Forcepoint

解決方案簡介

Forcepoint ONE: 雲端平台簡化混合式工作團隊的安全

使用案例

- 針對採用混合辦公模式的員工與網際網路、雲 端和企業私有應用程式的互動，獲得能見度和 控制權。
- 防止敏感資料被受控管及非受控管裝置存取濫用。
- 控制對高風險 Web 內容和不同類型的 GenAI 網站的存取。
- 無需使用複雜的 VPN，而能從遠端快速安全 地存取企業內部業務資源和應用程式。

解決方案

- 統一的單一平台可讓使用者管理所有業務應用程式的一致安全性原則。
- 全雲端提供的服務，結合安全網站閘道 (SWG)、雲端存取代理 (CASB) 和零信任網路 存取 (ZTNA) 保護存取和資料。
- 整合式進階威脅防護和資料外洩防護，防止攻 擊者入侵並保護敏感資料。
- 其他功能包括遠端瀏覽器隔離 (RBI)、用 於掃描公有雲高風險設定的雲端安全態勢 管理 (CSPM)、用於移除內容威脅的內容 淨化與重組 (CDR) 等。
- 資料標記的Forcepoint Classification。

成果

- 簡化 - 將 Web、雲端和私人應用程式的安全性整合到一個統一的平台 (無代理程式支援)。
- 現代化 – 結合零信任 (ZT) 原則與安全存取服 務前端 (SASE) 架構，以及遠端瀏覽器隔離 (RBI) 和下載檔案清洗等進階安全功能。
- 無所不在 – 全球範圍皆可使用，擁有超過 300 個網路節點 (PoP)。
- 高可用 – 自 2015 年來，經過驗證運行時間超 過 99.99%。
- 快速的使用者體驗 – 使用分散式運算和自動擴充消除服務瓶頸。

資料優先的安全性

安全性愈益複雜，但還有更好的方法。 使用者現在可以在任何地點工作，資料遍佈各處，包括網站、雲端應用程式和私人應用程式。

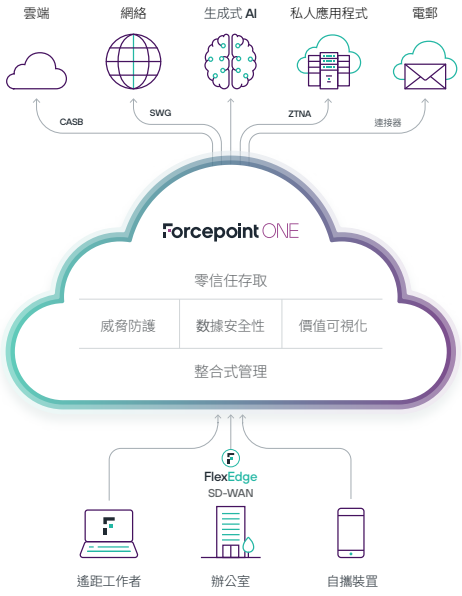
為了支援重返辦公室 (RTO) 計畫和混合式工作團隊，安全性團隊需要一個以資料為中心的整合式安全性平台。安全性控管措施需要具備一致的全貌瞭解與控制能力，才能延伸至整個網路、雲端和私人應用程式存取，以便組織在資料外洩前先發制人。

憑藉資料優先的解決方案，人員無論在哪裡工作，都能確保業務資料安全無虞

Forcepoint ONE 簡化安全管理

Forcepoint ONE 是一個整合式雲端平台，輕而易舉地實現安全性。您可以快速採用 Zero Trust 和 Security Service Edge (SSE，即 SASE 的安全性元件)，因為我們統整了SWG、CASB 和 ZTNA 在內的關鍵安全性服務。

控制對不同類型 GenAI 網站的存取並持續執行防護措施來保護敏感資料並防止惡意軟體暴露，安全地採用 GenAI 等新技術，進而釋放生產力。



為各地工作的人員隨處保護資料

Forcepoint ONE 的雲端原生零信任功能包 括：

- → **適用於雲端和私有應用程式的無代理 DLP 安全性。**從個人設備安全使用私人企業 Web 應用程序，同時確保敏感資料的安全。
- → **整合式進階威脅防護和資料安全性。**透過各地一致的控制，防止資料遺失或洩露，並阻止駭客入侵。
- → **適用於雲端、網頁和私人應用程式存取的統一閘道。**針對 SWG、CASB 和 ZTNA 在同一處管理的業務應用程式進行身分型存取控制。
- → **全球範圍皆可存取且能夠動態擴充** – 建構在 AWS 上的 300 個網路節點，無論員工在何處工作，皆能提 供快速、低延遲連線能力和 99.99%可用度。

網路、雲端和私人應用程式的統一安全管理

- → **雲端：**CASB 更細微地控制任何裝置存取企業軟體 即服務 (SaaS) 應用程式和資料。CASB 即時封鎖敏 感資料下載和惡意軟體上傳。CASB 靜態掃描熱門 公雲軟體服務 (SaaS) 和基礎架構服務 (IaaS)，以偵 測惡意軟體和敏感資料，並且在必要時進行防護。 CASB 偵測 Shadow IT 應用程式，控制所有受控管裝 置的雲端存取。
- → **網路：**SWG 根據風險和類別監控及控制與任何網站的互動，阻止下載惡意軟體或將敏感資料上傳至個人檔案共享和電子郵件帳戶。我們的裝置上Web 安全性可在任何地方的託管裝置上執行接受的使用原則。
- → **企業私有應用程式：**ZTNA 保護並簡化對內部應用程式的存取，避免了與 VPN 相似的複雜度和風險。

整合式進階威脅防護和資料安全

- → **資料外洩防護 (DLP)：**在上傳和下載檔案及文字時 皆會掃描是否含有敏感資料，並根據情況封鎖、追 蹤、或加密。
- → **惡意軟體掃描：**在上傳和下載檔案時皆會掃描是否 含有惡意軟體，如偵測到惡意軟體就會立即封鎖。

整合式的可見性與控制

- → **整合式管理套件，用**於跨 SSE 管道進行配置、監控和報告。
- → **登入原則**用於根據使用者的位置、裝置類型、裝置姿態、使用者行為和使用者群組，控制對 Web、雲端或私人應用程式的存取。這些參數有助於防止帳戶遭到盜用。
- → **易於使用的 DLP 原則，**用於控制託管 SaaS 應用程式、私人應用程式和網站的敏感資料及惡意軟體上傳，以及託管 SaaS 和 IaaS 中儲存的資料。
- → 適用於 Windows 和 MacOS 的裝**置上代理程式**，支援非瀏覽器的 SWG、CASB、或 ZTNA 以實現非瀏覽器用戶端應用程式和影子 IT 控制。
- → **統一的分析與數值視覺化**，可迅速針對單一雲端安 全平台的安全風險、總體使用狀況及相關影響提供 洞察報告。

根據需求提供額外功能

- → **雲端安全性態勢管理 (CSPM)：**掃描 AWS、Azure 和 GCP 使用者設定，找出高風險設定，並提供手動 或自動修復。
- → **SaaS 安全性態勢管理 (SSPM)：**掃描 Salesforce、ServiceNow 和 Office 365 使用者設定，找出高風險 設定，並提供手動或自動修復。
- → **遠端瀏覽器隔離 (RBI)：**藉由在雲端託管虛擬機器 (VM) 上使用瀏覽器，保護使用者在本機裝置上免受 網路傳播的惡意軟體威脅。
- → **Forcepoint Classification**：利用 AI 支援的建議進行資料標記，以提高標記的準確性。
- → **AMDP：**分析受控惡意軟體沙箱中的檔案行為以辨識隱藏和惡意的內容。

訂閱簡便的安全性解決方案

提供使用者人數計價的年度訂閱方案：

- → **整合版本**，適用於網路 、雲端和企業內部 應用程式 安全管理。
- → **Web 安全性版本**包括網路閘道加上用於無限雲端應用程式的內聯 CASB，以及用於未分類和新註冊站點的 RBI 必需品，以便稍後新增對雲端應用程式的 API 支援和對私有應用程式的支援。
- → **ZTNA 版**本保護無限數量的私人應用程式。
- → **CASB 版**本可內聯保護無限數量的雲端應用程序，並包括 3 個應用程式的 API，並且能夠添加其他應用程式套件或專用 API 輪詢節點。
- → **所有訂 閱** 均包含集中式雲端管理、資料遺失防護原則、通過端點代理程式的自動存取，以及綜合報告。

forcepoint.com/contact