企業雲端化的資安考量與方案 - 從零信任網路架構開始

SE Manager: Nicholas Hsiao

Email: nhsiao@paloaltonetworks.com

NIST 選擇 Palo Alto Networks 作為零信任架構專案

paloalto NETWORKS | Blog

Palo Alto Networks | Network Security | SASE | Cloud Native Security | Security Operations

NIST 選擇 Palo Alto Networks 作為零信任架構專案

未分類

75 people reacted | 1

By Ryan Gillis
11 8 月, 2021 at 2:05 上午
1 min. read

This post is also available in: English (英語) 日本語 (日語)

2021 年 5 月拜登政府「改善國家網路安全性」行政命令概述美國政府針對強化網路防禦所必須採取的一系列行動。特別是其中一項條款，要求部門與機關開發一套實作零信任架構 (ZTA) 的策略，這作為行政命令中的主要計劃，可能已經獲得廣泛的關注。

儘管零信任架構是一個關鍵安全性概念，但其實作方面仍未獲得普遍的理解。為了協助處理此差距並支援聯邦政府的零信任旅程，Palo Alto Networks 很榮幸獲選為協作者，與國家標準與技術研究院 (NIST) 國家網路安全卓越中心 (NCCoE) 展開合作，共同完成新啟動的實作零信任架構專案。Palo Alto Networks 技術將部署至 NCCoE 並開發實用且協作的方法，藉此設計出符合 NIST SP 800-207 零信任架構中所記載宗旨與原則的零信任架構。

受到疫情大流行影響轉變為遠端工作的期間，政府組織明顯加快改用雲端的步調。我們現在觀察到混合式工作出現新的演進，採用零信任架構的需求有所提升，藉以確保實現所有數位環境中一致的安全政策執行。

網路與雲端中所需的安全策略必須從具備可視性開始，也就是必須能夠識別企業整體暴露的 IT 基礎結構以及攻擊範圍。

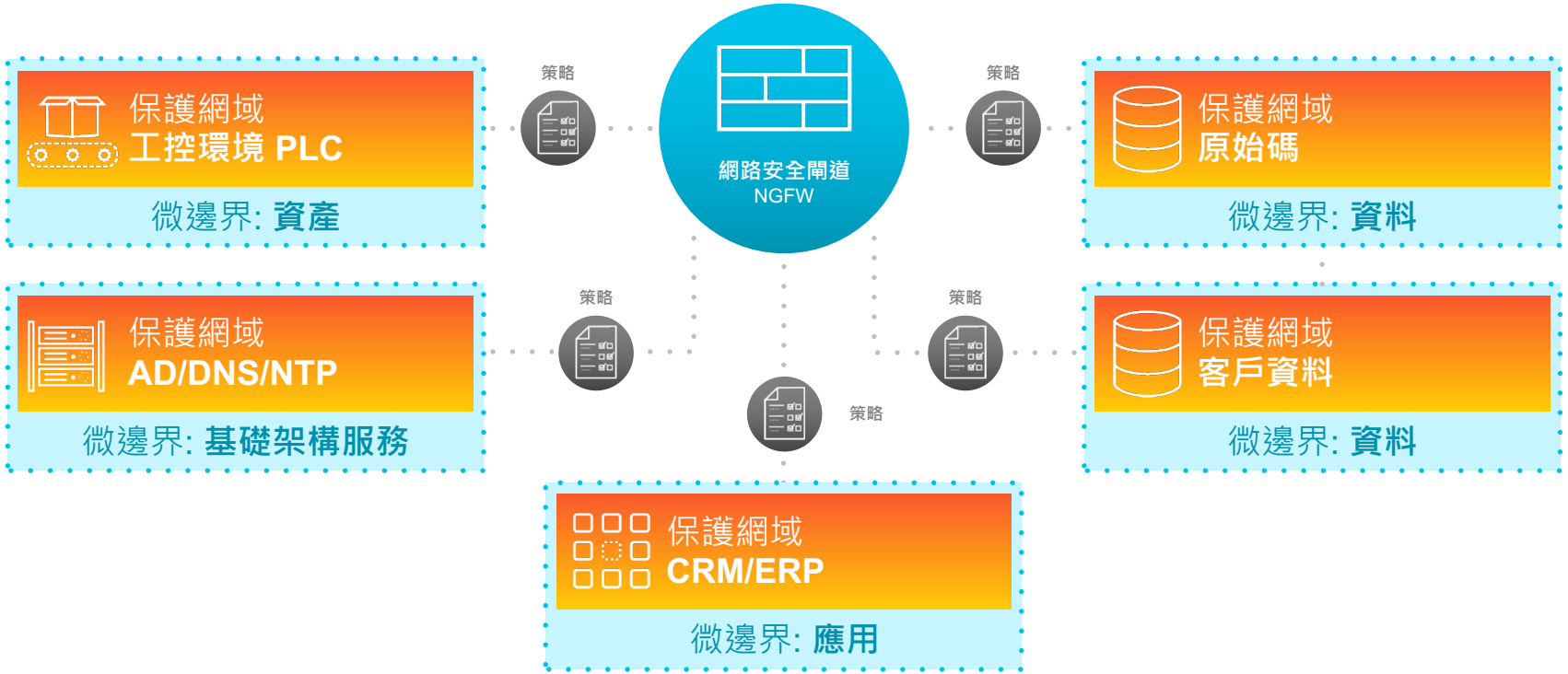
零信任方法需要從頭開始設計的解決方案，藉此持續且可靠地識別所有使用者、裝置與應用程式，而不論其位置在何處。如此可讓政府 IT 團隊在整個機構中一致地套用以脈絡為基礎的政策，透過持續驗證對機構網路與數據的存取，從而確保數位轉型的安全性。例如 User-ID、App-ID、Device-ID 與以政策為基礎的驗證等功能，將協助機構實作零信任架構，進而協助保護網路與使用者。

行政命令強調了利用 NIST 所開發的標準與指導，在所有聯邦網路與雲端環境中實作零信任的重要性。在目前正在建立的 NIST/NCCoE 實驗室環境中，Palo Alto Networks 技術能夠處理 NCCoE 高階概念性零信任架構的所有核心 (政策執行點、政策引擎、政策管理員) 與功能元件 (數據安全、端點安全、身分和存取管理、安全分析)。

五年多以來，Palo Alto Networks 已建立相關技術，持續協助企業在其網路與雲端環境中實作零信任。隨著行政命令現在將國家的注意力集中在零信任，我們很榮幸將實際經驗與專業知識帶入 NCCoE 的零信任架構專案，並進一步承諾提供聯邦機構保護其關鍵任務所需的相關指導與工具。

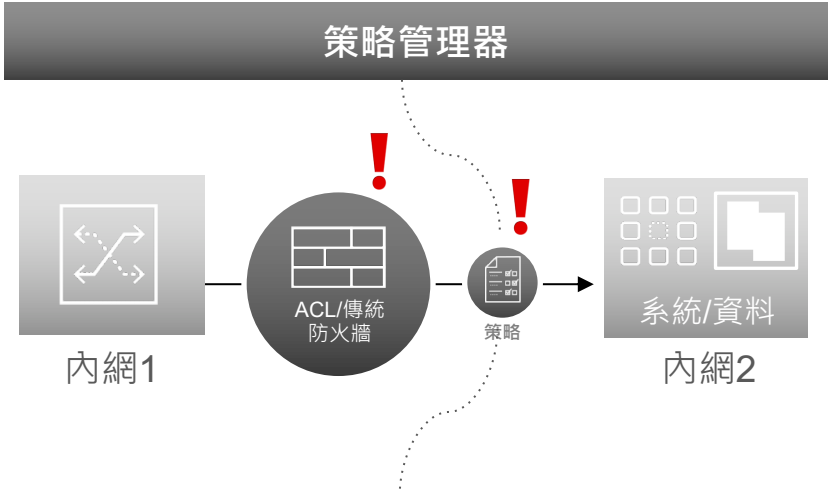
https://www.paloaltonetworks.com/blog/2021/08/nist-nccoe-zero-trust-architecture/?lang=zh-hant

零信任網路的基礎：建立保護網域



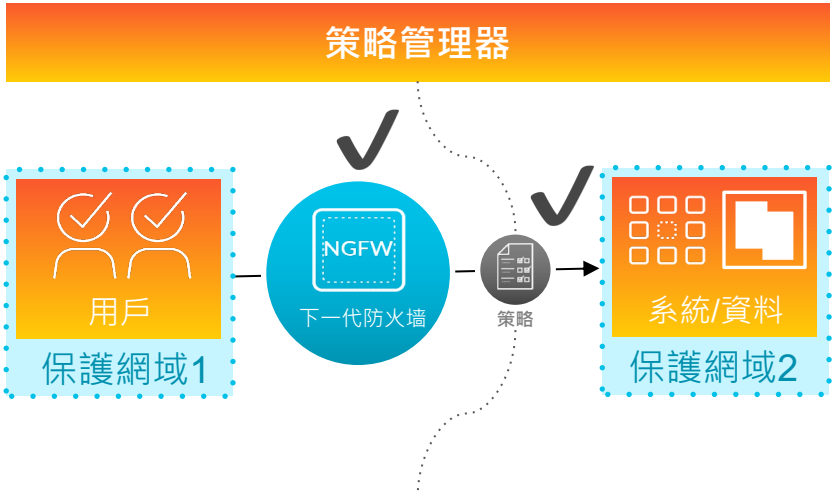
零信任網路：制定網路隔離政策，選擇合格的方案

傳統防護方式對內部網路
的存取只做有限度的控制



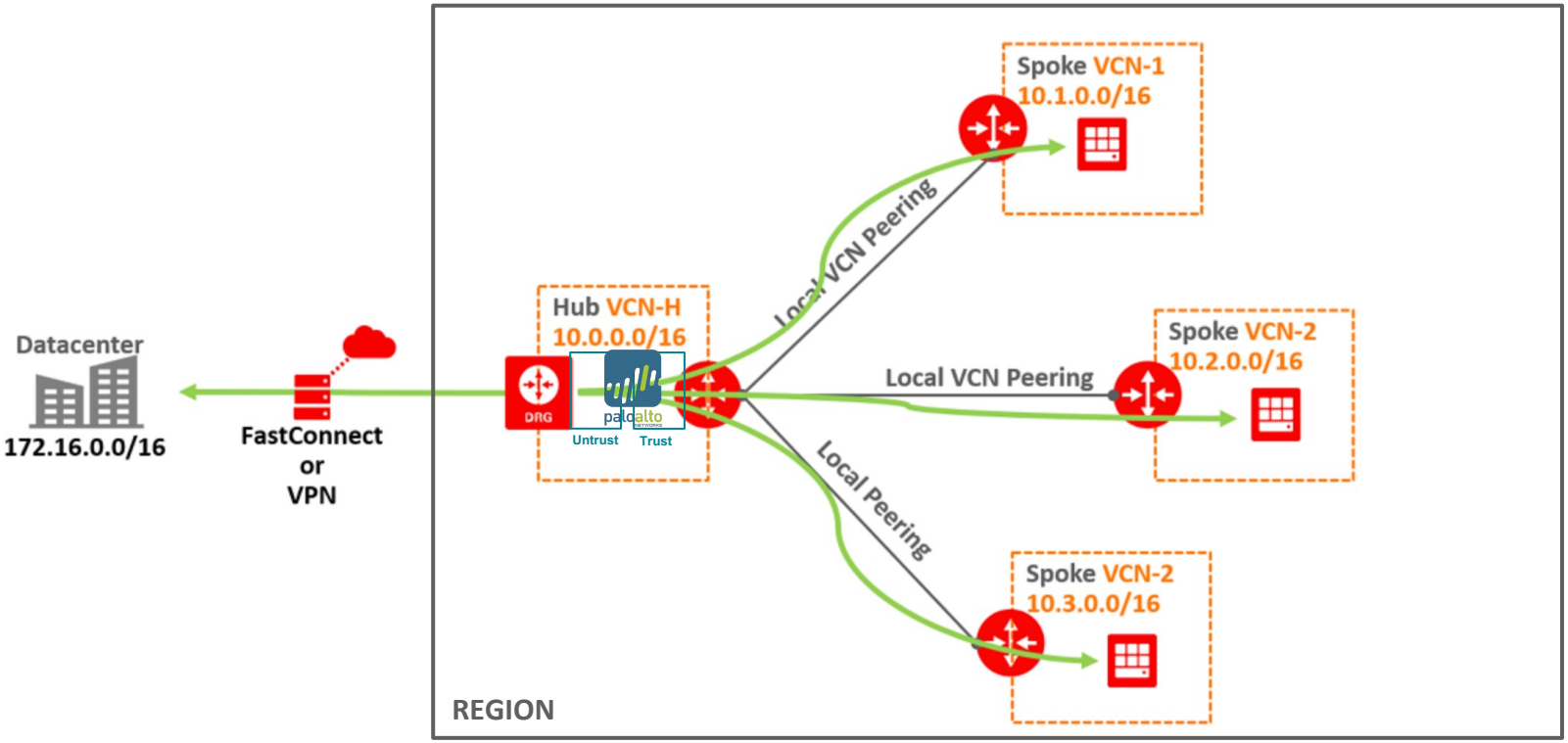
來源	目的地	端口	動作
10.1.0.0/24	10.0.1.21	443	Allow

從L2-L7的策略控制
實現保護網域之間的有效隔離

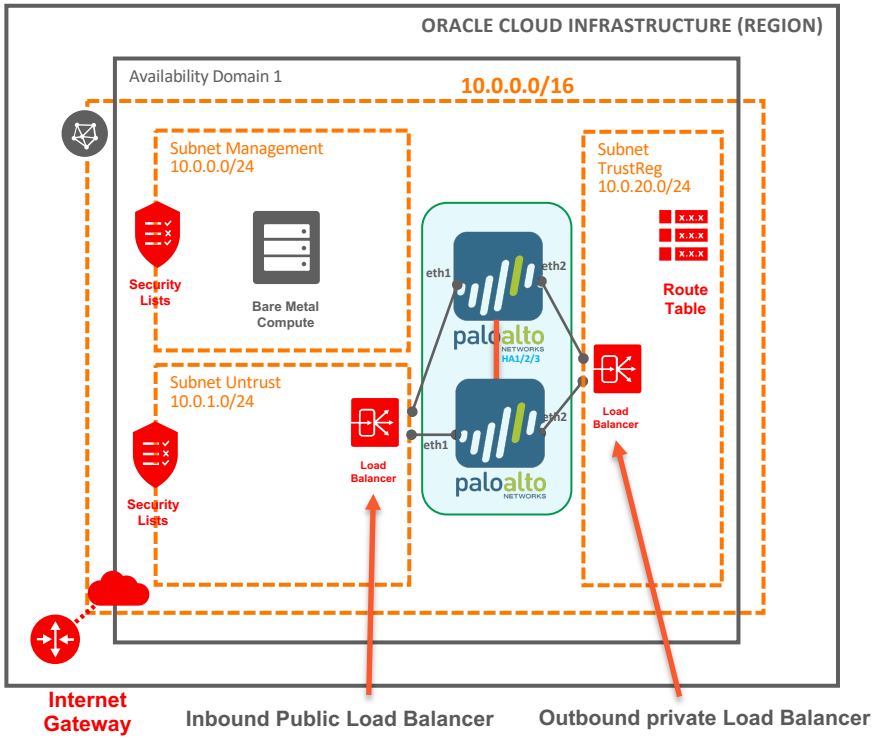


來源	目的地	用戶	應用	時間	動作
10.1.0.0/24	10.0.1.21	ad\user1	SAP	working_hours	Allow

範例： Oracle 上雲後的概念架構



範例：Oracle 上 OCI 的 High Availability 基本架構



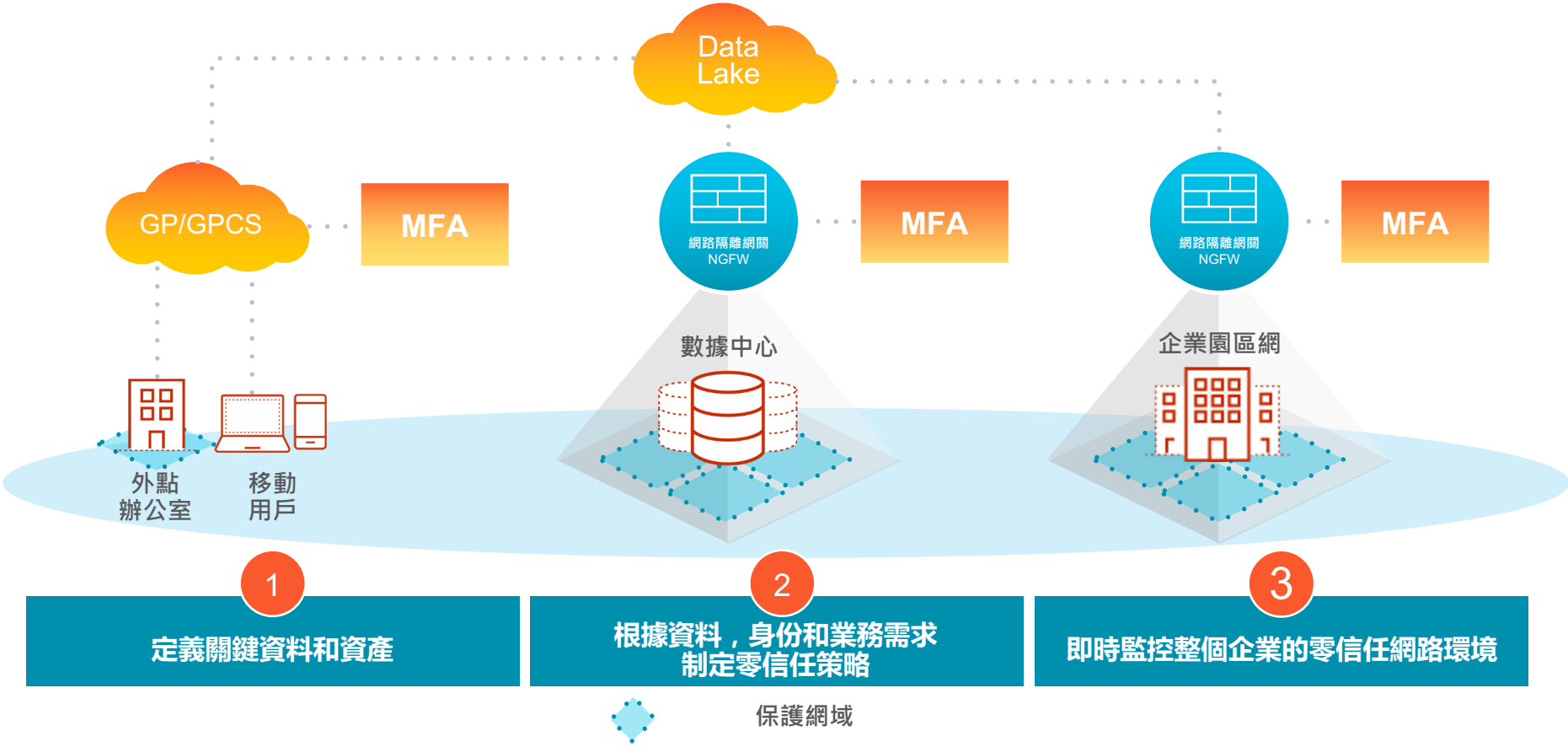
Use Case

- 在 Load-Balancer 之後的多個網域能夠使用 NGFW VM-Series
- 利用在 VM-Series 中的 trust interface 進行 Source NAT，確定流量能夠走回對的實體中。
- 能夠設定 Active/Standby 甚至 Active/Active 來確定 session 同步
- 內部流量可以串接 NGFW 進行政策檢查

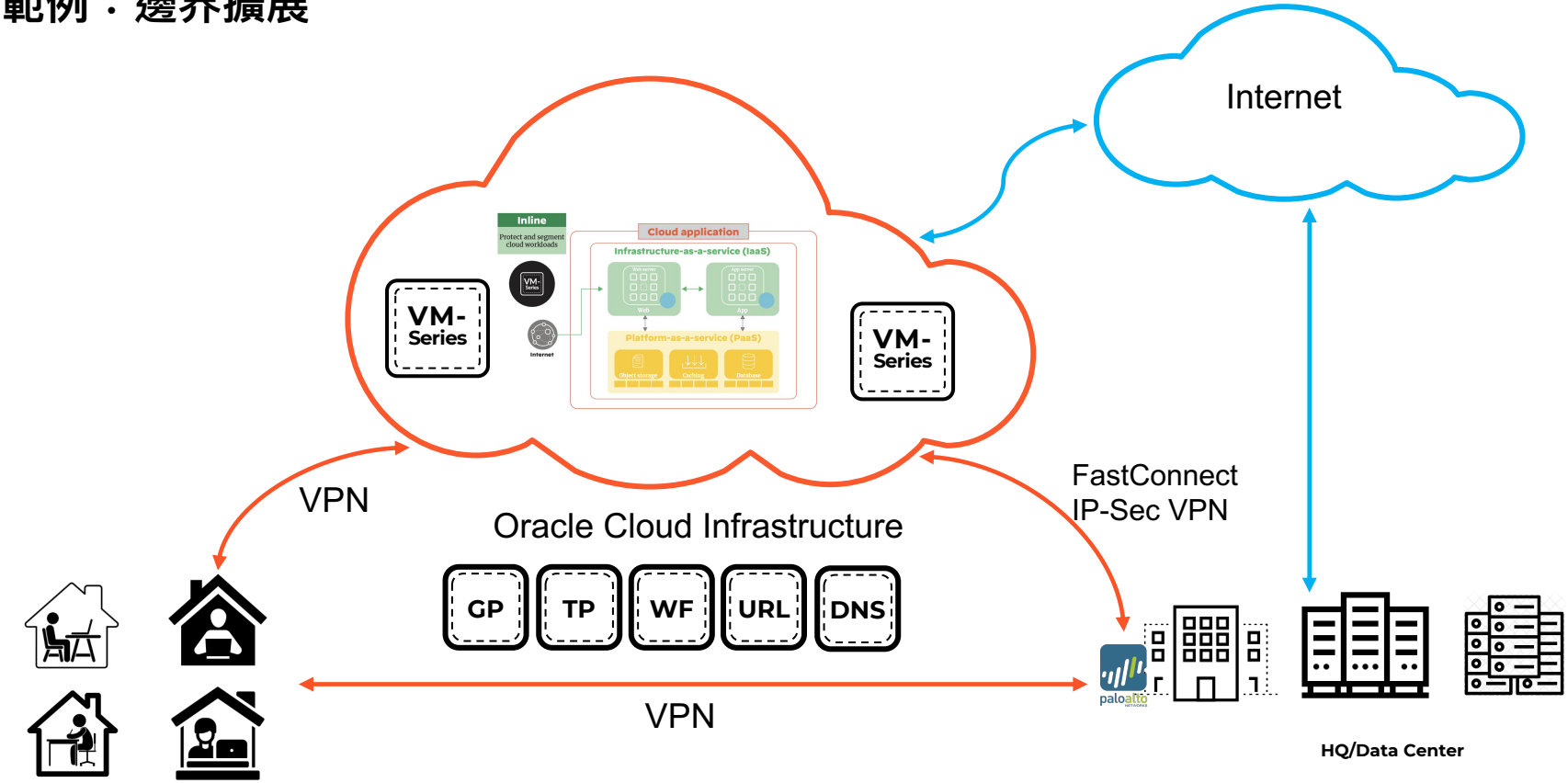
概念

- 利用政策確定資料流的正確以及合法性 (縮小 Trust Zone , Micro-Segmentation)，確定資料流的身份
- 對允許的流量，啟用資安政策，進行內容檢測

零信任網路：邊界的擴展

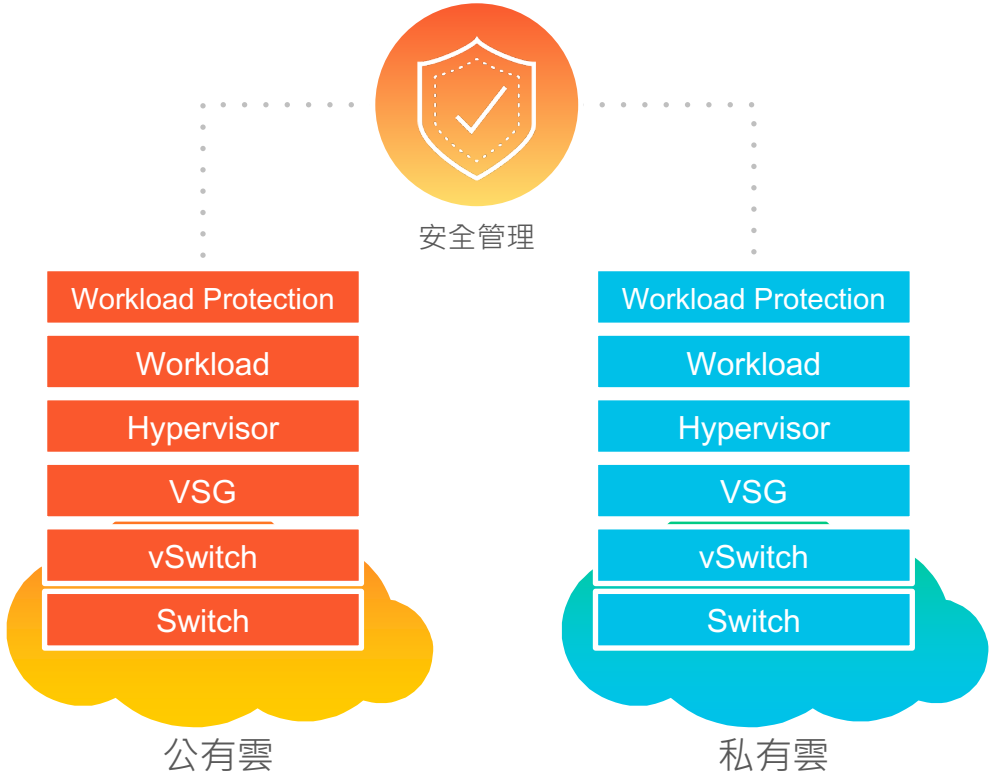

Data Lake
GP/GPCS
MFA
網路隔離網關 NGFW
MFA
網路隔離網關 NGFW
MFA
數據中心
企業園區網
外點辦公室
移動用戶
1
定義關鍵資料和資產
2
根據資料，身份和業務需求制定零信任策略
3
即時監控整個企業的零信任網路環境
保護網域

範例：邊界擴展



零信任網路：擴展到公有雲和私有雲

- 虛擬隔離閘道（VSG）作為零信任網路策略的控制
- 透明服務嵌入
- 一致的策略和管理



Prisma Cloud: Cloud Native Security Platform

Cloud Security Posture Management

Monitor posture, detect and respond to threats, maintain compliance

- Visibility, Compliance & Governance
- Threat Detection
- Data Security

Cloud Workload Protection

Secure hosts, containers, and serverless across the application cycle

- Host Security
- Container Security
- Serverless Security
- Web Application & API Security

Cloud Network Security

Monitor and secure cloud networks, enforce microsegmentation

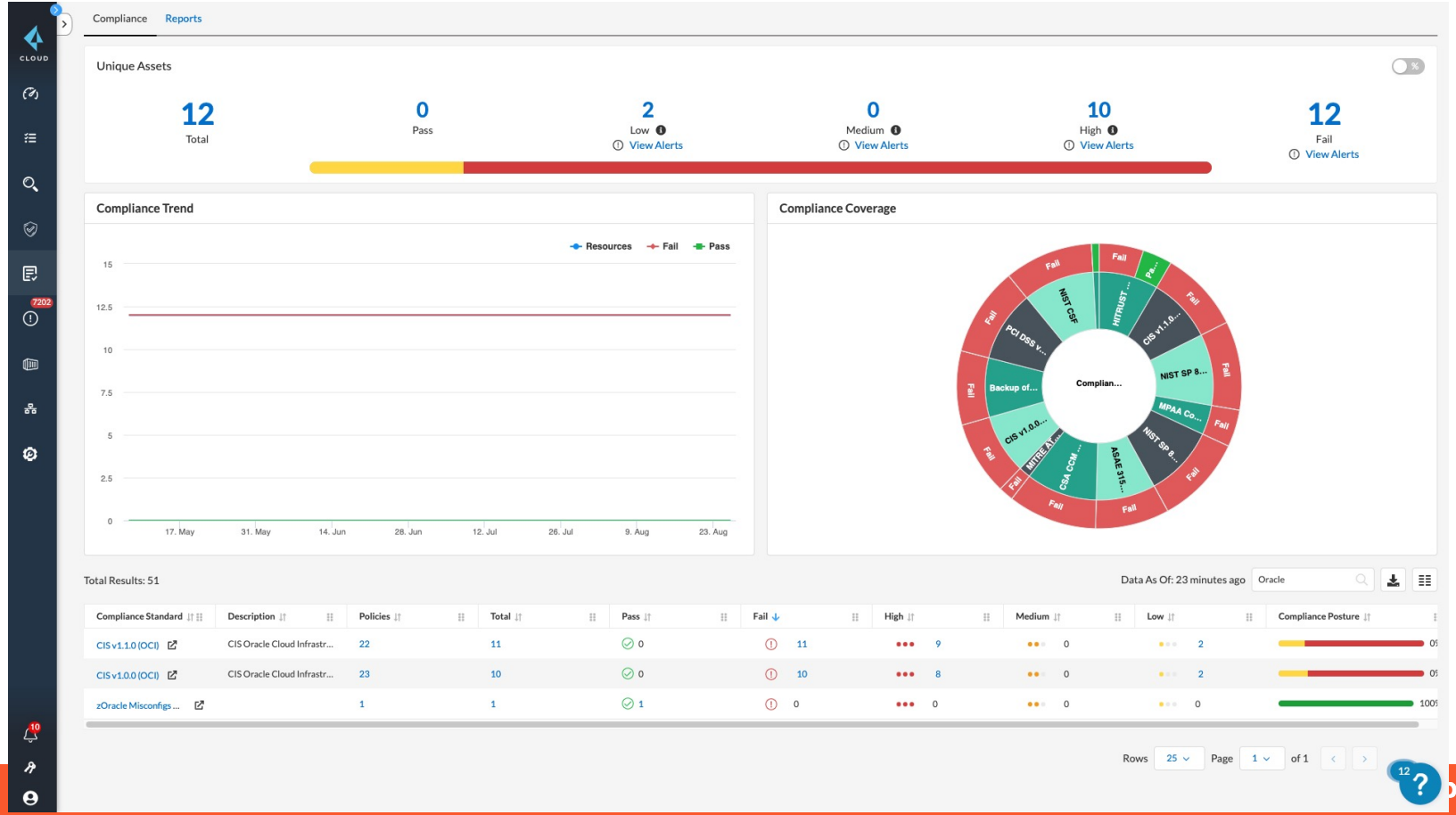
- Identity-Based Microsegmentation

Cloud Infrastructure Entitlement Management

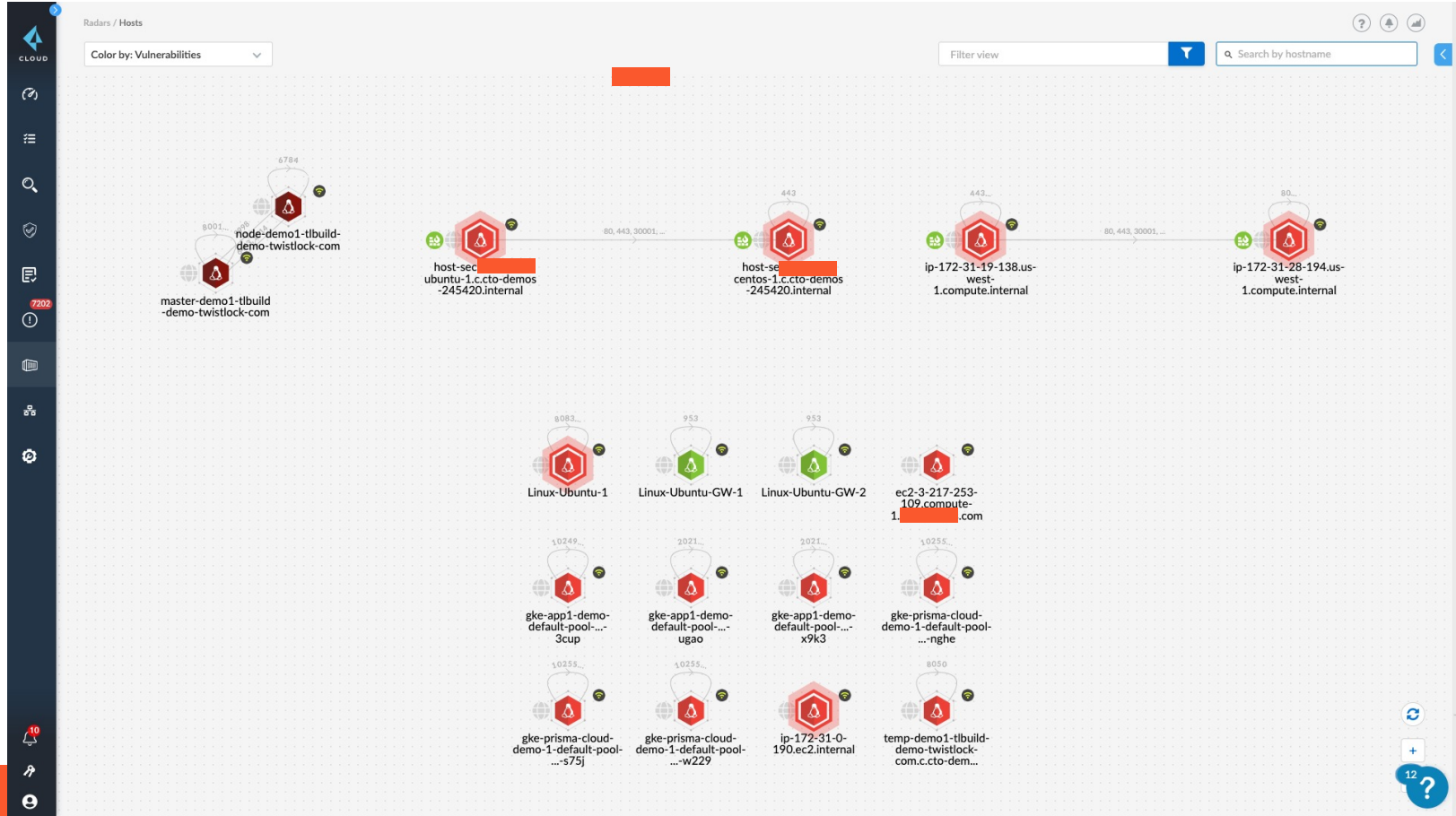
Enforce permissions and secure identities across workloads and clouds

- IAM Security

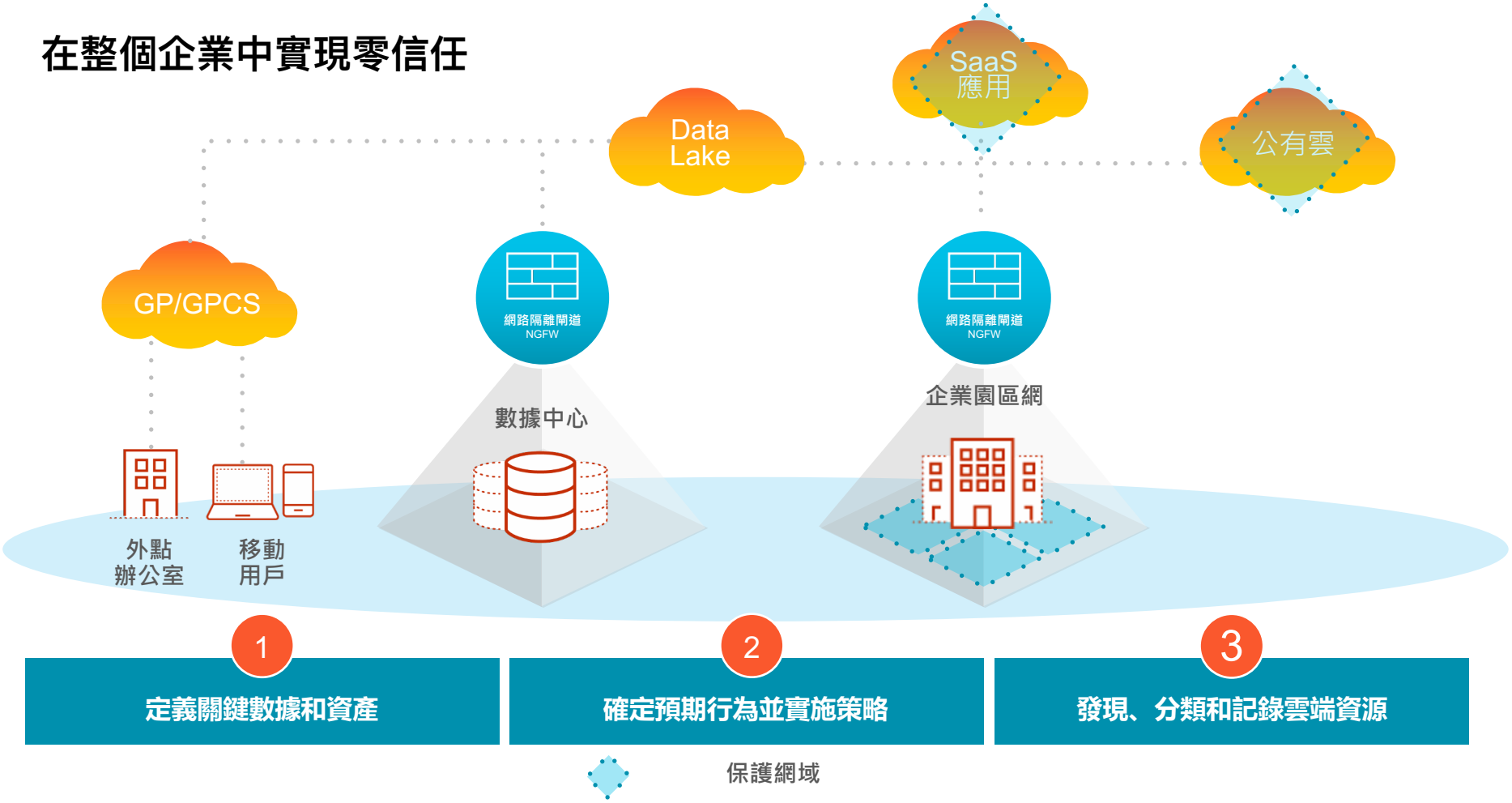
範例： Compliance



範例： Workload protection



在整個企業中實現零信任



1 **定義關鍵數據和資產**

2 **確定預期行為並實施策略**

3 **發現、分類和記錄雲端資源**

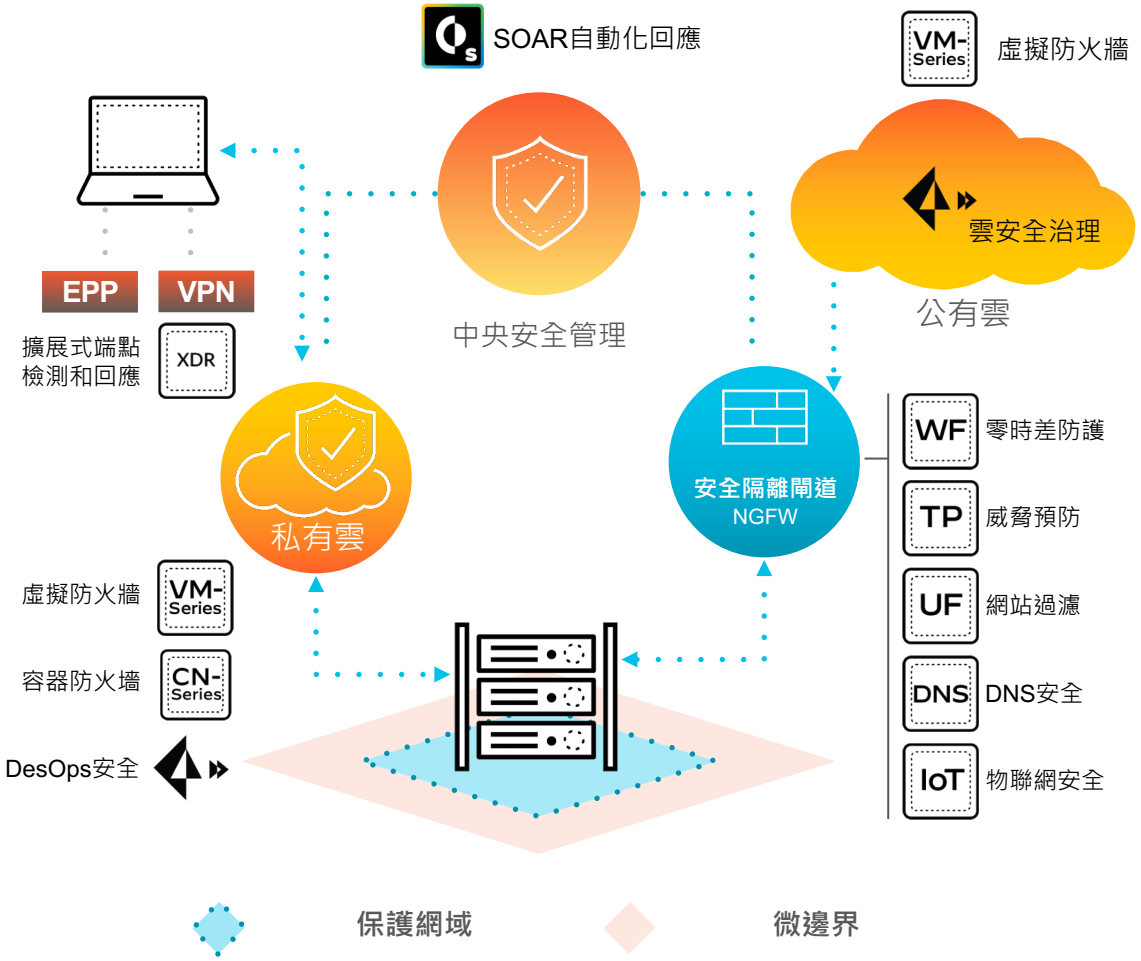
保護網域

零信任網路：由內而外的設計

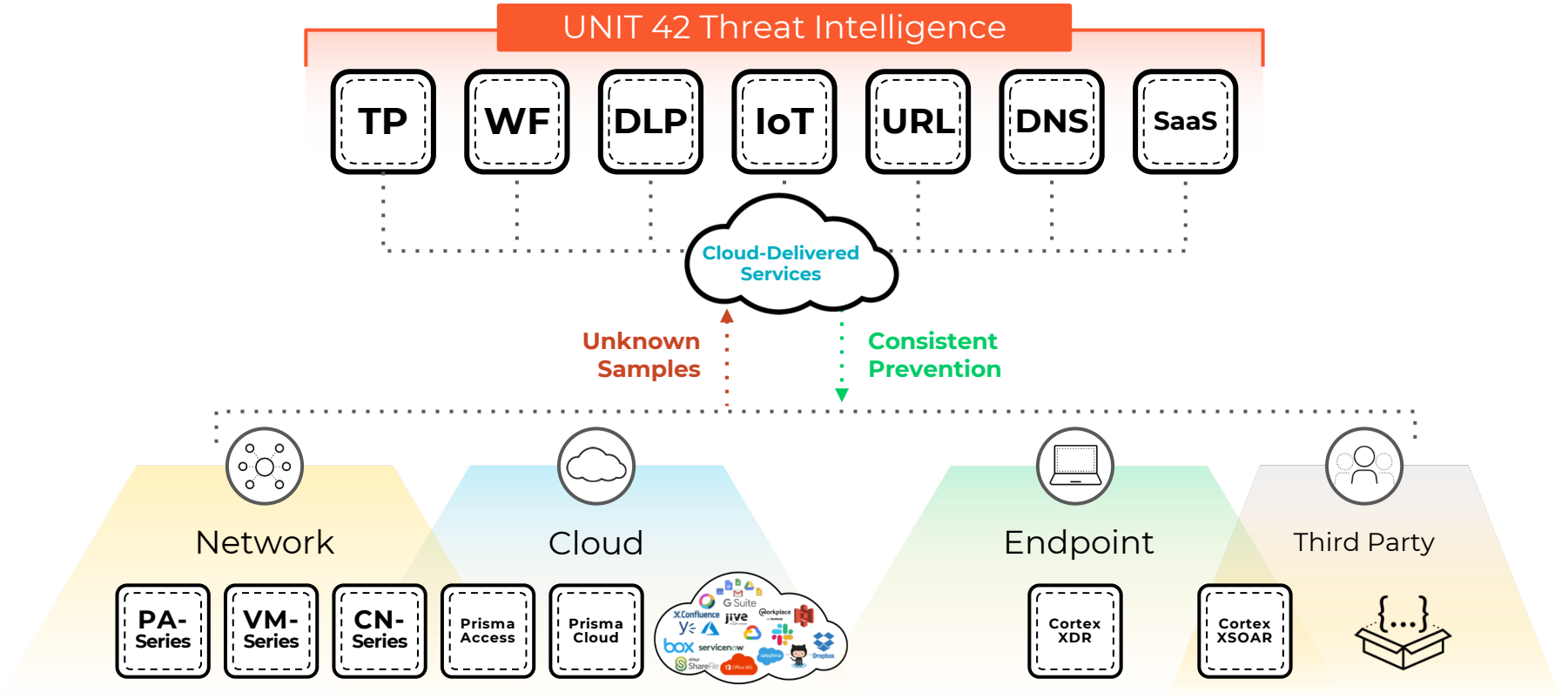
- 追蹤數據並隨時隨地對其進行保護。
- 通過分段閘道擴展一致策略
- 阻止跨網路、端點和雲的惡意程式與漏洞攻擊

零信任網路：由內而外的設計

- NGFW控制對各個安全網域存取
  - 中央安全管理提供任何位置的全局策略管理
  - 策略優化器可以幫助用戶自動創建零信任策略
- 通過安全訂閱服務防禦已知和未知威脅
- 阻止端點受到惡意軟體和漏洞攻擊
- 終端VPN將一致的安全管控策略擴展至遠端網路和移動用戶



Security Services: Best-of-breed with Platform Consistency



Thank you

paloaltonetworks.com

Nicholas Hsiao
nhsiao@paloaltonetworks.com