Illumio Segmentation

控制橫向移動，阻止入侵與勒索軟體攻擊演變成網路災難。

適用於現代網路的現代分段防護

當今的網路規模龐大、混合部署且不斷變動，正是網路攻擊的絕佳條件。

光是過去一年，就有 88% 的組織遭到勒索軟體攻擊，其中 58% 因此被迫中斷營運。

在當今混合、多雲環境、遠端工作與分散式應用程式並存的世界裡，傳統邊界早已不復存在。

攻擊者一旦入侵，便會在您的網路中快速擴散，悄悄感染關鍵資料與系統。這種橫向移動難以偵測，使入侵不僅更頻繁，也更複雜、破壞力更大。

資安專家一致認為，以分段防護為基礎的零信任（Zero Trust）作法，是遏止入侵、降低風險與建立韌性最有效的方式。

Illumio Segmentation 讓您能夠掌握細緻的網路流量可視性、修補弱點、阻止未經授權的橫向移動，並遏止入侵——無論是在雲端、資料中心或端點上。

主要優勢

完整且細緻的可視性

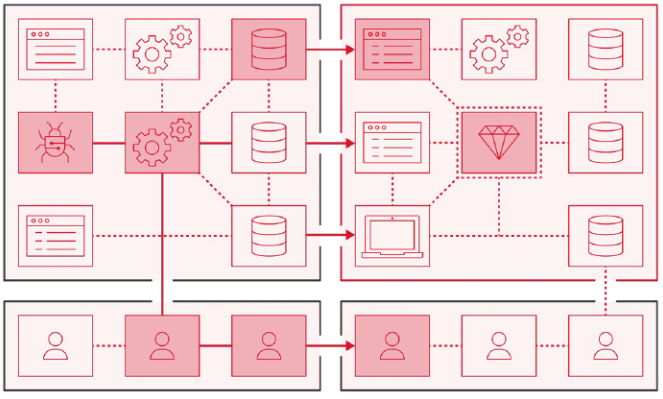
描繪工作負載之間的通訊方式，找出隱藏風險，再建立政策，自動封堵典型的勒索軟體傳播路徑，避免其擴散。

簡化分段防護

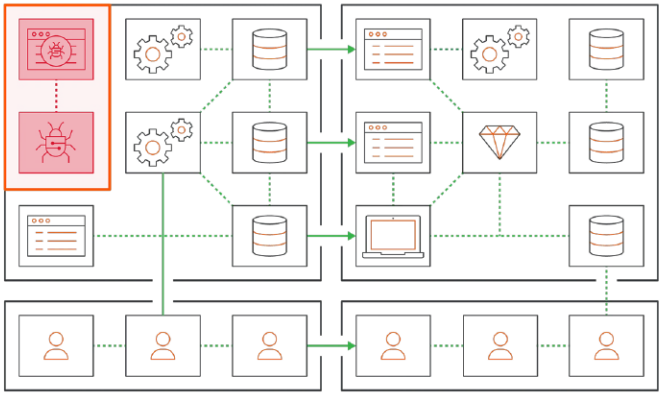
對雲端、端點與資料中心的所有工作負載進行分段。阻止入侵擴散，隔離遭入侵的系統。獲得可隨您規模擴展的分段防護。

零信任，毫不費力

分段防護是任何零信任策略的基石。落實最小權限存取，消除混合多雲環境中的隱含信任。



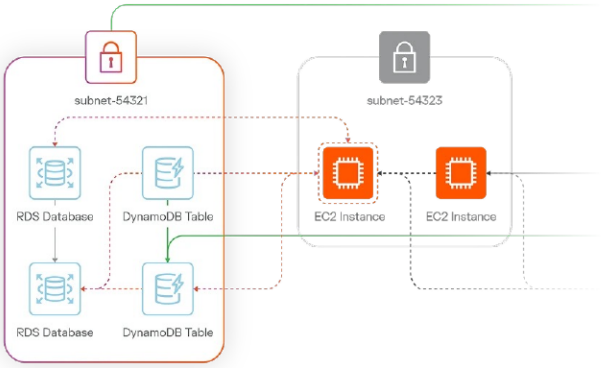
沒有分段防護，入侵會快速擴散



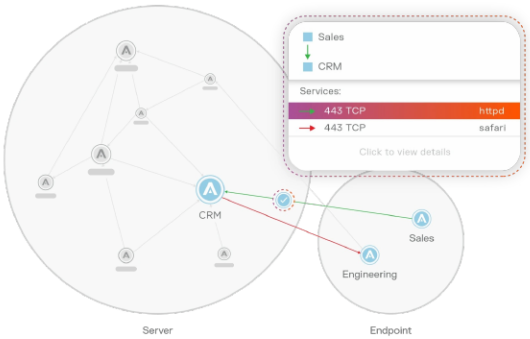
有了分段防護，入侵得以被遏止並偵測到。

適用於所有環境的單一分段防護方案

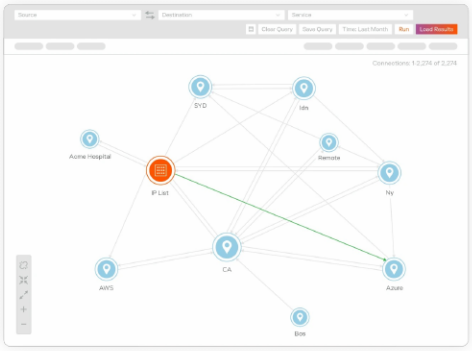
無論您的工作負載位於何處——雲端、端點或資料中心——Illumio Segmentation 都能提供一致、簡單且可擴展的單一解決方案。告別各自為政的孤立工具，迎接能適應您整體環境的統一零信任安全。



在源頭遏止雲端攻擊。視覺化雲端應用程式、資源、流量與中繼資料，並在混合、多雲環境與容器中建立一致、動態的分段防護。



在單一工作站、筆記型電腦或虛擬機器上遏止入侵，甚至在其他資安工具偵測到之前。視覺化端點與應用程式的流量通訊，並在整個網路中落實最小權限存取。



在地端資料中心、容器、IT/OT 與虛擬機器中遏止入侵。無論您的網路架構、規模或複雜度如何，都能看見所有流量。在不中斷營運的情況下對工作負載進行分段。

善用 AI 安全圖譜

Illumio 平台建構於 AI 安全圖譜之上，讓您即時、無與倫比地掌握攻擊面。Illumio Insights 與 Illumio Segmentation 協同運作，提供全面的入侵遏止能力。

Illumio Insights 提供 AI 雲端偵測與回應（CDR），可識別橫向移動風險、偵測攻擊，並在雲端規模下即時遏止威脅。Illumio Segmentation 則協助您快速看見風險並設定政策，防止入侵擴散。

使用 Illumio Segmentation 遏止入侵

illumio.com/illumio-segmentation

關於 Illumio

Illumio 是入侵與勒索軟體遏止領域的領導者，重新定義組織如何遏止網路攻擊並實現營運韌性。我們的入侵遏止平台由 Illumio AI 安全圖譜驅動，可識別並遏止橫跨混合多雲環境的威脅，在攻擊演變成災難之前阻止其擴散。

Illumio 在 Forrester Wave™ 微分段評估中獲評為領導者，協助企業落實零信任，強化支撐全球運轉的基礎設施、系統與組織之網路韌性。

版權所有 © 2025 Illumio, Inc. 保留一切權利。Illumio® 為 Illumio, Inc. 或其關係企業在美國及其他國家的商標或註冊商標。本文件所提及的第三方商標均屬其各自所有者之財產。