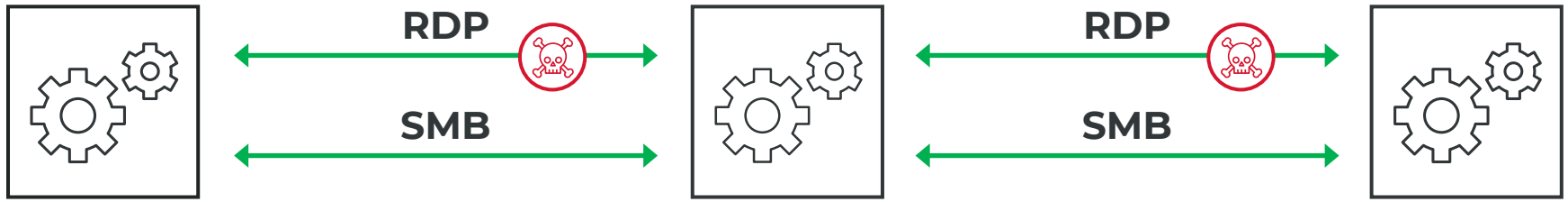
# All Threats have only 2 ways to move

**#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 0x4fe82624611139e55      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.**

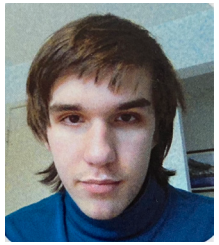
# All threats share one thing in common:
## *They all want to spread.*

**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**

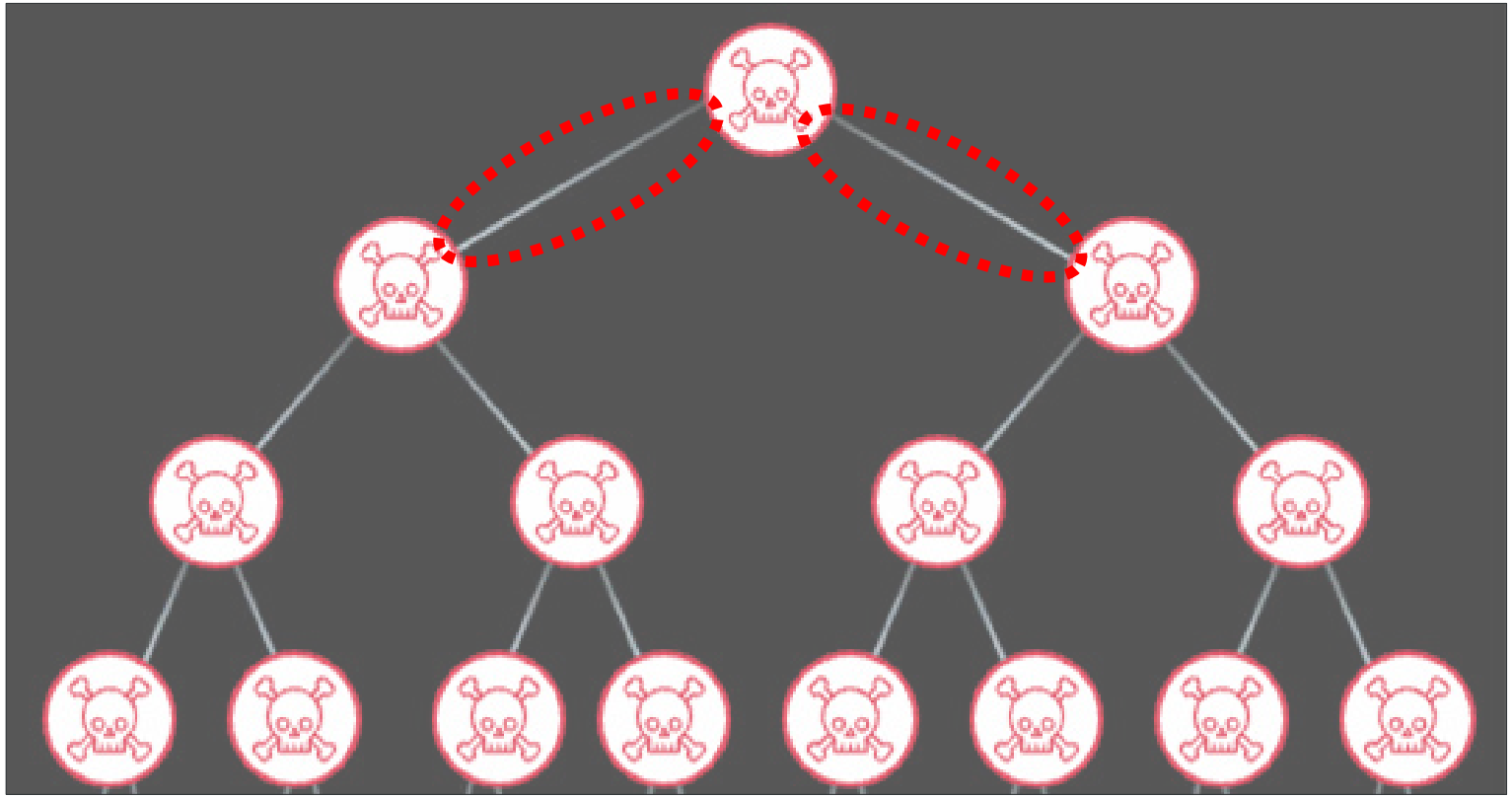


**Opportunistic teenager**
**(my son)**

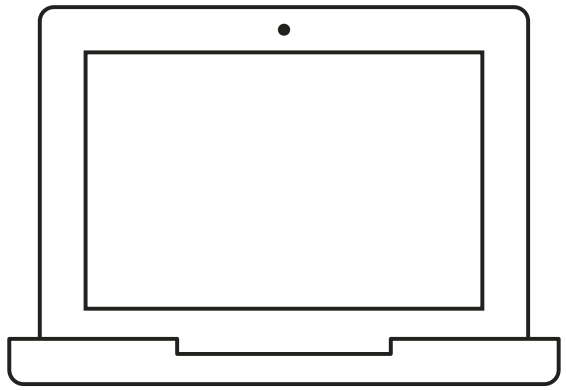
# W hat is m ore critical? The W orkload or the Segm ent?

**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**:

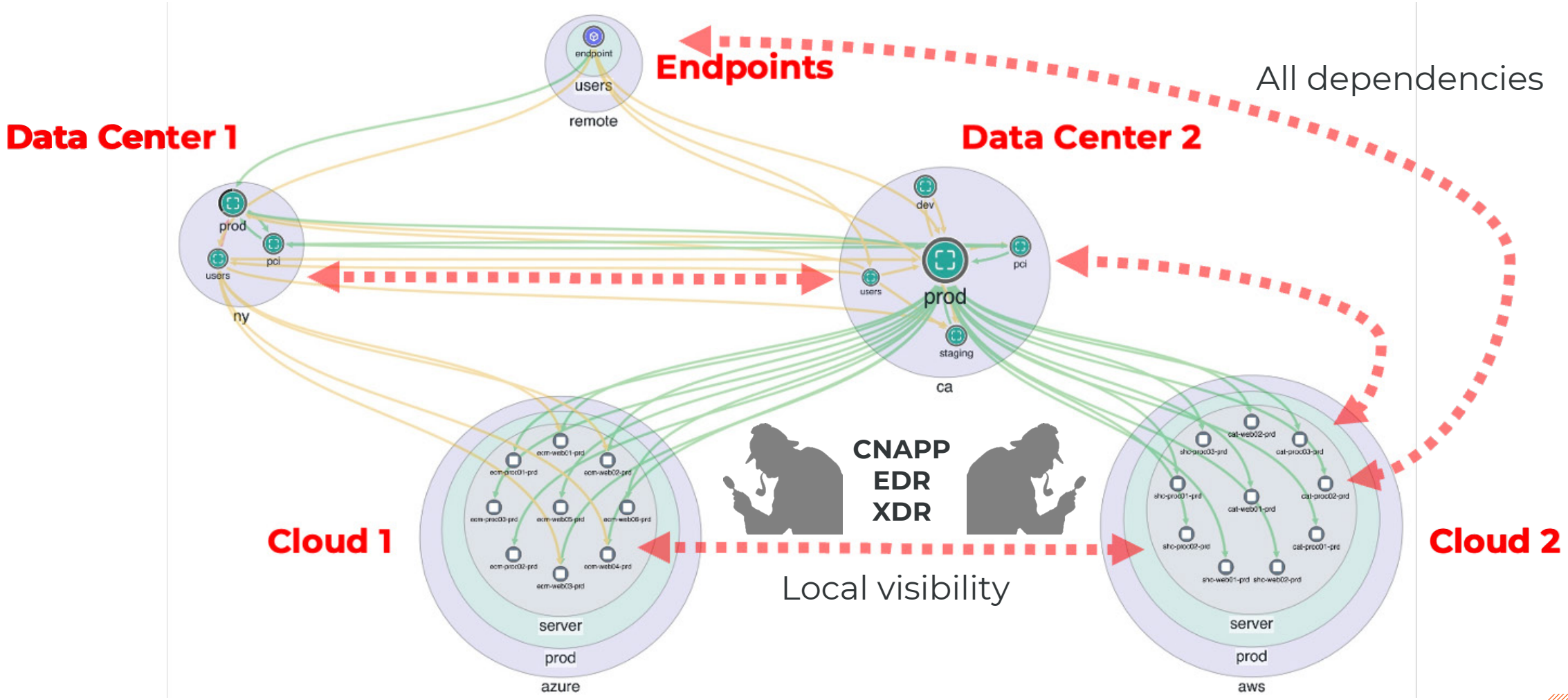
~ Asymmetric.
- Sporadic.
- KB outbound, MB inbound.

**Example of abnormal behavior**:

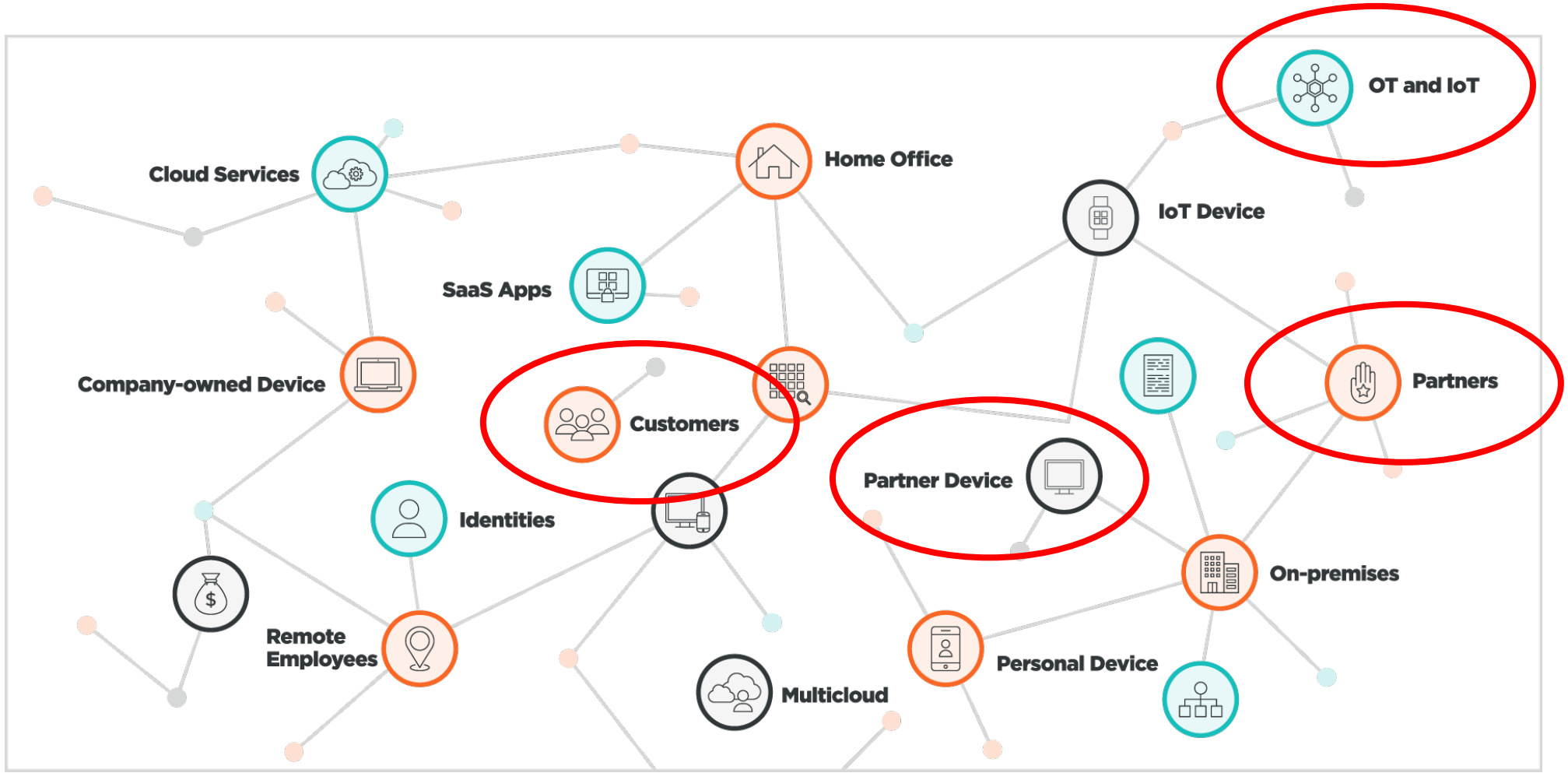
- 10 Gig of sustained traffic outbound over either port.
- Destination to known malicious IP's.
- Activity during idle hours.

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

# Visibility, into everywhere your data can live

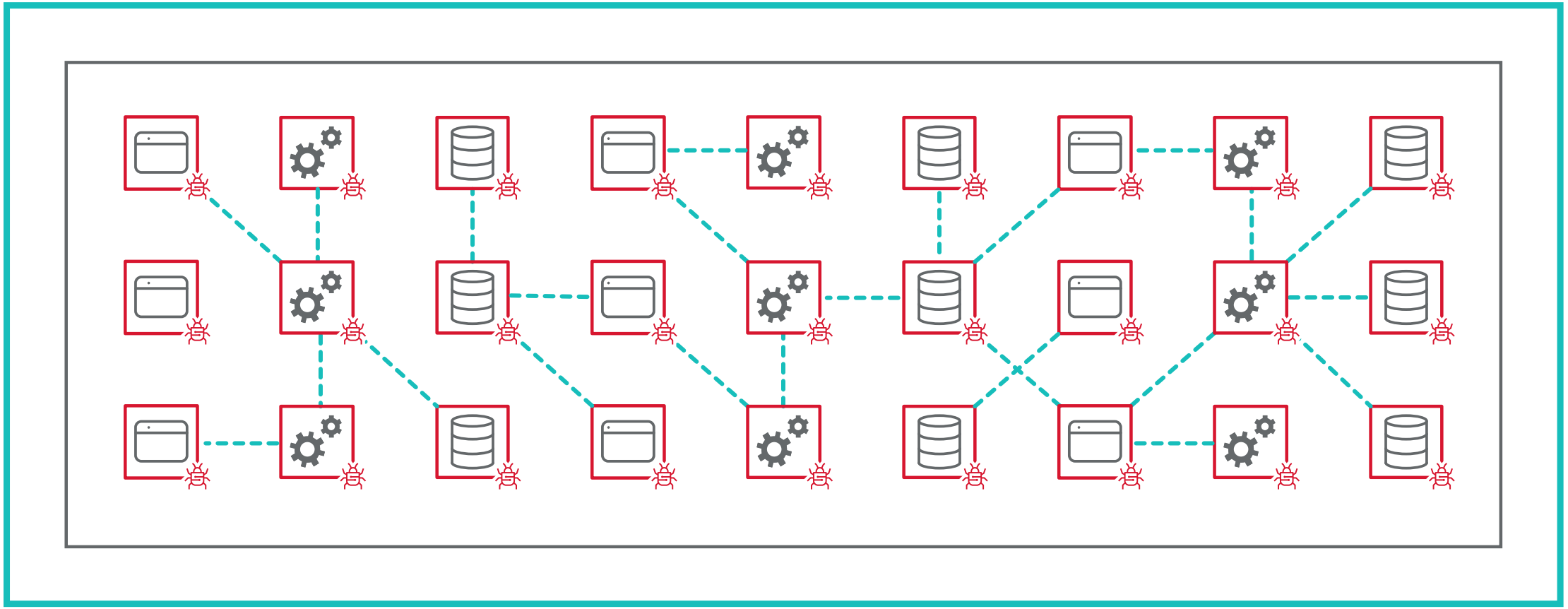


# Reality Check: Not all entry points are under your control

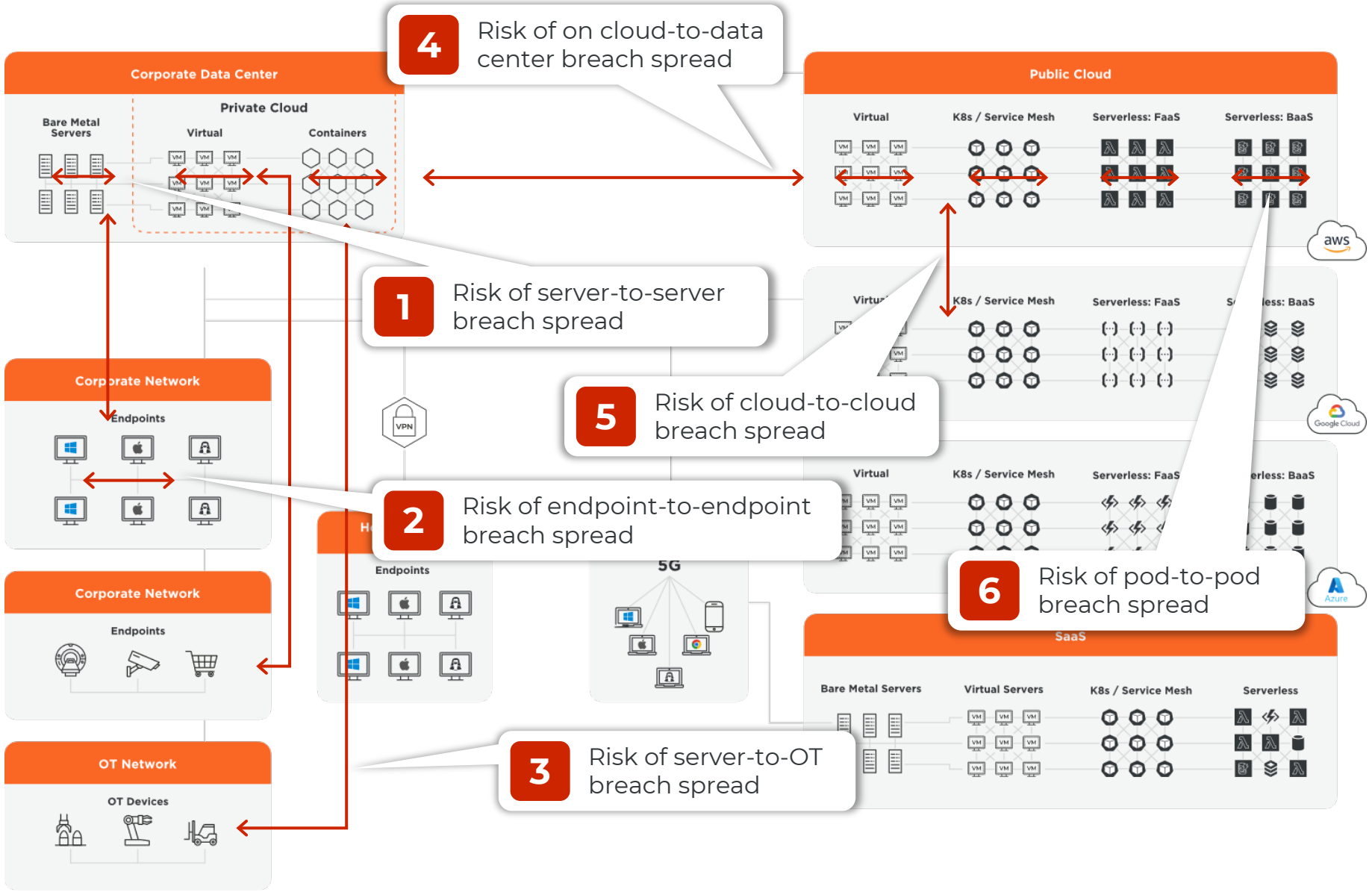


# Open ports, in listening mode, are like unlocked doors

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



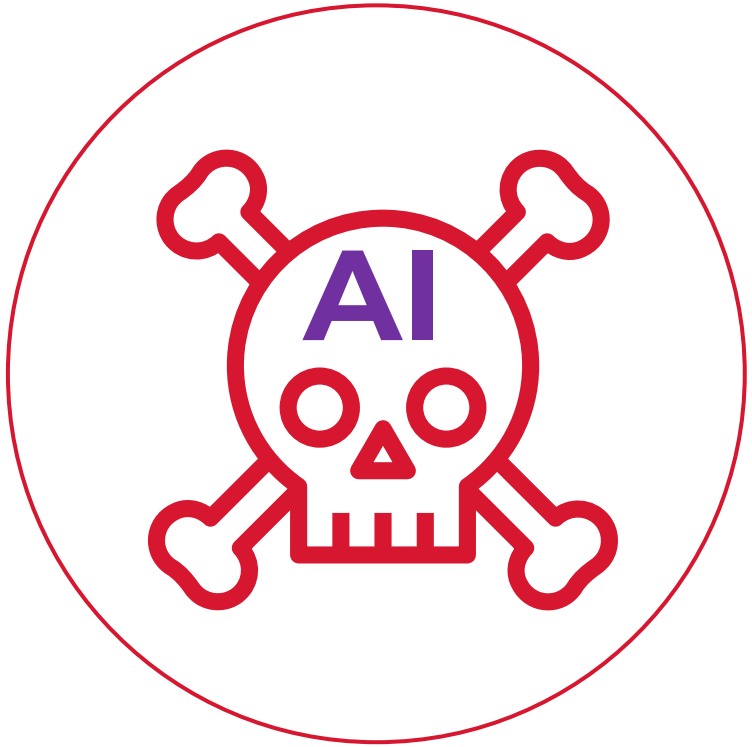
With limited visibility, threat actors have many entry points to choose from.



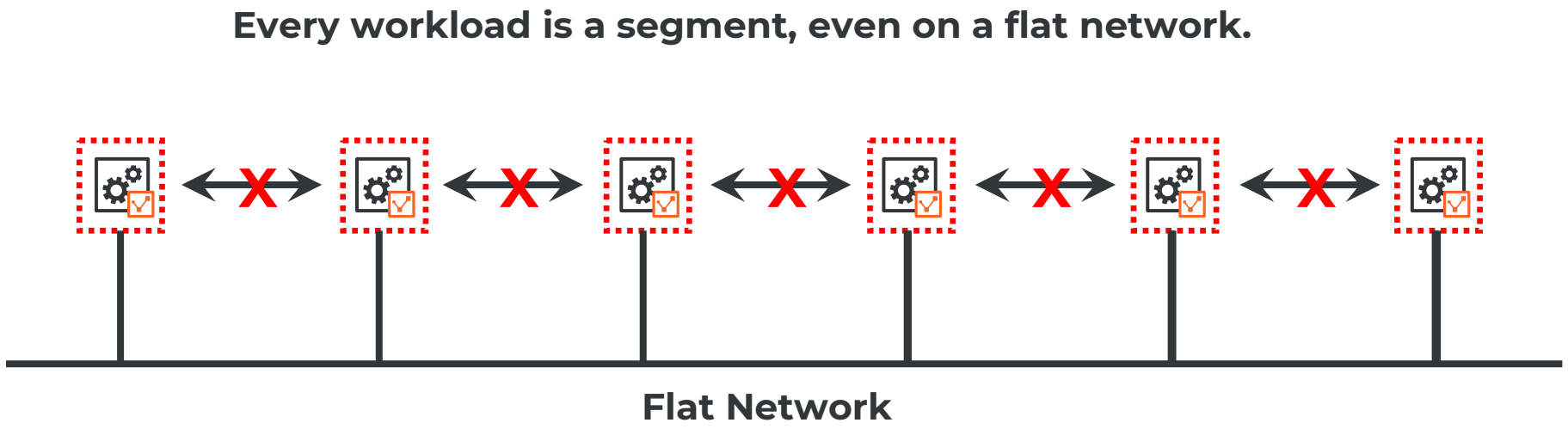
# Future-Proof against AI-Generated Malware

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

**It will want to spread**.

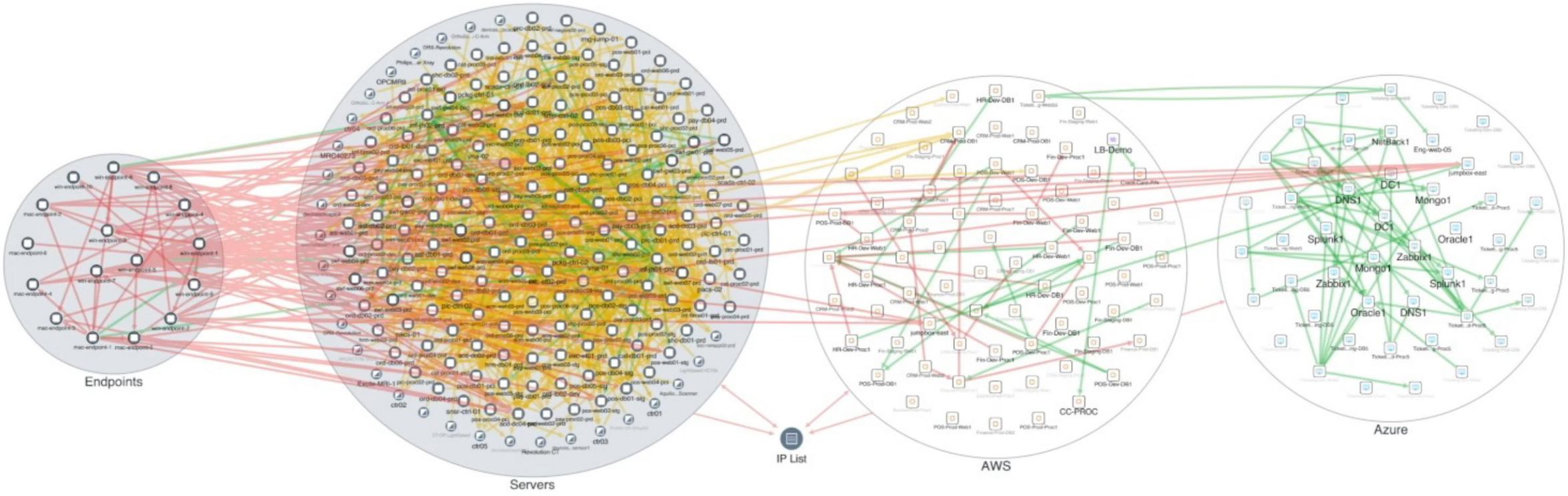


# Zero Trust = Every workload a dedicated trust-boundary

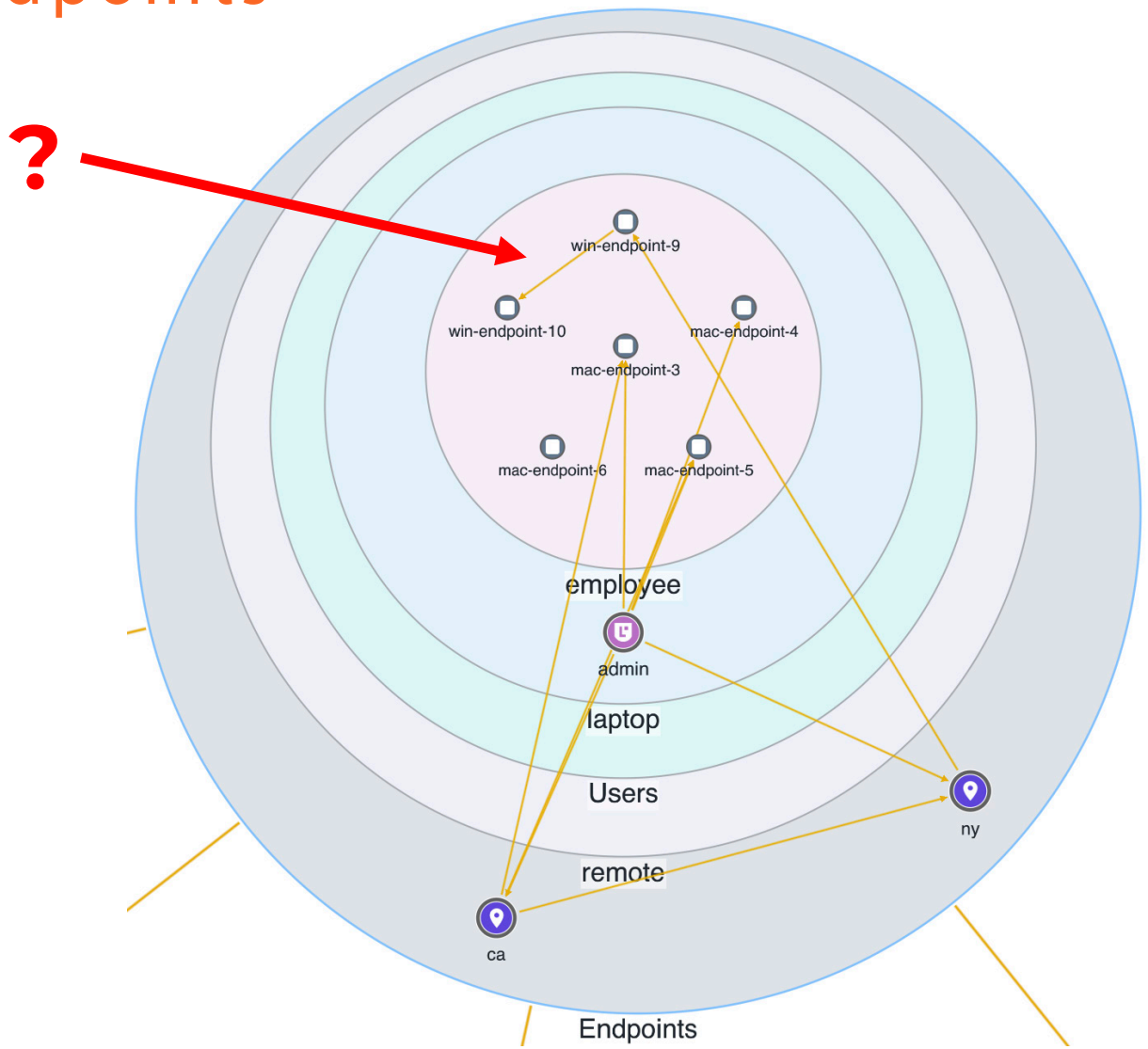


# 100% visibility, with *no dependency on security appliances*

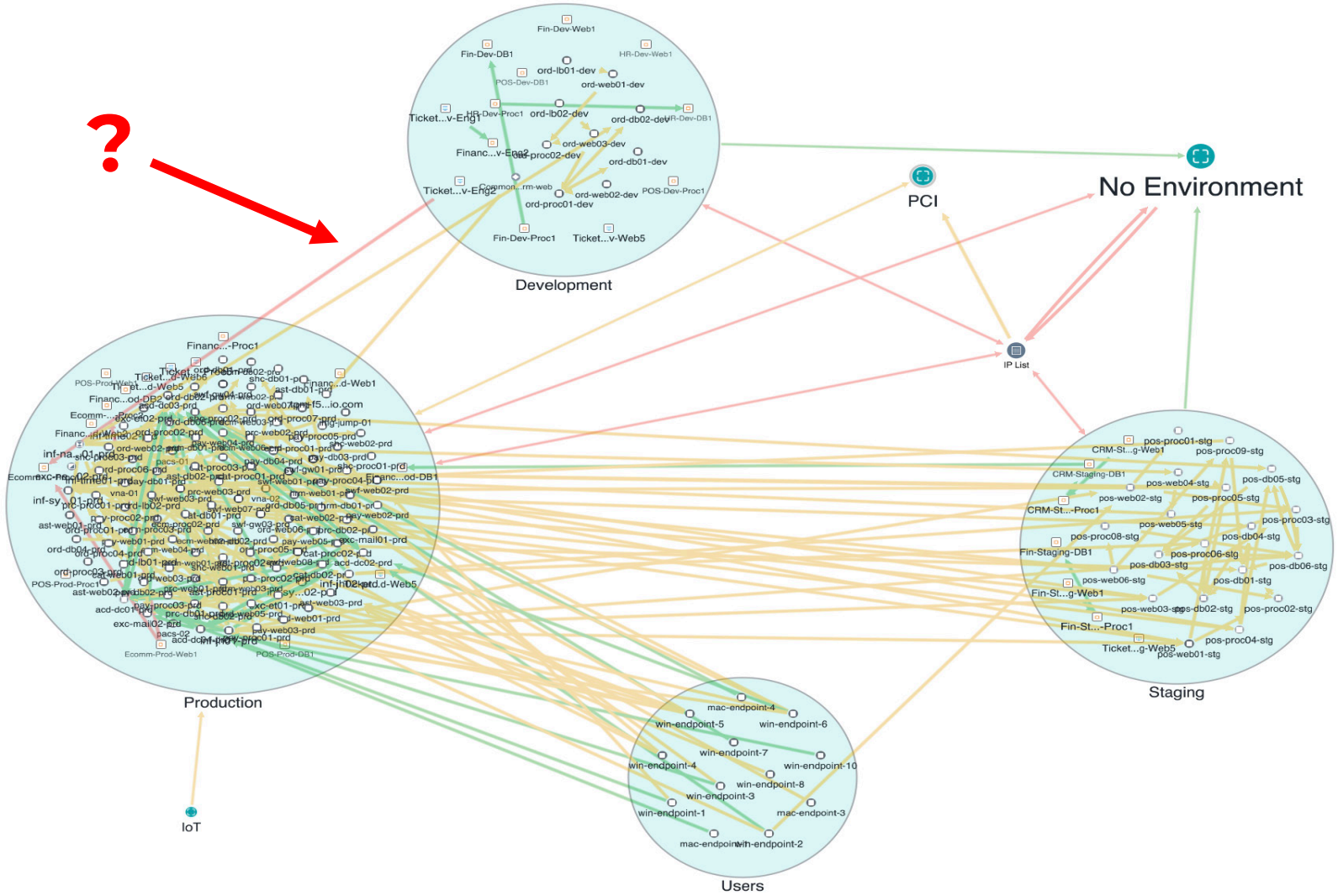
**Endpoints** **Data Center** **AWS** **Azure**



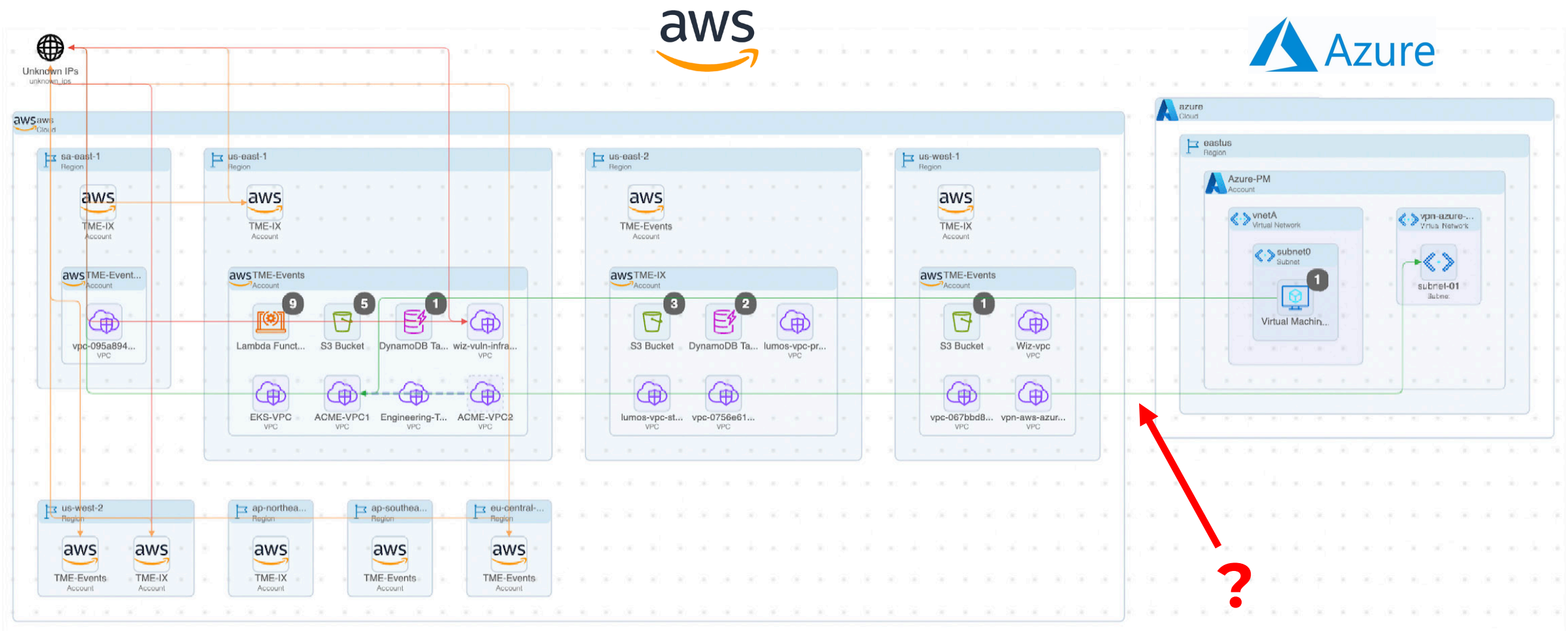
# Visibility: Endpoints



# Visibility: Data Center

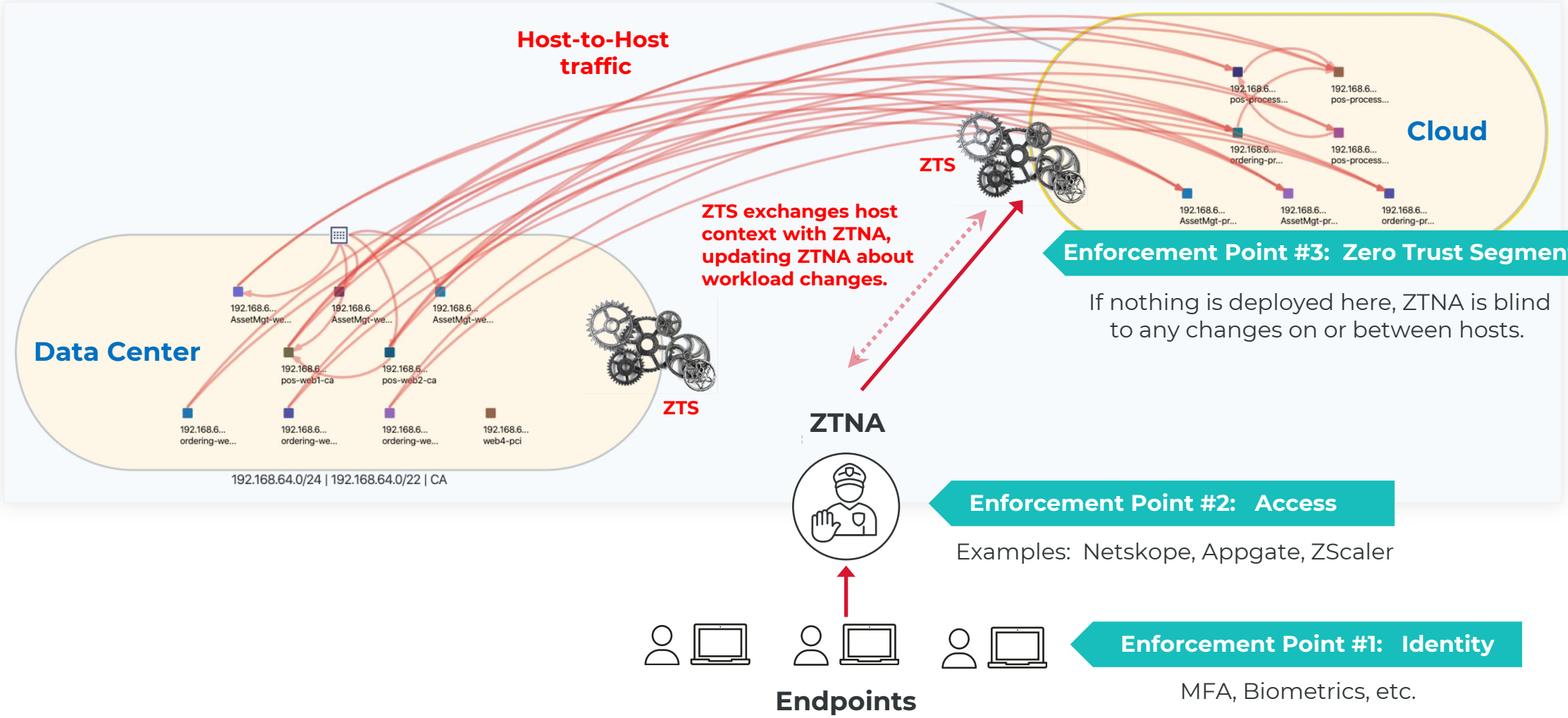


# Visibility: Cloud

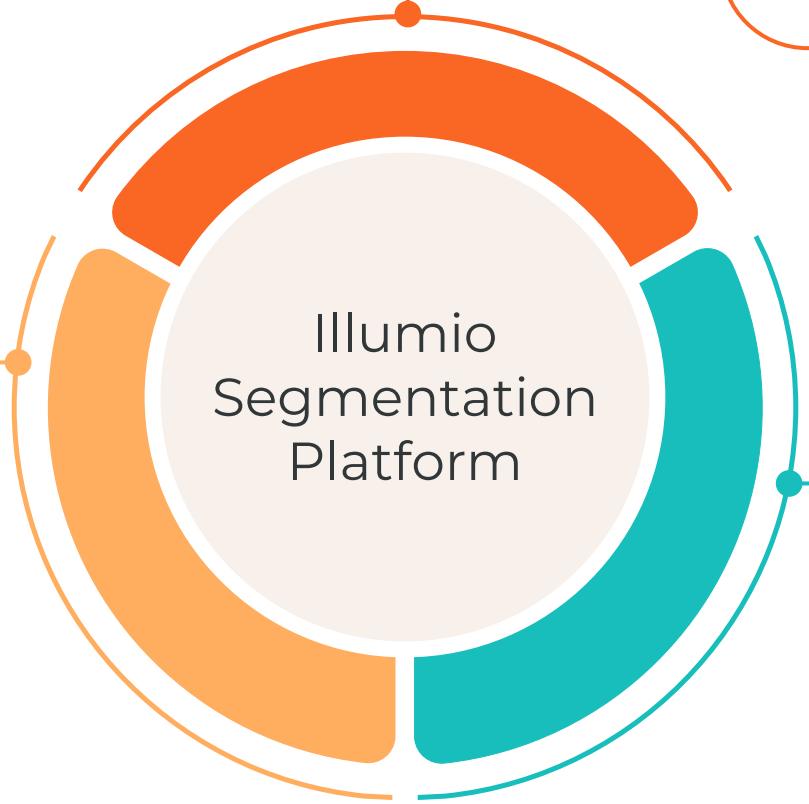


# ZTNA + Identity + ZTS = Zero Trust

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



# Illumio ZTS Platform: Zero Trust Segmentation eveywhere




## 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