proofpoint.

解決方案 簡介

Proofpoint Collaboration Security Prime

防範透過電子郵件及其他管道發起的 AI 規模攻擊



主要亮點

- 以 99.999% 的效力攔截種類最廣泛的威脅
- 將保護範圍擴及電子郵件及其他領域
- 透過基於風險的指導和洞察，增強人類的韌性
- 最小化內部及供應商帳戶遭入侵所造成的影響
- 透過統一的平台簡化操作，實現工作流程自動化
- 透過整合，降低分散解決方案所產生的成本與複雜性

這套解決方案屬於 Proofpoint 整合式人本安全平台的重要組成，用於保護智能體工作環境中的人員和資料。

概述

隨著組織進入智能體時代，他們正在採用人工智慧驅動的工具和助理來幫助人們更有效地工作。這些人工智慧代理正逐漸成爲擴展勞動力的一部分，透過電子郵件、訊息平台、雲端應用程式等與員工、應用程式和其他代理商進行互動。隨著工作空間的擴大，攻擊面也隨之擴大，攻擊者已經開始利用這些可信賴的通訊管道。

作爲因應，許多組織被迫採取零散的、以單點產品爲主的資安方式。但這將在其防禦體系中造成額外漏洞，導致團隊各自爲政，並增加營運的複雜性。

爲了防禦當今跨多管道、多階段的人工智慧規模化攻擊，以及保護可信賴的互動 — 無論是人與人之間的互動、人與人工智慧助理之間的互動、人與雲端應用程式之間的互動 — 組織需要採取更全面的方式。Proofpoint Collaboration Security Prime 可以提供協助。Proofpoint Prime 在智能體工作環境中整合威脅偵測與回應。

它可以幫助您：

- 以無與倫比的精準度防禦多管道、多階段攻擊
- 最小化員工及供應商帳戶遭入侵的影響
- 與供應商、合作夥伴和客戶建立安全可靠的業務通訊
- 透過精準的人爲風險導向教育，全面強化人員的抵禦能力與韌性
- 透過自動化精簡安全營運流程

©Proofpoint, Inc.2026 01

在人們協作的任何地方 - 無論是電子郵件還是其他平台 - 都能保護他們的安全。

隨著工作方式不斷朝向更互聯互通和人工智慧輔助的工作環境，Proofpoint Collaboration Security Prime 隨時守護人員安全。它可以阻止跨電子郵件、協作和訊息工具（如 Microsoft Teams、Slack）、社交媒體和基於雲端的應用程式的多管道攻擊。更重要的是，此舉不會干擾工作流程。

Proofpoint Prime 可保護擴充工作空間內的人員免受各種威脅，包括：

- 進階網路釣魚
- 商業電子郵件詐騙 (BEC)
- 電話導向攻擊傳遞 (TOAD)
- 電子郵件轟炸
- 勒索軟體
- 帳號接管
- AI 生成的攻擊和 AI 利用技術，例如提示注入。

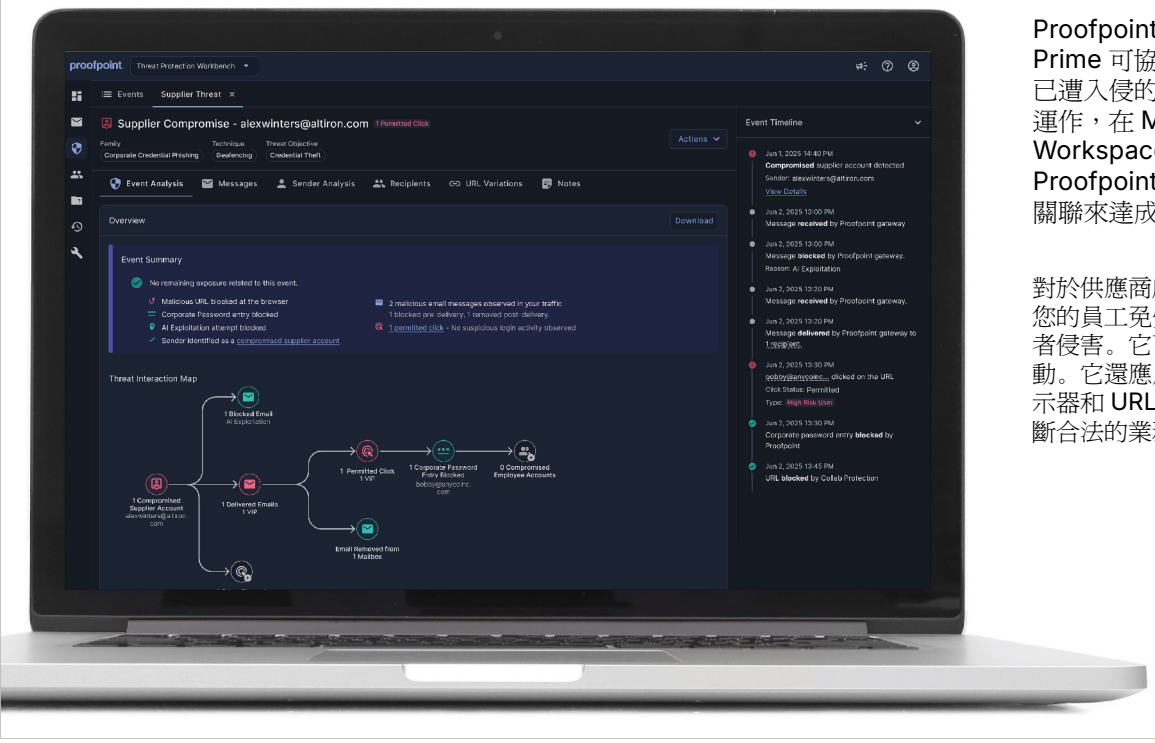
此外，它還能阻止威脅生命週期各個階段的攻擊 — 從交付前到交付後，從點擊到登入，確保防護滴水不漏。

Proofpoint Prime 採用 Proofpoint 的 Nexus® AI 技術，提供無與倫比的威脅防護，效力高達 99.999%。它利用我們豐富的威脅情報、先進的語言模型、關係圖、機器學習、行爲分析和電腦視覺來實現這一目標。這些技術協同工作，在威脅造成危害之前偵測並加以阻止。

Nexus® AI 模型以網路安全領域最大、最多樣的資料集之一訓練而成。

防範帳戶遭到入侵

攻擊者利用盜用的身份資訊存取合法帳戶，並發動多階段攻擊。攻擊者不僅濫用員工帳號，還會利用可信供應商的帳號，進一步擴大威脅範圍。在以協作爲導向並由智能體輔助的工作環境中，降低這些威脅的影響至關重要。



Proofpoint Collaboration Security Prime 可協助您偵測、調查並控制已遭入侵的員工帳戶。它能跨平台運作，在 Microsoft 365、Google Workspace、Okta 等，並透過 Proofpoint 生態系統中的身份與活動訊號關聯來達成。

對於供應商威脅，Proofpoint Prime 可保護您的員工免受利用遭入侵的第三方帳戶的攻擊者侵害。它可以識別源自供應商帳戶的可疑活動。它還應用了自適應保護措施（例如警告指示器和 URL 隔離），以降低風險，同時不會中斷合法的業務通訊。

圖 1. Proofpoint Collaboration Security Prime 可封鎖並關聯電子郵件、訊息傳遞和協作、雲端和供應商管道中的威脅。

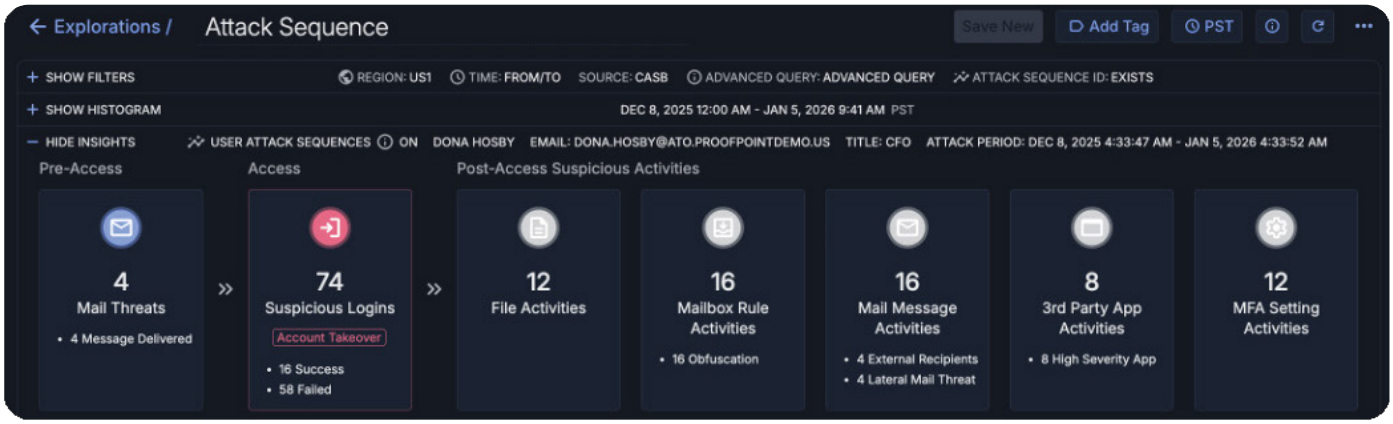


圖 2. Proofpoint Collaboration Security Prime 不僅揭示攻擊序列全貌，更能自動化遏制威脅，確保防護快

保護您值得信賴的業務通訊

攻擊者經常使用冒充手段，將自己滲入受信任的商業通訊中。當您的組織遭到冒充時 — 無論是透過直接網域欺騙還是使用類似的網域 — 都會使您的員工、客戶和合作夥伴面臨風險。更重要的是，它還會對您的品牌造成嚴重損害。

Proofpoint Collaboration Security Prime 可以幫助您主動降低這些身分冒用風險。它讓您可以完全了解使用您信任的網域發送的所有電子郵件，包括第三方發送的電子郵件。您不僅可以獲得強大的工具，還可以獲得專家顧問的指導，他們將指導您完成電子郵件身分驗證部署的每一步。這有助於您實現完全的 DMARC 合規性，並防止攻擊者偽造您的網域。

我們的防護範圍不僅涵蓋使用者產生的電子郵件，亦包括一個安全、專用的環境，用於傳遞應用程式產生的訊息，以及第三方 SaaS 供應商代表您發送的電子郵件。

此外，Proofpoint Prime 還提供進階的相似網域偵測功能。它會動態監控網路上與您的網域非常相似的網域名稱。它還提供了有關其註冊細節以及潛在濫用情況的詳細資訊。

我們的防護不僅止於偵測。我們可代表您採取行動，透過與註冊商、主機服務商及頂級網域 (TLD) 管理機構的緊密合作，關閉惡意網域與 URL。我們的專業人員負責管理整個流程，讓您的團隊專注於核心業務運作。

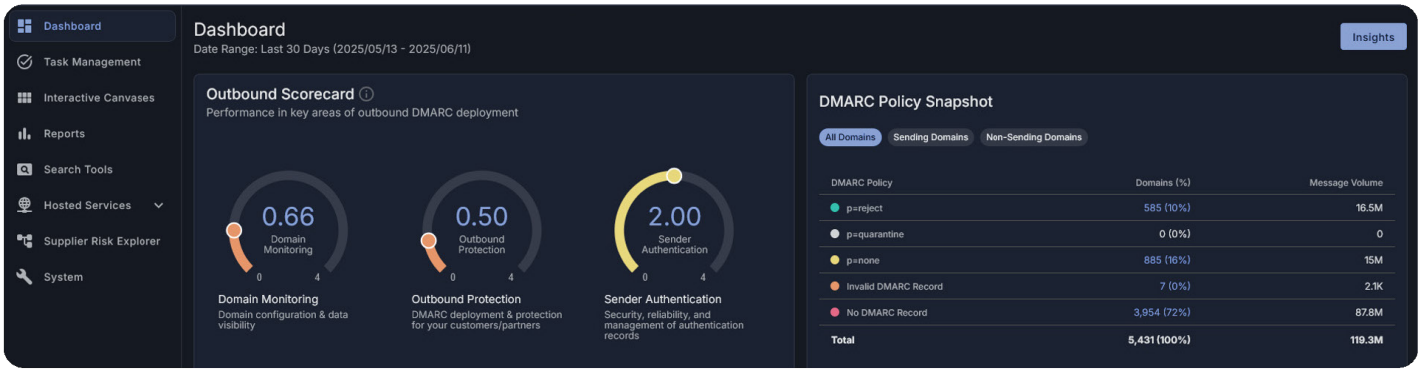


圖 3。Proofpoint Collaboration Security Prime 提供對冒充威脅的可視性，例如網域欺騙和惡意仿冒。

透過基於風險的指導來增強人員韌性

隨著工作日益協作且充滿動態變化，人員必須持續強化韌性，才能有效抵禦不斷演進的網路攻擊。這需要超越以合規爲導向的培訓，轉向人爲風險管理— 即時教育，反映使用者的工作方式和他們面臨的實際風險。

Proofpoint Collaboration Security Prime 透過引導員工做出更安全的選擇，幫助您的組織實現這種轉變。它提供自動化、有針對性的、基於人類風險的學習，這種學習方式是根據每個使用者的行爲、角色、攻擊暴露情況和獨特的風險狀況量身定制的。利用人工智慧技術，Proofpoint Prime 只需一鍵操作即可將現實世界的威脅轉化爲即時模擬。這樣可以確保教育與積極的風險訊號保持一致，從而推動可衡量的、持久的行爲改變。

學習模組不僅會根據個人風險訊號進行調整，還會透過引人入勝、遊戲化的體驗來呈現。因此，使用者更有動力參與，他們的安全行爲也會隨著時間的推移而得到強化。學習者可透過直覺化的儀表板清楚掌握其進度，並保持資訊透明與責任感。

同時，管理人員能輕鬆地調整方案，以符合組織的風險優先順序。結果是更高的員工參與度、可衡量的行爲改變，以及整個組織內更強大的安全文化。



圖 4。Proofpoint Collaboration Security Prime 能夠提供對真實使用者行爲的可視性，從而支持有針對性、以風險爲導向的學習。

簡化安全操作

隨著威脅從電子郵件擴展到協作工具、雲端平台和供應商生態系統，安全團隊面臨著用更少的資源完成更多工作的壓力。在這種環境下，各自獨立的解決方案並不能讓事情變得更容易。它們不僅會增加複雜性，還會減慢回應時間並增加營運成本。這些因素使得在大規模環境中降低風險更加困難。

Proofpoint Collaboration Security Prime 透過統一威脅偵測和調查，以及自動化工作流程和回應，簡化您的安全營運。威脅防護工作台透過原生整合，匯集來自電子郵件、訊息、協作平台、雲端帳號及供應商生態系的偵測洞察與攻擊鑑識。這使得團隊能在單一整合工作平台中調查事件並採取果斷行動，以達到最大效率。

Proofpoint Prime 也能幫助團隊有效地決定優先順序。威脅交互圖能夠在多個控制點之間關聯威脅與安全事件，並提供攻擊路徑的視覺化地圖。這使得分析人員能夠快速識別出最關鍵的事件。同時，它也會自動檢查用戶報告的訊息，修復惡意內容，並向用戶提供回饋。因此，既減少了人工操作，也加強了安全的使用者行爲。

這樣可以提升回應速度，降低操作複雜度。您的安全團隊能以更少的資源實現更多效益— 而不犧牲防護效能。

選擇合適的防護級別

Proofpoint Collaboration Security Prime 提供多個層級。這樣一來，您就可以根據組織的風險狀況和營運需求來制定防護措施。每個層級都建立在前一個層級的基礎上。保護範圍從核心電子郵件威脅拓展至協作通道、帳戶被入侵、人爲風險降低以及先進的品牌保護。

請查看下一頁以了解我們提供的功能。

proofpoint.

About Proofpoint, Inc. Proofpoint, Inc. 是 全球領先 的人員與智能體爲中心的 網路安全公司， 致力於保護 人員、 資料 及 AI 代理 在 電子郵件、雲端 與 協作工具 中的連結安全。 Proofpoint 是 超過 80 家 《財富》 百大企業、 逾 10,000 家 大型企業 及 數百萬家 中小型組織 的可信賴夥伴，協助其阻止威脅、 防止資料外洩， 並在 人員 與 AI 爲核心的工作流程 中建立韌性。 Proofpoint 的 協作與資料安全平台 協助各規模組織 在安全且自信地擁抱 AI 的同時， 保護並賦能其人員。 詳情請參閱 www.proofpoint.com 。

與 Proofpoint 連結： LinkedIn

Proofpoint 是 Proofpoint, Inc. 在美國 及/或其他 國家/地區 的註冊商標 或商號 。 本文所載其他商標 均爲其各自所有者 的財產。

©Proofpoint, Inc.2026

	可用功能	Core Email Protection	Collaboration Security層級 2	Collaboration Security層級 3	Collaboration Security Prime
電子郵件安全	BEC、網路釣魚、回撥式網路釣魚和惡意軟體防護	●	●	●	●
	由 Nexus AI 驅動的多層次偵測架構	●	●	●	●
	來自超過 280 萬客戶的無與倫比威脅資料	●	●	●	●
	附件與 URL 沙箱檢測	●	●	●	●
	即時 URL 防護：重寫與沙箱	SEG	SEG	SEG	SEG
	隔離對已重寫 URL 的可疑點擊	VAPs*	所有使用者*	所有使用者*	所有使用者*
	反垃圾郵件和灰色郵件偵測	●	●	●	●
	情境式電子郵件警示標籤	●	●	●	●
	郵件防護自我學習 依使用者行爲調整	●	●	●	●
	可配置的郵件路由策略	SEG	SEG	SEG	SEG
	自動訊息修復	●	●	●	●
	自動管理濫用信箱	●	●	●	●
	Very Attacked People (VAP)™、威脅行爲者與全球情報。	●	●	●	●
多管道， 多階段威脅防護	偵測並修復被入侵的雲端帳戶		●	●	●
	阻擋透過訊息與協作應用程式傳送的惡意 URL		●	●	●
	供應商帳戶保護		●	●	●
人員韌性與安全意識	系統能依據風險情境自動引導使用者			●	●
	利用基於真實威脅的模擬演練來建立員工的安全意識			●	●
	將主動威脅轉化爲安全模擬			●	●
冒充防護	透過電子郵件身份驗證防止品牌濫用				●
	偵測並修復惡意仿冒網域				●
	提供安全的應用程式郵件中繼服務，具備 250 GB 容量				●

SEG = 僅限安全電子郵件閘道部署

*僅限 SEG 部署。

©Proofpoint, Inc.2026