零信任安全：
6大實施障礙與解決方案

- 台灣二版　高級產品經理　盧 惠 光 (Kenneth Lo)

議　程

- 什麼是零信任安全
- 6大實施障礙
- 解決方案和策略
- Q&A問答

什麼是零信任安全？

- 零信任是一種用於保護機構的**安全性模型**，其依據為不應預設信任任何使用者或裝置，即使對方已存在於機構的網路內。零信任機制會在整個網路上 (而不只是在信任的範圍內) 強制執行嚴格的身分驗證和授權，藉此**移除隱含的信任**。在這個模型中，所有存取資源的要求都會視為來自不受信任的網路，直到經過檢查及驗證為止

- Forrester Research 分析師 John Kindervag 在 2010 年首次提出零信任安全性模型。這標示了與傳統 IT 安全性模型不同的發展；傳統模型主要著重於在網路範圍中保護存取權，並假設內部的一切都值得信賴

現實與期望

- 根據 Gartner 的數據，到 2025 年，60% 的組織將採用零信任作為安全的起點
- 迄今為止，只有 23% 的中小型企業（SME）完全採用了零信任安全計劃
- 中小型企業平均需要 2-3 年 時間才能完全實施零信任架構

- https://jumpcloud.com//wp-content/uploads/2022/02/202202-WP-ZeroTrustDemystified.pdf

6大實施障礙

1. 拋棄過時技術
2. 有限的資源
3. 意外的授權成本
4. 用戶採用不足
5. 領導層支持不足
6. 工具不兼容性

1. 拋棄過時技術

- 成熟的組織必須處理他們**已經存在的基礎設施**
- 匆忙進行改變的人，已經被證明**會減慢**甚至**破壞關鍵系統**
- **改造**舊系統，很多是一個**昂貴的選項**
- 建議制定一個路線圖，**逐步遷移**

2. 有限的資源

- 零信任實施需要**勞動力、時間和財務**等資源
- 團隊中是否有人知道如何**設計及設置**網絡微分段?
- 外包的初始成本可能看似高昂，但不要低估**長期回報**
- 優先考慮對 IT 安全產生最大成效的低成本舉措 e.g. MFA

3. 意外的授權成本

- SaaS, Cloud First, Cloud Smart, A.I, ……..
- SaaS應用程序運行在瀏覽器上，**管理員很少需要擔心操作系統的兼容性問題**
- **免費服務級別無法提供足夠的支持、功能和所需的完整解決方案**
- **53%**的企業將**超過10%的預算**用於**未充分利用、未託管或未考慮的雲資源** (1)

(1) https://www.forbes.com/sites/waynerash/2023/03/14/half-of-enterprises-waste-over-10-of-their-budget-on-software-saas-and-cloud-infrastructure-according-to-survey/?sh=2fc5e3fd6c3f

4. 用戶採用不足

- 根據麥肯錫的數據，組織中 **70%** 的變革計劃因**員工的抵制**而**失敗**
- 導致零信任（Zero Trust）用戶採用不足的常見原因包括：
  - ✓ **對零信任的誤解**
  - ✓ **不清晰的溝通**
  - ✓ **對零信任架構的陌生**
  - ✓ **效率低下的培訓**

5. 領導支持不足

- 領導層對建立零信任架構（ZTA）的重要性缺乏理解
- IT 管理員最好能讓領導層了解：
  - ✓ **零信任是什麼意思？**
  - ✓ **我們需要哪些技術、工具和資源？**
  - ✓ **現有基礎設施存在哪些漏洞？**
  - ✓ **數據泄露的平均成本是多少？**
  - ✓ **被盜數據可能給我們帶來多大的損失？**
  - ✓ **數據泄露有多常見？**

6. 工具不兼容性

- 匆忙購買零信任架構（ZTA）解決方案，卻意識到它們與現有基礎設施不兼容
- 考慮與一個足夠靈活的供應商合作，以根據您的實際需求定制解決方案

解決方案和策略

- ✓ 身份認證、身份認證、和身份認證
- ✓ 零信任遠端訪問不僅僅是遠端訪問
- ✓ SASE 和零信任
- ✓ PAM 仍然是零信任的核心
- ✓ 持續監測最重要，但也最困難

◇ 解決方案和策略

✓ 身份認證、身份認證、和身份認證

提供了一個**開放的目錄平台**，可以在 Windows、Mac 和 Linux 上統一設備和身份，並具有基於雲的 SSO、MDM、MFA、PAM 等功能。這個平台結合了**身份、訪問**和**設備管理**

常見 IT 方案

構建新目錄

構建雲目錄以集中身份，以管理您的所有訪問需求

替換 AD

消除本地基礎架構並從雲中管理現有標識

遠端工作

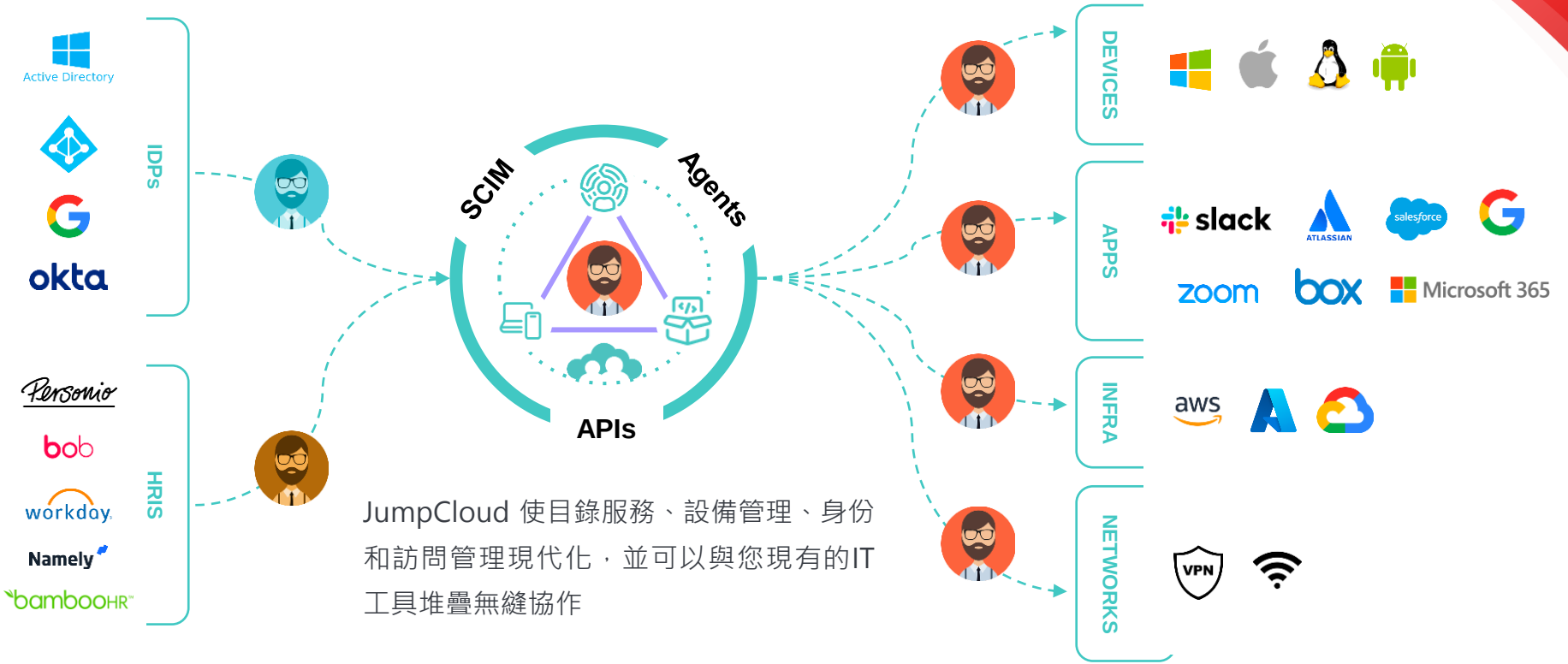
安全地管理設備並訪問 IT 資源，無論它們位於何處

零信任安全

實施零信任，確保使用者從單個雲目錄平臺訪問所有資源

jumpcloud

統一 IT 和安全基礎設施



JumpCloud 使目錄服務、設備管理、身份和訪問管理現代化，並可以與您現有的IT工具堆疊無縫協作

jumpcloud

jumpcloud

身份

OPEN DIRECTORY

Google Workspace · Microsoft 365 · Namely · okta · Active Directory · Personio · workday · bamboohr · {REST APIs}

IMPORT & AUTOMATE

訪問

SSO

salesforce · Atlassian · aws

SAML SCIM OIDC

LDAP

LEGACY APPS · NAS

IT RESOURCES

RADIUS

WIFI · VPN

設備

AGENT & MDM

CROSS-OS · SERVERS · MOBILE

PATCHING

條件訪問

PUSH MFA

INSIGHTS

目錄分析

可報告的事件

車隊診斷

◇ 解決方案和策略

✓ 零信任遠端訪問不僅僅是遠端訪問

Parallels®

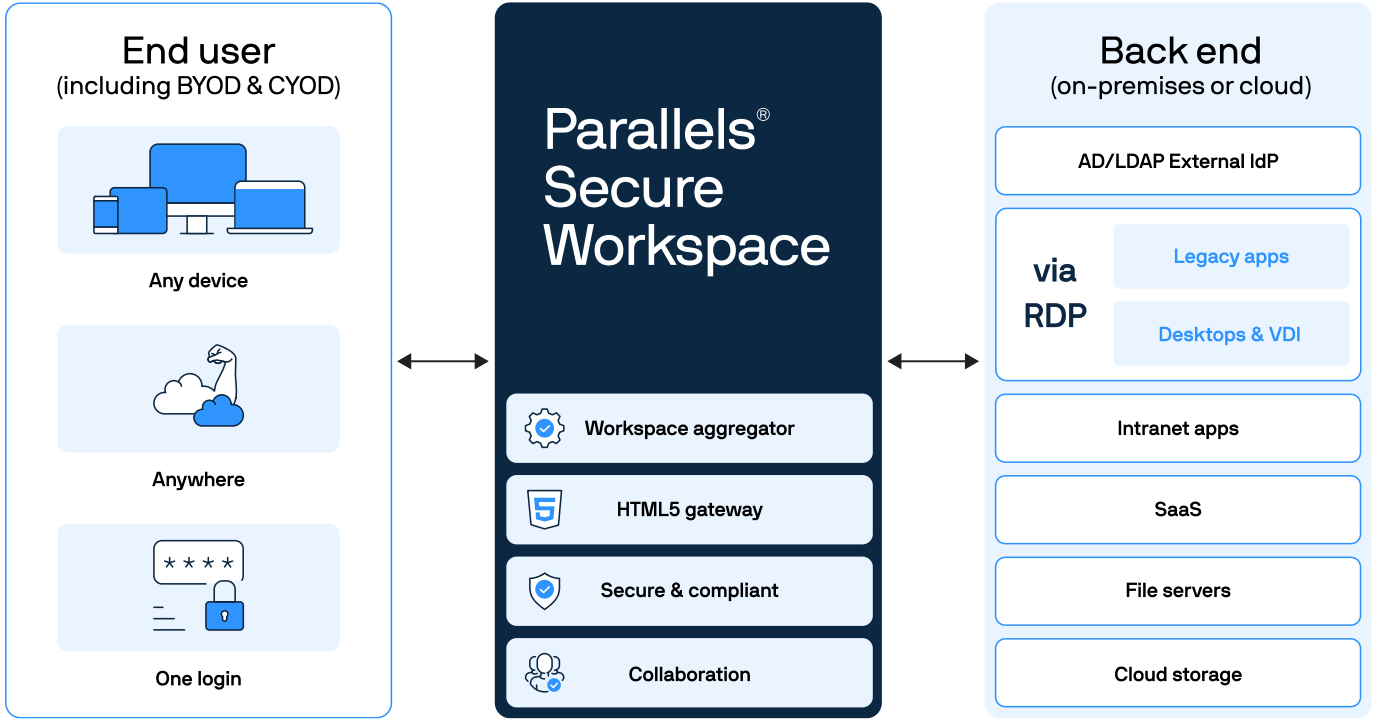
Parallels Secure Workspace

將安全重點從以周邊為中心的模型轉向**連續驗證**和**遠程瀏覽器隔離 (RBI)**

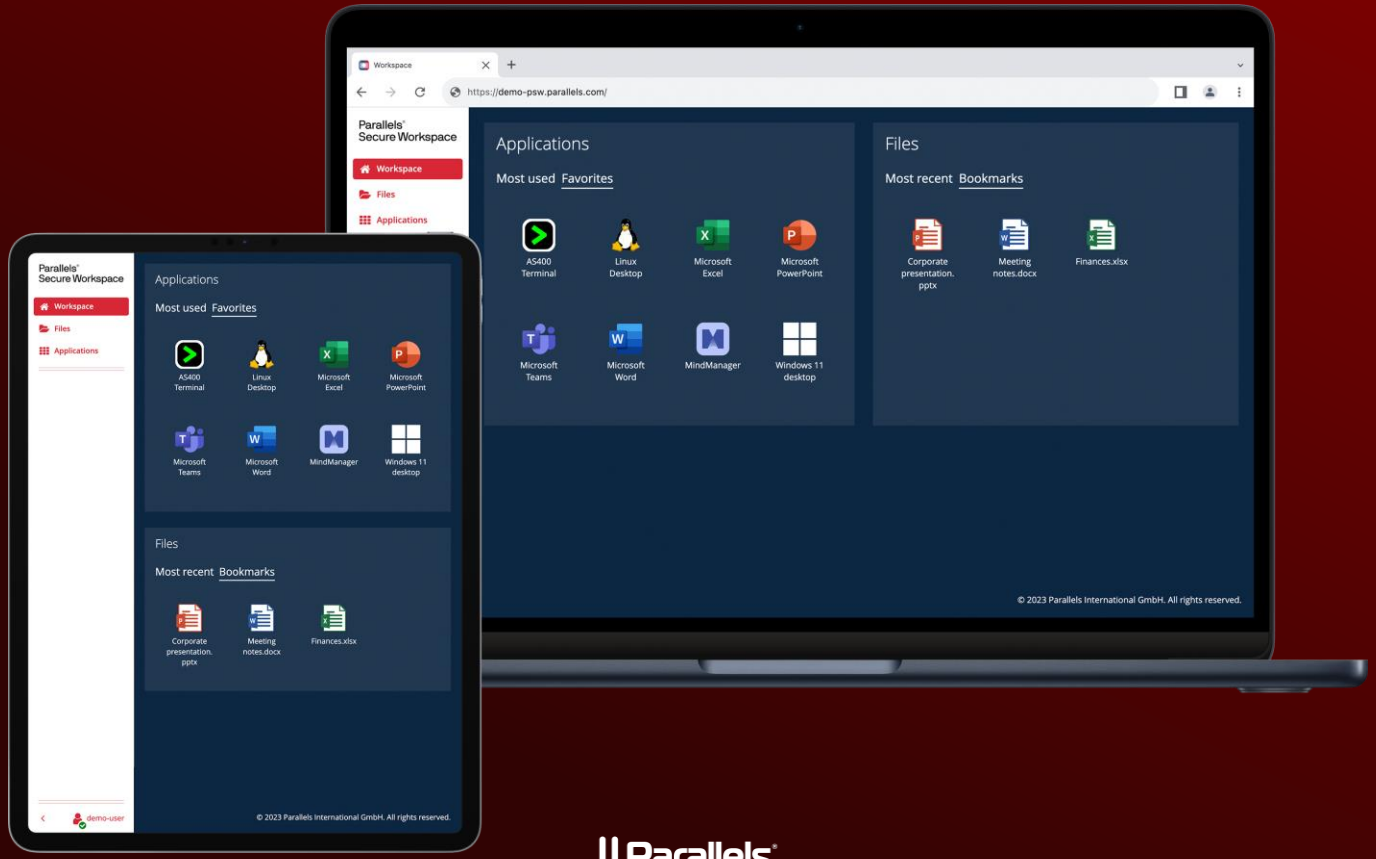
無論用戶在哪裡或來自哪裡

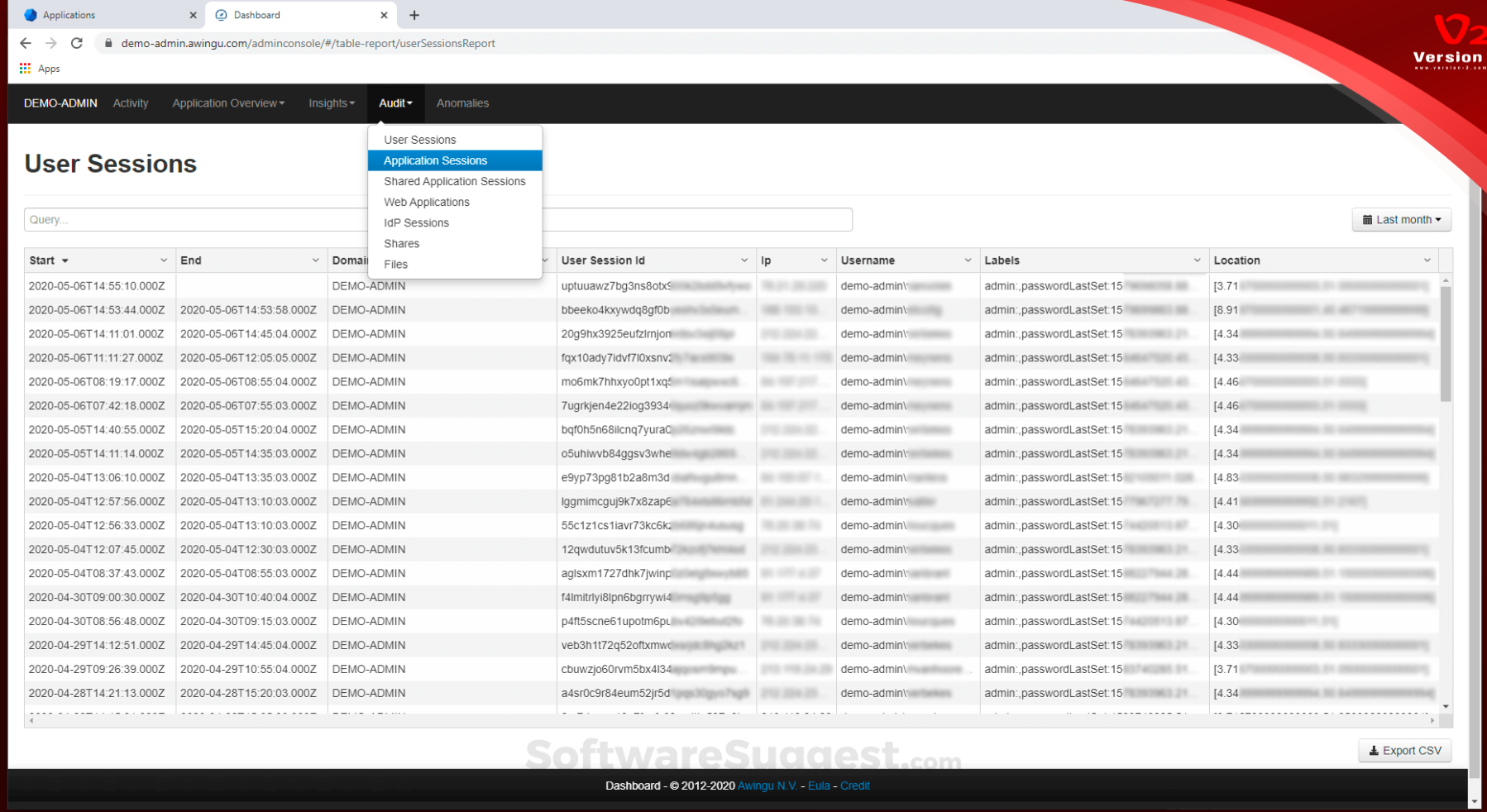
這有助於解決傳統企業控制的局限性，並將保護措施擴展到更靈活的邊界之外

Parallels Secure Workspace all-in-one architecture



控制對應用程序和資源的訪問權限





✓ SASE 和 零信任

NORD SECURITY

NordLayer

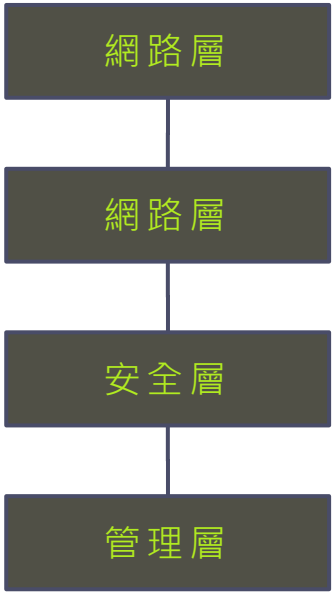
遠端安全存取解決方案

以 SASE 和 零信任（Zero Trust）為基礎，引入了針對互聯網、網路和資源訪問控制的 SaaS 安全功能，包括**零信任網路訪問**、**防火牆即服務**、**安全網關等功能**，以保護您的網路和數據

分層技術

NordLayer 旨在將最佳實踐整合到 SASE 框架中，SASE 框架是一個由使用者友好介面支援的疊加安全網格

Did you know: AES 256-bits encryption refers to 'Military Grade,' established by the U.S. National Institute of Standards and Technology. The estimate of its decryption is 27 trillion trillion trillion trillion trillion years — in contrast, the universe has only existed for 15 billion years.



共用和專用IP、網路分段、網站到網站

IaaS、專用伺服器和互連、智慧遠端訪問

零信任網路訪問、越獄設備檢測、自定義 DNS、AES256加密、2FA和生物識別身份驗證

集中控制面板

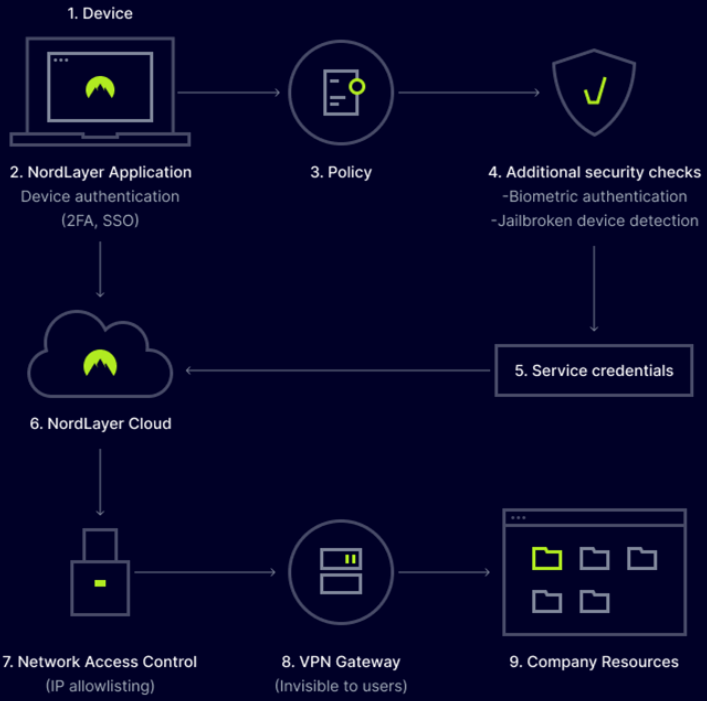
NordLayer

我們的核心產品 - 我們如何協助您的客戶

- **在 SASE 上執行我們的：**
  - ✓ 雲原生安全與網路平臺
  - ✓ 威脅防護
  - ✓ 安全的遠端訪問
  - ✓ 集中管理
- **保護 混合環境：**
  - ✓ 安全訪問管理
  - ✓ BYOD 策略和支援
  - ✓ 輕鬆的可擴充性
  - ✓ 無縫集成
- **實現零信任安全模型：**
  - ✓ 身份和訪問管理
  - ✓ 網路分段和閘道
  - ✓ 應用程式訪問控制
  - ✓ 雲原生 ZTNA 控制器
- **合規 & 標準：**
  - ✓ HIPAA
  - ✓ GDPR
  - ✓ ISO 27001
  - ✓ PCI-DSS

NordLayer

網路安全



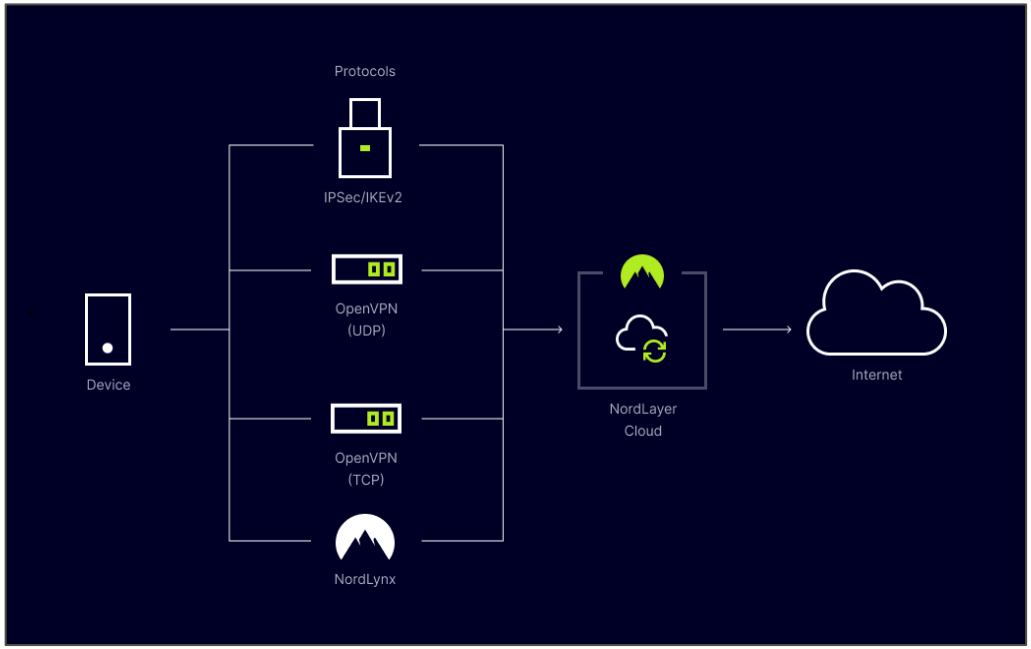
NordLayer

1. 使用安全的身份驗證方法登錄您的設備
2. 使用安全登錄訪問 NordLayer 應用程式並設置多因素身份驗證（2FA，SSO）
3. 策略：建立網路分段團隊，分配用戶許可權，並根據員工信任級別創建網關
4. 在此階段可以啟用額外的安全檢查，例如生物識別，以便進一步驗證。NordLayer 還將檢測網路上已越獄/已取得 root 許可權的 iOS 設備
5. 提供給閘道的服務憑據
6. NordLayer Cloud：透過 NordLayer 安全隧道連接到工作應用程式，對來自網路邊界外的活動進行加密
7. 網路存取控制：IP 允許清單使管理員能夠設置特定的用戶許可權，以便使用者只能訪問與其工作角色相關的資源
8. 通過分配給特定 VPN 閘道的使用者（每個使用者都具有唯一的團隊訪問許可權）來確保網路分段
9. 對公司資源的訪問許可權按 IP 位址進行細化 - 僅基於使用者完成工作所需的內容，僅此而已

網 路

為了與客戶的架構和用例實現最佳相容性和集成，我們有多種協定可供選擇，我們的伺服器原生支援這些協定

從客戶端設備到 NordLayer 的基礎設施（共用閘道或私有閘道）會創建一個加密的安全連接



NordLayer

✓ PAM 仍然是零信任的核心

senhasegura

特權帳號管理解決方案

提供了一個全面的**特權訪問管理（PAM）解決方案**，包括以下功能，**集中管理特權帳戶**，實施詳細的**訪問限制**，監控用戶活動並創建詳細的**審計軌跡**

雲身份和訪問管理：簡化身份管理，具有多因素身份驗證、基於角色的控制、審計軌跡和詳細報告，並與現有身份提供者兼容

PAM 360º 特權管理平臺

ACCOUNT AND SESSION

- PAM CORE
- Domum Remote Access
- MySafe

GO ENDPOINT MANAGER

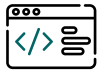
- GO Endpoint Manager Windows
- GO Endpoint Manager Linux

DEVOPS SECRET MANAGER

- DevOps Secret Manager

MULTI CLOUD

- Cloud IAM
- CIEM



CERTIFICATE MANAGER

- Certificate Manager

SaaS, Subscription (Self managed), Perpetual (On premises)

senhasegura

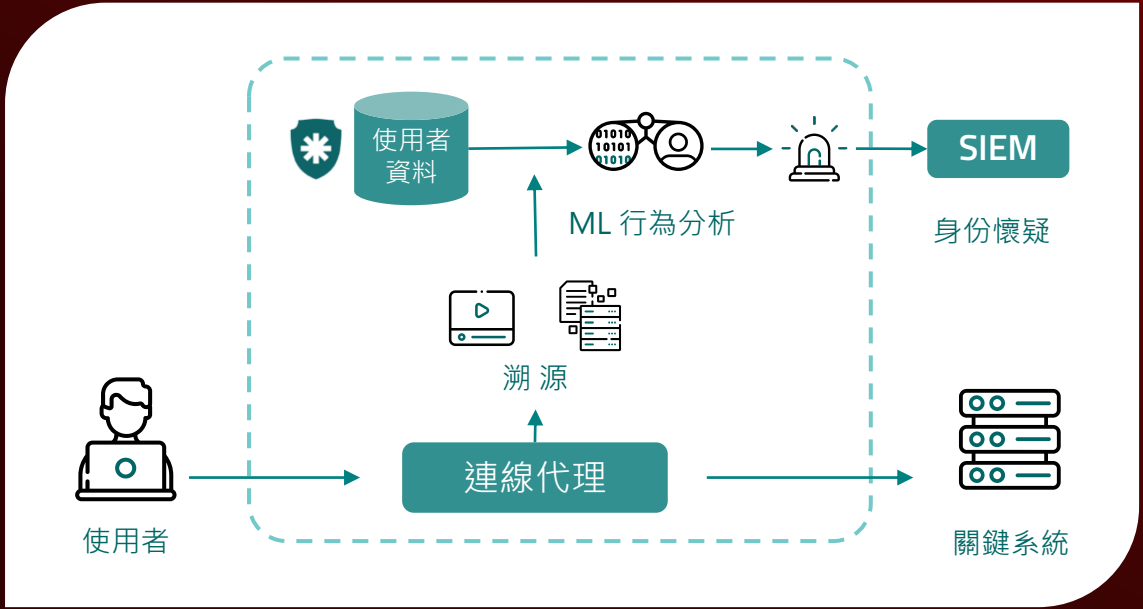
保護特權憑據

- 隨時隨地，任何人都可以安全訪問
- 審計和報告任何資產或應用程式的特權活動
- 輪換員工和第三方密碼，包括應用程式、操作系統、雲資源和資料庫的密碼
- 為承包商和臨時雇員提供安全的第三方訪問
- 安全的網路管理設備和關鍵基礎設施
- 從 Unix 和 Linux 到 Windows 和 Mac OS 的所有主要平臺的安全特權提升
- 漏洞評估、監管報告和補救措施

這意味著它已準備好滿足業務和市場合規性要求，例如 LGPD、GDPR、PCI DSS、SOX、NIST、HIPAA、ISO 27001 和 ISA 62443

用戶和實體行為分析

- 可以實時監控用戶行為，以立即識別可疑行為並防止惡意行為



問題

儘管PAM解決方案提供問責制，但惡意參與者可能會獲得憑據訪問許可權

解決方案

Senhasegura實現了實時監控用戶行為，以在行為偏差期間自動檢測並阻止許可權濫用

影響

使公司能夠即時檢測惡意行為，從而縮短響應時間。還可以抑制欺詐行為，因為在線檢測欺詐行為比通過離線審計更有效

✓ 持續監測最重要，但也最困難

UnderDefense

資安威脅偵測應變服務(MDR)

致力於幫助企業**預測**、**防止**、**檢測**和**應對**現代高級和具有侵略性的網絡攻擊。他們的MAXI MDR + SOAR 安全即服務平台由 **24/7** 的團隊支持，為您的業務提供全方位的保護。無論您處於哪個階段，UnderDefense 都能為您提供高效且實惠的前沿安全解決方案

服務組合：

24x7x365 託管威脅回應

75位安全工程師監視您的網路並保護您免受惡意攻擊者、勒索軟體和資料遺失

合規與 vCISO

快速輕鬆地獲得合規性，SOC2、ISO 27001、PCI DSS、GDPR ，我們對它們瞭如指掌，我們的 vCISO 將使其付諸實行

事件取證和資料洩露恢復

您需要快速獲得解答及恢復
我們能快速有效地調查、控制和補救關鍵安全事件

滲透測試 (Penetration Test)

在駭客找到您的弱點之前。定期的健康檢查，對於成功的公司來說是必須的，我們是最擅長破壞安全的

- **三大好處：修復速度、卓越的 Python和自動化專業知識、非常划算**

安全監控 / MDR 包

- 我們的安全監控是**定制的** 滿足每個公司的需求。我們將了解您的環境，並可以為您的安全團隊提供遠程增強功能。合作的基本模式有以下三種：

為您打造 SOC	共同管理 SIEM/MDR/NTA	遠程 SOC 團隊
當您決定與本地團隊一起構建SOC，並且需要支持來為您的團隊選擇、計劃、實施和配置SIEM/IR工具並設置適當的流程時。我們就您的特定案例所需的最優化解決方案向您諮詢，維護您的SIEM，為您的部署建立新的關聯	當您已經擁有或計劃購買SIEM但您想從投資中獲得答案和ROI但您無法聘請安全團隊或安全團隊不想在夜班期間工作，因此您需要擴展您的安全團隊與UD工程師一起配置、維護和監控	當您在內部擁有自己的CIRT團隊並且只需要我們的分析師進行監控和通知時。在這種情況下，我們可以在您自己的環境中工作或使用我們的AWS雲部署Splunk來監控事件並通知CSIRT團隊。您將收到調查結果報告，並與安全團隊保持持續溝通

UD MDR 訂閱入職流程（30 天）

1天	5天	8天	14天	2天
				
歡迎電子郵件	**啟動與規劃**	**連接和存取**	**服務配置**	**服務啟動**
• 介紹 • 入職表格請求 • 設置技術開始	• 技術啟動 • 審查技術文件 • 制定項目計劃和時間表 • 設置通訊渠道 • 定義需要建立的存取權限/憑據	• 建立新的客戶租戶 • 準備編譯 • 傳感器 • 通過 RMM 運送和部署傳感器 • 驗證和確認連接和訪問	• 配置和規範化i資料擷取 • 環境壓力測試 • 系統微調 • 誤報補救 • 自動化引擎 • 與客戶環境集成	• 定義升級程序和 IR 參與 • 啟動 “保護模式” • 服務集成驗證 • 服務期開始

共同管理 SIEM 的好處

超越警報以提高風險意識

共同管理的SIEM為您提供警報之外的風險意識；您將很快收到事件調查和風險驗證

加速分析、遏制和響應

通過利用來減少響應已知和未知威脅活動所需的時間。我們優先考慮威脅響應引擎

擴展您的團隊並降低成本

通過利用，減少建立自己的SIEM工程師和威脅分析師團隊的需要。我們是您的 24x7x365 虛擬團隊

轉向智能驅動的運營

我們的全球威脅情報中心工具和資源可以增強您當前的網絡安全策略

Version 2 台灣二版
www.version-2.com.tw

台灣總代理-台灣二版

資安解決方案

jumpcloud	雲端身份驗證目錄解決方案
senhasegura	特權帳號管理解決方案
Parallels	Parallels Secure Workspace
UnderDefense	資安威脅偵測應變服務(MDR)
NordLayer	遠端安全存取解決方案