Netskope One SASE Device Intelligence

資料表

Netskope One SASE Device Intelligence 為企業分公司 IT、IoT 和 OT 裝置提供脈絡驅動安全性

利用整合於統一 SASE 閘道中的裝置情報保護企業分公司環境中的所有裝置，支援分類、脈絡推導和全面可見性，有效管理資產。動態評估風險、執行控制措施並協調行動以抵禦現代威脅，同時確保合規性。

為何 Netskope 是最佳選擇？

Netskope Device Intelligence 解決方案利用 HyperContext® （無代理程式智慧裝置安全平台，提供精細的裝置脈絡）探索企業網路上的受管理和未受管理裝置。此解決方案可進一步分析數百個來自已探索裝置的參數，並利用豐富的脈絡情報進行裝置分類、動態風險評估、跨 LAN、WAN 和雲端的精細存取控制以及網路分段，為連網裝置促進零信任安全性。

充分發揮 AI/ML 驅動安全性的能力

Device Intelligence 整合於 Netskope 統一 SASE 閘道中，也可從 Netskope SASE 雲端取得。

- **裝置分類和可見性：**無代理程式裝置探索結合豐富的脈絡情報，支援自動化分類和裝置對映，並針對裝置活動和行為提供深入洞見。
- **網路安全資產管理：**針對已發現資產提供精細搜尋和報告，透過內建的資產清單引擎進行全面性網路安全資產管理，並與 ServiceNow CMDB、VA、MDM、EDR 整合以校準資產清單和資產管理資料庫。
- **裝置風險評估：**持續監測裝置以偵測異常、產生專屬的裝置風險評分，並根據裝置分類和標籤來對映警報。透過 SIEM 和 SOAR 整合簡化 SOC 自動化並使警報處理豐富化。
- **存取控制和分段：**根據脈絡和即時裝置行為進行動態裝置分組和微分段，提供精細、準確的經授權裝置存取，並利用現有網路系統（例如防火牆和網路存取控制）協調行動。

主要效益和能力

裝置探索

利用 ML 驅動的洞見完整呈現所有連網裝置及其風險概況，以有效追蹤和控制裝置，並遵守嚴格的稽核與合規性原則。

唯一裝置身分和分組

透過傳統的指紋辨識技術分析數百個裝置參數，產生唯一裝置識別碼和真實性評等。可將展現相似特性的裝置歸為同一群組，以便執行統一原則並建立群組的正常功能和行為。

AI/ML 驅動風險評估

辨識裝置層級的異常行為，並就裝置層級風險、威脅以及緩解威脅概況的最佳實務提供洞見與分析。

縮小攻擊表面

與 Cisco Meraki、Juniper Mist、Aruba ClearPass、Cisco ISE 等平台整合，在安全區域或微區段內動態進行裝置分組，以隔離高風險裝置並防止威脅的橫向移動（東西向）。

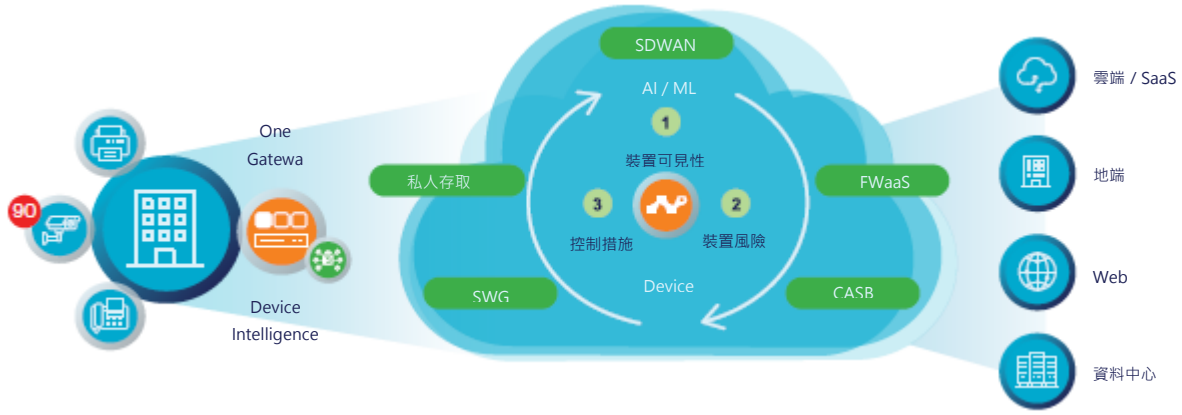
裝置脈絡豐富化

從部署在客戶環境中的多個安全性解決方案（包括 Tanium、Qualys、Infoblox、Microsoft Entra 和 ServiceNow 及其他整合）擷取資料，並執行高度準確且精細的原則決策。

動態 IDS 警報調整

動態警報調整確保您的團隊可優先處理真正的威脅，簡化工作流程，使網路維運變得更安全、更迅速且更有效。

Netskope One SASE



實際運作：某支保全攝影機被偵測到與命令和控制伺服器通訊之後，風險評分變成 90 並且被視為不安全，被在統一 SASE 閘道上運作的 Netskope Device Intelligence 動態封鎖。

Netskope 的獨特之處

Netskope One SASE 是融合式安全與網路即服務平台。Netskope One SASE 因裝置情報而進一步強化，此功能以服務形式在 Netskope 統一 SASE 閘道和 Netskope SASE 雲端運作，利用 AI/ML 探索、分類和建立脈絡。它透過第三方整合增強此功能，為所有 IT、OT 和 IoT 裝置提供全面可見性和有效的資產管理。此解決方案持續評估風險並與異常偵測工具整合，納入由 LLM 輔助、經過脈絡豐富化的威脅資訊，可用於根據即時裝置行為進行精準的存取控制。在 Netskope 統一 SASE 閘道、SSE 以及現有的網路基礎架構（例如防火牆和網路存取控制）上執行這些控制措施，保護分公司不被所有易受攻擊的 IoT 和 IT 裝置影響。

您的需求	NETSKOPE 解決方案
零信任存取	Netskope Device Intelligence 提供自適應存取控制、微分段並持續對所有已驗證裝置進行風險評估，將零信任延伸至 IT、IoT 和 OT 環境。
營運合規性	Netskope Device Intelligence 根據豐富的裝置遙測資料採取行動以找出和彌補安全性缺口，並滿足法規遵循要求。
可據以採取行動的警示情報	Netskope Device Intelligence 透過與 SIEM 平台的整合來應對資安事件。透過 SOAR 執行腳本大規模將警報處理自動化。
加強安全性和存取管理	Netskope Device Intelligence 與網路安全系統（包括防火牆、網路存取控制和存取點）無縫整合，以促進安全的裝置存取。
與 SASE 願景一致	Netskope Device Intelligence 的目標是將所有連網裝置納入稱為 Netskope One SASE 的統一安全存取服務邊緣 (SASE) 框架下，從集中式管理平台提供對分散式裝置的全面可見性、靈活的原則執行以及事件管理。