CISCO
SECURE

零信任網路安全

Jarvett Lin | 林秉忠 | jarlin@cisco.com
Cisco Taiwan

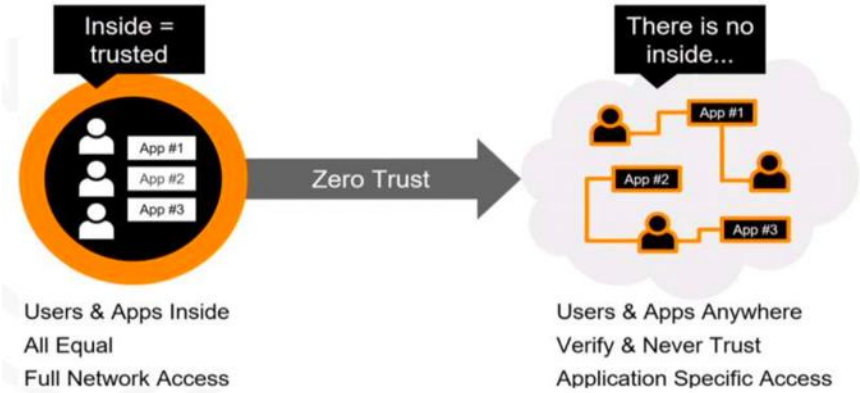
2024

The bridge to possible

零信任概念

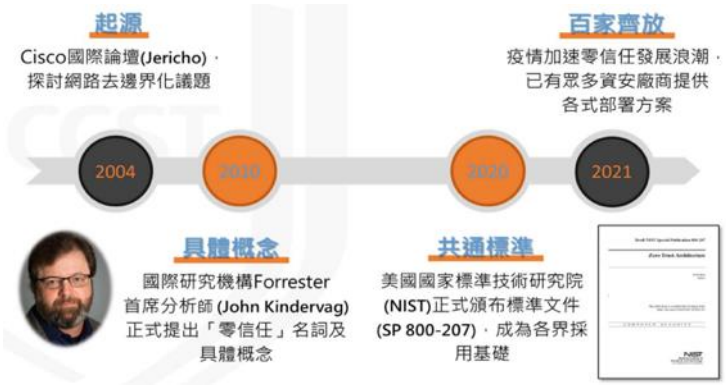
- 零信任希望突破傳統網路模型的資安窘境，並能保護資料存取
  - 不是保護網路存取，而是保護資料/應用存取
  - 無具體邊界，使用者/設備與資料/應用無處不在
  - 任何資料存取永不信任且必須驗證
  - 技服政府零信任網路說明文件 – 111/07/14

- **國家資通安全發展方案(110年至113年)**
  - **推動政府機關導入零信任網路**
    完善政府網際服務網防禦深廣度
  - **導入零信任網路是一段逐步成熟之過程**
    不是一次大規模替換基礎架構與存取流程
    而零信任網路身分鑑別為優先導入機制
  - 政府零信任網路機制導入建議 – 111/08/12



零信任演進與共通標準 – NIST SP800-207

- 2020年美國國家標準技術研究院(NIST)正式頒布標準文件
  SP 800-207：Zero Trust Architecture
  成為各界採用基礎



- 美國是目前規劃最具體之國家，除了有明確政策與時間表之外，並透過國家資安卓越中心 (NCCoE)推動商用產品符合NIST零信任架構

- AWS
- Appgate
- Broadcom
- Cisco
- DigiCert
- F5
- Forescout
- Google Cloud
- IBM
- Ivanti
- Lookout
- Mandicant
- McAfee
- Microsoft
- Okta
- ...etc

美國零信任架構落地合作廠商

針對零信任資安基礎架構提出三個切入的維度

NIST SP800-207

增強的身份治理
(Enhanced Identity Governance)

確保只有正確的用戶和安全的設備才能訪問應用程序

應用服務間的微分割
(Micro-Segmentation)

保護您應用程序中的所有連接

軟體定義網路基礎架構
(Network Infrastructure and Software Defined Perimeters)

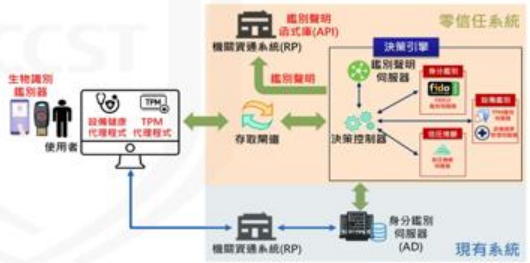
保護網路(包括IoT)上的所有用戶和設備連接

單一而全面的設計思維，確保橫跨網絡，應用程序乃至於多雲環境的所有訪問。

國家資通安全研究院

政府零信任網路架構

- 參考NIST零信任架構，結合向上集中防護需求，政府零信任網路採存取門戶部署方式，具備身分鑑別、設備鑑別及信任推斷3大核心機制
  - 身分鑑別：FIDO2身分鑑別與鑑別聲明
  - 設備鑑別：TPM設備鑑別與設備健康管理
  - 信任推斷：基於分數與情境之信任推斷機制



金管會發布「金融資安行動方案」2.0

六、鼓勵零信任網路部署，強化連線驗證與授權管控

世界重要國家政府推動規劃

- 零信任已從概念探討階段進入實務部署規劃，世界重要國家之政府紛紛建立國家零信任網路安全戰略

美國：具體規劃2024年前聯邦網路完成初步遷移。

歐盟：2020年建立歐盟網安戰略，提出標準框架，協助成員國轉型。

- 行政院「國家資通安全發展方案(110年至113年)」之「善用智慧前瞻科技、主動抵禦潛在威脅」推動策略，發展零信任網路資安防護環境，**推動政府機關導入零信任網路**，完善政府網際服務網防禦深廣度

111	112	113
‧身分鑑別：以生物識別鑑別器進行無密碼雙因子身分鑑別	‧設備鑑別：基於信任平台模組(TPM)之設備鑑別，並進行設備健康管理	‧信任推斷：依設備健康狀態、資安威脅情資及使用者情境等資訊，動態支援存取決策

資通安全責任等級A級公務機關

身分及設備兩相驗證，授予相應權限，並循環監控

從哪裡開始

Workforce
User and device access

Workload
Application and workload access

Workplace
Network access

Secure Access

如何確認存取人員身分正確？

他們存取的是對的應用嗎？

他們使用的存取設備是否已受信任？

他們使用的存取設備安全嗎？

Secure Workload

在企業系統中使用哪些應用？

應用與資料流是如何溝通的？

這些溝通是否安全與可信任？

Secure Network

用戶和設備是否通過身份驗證？

他們被授予什麼訪問權限？

網路內設備是否安全？

是否基於信任存取原則來設計網路分段(segmentation)？

訪問無處不在 - 如何獲得可見性並確保安全、受信任的訪問？

國家資通安全研究院
政府零信任網路架構中的3大核心機制：

1. 身分鑑別

使用者驗證: Push、OTP 、FIDO2 、Phone 、SMS 、Security Key 、Token(HW/SW)

2. 設備鑑別

設備健康度: checks for updated OS 、browser and compliance with security policies

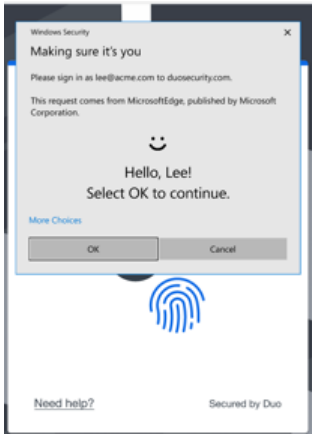
3. 信任推斷

連線信任: who accesses 、which applications 、which devices 、 what locations 、 which authentication

身分鑑別

- FIDO2無密碼雙因子身分鑑別
  - 提供Duo Push 推播和 WebAuthn(FIDO2) 和 Biometrics 生物識別
  - 使用者以生物識別鑑別器(實體安全金鑰或手機APP)進行身分鑑別

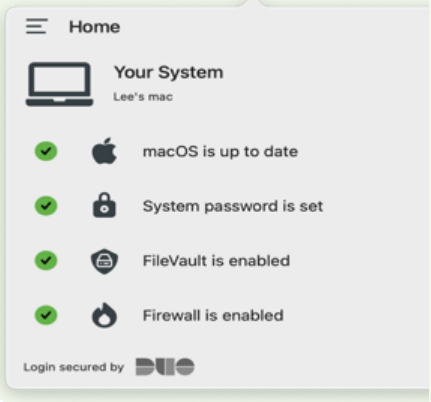
- Authenticators:
  - Touch ID
  - Face ID
  - Windows Hello
  - FIDO2 security keys
  - Duo Mobile



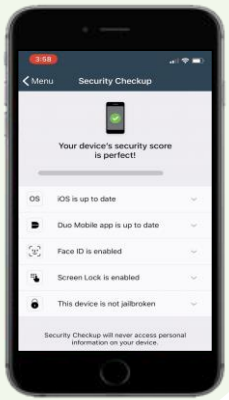
設備鑑別

- 設備健康管理
  - 持續更新設備健康狀態
  - 依設備健康狀態隨時換算設備健康信任等級

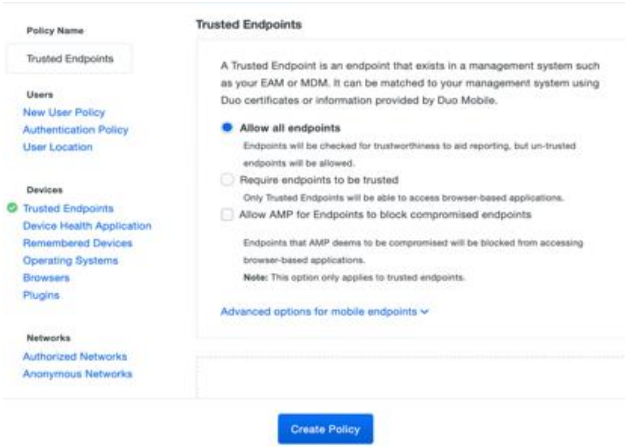
Device Health App



Duo Mobile



Duo Trusted Endpoints

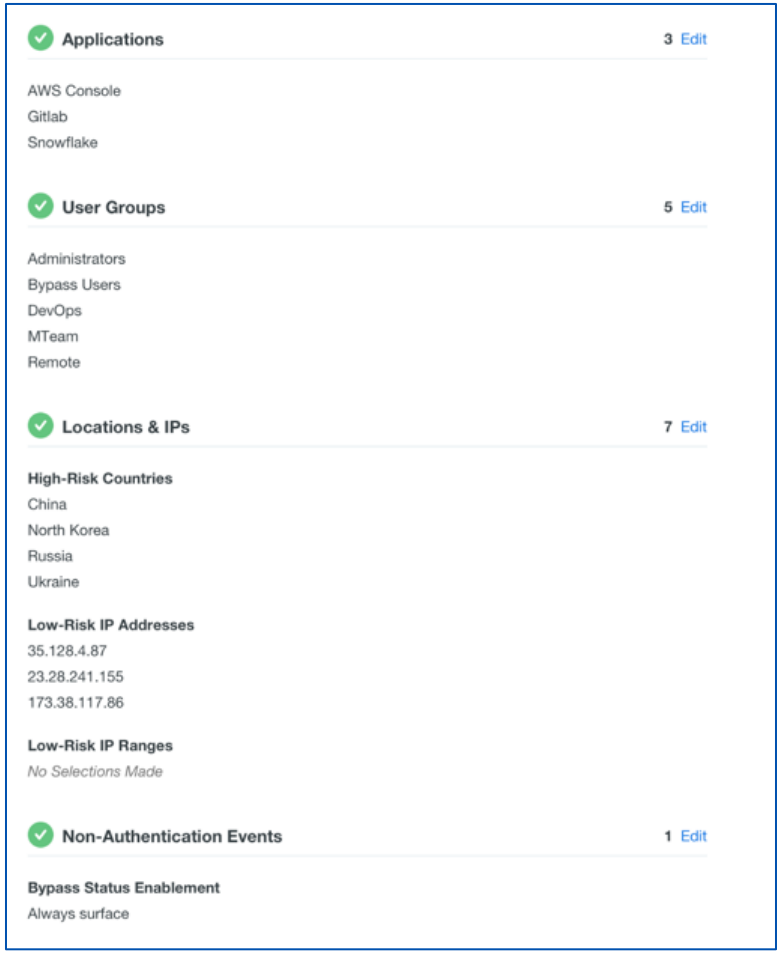


信任推斷

- 基於分數與情境之信任推斷機制

建立風險評估政策:

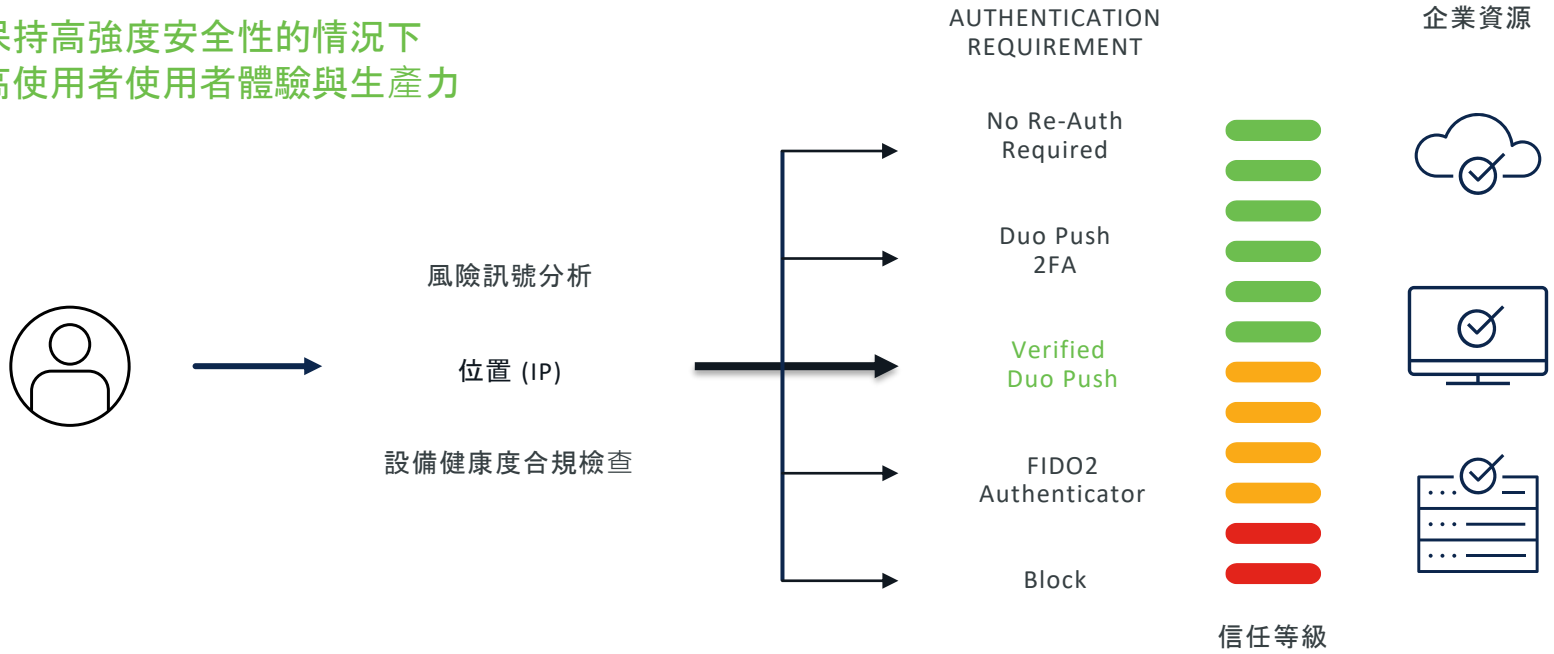
- **認證應用程式**
- **使用者與群組**
  - ✓ Administrators
  - ✓ Bypass Users
  - ✓ DevOps
  - ✓ RemoteWork
  - ✓ User
- **認證連線地區和IP**
  - ✓ **連線國家**
  - ✓ **單一IP或網段名譽**



基於風險 信任推斷的驗證

根據風險等級動態調整驗證需求

在保持高強度安全性的情況下
提高使用者使用者體驗與生產力



風險訊號: Known Attack Patterns

1. **使用者標記的可疑登入**: 使用者表示他們並未負責某次登入。
2. **異常和可疑活動:** 有不尋常的驗證特徵，例如重複的驗證失敗.
3. **推播轟炸(Push spray):** 驗證顯示入侵者在多個使用者中進行非針對性的推送攻擊的特徵.
4. **推播釣魚(Push phishing):** 驗證顯示入侵者進行針對性的推送騷擾攻擊的特徵.
5. **不合理的旅行距離:** 使用者似乎從一個基於過去驗證位置無法到達的新地點進行驗證.
6. **國家代碼不匹配:** 驗證設備和存取設備似乎在兩個不同的國家.

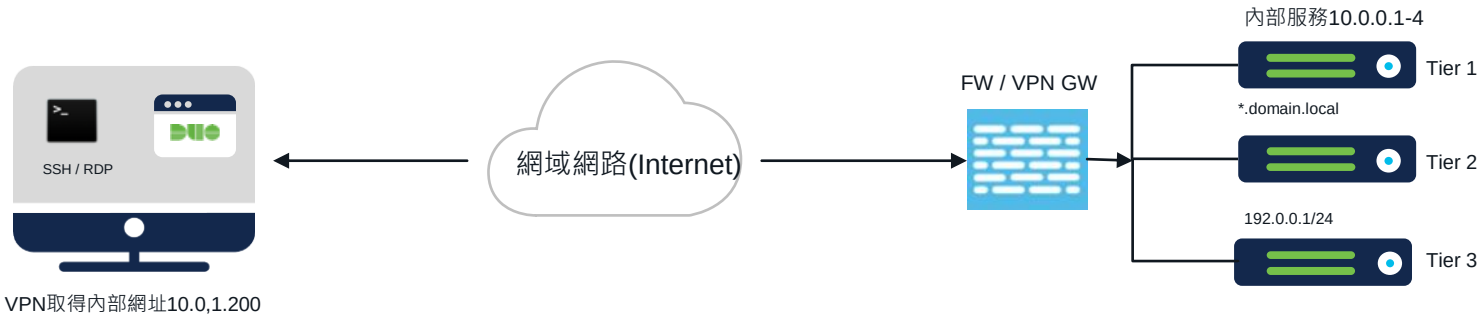
國家資通安全研究院
於111年
提出政府零信任網路說明文件

存取閘道

- 存取閘道(Access Gateway)負責網路導向與連線，為機關資通系統(RP)之存取門戶
  - 不論來自內部或外部網路之存取，必須且唯一經由存取閘道
  - 為唯一公開存取之組件，存取全程必須隱藏內部網路路徑(如利用反向代理技術)
  - 必須實施負載平衡機制以避免效率瓶頸
  - 必須實施可有效防止阻斷服務攻擊之機制

傳統VPN連線方式

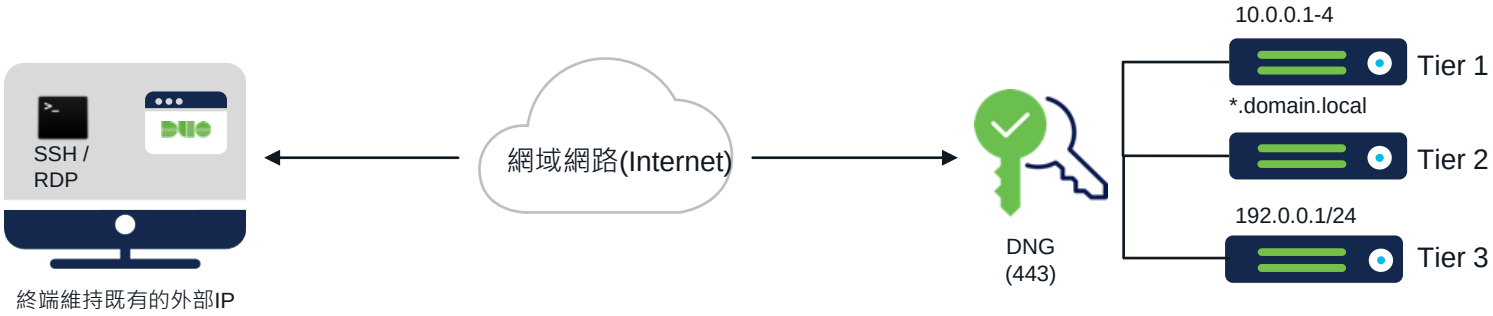
- VPN撥號連線至Datacenter並取得內部IP位址



可以存取任何服務，需透過ACL或Segmentation做限制

代理存取閘道(反向代理)

- 不需 VPN 的遠端存取私人應用程式



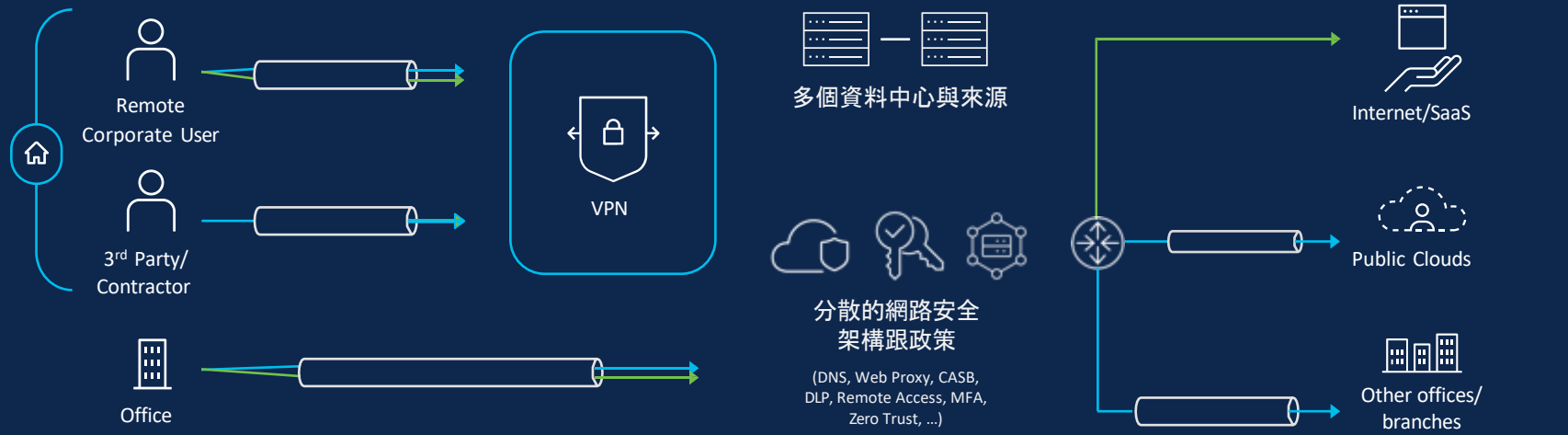
Supports: HTTP/S | SSH | RDP | SMB

Cisco Secure Access

分支機構與遠距辦公者的安全混合雲辦公解決方案

現今的挑戰

現行的網路架構設計往往並不是專門為分行/混合辦公設計的



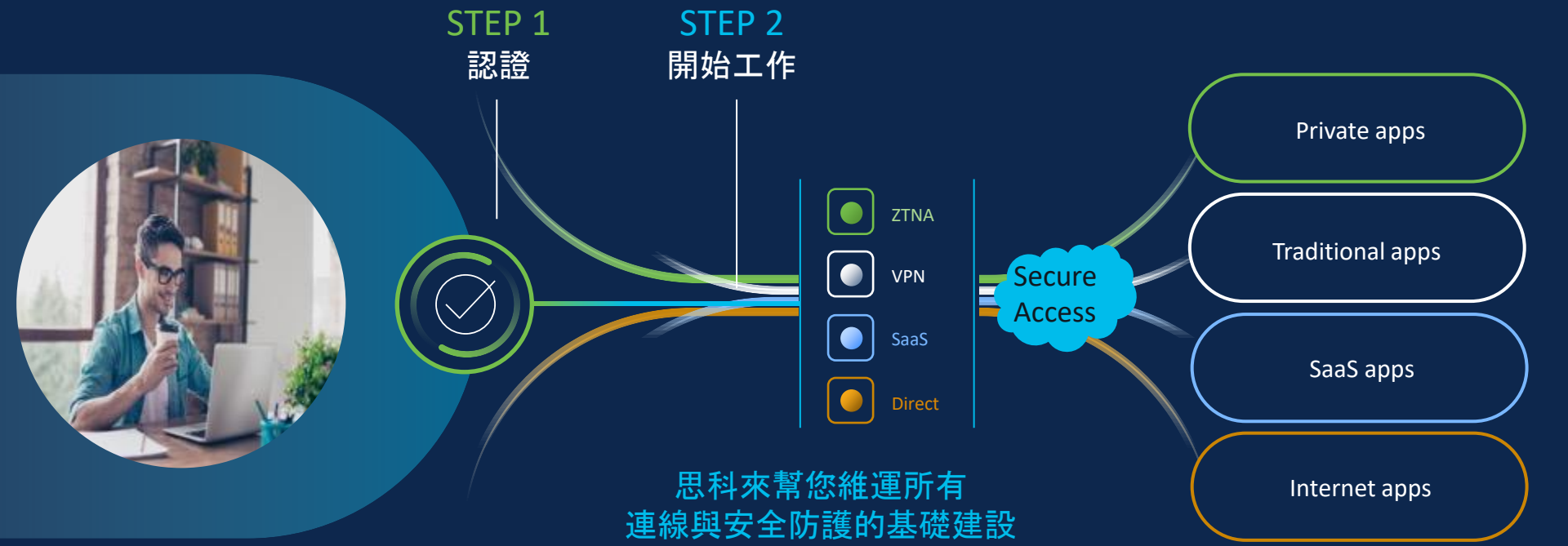
不好的用戶體驗
生產力降低

大量的異質解決方案和供應商
操作和成本的複雜性增加

安全管理的複雜性和碎片化

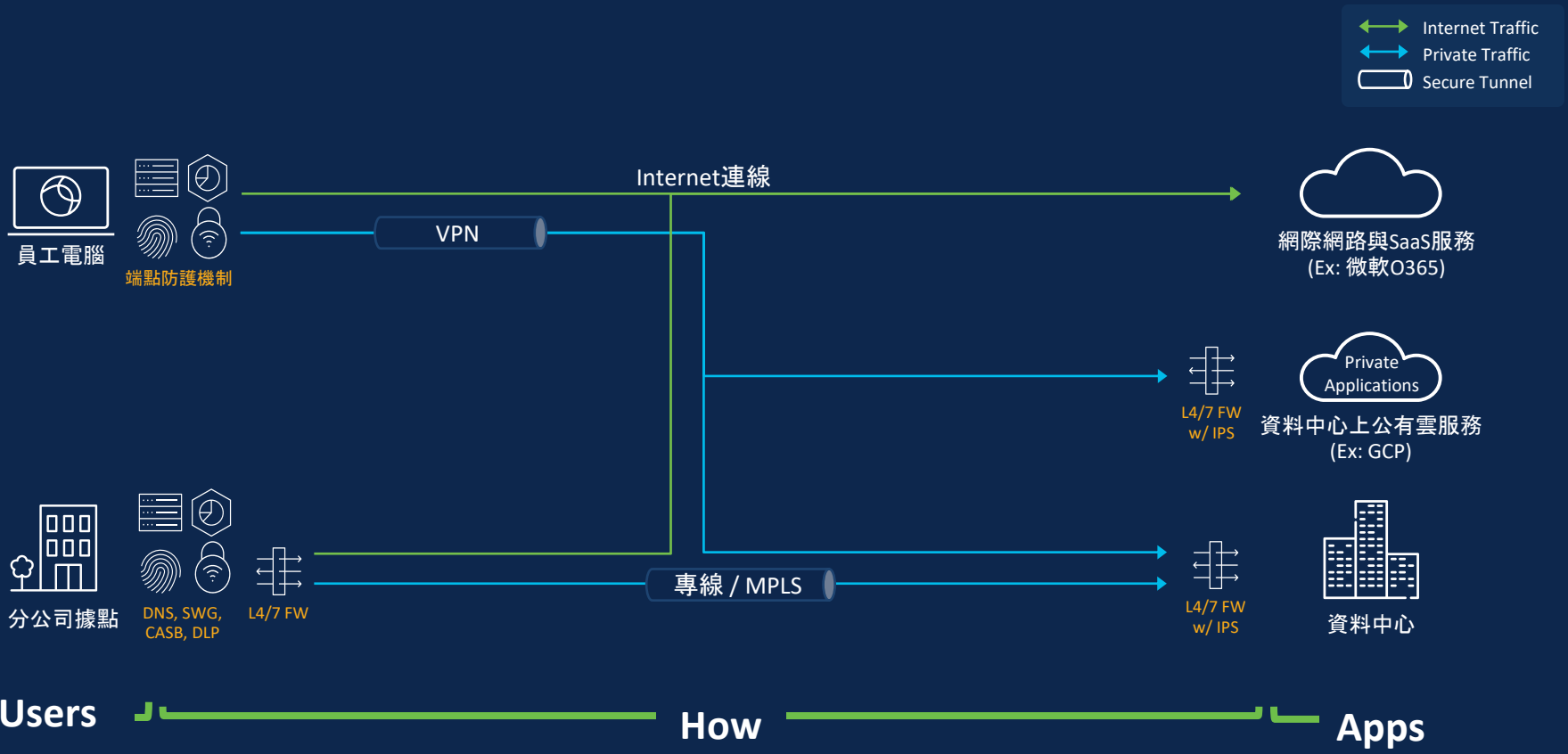
現況：為了不同的企業應用，配置對應的連線方式

不管使用者在何處，都有相同的連線體驗

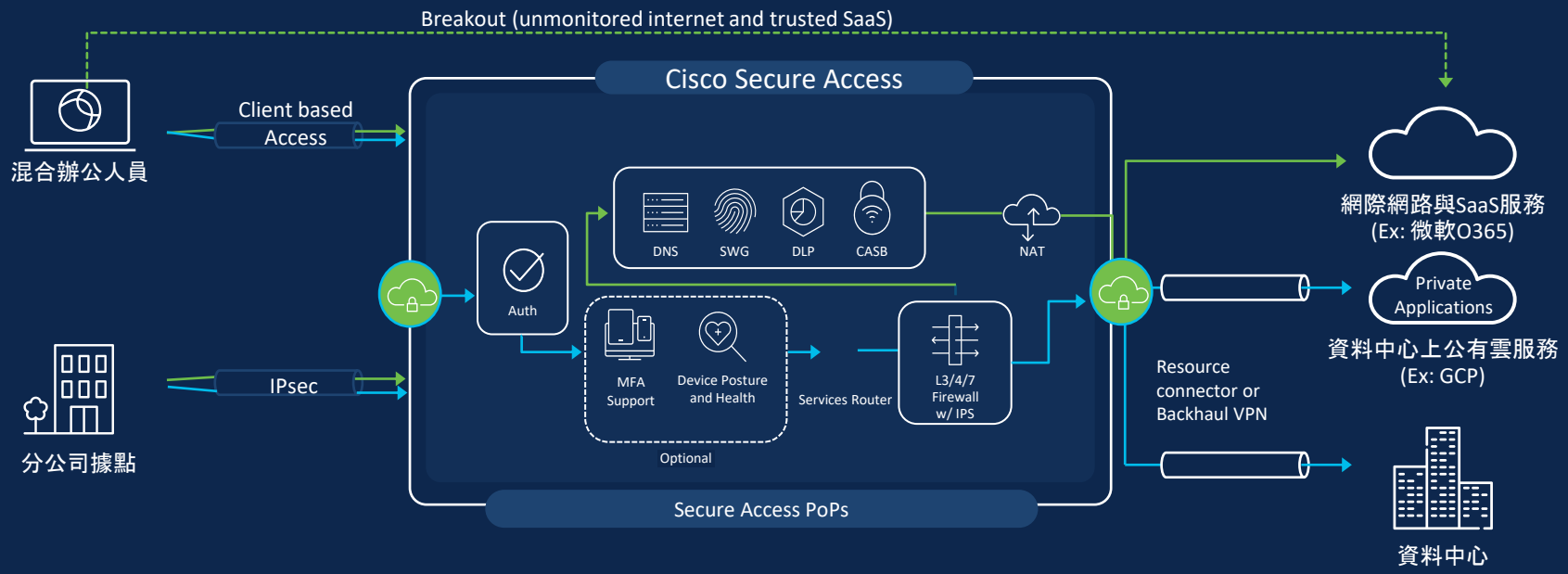


It just works. No drama, no fuss. Just pure, unadulterated convenience.

現況：各種來自不同品牌的資安防禦機制集中在分行與端點

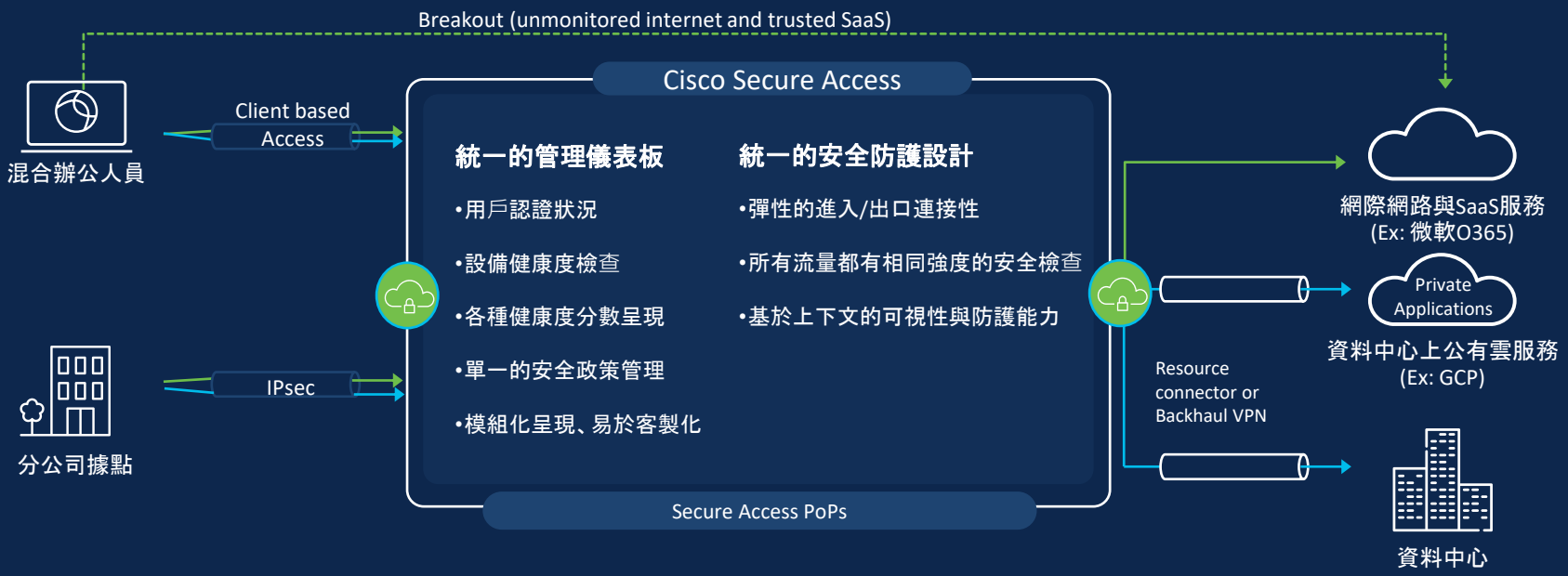


導入SSE：將防禦機制集中，易於部署與管理



Users — How — Apps

導入SSE：將防禦機制集中，易於部署與管理



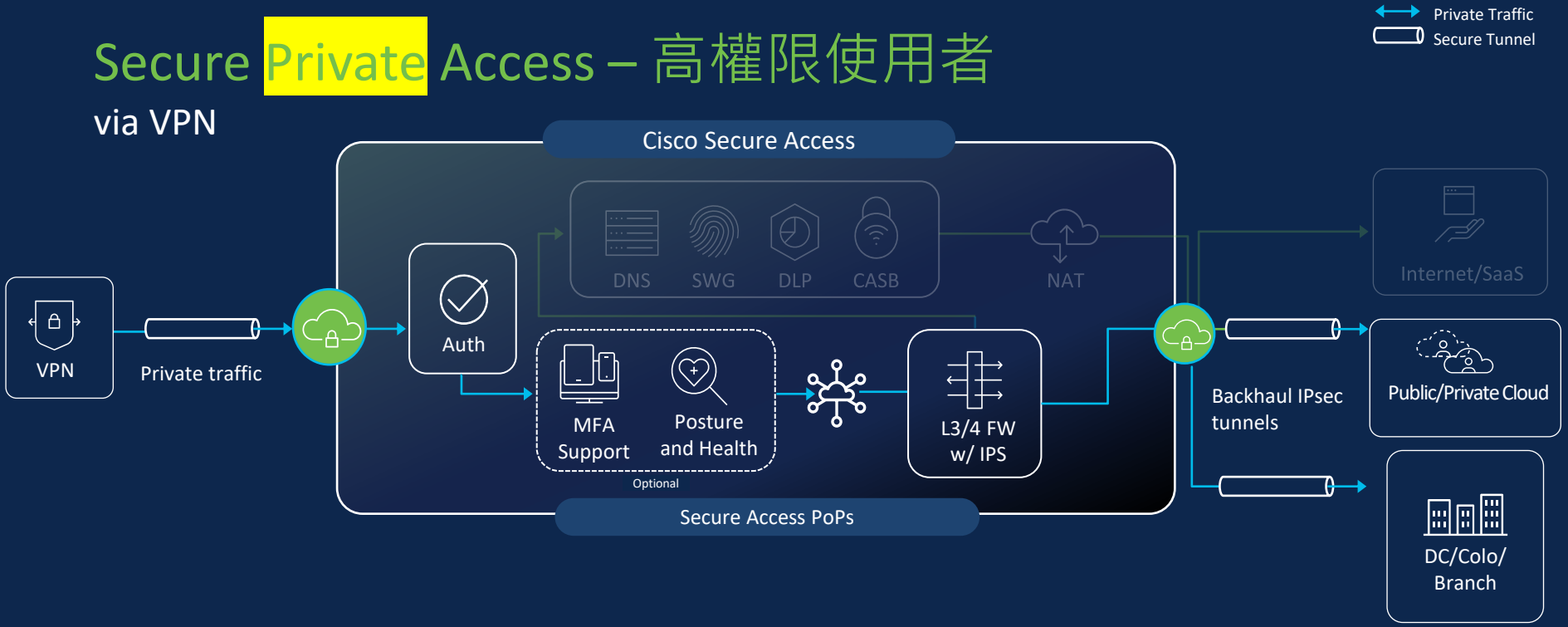
Users — How — Apps

Use Cases

- Secure Private Access
  - Via VPN
  - Via ZTNA (Client Based)
  - Via ZTNA Clientless
- Secure Internet Access
  - VPN full tunnel
  - Branch traffic

Secure Private Access – 高權限使用者

via VPN



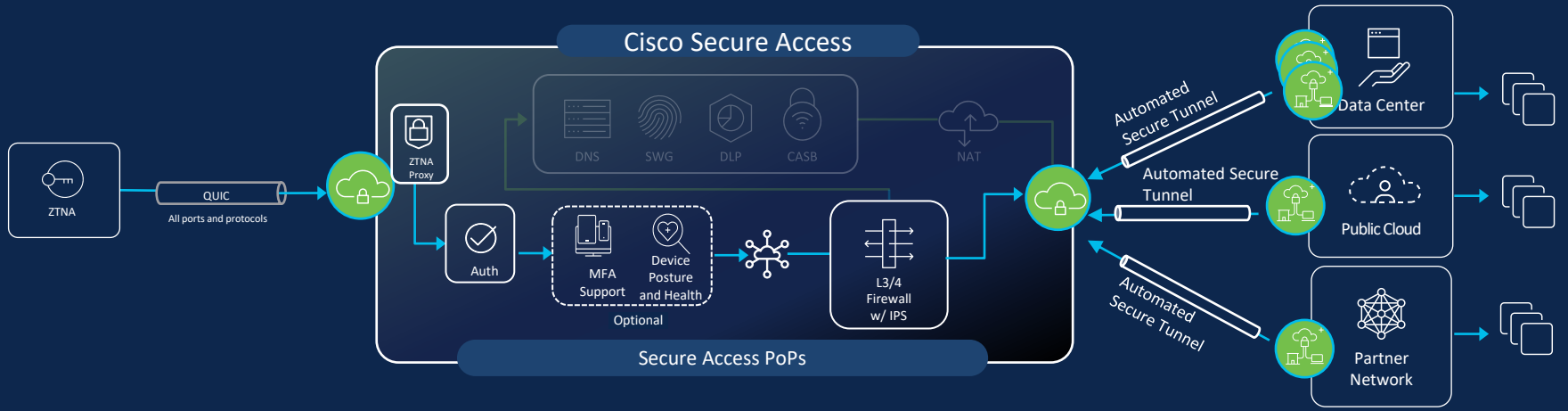
Benefits

- SAML 2.0 + cert-based authentication
- Posture verification (optional)
- Trusted Network Detection
- Start before logon
- IPS
- Granular context-based control

Secure Private Access (Client-based ZTNA) – 企業員工

Private Traffic
Secure Tunnel

No VPN

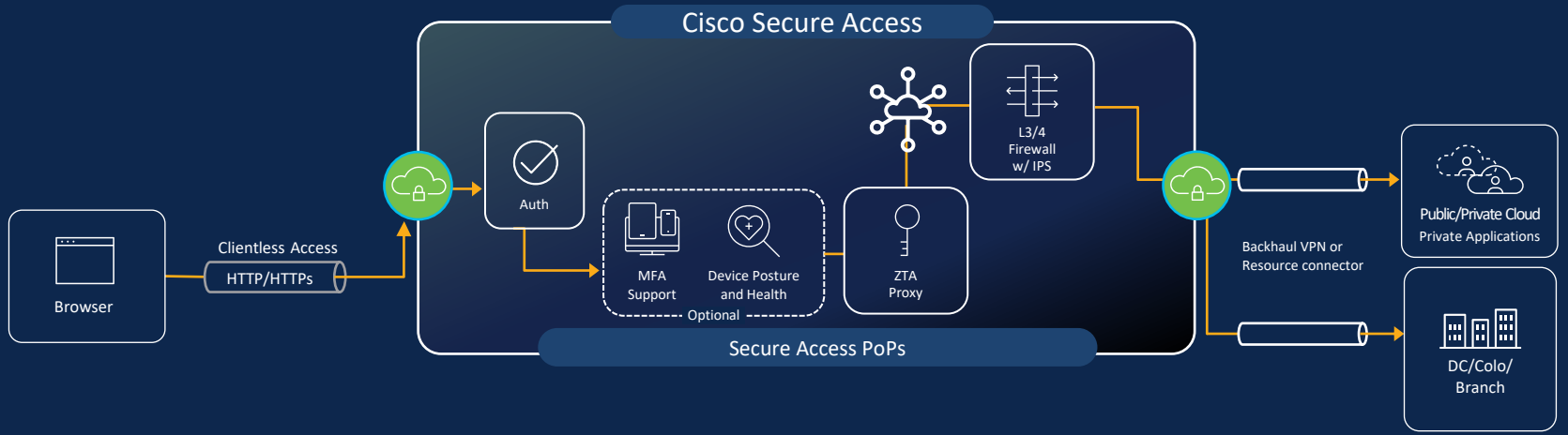


Benefits

- Reduced attack surface
- Inline security capabilities
- «Just works» user experience
- Performance benefits QUIC & MASQUE
- Per App tunnel
- Inside out TLS connections from resource connectors
- App is behind proxy, not visible to client
- No routing/IP/network connectivity
- Zero trust per application policy

Secure Private Access – 委外人力、合約廠商

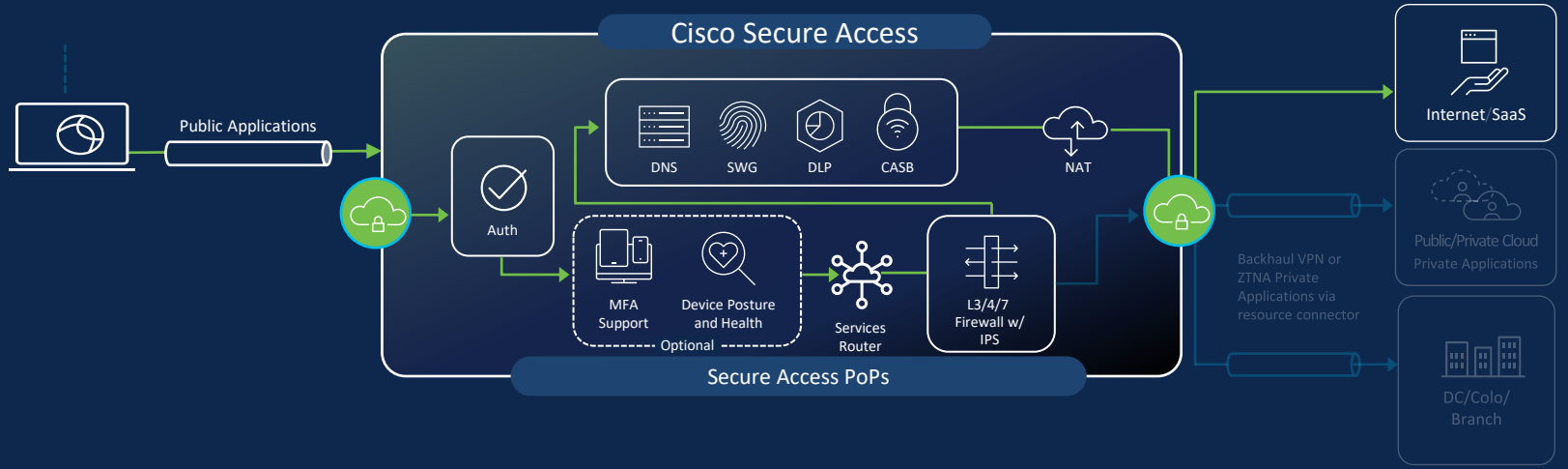
No VPN, No Client



Capabilities

- Clientless
- App-specific access
- Undiscoverable IP address
- Least privileged user access
- Reduced threat surface

Secure Internet Access – 移動辦公上網保護

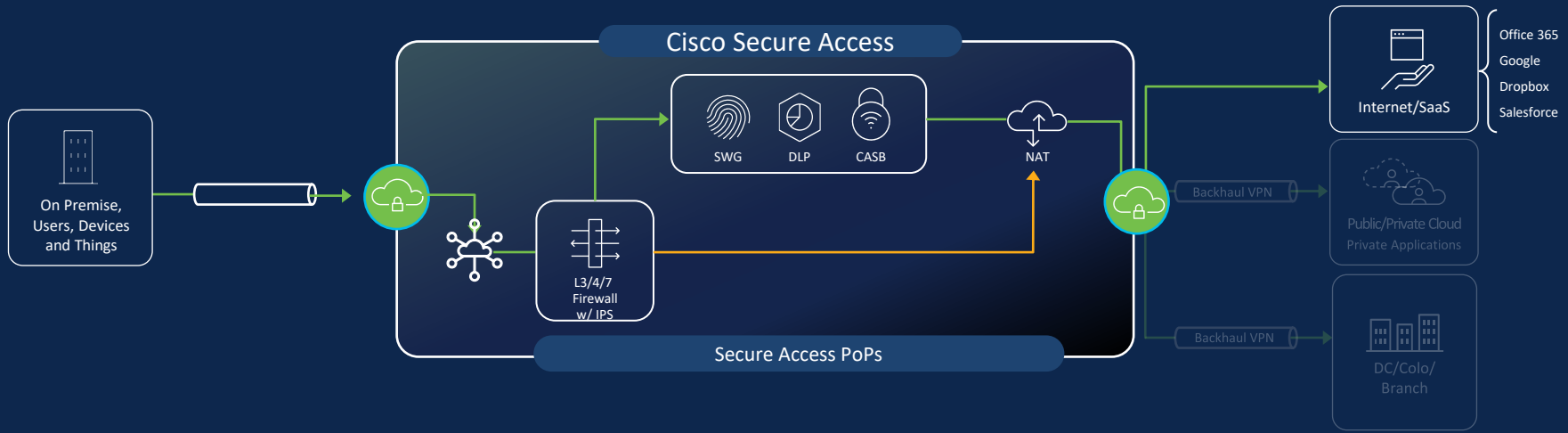


Capabilities

- SAML 2.0 + cert-based authentication
- Posture verification (optional)
- IPS
- Single Inline inspection
- Application policy

Secure Internet Access – 辦事處安全保護

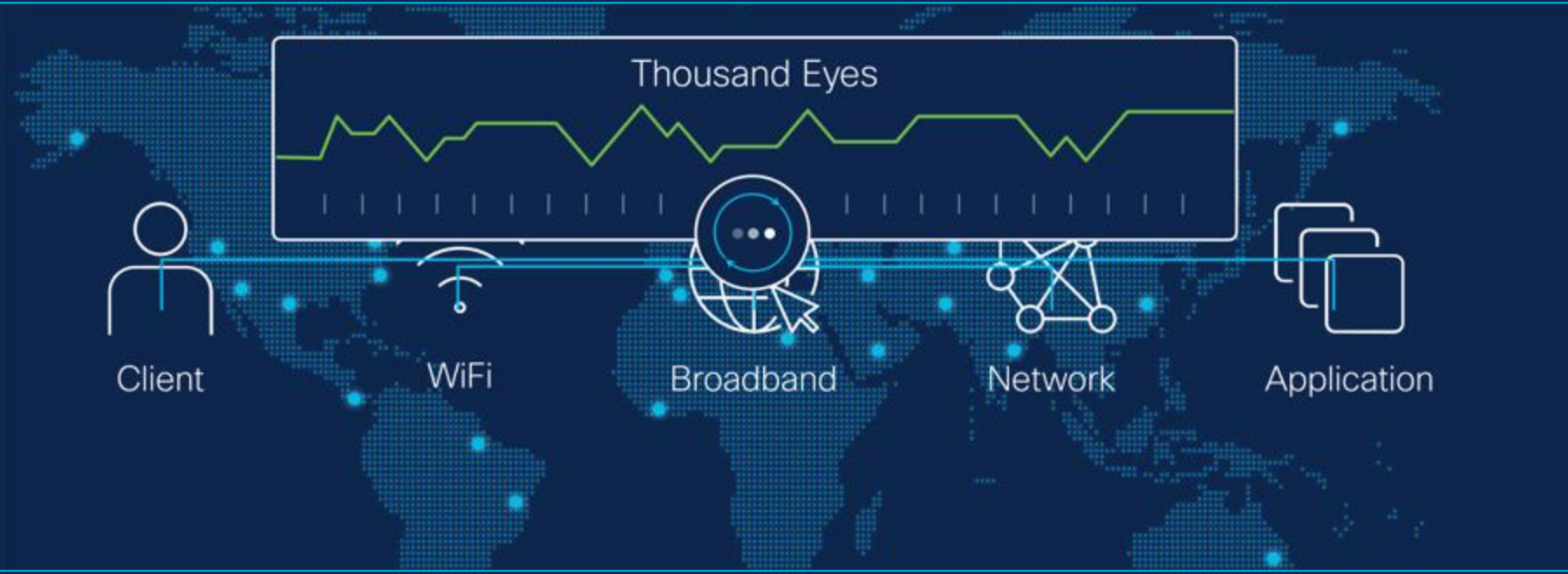
Branch



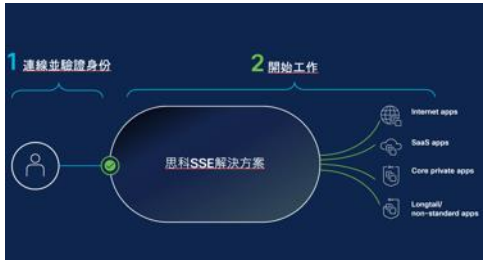
Capabilities

- Auto tunnels with Catalyst SD-WAN (Dec. 2024)
- 1 GBps per tunnel
- BGP
- ECMP support
- Active/Standby
- Overlapping subnets/Outbound NAT

One More Thing: 保護用戶安全的同時兼顧使用者體驗



分行導入安全服務邊緣(SSE)架構後所具備的能力



簡單直覺的使用者體驗

- 任何使用者任何地點
  1. 完成身份驗證
  2. 存取資源開始工作

完整的安全防護能力

- 資安即服務
  1. 隨時部署立即上線
  2. 保護使用者互聯網安全
  3. 禁止使用者任意傳送機敏資料

統一的安全管理體驗

- 統一的資安維運體驗
  1. 連線品質即時掌控
  2. 多種防禦機制單一管理平台
  3. 思科原廠統一支援

Q&A