illumio

# 隨著 AI 的日益普及,如何使用 Zero Trust 網路來提高網路彈性

Louis Cheung

Sr. Regional Systems Engineer

CISSP CISA CCSP CKA

Apr 2025

# 開放風險導致攻撃成功！


OT and IoT
Cloud Services
Home Office
IoT Device
SaaS Apps
Company-owned Device
Partners
Customers
Partner Device
Identities
On-premises
Remote Employees
Personal Device
Multicloud

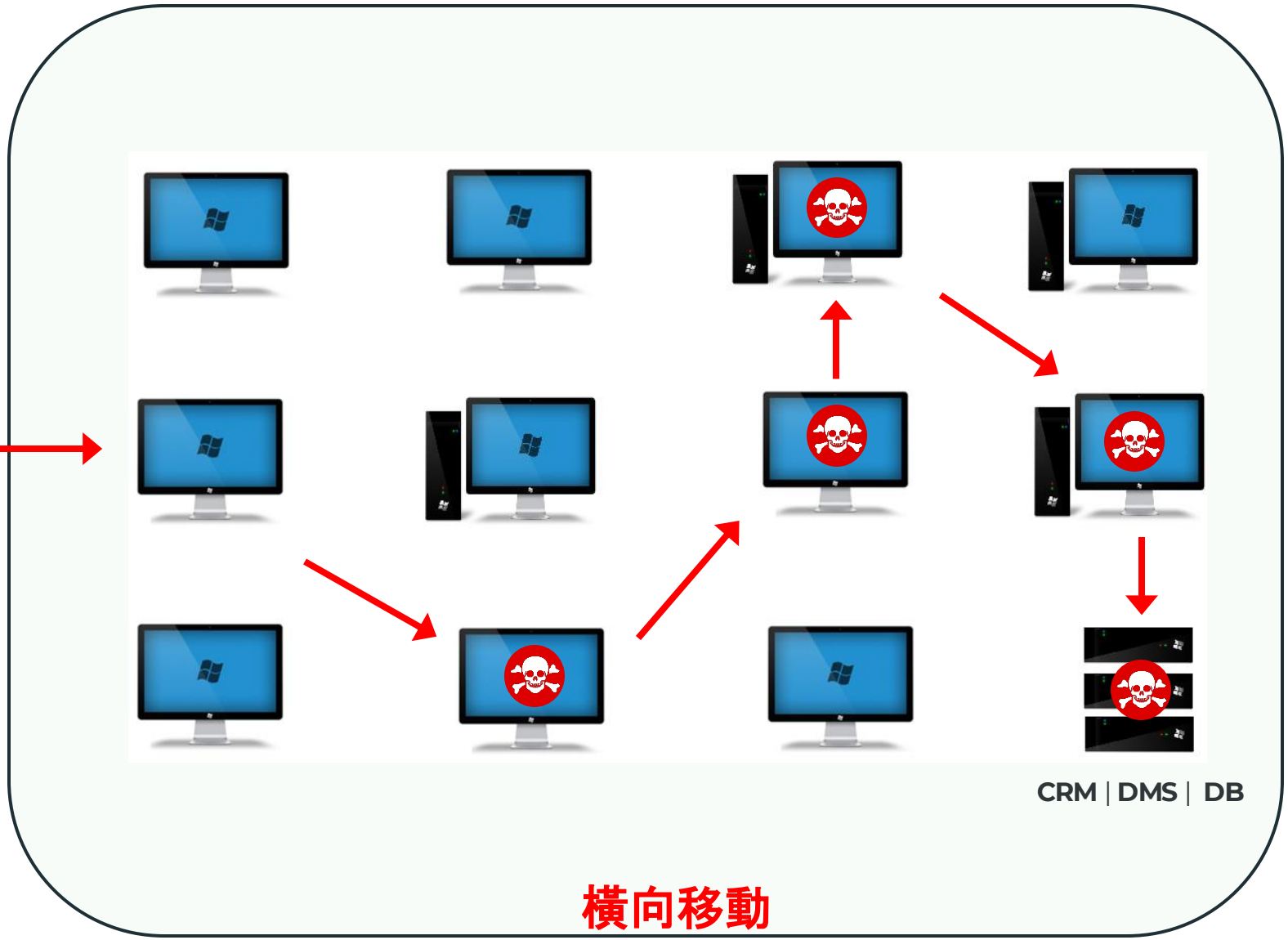
大多數攻擊都是從

**零號帶原者！**


攻擊的成功

在於其

**傳播能力...**



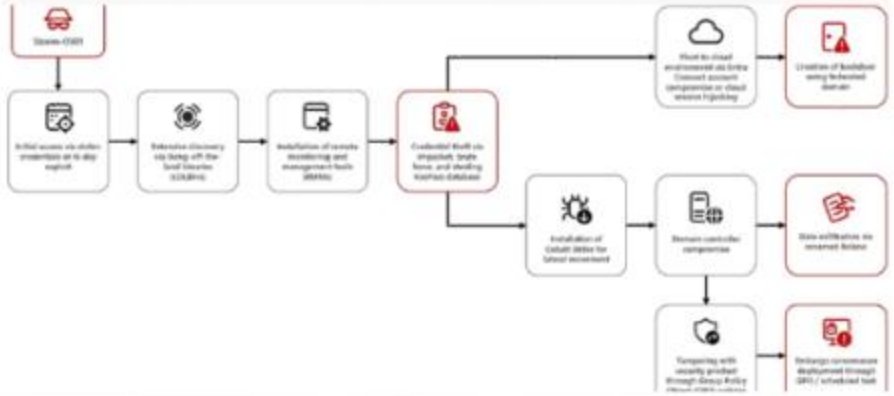
新聞

# 駭客組織Storm-0501偷走憑證攻入Entra ID，橫向移動範圍從內部跨至雲端

破壞混合雲環境的安全，針對駭客組織Storm-0501從事勒索軟體攻擊，最近出現新的攻擊手法，過程中藉由Entra ID（原Azure AD）橫向移動到雲端環境並植入後門，以便持續存取受害組織內部網路

讚 6 分享

文/ 周峻佑 | 2024-10-01 發表



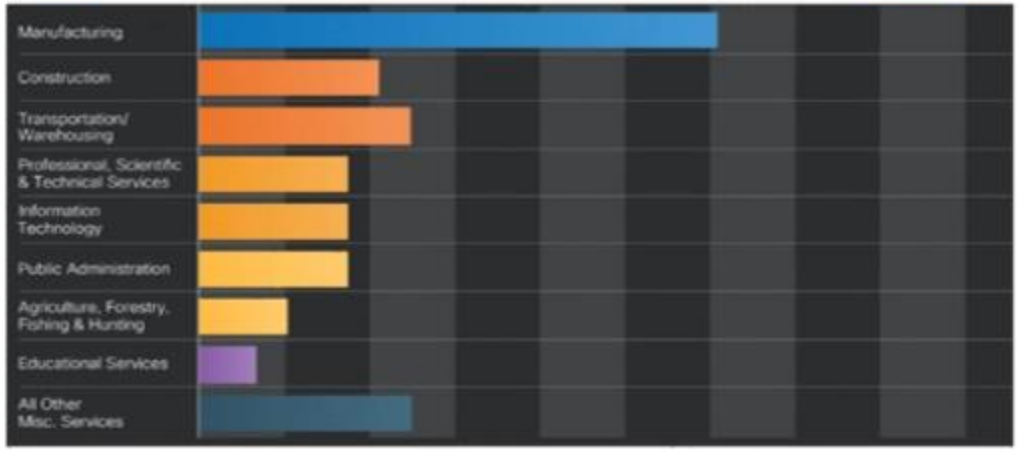
新聞

# 勒索軟體BlackByte利用VMware虛擬化平臺漏洞發動攻擊

研究人員發現，勒索軟體駭客組織BlackByte在攻擊行動裡，利用2個月前VMware修補的身分驗證漏洞CVE-2024-37085，以便控制ESXi虛擬化平臺

文/ 周峻佑 | 2024-08-29 發表

讚 12 分享





*CISO 面臨的挑戰是企業級環境容易受到網路橫向移動的影響。Attivo Networks 首席安全倡導者兼 CMO Carolyn Crandall 表示，大多數 CISO 都熟悉橫向移動在攻擊中的作用，但組織需要以行動來支援這些知識。*

這些駭客利用SMB及RDP這兩個遠端存取管道，進入受害組織的其他系統、資料夾及檔案，並透過NTLM進行身分驗證。他們也藉由竄改系統登錄檔，或是手動從重要系統移除EDR系統的方式，來降低受害組織的資安防護強度，其中1起事故駭客甚至竄改ESXi主機的root密碼。

值得留意的是，這些駭客除了利用上述漏洞，攻擊手法也出現變化，首先，是勒索軟體在啟動的過程中，會一口氣部署4個用於自帶驅動程式（BYOVD）攻擊的驅動程式，這些元件來自微星系統超頻工具Afterburner、Dell用戶端韌體更新工具、技嘉主機板公用程式，以及防毒軟體Zemana。這些駭客並非首度濫用合法驅動程式，但研究人員指出，過往這些駭客只會運用2至3支驅動程式。

illumio

# AI 放大了風險

July 傑立資訊

2023 年 | 08 月 | 15 日

# 資安專家警告：駭客已經盯上 ChatGPT，連不會 coding 的壞傢伙都能用它發動網路攻擊 [轉載自科技報橘]

# 資安小貼士：提防假冒ChatGPT應用程式及釣魚網頁

人工智能聊天機器人ChatGPT在2022年11月推出後短短兩個月便獲得1億用戶垂青，最近更推出一項名為ChatGPT Plus的付費訂閱服務。不幸的是，黑客亦借此機會，通過提供虛假的應用程式或免費使用高級服務作招徠，誘使用戶下載惡意軟件或分享敏感資訊。

發佈日期: 2023年02月28日 | 4377 觀看次數

## AI 面臨的風險

### ChatGPT 插件中發現巨大安全漏洞後發出警告

**Warning After Huge Security Flaws Found in ChatGPT Plugins**

The security of OpenAI's GPT store is thrown into doubt after researchers find vulnerabilities that could lead to data loss.

Written by nicholas fearn

Published on March 14, 2024


## AI 帶來的風險

### AI 產生的虛假 Github 儲存庫竊取登入憑證

**AI-Generated Fake GitHub Repositories Steal Login Credentials**

AI | Cyber Security News | Malware

PUBLISHED ON MARCH 11, 2025 BY DIVYA

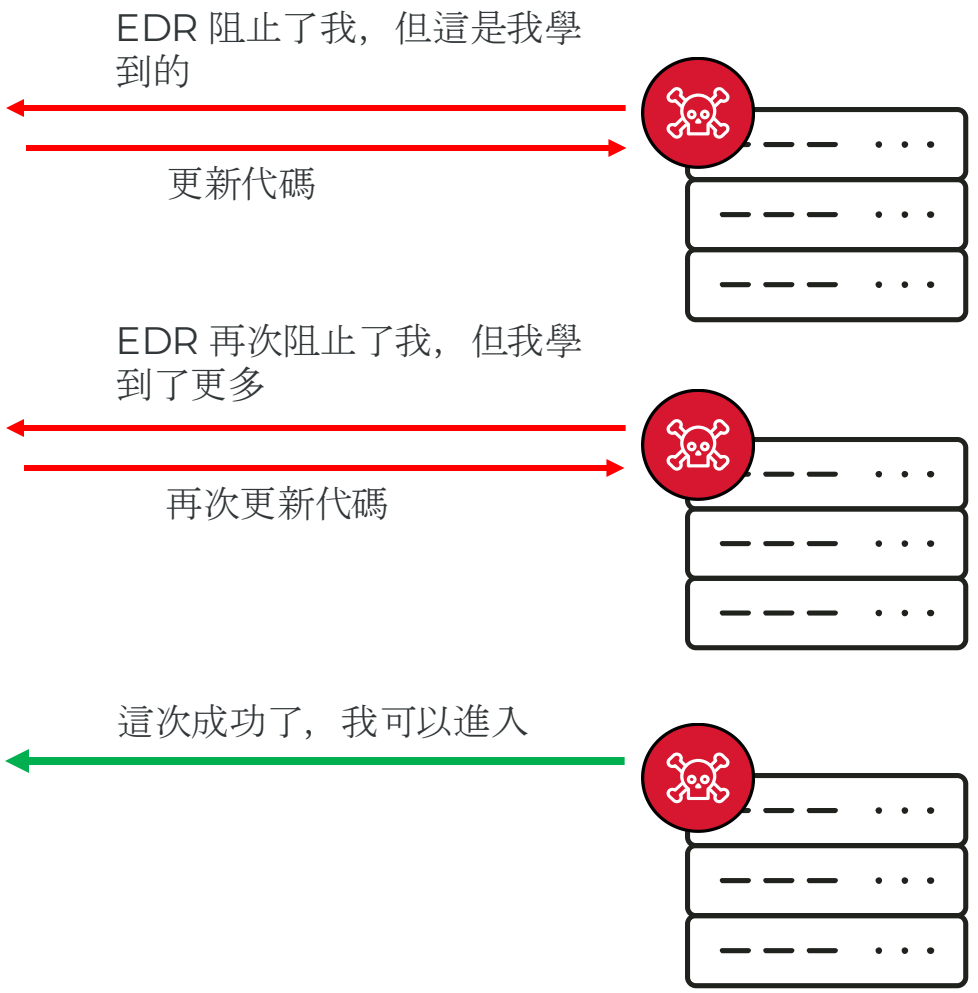

A concerning cybersecurity threat has emerged with the discovery of AI-generated fake GitHub repositories designed to distribute malware, including the notorious SmartLoader and Lumma Stealer.


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.

# 即時變形可能性


EDR 阻止了我，但這是我學到的
更新代碼
EDR 再次阻止了我，但我學到了更多
再次更新代碼
這次成功了，我可以進入

# 答案不一定是更多的 AI

做好基礎知識：

- 減少學習面
- 控制對資源的訪問
- 遏制攻擊
- 安全恢復

答案是零信任

illumio

# 零信任

一種旨在通過消除數字系統中的**隱式信任**來**阻止數據洩露和防止網路攻擊成功**的策略.

# 深度防禦 Defence In-depth

防止感染開始(**infection start**)的保護措施

和

防止感染傳播 (**infection spreads**)！

壞人總會想辦法進來的！

**因此，每個組織都需要一個網路遏制策略！**

**（網路和運營韌性）**

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

**能夠吸收潛在的中斷，同時繼續滿足服務級別的目標。**

Gartner Cyber Resilience Framework

# 金管會零信任架構實作參考原則分級表 - 網路

| 項次 | 功能 | 原則 | 等級 |
|---|---|---|---|
| 3.1 | 網路區隔 | 具網段隔離機制，採最小需求原則限制存取資源之網路連線，並得限制同網段主機間連線及資源存取，防止攻擊者利用遭入侵的主機作為跳板機進行橫向擴散。 | I |
| 3.2 | 網路區隔 | 具軟體定義網路(SDN)或網路微分段(Micro-Segmentation)機制，可以依據業務需求或動態屬性(如人員身分、設備樣態及連線時間等)調整網路防護邊界；並可以個別主機或個別系統為獨立網路區隔，縮小攻擊表面。 | II |
| 3.3 | 流量管理 | 呈現對系統、端點與網路間連線的相依性關係，可以單一設備為單位延伸看到相關系統、端點與網路之狀態，並具備流量異常監控及應處機制。 | II |
| 3.4 | 流量加密 | 於資源存取路徑之資料傳輸加密(如採https等加密協定)。 | I |
| 3.5 | 網路韌性 | 對網路連線紀錄具有即時偵測及回應機制(如NDR)，可因應業務需求、偵測到入侵指標(IOC)或遭受攻擊時，動態調整網路設定(如調整網路防護邊界即時隔離、切換備援路由或資源配置等)或即時告警，以維持網路服務，將對業務影響最小化 | III |
| 3.6 | 可視性分析 | 整合或收容事件日誌，建立定期審查及異常行為之偵測、告警及回應機制，如集中收容於SIEM平台並與資安監控機制(SOC)整合，針對入侵指標(IOC)或攻擊行為樣態(Mitre ATT&CK TTP)進行即時的判斷與回應(如事件單、SOAR Playbook等)。(參照F-ISAC威脅情資及金融資安監控組態基準) | III |
| 3.7 | 自動化治理 | 具可依資安政策、工作流程情境及網路態勢快速調適之網路管理機制。 | IV |

Source: https://www.fsc.gov.tw

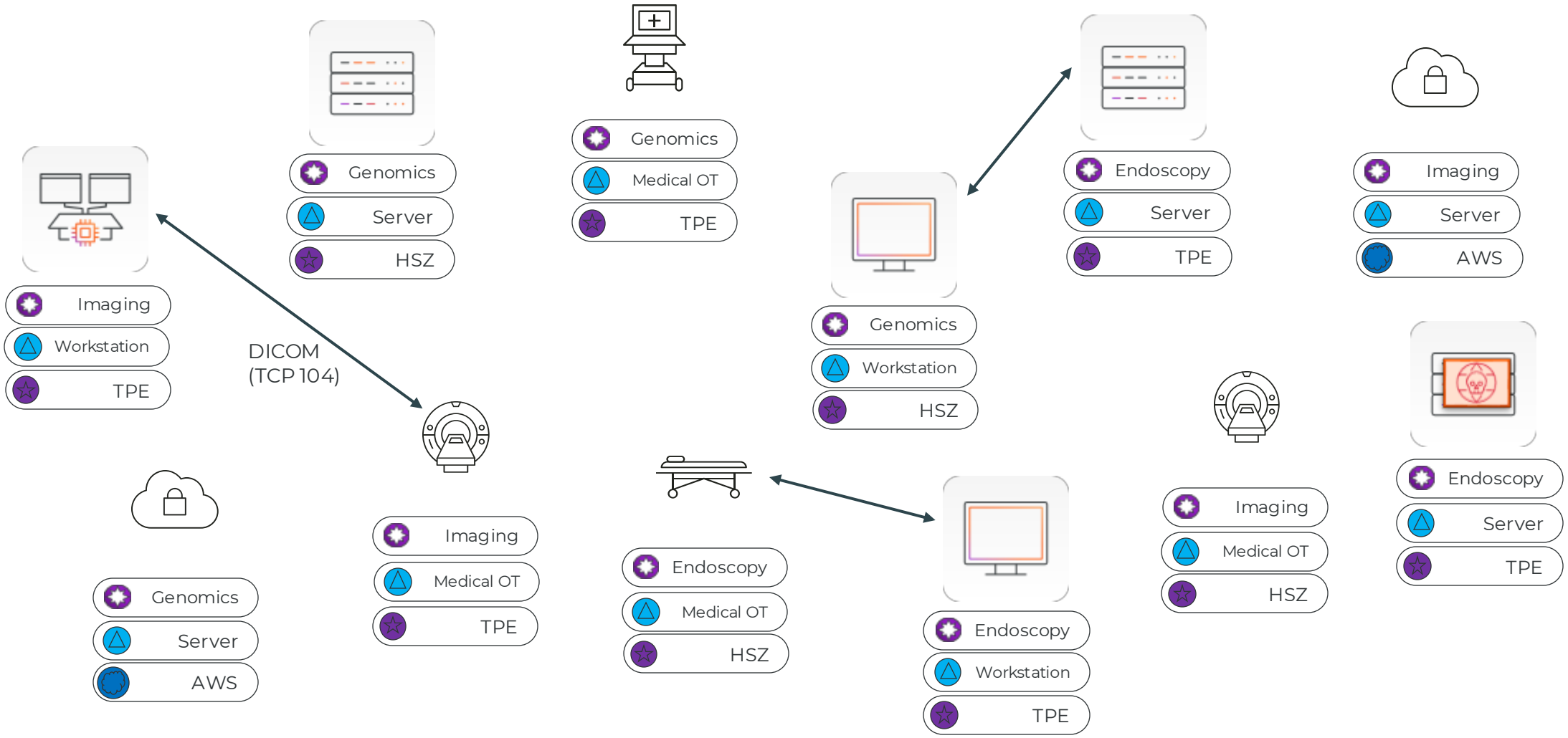
# 遏制策略
# (Containment Strategy)

# Minimum Viable Operation (MVO)

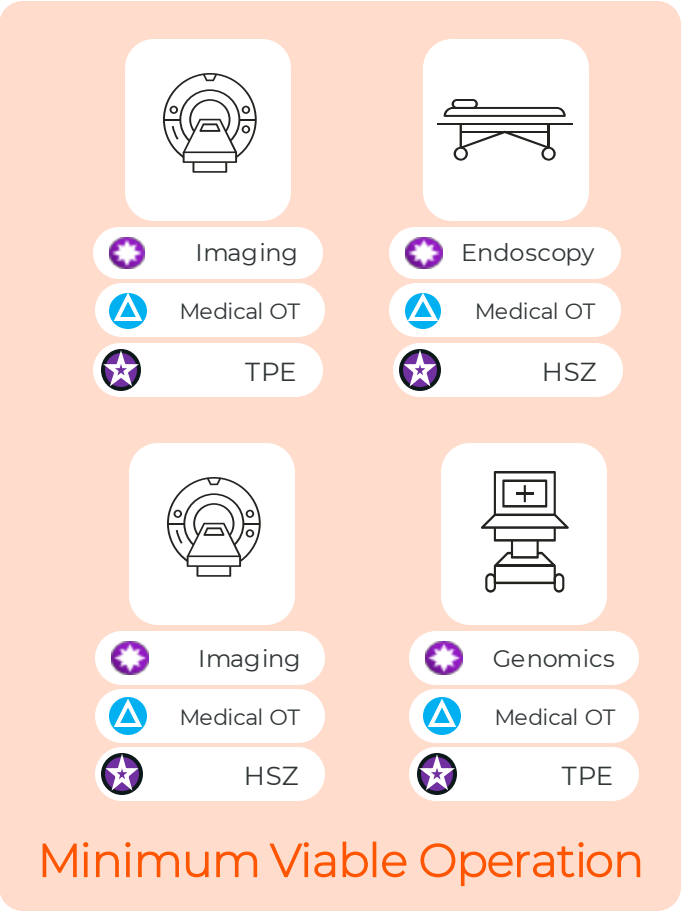
## 最小可行操作

- 企業最低限度的營運
- 這是一組不能失敗的服務，因為失敗將代表可能對社會產生影響的安全關鍵服務

# 識別 - 資產、漏洞和連接


Genomics
Server
HSZ
Genomics
Medical OT
TPE
Endoscopy
Server
TPE
Imaging
Server
AWS
Imaging
Workstation
TPE
DICOM
(TCP 104)
Genomics
Workstation
HSZ
Endoscopy
Server
TPE
Genomics
Server
AWS
Imaging
Medical OT
TPE
Endoscopy
Medical OT
HSZ
Endoscopy
Workstation
TPE
Imaging
Medical OT
HSZ

# 使用 Context 進行保護 - MVO

illumio

# 透過零信任實踐MVO

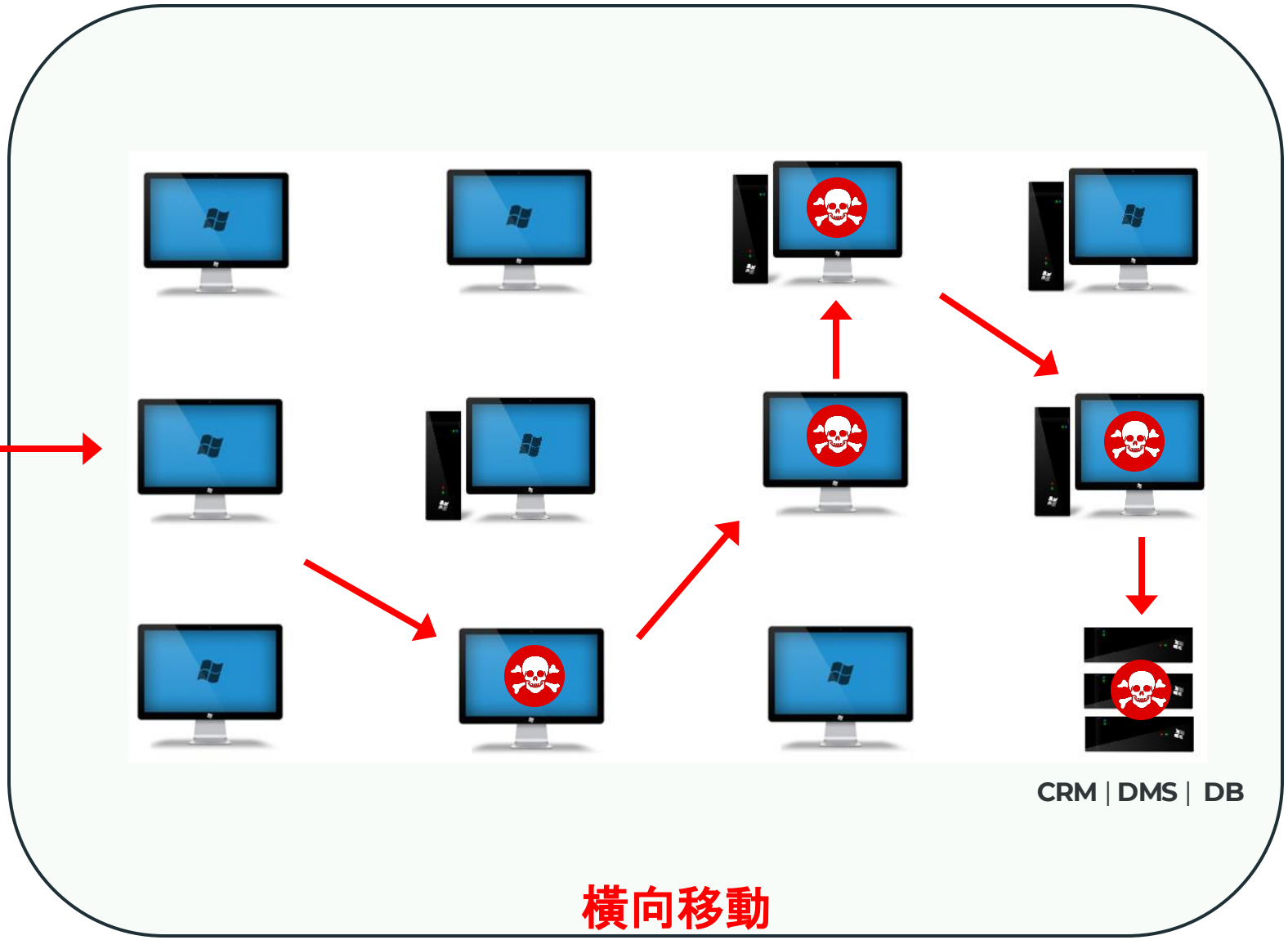
大多數攻擊都是從

**零號帶原者！**


攻擊的成功

在於其

**傳播能力...**



# 零信任微分段

是遏制策略

**停止傳播!**


最小可行操作

CRM | DMS | DB

MVO

Illumio! 停止傳播!

# 微分段平臺是如何做到的?

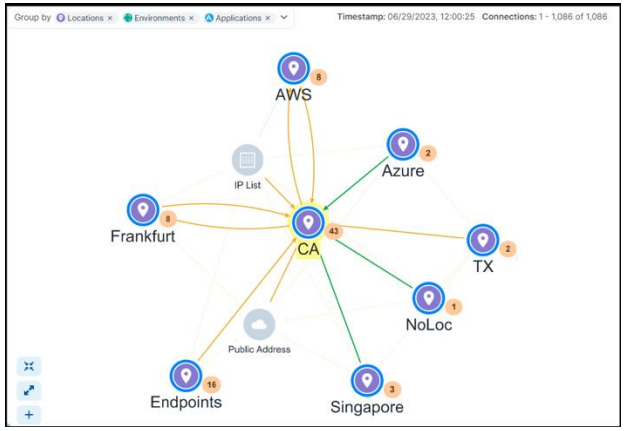
## 識別資產

| 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 |

資產盤點

( 知道你擁有什麼 )

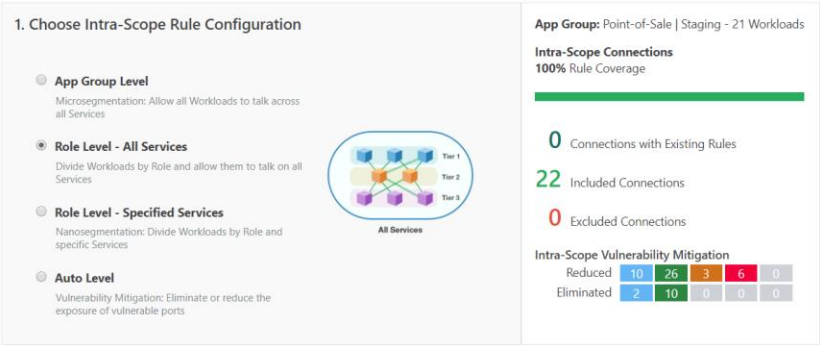
## 見風險




地圖

(了解他們的工作)

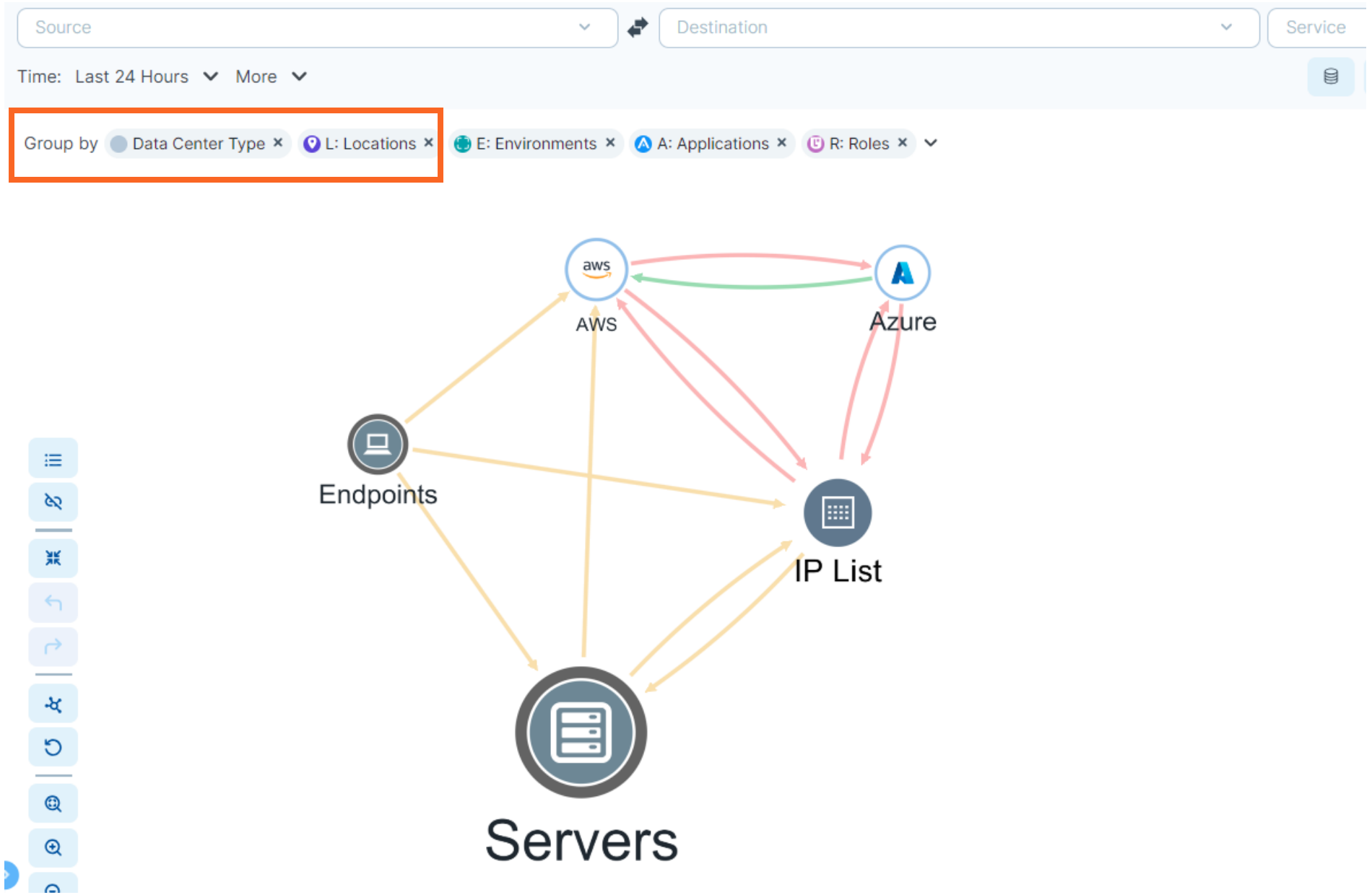
## 遏制風險



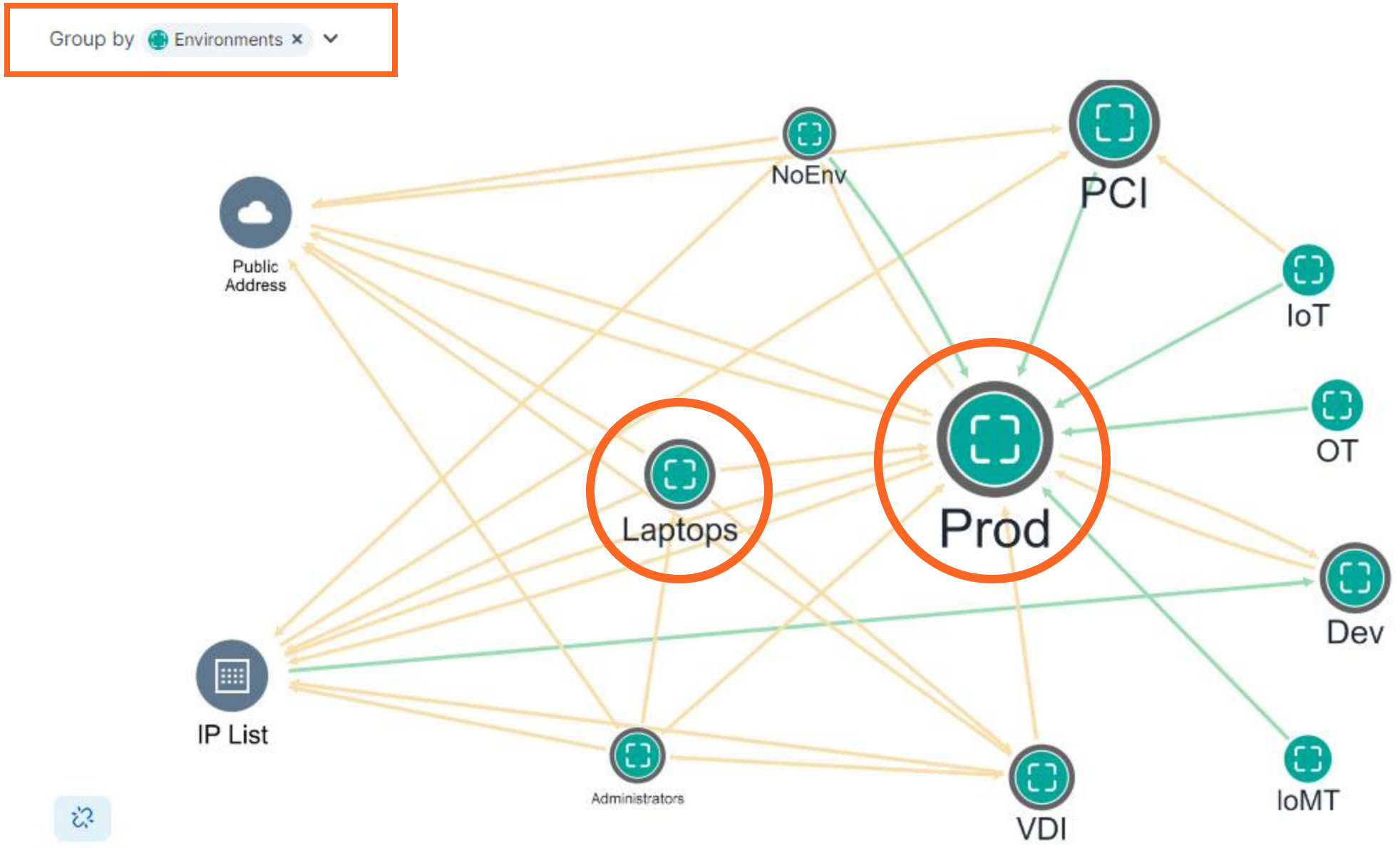

智慧策略

(知道如何保護他們)

# 地圖 – 單一管理平臺 — 伺服器 | 端點 | 容器 | 雲

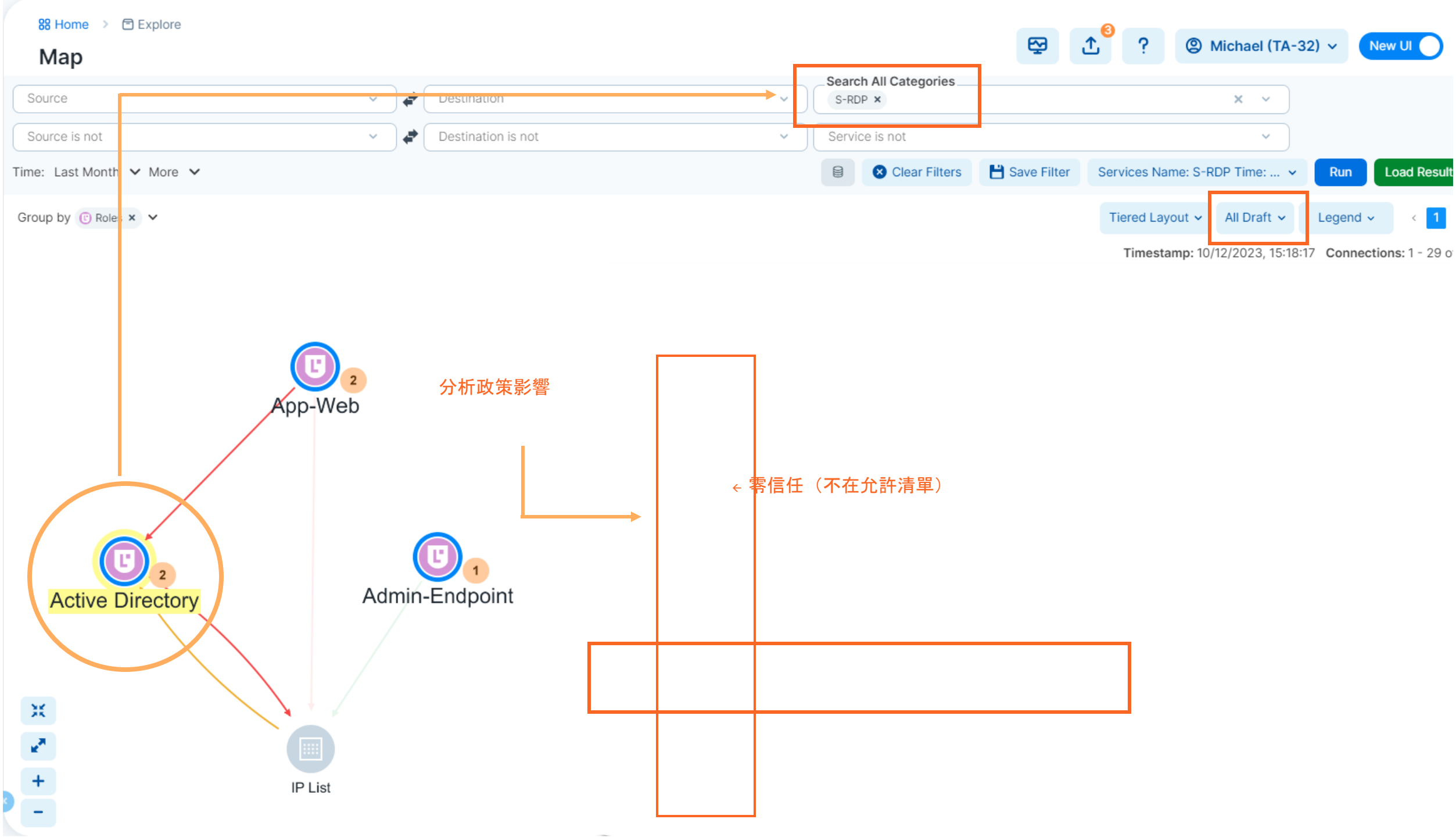


# 地圖 – 單一管理平臺 — 伺服器 | 端點 | 容器 | 雲





Confiden


Home
Explore
Map
Michael (TA-32)
New UI
Source
Destination
Search All Categories
S-RDP
Source is not
Destination is not
Service is not
Time: Last Month
More
Clear Filters
Save Filter
Services Name: S-RDP Time: ...
Run
Load Result
Group by
Tiered Layout
All Draft
Legend
Timestamp: 10/12/2023, 15:18:17
Connections: 1 - 29
App-Web
2
分析政策影響
Active Directory
2
Admin-Endpoint
1
← 零信任（不在允許清單）
IP List

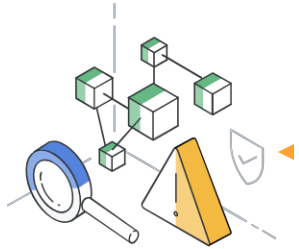
# 檢測 – 更快檢測到攻擊


偵察

偵察

偵察

可疑系統
- EDR/MDR
- 隔離

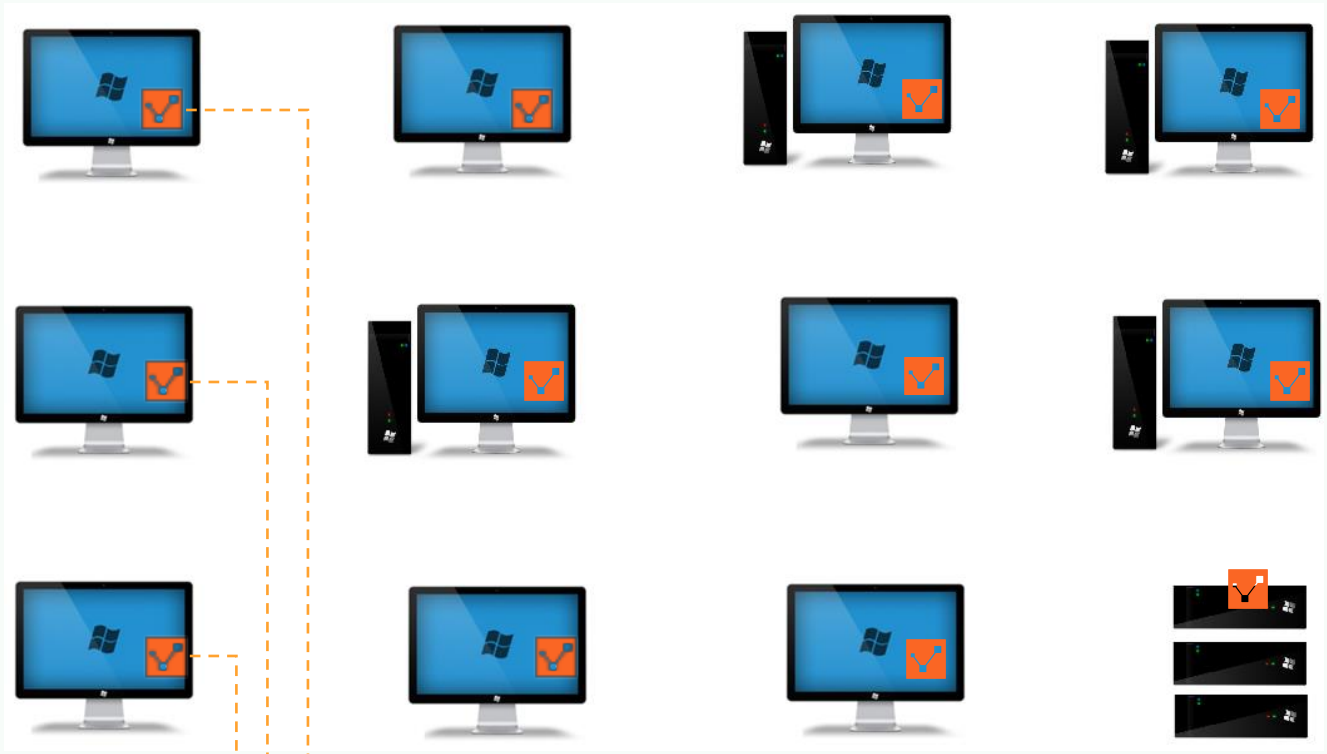


日誌

日誌

SIEM/SOAR工具

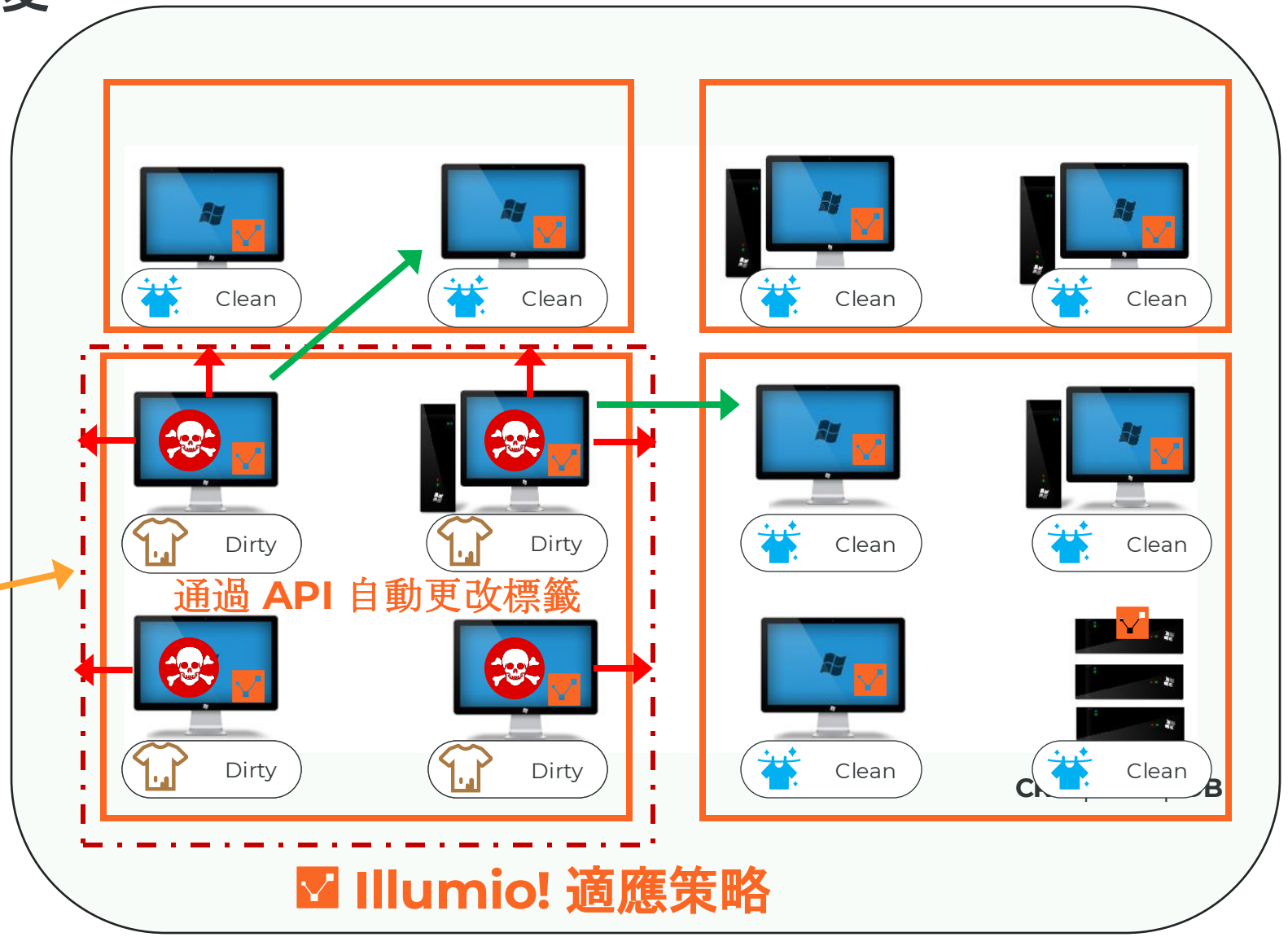
Illumio策略計算引擎 (PCE)



CRM | DMS | DB

Illumio 監控網路流量

# 安全事件應變 - 安全恢復

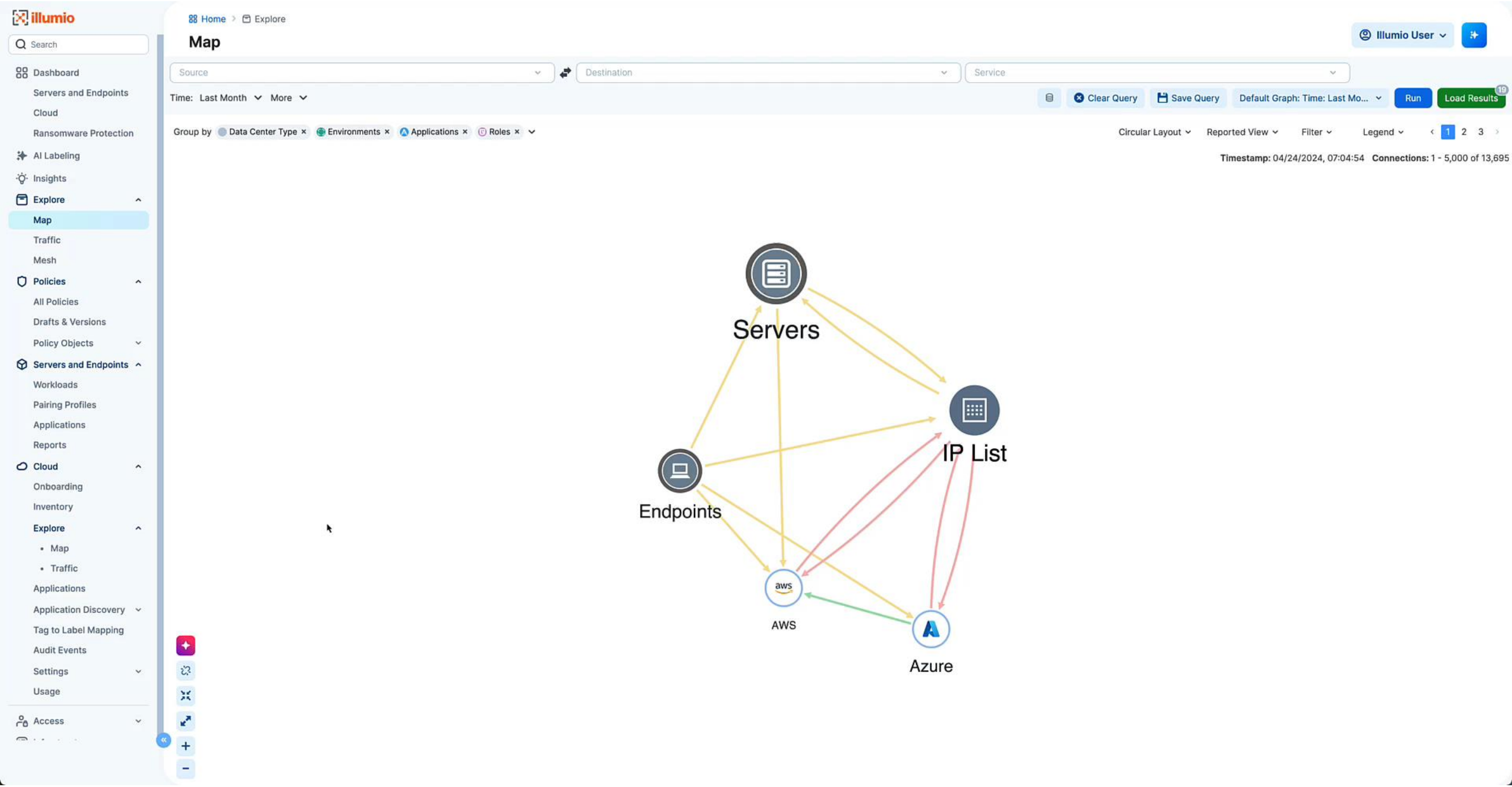



備份

取證分析

illumio

# Illumio如何使用 AI


illumio
Search
Dashboard
Servers and Endpoints
Cloud
Ransomware Protection
AI Labeling
Insights
Explore
Map
Traffic
Mesh
Policies
All Policies
Drafts & Versions
Policy Objects
Servers and Endpoints
Workloads
Pairing Profiles
Applications
Reports
Cloud
Onboarding
Inventory
Explore
Map
Traffic
Applications
Application Discovery
Tag to Label Mapping
Audit Events
Settings
Usage
Access
Home
Explore
Map
Illumio User
Source
Destination
Service
Time: Last Month
More
Clear Query
Save Query
Default Graph: Time: Last Mo...
Run
Load Results
19
Group by
Data Center Type
Environments
Applications
Roles
Circular Layout
Reported View
Filter
Legend
1
2
3
Timestamp: 04/24/2024, 07:04:54
Connections: 1 - 5,000 of 13,695
Servers
IP List
Endpoints
aws
AWS
Azure

illumio

Home / Insights

# Malicious IP Threats

Search ⌘ K

Inbound | Outbound | Last 24 hours compared to Previous 24 hours

- Dashboard
  - Servers & Endpoints
  - Cloud
  - Ransomware Protecti...
- Insights NEW
  - Insights Hub
  - Risky Traffic
  - Malicious IP Threats
  - Known and Unknown I...
  - Cross Account Traffic
  - Traffic to Country
  - Cloud Configurations
  - Shadow LLMs
  - Resource Traffic
- Explore
- Policies
- Servers & Endpoints
- Cloud
- Access
- Infrastructure
- Settings
- Troubleshoot
- Support

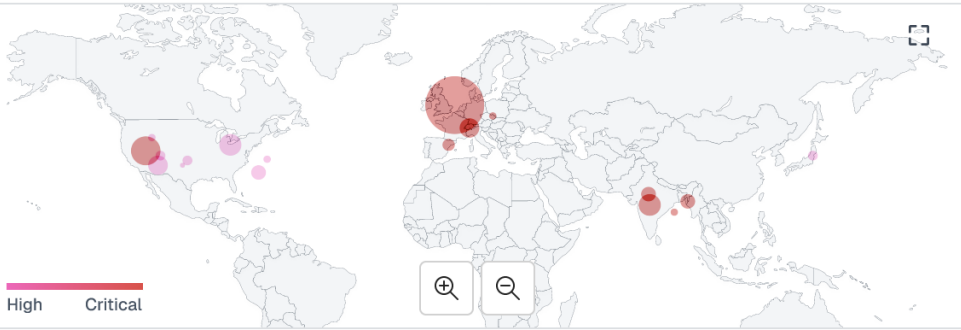
## Top 10 Malicious IPs

Flows | Bytes

| | |
|---|---|
| 89.45.32.111 | 2.3K ↓10 |
| 179.60.123.45 | 2.1K ↓2 |
| 102.133.44.56 | 1.9K ↓4 |
| 182.75.33.20 | 1.6K ↓20 |
| 45.227.252.88 | 1.6K ↓8 |
| 203.0.113.5 | 1.4K ↓10 |
| 91.200.12.77 | 1.2K ↓10 |

## Global Threat Map

Flows | Bytes




Top 3 Countries: UK 23K | USA 20K | India 12K

## Top 10 Subscriptions with Malicious IP Flows

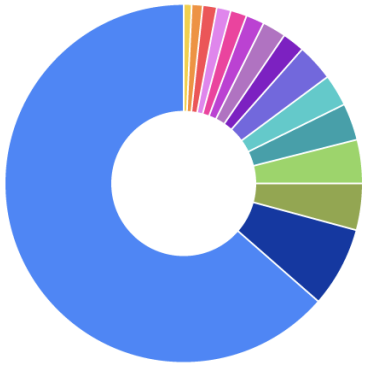
Flows | Bytes

| | |
|---|---|
| 012345678901 | 175K ↓1K |
| aws-org-0011223344 | 67K ↓500 |
| aws-id-098765432123 | 50K ↓1K |
| account-id-654321789012 | 40K ↓30 |
| azure-tenant-abcdef123456 | 32K ↓20 |

| Subscriptions | From External IPs | | Flows Now | Flows Prev | Δ Flows |
|---|---|---|---|---|---|
| 012345678... | 167.94.146.20 | +3 | 52 GB | 54 GB | ↑ 2 GB |

## Top 15 Roles Communicating with Malicious IPs

Flows | Bytes



- 850K GlobalCatalog
- 100K LDAP
- 70K NetBackup
- 68K Mcafee
- 65K Trendmicro
- 50K MongoDB
- 49K Commvault
- 47K iSCSI
- 45K Zabbix
- 43K DomainController
- 42K SAP Hana
- 30K Teradata
- 29K NFS
- 22K Puppet
- 18K Solr

## Top 10 Malicious Ports & Protocols

Flows | Bytes

# Shadow LLMs

Last 24 hours compared to Previous 24 hours

Dashboard
Servers & Endpoints
Cloud
Ransomware Protecti...
Insights NEW
Insights Hub
Risky Traffic
Malicious IP Threats
Known and Unknown I...
Cross Account Traffic
Traffic to Country
Cloud Configurations
Shadow LLMs
Resource Traffic
Explore
Policies
Servers & Endpoints
Cloud
Access
Infrastructure
Settings
Troubleshoot
Support

## LLMs in Use

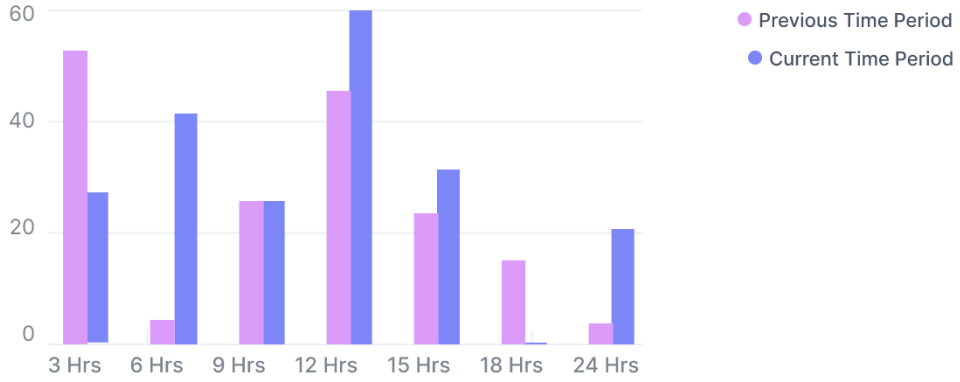
Search

Show All Data

| LLM | Flows Now | Flows Prev | Bytes Now | Bytes Prev | Δ F |
|---|---|---|---|---|---|
| DeepSeek | 13.79K | 13.79K | 52 GB | 52 GB | ↓ |
| ChatGPT | 5.66K | 5.66K | 1.45 GB | 1.45 GB | ↓ |
| Anthropic | 1.08K | 1.08K | 20 MB | 20 MB | ↓ |
| Mosaic | 202 | 202 | 55.09 KB | 55.09 KB | ↓ |
| Meta | 343 | 343 | 33 KB | 33 KB | ↓ |
| Gemini | 800k | 800k | 29.02 KB | 29.02 KB | ↓ |

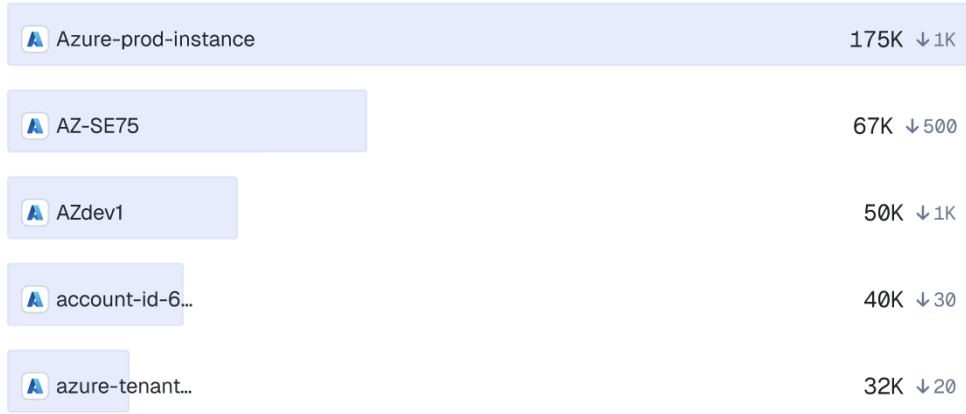
## Number of Workloads using LLMs

Search




## Top 5 Subscriptions with LLM Usage

Flows Bytes




| Source | Destination LLM | Flows | Flows | Bytes | Bytes |
|---|---|---|---|---|---|
| Azure-prod-instance | | 15.79K | NEW | 54 GB | |
| AZ-SE75 | | 15.66K | NEW | 1.45 GB | |
| AZDev1 | | 10K | NEW | 54 GB | |
| | ChatGPT | 6K | ↓ 3% | 60 TB | ↓ 34.4 |
| | DeepSeek | 2K | NEW | 54 GB | |
| account-id-654321 | | 5.66 | NEW | 1.45 GB | |
| Azure-tenant-abcde | | 5.66 | NEW | 1.45 GB | |

## Top 15 Sources communicating with LLMs

Flows Bytes

illumio

# “組織終於開始認真對待零信任...[並且] 他們都在使用微分段進行零信任”

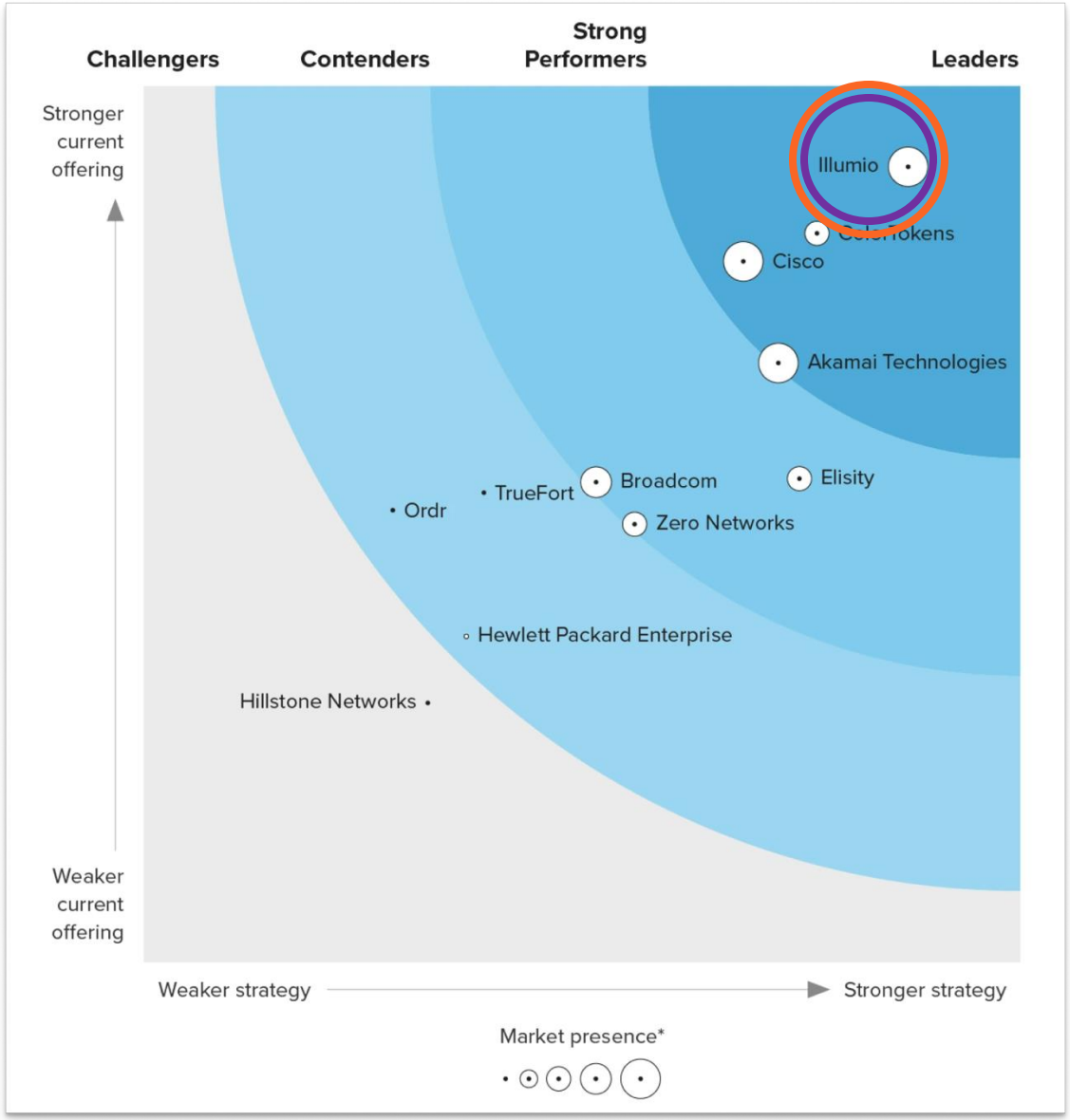
FORRESTER®

**The Microsegmentation Solutions Landscape, Q2 2024**

**By David Holmes with Joseph Blankenship, Lok Sze Sung, Michael Belden**

# Illumio 被評為 2024 年 Forrester Wave 微分段領導者!

**The Forrester Wave™:**
**Microsegmentation Solutions, Q3 2024**



# 微 分 段