Forcepoint Insider Threat

以無與倫比的能見度洞悉使用者的行為，有效保護 IP 及偵測內部威脅

FORCEPOINT
POWERED BY Raytheon

Forcepoint Insider Threat

以無與倫比的能見度洞悉使用者電腦的早期活動，防止因系統遭到劫持、內部人士心懷惡意或使用者粗心大意而使資料遭竊或外洩。

前言

Forcepoint Insider Threat 助政府和名列《財富》百大企業的客戶識別及遏止內部威脅已逾 15 年之久。部署的端點數量超過 100 萬個，Forcepoint Insider Threat 備受肯定的解決方案為全球某些擁有最敏感資料的組織提供防護。其中一家名列《財富》百大企業的零售客戶，部署首年即達到 60% 的投資報酬率。

15

逾 15 年的內部威脅制止經驗

1,000,000

超過 100 萬個端點受到保護

投資報酬率：
60%

還本：
< 16 個月

Forcepoint Insider Threat 能以比的能見度洞悉電腦使用者的早期活動，協助您透過以下方式防止資料遭竊或外洩：

偵測

偵測可疑的活動，無論是出於意外還是蓄意。

防護

防護系統受到劫持、內部人士做出惡意之舉或使用者意外出錯，確保您的智慧財產(IP)不受侵害。

建構

建構標準行為的基準，在使用者開始偏離正軌時及早指出潛在的風險。

提供脈絡

提供使用者的行為脈絡，協助您進行調查。

識別

自動識別您風險最高的使用者。全面的威脅感知能力，可讓您掌握有關危險行為的脈絡。這能讓您判定系統是否遭劫持、員工是否做出惡意之舉，或是否屬於意外性質。

Forcepoint Insider Threat 能讓您的組織如虎添翼

Forcepoint Insider Threat 省時省力，能自動為您風險最高的使用者計分和排定優先次序，而不必從上千個警示中費力尋找答案。這能讓您的團隊專注於優先次序較高的工作並提升效率。Forcepoint Insider Threat 也提供必要的脈絡和鑑識證據以作為無可否認的歸因判定及證物間環環相扣關連的基礎，從而簡化調查、起訴和法規遵循的流程。

FORCEPOINT INSIDER THREAT 的 ：

其他廠商皆無法在單一產品中結合所有這些優點，防禦您的資料受內部威脅所侵害。

- 只有 Forcepoint Insider Threat 能同時在 Windows 和 Mac OS 端點上提供 DVR 擷取與播放功能。
- 我們的「命令中心」具有超高的直覺能力，有助於識別風險最高的使用者，快速檢視可揭示更廣泛風險的模式。
- Forcepoint Insider Threat 能讓您精細控制何時蒐集資料，以及需特別蒐集什麼內容以保護使用者的隱私。
- Forcepoint Insider Threat 與 Forcepoint DLP 進行整合，協助您在偵測到危險行為後快速作出更明智的補救對策。

主要特色：

除了 Forcepoint 外，目前沒有任何一家廠商在單一產品中提供這些關鍵的內部威脅防禦功能。

- 蒐集和彙總中繼資料以建立使用者和工作群組的行為基準，讓您之後能自動偵測使用者是否做出偏離正軌的異常行為。
- 與 Forcepoint DLP 進行整合，提供您所需的鑑識能力，以便在偵測到危險的使用者行為後快速做出更明智的補救對策。
- 警示彙總功能可迅速識別出風險最高的使用者。
- 影片蒐集與播放功能有助於加快調查速度，因為其能釐清責任歸屬，顯示員工的意圖，也能被法庭所採納。

以無與倫比的能見度洞悉使用者的行為

Forcepoint Insider Threat 的功能

Forcepoint Insider Threat 解決方案針對內部威脅所打造，不是一種針對特定問題做出改造的現有解決方案，而是一種無與倫比的獨特安全性工具，旨在避免資料因惡意或意外威脅而受到侵害。Forcepoint Insider Threat 是由一群職業生涯皆投入於資訊保護領域的網域安全專家所領導開發。

Forcepoint Insider Threat 提供以下無比的資料保護功能：

- 防範內部人士的無心之過以及惡意行為所造成的威脅。
- 影片重播功能提供完整的行為脈絡，能迅速辨別出惡意行為，非技術人員也能輕易檢視和瞭解，透過可自訂的以業務為導向的政策，同時兼顧員工隱私。
- 分析功能會為行為異常的使用者排定優先次序，並讓您深入檢視其行動，包括過往的行為。
- 整合式企業級系統讓您無需購買或維護許多獨立軟體應用程式。
- 分散式架構能防止效能受到衝擊。
- 備受肯定且運作穩定的輕型代理程式。
- 從多處來源蒐集資料，包括 Forcepoint DLP。
- 偵測危險行為，即便使用者未處於企業網路中也能偵測。

Forcepoint Insider Threat 的元件

使用者行為風險分析評級引擎

• Forcepoint 賦予必要的能見度以便及早發現警告，得知使用者已遭駭、做出惡意之舉或是意外失誤，以免敏感資料遭到侵害或竊取。

• Forcepoint Insider Threat 省時省力，能自動為組織內風險最高的使用者計分和排定優先處理次序，讓您不必從上千個警示中費力尋找答案。

• Forcepoint Insider Threat「命令中心」具有超高的直覺能力，有助於識別風險最高的使用者，快速檢視可揭示更廣泛風險的模式。

• Forcepoint Insider Threat 影片擷取和重播功能提供無與倫比的能見度，讓您洞察可疑的行為以免其演變成實際問題（例如開後門、資料囤積）。

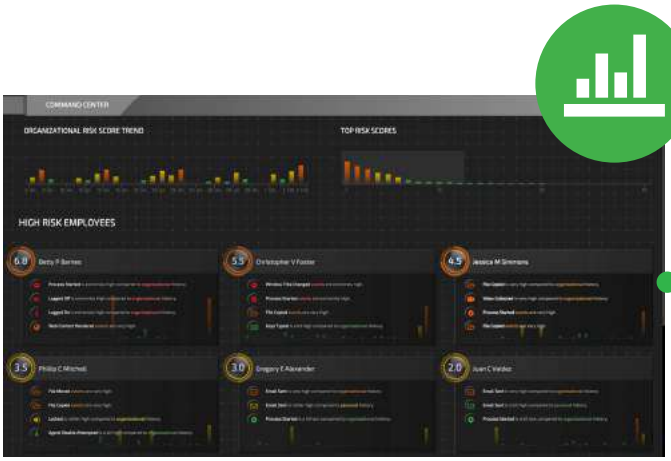
FORCEPOINT INSIDER THREAT 如何針對內部威脅提供防護

• 橫跨各種管道建立個人行為和組織行為的基準，以瞭解什麼是期望的標準行為。

• 找尋個人行為的異常之處，以偵測出任何潛在的內部威脅（無論是有心還是無意）。

• 每天為每位使用者提供綜合性的風險分數，並迅速突顯 30 天的風險趨勢。

• 將較危險的使用者排定優先次序，藉此簡化調查流程。



將較危險的使用者排定優先次序，藉此簡化調查流程

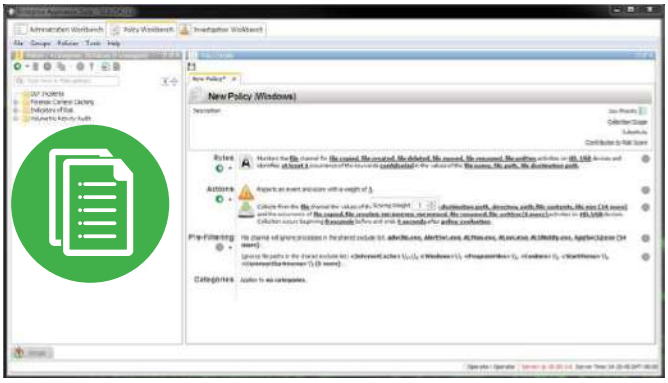
政策導向的危險行為辨識技術

• 客戶可根據一組或一系列活動，定義一些已知較危險的特定行為。

• 這些資安政策提供多種活動監控的偵測作業，包括從 PII 和 HIPAA 法規要求到 IP 保護和部份惡意程式偵測。

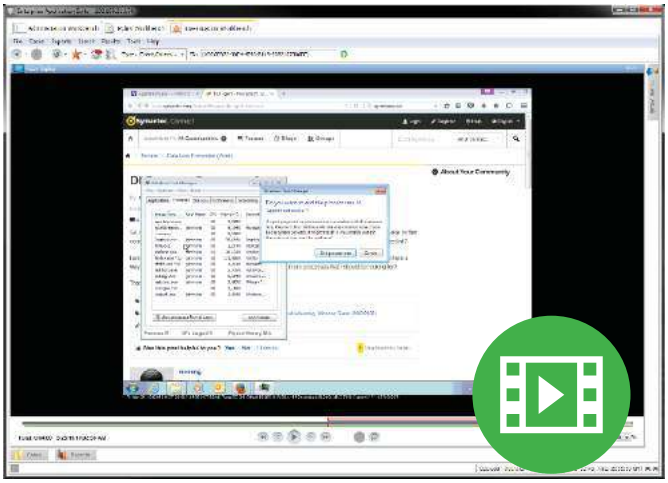
• 這些客戶特定的資安政策會影響整體風險分數。

• 客戶可手動調整這些資安政策的權重，以調整其對於整體風險分數的比重。



風險分數的構成因素可視覺化呈現

• 每天會針對每位使用者產生簡單易懂的直覺式圖表，讓調查人員能迅速瞭解是何種活動令使用者獲得了較高的風險分數。



支援 DVR 的桌面影片重播功能

• 螢幕截圖的擷取和播放能提供完整風險情境感知能力，讓您以無與倫比的能見度洞察可疑的行為，以免其演變成實際問題。

• 資安政策能提供必要的脈絡和證據來判定肇事的使用者是誰，以及判定其是否已遭駭、做出惡意之舉或是純粹意外失誤。

• 調查人員可輕易針對高風險使用者透過桌面影片重播功能檢視任何可疑的活動，而且法庭接受經由此方式來判定肇事的使用者。

風險活動時間表的檢閱與額外的鑑識細節

• Forcepoint Insider Threat「命令中心」省時省力，能自動為您風險最高的使用者計分和排定優先次序，而不必從上千個警示中費力尋找答案。

• 輕鬆取得危險使用者和擴展式時間表的詳細資訊，顯示出使用者目前實際做出哪些行為而被認定為較危險的使用者。

• 紀錄和播放功能可讓您瞭解使用者的意圖並簡化調查流程。

• 為您提供使用者行為的相關脈絡與內容，協助釐清責任歸屬和起訴惡意之行為。

如欲安排 Demo 展示事宜或獲得更多資訊，請造訪 www.forcepoint.com/contact。

偵測可疑的活動，無論是出於意外還是蓄意。

聯絡方式
www.forcepoint.com/contact

[BROCHURE_FORCEPOINT_INSIDER_THREAT_TCH] 400011.030117

FORCEPOINT
POWERED BY Raytheon