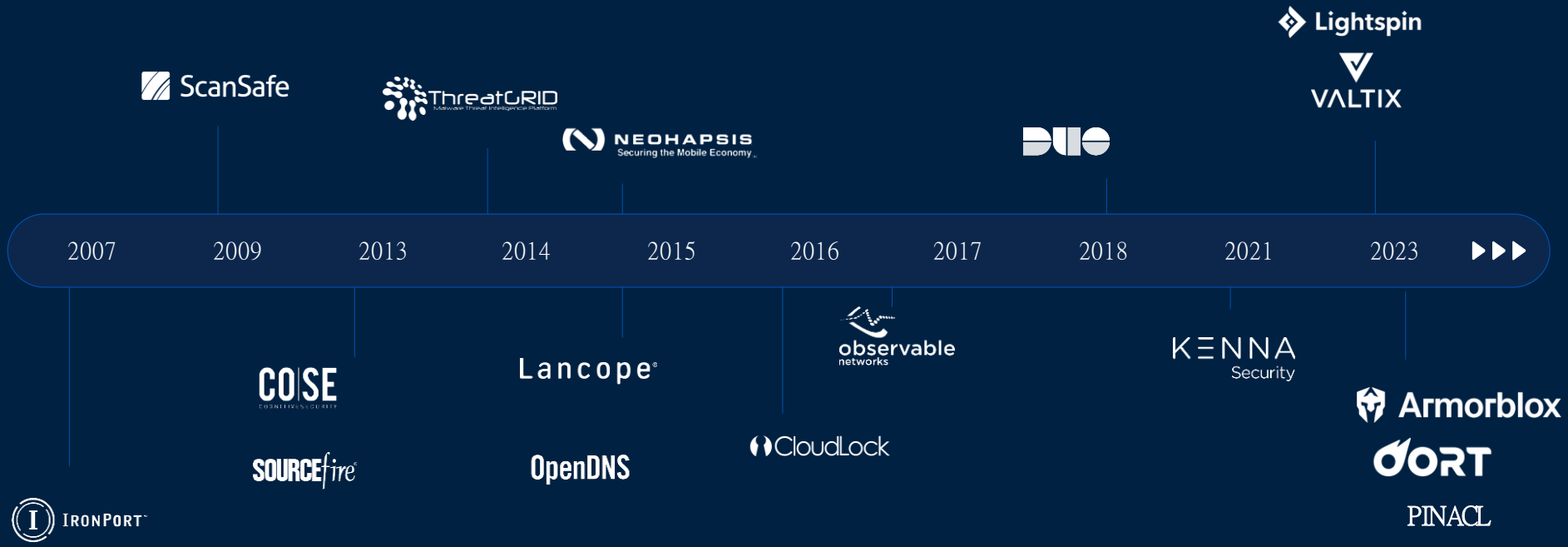
思科零信任架構

Segmentation: Data Center, Cloud, and Campus/Branch

Jarvett Lin | 林秉忠 | 思科全球資安資深業務經理

August, 2024

Cisco Security acquisitions



透過收購、投資和策略合作夥伴關係增強我們的人工智慧能力

Acquisitions

splunk> a CISCO company

Armorblox now part of CISCO

MindMeld

babblelabs

PERSPICA

voicea

ACCOMPANY

Investments

ROBUST INTELLIGENCE

DataRobot

cogniac

moogsoft Continuous Assurance

securiti

habana

AISERA

scale

dremio

MISTRAL AI_

uniphore

cohere

Paxata

$1B Investment Fund
AI Infrastructure and AI Software

Partnerships

NVIDIA

AMD

intel

aws

Microsoft

AI Partner Specialization Training for Channel Partners

Security for AI, AI for security

保護 AI 堆疊並透過 AI 增強安全性

安全使用人工智慧	Protect the use of AI, leveraging partners to help co-develop custom models
大型 AI 資料中心的 AI 原生安全	Hypershield AI capabilities to auto-detect application behaviors, write and test compensating controls and discover anomalies in application behaviors
下一代 SOC	AI-powered capabilities from Splunk and Cisco XDR to supercharge threat detection, prevention and remediation

Cisco Secure in AI/ML

Armorblox
now part of cisco

人工智慧安全威脅防護領導者，情報大數據。
Large Language Models (LLMs)

ORT
now part of cisco

帳號接管是第一大攻擊因素，透過ML來發現隱藏的IAM攻擊

PINACL

Lightspin

VALTIX

威脅情資生成

AI-分析 情資威脅大數據分析，自動化規則生成

簡化安全維運

AI- 驅動安全策略管理、配置、排除故障、可視化、操作

複雜的攻擊預防

AI-使能 SOC 助手，事件優先級、事件調查、整改建議

大語言模型的安全使用Responsible AI

模型監控和模型安全、數據丟失防護、合規性評估

CISCO
SECURE

零信任以及網路管理的挑戰

使用者、裝置和應用程式無所不在

IT 格局的重大轉變

Hybrid work is the norm

Remote Users

Personal &
Mobile Devices

IoT Devices

Transition to multi-cloud and SaaS

SaaS
Applications

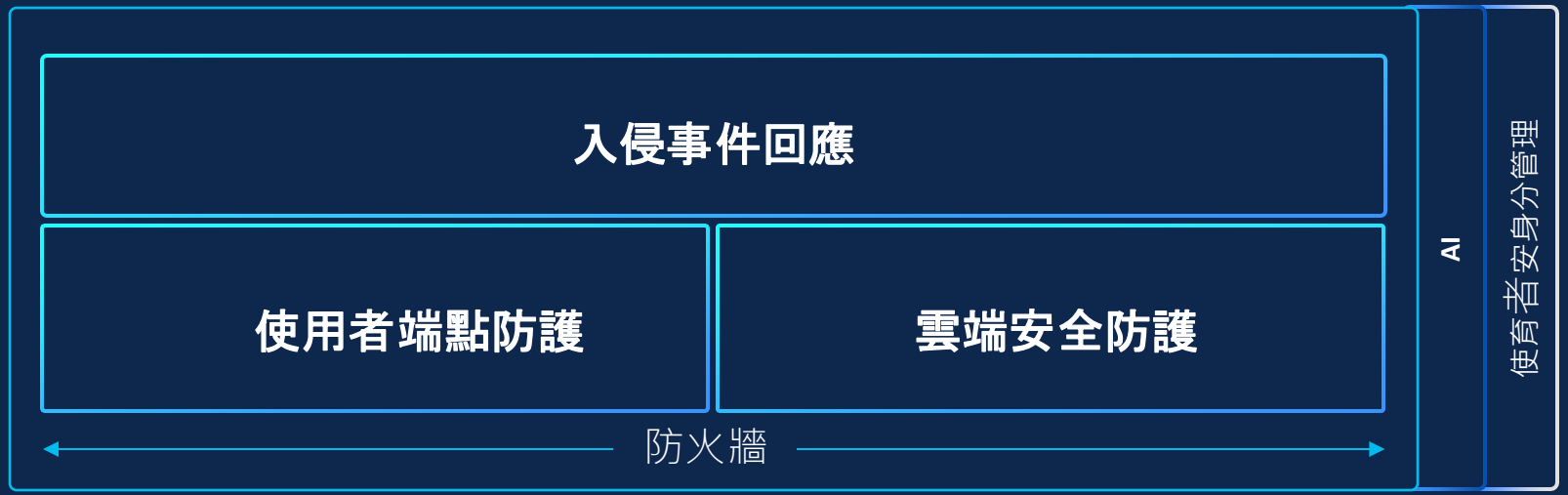
Hybrid Cloud
Infrastructure

Cloud Native

Everything is encrypted

95% of web traffic, 86% of malware and
100% of SaaS traffic is encrypted

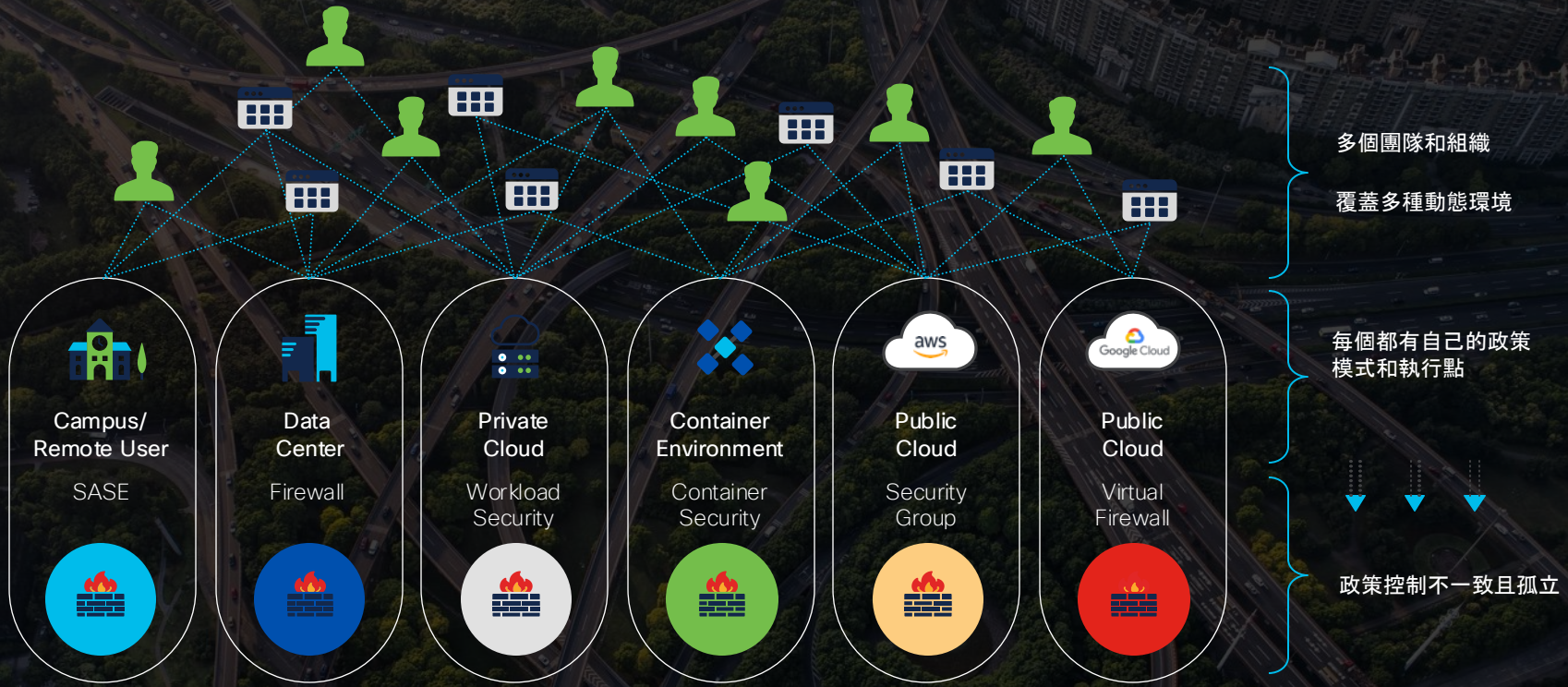
整體說來我們需要保護什麼？



資訊安全事件管理 (SIEM)

IT 團隊的挑戰

混合環境中的工具和策略複雜性




Data Center
Cloud
Campus/Branch

我們面臨的挑戰

The current state “before” scenario

Data Center

Cloud

Campus/Branch

Risk of Business Interruption | *Increased likelihood and impact of a breach*

Visibility gaps | Unknown *communications, dependencies, and application risk*

Visibility gaps for connected devices
Device sprawl and IoT are out of control

Exposure from limited East/West Enforcement | *Attack surface across workloads is too large*

Complex, static security policies lag behind | *Need adaptive, automated, and scalable policies*

Can’t meet Regulatory Compliance | *Risk of failing audits*

Limited enforcement | *Need least privileged risk-based access control for users, apps, workloads, and devices*

Can’t simplify and standardize at scale | *Can’t change policies fast enough to keep up with the business*

我們想達成的目標

The “after” scenario they are seeking

Data Center

Total Visibility | *Know every app, workload, and dependency*

Consistent and Effective Policies | Automate policies to keep pace with change

Reduced Attack Surface | *Know the risk level of your workloads*

Cloud

Campus/Branch

Total Visibility
Know every user and device

Automated Containment
Contain infected devices+revoke access

Achieve least Privilege Access
Restrict access by Users/Devices

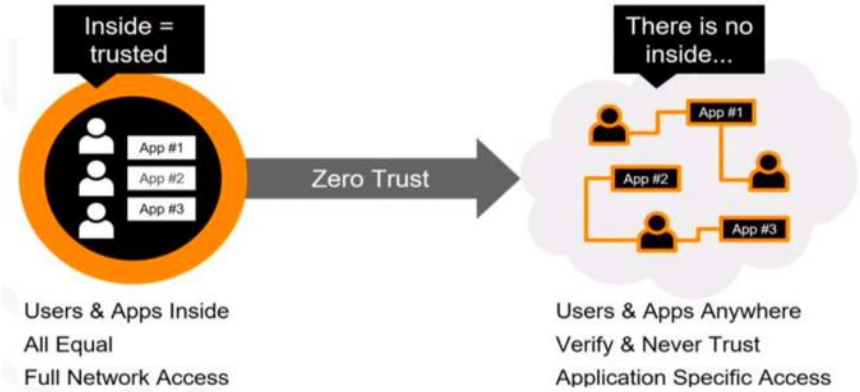
Complete Zero Trust Microsegmentation | *App to app and user to app control to limit scope of a breach*

Compliance Adherence | *Visibility into compliance status in real time*

零信任概念

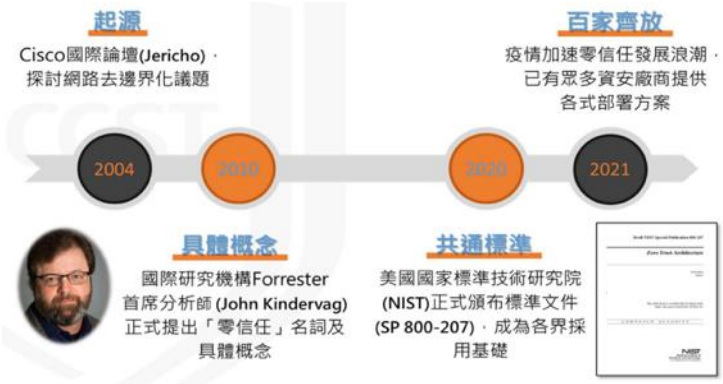
- 零信任希望突破傳統網路模型的資安窘境，並能保護資料存取
  - 不是保護網路存取，而是保護資料/應用存取
  - 無具體邊界，使用者/設備與資料/應用無處不在
  - 任何資料存取永不信任且必須驗證
  - 技服政府零信任網路說明文件 – 111/07/14

- **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)

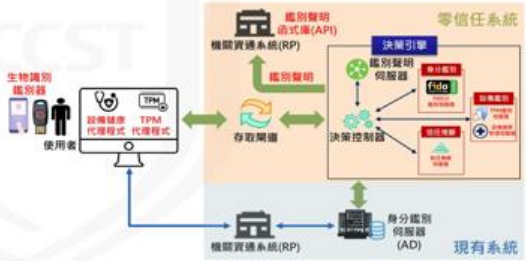
保護網路(包括IoT)上的所有用戶和設備連接

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	歐盟
具體規劃2024年前聯邦網路完成初步遷移。	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	設備鑑別	信任推斷
以生物識別鑑別器進行無密碼雙因子身分鑑別	基於信任平台模組(TPM)之設備鑑別，並進行設備健康管理	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

CISCO
SECURE

零信任該如何進行

從哪裡開始

Workforce
User and device 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？

Workload
Application and workload access

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？

Workplace
Network access

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

技術上的控制方法

- **定義網路邊界, 驗證網路存取**
  - **防火牆建立防線**
  - **軟體定義的網路邊界** (SD-Wan, VPN, ZTNA)
  - **網路存取的身分驗證** (NAC, Network Access Control)
- **持續驗證使用者以及安全性**
  - **設備是否符合安全規範**
  - **使用者是否為真正合法使用者** (Password vs MFA)
- **維持最小的網路及系統授權**
  - **是否有權存取系統**
  - **是否有權使用特定網路協定**

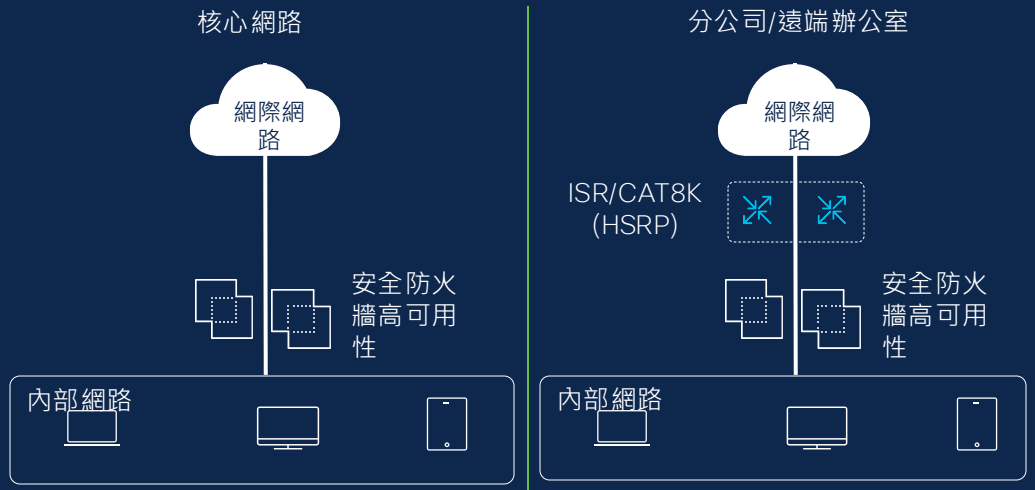
定義網路邊界，驗證網路存取
定義網路邊界

結果

- 改善分公司和/或園區邊緣的保護

為什麼選擇思科

- 無需解密即可實現應用程式可見性和執行
- 加密流量中的風險意識
- SD WAN 功能
- 最佳威脅防護、Snort 3 和 Talos



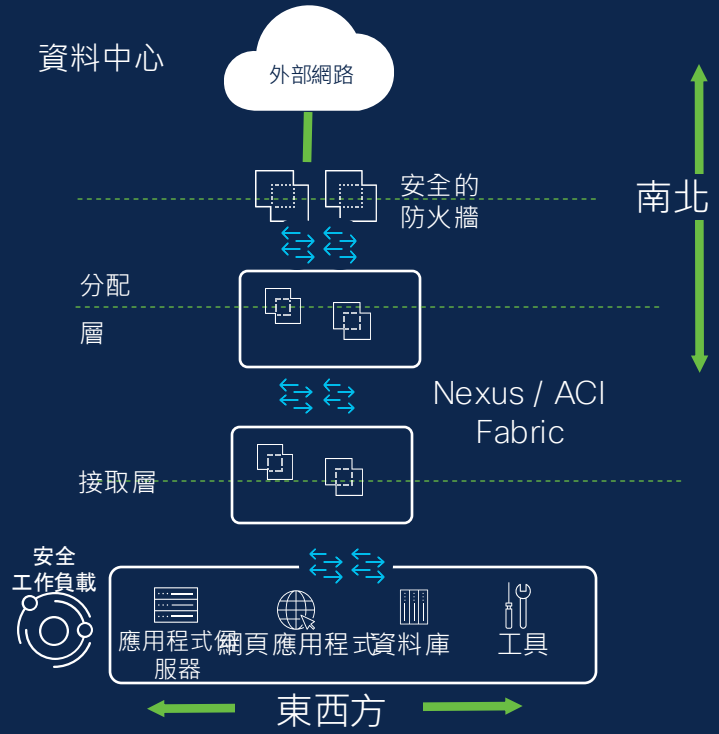
定義網路邊界，驗證網路存取
內部安全訪問

結果

- 減少攻擊面並增強任何地方的工作負載威脅防護

為什麼選擇思科

- 微分段、策略發現和自動化
- 最佳威脅防禦、Snort 3 和 Talos
- 隨處部署（混合、多雲、ACI、容器）
- 可擴展性和集群



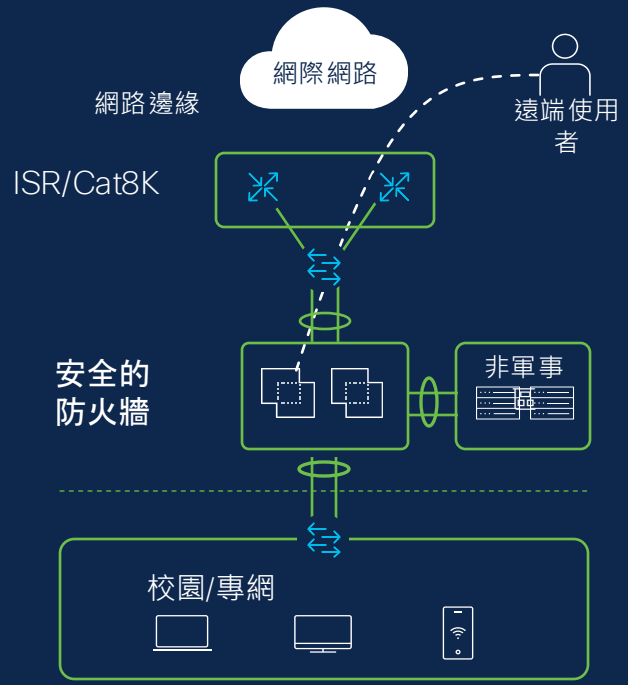
定義網路邊界，驗證網路存取端點
安全訪問

結果

- 任何用戶從任何設備對任何位置的任何應用程式進行基於風險評估的安全訪問

為什麼選擇思科

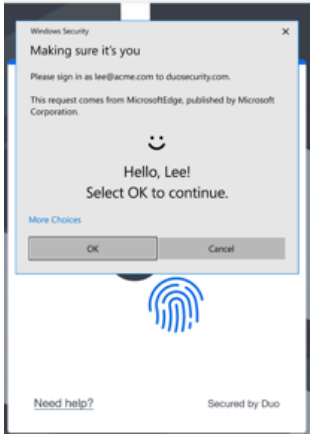
- 動態概況、態勢與政策評估
- 持續可信任訪問
- 最佳威脅防護、Snort 3 和 Talos
- 統一安全客戶端服務（VPN、威脅防禦、NVM、SSE、安全態勢）
- 3100/4200：內嵌硬體加密卸載和加速



持續驗證使用者以及安全性

- 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

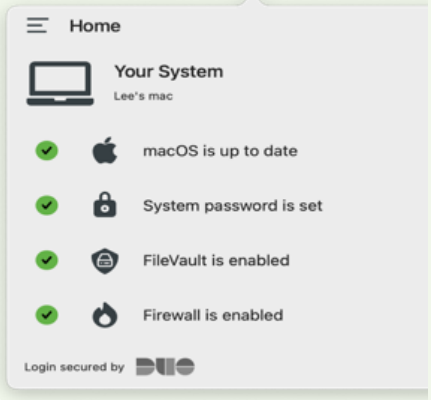
- Authenticators:
  - Touch ID
  - Face ID
  - Windows Hello
  - FIDO2 security keys
  - Duo Mobile

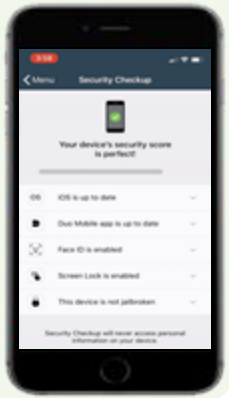


設備鑑別

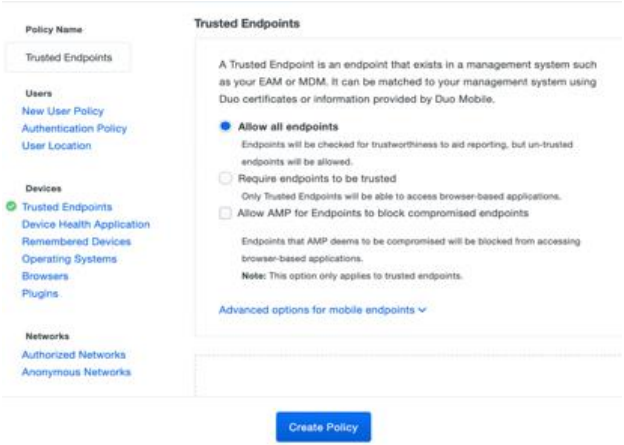
- 設備健康管理
  - 持續更新設備健康狀態
  - 依設備健康狀態隨時換算設備健康信任等級

Device Health App Duo Mobile





Duo Trusted Endpoints

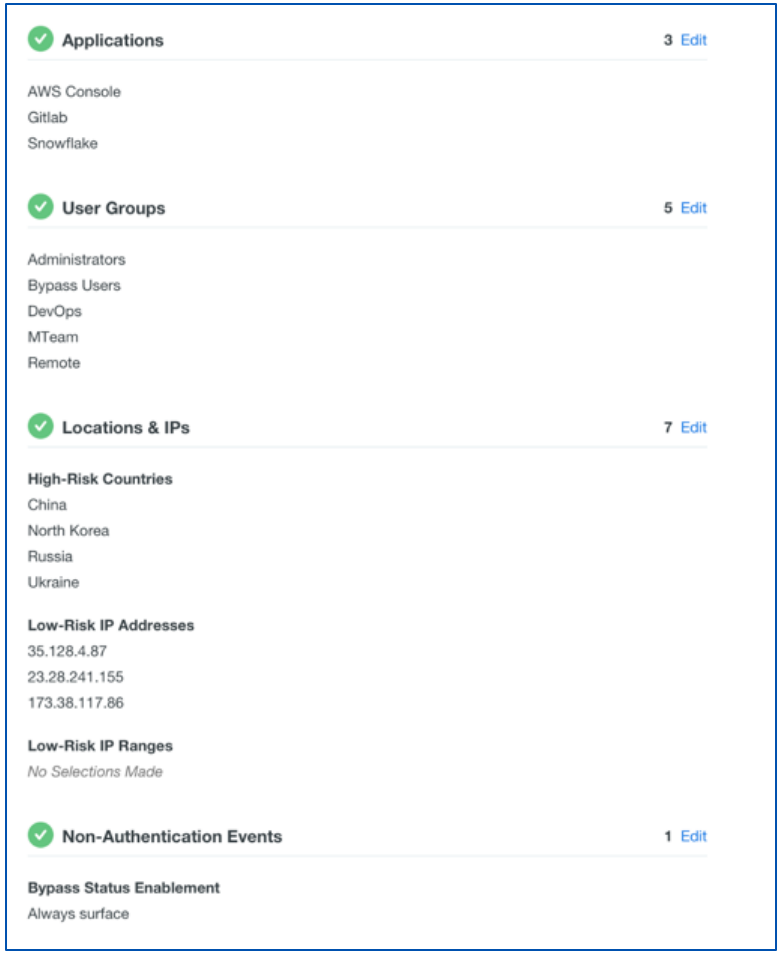


信任推斷

- 基於分數與情境之信任推斷機制

建立風險評估政策:

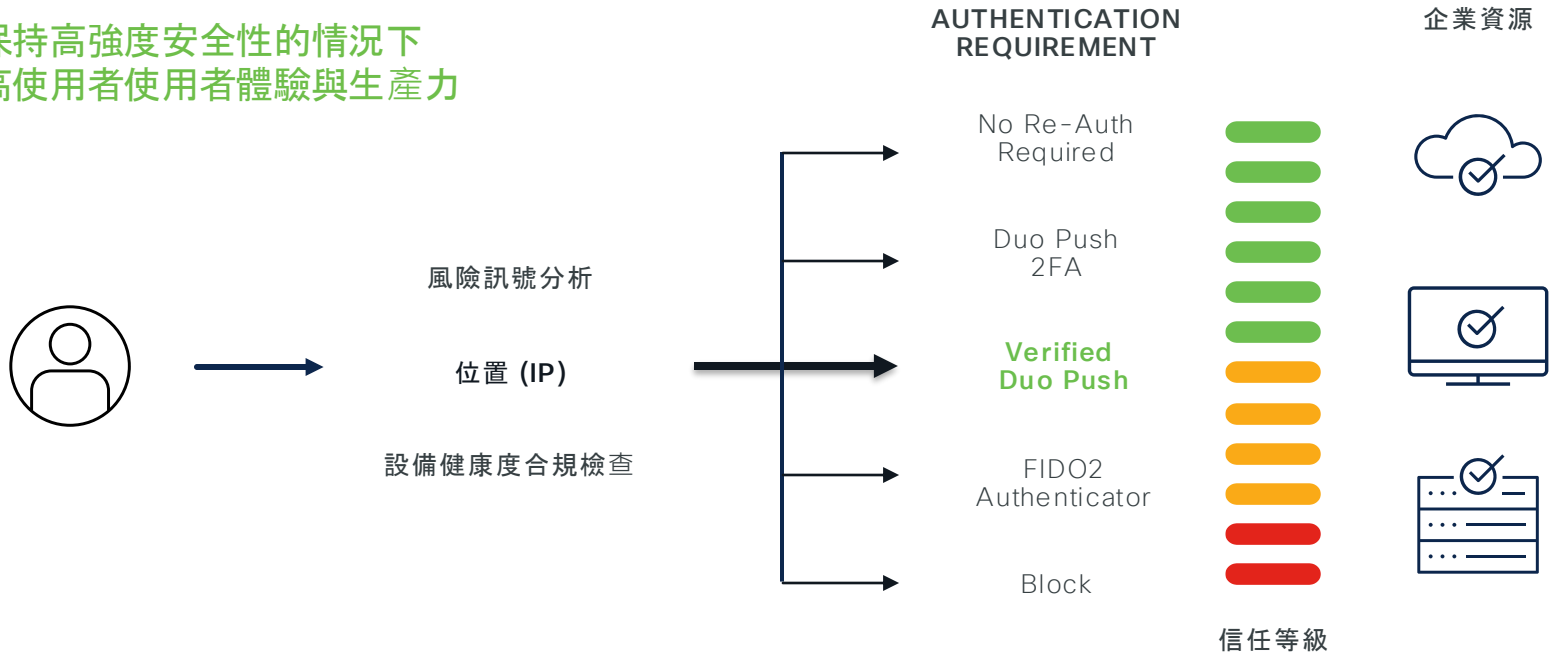
- **認證應用程式**
- **使用者與群組**
  - ✓ Administrators
  - ✓ Bypass Users
  - ✓ DevOps
  - ✓ RemoteWork
  - ✓ User
- **認證連線地區和IP**
  - ✓ **連線國家**
  - ✓ **單一IP或網段名譽**



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

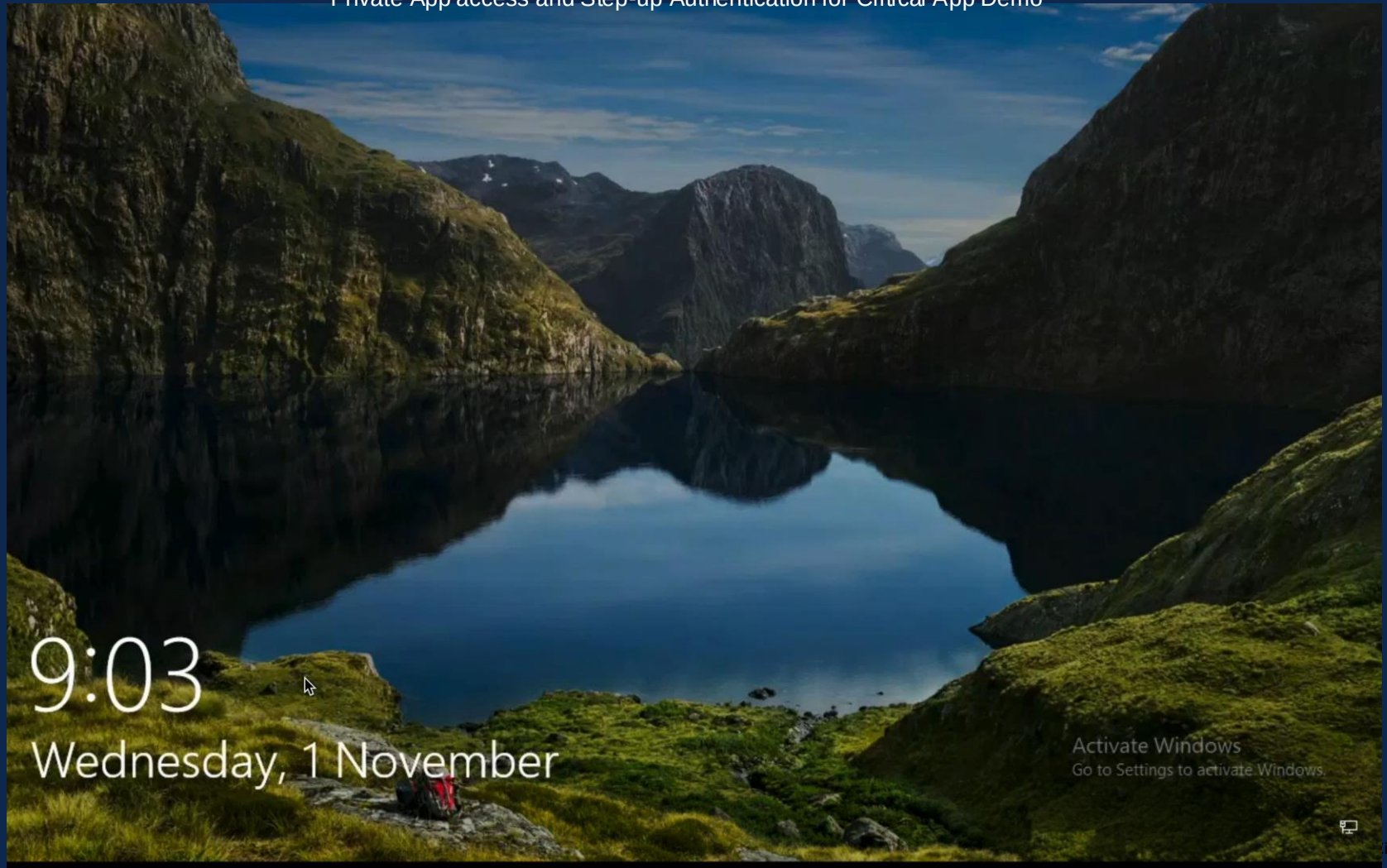
在保持高強度安全性的情況下
提高使用者使用者體驗與生產力



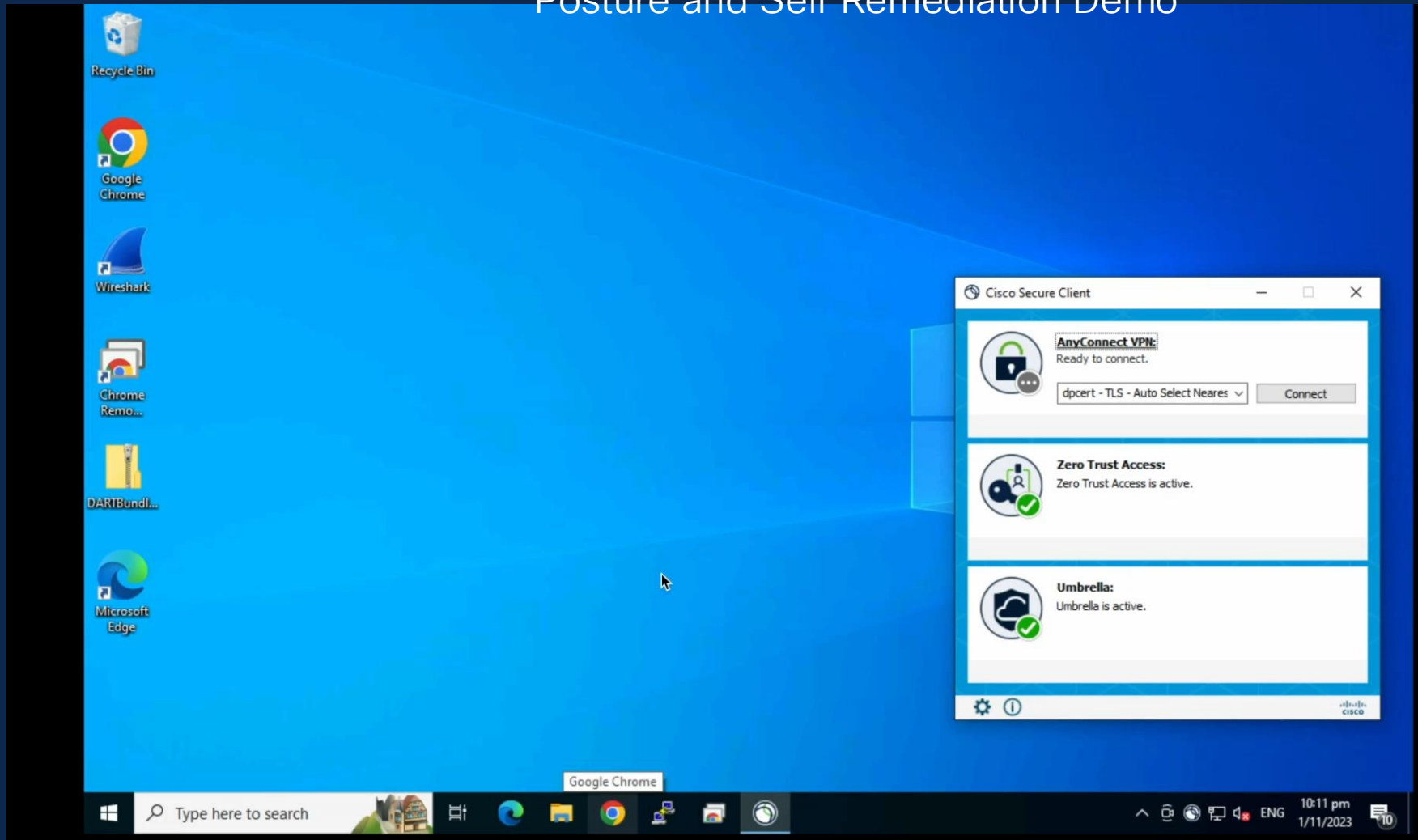
風險訊號: Known Attack Patterns

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.

Private App access and Step-up Authentication for Critical App Demo

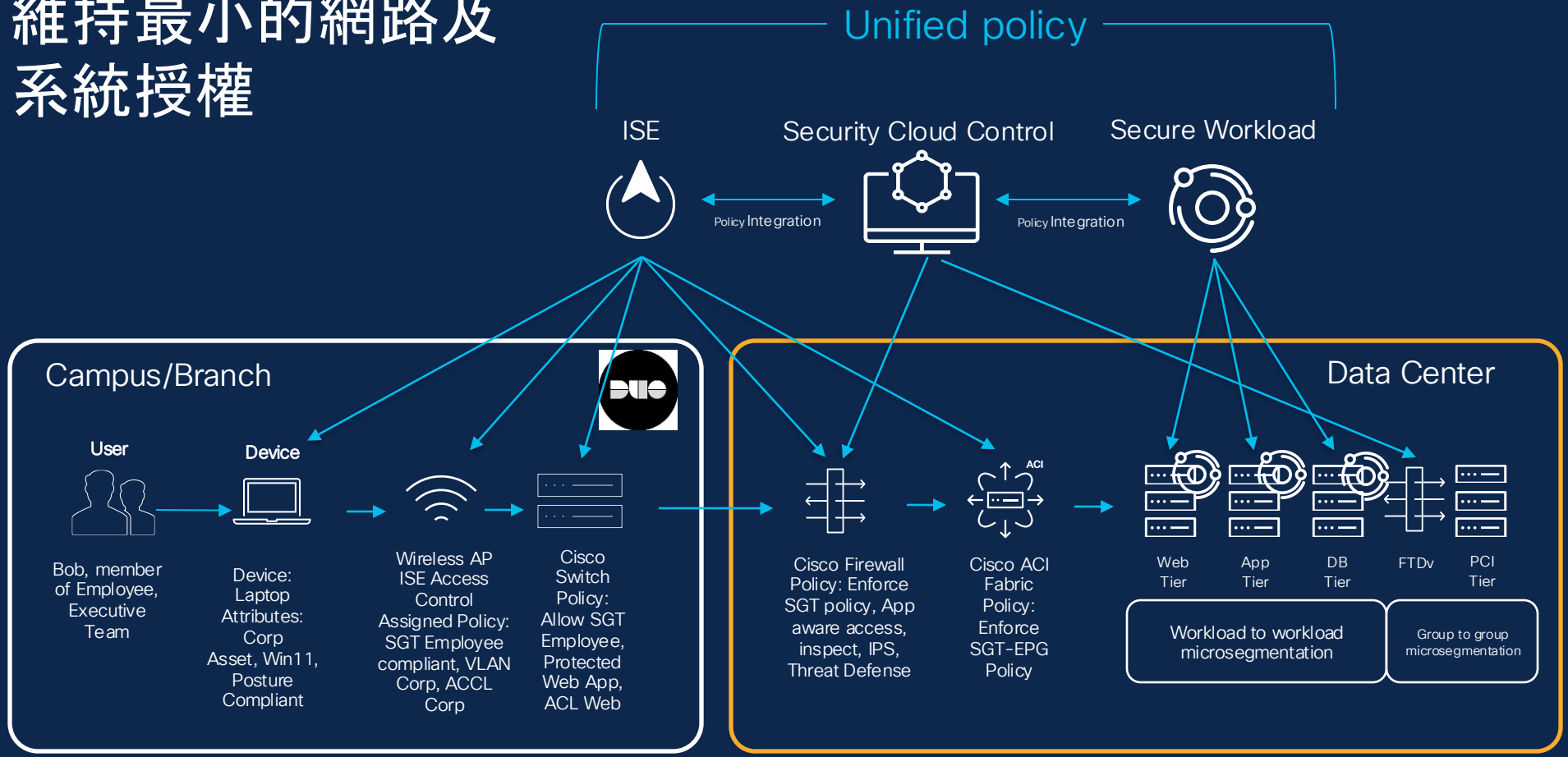


Posture and Self Remediation Demo



Zero Trust Access on Apple Device

維持最小的網路及系統授權



Why Cisco?

Cisco Security Solutions

Know which security solutions deliver segmentation outcomes

Data Center

Cloud

Campus/Branch

Secure Workload | *Zero trust micro-segmentation & workload protection to secure applications and data across multi-cloud environments, native multi-cloud policy integration and control*

Identity Services Engine (ISE) | *Dynamic network segmentation and access control to enhance security and compliance across your network*

Security Cloud Control | Centralized management and policy enforcement, enabling consistent segmentation and threat defense across multi-cloud environments

Firewall | *Advanced threat protection and zone-based segmentation to safeguard your network and assets*

Coming Soon: **Hypershield** | *Distributed, AI-native architecture that delivers security enforcement everywhere*

Multi Cloud Defense | *multidirectional protection across hybrid cloud, block ingress/egress and lateral movement*

Cloud Protection Suite | *End-to-end security solution for applications, workloads, networks, and clouds*

Why Cisco

Learn what our advantages are

Data Center

Secure Workload
More complete: Microsegmentation, visibility, & policy discovery vs. top competitors

Secure Workload & Firewall
Complete North-South and East-West segmentation solution

Cloud

Campus/Branch

Identity Services Engine (ISE)
Complete profiling and visibility of users and devices (IT and OT) delivers end-to-end segmentation vs. challenging multi-vendor strategy

Security Cloud Control
Centralized, consistent segmentation and threat defense across multi-cloud environments vs. challenging multi-vendor management

Firewall
Threat protection including visibility of threats in encrypted traffic to enforce segmentation vs. high cost of hardware decryption

Multi Cloud Defense
Standardizing multi cloud threat defense and removing complexity

Integrated Policy and Context Sharing
Shared context and integrated policy allows for end-to-end dynamic security policy

Coming Soon: **Hypershield**
Autonomous segmentation, distributed exploit protection, and self-qualifying updates

Be confident in segmentation

Cisco can deliver what nobody else can

謝謝指教