Netskope SaaS 安全態勢管理 (SSPM)

資料表

SaaS 可見性、安全性及合規性

現代 SaaS 應用程式可能具有數百個組態設定，以及眾多連接的第三方應用程式，這些應用程式往往會將資料、權限和特權延伸至受管理邊界之外。Netskope SSPM 是 SaaS 資料保護的第一道防線。

為何 Netskope 是最佳選擇？

Netskope SSPM 強化我們領先業界的 CASB，為組織提供全面的內嵌保護和以 API 為基礎的保護。強大的圖形化偵測和視覺化利用跨應用程式規則，在不同應用程式之間將脈絡相關聯以揭露隱藏風險。警報和通知內建引導式補救以修正安全性配置錯誤，並確保符合 CIS、PCI-DSS、NIST、HIPAA、CSA、GDPR、AIPCA、ISO 等業界標準。

Netskope SSPM 價值

- **預先定義的安全性與合規性規則：**涵蓋業界基準和標準，能夠快速部署 SaaS 安全性及合規性措施。
- **圖形化偵測和視覺化：**支援跨應用程式規則，在不同的 SaaS 應用程式之間將脈絡整合。
- **深入洞悉已連接和第三方應用程式：**揭露並緩解額外風險。
- **定義自訂規則和設定檔：**除了同類最佳現成規則與偵測之外，也可配合組織的特定需求。
- **加快補救速度：**提供逐步指引，快速解決安全風險。
- **全面的 API 集合：**可輕鬆整合至現有的安全性和自動化工作流程，以防止業務中斷。
- **統一檢視警報和事件：**包含來自整個 Netskope 平台的資訊。

主要效益和能力

圖形化偵測和視覺化

利用跨應用程式規則在不同的 SaaS 應用程式之間將脈絡相關聯，揭露隱藏風險。

SaaS 可見性，包括第三方 OAuth 應用程式

持續探索和監測 SaaS 配置、使用者和第三方 OAuth 應用程式，以消除盲點並管理風險。

SaaS 合規性

依據預先定義的最佳實務和業界標準進行驗證，以揭露並緩解配置錯誤和過度寬鬆的使用者存取權限。

引導式補救

警報包含逐步指示和自動化，快速修復 SaaS 配置錯誤。

可自訂規則和配置

SSPM 包含定義自訂規則和設定檔的功能，滿足您的 SaaS 安全性需求。

快速將異常情況轉換成新的偵測規則

強大的查詢語言可讓您搜尋異常情況，並根據結果輕鬆建立新的偵測規則。

廣泛整合

Netskope Cloud Exchange 支援與 Snowflake 和 Jira 進行 RESTful API 整合（用於工單處理），以及與 SIEM/SOAR 工具整合（用於自動化和協調）。

整合式 SASE 架構的一部分

SSPM 與 Netskope CSPM、NG-SWG、CASB、DLP、ZTNA、CFW、RBI 和進階分析互補，一切都在單一平台、單一主控台和單一原則引擎上提供。

「Netskope 提供對 SaaS 使用情況和風險暴露的可見性，這是我們過去所欠缺的。」

– 資訊安全經理
大型企業多元化消費者服務公司

netskope

探索和控制第三方 SaaS 應用程式和外掛程式

使用者正以越來越快的速度將不受信任的第三方 OAuth 應用程式連接至受管理的應用程式，例如 Microsoft 365、Google Workspace、Salesforce 和 Zoom。雖然這些未受管理的「外掛程式」實用且容易連接，但它們可能被攻擊者入侵，並用來存取受管理資源或竊取資料。由於這些應用程式的治理和資料移動發生在企業邊界之外的雲端，因此無法使用 CASB 或 SWG 解決方案加以探索或監測。

同樣地，EDR、XDR、相關 SIEM 等安全性工具也缺乏對這些應用程式的可見性。以下是組織因為這些應用程式而承擔的一些風險：

- **OAuth 漏洞**：通常使用 OAuth 連接第三方應用程式，OAuth 是被廣泛使用的協定，允許第三方存取資源。漏洞可能源自主要和第三方應用程式的實作，以及 OAuth 服務本身。
- **資料外洩**：授予第三方應用程式存取權限可能會使敏感資料暴露於潛在的安全漏洞之下。如果若未妥善保護或配置第三方應用程式，攻擊者可能未經授權存取敏感資料。
- **資料濫用**：某些第三方應用程式可能會收集資料並將資料用於非預定或未揭露的用途。
- **違規**：第三方應用程式可能存取超過其預定功能所需數量的資料，違反合規性或隱私法規。
- **失控**：第三方應用程式或許能夠控制帳戶或資料的某些部分，可能危及其他資源。
- **供應商風險**：如果第三方應用程式供應商遭入侵，該應用程式可能被當作特洛伊木馬，用以存取資料或發動供應鏈攻擊。

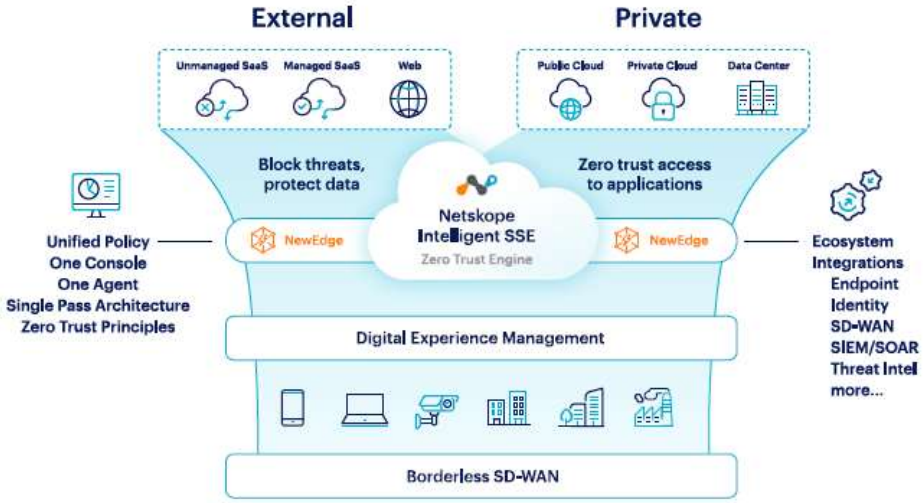
Netskope SaaS 安全態勢管理 (SSPM) 可探索並控制透過附加元件或外掛程式與組織的受管理應用程式建立的連線，以降低與第三方應用程式相關的風險。Netskope SSPM 持續監測組態設定中是否有任何與第三方應用程式的連線，並自動確定這些應用程式的風險評分以方便您採取行動，例如封鎖風險最高的應用程式。

SSPM 效益

- **提高可見性**：全面檢視和監測 SaaS 生態系統。
- **保護 SaaS 資料**：將敏感資料保留在 SaaS 生態系統內，防止資料外洩至未知位置和應用程式。
- **降低風險和縮小攻擊表面**：控制未知 SaaS 應用程式，並切斷危險連線以降低風險。
- **維持合規性**：防止使用者因連接高風險應用程式和外掛程式而危及稽核或洩露敏感資料。

Netskope 的獨特之處

Netskope 協助您降低風險、加快效能，並針對任何雲端、Web 和私有應用程式活動提供無與倫比的可見性。為了促進安全協作，Netskope 可靠地在信任與風險之間取得平衡，並提供可適應環境變化的精細控制。Netskope 平台可防範進階和雲端威脅，並跨所有向量（任何雲端、任何應用程式、任何使用者）保護資料。單通道架構提供快速的使用者體驗並簡化操作。



特色	能力
支援合規性措施	依據預先定義的最佳實務規則和業界標準（包括 CIS、NIST、HIPAA、PCI、CSA、GDPR、AIPCA、ISO 等）驗證安全態勢。
防止配置錯誤並降低風險	配置錯誤仍然是 SaaS 應用程式最常見的安全性問題。Netskope SSPM 使用圖形化偵測和視覺化，簡化安全態勢管理與合規性。
探索和控制第三方 SaaS 應用程式	Netskope SSPM 持續監測受管理應用程式的組態設定中是否有任何與第三方應用程式的連線，發現時會自動確定風險評分，您可以封鎖或控制這些應用程式，以降低風險。
補救	逐步指示和自動化，快速解決安全風險。可透過 RESTful API 匯出警報與合規性結果，以整合至工單處理和補救協調工作流程。
整合式 SASE 架構	Netskope SSPM 與 Netskope CASB、SWG、DLP、ZTNA 及其他 Netskope 產品整合，提供無縫且統一的管理、可見性和安全性解決方案。
SaaS 應用程式支援	支援 SaaS 應用程式，包括 Box、Dropbox、Egnyte、Facebook Workplace、GitHub、Google Workspace、Okta、Microsoft 365、Salesforce、ServiceNow、ShareFile、Slack、Workday、Zendesk、Azure AD、Zoom。
全球涵蓋和效能	Netskope SSPM 只是 Netskope NewEdge 提供的眾多服務之一。Netskope NewEdge 是涵蓋全球的安全私有雲端，從零開始打造，以追求最高效能和服務韌性。

netskope

Netskope 是全球 SASE 領導者，重新定義雲端、資料和網路安全，協助組織套用零信任原則以保護資料。Netskope 平台快速且易於使用，無論人員、裝置和資料位於何處，都能提供最佳化存取和即時安全性。瞭解 Netskope 如何協助客戶在 SASE 旅程中應對任何挑戰，請造訪 netskope.com。