

Trend Vision One™ - Endpoint Security

專為端點、伺服器及雲端工作負載最佳化的防範、偵測及回應

Trend Vision One™ - Endpoint Security 是一套領先的端點防護解決方案，專為保護端點、伺服器及雲端工作負載而打造，整合了進階威脅防護、EDR/XDR 以及威脅情報。這套解決方案能協助您簡化 IT/資安營運、降低複雜性，並獲得最佳的資安成效，涵蓋您的企業內、雲端、多重雲端以及混合環境。

Trend Vision One™ 是一套現代化雲端原生網路資安平台，提供了最廣泛的原生解決方案以及第三方整合能力，讓您將端點和工作負載防護與其他防護產品、威脅情報、SIEM、協調系統、建構流程、受攻擊面管理連結起來。Trend Vision One 支援多元混合 IT 環境，有助於自動化並協調工作流程，提供專業的資安服務，讓您更快攔截敵人並掌握您的資安風險。

整合式 EDR

有了 Trend Vision One 您的客戶將獲得 XDR 的優勢以及整合式 EDR 功能。

- 接收經過優先次序過濾、可採取行動的警報以及完整的事件檢視。
- 跨 Linux 和 Microsoft Windows 系統調查問題根源與攻擊執行狀況，找出攻擊的範圍並直接觸發回應。
- 透過多種方式追蹤威脅（從強大的查詢到簡單的文字搜索），主動精確掌握駭客的攻擊手法或技巧，並釐清環境當中的可疑活動。
- 藉由趨勢科技的自動化情報或客製化情報掃描，持續搜尋是否有最新發現的入侵指標 (IoC)。

多層式防範、偵測及回應提供完整的威脅防護

透過自動化的進階資安控管與領先業界的最新威脅情報來獲得即時的防護，防範日益多樣化的威脅。

有了豐富完整的多層式防範、偵測及回應功能，例如：現代化惡意程式防護與勒索病毒防護、裝置控管、主機入侵防護、應用程式控管、機器學習/AI 等等，您就能即時保護自己的端點、虛擬桌面、伺服器以及雲端工作負載。

防護點

- 實體端點
- Microsoft® Windows® 個人電腦與伺服器
- Mac 電腦
- POS 銷售櫃台系統和 ATM 提款機
- 伺服器
- 雲端工作負載
- 虛擬機器

威脅偵測能力

- 高準度機器學習
- (執行前靜態檔案偵測和執行中程序分析)
- 行為分析 (防範腳本、隱碼注入、勒索病毒、記憶體和瀏覽器攻擊)
- 記憶體內無檔案惡意程式分析
- 變種防範
- 普查
- 網站信譽評等
- 漏洞防護 (主機防火牆、漏洞攻擊防護)
- 幕後操縱 (C&C) 通訊攔截
- 資料外洩防護 (DLP)
- 裝置與應用程式控管
- 勒索病毒復原
- 沙盒模擬分析及入侵偵測整合
- 延伸式偵測及回應 (XDR)

專為您伺服器及雲端工作負載打造的防護

專為混合雲設計的現代化雲端原生防護

- 工作負載從啟動的那一刻開始就可能遭到攻擊，趨勢科技內建工作負載偵測功能，與 AWS、Microsoft Azure、Google Cloud Platform、VMware 以及 Microsoft Active Directory 整合，從工作負載建立的那一刻起便立即提供防護。
- 消除部署多套單一面向解決方案的成本，透過單一管理主控台，讓實體、虛擬、雲端、容器及使用者端點環境皆享有一致的防護。
- 透過一致性監控和記錄檔檢查功能來監控 Docker 和 Kubernetes 平台是否出現任何遭到變更或攻擊的跡象。
- 採用容器漏洞防護 (透過 IPS)、即時惡意程式防護，以及容器橫向網路流量檢查，來保護執行時期的容器。

端點、伺服器及其應用程式的入侵與漏洞防護

入侵防護模組可保護您的環境，防範已知及零時差漏洞攻擊、SQL 隱碼注入攻擊、跨網站腳本攻擊，以及其他網站應用程式漏洞。

我們的漏洞防護與入侵防護能提供虛擬修補，在廠商釋出修補更新之前預先防堵已知的漏洞。並有我們領先全球的 Zero Day Initiative (ZDI) 漏洞懸賞計畫作為後盾。

檔案一致性監控

一致性監控模組能掃描系統登錄數值、登錄機碼、系統服務、處理程序、已安裝軟體、連接埠以及檔案的非預期性變更。一致性監控模組會使用一個基準的安全狀態作參考來掃描上述項目，並在偵測到任何非預期性變更時新增一筆事件記錄 (可選擇性發出警報)。

記錄檔檢查

記錄檔檢查模組可協助您發掘您作業系統與應用程式記錄檔中可能埋藏的重要事件。

記錄檔檢查模組可讓您：

- 偵測可疑行為。
- 蒐集來自異質環境的事件，包括不同的作業系統和各種應用程式。
- 檢視事件，例如錯誤與資訊事件 (磁碟已滿、服務啟動、服務停止等等)。
- 產生及維護系統管理員活動的稽核記錄 (系統管理員登入或登出、帳號鎖定、政策變更等等)。

Endpoint Security 中的記錄檔檢查功能可提供第三方記錄檔的即時分析。記錄檔檢查規則與解碼功能提供了一套框架來解讀、分析、排序與交叉關聯事件，涵蓋各式各樣的作業系統。

第三方認證的領先地位

- 趨勢科技自 2002 年起即獲選為 Gartner 端點防護平台神奇象限 (Magic Quadrant for EPP) 領導者 (連續 19 年)
- 連續 5 年 (2022 年) 蟬聯雲端工作負載防護市場占有率 (Cloud Workload Security Market Share) 第一
- Forrester New Wave™: 延伸式偵測及回應 (XDR) 領導者 (2021 年第 4 季)
- MITRE Engenuity ATT&CK (2022 年) - Linux 防護力第一，能 100% 偵測及防範所有針對 Linux 主機的攻擊。

保護您的 Linux 平台

趨勢科技的平台廣泛支援各種 Linux 發行版本與數百種 Linux 核心，以及 Solaris™、AIX® 和 HP-UX®。

實現符合成本效益的法規遵循

採用單一、整合又符合成本效益的解決方案來達成重大法規遵循要求，例如：GDPR、HIPAA、NIST 等等。

Trend Vision One - Endpoint Security 產品

	Core	Essentials	Pro
主要端點類型	使用者端點與基礎伺服器	使用者端點與基礎伺服器	關鍵端點 (包括伺服器和工 作負載)
Windows、Linux 和 Mac OS	●	●	●
惡意程式防護、行為分析、機器學習、網站信譽評等	●	●	●
裝置控管	●	●	●
資料外洩防護 (DLP)	●	●	
防火牆	●	●	●
應用程式控管	●	●	●
入侵防護 - IPS (作業系統)	●	●	●
虛擬化防護	●	●	●
EDR-XDR		●	●
入侵防護 - IPS (伺服器應用程式)			●
一致性監控 / 記錄檔檢查			●
	Core	Essentials	Pro
電子郵件防護	+	+	+
行動安全防護	+	+	+
網路防護	+	+	+
雲端防護	+	+	+
零信任安全存取	+	+	+
MDR / Service One		+	+
受攻擊面風險管理 (ASRM)		+	+

+ 代表附加選項

©2023 年版權所有。趨勢科技股份有限公司保留所有權利。Trend Micro、t 字
球形標誌、Apex One 及 Trend Micro Apex Central 是趨勢科技股份有限公司
的商標或註冊商標。所有其他公司和產品名稱為該公司的商標或註冊商標。本
文件之內容若有變動，恕不另行通知。[DSOI_Datasheet_Template_221213TW]

如需有關我們蒐集哪些個人資料的詳細內容和理由，請參閱我們的網站上的「
隱私權聲明」：trendmicro.com/privacy