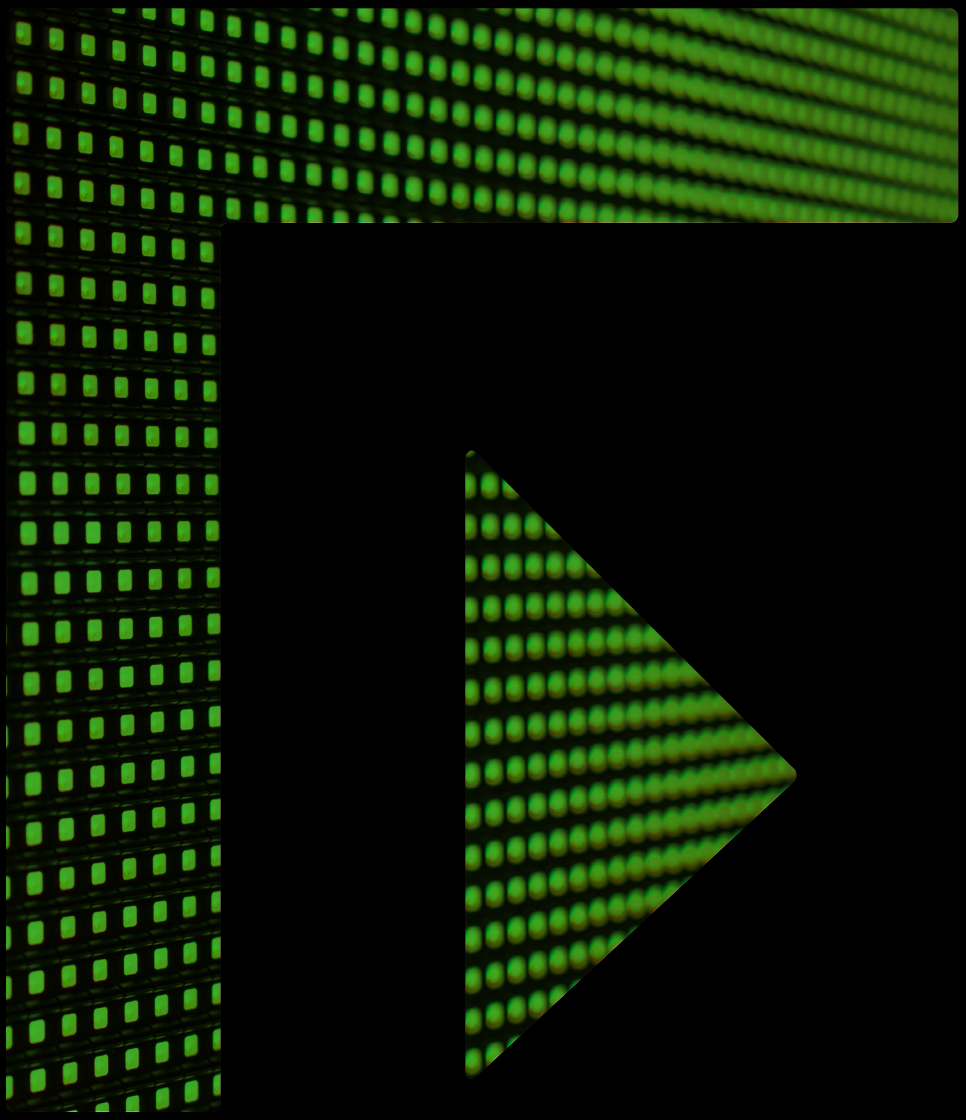


Forcepoint Email Security

FORCEPOINT 雲端及本地部署的電子郵件安全系統

FORCEPOINT
POWERED BY Raytheon

Forcepoint Email Security

FORCEPOINT雲端及本地部署的電子郵件安全系統

多數大規模的網路攻擊起源於電子郵件，使用進階、融合各種戰術如社交工程誘餌與目標式網路釣魚，在整個攻擊中這些多階段威脅混合了網頁和電子郵件元素，這在受駭前提供了從阻殺鏈（Kill Chain）中阻止他們的機會。

將電子郵件的使用與安全性發揮極致

Forcepoint Email Security 能辨識出目標式攻擊、高風險使用者與內部威脅，同時能授權行動工作者安全工作並安全使用如Office365或企業版Box等新興科技。

從外部的攻擊活動到內部傳出的資料竊取或殭屍網路通訊，Forcepoint Email Security利用內容感知防禦技術保護混合環境，並視電子郵件系統為一個完整連線防禦系統的一環來保護，以對抗進階持續威脅（Advanced Persistent Threat, APT）或其他種類先進威脅。

電子郵件面臨的挑戰

- 電子郵件經常在APT進階攻擊的早期階段被利用。
- 必須在電子郵件下更多功夫，以解決資料竊取和內部威脅。
- 企業經常使用Office 365及其他雲端服務來拓展業務與競爭力。
- 危險的用戶習慣很容易導致安全漏洞和資料外洩。

「最後，我們非常滿意 Forcepoint 的產品，Forcepoint Email Security 恰如其分地工作並在任何問題傳到我們伺服器之前先將它擋下。」

—Lowe Lippmann 資訊系統經理 Ray Finck

Forcepoint Email Security 功能

阻擋 APT 及其他進階目標式威脅

Forcepoint 的先進分類引擎 (ACE) 是所有 Forcepoint 解決方案的核心，ACE 能辨識惡意的誘餌、漏洞攻擊包、新興威脅、殭屍網路通訊以及威脅阻殺鏈中的其他進階威脅活動，這使 Forcepoint Email Security 系統能在早期階段就發現攻擊。透過內含完全整合、檔案行為沙箱的強大評估功能，它甚至能辨識出零時差惡意程式的威脅。

保護機敏資料以防外部攻擊與內部威脅

爲了對付惡意的內部威脅或潛在的網路攻擊，監控對外的通訊是絕對必要的，對資料竊取的法規遵循需求以及企業營運需求也同樣需要。唯有 Forcepoint 能提供防止資料滲入或洩出的技術，例如：

- 透過 OCR 辨識找出藏匿在圖檔中的敏感資料，例如掃描的文檔或螢幕快照。
- 加密檔案偵測技術能夠辨認防止辨識的自訂加密檔案。
- 滴漏式資料外洩防護 (Drip data loss prevention) 監控技術能夠辨識以長時間少量方式外洩的敏感資料。
- 對經常嵌入 MS Office 文件中的惡意檔案與巨集作進階分析。

支援行動工作的同時，確保安全採用雲端科技如 OFFICE 365 或 BOX 企業版

IT 部門絲毫不敢懈怠維護現有系統，同時支援越來越多的行動工作者與採用 Office 365 等新技術的需求。Forcepoint Email Security 提供業界領先的功能，利用系統及其他資訊來控制通訊，例如阻止存取易受攻擊行動裝置上的機敏電郵附件，同時允許完整存取完全安全的筆電。這些對內與對外的防禦技術對 Office 365 也全部支援。

辨識「高風險」的使用者行為並教育使用者提高認知

Forcepoint Email Security 中所搜集到的豐富資訊被許多政策用來回報並識別可能需要 IT 特別關注的系統，他們能產生入侵指標 (Indicators of Compromise) 的報表以辨識受感染的系統，以及更多關於可疑行為的主動報表，包括潛在內部威脅如心生不滿的員工行為。使用者回饋功能可在員工犯錯時教育他們，協助學習並瞭解安全的電子郵件使用實務。

提升防護的模組

選配混合雲的部署	**利用 Forcepoint 全球雲端服務以達到更好效能與擴充性** 以雲端預先過濾服務與本地威脅防禦系統結合，透過業界領先的反垃圾郵件 SLA 來保留頻寬。此混合模組能將 URL 沙箱與網路釣魚教育功能加到電子郵件安全解決方案中。
電子郵件 DLP	**以企業等級的內容感知 DLP 阻擋資料竊取** 為對付內部威脅與資料竊取惡意程式，並達到法規遵循目標以及進一步降低個資或知識產權外洩的風險。進階功能可偵測隱藏在圖檔或自訂加密檔案中的資料竊取，甚至為了躲避偵測而透過少量且長時間的方式往外傳輸資料。
雲端沙箱	**整合行為沙箱，以自動或人工分析惡意程式檔案** 使用整合的檔案沙箱來補強 Forcepoint ACE 分析功能，以進行額外的深度檢查。利用在虛擬環境的行為分析技術來找出零時差攻擊或其他進階惡意程式的惡意行為。可自動或手動檢測檔案，以制定詳細的鑑識報告。
電子郵件加密	**確保機敏資料通訊的機密性** Forcepoint 電子郵件加密模組是政策驅動的技術，能安全傳遞電子郵件通訊。透過簡易管理功能，減少傳統在成本及複雜度上的阻礙，不需要複雜的金鑰管理或額外硬體。
影像分析	**辨識明白清晰的影像以強制執行可接受的使用模式與符合規範** Forcepoint 影像分析模組可讓雇主主動採取措施以監控、教育並強制執行有關色情圖像附件的企業電子郵件政策。

「Forcepoint Email Security非常有吸引力，因為它除去了我們管理電子郵件安全的費用開支，並在使用彈性與易用性方面超乎我們預期，總之Forcepoint Email Security讓我們能對使用者提供更有彈性、專業且具成本效益的服務。」

—NCP IT部門主管Martin Law

Forcepoint 解決方案背後的力量

FORCEPOINT ACE

Forcepoint ACE 先進分類引擎使用複合風險評分和預測分析技術，為網頁、電子郵件、資料和行動安全提供即時、在線的內容情境感知防禦以達到最有效的安全性。它領先業界的資料竊取防護技術是靠著資料感知的防禦能力來分析進出的流量，以遏止資料竊取。用於即時安全、資料與內容分析的分類指標是多年研發的成果，使 ACE 能每天檢測比傳統防毒引擎更多的威脅（相關數據每日更新在 http://securitylabs.forcepoint.com）。ACE 是所有 Forcepoint 解決方案背後的主要防禦技術，由 Forcepoint ThreatSeeker Intelligence Cloud 全球智能網路威脅情資所支援。

8 大關鍵領域的整合防禦評估功能

- 提供 10,000 種分析以支援深度檢查
- 預測性安全引擎可預見即將發生的行動
- 在線防護不僅能監控還能阻擋威脅

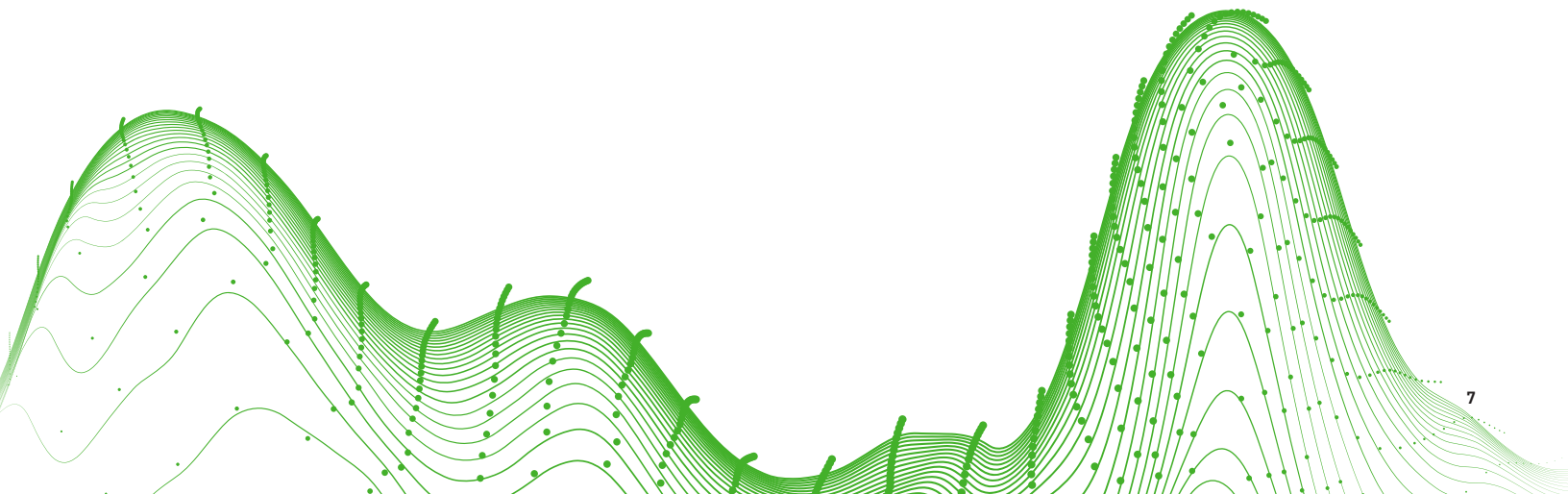
Forcepoint ThreatSeeker Intelligence

Forcepoint ThreatSeeker Intelligence全球智能網路威脅情資由Forcepoint安全實驗室負責，為所有Forcepoint安全產品提供核心匯集的安全情資。它整合超過9億個端點包括來自Facebook的大量網頁分析，透過Forcepoint ACE安全防禦技術，每日分析多達50億個網頁請求。

這種對安全威脅的廣泛了解使Forcepoint ThreatSeeker Intelligence能提供即時安全更新以阻擋進階威脅、惡意程式、網路釣魚攻擊、誘餌與詐騙並提供最新的網頁評級。Forcepoint ThreatSeeker Intelligence在規模上以及使用ACE即時防禦分析各方匯集的輸入表現上無與倫比。當您升級到Web Security，Forcepoint ThreatSeeker Intelligence可協助減少曝露在網頁威脅與資料竊取的風險。

TRITON 架構

憑藉一流的安全性與統一的架構，TRITON架構能提供輕鬆上手的點擊式防護，並具有Forcepoint ACE即時且在線的防禦力。ACE先進分類引擎無可匹敵的即時防禦力是由Forcepoint全球智能網路威脅情資以及Forcepoint安全實驗室的專家所支援。強而有力的成果是一個具有統一使用者介面及統一安全情資的統一架構。



與我們聯繫

886-2-8758-2970 fkuo@forcepoint.com

www.forcepoint.com/contact

[BROCHURE_FORCEPOINT_EMAIL_SECURITY_EN]

FORCEPOINT

POWERED BY Raytheon