趨勢科技

ScanMail™ Suite for Microsoft® Exchange™

優異的防護、更輕鬆的管理。

絕大多數的針對性攻擊和勒索病毒事件都是從網路釣魚郵件開始，換句話說，您的電子郵件防護比以往更加重要。但不幸的是，大部分的郵件伺服器防護解決方案，包括 Microsoft Exchange Server 內建的防護，都採用一些較老舊的技術，而這些技術無法偵測今日的現代化惡意程式、惡意巨集、惡意網址，以及無檔案式攻擊。

ScanMail™ Suite for Microsoft® Exchange™ 採用預判式機器學習、文件漏洞偵測、客製化可疑檔案與網址沙盒模擬分析等其他解決方案所沒有的防禦技巧，來防範針對性網路釣魚和勒索病毒攻擊。

此外，還有一些可幫您節省時間的功能，例如：集中管理、搜尋與清除 (Search and Destroy) 以及角色導向的存取控管，讓 ScanMail 成為最容易安裝及操作的防護之一，並且享有盛名。

優勢

優異的針對性網路釣魚和勒索病毒攻擊防護

- 採用最先進的偵測技巧 (如預判式機器學習與文件漏洞攻擊偵測) 來發掘檔案、巨集與腳本中的未知威脅。
- 在郵件送達使用者信箱之前預先攔截含有惡意網址的郵件，並且在使用者點選連結時再對網址進行一次分析。
- 防止歹徒利用已遭入侵的帳號或裝置從內部發出電子郵件的多重階段攻擊。
- 當搭配趨勢科技 Deep Discovery™ Analyzer 一起使用時，可在客製化沙盒模擬環境當中動態分析可疑檔案和網址，並且將入侵指標 (IoC) 分享給其他趨勢科技解決方案或第三方廠商資安產品。
- 利用專家系統與機器學習等人工智慧來檢查電子郵件標頭、內容、作者以攔截變臉詐騙 (BEC) 攻擊，並且針對高風險的使用者套用更嚴格的防護規則。
- 利用我們獨家的 Writing Style DNA (寫作風格 DNA) 技術來防範假冒高階主管名義發信的詐騙。ScanMail 這項防護功能採用機器學習技術預先學習某高階主管的寫作風格，當收到宣稱來自該主管的英文郵件時，會檢查其寫作風格是否跟機器學習技術所學到的相符。

降低 IT 成本

利用強大的群組設定與管理，以及集中式記錄檔與報表，簡化電子郵件防護作業。

- 創新的搜尋與銷毀 (Search and Destroy) 功能可減輕企業搜尋電子郵件的繁複工作。
- 透過集中管理、範本導向的資料外洩防護 (DLP) 來簡化法規遵循與資料隱私權計畫。

軟體

防護點

- 郵件伺服器
- 內部檢查
- 內送和外寄的資料

威脅與資料防護

- 防毒
- 勒索病毒
- 網站威脅防護
- 垃圾郵件防護
- 網路釣魚防護
- 內容過濾
- 資料外洩防護
- 針對性攻擊

主要功能

防範魚叉式網路釣魚和針對性攻擊

有別於其他電子郵件防護解決方案，ScanMail 提供了強化式網站信譽評等、文件漏洞攻擊偵測、沙盒模擬執行分析，以及客製化威脅情報。這些進階防護功能結合起來，能提供完整防護來防範電子郵件威脅，包括：APT 和其他針對性威脅相關的魚叉式網路釣魚攻擊。

- 偵測 Adobe PDF、MS Office 及其他文件格式的已知及未知漏洞。
- 若與選購的 Deep Discovery Analyzer 整合，還可進行惡意程式模擬執行分析，並且產生客製化威脅情報及適應性安全更新。
- 運用業界領先的全球威脅情報提供立即的防護，防止威脅進入您的環境。

資料外洩防護 (DLP) 附加模組

延伸您現有的防護以支援法規遵循作業，同時預防資料外洩。這套整合式資料外洩防護可簡化資料防護，讓您清楚掌握及監控移動中與儲存中的資料。

- 搜尋並追蹤您郵件系統內所傳遞以及郵件資料庫當中所儲存的敏感資料。
- 藉由 100 多種法規遵循範本來加快設定並提升準確率。
- 讓法規遵循人員利用 Control Manager™ 來集中管理端點至閘道各種趨勢科技產品的資料外洩防護政策及違規事件。

專為 Microsoft® Exchange 而最佳化

ScanMail 能與您的 Microsoft 環境密切整合，以最低的系統負荷提供高效率的電子郵件防護。

- 可搭配趨勢科技 Cloud App Security 來支援 Office 365 與 Exchange Server 混合的環境。
- 利用 TrustScan (信賴掃瞄) 來避免重複檢查，此外更採用多重執行緒掃瞄與 CPU 用量調節技術。
- 與 Microsoft® System Center Operations Manager 及 Outlook® Junk E-mail Filter 整合。
- 採用角色導向存取控管來防止政策遭到未經授權的變更。

創新的搜尋與銷毀功能

有別於 Exchange 內建的工具，ScanMail 的搜尋並清除 (Search and Destroy) 功能可迅速而準確地尋找電子郵件。

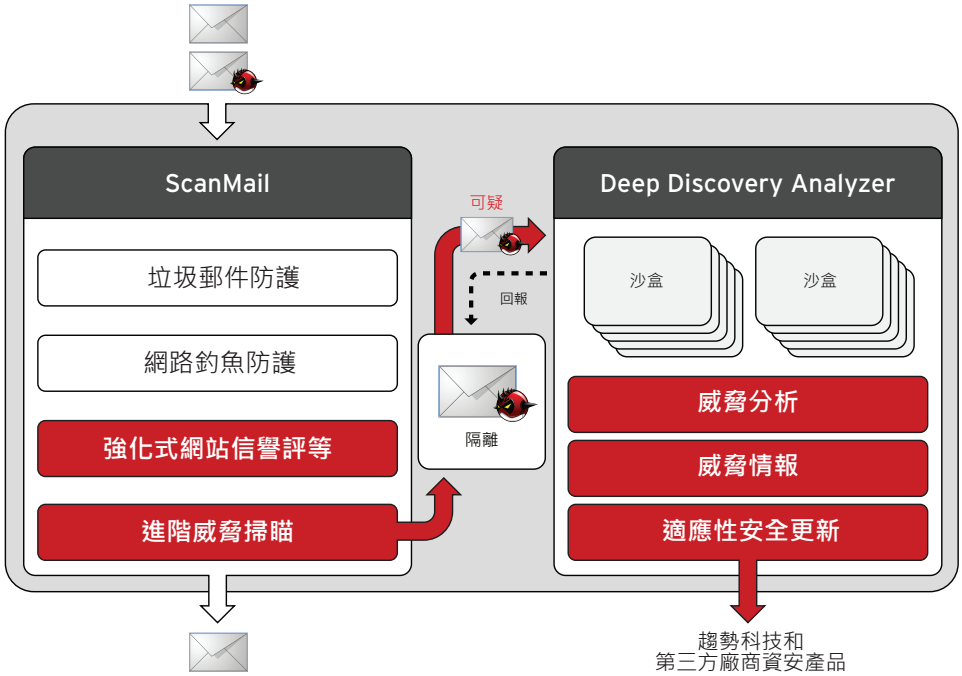
- 提供關鍵字和正規表示法 (regular expression) 的搜尋方式來搜尋 Exchange 資料庫。
- 讓系統管理員快速回應法務、人事或資安部門的緊急要求，搜尋、追蹤某些特定郵件，必要時甚至將郵件永久刪除。

主要效益

- 防止一般使用者遭到針對性攻擊，如魚叉式網路釣魚。
- 提供領先的雲端防護，在郵件伺服器攔截威脅，不讓威脅侵害使用者。
- 提供資料的掌握及監控，預防資料外洩，支援法規遵循。
- 藉由原生的 64 位元支援來加快處理速度。

Connected Threat Defense 環環相扣的威脅防禦

趨勢科技郵件防護解決方案能搭配 Deep Discovery Analyzer 來提供沙盒模擬執行功能並分享入侵指標。如此就能串連您的電子郵件、端點及網路防禦，讓您偵測、分析、調整及回應針對性攻擊。



ScanMail Suite

ScanMail Suite 郵件防護套裝軟體全新內建針對性攻擊防護。

強化式惡意網址防護：可攔截內文或附件內含有惡意網址的電子郵件。當使用者點選網址時，再對網站進行一次分析。它採用趨勢科技 Smart Protection Network™ 經由大數據及預測技術所關聯分析而來的威脅資訊。

進階威脅掃描引擎：採用預判式機器學習及經驗式分析邏輯來偵測已知及零時差漏洞攻擊，可偵測 Adobe PDF、MS Office 巨集、腳本以及其他文件格式當中的進階惡意程式。此外，還可掃瞄 Exchange 的郵件資料庫是否有防護建置之前即已入侵的針對性威脅。

若與 Deep Discovery Analyzer 整合，ScanMail 還能將可疑的附件檔案與網址隔離並立刻自動執行沙盒模擬分析，由於是在內網執行，因此絕大部分的郵件遞送作業皆不受影響。

Deep Discovery Analyzer (另外選購)

Deep Discovery Analyzer 是一個提供沙盒模擬執行分析、深度威脅分析以及本地端防護更新的硬體裝置，也是個單一整合情報平台，為趨勢科技 Connected Threat Defense 環環相扣的威脅防禦核心。

客製化威脅分析：提供一個安全的沙盒模擬環境來進行潛在惡意附件檔案與網址的自動化深度模擬執行分析。讓客戶建立多個與其主機環境完全相同的客製化系統映像來分析可疑物件。其專利的沙盒模擬分析技術在 2017 年 NSS Labs 入侵偵測 (Breach Detection) 測試當中展現 100% 的威脅與躲避技巧偵測率。

客製化威脅情報：將您環境所遭遇的攻擊資訊與趨勢科技豐富的威脅情報連結來提供深入的分析，協助執行事件風險評估、情況控制與矯正。

適應性安全更新：針對沙盒模擬分析過程當中新發現的幕後操縱 (C&C) 伺服器位置與惡意下載網站來產生客製化防護更新。讓趨勢科技端點及閘道產品，以及第三方廠商網路防護層獲得更好的適應性防護。

系統需求

ScanMail Suite 支援所有與 Microsoft Exchange 相容的虛擬環境。

Microsoft Exchange 系統需求

ScanMail 搭配 Microsoft Exchange Server 2016

資源	需求
處理器	x64 架構處理器，支援 Intel™ 64 架構 (原名 Intel EM64T) x64 架構電腦，採用支援 AMD64 平台的 AMD™ 64 位元處理器
記憶體	1 GB 記憶體，保留給 ScanMail 專用 (建議 2 GB)
硬碟空間	5 GB 可用硬碟空間
作業系統	Microsoft™ Windows Server™ 2016 Standard 或 Datacenter (64 位元) Microsoft™ Windows Server™ 2012 R2 Standard 或 Datacenter (64 位元) Microsoft™ Windows Server™ 2012 Standard 或 Datacenter (64 位元)
郵件伺服器	Microsoft Exchange Server 2016
網站伺服器	Microsoft Internet Information Services (IIS) 10.0 Microsoft Internet Information Services (IIS) 8.5 Microsoft Internet Information Services (IIS) 8.0
瀏覽器	Microsoft™ Internet Explorer™ 7.0 或更新版本 Mozilla Firefox™ 3.0 或更新版本
MSXML	4.0 Service Pack 2 或更新版本
.NET Framework	4.5 或 4.6

ScanMail 搭配 Microsoft Exchange Server 2013

資源	需求
處理器	x64 架構處理器，支援 Intel™ 64 架構 (原名 Intel EM64T) x64 架構電腦，採用 AMD™ 64 位元處理器
記憶體	1 GB 記憶體，保留給 ScanMail 專用 (建議 2 GB)
硬碟空間	5GB 可用硬碟空間
作業系統	Microsoft™ Windows Server™ 2012 R2 Standard 或 Datacenter (64 位元) Microsoft™ Windows Server™ 2012 Standard 或 Datacenter (64 位元) Microsoft™ Windows Server™ 2008 R2 Standard 含 Service Pack 1 或更新版本 (64 位元) Microsoft™ Windows Server™ 2008 R2 Enterprise 含 Service Pack 1 或更新版本 (64 位元) Microsoft™ Windows Server™ 2008 R2 Datacenter RTM 或更新版本 (64 位元)
郵件伺服器	Microsoft Exchange Server 2013 SP1 或更新版本
網站伺服器	Microsoft Internet Information Services (IIS) 8.5 Microsoft Internet Information Services (IIS) 8.0 Microsoft Internet Information Services (IIS) 7.5
瀏覽器	Microsoft™ Internet Explorer™ 7.0 或更新版本 Mozilla Firefox™ 3.0 或更新版本
MSXML	4.0 Service Pack 2 或更新版本
.NET Framework	4.0 或 4.5

ScanMail 搭配 Microsoft Exchange Server 2010

資源	需求
處理器	x64 架構處理器，支援 Intel™ 64 架構 (原名 Intel EM64T) x64 架構電腦，採用 AMD™ 64 位元處理器
記憶體	1 GB 記憶體，保留給 ScanMail 專用 (建議 2 GB)
硬碟空間	5GB 可用硬碟空間
作業系統	Microsoft™ Windows Server™ 2012 R2 Standard 或 Datacenter (64 位元) Microsoft™ Windows Server™ 2012 Standard 或 Datacenter (64 位元) Microsoft Windows Server 2008 R2 或更新版本 (64 位元) Microsoft Windows Server 2008 含 Service Pack 2 或更新版本 (64 位元) Microsoft Small Business Server (SBS) 2011* *Microsoft Small Business Server (SBS) 2011 曾搭配 ScanMail 第 12 版進行過有限的相容性測試。安裝前，建議先解除安裝 Microsoft ForeFront 之後再於 Microsoft Small Business Server (SBS) 2011 安裝 ScanMail。
郵件伺服器	Microsoft Exchange Server 2010 SP3 或更新版本
網站伺服器	Microsoft Internet Information Services (IIS) 8.0 Microsoft Internet Information Services (IIS) 7.5
瀏覽器	Microsoft™ Internet Explorer™ 7.0 或更新版本 Mozilla Firefox™ 3.0 或更新版本
MSXML	4.0 Service Pack 2 或更新版本
.NET Framework	3.5 Service Pack 1