Netskope One 威脅防護

資料表

防範 Web 和雲端威脅

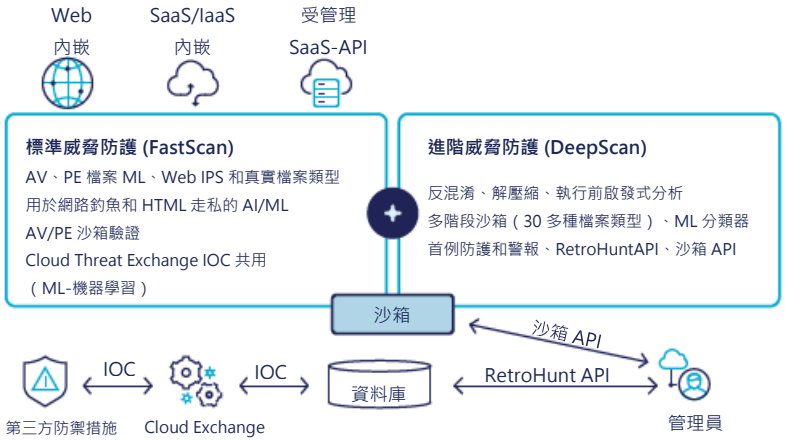
針對內嵌 Web 和雲端流量以及受管理應用程式和雲端服務中的靜態資料提供多層威脅防護，抵禦惡意軟體和進階威脅。此外，透過整合在防禦措施與威脅情報來源之間進行自動化雙向威脅情報共用。

為何 Netskope 是最佳選擇？

Netskope One 安全服務邊緣 (SSE) 威脅防護針對進階惡意軟體（例如勒索軟體）和網路釣魚提供高效力威脅偵測和攔截。如需詳細資訊，請參閱最近的 AV-Test 報告。有別於端點，對於只有幾毫秒的時間可偵測威脅的閘道而言，威脅防護效果堪稱「同類最佳」，並提供快速的使用者體驗。

為安全存取服務邊緣 (SASE) 架構提供全面的 SSE 威脅防護

- **內嵌機器學習分析：**標準威脅防護提供針對新型惡意軟體的首例威脅防護，以及反惡意軟體、Web IPS、沙箱、威脅情報來源和自動化 iOC 共用。
- **DeepScan 背景分析：**進階威脅防護提供反混淆和遞迴檔案解壓縮、執行前啟發式分析，以及支援 30 多種檔案類型的多階段沙箱與行為分析。
- **首例防護和警報：**DeepScan 新型惡意軟體偵測針對首批暴露使用者提供首例防護和警報，此外，Cloud Exchange 可將 SOAR、XDR 和 MDR 服務調查自動化。
- **沙箱和 RetroHunt API：**新的進階沙箱 API 用於提交檔案，並結合 MITRE ATT&CK 分析。此外，透過檔案雜湊值呼叫的 RetroHunt API 可判定檔案屬於惡意或良性。



主要效益和能力

經驗證的有效威脅防護

在最近的 AV-TEST 中，Netskope One SSE 的不可移植可執行檔 (PE) URL 偵測率為 99.29%，PE URL 偵測率為 99.89%。如需詳細資訊，請參閱報告。

防範未知惡意軟體

以 AI/ML 為基礎的新型 PE 惡意軟體、網路釣魚威脅和 HTML 走私攻擊偵測，提供零日防護。

標準和進階沙箱

所有 AV 和 ML 標準威脅偵測都會經過沙箱處理。進階沙箱增加 MITRE ATT&CK 詳細分析、沙箱 API 檔案提交、透過雜湊值呼叫的 RetroHunt API，以及獨特的首例偵測。

自動化威脅情報共用

Cloud Threat Exchange 免費提供給客戶，將防禦措施之間的雙向 IOC 共用自動化，包括端點、電子郵件安全性和威脅情報來源。

混合工作第一道防線

轉型至 SSE 以涵蓋任何使用者、裝置和位置，而非將流量繞回至無法對應用程式和雲端服務進行解碼的舊有安全設備。

「Netskope 的 PE 檔案 URL 偵測率為 99.89%，非 PE URL 偵測率為 99.29%，網路釣魚攻擊偵測率為 96.77%。」

–AV-TEST 報告，2024 年 1 月

Netskope 的獨特之處

Netskope One 是融合式安全與網路即服務平台。

透過獲專利的零信任引擎、AI 創新以及最大的私有安全雲端，我們讓客戶輕鬆保護其業務和資料，同時提供非凡的終端使用者體驗並簡化操作。此平台提供 AI 驅動資料和威脅防護，可自動適應不斷變化的資料情勢，包括生成式 AI 普及和新型 AI 驅動攻擊。

特色	能力
標準威脅防護	提供反惡意軟體、以 ML 為基礎的 PE 檔案分析、AI/ML 即時網路釣魚和 HTML 走私偵測、AV/ML 驗證沙箱、Web IPS、真實檔案類型檢查，以及 40 多個威脅情報來源。Web 過濾也提供可封鎖的安全風險類別。
進階威脅防護	增加背景防禦，包括反混淆、遞迴檔案解壓縮、執行前啟發式分析、支援 30 多種檔案類型的多階段沙箱、ML 分類器和分析、首例防護和新偵測警報、用於檔案提交的沙箱 API、透過檔案雜湊值呼叫的 RetroHunt API，以及 MITRE ATT&CK 沙箱分析報告。此外，也支援將內嵌惡意軟體保留至客戶雲端儲存空間以及 API 檢查隔離。
Cloud Exchange	四個模組，共用威脅情報、將工作流程自動化、交換風險評分，以及匯出紀錄。免費提供給客戶，超過 70 個合作夥伴整合。Cloud Threat Exchange (CTE) 模組能與標準或進階威脅防護搭配使用，將客戶防禦措施之間的 IOC 更新自動化。
附加防禦措施（RBI、EB、FWaaS、IPS、DNS 安全性、UEBA）	加強威脅防護，目標型或延伸型遠端瀏覽器隔離 (RBI) 針對高風險網站和個人通訊，企業瀏覽器 (EB)、防火牆即服務 (FWaaS) 和入侵防護 (IPS) 針對非 Web 出口流量，DNS 安全性針對威脅和新網域，行為分析 (UEBA) 可偵測內部威脅、資料竊取和外洩、裝置或帳戶遭入侵，並在即時自適應存取原則中利用使用者信心指數 (UCI) 評分。
沙箱檔案類型支援	沙箱檔案格式包括：apk、.csv、.dex、.jar、.html、.htm、.json、.swf、.mht、.eml、.mbx、.pem、.crt、.cer、.key、.pdf、.txt、.sgm、.tsv、Unicode 文字檔案、.xhtml、.xml、.xpi、壓縮檔（.7z、.lzfse、.msix、.war、.whl、.rar、.rev、.tar、.zip）和 Microsoft 檔案（.accdb、.mdb、.chm、.xlsx、.xlsm、.msg、.pptx、.pptm、.xap、.docx、.docm、.msi、.bat、.cmd、.one、.lnk），可能包括其他檔案格式。

netskope

想要深入瞭解嗎？ 要求示範

Netskope 是全球 SASE 領導者，利用零信任原則和 AI/ML 創新來保護資料並抵禦網路威脅，將安全性和效能最佳化而不必妥協。數千個客戶仰賴 Netskope One 平台及其強大的 NewEdge 網路來降低風險並獲得無與倫比的可見性，掌握任何雲端、Web 和私有應用程式活動。深入瞭解：netskope.com。