



Good AI Gone Bad

A Zero Trust Story



Michael Adjei

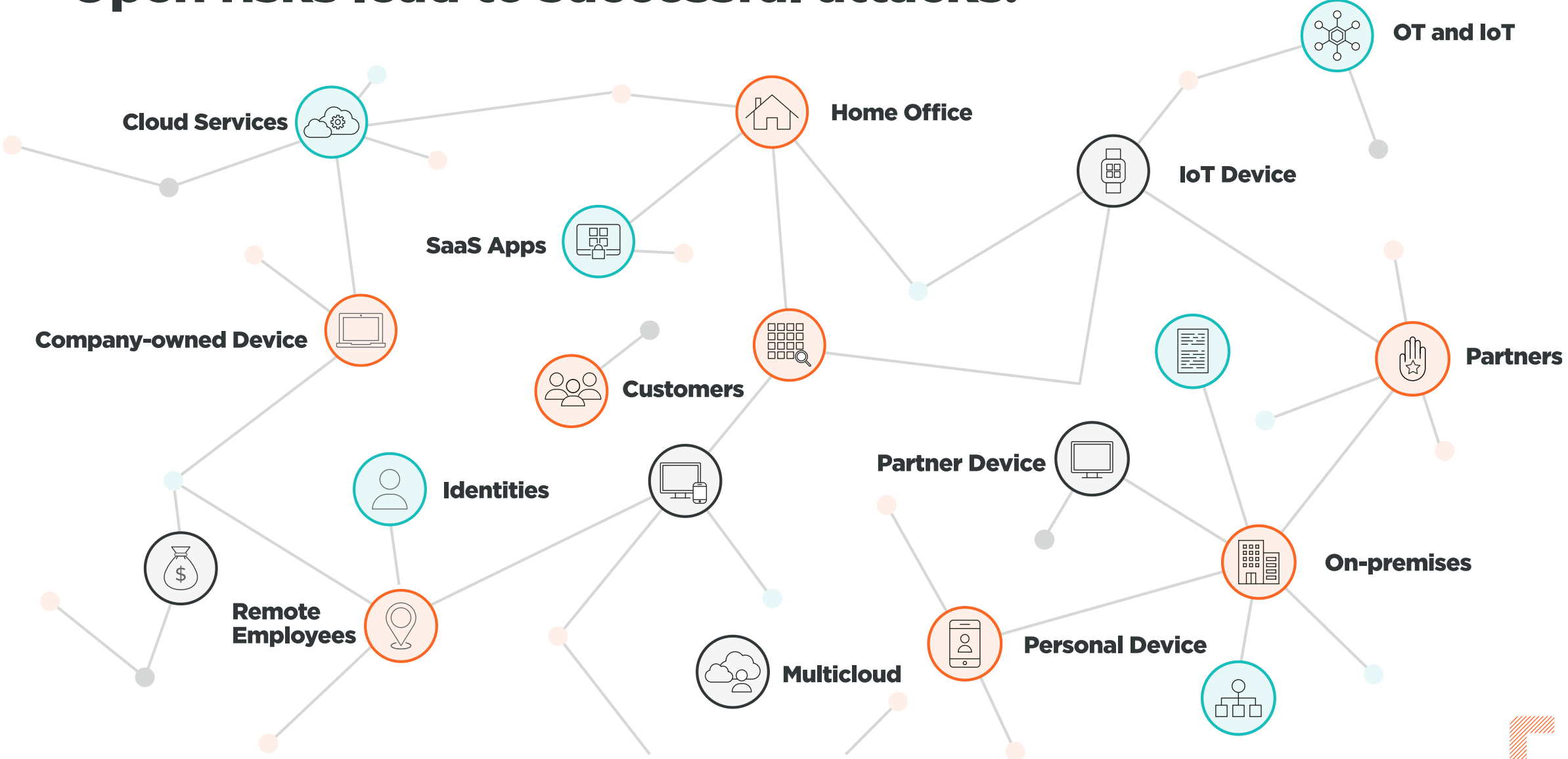
Director, Systems Engineering



Risks Today



Open risks lead to successful attacks!



Most attacks start from a

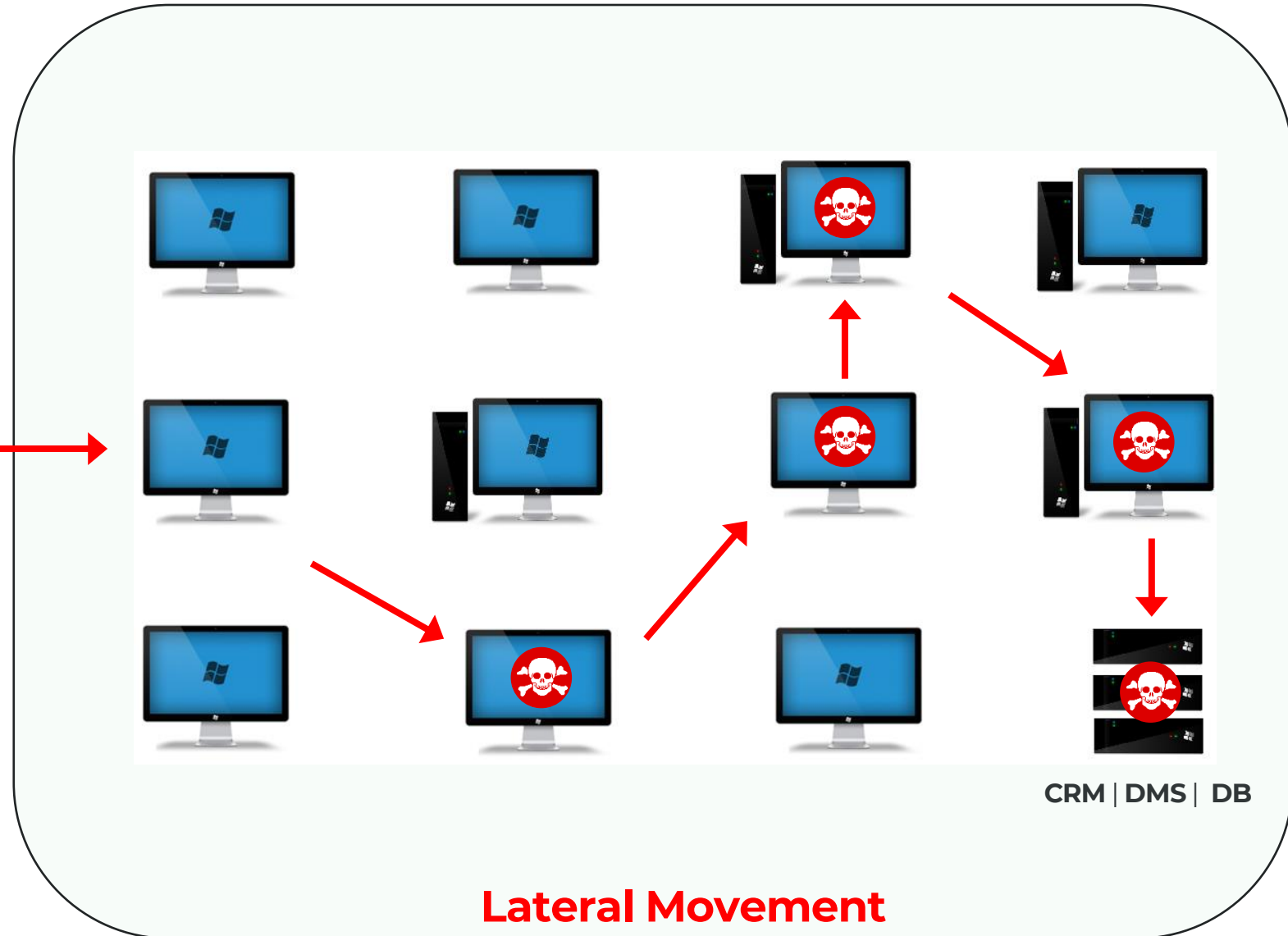
Patient Zero!



The success of an attack

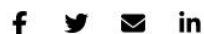
lies in its

ability to spread...



Lateral Movement


Ransomware



New BlackCat ransomware variant leverages Impacket for lateral movement

Steve Zurier August 18, 2023





HOME REGIONS TECHNOLOGY ANALYSIS VIDEOS

Expert says CISOs need to take lateral movement seriously

DEEP DIVE | ENTERPRISE SECURITY | NETWORKING | TOP STORIES

Alix Pressley | 9 April, 2021

CISOs are faced with the challenge of their enterprise-level environments being vulnerable to lateral movement in their networks. Carolyn Crandall, Chief Security Advocate and CMO at Attivo Networks, says most CISOs are familiar with the role lateral movement plays in attacks, but organisations need to back up this knowledge with action.

Conti Ransomware Hitting VMware vCenter With Log4j Exploit

BY MICHAEL NOVINSON
DECEMBER 17, 2021, 02:02 PM EST

'[The] Log4j2 vulnerability appears ... for Conti at the moment when the syndicate has both the strategic intention and the capability to weaponize it for its ransomware goals,' says AdvIntel in a security advisory.



Conti is pursuing lateral movement on vulnerable Log4j VMware vCenter servers, making them **the first major ransomware gang** revealed to be weaponizing the massive bug.

The Hacker News

Home Data Breaches Cyber Attacks Vulnerabilities Webinars Store Contact

Wanted Dead or Alive: Real-Time Protection Against Lateral Movement

May 01, 2023 The Hacker News

Cyber Threat / Authentication

Just a few short years ago, lateral movement was a tactic confined to top APT cybercrime organizations and nation-state operators. Today, however, it has become a commoditized tool, well within the skillset of any ransomware threat actor. This makes real-time detection and prevention of lateral movement a necessity to organizations of all sizes and across all industries. But the disturbing





AI Amplifies the **Risk**

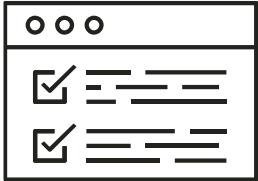


AI Deep Learning - Artificial Neural Network

Dataset



Hidden Layer



AI Interface



GPT-4

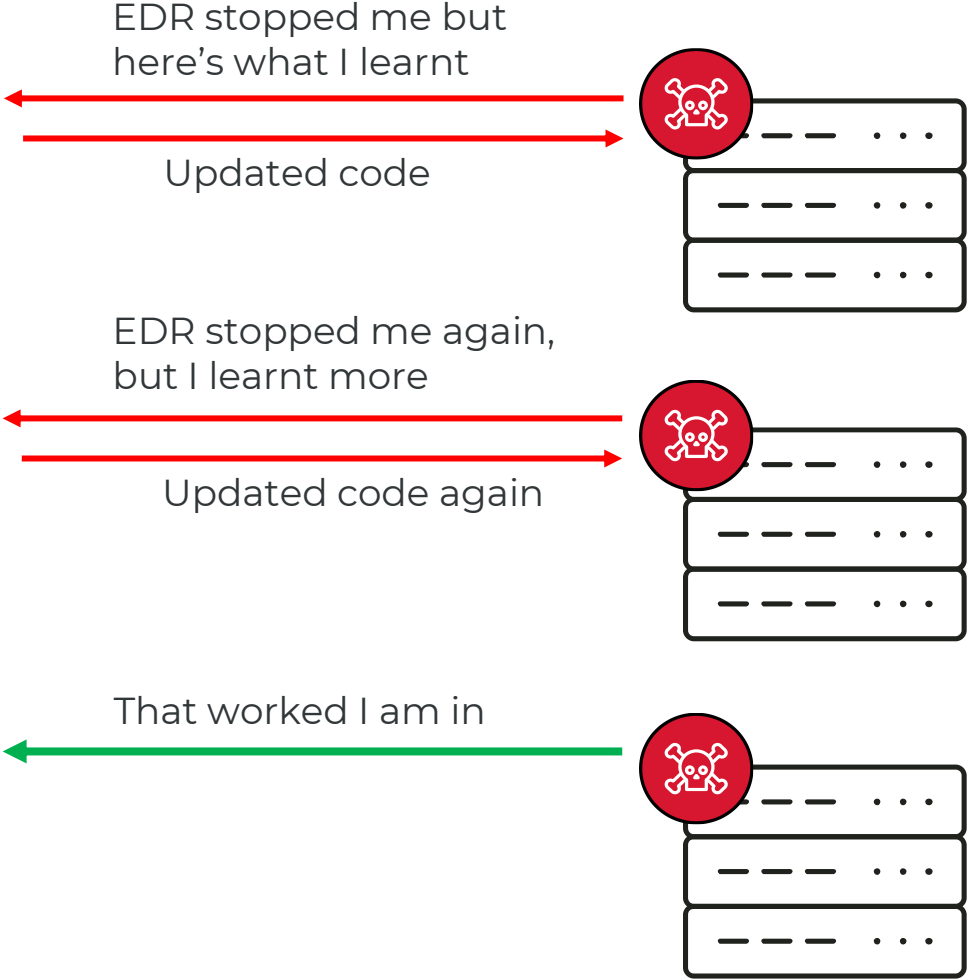
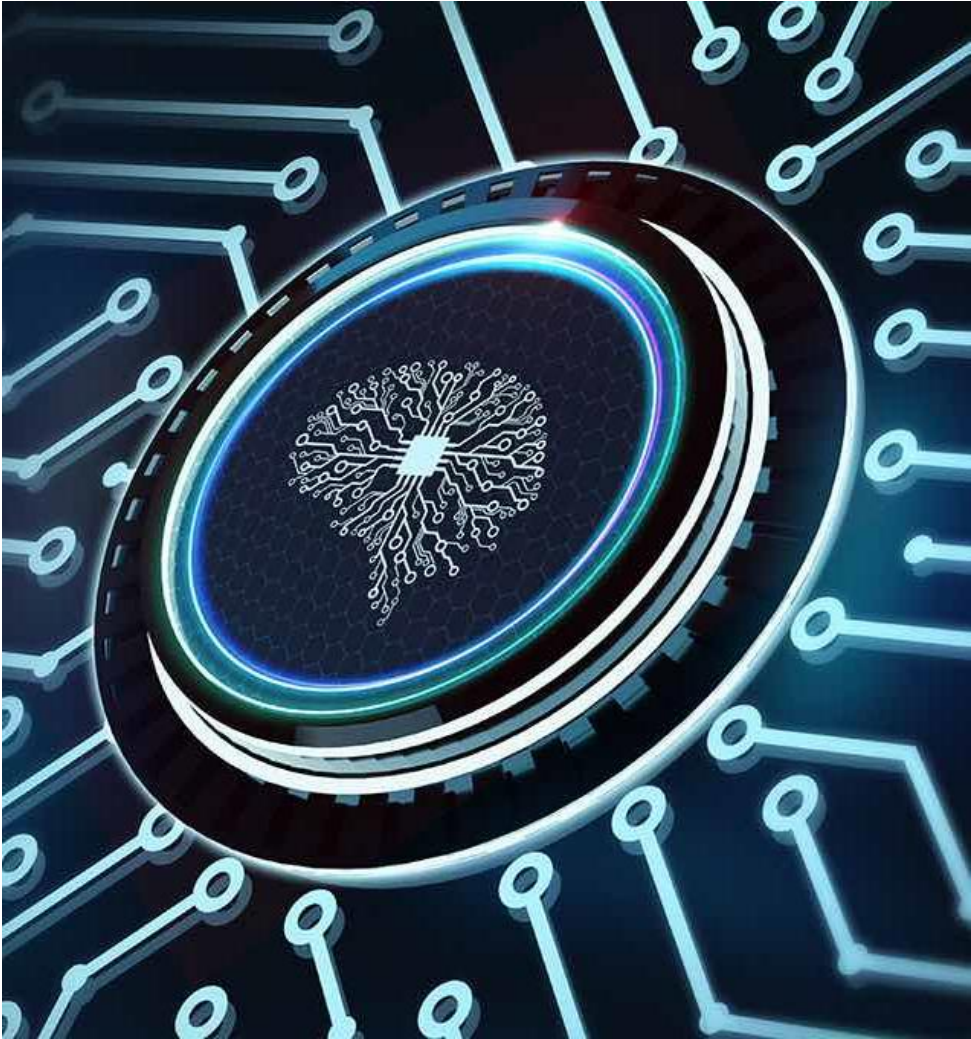
Cybersecurity

Researchers from UIUC reveal GPT-4's capability to autonomously exploit real-world vulnerabilities

- Recent research highlights OpenAI's GPT-4's ability to autonomously exploit real-world security vulnerabilities by analyzing CVE advisories.
- GPT-4 outperforms other models and open-source vulnerability scanners, showcasing an 87 percent success rate in exploiting critical vulnerabilities.
- The study underscores the significance of transparent information sharing in cybersecurity, dismissing reliance on security through obscurity.
- Despite encountering challenges with certain vulnerabilities, GPT-4 demonstrates adaptability and generalization capabilities, even beyond its training data.
- Cost-effective and efficient, GPT-4's estimated expense for a successful exploit stands at \$8.80 per attack, significantly lower than traditional penetration testing costs.



Real-time Morphing Possibility



The answer is **NOT** necessarily more AI

Get the basics right:

- **Reduce** the learning surface
- **Control** access to resources
- **Contain** an attack
- **Recover** securely

The answer **is** Zero Trust



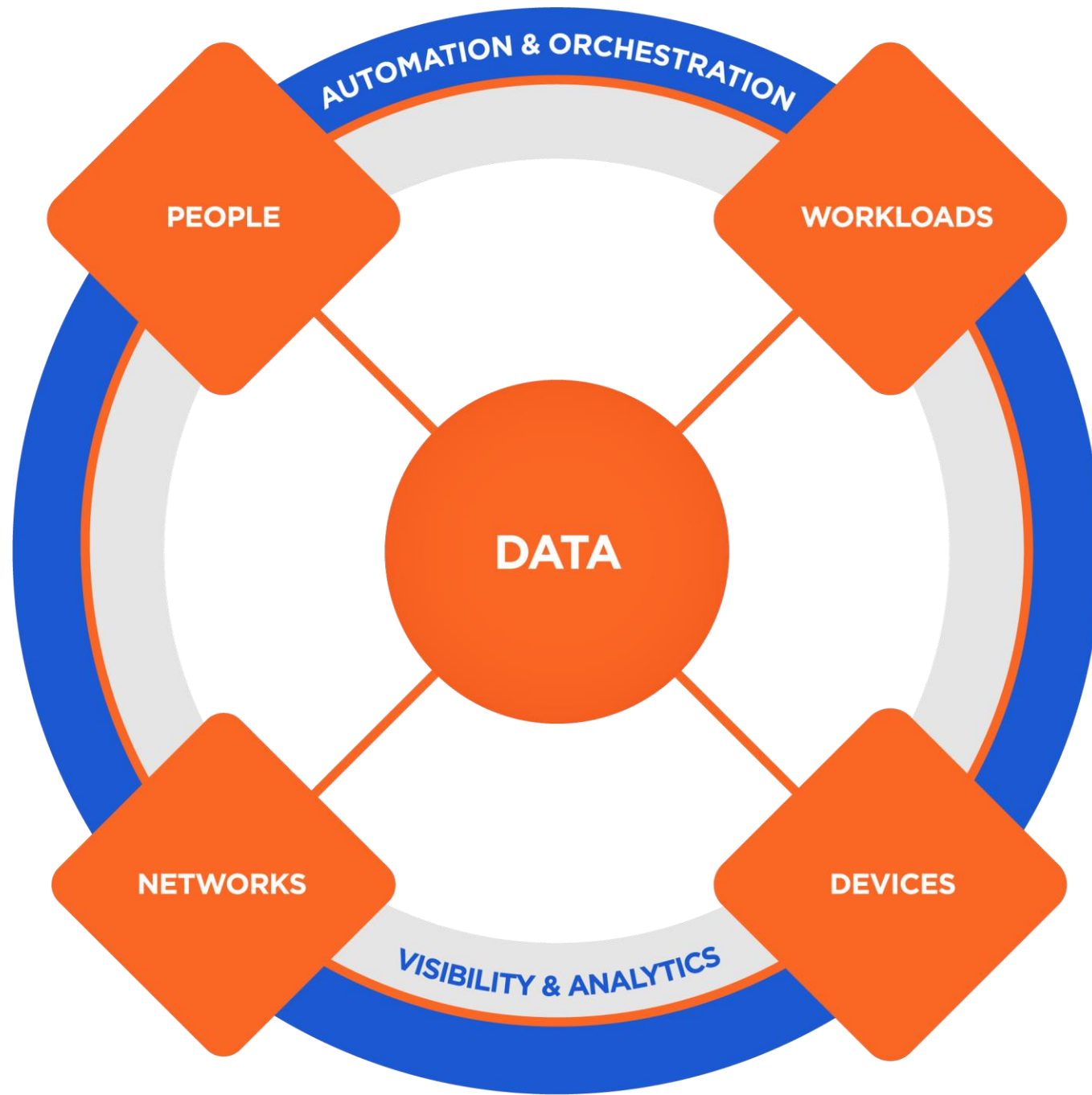


Addressing the **Risk**



Zero Trust

A strategy designed to **stop data breaches** and **prevent cyberattacks** from being successful by **eliminating implicit trust** from digital systems.





The bad guys will always find a way in!

**So, every organization needs a cyber
containment strategy!**

(Cyber & Operational Resilience)



The ability to absorb potential disruptions while continuing to meet service level objectives.

Gartner Cyber Resilience Framework



Containment Strategy

Cyber & Operational Resilience



Defence In-depth



Protections against how an **infection starts**

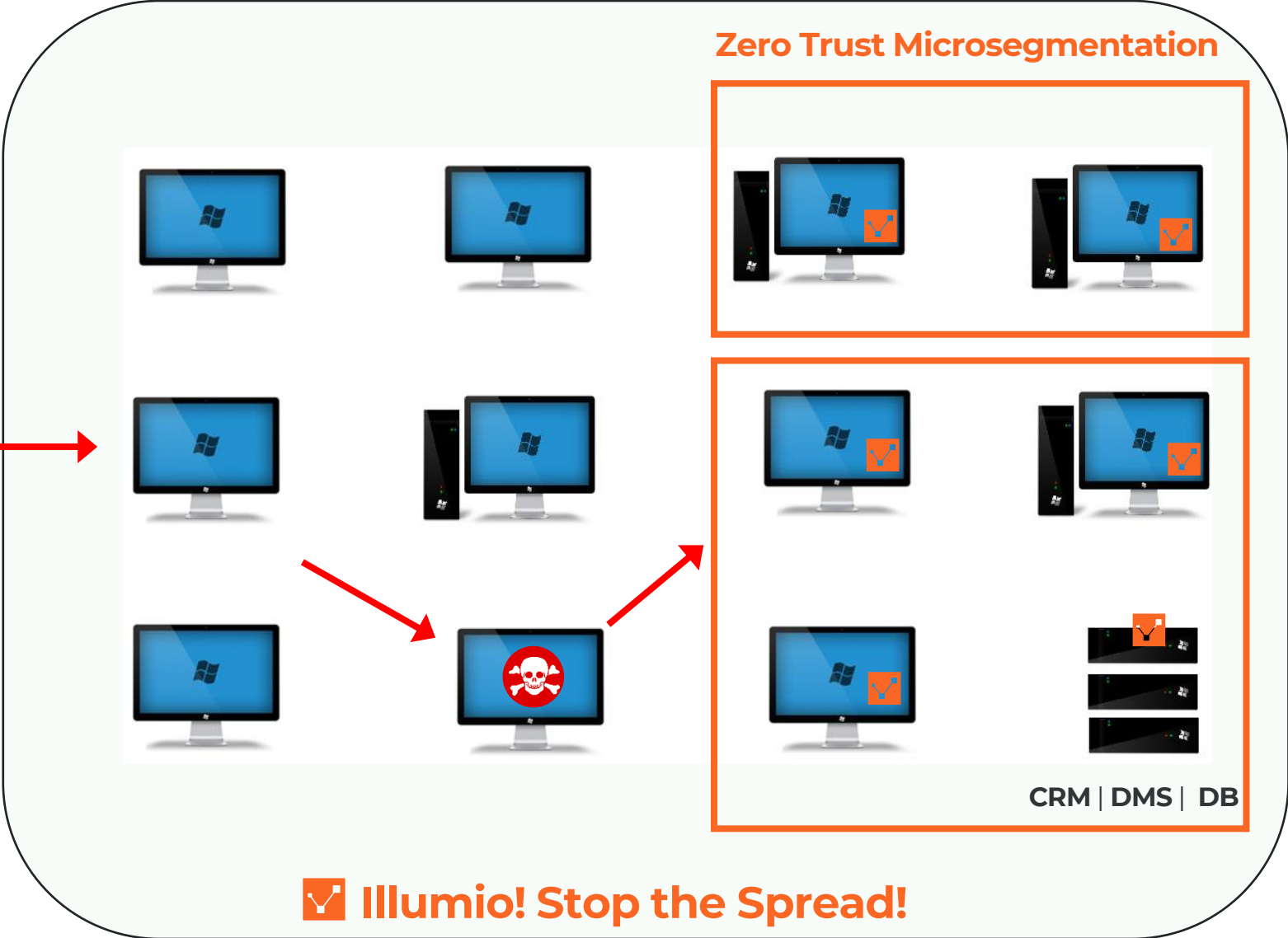
and

Protections against how an **infection spreads!**



Containment Strategy is to

Stop the Spread!



Zero Trust Microsegmentation

CRM | DMS | DB

 **Illumio! Stop the Spread!**

Protect with Context – Critical Business Assets

Hybrid Corporate Network

| | | | | |
|---------------|------------|---------------|-------------|-------------|
| | | | | |
| ★ Imaging | ★ Genomics | ★ Genomics | ★ Endoscopy | ★ Endoscopy |
| ▲ Workstation | ▲ Server | ▲ Workstation | ▲ Server | ▲ Server |
| ★ London | ▲ AWS | ★ Bristol | ★ London | ★ London |

| | | | |
|-----------|------------|------------|---------------|
| | | | |
| ★ Imaging | ★ Genomics | ★ Genomics | ★ Endoscopy |
| ▲ Server | ▲ Server | ▲ Server | ▲ Workstation |
| ▲ AWS | ★ Bristol | ▲ AWS | ★ London |

Critical Business Assets

| | |
|--------------|--------------|
| | |
| ★ Imaging | ★ Endoscopy |
| ▲ Medical OT | ▲ Medical OT |
| ★ London | ★ Bristol |

| | |
|--------------|--------------|
| | |
| ★ Imaging | ★ Genomics |
| ▲ Medical OT | ▲ Medical OT |
| ★ Bristol | ★ London |



Practical Zero Trust



How does the ZTS platform do it?

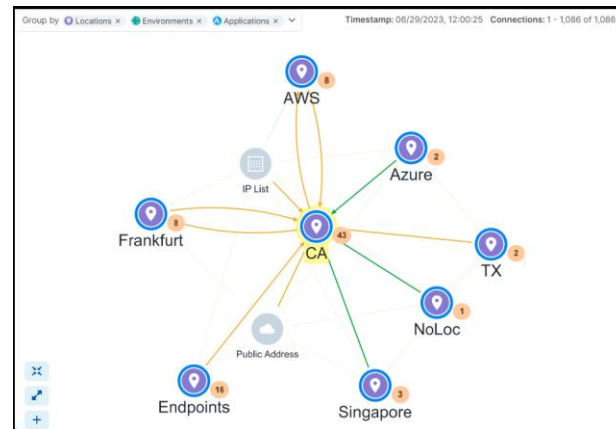
Identify Assets

| Name | Role | Application | Environment | Location |
|---------------|---------------|---------------|-------------|----------|
| ordering-db1 | Database | Ordering | Production | CA |
| ordering-db2 | Database | Ordering | Production | CA |
| ordering-lb1 | Load Balancer | Ordering | Production | CA |
| ordering-web1 | Web | Ordering | Production | CA |
| ordering-web2 | Web | Ordering | Production | CA |
| pos-db2-nv | Database | Point-of-Sale | Staging | CA |
| pos-db1-ny | Database | Point-of-Sale | PCI | NY |
| pos-db2-va | Database | Point-of-Sale | Staging | SYD |

Asset Inventory

(Know what you have)

See Risk



A Map

(Know what they do)

Contain Risk

1. Choose Intra-Scope Rule Configuration

- App Group Level**
Microsegmentation: Allow all Workloads to talk across all Services
- Role Level - All Services**
Divide Workloads by Role and allow them to talk on all Services
- Role Level - Specified Services**
Nanosegmentation: Divide Workloads by Role and specific Services
- Auto Level**
Vulnerability Mitigation: Eliminate or reduce the exposure of vulnerable ports

App Group: Point-of-Sale | Staging - 21 Workloads

Intra-Scope Connections
100% Rule Coverage

0 Connections with Existing Rules
22 Included Connections
0 Excluded Connections

Intra-Scope Vulnerability Mitigation

| | | | | | |
|------------|----|----|---|---|---|
| Reduced | 10 | 26 | 3 | 6 | 0 |
| Eliminated | 2 | 10 | 0 | 0 | 0 |

Intelligent Policy

(Know how to protect them)

Workloads

Workloads Container Workloads VENS

[+ Add](#) [- Remove](#) [Edit Labels](#) [Enforcement](#) [Visibility](#)

[Refresh](#)


Select properties to filter view

Customize columns 50 per page 1 - 50 of 9

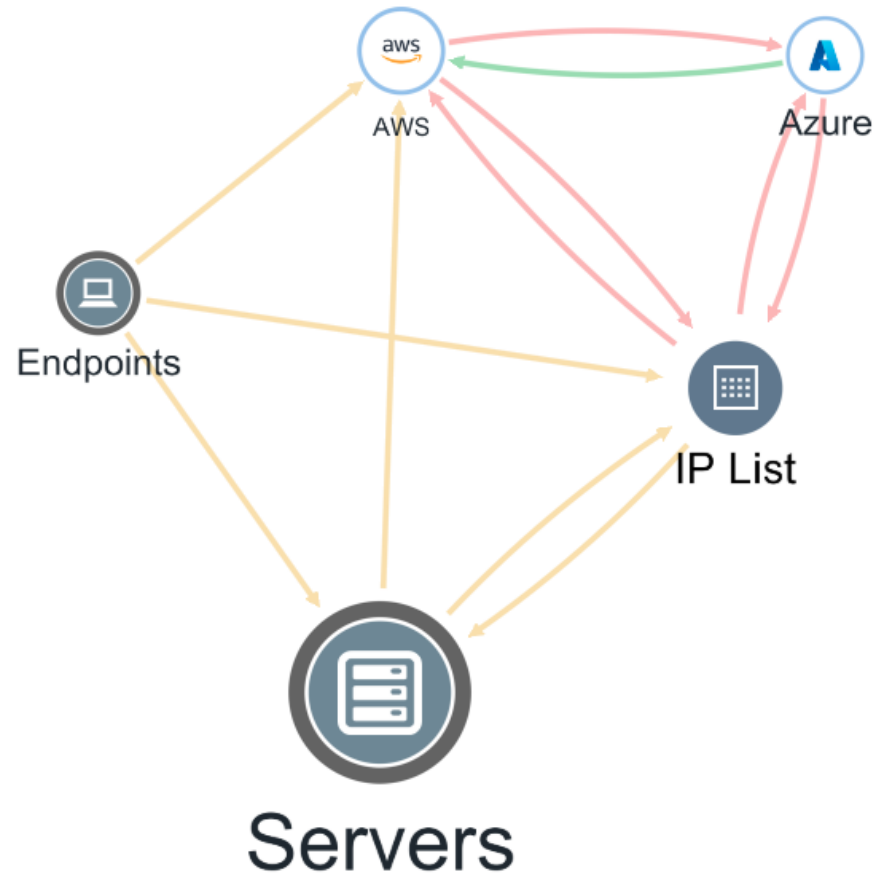
| <input type="checkbox"/> | Connectivity | V-E Score | Enforcement | Visibility | Policy Sync | Ransomware Exposure | Name | Labels |
|--------------------------|--------------|-----------|-------------|-------------------|-------------|---------------------|-----------------------------|----------------------------------|
| <input type="checkbox"/> | Online | 55 | Selective | Blocked + Allowed | Active | Protected | financeprodcaweb3 | Web Finance Prod CA High |
| <input type="checkbox"/> | Online | 55 | Selective | Blocked + Allowed | Active | Protected | financeprodcaweb2 | Web Finance Prod CA High |
| <input type="checkbox"/> | Online | 11 | Selective | Blocked + Allowed | Active | Protected | financeprodcaproc3 | Proc Finance Prod CA High |
| <input type="checkbox"/> | Online | 6.7 | Selective | Blocked + Allowed | Active | Protected | financeprodcaproc2 | Proc Finance Prod CA High |
| <input type="checkbox"/> | Online | 5 | Selective | Blocked + Allowed | Active | Protected | financeprodcaweb1 | Web Finance Prod CA High |
| <input type="checkbox"/> | Online | 5 | Selective | Blocked + Allowed | Active | Protected | financeprodcadb2 | DB Finance Prod CA High |
| <input type="checkbox"/> | Online | 2.8 | Selective | Blocked + Allowed | Active | Protected | financeprodcaproc1 | Proc Finance Prod CA High |
| <input type="checkbox"/> | Online | 2.2 | Selective | Blocked + Allowed | Active | Protected | financeprodcadb1 | DB Finance Prod CA High |
| <input type="checkbox"/> | Online | | Selective | Blocked + Allowed | Active | | Win-endpoint-6 | Workstations Users VDI Endpoints |
| <input type="checkbox"/> | Online | | Selective | Blocked + Allowed | Active | | Win-endpoint-1 | Workstations Users VDI Endpoints |
| <input type="checkbox"/> | Online | | Selective | Blocked + Allowed | Active | Critical | financedevawsdb2 | DB Finance Dev AWS |
| <input type="checkbox"/> | Online | | Selective | Blocked + Allowed | Active | Critical | ticketsprodazuredb1 | DB Tickets Prod Azure |
| <input type="checkbox"/> | Online | | Selective | Blocked + Allowed | Active | Critical | ticketsprodazureweb1 | Web Tickets Prod Azure |
| <input type="checkbox"/> | Online | | Selective | Blocked + Allowed | Active | Critical | usersprodsingaporeuserdesk1 | UserDesk Users Prod Singapore |

Map – Single Pane of Glass - Servers | Endpoints | Containers | Cloud

Source ↕ Destination Service

Time: Last 24 Hours ▾ More ▾ 

Group by Data Center Type × L: Locations × E: Environments × A: Applications × R: Roles × ▾

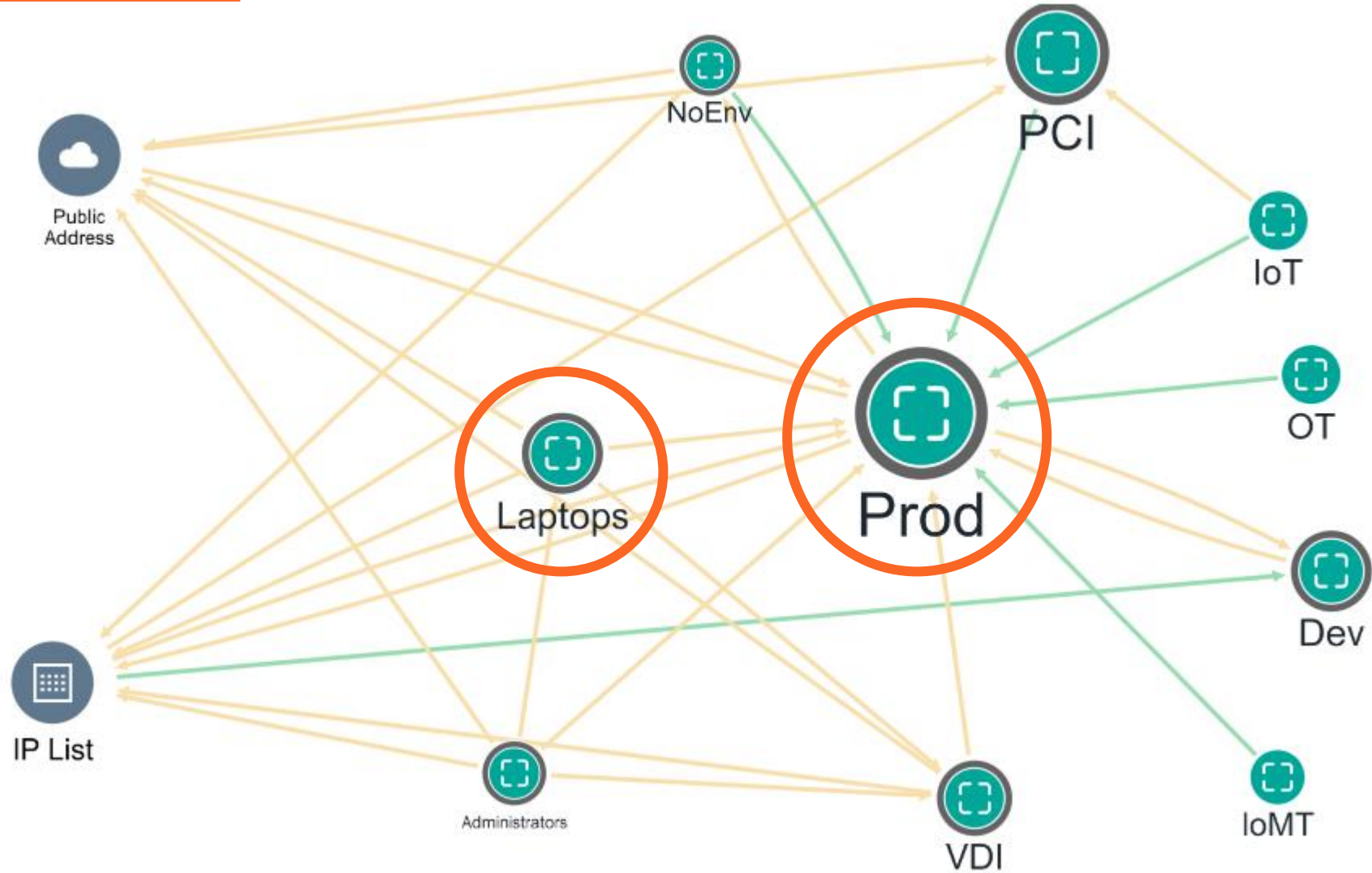


A vertical toolbar on the left side of the map contains several icons for navigation and interaction, including a list icon (iii), a search icon, a refresh icon, a back icon, a forward icon, a zoom in icon, a zoom out icon, a location pin icon, and a home icon.

Map – Single Pane of Glass - Servers | Endpoints | Containers | Cloud

Group by Environments x v

Policy Data v



Map

Source [] Destination [] Service []

Time: Last Month More

Clear Filters Save Filter Time: Last Month Run Load Results

Group by Applications

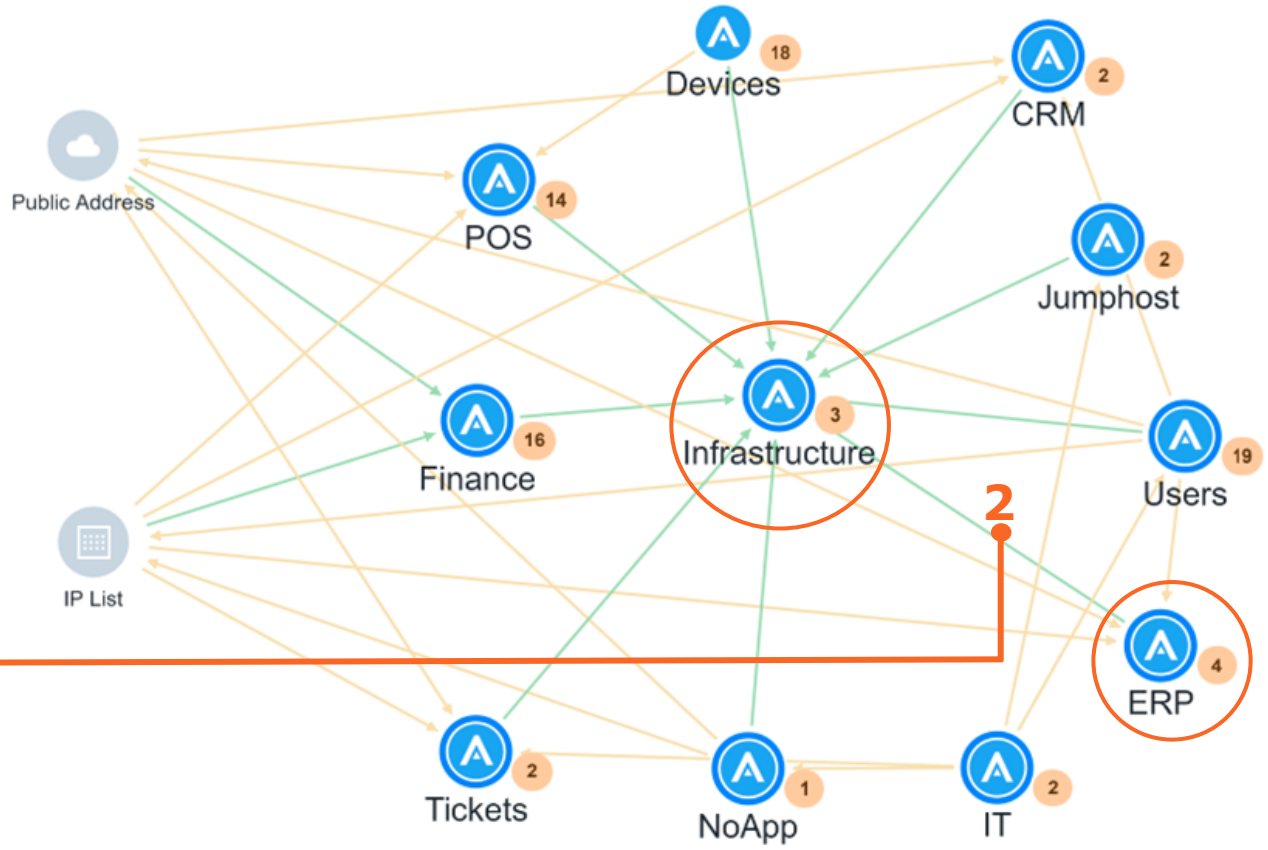
ERP
Infrastructure

Services:
389 UDP
389 TCP
88 TCP
123 UDP

Double-click to expand

Circular Layout All Draft Legend 1

Timestamp: 07/14/2023, 11:26:44 Connections: 1 - 1,086 of 1,086



2023 Gartner Market Guide for Microsegmentation

Zero Trust, risk of lateral movement and hybrid environments are **driving adoption**.

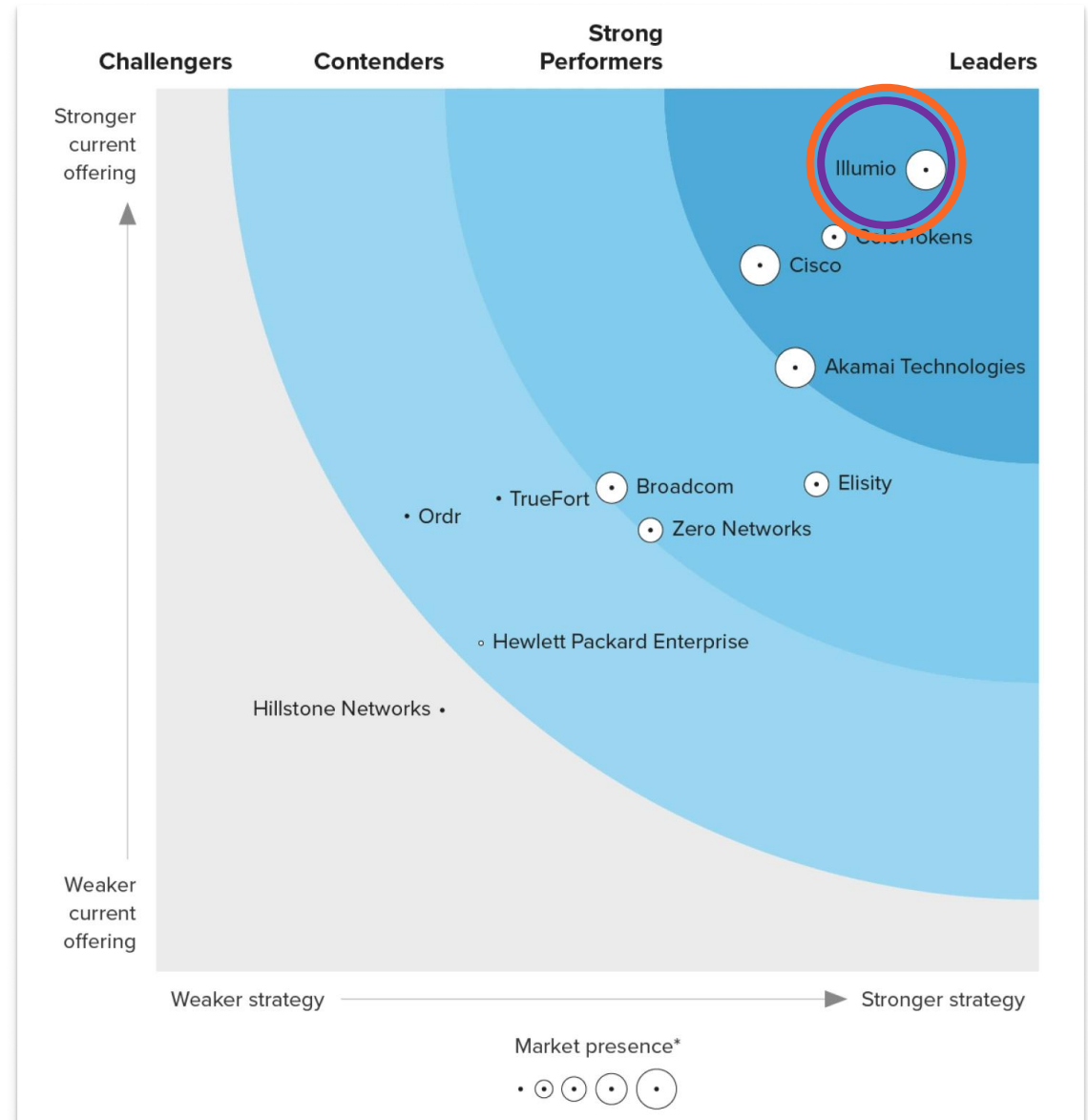
Gartner sees interest across **all verticals, geographies, and company sizes**.

Source: Gartner Market Guide for Microsegmentation

The Gartner logo is displayed in white text on a dark background. The background features a complex geometric pattern of overlapping squares and rectangles in shades of teal, grey, and black, with some areas having diagonal hatching. There are also several stylized corner brackets in orange and white scattered across the background.

Illumio Named a 2024 Forrester Wave Leader in Microsegmentation

The Forrester Wave™:
Microsegmentation Solutions, Q3 2024



Seg

men

tat

ion



illumio

The Zero Trust
Segmentation Company





Thank you

