illumio

零信任微切分

防火牆隔離的方式來保護網路，其實不如想像般可靠

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 – Zero Trust 零信任微分隔解決方案

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

illumio 是零信任分段的領導者

保護

- 全球財富排名百大的企業中，已有逾 15 家採用
- 超過 200 萬台主機受到保護，適用於各種規模的組織，從全球財富 100 強到小型全業

公司簡介

- 由聯合創始人於 2013 年創立：Andrew Rubin, CEO、PJ Kirner, CTO
- 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

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。原因是不具備自我防禦能力，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，它將所有主機都視為直接面對網際網路的不安全，整個網路都有受到威脅和惡意攻擊的可能。

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% 的勒索軟體感染需要不到 4 個小時的時間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「永不信任，一律驗證」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。

❶

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。

❷

持續監控

以零信任的模式為基礎，可視化組織中所有的連線狀態。

在所有連線建立前，檢視行為是否可被信任。

❸

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，提供平臺全年不休的安全監控和防護每個工作單元或應用，以阻止橫向移動－防止漏洞在裸機、VM 和 Container 上的任何資料中心或雲端蔓延。

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。可以說明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 可幫助您實現零信任

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。

兼容

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

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的建議，輕鬆完成 Policy 的管理、發佈與套用。

擴充

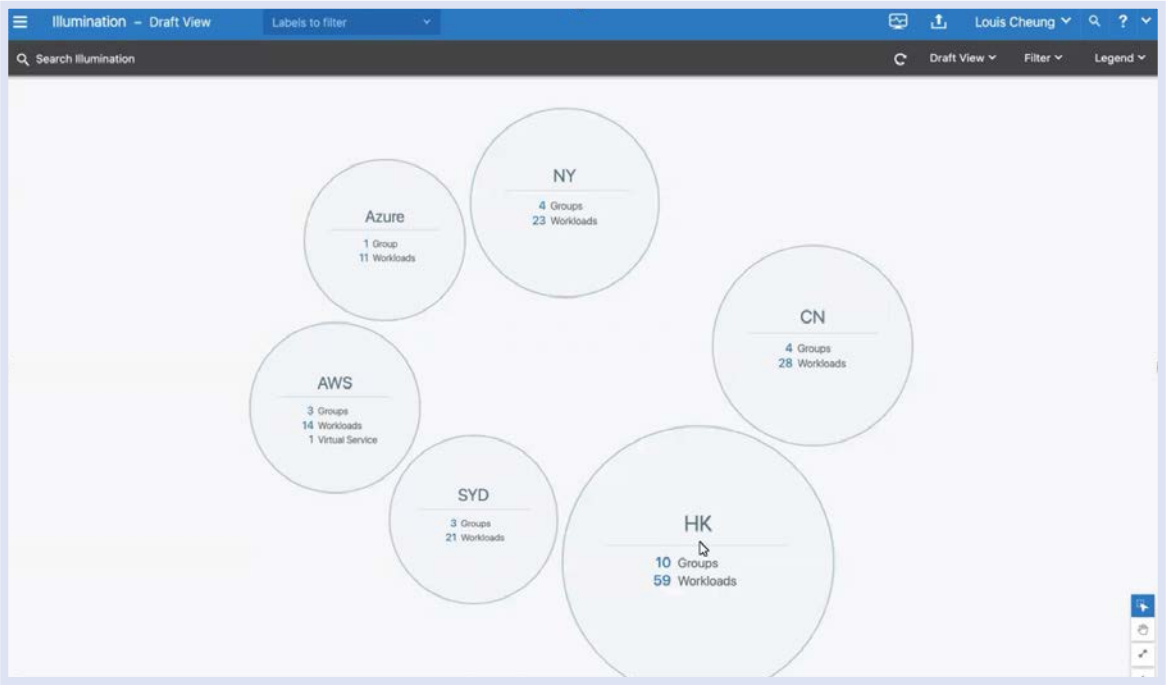
illumio 重視系統的穩定性，所以將代理程式極度輕量化，確保系統的運作不受影響。

安全

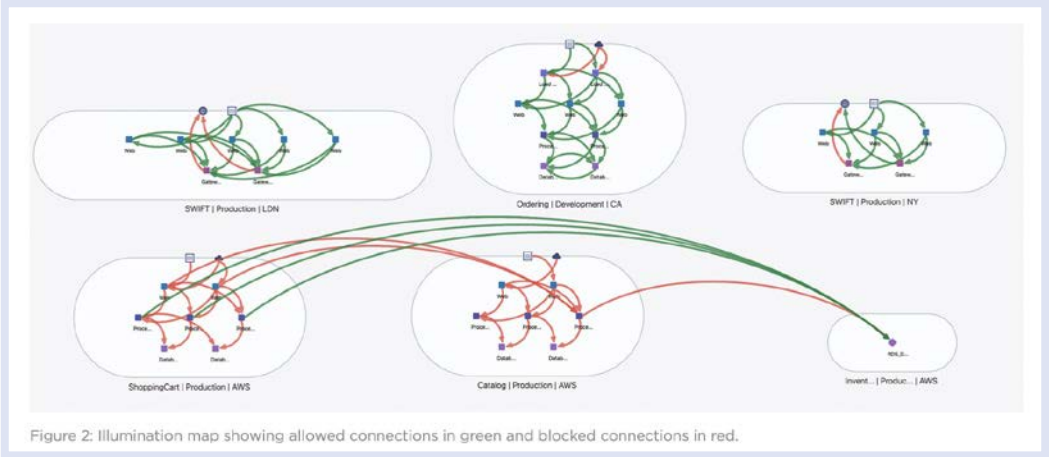
從區域(TW/US)、環境(正式區 / 測試區)、應用程式(HRM/CRM)、... 到最小維度的 "port"，illumio 可以在各層級執行微切分部署。

可靠

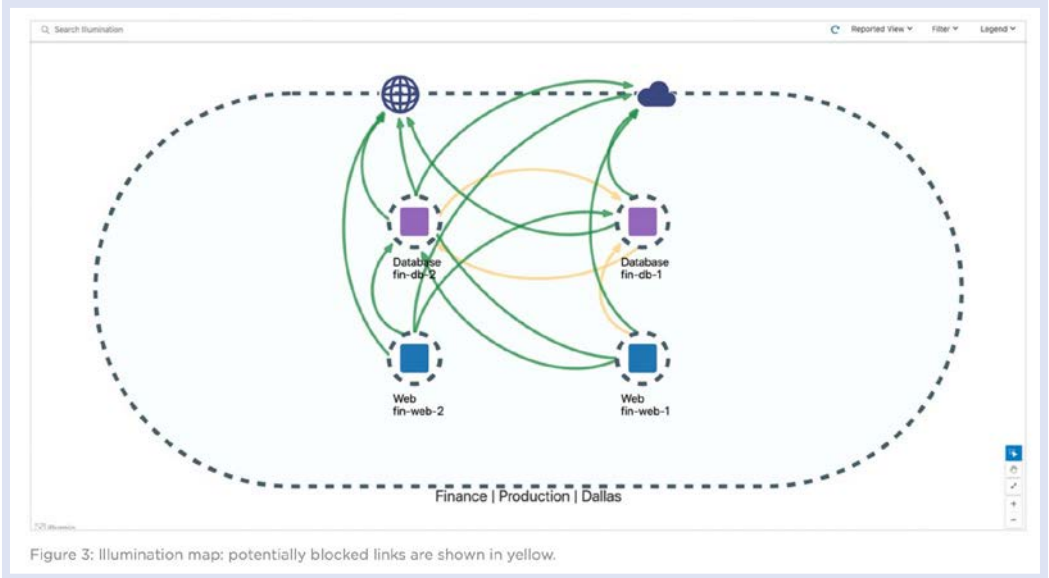
illumio 已在各行各業的環境中實踐微切分部署，導入效益經過許多客戶的驗證與肯定。



▲ 可視化看到不同區域之主機數量



▲ illumio 可視化地圖中，綠色為允許的連線，紅色為禁止的連線



▲ 黃色的線，則是預計會禁止的連線

▲ 透過整合主機弱點報告，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）

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 – 所有這些都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，將零信任變為現實。

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映射。

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使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，消除終端用使用者對環境構成的風險。

Illumio Endpoint

隨時隨地可視化端點流量

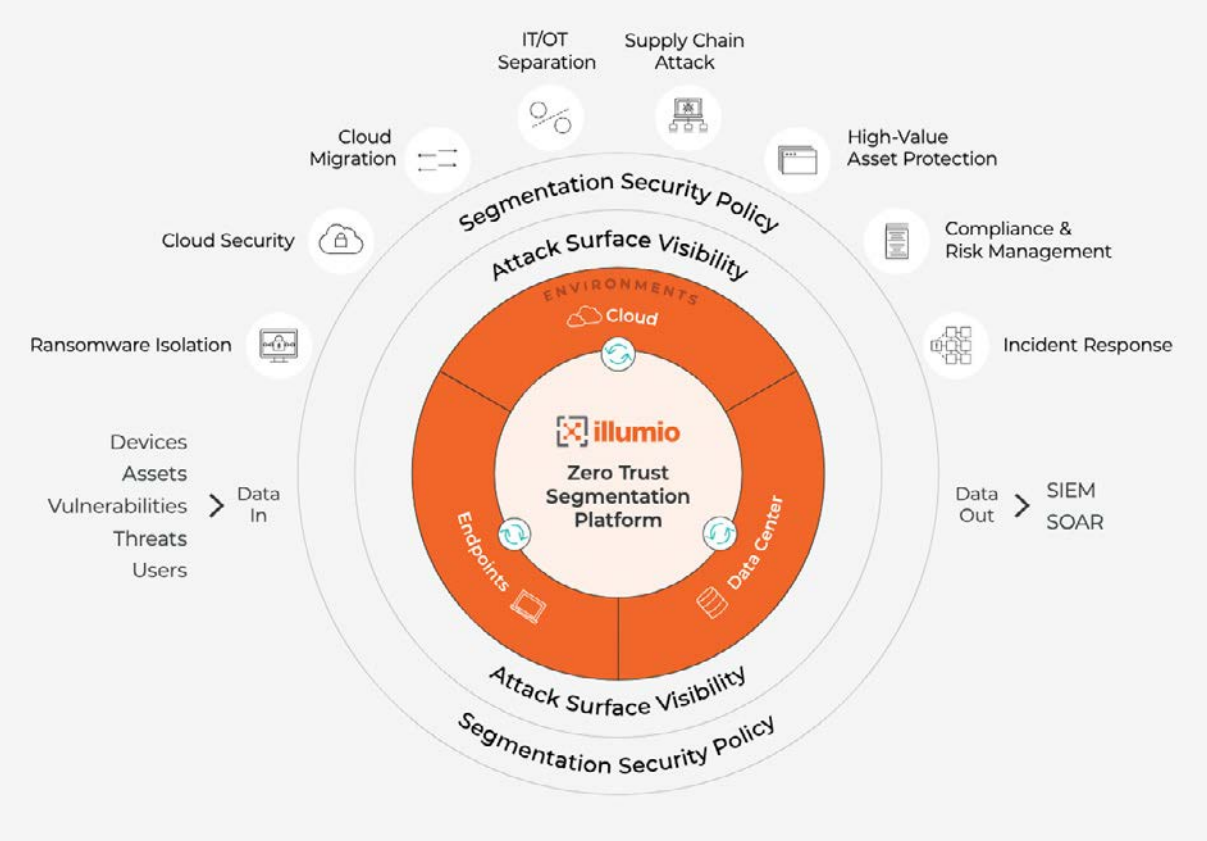
通過可視化流量來查看風險，無論設備是在辦公室、旅途中還是在家。

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。



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

Challenge	Apply Zero Trust control across 3,000+ servers and 600 applications located both on premises and in Azure and AWS clouds.
Before Illumio	Wanted to improve their security by applying Zero Trust micro-segmentation and least privilege. But existing tools were slow, inefficient and unable to integrate visibility with policy management.
After Illumio	Designed and applied Zero Trust Segmentation across the organization in under 3 months (compared with 12 to 18 months with legacy tools).
Testimonial	"Whenever we introduce new servers or applications, Illumio is part of the commissioning process. It's proven to be easy to deploy and implement. And Illumio has helped us be more application-centric." YC Chan Head of Infrastructure Engineering

QBE
Global Insurance Leader

Challenge	Apply Zero Trust Segmentation across 10,000 workloads in globally distributed data centers and multi-cloud environments.
Before Illumio	Used physical firewalls and virtual firewall appliances for segmentation. But as the organization grew, this approach proved to be labor-intensive, complex and almost unmanageable.
After Illumio	Rapidly applied flexible, scalable Zero Trust Segmentation. Now able to maintain consistent security as the organization expands and evolves.
Testimonial	"Illumio Core enables us to roll out firewall changes much faster than before. Previously, it would be days or weeks. Now it's minutes or hours." Nick Venn Global Collaboration and Cyber-Infrastructure Manager

HGC GLOBAL COMMUNICATIONS
Telecommunications Leader

Challenge	Apply Zero Trust Segmentation across a globally distributed organization with both on-premises assets and hybrid and private clouds.
Before Illumio	Commissioned an external audit that recommended Zero Trust Segmentation to achieve real-time visibility, prevent lateral movement and strengthen the risk posture across an expanding organization.
After Illumio	Reduced segmentation operational effort by 25% and segmented all high-value assets within 4 months of launching Illumio.
Testimonial	"Illumio Core proved to be technically superior, not just in terms of what it offers, but also its functionality and how it works. It was the most mature solution that actually delivers on its promises in a way that's stable and consistent." Jacqueline Teo Chief Digital Officer