Skyhigh Security

Skyhigh Security Private Access

企業私有服務存取 — 零信任網路存取

業界首款資料感知的零信任網路存取解決方案，可確保從任何位置和裝置對私有應用程式存取的安全，並利用整合資料外洩防護 (DLP) 功能控制資料協作。企業私有服務存取與我們的整合安全服務邊緣 (SSE) 解決方案相融合，將 Skyhigh Security 定位成獨一無二的一流整合雲端傳輸安全解決方案，以加快 SSE 部署。

主要應用實例

- 對私有應用程式的安全區隔連線
- 已知身分識別和情境存取
- 網路微分段，防止威脅橫向移動
- 以最低特權存取特定的授權應用程式
- 保護私有應用程式免受基於網際網路的暴露
- 透過替代 VPN 和 MPLS 降低成本並提高效能
- 與存取 SaaS 和私有應用程式一致的使用者體驗**主要應用實例**

零信任網路存取的需求

當前的業務轉型和遠端勞動力擴張使網路邊界安全失效。隨著企業資源從企業邊界轉移到多個分散式位置（如公共雲和地端私有數據資料中心），組織面臨著部署安全解決方案以保護其敏感數據的挑戰，同時需要從遠端位置和設備的無縫存取。

零信任網路存取 (ZTNA) 以「零信任」安全模型為基礎，對應用程式存取執行身分感知和情境感知政策，這意味著在預設情況下拒絕存取任何資源。

無論是內部或遠端的每個使用者和裝置都被認為是不安全且有風險，在允許存取敏感的私有資源之前，必須對其身分和安全態勢進行驗證。ZTNA 擺脫了固定邊界的安全架構，轉而採用更合理、軟體定義的邊界架構，其中包含一系列使用者和應用程式。根據 Gartner 預測，開放給生態系統合作夥伴的新數位業務應用中，有 超過 80% 將經由零信任網路存取進行存取。[1]

導入 Skyhigh Security 企業私有服務存取

業界首款零信任網路存取解決方案可搭載整合的資料外洩防護 (DLP) 和遠端瀏覽器隔離 (RBI) 功能，

使組織能夠對私有應用程式進行精確的「零信任」存取，應用政策來防止協作期間敏感資料遺失，並經由完全隔離的 Web 會話將私有應用程式與具有潛在風險的非託管裝置隔離開來。

以安全區隔的應用服務連線取代 VPN

VPN 並非專為大多數員工遠端連接到雲端/地端服務的部署設計，因此存在以下挑戰：

- 使用者需要存取的企業應用程式和資料分散在多個位置。經由集中式 VPN 集線器進行迴轉傳輸式的遠端連線，會產生嚴重的延遲問題。
- 遠端勞動力的流量成指數級增長，使網路頻寬受到限制，基礎設施的容量也不堪重負。
- 過度的隱性信任模型讓任何擁有有效登入金鑰的使用者能夠完全存取私有網路，從而增加資料暴露和威脅橫向移動的風險。

我們的解決方案

Skyhigh Security 企業私有服務存取利用超規模服務邊緣，實現對私有應用程式的安全、安全區隔的應用程式存取。無所不在的連線可減少網路延遲，讓使用者在存取 SaaS 和私有應用程式時擁有一致、無縫的體驗。

效益

- 超規模服務邊緣的正常運行時間達 99.999%，可不間斷存取企業資源。
- VPN 允許通過身分鑑別的使用者可存取整個網路，而企業私有服務存取則不同，主要透過對網路進行微分段，允許以「最低權限」存取特定經授權的應用程式，而不是存取整個底層網路。

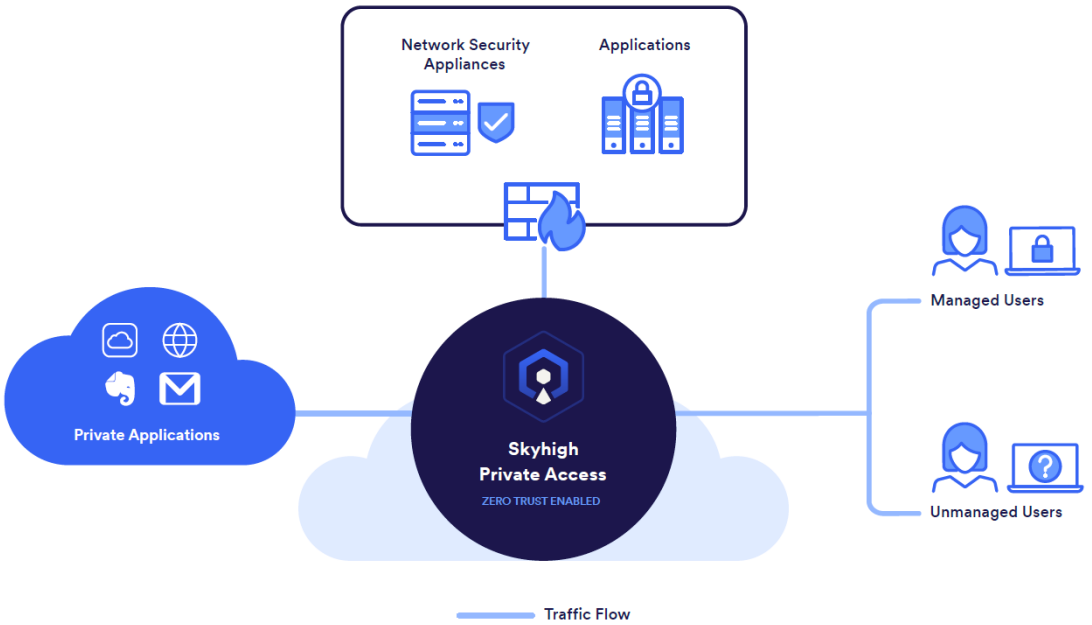

圖 3. 利用 Skyhigh Security 企業私有服務存取，實現安全區隔應用程式存取

整合的資料防護，確保遠端協作的安全

雖然傳統的 ZTNA 供應商側重於確保私有應用程式的遠端存取安全，但卻無法確保這些應用程式中敏感資料的安全性。在分散式勞動力的環境中，可在託管和非託管設備、第三方或連接的雲端服務之間進行資料的存取和協作。務必要加強防護，並防止任何連接實體的資料遺失。

我們的解決方案

Skyhigh Security 企業私有服務存取可與資料外洩防護 (DLP) 整合(須另加購相關 DLP 授權)，可經由嵌入的 DLP 政策，完全控制企業私有服務存取會話中進行協作的資料。

效益

- 支援嵌入的 DLP 進行深度資料檢查和分類，可防止遠端使用者在任何位置和裝置上進行協作時對敏感資料進行不當處理。
- 利用統一跨企業私有服務存取、端點、雲端和 Web 的 DLP 和威脅防護，安全團隊可受惠於敏感資料的整合可見性和控制。

為非託管裝置提供順暢支援

近來的遠端工作環境轉變，顯著增加登入非託管、自攜裝置工作的使用者比例，這些裝置往往經由不安全的遠端網路進行連線，繞過了傳統安全系統的控制。雖然組織鼓勵雲端協作以提高工作效率，但無監督的資料存取、經由非託管裝置共享資料，以及為這些裝置執行端點、雲端和 Web 安全政策所涉及的挑戰，都會帶來敏感資料暴露和網路攻擊的風險。

我們的解決方案

Skyhigh Security 企業私有服務存取可經由無代理程式、瀏覽器部署，確保非託管裝置的安全性。透過瀏覽器啟動的連線，讓員工、外部合作夥伴或第三方承包商之間能夠以最順暢的方式進行協作。

效益

- 無須安裝任何資源密集型代理設備，即可從非託管裝置無縫、安全地存取私有應用程式。
- 定義情境存取控制政策，根據裝置分類和安全態勢限制對私有資源的存取。

加快邁向 SSE 之路

安全存取服務邊緣 (SASE) 的新一代演進，將廣域網路 (WAN) 邊緣基礎設施平台與稱為安全服務邊緣 (SSE) 的高度融合安全平台結合在一起。SSE 旨在透過統一所有安全服務，解決動態、安全的存取需求。憑藉建立安全、身分識別驅動的應用程式存取，ZTNA 被認為是 SSE 架構的核心元件。

Skyhigh Security 企業私有服務存取採用 Skyhigh Security 的架構準則建構而成，可無縫整合我們的安全服務邊緣 (SSE) 解決方案，其中包括安全網頁閘道 (SWG)、雲端存取安全代理 (CASB)、資料外洩防護 (DLP) 和遠端瀏覽器隔離 (RBI)。該解決方案與 Microsoft Active Directory 和 Okta 等身分識別提供者整合，進行 SAML SSO 身分鑑別，以持續對存取私有應用程式的使用者進行身分鑑別和驗證。

藉此將 Skyhigh Security 定位成獨一無二、可利用統一的解決方案解決 SSE 網路安全難題，其透過集中式可見性和事件管理、適應性和精確存取控制、端至端的資料防護和裝置至雲端的進階威脅防護，解決遠端勞動力部署的複雜性。

利用與領先的 SD-WAN 供應商合作，Skyhigh Security 可提供無所不在、簡化、可靠和低延遲的雲端安全服務，為加快 SSE 部署制定路線圖。

如需瞭解更多資訊

探索 Skyhigh Security 業界領先的資料感知雲地混合安全平台。 如需瞭解更多資訊，請聯絡您的銷售客戶經理或合作夥伴。

Skyhigh Security

3099 North First Street
San Jose, CA 95134
888.847.8766
skyhighsecurity.com

2023 年 10 月。