GSS 叡揚資訊
Galaxy Software Services

DevSecOps

全方位應用程式安全解決方案

illumio

illumio

零信任網路微切分

防火牆隔離的方式來保護網路，其實不如您想像的可靠

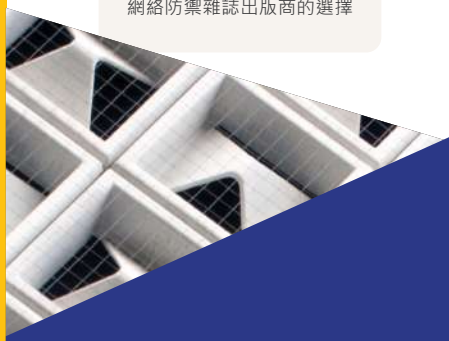
Forrester New Wave™
評為微分段領導者

被評為 2022 年 Gartner®
最酷供應商

CRN 科技創新獎

RemoteTech 突破獎

網絡防禦雜誌出版商的選擇



illumio – 零信任網路微切分解決方案

The Forrester New Wave™: Microsegmentation, Q1 2022

The Forrester Wave™ for Zero Trust eXtended Ecosystem Platform Providers, Q3 2020

Gartner
COOL VENDOR 2022
Illumio Named a 2022 Gartner® Cool Vendor

Gartner Peer Insights.
4.5

面對日新月異的資安威脅，傳統防火牆的防護模式，真的能安心嗎？

您只用防火牆隔離的方式來保護網路嗎？防火牆是網路安全中的一種基礎設施，它通常用於阻止未經授權的訪問和保護南北向的網路免受攻擊。但是，只有防火牆是不足以實現完全的零信任架構的。這是因為防火牆不容易達成與控管東西向的防護，一旦位於所謂「信任區域」的主機遭受入侵，Data Center 也會隨之遭殃。然而，零信任架構是將所有主機都視為直接面對不安全的網際網路，因此整個網路都有可能受到威脅和惡意攻擊的影響。

攻擊的速度、蔓延和數量正在增加風險

- 76% 的組織在過去兩年中受到勒索軟體的攻擊
- 63% 在過去一年中遭到破壞
- 識別違規行為平均需要 212 天
  控制違規行為平均需要 75 天
- 企業平均花 37 天和花費 240 萬美元（中位數）
  來查找違規行為並從中恢復

據微軟統計，近 97% 的勒索軟體感染在不到四個小時內就能成功滲透到目標中。最快的更可以在不到 45 分鐘的時間內接管系統。

實現零信任「永不信任，一律驗證」

零信任會依循「實踐網路最小連線存取及預設不信任」的原則，並運用其他多項網路安全性方法，包括網路分段和嚴謹的存取控制。在零信任網路裡，網路安全的重心不再是建立圍牆和防禦線，而是通過多種安全控制機制來保護網路中的每一個資源，從而確保網路安全。這些安全控制機制包括多因素身份驗證、存取控制、網路分段、加密和審計等。

1 預設所有的行為都不可信任

企業應該假設惡意程式可能存在網路中，朝向如何預防、阻止橫向擴散（竊取或破壞更多資料）至關重要。

2 持續監控

以零信任的模式為基礎，可視化企業中所有的連線狀態。

在所有連線建立前，檢視行為是否可被信任。

3 落實最低權限存取

避免系統橫向連線處於寬鬆開放狀態，僅在系統功能必要時才放行連線。

產品介紹

Illumio 於 2013 年創立於美國加州桑尼維爾市，是一家專注於零信任安全的公司，其宗旨是安全應該成為傳統資料中心和公有雲中敏捷計算的推動者。

Illumio 從資安和資訊領域的各個領袖中挖掘菁英，包括 Cisco、Juniper、VMware、Nicira、McAfee、Fortify 和 Riverbed，結合產業中豐富的知識和良好的業績記錄，使 Illumio 成為雲端和資料中心安全的新基礎；並在 2020Q3、2022Q1 年榮獲 Forrester Leader 象限、Gartner Peer Insights 獲得 4.5 顆星的高分（滿分 5 星）。

Illumio 身為 Zero Trust Security Solution 的市場領導者，提供平臺全年無休的安全監控並防護每個工作單元或應用，以阻止橫向移動 - 防止漏洞在任何資料中心或雲端的裸機、VM 和 Container 上蔓延。

Illumio 是實現零信任安全的理想選擇，採用微切分技術，可以讓企業保護其網路免受網路攻擊和資料洩露的威脅，同時提高網路的可見性和可管理性。

利用微切分（Segmentation）將安全嵌入系統作業之中

微切分是一種提升現有網路安全的技術，可以將網路中的應用程式和服務切分成小的、可管理的部分，以提高網路安全性。這種技術利用了網路分段的概念，將網路中的應用程式和服務劃分為更小的子網，從而降低了網路攻擊的風險。這有助於企業提高其網路安全性，保護其網路免受網路攻擊和資料洩露的威脅。

Illumio 實現零信任

部署迅速

illumio 能在數天或數週的時間內完成企業零信任的環境部署。

支援廣泛

illumio 支援多種作業系統，其 Policy 可以輕鬆的套用在數十萬個端點中，管理超過上百萬條連線。

簡易管理

illumio 不但簡化許多 Policy 的設定工作，還能自動根據當前環境提供設定建議，輕鬆完成 Policy 的管理、發佈與套用。

穩定、輕量化

illumio 重視系統的穩定性，所以將代理程式極度輕量化，確保系統的運作不受影響。

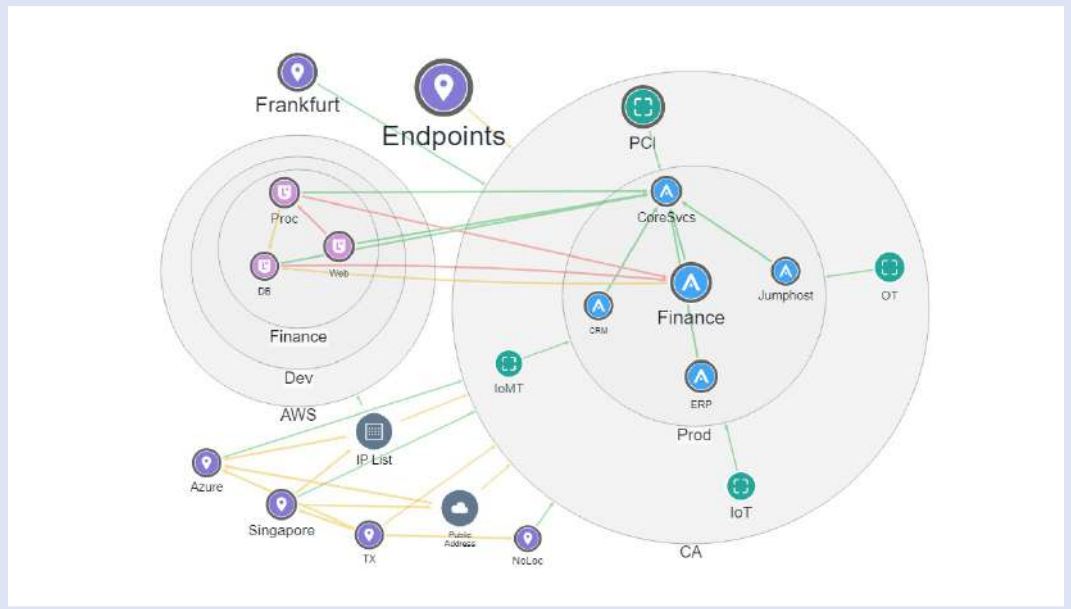
自然語言標籤

從區域 (TW/US)、環境 (正式區 / 測試區)、應用程式 (HRM/CRM) 等到最小維度的 "port"，illumio 可以在各層級執行微切分部署。

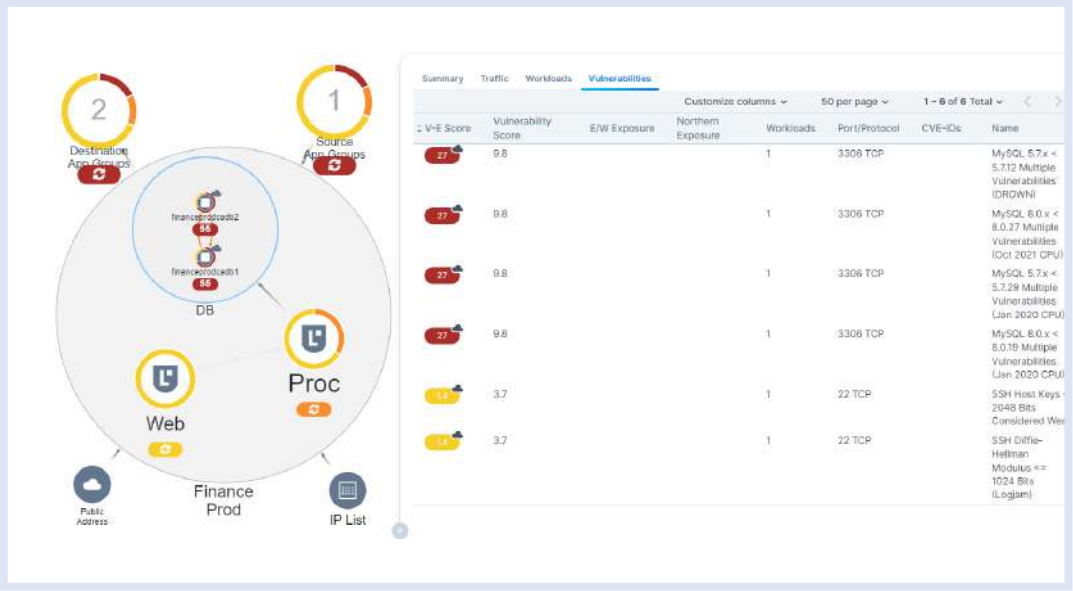
高穩定度

illumio 已在各行各業的環境中實踐微切分部署，導入效益經過許多客戶的驗證與肯定。

▲ 可視化看到不同區域之主機數量



▲ Illumio 可視化地圖中清楚顯示放行 (綠色線) 與禁止 (紅色線) 的連線狀態，
並可預判完全模式下會禁止的連線狀態 (黃色線)



▲ 整合主機弱點報告，將已知風險的連線可視化，可以優先進行阻絕高風險連線的主機 (額外授權)

零信任網路統一管理平台

微切分是一種提升現有網路安全的技術，可以將網路中的應用程式和服務切分成小的、可管理的部分，以提高網路安全性。這種技術利用了網路分段的概念，將網路中的應用程式和服務劃分為更小的子網，從而降低了網路攻擊的風險。這有助於企業提高其網路安全性，保護其網路免受網路攻擊和資料洩露的威脅。

簡單、快速且經過驗證的微切分 Segmentation 解決方案

Illumio Core

針對雲端資料中心工作負載進行分段，通過三個簡單的步驟來阻止傳播，從而減少漏洞和勒索軟體的影響。提供可視性、極其簡單的策略建立引擎以及自動分段和執行來阻止攻擊移動。

Illumio Core

查看任何工作負載

流量在所有代理和無代理工作負載（如容器、IOT 和虛擬機）中可見 - 在單個控制台中。

任何規模的細分

通過防止橫向擴散來阻止漏洞的傳播 - 無論架構、規模或複雜性如何。

在幾分鐘內提供保護

自動阻止不必要的連接 - 無需編寫繁瑣的防火牆規則或接觸網路。

幫助企業瞭解安全風險並跨混合雲和多雲協調雲工作負載策略

Illumio Cloud Secure

雲原生工作負載的無代理分段，通過跨混合雲和多雲環境的可見性和無代理控制，實踐雲端零信任。

Illumio CloudSecure

收集應用的洞察分析

輕鬆連接 AWS 和 Azure 帳戶。即時收集和整合物件元數據，以獲得流量遙測見解和應用依賴關係。

優化安全狀況

利用即時遙測數據創建和實施精心設計的訪問規則，保護網路的關鍵部分免受基於雲的安全威脅。

評估網路風險

工作負載和連接物件的全面應用依賴關係圖讓發現安全風險變得簡單。

Endpoint Security 將成為端點安全力量的倍增器

Illumio Endpoint

端點設備的細分。通過將零信任擴展到端點設備，消除終端使用者對環境構成的風險。

Illumio Endpoint

隨時隨地可視化端點流量

通過可視化流量來查看風險，無論設備是在辦公室、旅途中還是在家。

控制應用訪問

不允許端點訪問整個數據中心 - 僅允許定義的使用者存取正確的應用。

保護端點暴露

在其他安全解決方案檢測到攻擊之前，將已知和未知的網路攻擊圍堵在單個設備中。

illumio 是零信任網路微切分的領導者

保護

- 全球財富排名百大的企業中，已有逾 20 家採用
- 超過 350 萬台主機受到保護，適用於各種規模的組織，從全球財富 100 強到小型企業

公司簡介

- 由聯合創始人 Andrew Rubin, CEO、PJ Kirner, CTO 於 2013 年創立
- 全球 500+ 員工

融資 / 估值

- $582.5M/$2.75B

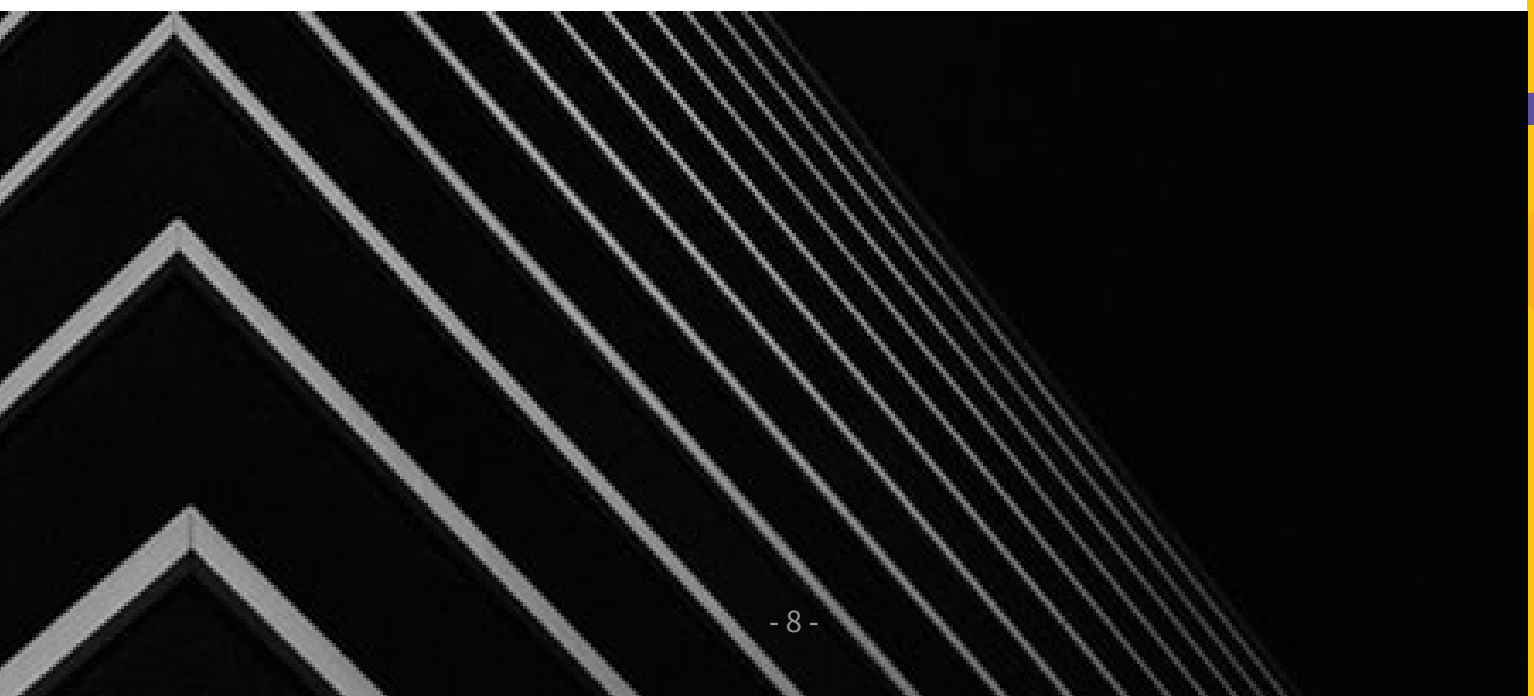
客戶包括

BNP PARIBAS · BlueCross BlueShield · BT · CATHAY PACIFIC · DocuSign · MGM · Morgan Stanley · ORACLE · QBE · salesforce · servicenow

案例分享

- More than 15% of the Fortune 100
- 6 of the world's 10 largest banks
- 5 leading insurers
- 3 of the top 5 enterprise SaaS providers

CATHAY PACIFIC Leading Global Airline	
挑戰	零信任控制應用於 3,000+ 台伺服器和 600 個應用程式，位於本地和 Azure、AWS 雲端。
使用Illumio之前	希望透過應用零信任的微分割和最低權限原則來提升安全性。但現有工具運作緩慢、效率低下，無法將可見性與策略管理整合在一起。
使用Illumio之後	在不到 3 個月的時間內，設計並應用了整個組織的零信任分割（與傳統工具的 12 至 18 個月相比）。
推薦	「每當我們引入新的伺服器或應用程式時，Illumio 都是投入運作流程的一部分。它被證明是容易部署和實施的。而且，Illumio 幫助我們更加注重應用程式。」—— YC Chan, 基礎架構工程師負責人



GSS 叡揚資訊
Galaxy Software Services

Checkmarx

illumio

mend.io

資安服務

orca security

digital.ai

SECURE CODE WARRIOR

AVC
Application Vulnerability Correlation

資安學程

叡揚資訊成立於 1987 年，是台灣資訊軟體業的領導廠商，於應用系統開發逾 30 多年經驗，以改善資訊安全、提高企業效能為使命，全方位引進國際前瞻領導性知名品牌，致力為各大企業及組織提供 DevOps 應用程式安全解決方案、顧問及整合服務，目標打造提供台灣企業良好的資安平台，優質服務累積廣大的客戶群，包含醫療業、政府國營事業、金融業、壽險業、電信業、交通運輸業、製造業、高科技業等等。

服務範圍：包括源碼檢測服務、開源碼檢測及管理、APP 黑箱安全檢測、Mobile & APP 自動化連續測試平台、行動應用安全保護、微切分技術保護營運環境、工具使用建置及導入建議、SSDLC 整合、軟體 Coding 安全課程、Java 解決方案等，未來也將持續引進國際頂尖資安資訊及技術，協助客戶有效提升應用系統安全強度，建立堅強資安防線。期許透過卓越的軟體與服務，帶領客戶透過 IT 創新提升企業產能及核心競爭力。

GSS 叡揚資訊 Galaxy Software Services
台北市中山區德惠街 9 號 5 樓 www.gss.com.tw
(02)2586-7890 service@gss.com.tw