

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。
- 控制對高風險網路內容的存取。
- 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

- 單一管理平台，可在單一主控頁面，透過單一端點代理程式，管理適用於所有應用程式的安全政策。
- 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 (詳細資訊請參閱第 2 頁)。

成果

- 簡單化 – 將網路、雲端和內部應用程式的安全性整合於一組政策、單一主控台和單一端點程式 (亦提供無端點支援)。
- 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) 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。

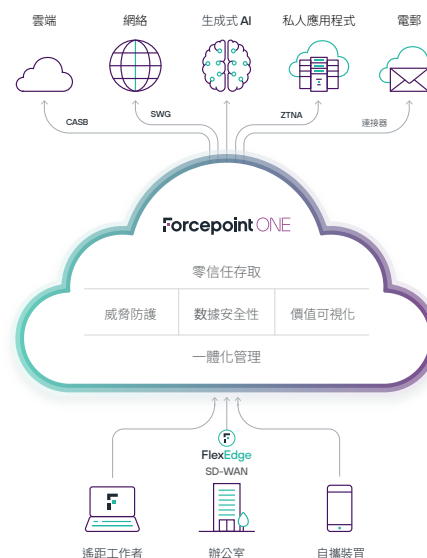
為了支援重返辦公室 (RTO) 計畫和混合式工作團隊，安全性團隊需要一個以資料為中心的整合式安全性平台。安全性控管措施需要具備一致的全貌瞭解與控制能力，才能延伸至整個網路、雲端和私人應用程式存取，以便組織在資料外洩前先發制人。

利用資料優先解決方案，無論在何處工作都可確保企業資料的安全。

Forcepoint ONE 簡化安全管理

全雲端平台 Forcepoint ONE 可簡化安全管理。我們整合了重要安全性服務，包括網站安全閘道 (SWG)、雲端存取資安代理 (CASB) 和零信任網路存取 (ZTNA)，讓您可以快速採用零信任和服務安全 (SSE, SASE 的安全性元件)。

我們提供單一平台、單一主控台和單一代理程式，整合資安解決方案。利用一組安全性政策就能獲得能見度、控制存取，以及在受控和非受控應用程式和所有裝置上保護您的資料安全。





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：

- **雲端及內部應用程式的無端點員工自攜裝置安全性** – 在個人裝置中安全使用企業內部業務網站應用程式，同時保障機敏資料安全。
- **整合式進階威脅防護和資料安全** – 橫跨所有閘道避免資料外洩或外流，並防止駭客入侵。
- **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，控制所有受控裝置的雲端存取。
- **網路：**SWG 根據風險和類別監控與任何網站的互動，封鎖惡意軟體下載或敏感資料上傳到個人資料、分享和電子郵件帳號。我們在裝置上執行的 SWG，可在任何地方的受控裝置上執行管理政策。
- **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。

一致性政策簡化執行

- **單一管理主控台**用於設定、監控和產出報表。
- **統一登入策略**根據使用者位置、裝置類型、裝置狀態、使用者行為和使用者群組, 控制對網路、雲端 或內部應用程式的存取。這些參數可防止帳號遭到 盜用。
- **統一的 DLP 政策**, 可控制受控管 SaaS 應用程式和 網站的敏感資料與惡意軟體之下載和上傳, 亦可控 制儲存在受控管 SaaS 和 IaaS 中的資料之下載和上 傳。
- **統一裝置代理程式**, 適用於 Windows 和 MacOS 系 統, 能夠支援非瀏覽器用戶端應用程式和 Shadow IT 控制的 SWG、CASB 及 ZTNA。
- **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。
- **雲端防火牆**: SWG 的附加元件, 可保護所有的網路流 量, 防範專為利用易受攻擊的分支機構站點而設計 的攻擊。

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。
- **網路安全版本**, 可讓客戶日後新增雲端和企業內部 應用程式支援。
- **所有訂閱**包括集中式雲端管理、含資料外洩防護功 能的統一政策、透過單一端點程式的自動化存取以 及全面的報告功能。

forcepoint.com/contact