



Trellix 端點 安全(HX)

利用前線回應的知識，阻擋攻擊

每天都會出現新的網路攻擊、新的漏洞或新的勒索軟體目標。安全團隊發現，已越來越難以應付對他們的用戶、公司資料和智慧財產權的威脅，且並不一定能提供額外幫助。回應者背負了過多的工具，這些工具無法協同工作，且產生的雜音多過於有用的訊號。現有的系統並不一定能夠對這些高階威脅提供足夠的偵測和回應。

Trellix 端點安全(HX)藉由使用深度防禦模型，來防禦現今的網路攻擊。端點安全(HX)的模組化架構，將預設引擎和可下載模組互相結合，以保護、偵測、回應和管理端點安全性。

重點

- 防範針對端點的大部分網路攻擊
- 偵測並阻擋攻擊行為，以減少其影響
- 藉由發現威脅而非追逐警報，以改善生產力和效率
- 使用單一、占用空間小的代理，最小化對最終用戶的影響
- 藉由可下載模組來獲得額外的保護和功能
- 遵守「支付卡產業資料安全標準(PCI-DSS)」和「健康保險流通與責任法案(HIPAA)」等法規
- 地端或雲端部署

為了防範常見的惡意軟體，端點安全(HX)使用了依據簽章的端點防護平台(EPP)引擎。為尋找尚不具有簽章的威脅，惡意軟體防護(Malware Guard)會使用機器學習，其中包含來自網路攻擊前線的知識。針對常見軟體和瀏覽器中漏洞的攻擊，漏洞防護(Exploit Guard)則會使用行為分析引擎，來確定是否正在使用漏洞並阻止其執行。此外，Trellix 也會不斷開發出新模組來偵測攻擊技術，並加速對新興威脅的回應。例如，流程防護(Process Guard)的開發，即是為了防止憑證外洩。

即使有最好的保護，違規行為也是無法避免的。為了確保能做出實質回應、大幅減少業務中斷，端點安全(HX)因此包含了端點偵測和回應功能，這些功能是仰賴由一線回應人員的幫助下所開發的即時入侵指標(IOC)。Trellix 工具還可以：

- 在幾分鐘內，搜索調查出數萬個端點上的已知與未知威脅
- 識別並詳細說明用於滲透端點的攻擊向量
- 確定是否在特定端點上發生(並持續)攻擊，及其傳播位置
- 建立端點受損的時間表、持續時間，並追蹤事件

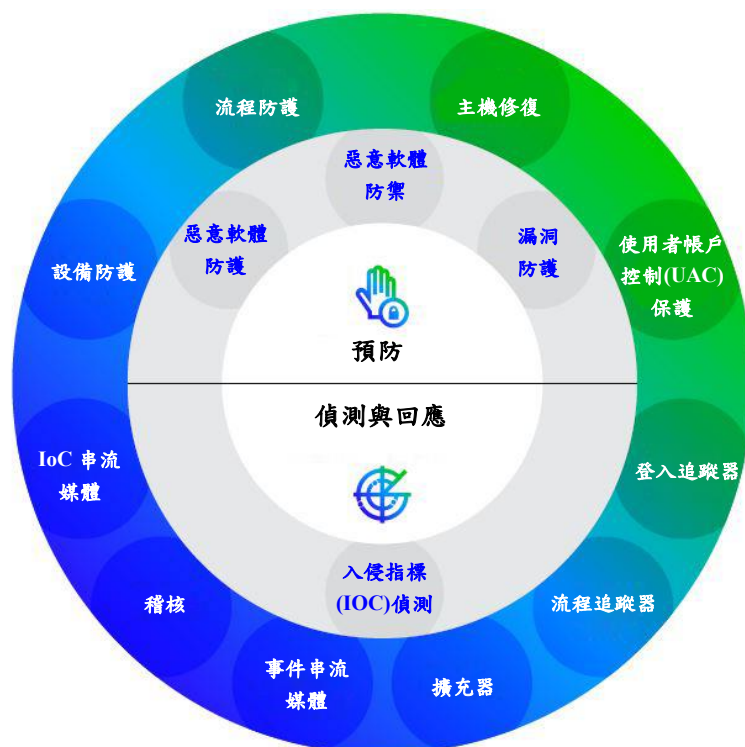


圖 1：Trellix 端點安全(HX)核心引擎(內圈)和可用模組(外圈)。

今日的威脅並不會僅發生在一個端點上，因此，在單一端點上進行修復，並不能解決大多數的資安漏洞。全面修復可有效溝通與指向可能隱藏威脅的所有設備，並即時將這些資訊建立關聯性。端點安全(HX)與 Trellix XDR 自然地整合，無縫連接所有 Trellix 技術和服務，以偵測和回應所有最複雜的威脅。

主要特點

- 單一代理使用深度防禦而最小化配置，並最大化檢測和阻擋
- 用於分析和回應端點安全(HX)內威脅的整合工作流程
- 防禦惡意軟體，包括反惡意軟體防護、機器學習、行為分析、入侵指標(IOC)和端點可見性
- 與 Trellix XDR 自然地整合，獲得更多可見性和控制力，以全面修復組織中的所有威脅

附加特點

- 企業搜尋(Enterprise Search)可快速找到並闡明可疑活動和威脅
- 在特定時間範圍內進行數據採集(Data Acquisition)，以進行詳細深入的端點檢查和分析
- 端到端可見性(End-to-end visibility)，能使安全團隊更快速搜尋、識別和辨別出威脅等級
- 偵測和回應功能可快速偵測、調查和遏制端點，以加快回應速度
- 易於理解的介面，可快速詮釋和回應任何可疑的端點活動

支援作業系統和環境

Windows	Windows 7, 8, 8.1, 10, 11 伺服器 2008R2, 2012R2, 2016, 2019
Mac	10.9 - 10.15, 11, 12, 13
Linux	RHEL 6.8 - 6.10, 7.2 - 7.9, 8.0 - 8.3 CentOS 6.8 - 6.10, 7.2 - 7.7, 8.0 SUSE 11 SP3, SP4, 12 SP2 - SP5, 15 GA Open SUSE Leap 15.1, 15.2 Ubuntu 14.04, 16.04, 18.04, 19.04, 20.04 LTS Amazon Linux AMI 2018.3, AM2, Amazon Linux 2 Oracle Linux 6.10, 7.6, 8.1, 8.2

可導入選項：實體設備、虛擬設備、雲端託管設備。

瀏覽 [Trellix.com](https://trellix.com) 以深入瞭解。



關於 Trellix

Trellix 是一家重新定義網路安全和熱情工作之未來的全球性公司。該公司的開放式本地擴展偵測和回應(XDR)平台，可協助面臨當今最先進威脅的組織對其營運防護和復原能力充滿信心。Trellix 與廣泛的合作夥伴生態系統，透過機器學習和自動化加速技術創新，為超過 40,000 家企業和政府客戶提供即時安全。欲知更多資訊，可瀏覽 <https://trellix.com>。