數位轉型的安全浪潮
以及零信任平台

詹鴻基 Jason
Palo Alto Networks 資安顧問

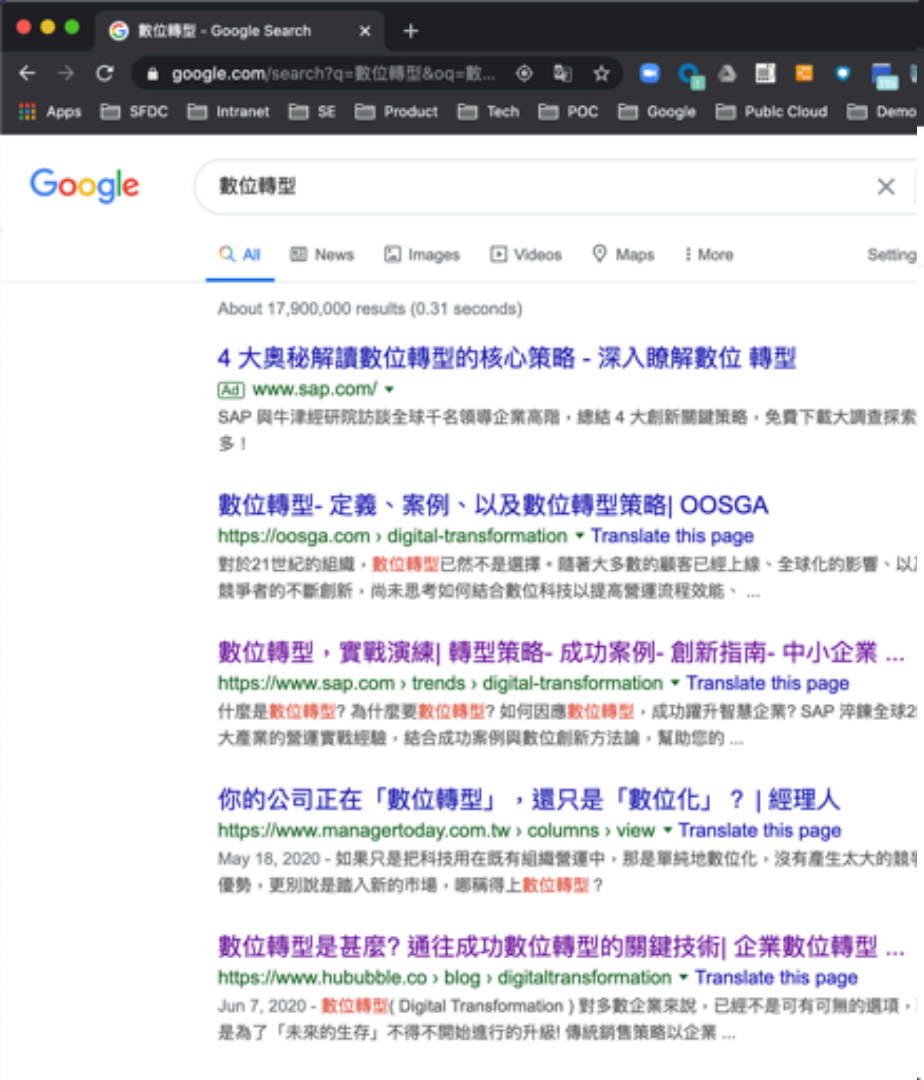
August 2020

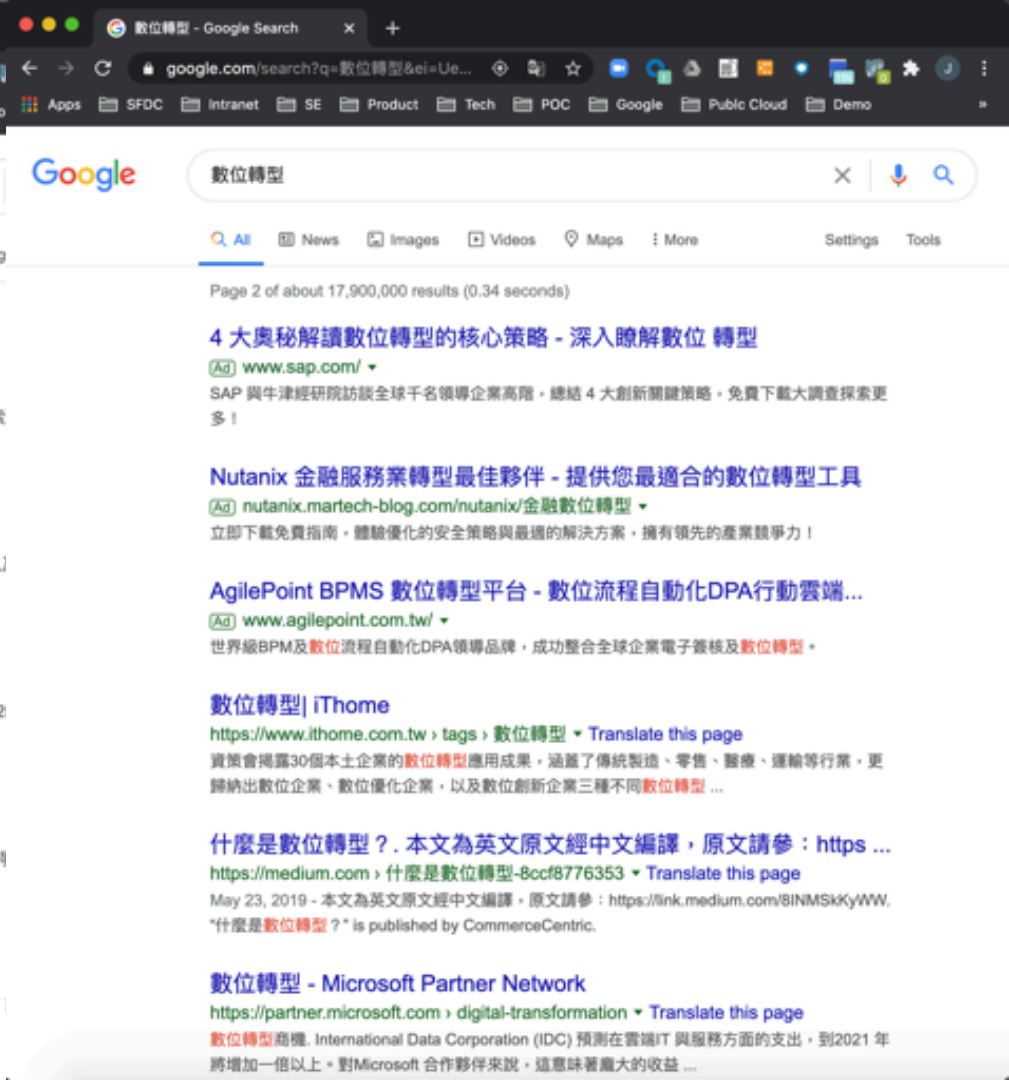
Agenda

- 數位轉型對於資訊安全的衝擊
- 後疫情時代工作模式改變的資安思維
- 零信任平台

數位轉型對於資訊安全的衝擊

paloalto NETWORKS


數位轉型 - Google Search
google.com/search?q=數位轉型&oq=數...
Apps SFDC Intranet SE Product Tech POC Google Public Cloud Demo
Google
數位轉型
All News Images Videos Maps More Setting
About 17,900,000 results (0.31 seconds)
4 大奧秘解讀數位轉型的核心策略 - 深入瞭解數位 轉型
Ad www.sap.com/
SAP 與牛津經研院訪談全球千名領導企業高階，總結 4 大創新關鍵策略，免費下載大調查探索
多！
數位轉型- 定義、案例、以及數位轉型策略| OOSGA
https://oosga.com › digital-transformation Translate this page
對於21世紀的組織，數位轉型已然不是選擇。隨著大多數的顧客已經上線、全球化的影響、以
競爭者的不斷創新，尚未思考如何結合數位科技以提高營運流程效能、 ...
數位轉型，實戰演練| 轉型策略- 成功案例- 創新指南- 中小企業 ...
https://www.sap.com › trends › digital-transformation Translate this page
什麼是數位轉型? 為什麼要數位轉型? 如何因應數位轉型，成功躍升智慧企業? SAP 淬鍊全球2
大產業的營運實戰經驗，結合成功案例與數位創新方法論，幫助您的 ...
你的公司正在「數位轉型」，還只是「數位化」？| 經理人
https://www.managertoday.com.tw › columns › view Translate this page
May 18, 2020 - 如果只是把科技用在既有組織營運中，那是單純地數位化，沒有產生太大的競
優勢，更別說是踏入新的市場，哪稱得上數位轉型？
數位轉型是甚麼? 通往成功數位轉型的關鍵技術| 企業數位轉型 ...
https://www.hububble.co › blog › digitaltransformation Translate this page
Jun 7, 2020 - 數位轉型(Digital Transformation) 對多數企業來說，已經不是可有可無的選項，
是為了「未來的生存」不得不開始進行的升級! 傳統銷售策略以企業 ...


數位轉型 - Google Search
google.com/search?q=數位轉型&ei=Ue...
Apps SFDC Intranet SE Product Tech POC Google Public Cloud Demo
Google
數位轉型
All News Images Videos Maps More Settings Tools
Page 2 of about 17,900,000 results (0.34 seconds)
4 大奧秘解讀數位轉型的核心策略 - 深入瞭解數位 轉型
Ad www.sap.com/
SAP 與牛津經研院訪談全球千名領導企業高階，總結 4 大創新關鍵策略，免費下載大調查探索更
多！
Nutanix 金融服務業轉型最佳夥伴 - 提供您最適合的數位轉型工具
Ad nutanix.martech-blog.com/nutanix/金融數位轉型
立即下載免費指南，體驗優化的安全策略與最適的解決方案，擁有領先的產業競爭力！
AgilePoint BPMS 數位轉型平台 - 數位流程自動化DPA行動雲端...
Ad www.agilepoint.com.tw/
世界級BPM及數位流程自動化DPA領導品牌，成功整合全球企業電子簽核及數位轉型。
數位轉型| iThome
https://www.ithome.com.tw › tags › 數位轉型 Translate this page
資策會揭露30個本土企業的數位轉型應用成果，涵蓋了傳統製造、零售、醫療、運輸等行業，更
歸納出數位企業、數位優化企業，以及數位創新企業三種不同數位轉型 ...
什麼是數位轉型？. 本文為英文原文經中文編譯，原文請參：https ...
https://medium.com › 什麼是數位轉型-8ccf8776353 Translate this page
May 23, 2019 - 本文為英文原文經中文編譯，原文請參：https://link.medium.com/8INMSkKyWW.
"什麼是數位轉型？" is published by CommerceCentric.
數位轉型 - Microsoft Partner Network
https://partner.microsoft.com › digital-transformation Translate this page
數位轉型商機. International Data Corporation (IDC) 預測在雲端IT 與服務方面的支出，到2021 年
將增加一倍以上。對Microsoft 合作夥伴來說，這意味著龐大的收益 ...

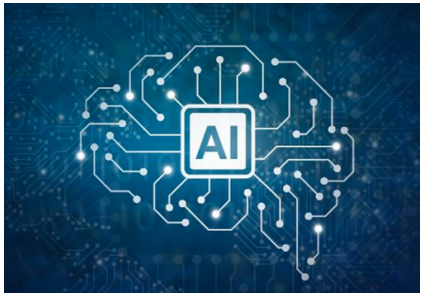
數位轉型是什麼

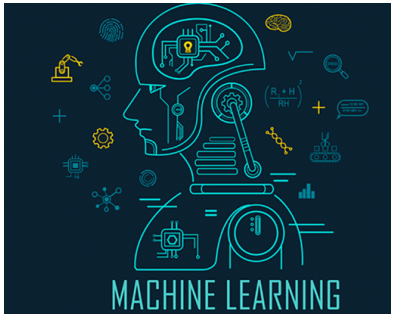
數位轉型下的資安思維

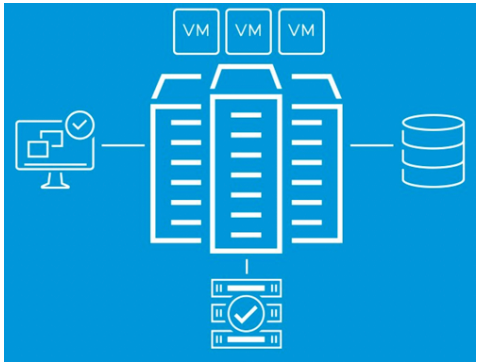
- 新興技術的使用與資訊安全的相對應
- 進階威脅攻擊持續發酵
- 已知問題但仍未做好準備

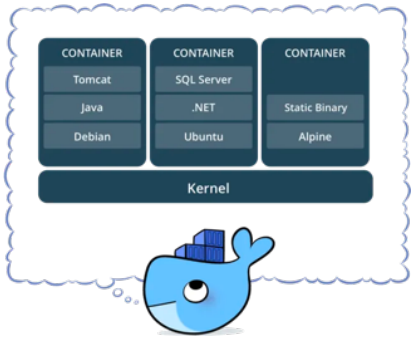
新興技術的使用與資訊安全期待

- Cloud
- Container
- AI/ML
- Hyperconverged



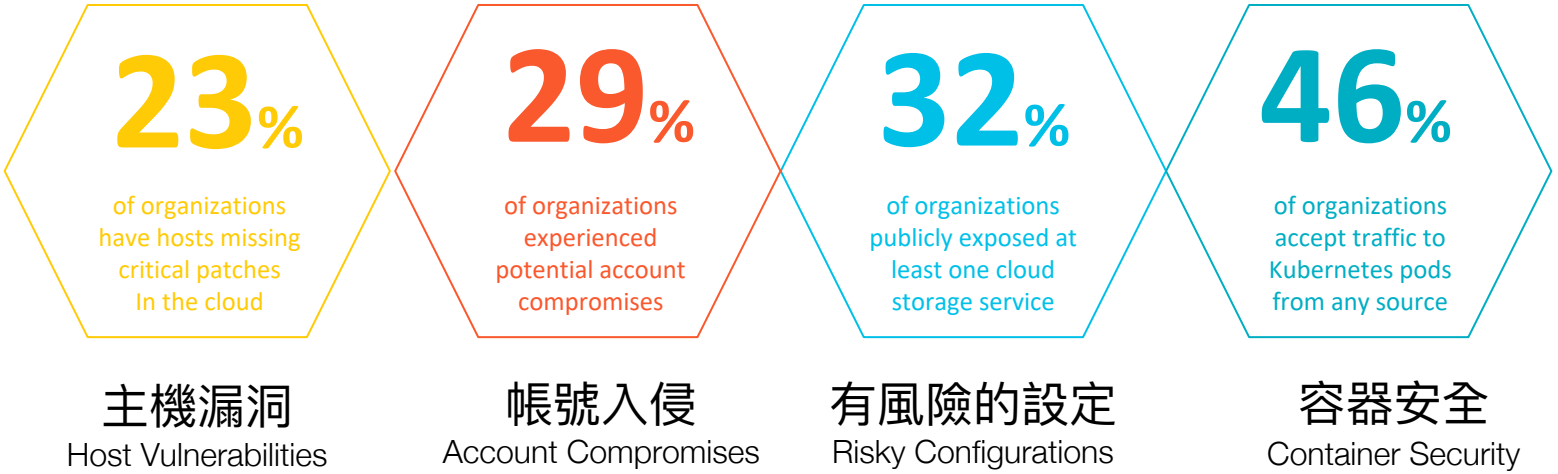






新興技術的使用與資訊安全期待

- 到2023年，有99%的雲端風險是由於客戶的設定導致錯誤



source: https://start.paloaltonetworks.com/5-key-cloud-security-trends

進階威脅攻擊持續發酵

- 2019年世界經濟論壇之全球風險報告指出可能性最高的十大風險中，「數據詐騙或數據盜竊」及「網路攻擊」排名高居第四及第五，前三項都是自然天候相關。
- PwC「2018 年全球經濟犯罪調查」結果顯示，惡意軟體攻擊(46%)成為臺灣企業最常遇見 之威脅，遠高於全球(36%)及亞太區(33%)之統計結果。而網路釣魚攻擊穩居 第二，其對企業的威脅不容小覷。
- 這幾個月台灣的重大資安事件層出不窮，影響範圍及金額相比過去只增不減

進階威脅攻擊持續發酵

國際 最新

駭入Garmin勒索千萬美金　俄羅斯駭客奢華生活遭起底

編輯：廖梓翔 | 2020-07-27 15:47

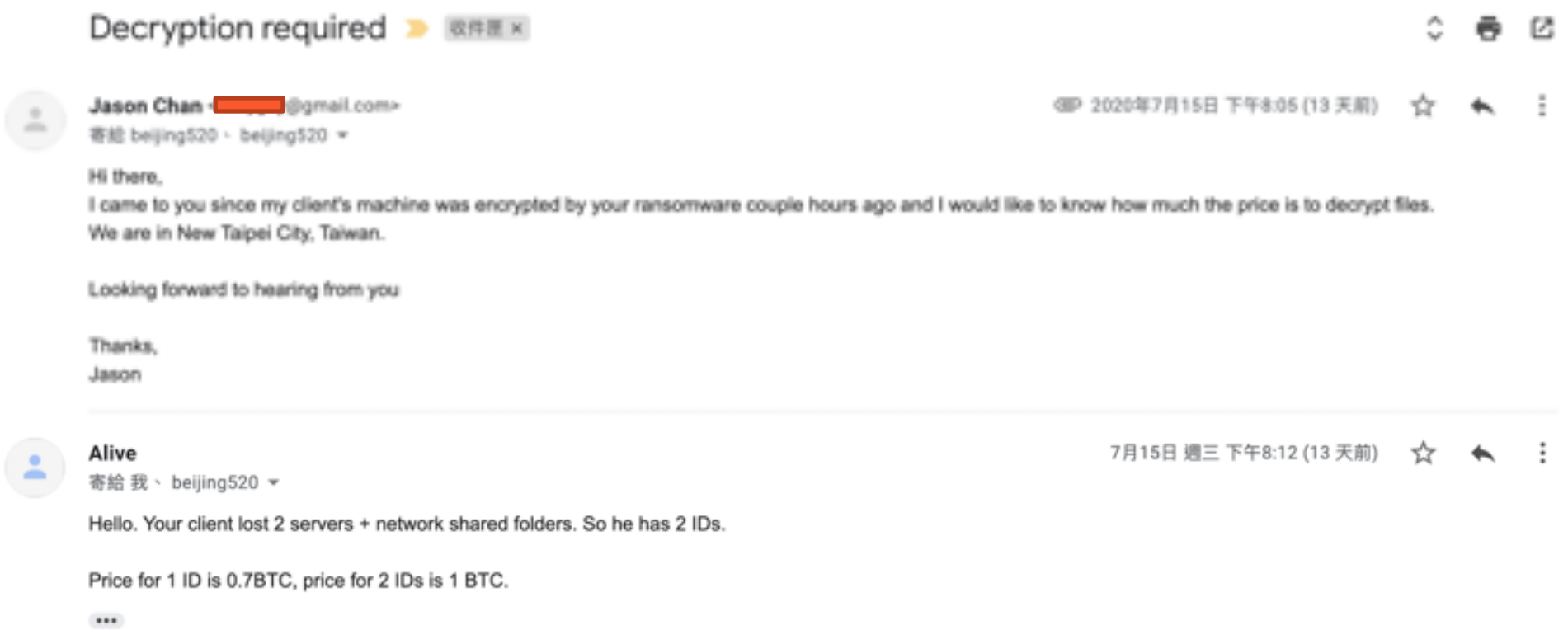
Garmin | 駭客 | 勒索病毒 | Evil Corps | Maksim Yakubets

LINE

Next

此次Garmin遭駭背後的原兇，據悉是俄羅斯駭客組織Evil Corps所為，圖為Evil Corps負責人雅庫貝塔斯遭FBI通緝圖樣。（圖／翻攝自FBI）

Case Sharing - 北京520



Decryption required 收件匣 ×

Jason Chan <[redacted]@gmail.com> 2020年7月15日 下午8:05 (13 天前)

寄給 beijing520、beijing520

Hi there,
I came to you since my client's machine was encrypted by your ransomware couple hours ago and I would like to know how much the price is to decrypt files.
We are in New Taipei City, Taiwan.

Looking forward to hearing from you

Thanks,
Jason

Alive 7月15日 週三 下午8:12 (13 天前)

寄給 我、beijing520

Hello. Your client lost 2 servers + network shared folders. So he has 2 IDs.

Price for 1 ID is 0.7BTC, price for 2 IDs is 1 BTC.

已知問題但仍未做好準備

- 企業要維持競爭優勢，防範各種來自內外部的威脅則是成功轉型不可或缺的先決要件。
- PwC「2018 全球資訊安全調查報告」指出，全球有 44%企 業沒有完整資安策略、48%缺乏員工資安意識訓練計畫，及 54%缺乏事故反 應流程。雖然網路攻擊非常嚴重，但PwC 「2018 年全球經濟犯罪調查」結果 指出，36%的臺灣企業不認為它們會成為網路攻擊的目標，或不知道是否成為網路攻擊的目標。

資訊安全團隊面臨的狀況

Ale

日益增加 調查
員無法等 數

帶風向 >>>>> 查證 = 浪費時間

什麼是 SOAR？

Security (安全)、**O**rchestration (協調)、**A**utomation (自動化) 和 **R**esponse (回應)

Orchestration (協調)

劇本、執行手冊、工作流程

合理組織動作的計劃

從中央位置控制、啟動安全產品堆疊

Automation (自動化)

自動化指令碼

可擴充的產品整合

機器執行劇本任務

Response (回應)

案例管理

分析和報告

溝通和協作

Cortex XSOAR

是工作流程自動引擎

Respond to incidents with speed and scale

- **100s** of product integrations
- **1000s** of security actions
- Intuitive, **visual playbook editor**

範例：釣魚信件回應方式

問題：釣魚信件攻擊

大量警示

網路釣魚攻擊頻繁且容易執行，常常是安全攻擊的最常被使用的破口之一

耗時曠日的過程

資安團隊必須從郵件系統，防火牆等不同的工具來調查或是處理釣魚信件的威脅攻擊

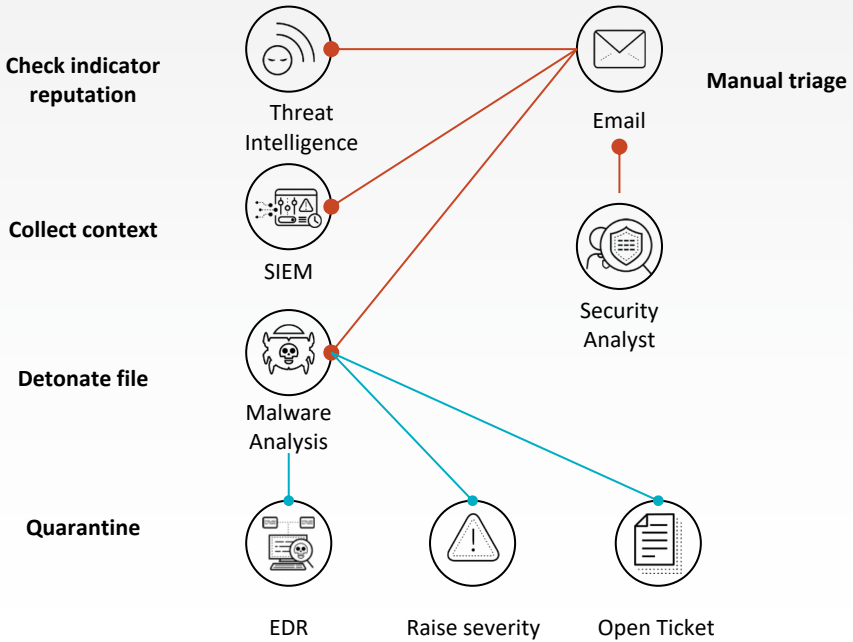
一直出現，不斷增長

95% 的針對企業攻擊手法很多都是魚叉式網路釣魚(spear phishing)[1]

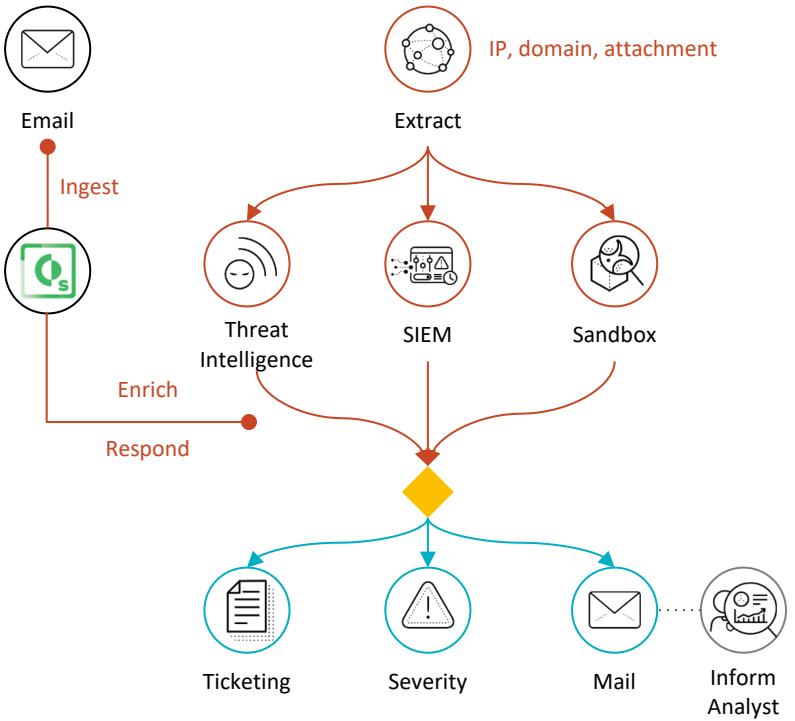
[1]Source: https://www.networkworld.com/article/2164139/network-security/how-to-blunt-spear-phishing-attacks.html

我們的方法：網路釣魚回應

Before



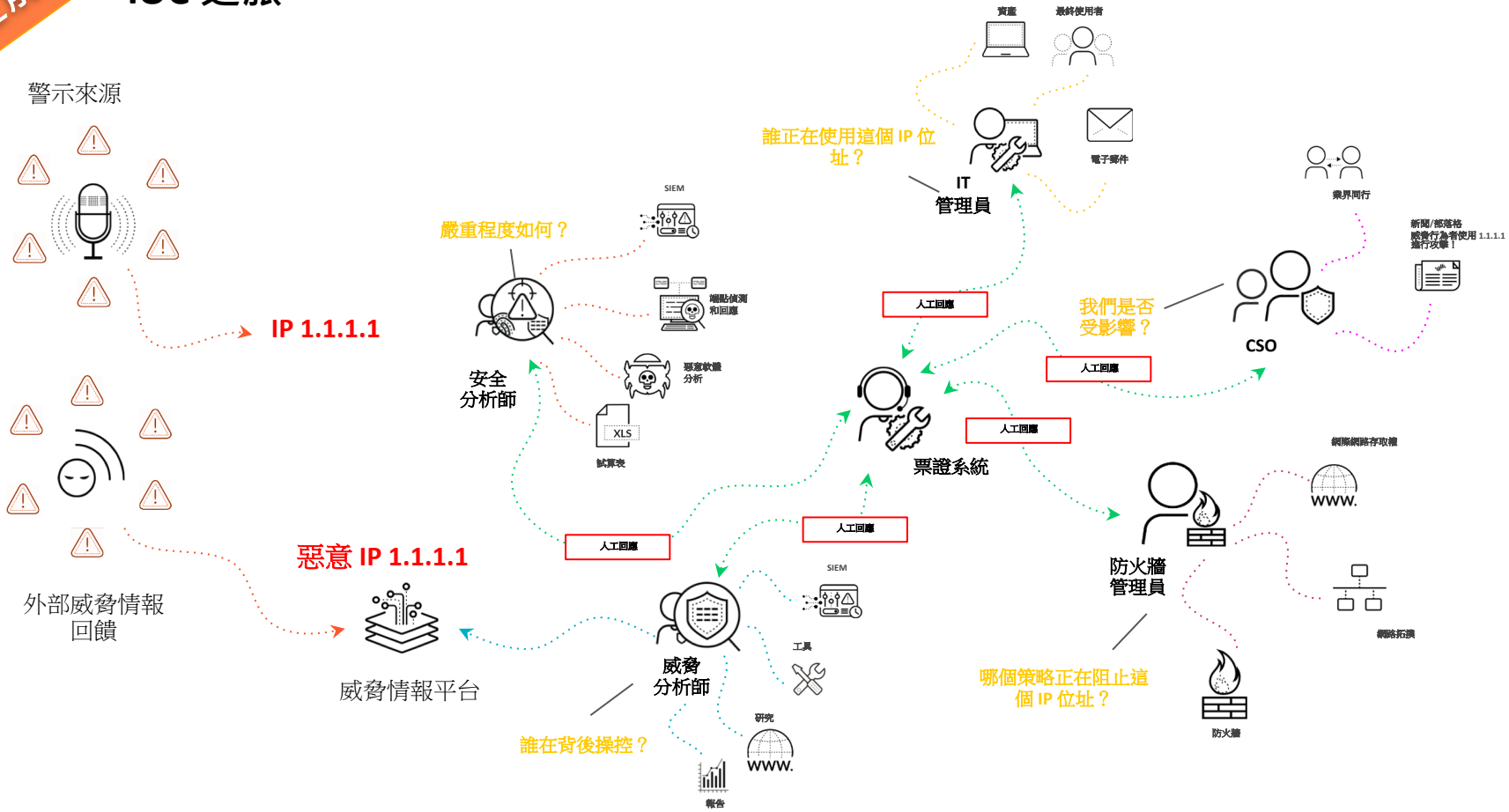
After



範例：IOC查找

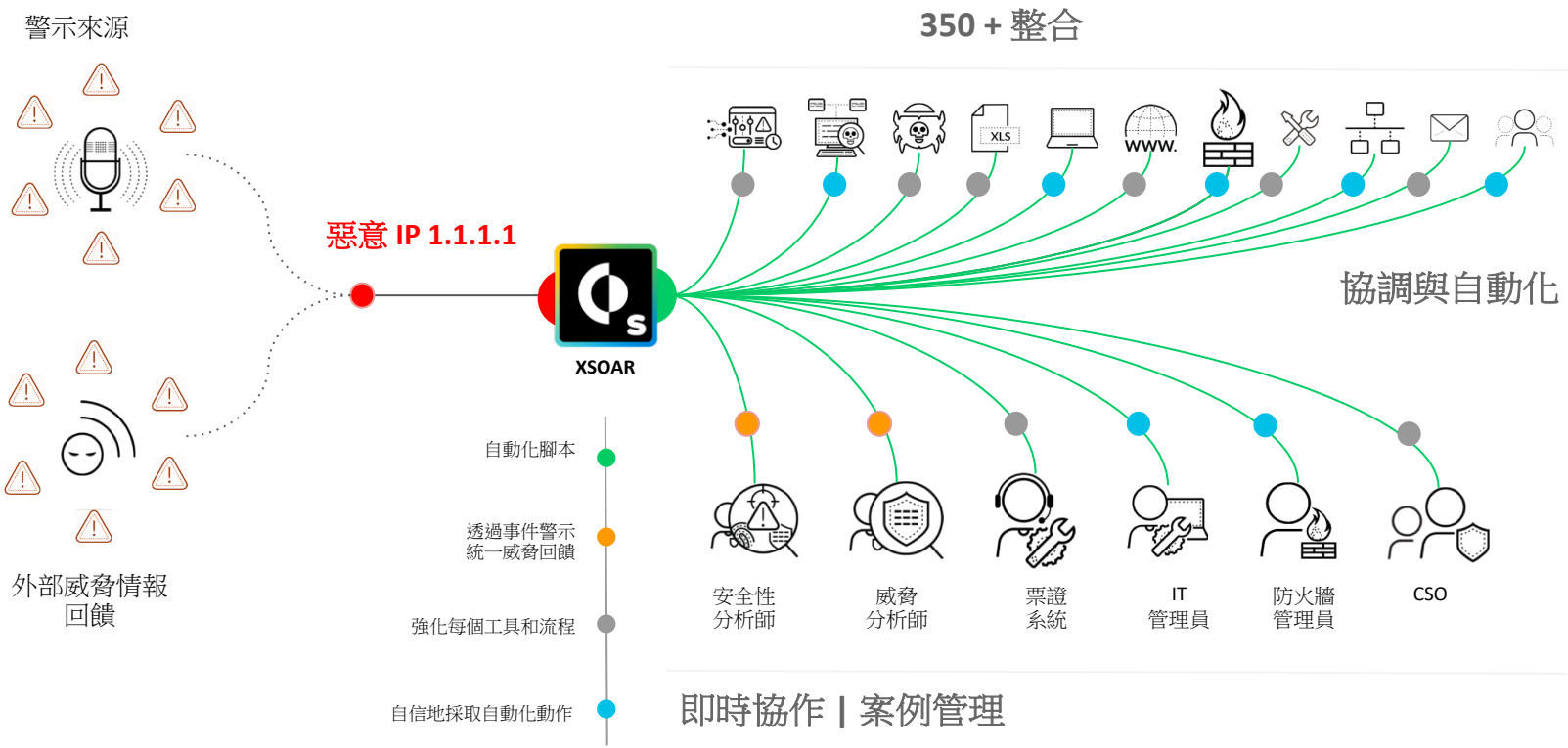
之前

IOC 之旅


警示來源
IP 1.1.1.1
外部威脅情報
回饋
惡意 IP 1.1.1.1
威脅情報平台
嚴重程度如何？
SIEM
端點偵測
和回應
惡意軟體
分析
XLS
試算表
安全
分析師
人工回應
誰正在使用這個 IP 位
址？
資產
最終使用者
電子郵件
IT
管理員
我們是否
受影響？
CSO
業界同行
新聞/部落格
感覺行為者使用 1.1.1.1
進行攻擊！
票證系統
人工回應
人工回應
人工回應
人工回應
防火牆
管理員
網際網路存取權
WWW.
網路拓撲
哪個策略正在阻止這
個 IP 位址？
防火牆
威脅
分析師
SIEM
工具
研究
WWW.
報告
誰在背後操控？

之後

使用 Cortex XSOAR 展開 IOC 之旅



後疫情時代工作模式改變的資安思維

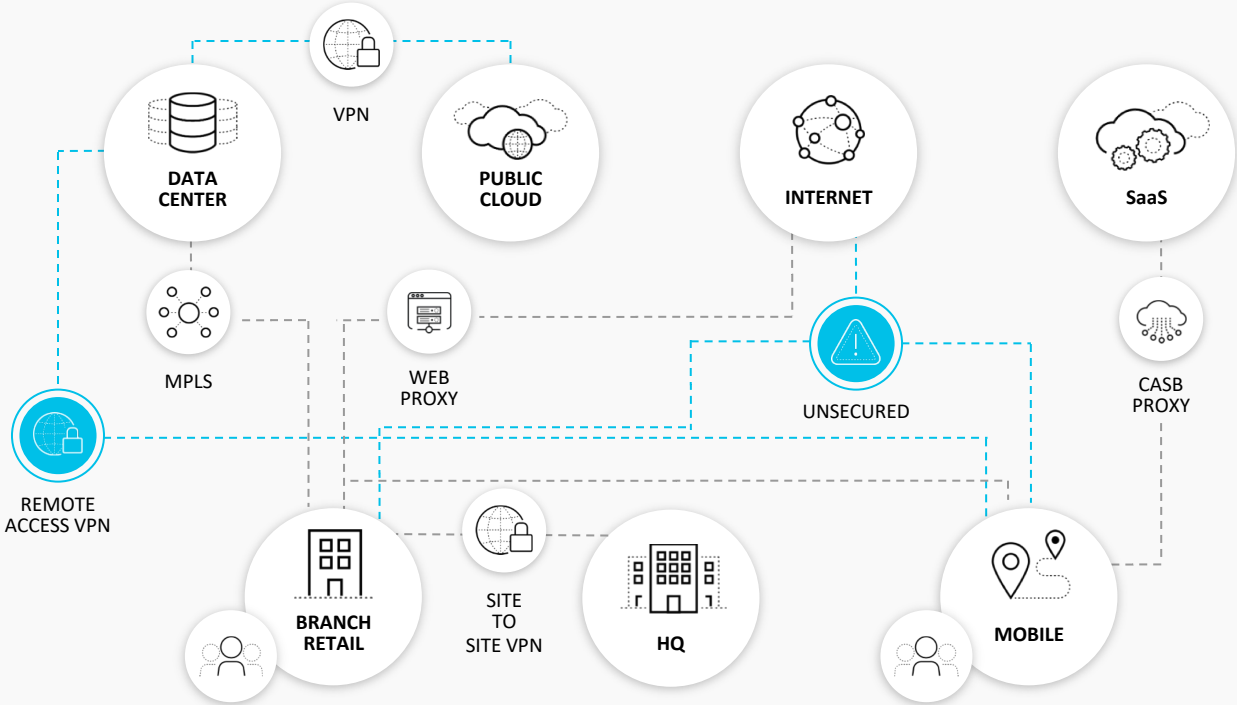
SASE - Secure Access Service Edge

- 2019 年 Gartner 全新定義最新的 SASE (Secure Access Service Edge) 市場，根據現今企業對於網路與資安的需求，需要對企業進行『架構轉型 (Architecture transformation)』

- Gartner 根據現今數位企業 (Digital Business) 的需求，結合企業所需的四個面向來分析，這四個面向分別是身份辨識需求(Identity-Driven)、原生型網路平台(Cloud Native)、全球化分散式佈署 (Globally Distributed)及支援行動用戶 (Supports All Edges)。

- Gartner預計到2024年至少40%的企業將有明確的策略採用SASE，高於2018年底的不到1%。” SASE體系結構可識別用戶和設備，應用基於策略的安全性，並提供對相應應用程序或數據的安全訪問。無論使用者，應用程式或設備位於何處，該方法都可以使組織應用安全訪問。

現今的雲端存取安全解決方案相對複雜



1 複雜

2 使用者體驗較為不佳

3 資安空窗期

商業導向正在推動改變

採用雲端

94% of businesses
the cloud

2019 State of the Cloud Report

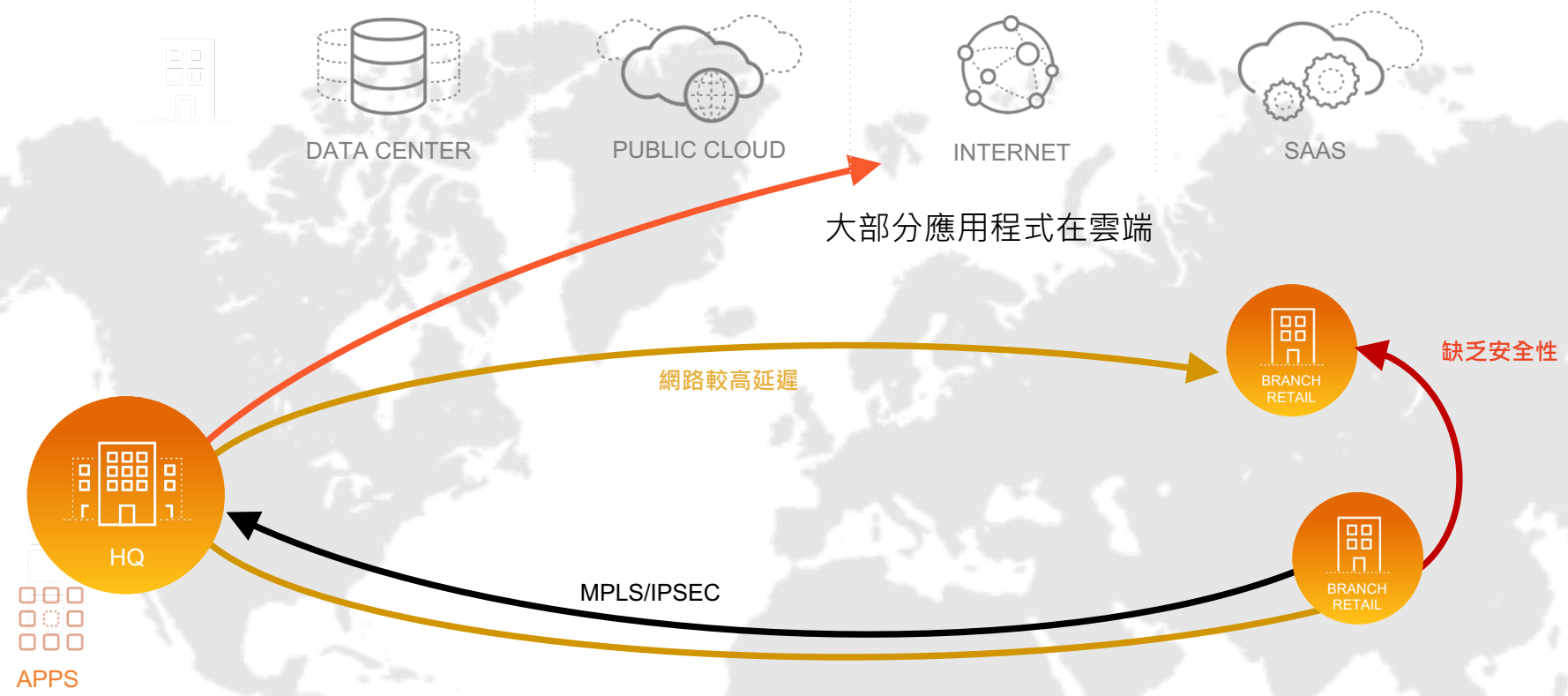
WAN的轉型

60% of enterprises will have
mplemented SD-WAN

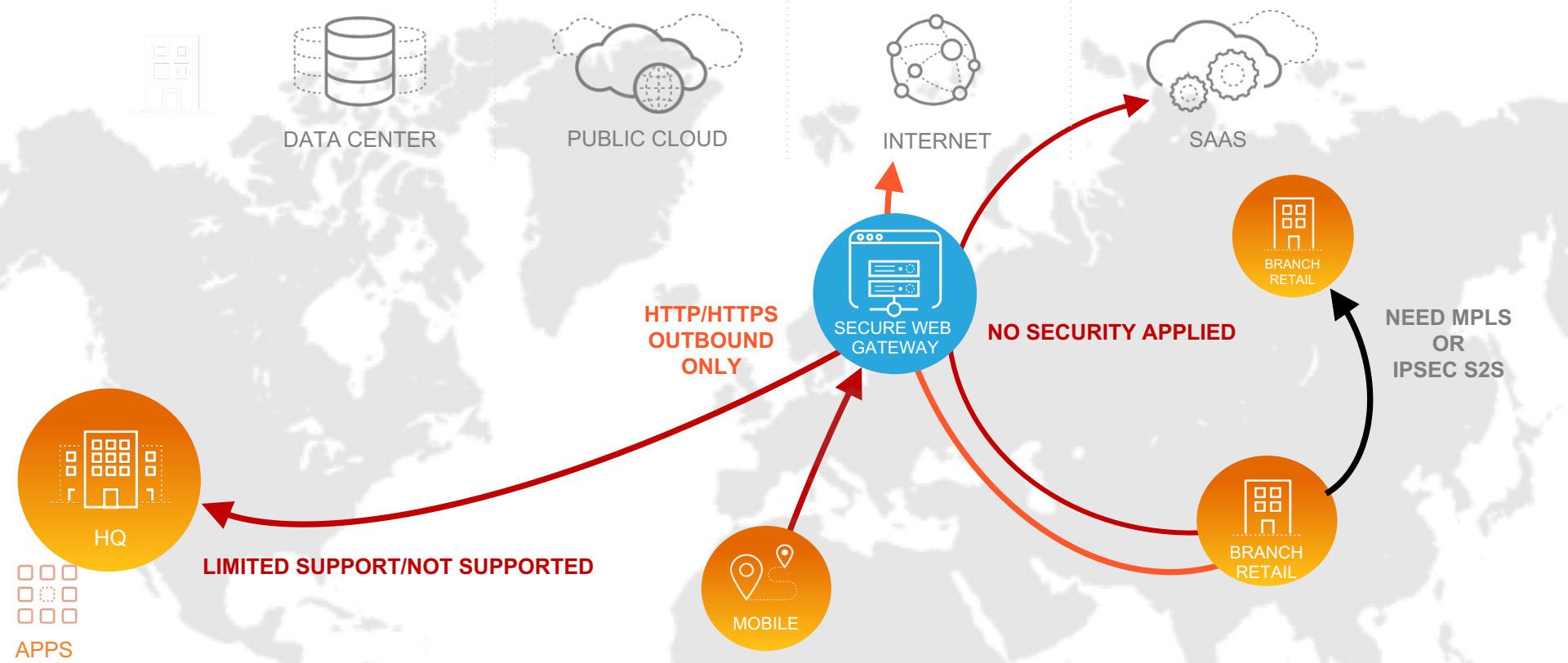
rtner Magic Quadrant for WAN Edge
Infrastructure

在家上班 WFH (Work From Home)

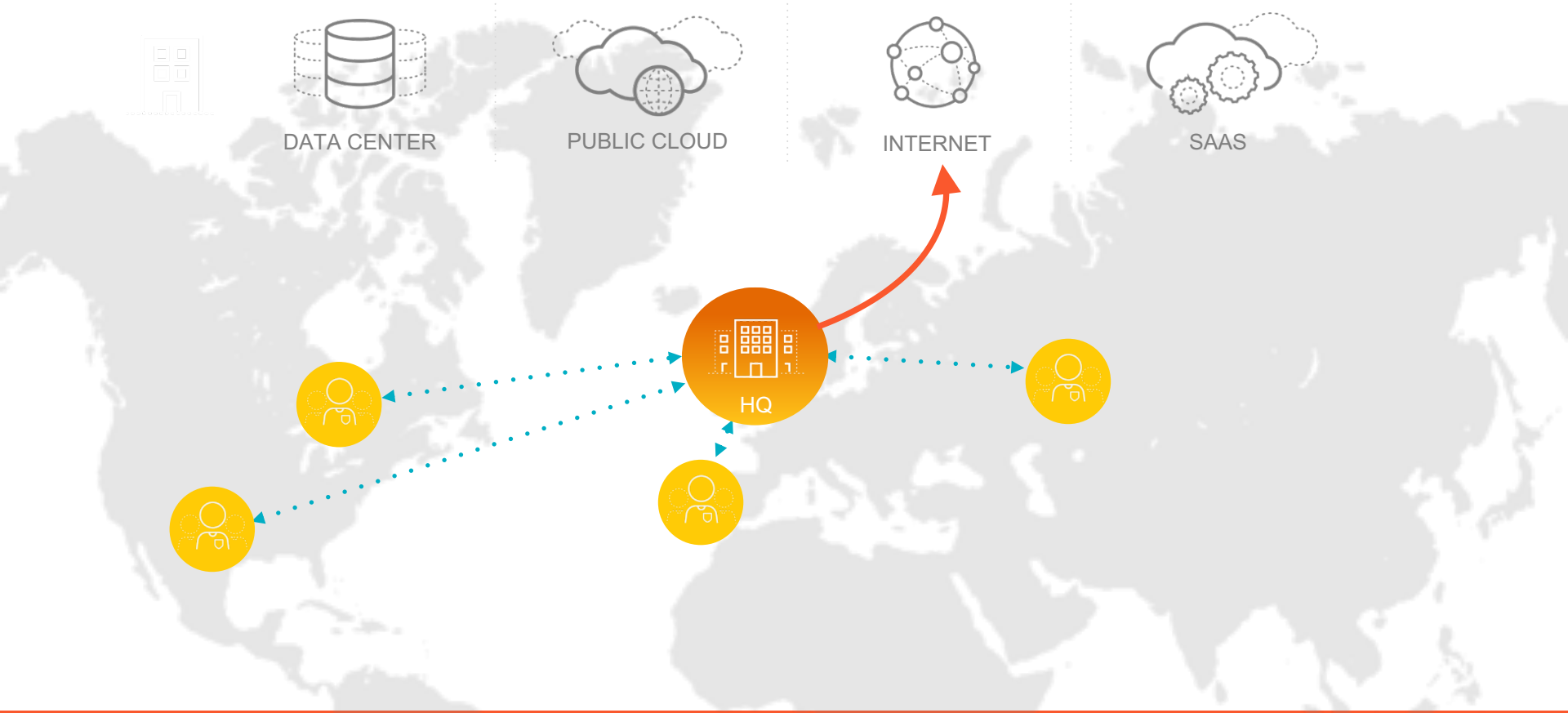
傳統分點網路架構


DATA CENTER
PUBLIC CLOUD
INTERNET
SAAS
大部分應用程式在雲端
網路較高延遲
缺乏安全性
BRANCH RETAIL
BRANCH RETAIL
HQ
MPLS/IPSEC
APPS

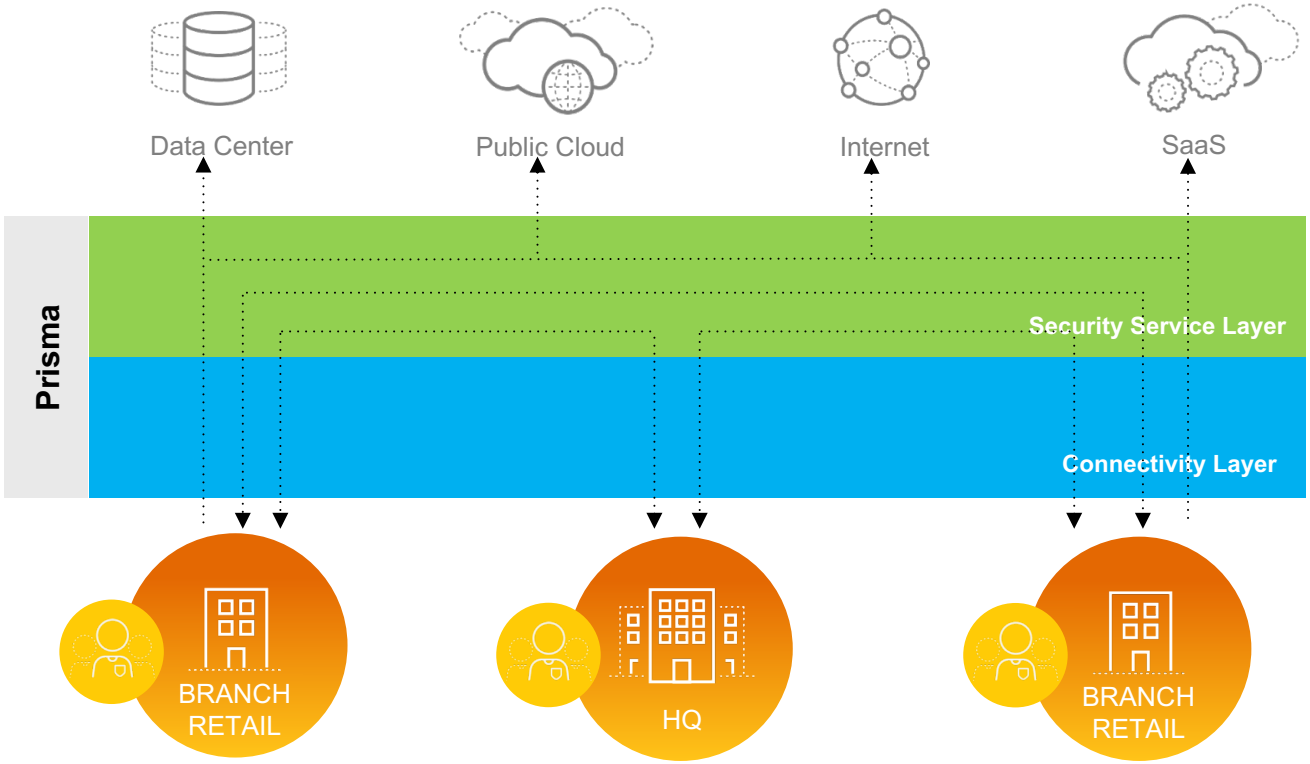
傳統分點網路架構 (SWG)



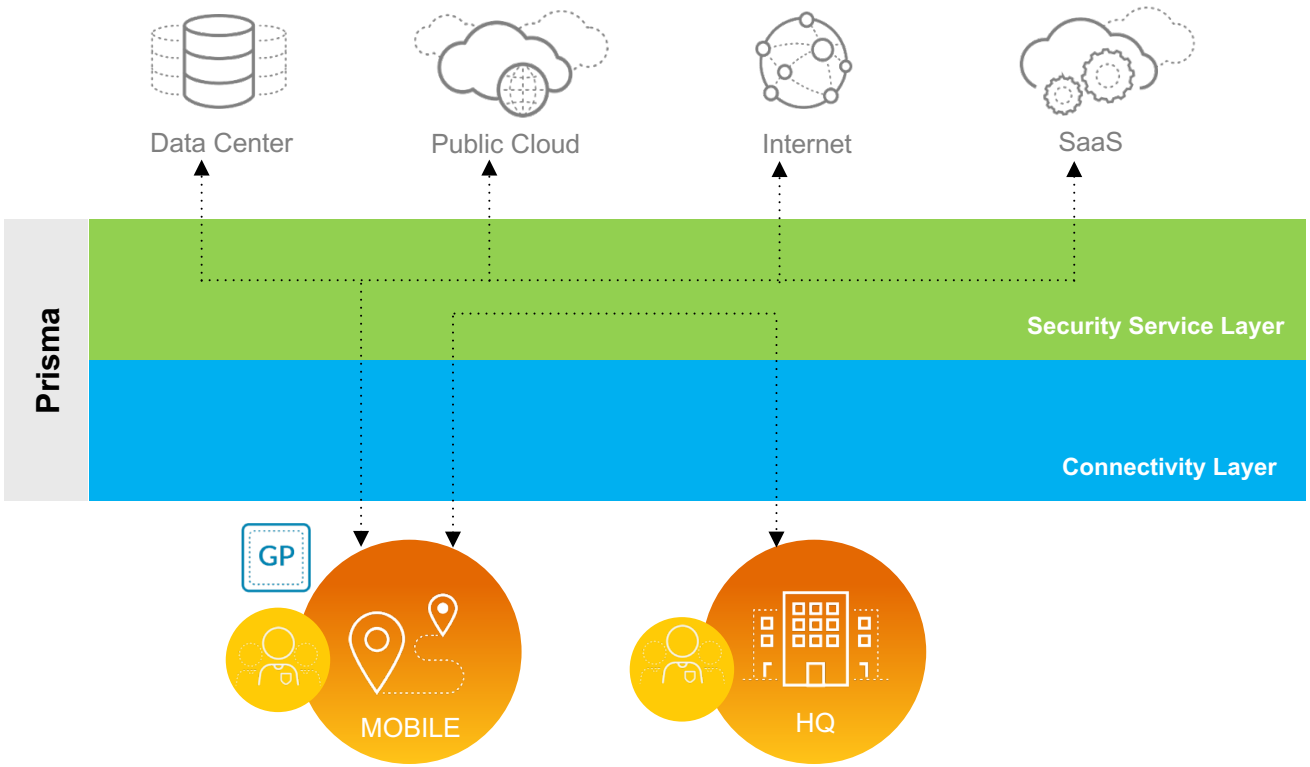
傳統遠端使用者架構



分點辦公室



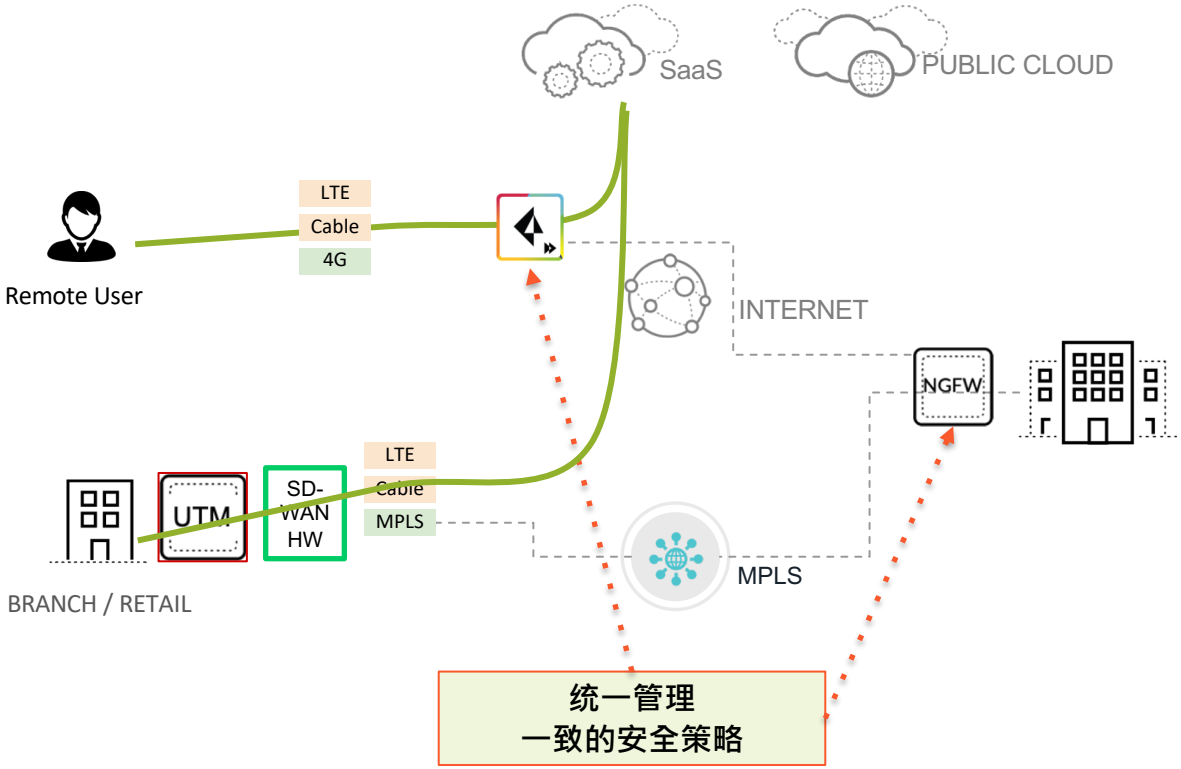
移動使用者安全存取



全球超過 100個節點覆蓋，支援彈性與動態部署

Europe Region		North America Region	South America Region	ANZ Region	Asia Region
Andorra	Luxembourg	Canada Central	Argentina	Australia East	Bangladesh
Austria	Moldova	Canada East	Bolivia	Australia South	Cambodia
Belarus	Monaco	Canada West	Brazil Central	Australia Southeast	Hong Kong
Belgium	Netherlands Central	Costa Rica	Brazil East	New Zealand	India North
Bulgaria	Netherlands South	Mexico Central	Brazil South	**Middle East Region**	India South
Croatia	Norway	Mexico West	Chile	Egypt	India West
Czech Republic	Poland	Panama	Columbia	Israel	Indonesia
Denmark	Portugal	US Central	Ecuador	Jordan	Malaysia
Finland	Romania	US East	Paraguay	Kuwait	Myanmar
France North	Russia Central	US Northeast	Peru	Saudi Arabia	Pakistan South
France South	Russia Northwest	US Northwest	Venezuela	Turkey	Pakistan West
Germany Central	Slovakia	US South	**Africa Region**	United Arab Emirates	Papua New Guinea
Germany North	Slovenia	US Southeast	Kenya	**Japan Region**	Philippines
Germany South	Spain Central	US Southwest	Nigeria	Japan Central	Singapore
Greece	Spain East	US West	South Africa Central	Japan South	South Korea
Hungary	Sweden		South Africa West		Taiwan
Ireland	Switzerland				Thailand
Italy	UK				Vietnam
Liechtenstein	Ukraine				
Lithuania	Uzbekistan				

量身打造的分行與移動使用者安全存取邊際服務



FWaaS 防火牆即服務

Prisma™ Access，雲端防火牆服務，通過Palo Alto Networks全套NGFW安全功能保護分點或移動使用者免受威脅

零信任網路安全

對所有應用程序實施基於安全上下文（上下文）的訪問，並對所有應用程序和服務實施一致的可見性和安全策略

VPN

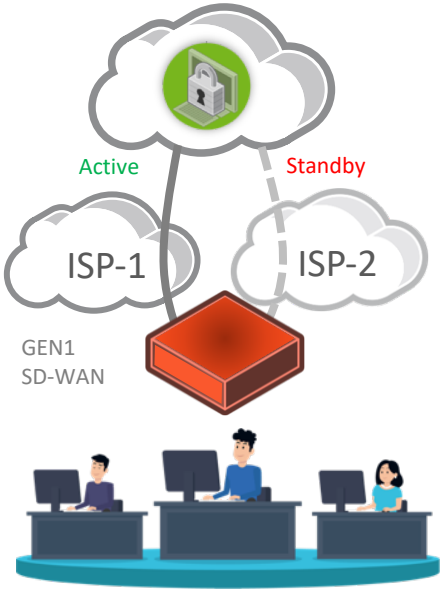
通過Prisma™Access全全網狀VPN連接移動端使用者和分點機構，並消除VPN站點到站點的複雜性

SD-WAN

將Palo Alto Networks防火牆利用SD-WAN邊緣設備，並在用戶網路環境中安全地部署SD-WAN

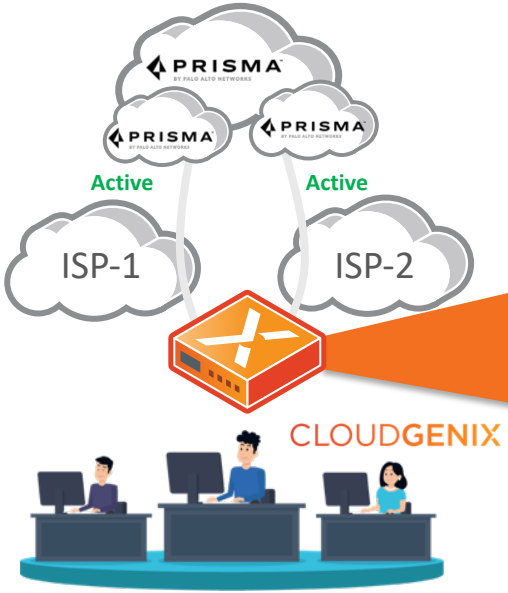
CloudGenix 新一代SD-WAN

Gen-1 SD-WAN

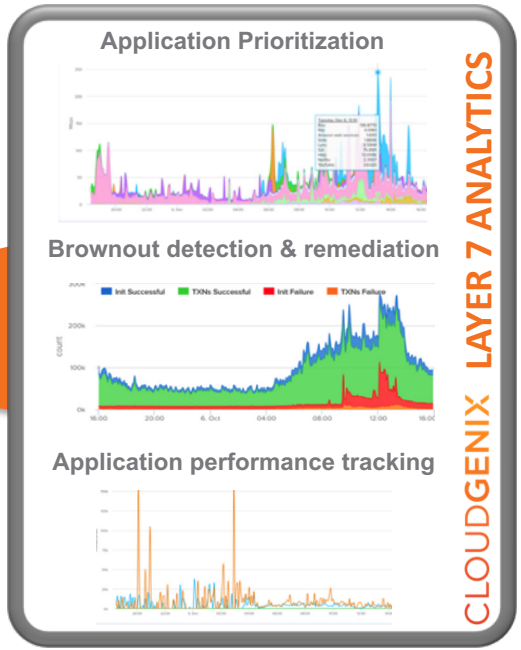


缺少智慧負載平衡
缺少網路可視性
缺少路徑檢測及修復
多個設備維運成本較高

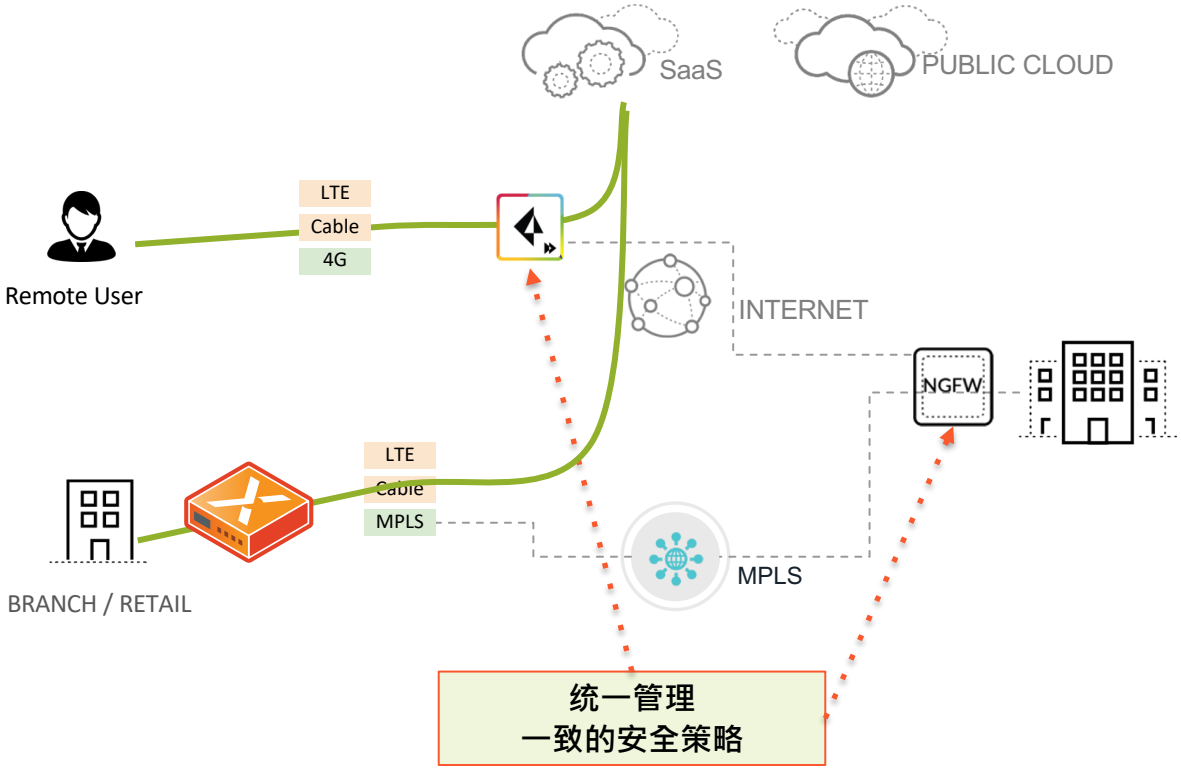
CLOUDGENIX



智能Active-Active 負載平衡
Layer 7 效能追蹤
路徑檢測及修復
無中斷第七L7切換
一鍵整合 Prisma Access



量身打造的分行與移動使用者安全存取邊際服務



FWaaS 防火牆即服務

Prisma™ Access，雲端防火牆服務，通過Palo Alto Networks全套NGFW安全功能保護分點或移動使用者免受威脅

零信任網路安全

對所有應用程序實施基於安全上下文（上下文）的訪問，並對所有應用程序和服務實施一致的可見性和安全策略

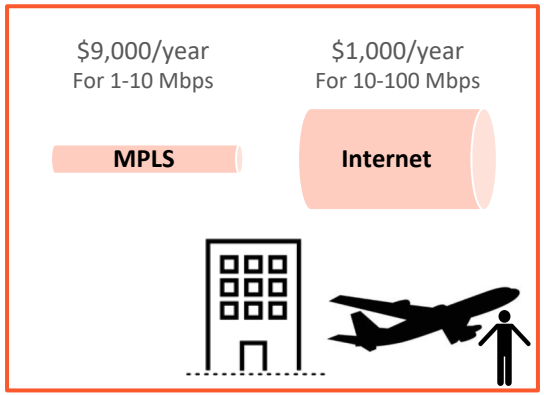
VPN

通過Prisma™Access全全網狀VPN連接移動端使用者和分點機構，並消除VPN站點到站點的複雜性

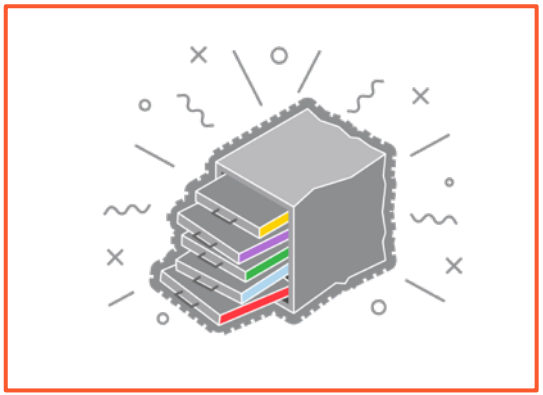
SD-WAN

將Palo Alto Networks防火牆利用SD-WAN邊緣設備，並在用戶網路環境中安全地部署SD-WAN

實質帶來效益



節省成本



降低維運複雜度

提升雲端服務使用

範例：疫情助力監控

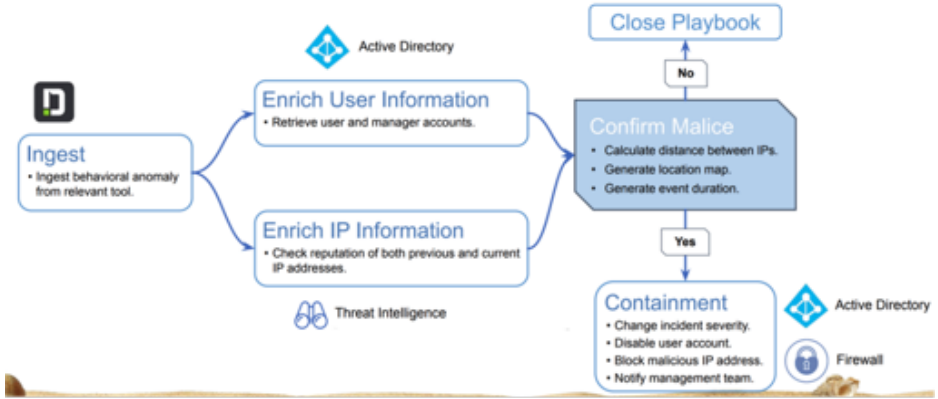
XSOAR協助疫情監控自動化

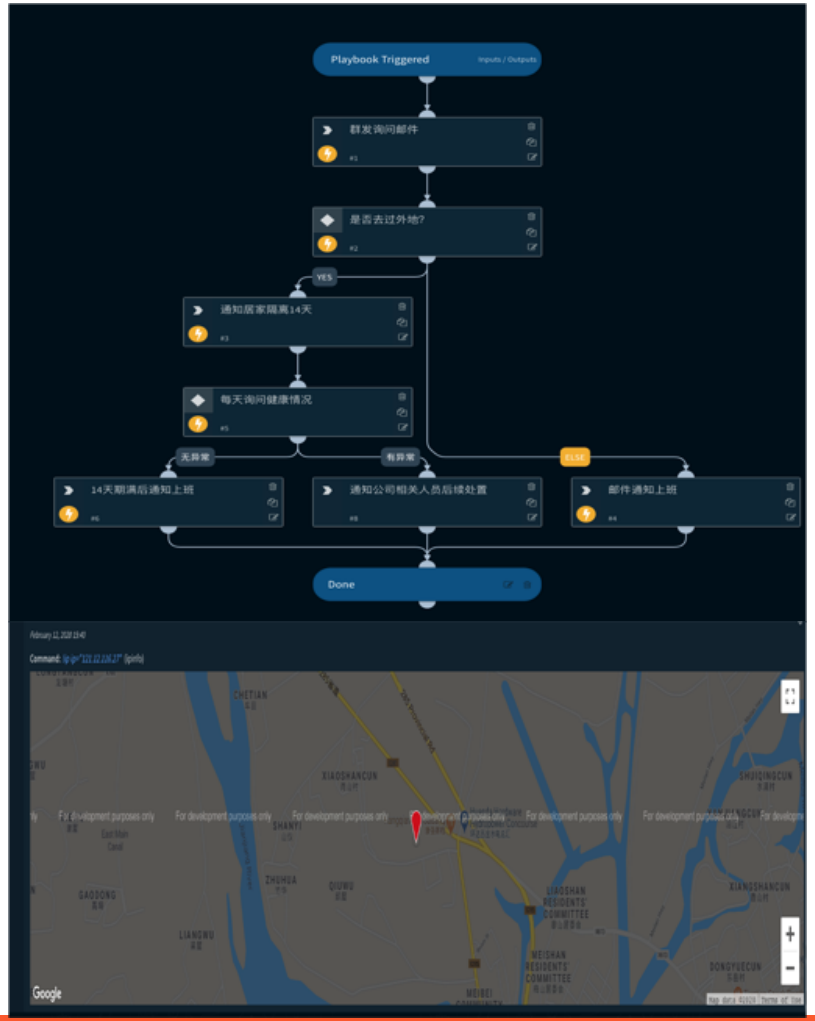
員工在家隔離監控

- 廣播信件通知
- 接收員工回覆
- 通知隔離與否
- 狀況回報
- 隔離期滿通知上班
- 地圖定位遠端辦公位置（VPN）

遠端(在家)辦公的安全威脅

- 使用VPN遠端辦公，帶來了安全威脅。若發現”不可能的旅行者”便第一時間阻斷IP並封鎖帳號





XSOAR使用者自助服務自動化

使用者遠端申請後，透過Playbook收集資訊做出判斷，自動回覆使用者，無需IT管理人員介入。

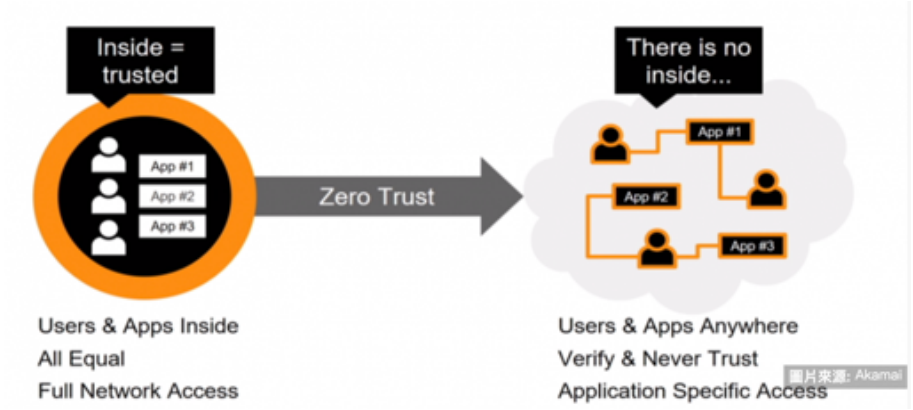
- 帳號解鎖
- 申請虛擬機資源
- 申請雲端資源
- 帳號申請及權限分配
- 申請遠端辦公相關資源，如VPN帳號及手機收信等等
- 設備申請流程

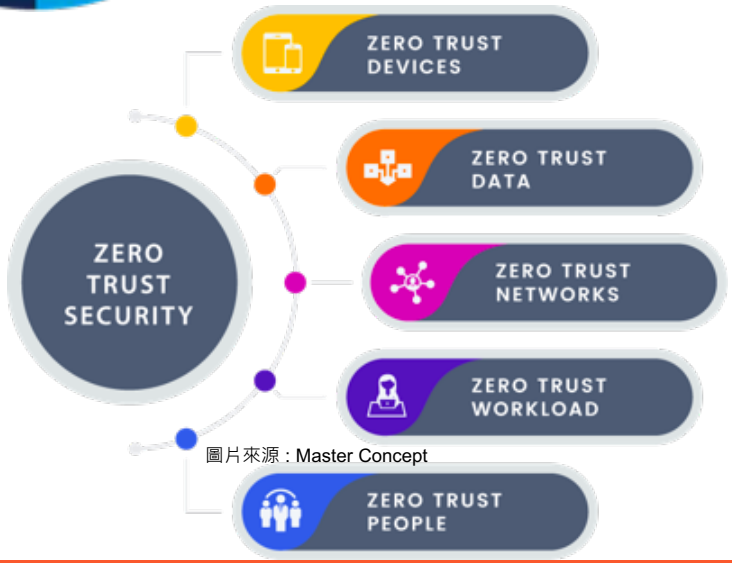
零信任平台

零信任安全模型

- Zero Trust是一種基於嚴格身份驗證過程的網路安全模型。該框架確定只有經過身份驗證和授權的用戶和設備才能訪問專用網絡，應用程序和數據。 同時，它可以保護那些應用程式和用戶免受Internet上進階威脅的侵害。

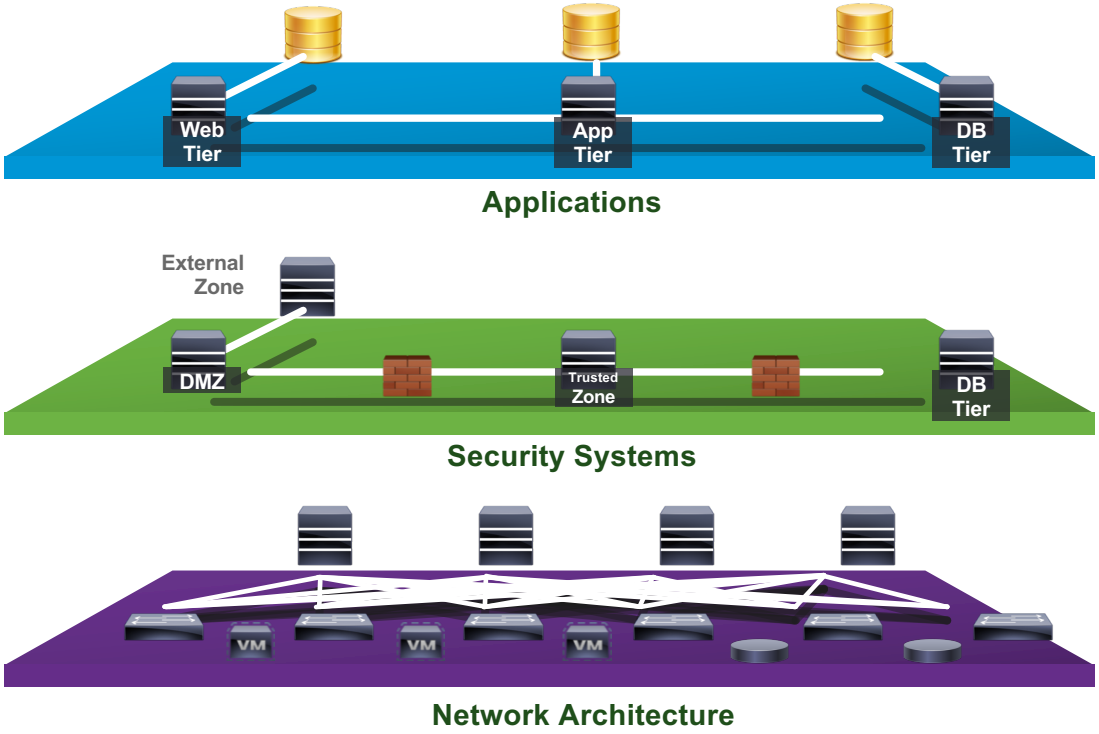
圖片來源：Cisco





圖片來源：Master Concept

安全層和傳輸層在分離，採用基於應用而非地址網段的管控模式



Google的Beyond Corp

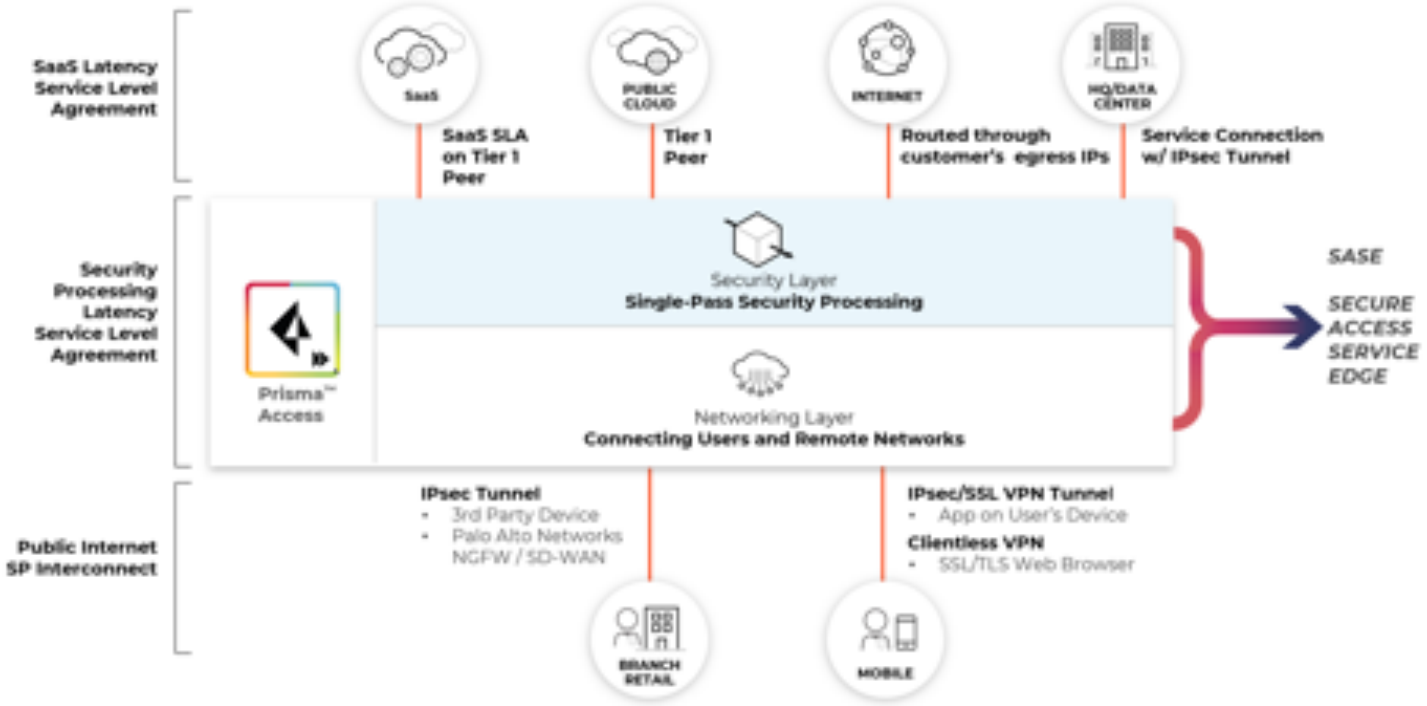
2011年提出概念，2017年基本可用，2020年商務

1. 企業應用程式和服務不再對公用網路可見
2. 企業內網的邊界消失
3. 基於身份，設備，環境認證的精準訪問
4. 僅對特定應用而非逐步網路授予訪問權限
5. 提供網路通信的端到端加密

BeyondCorp遵循的準則：

1. 服務訪問權限的授予基於我們發起連接時所在的網路不能決定您可以訪問的服務
2. 對您和您的設備的了解
3. 對服務的所有訪問都必須通過身份驗證，獲得授權並進行加密

BeyondCorp + Zero Trust = SASE （ Secure Acces Service Edge)



部署的時間
從傳統的

月
到
天

Palo Alto Networks零信任平台

定義保護範圍

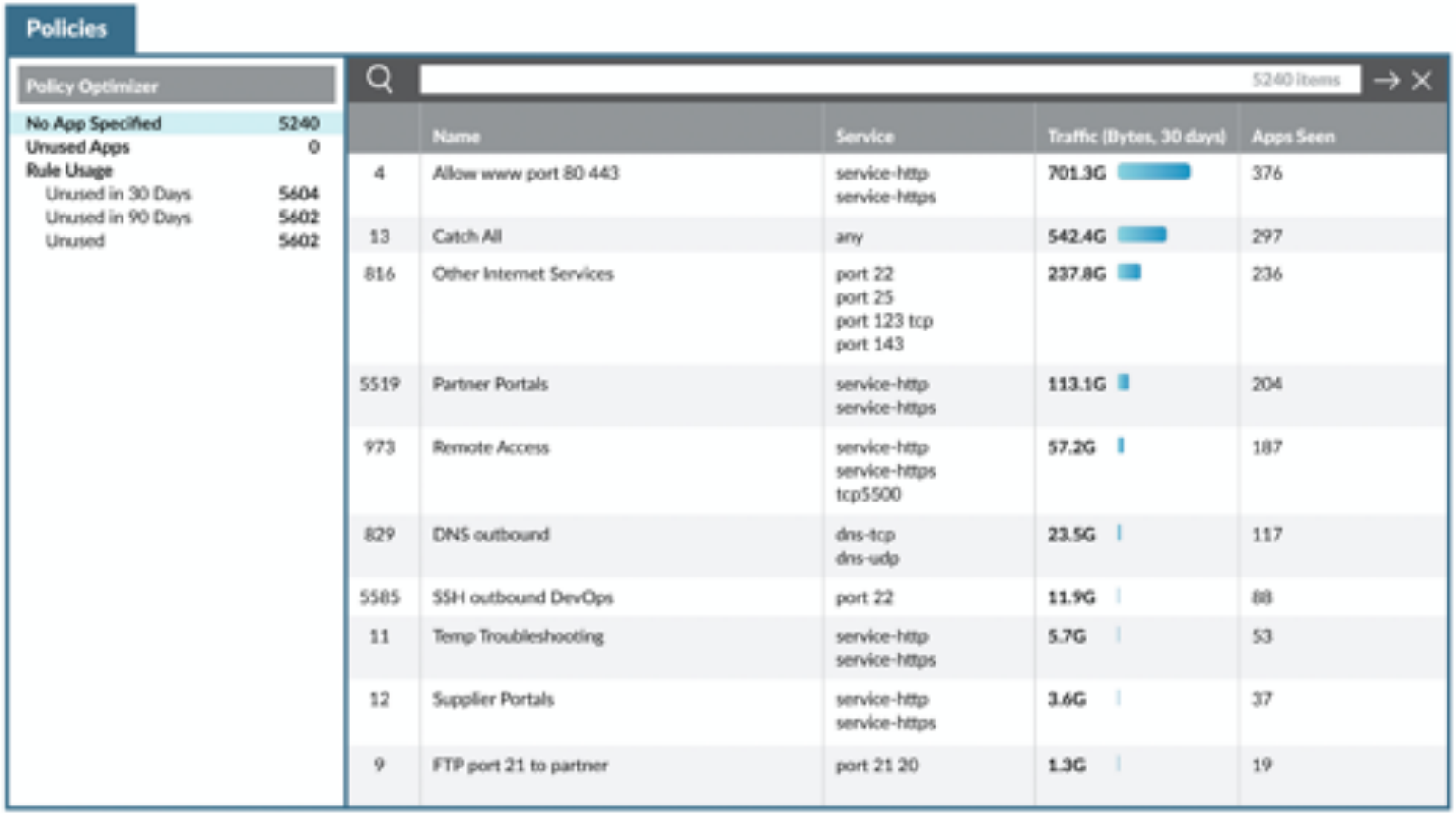
定義保護範圍時，您必須考慮所有關鍵數據、應用程式、資產或服務 (DAAS)

- **資料**：支付卡資訊 (PCI)、受保護醫療資訊 (PHI)、個人可識別資訊 (PII) 和智慧財產 (IP)
- **應用程式**：現成或自訂的軟體
- **資產**：SCADA 控制、銷售點終端、醫療設備、製造資產，以及物聯網 (IoT) 裝置
- **服務**：DNS、DHCP 和 Active Directory®

對應交易流量

- 為正確設計網路，瞭解系統如何運作至關重要。流量在網路中的移動方式 (專用於保護範圍中的數據) 將影響保護該數據的方法。這種理解來自掃描和對應網路中的交易流量，藉此確定各種 DAAS 元件與網路上其他資源互動的方式。
- 透過記錄特定資源的互動資訊，即使缺乏完整情境，也可以約略地估算流量。這項資訊仍可提供有價值的數據，讓您避免缺乏洞察的盲目控制。
- 零信任是一種流量型架構。瞭解系統的設計運作方式之後，流量地圖就會告訴您需要嵌入控制的位置。
- 零信任是一個疊代程序。

舊規則在策略優化器中



建構零信任網路

- 傳統上，任何網路設計的第一步皆為建構網路。
- 在零信任之旅中，建構網路是第三步。此外，零信任網路將會量身打造，而非使用特定的通用設計。定義保護範圍並對應流量之後，零信任架構將會變得具體。
- 架構要素首先會將新世代防火牆部署為區隔閘道，以便強制將精密的第七層存取當做保護範圍的微型周邊。
- 使用這種架構時，存取保護範圍內資源的每個封包都將通過新世代防火牆， 因此可以強制執行第七層政策，同時控制和檢查存取。

建立零信任政策

- **誰**應該存取資源？這可定義「聲稱身分」。
- **哪個**應用程式是封包聲稱身分用於存取保護範圍內資源的應用程式？
- **何時**聲稱身分會嘗試存取資源？
- **何處**是封包的目的地？
- **為什麼**這個封包會嘗試存取保護範圍內的這個資源？
- 封包的聲稱身分**如何**透過特定的應用程式存取保護範圍？

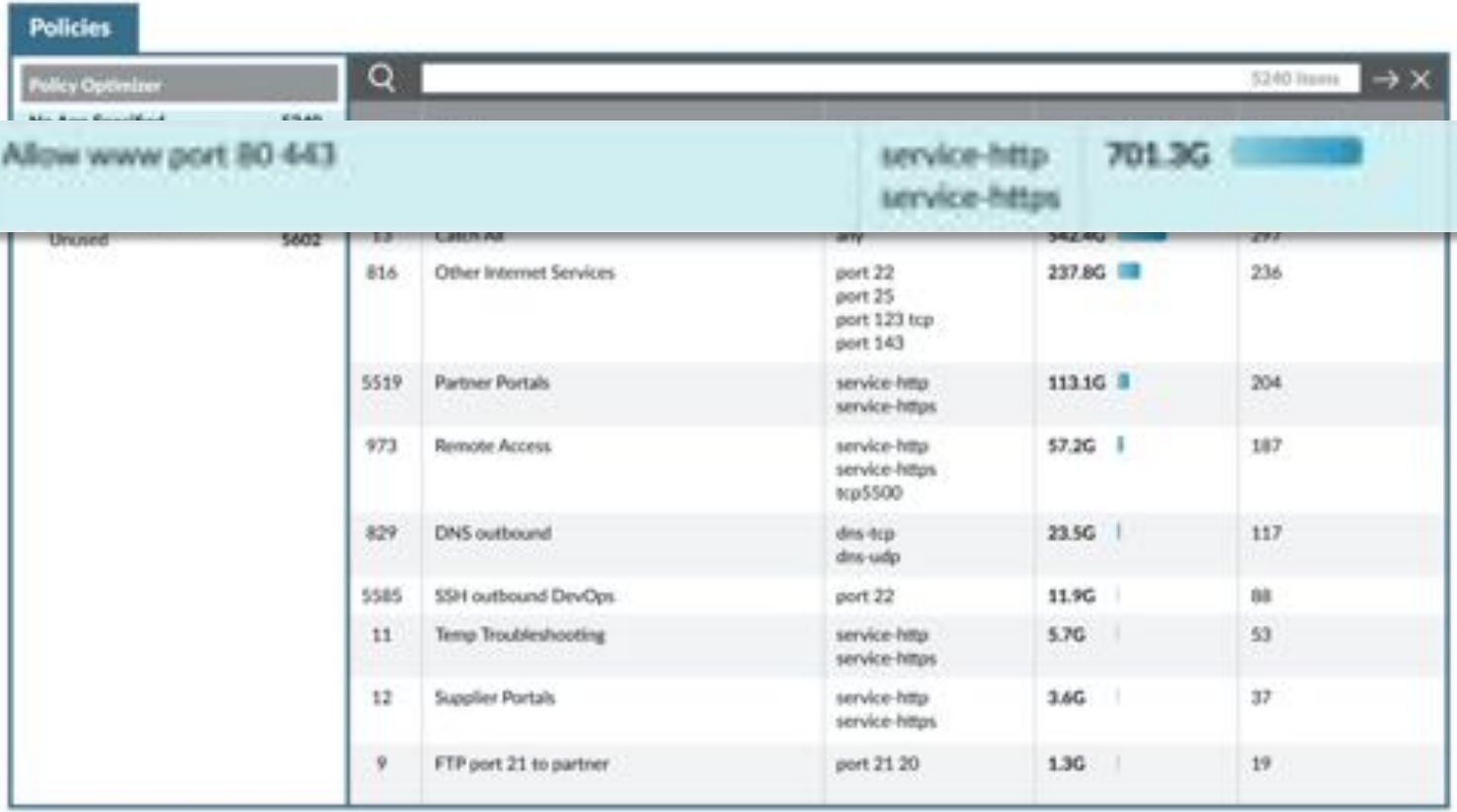
不應存在「未知流量」

1. 在零信任中，沒有「未知流量」。如果您不知道該流量為何，就不應該允許其存取保護範圍。

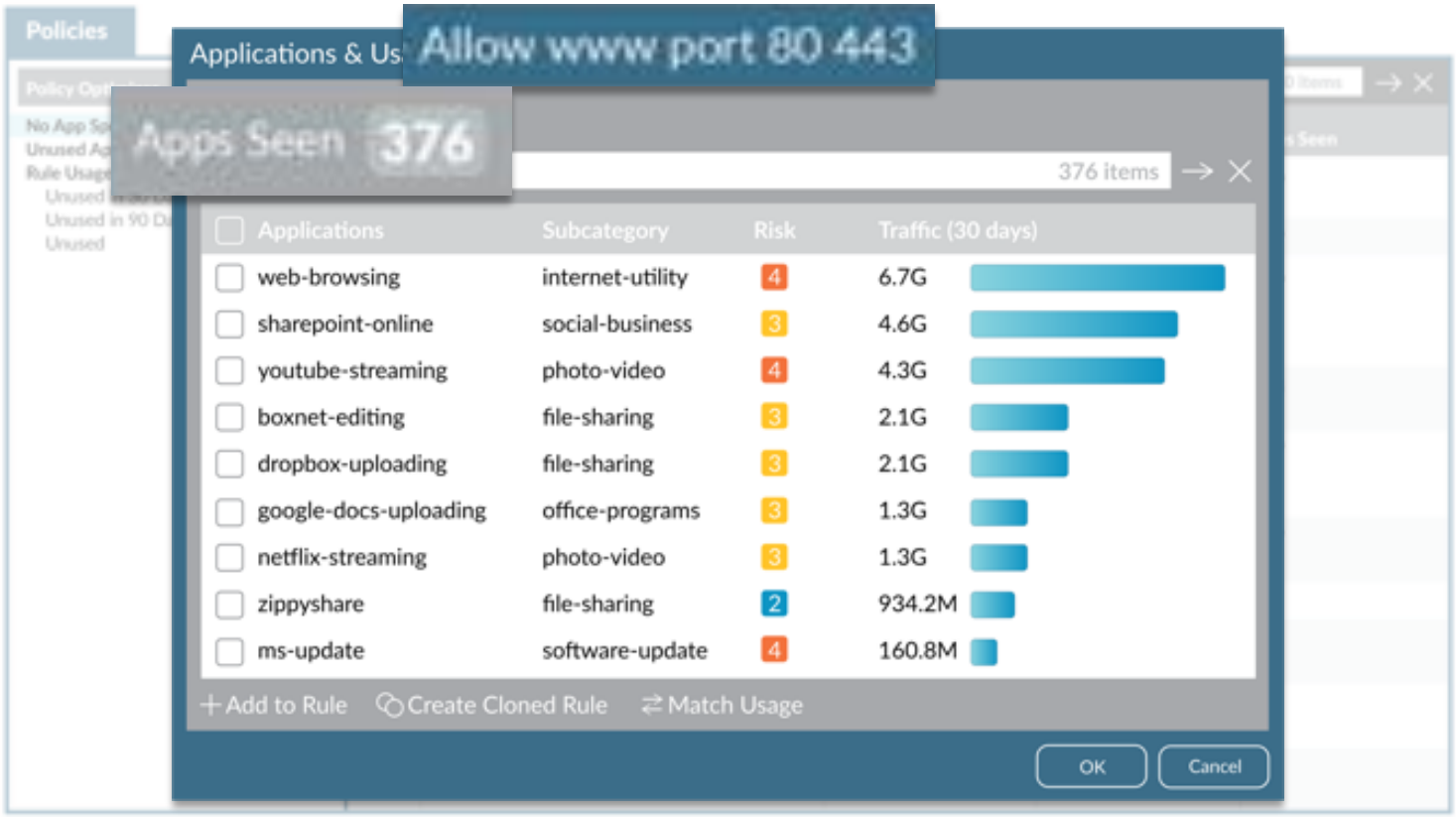
2. 必須判斷是否應該允許該流量，藉此讓這種流量變成已知的。

對象	內容	時間	位置	原因	方式	動作
User-ID	**App-ID**	**時間**	**系統物件**	**分類**	**Content-ID**	—
Sales	Salesforce	工時	美國	中毒	SFDC_CID	允許
Epic_Users	Epic	任何	Epic_Svr	中毒	Epic_CID	允許

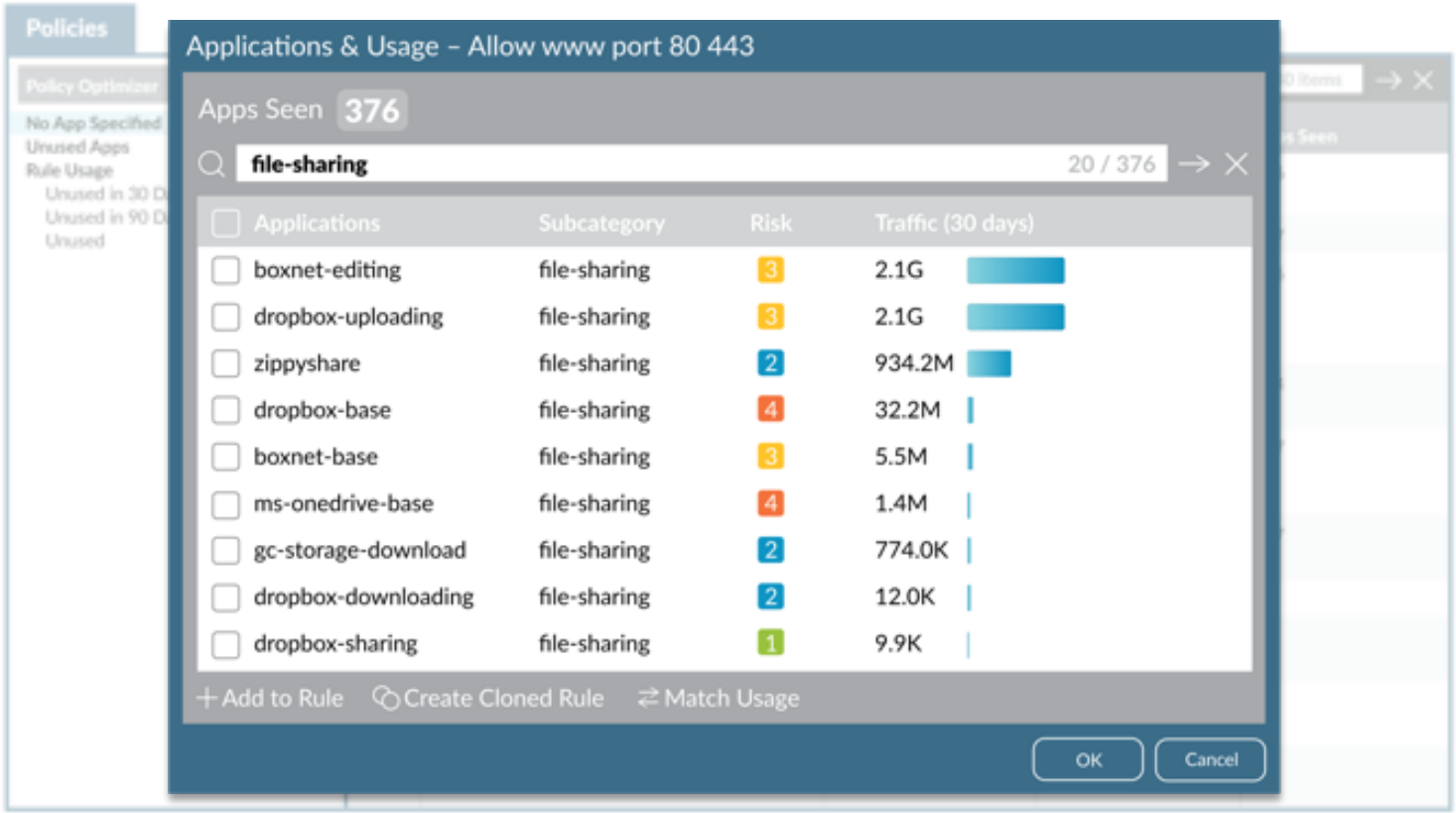
第一步：選擇一個優化的傳統規則



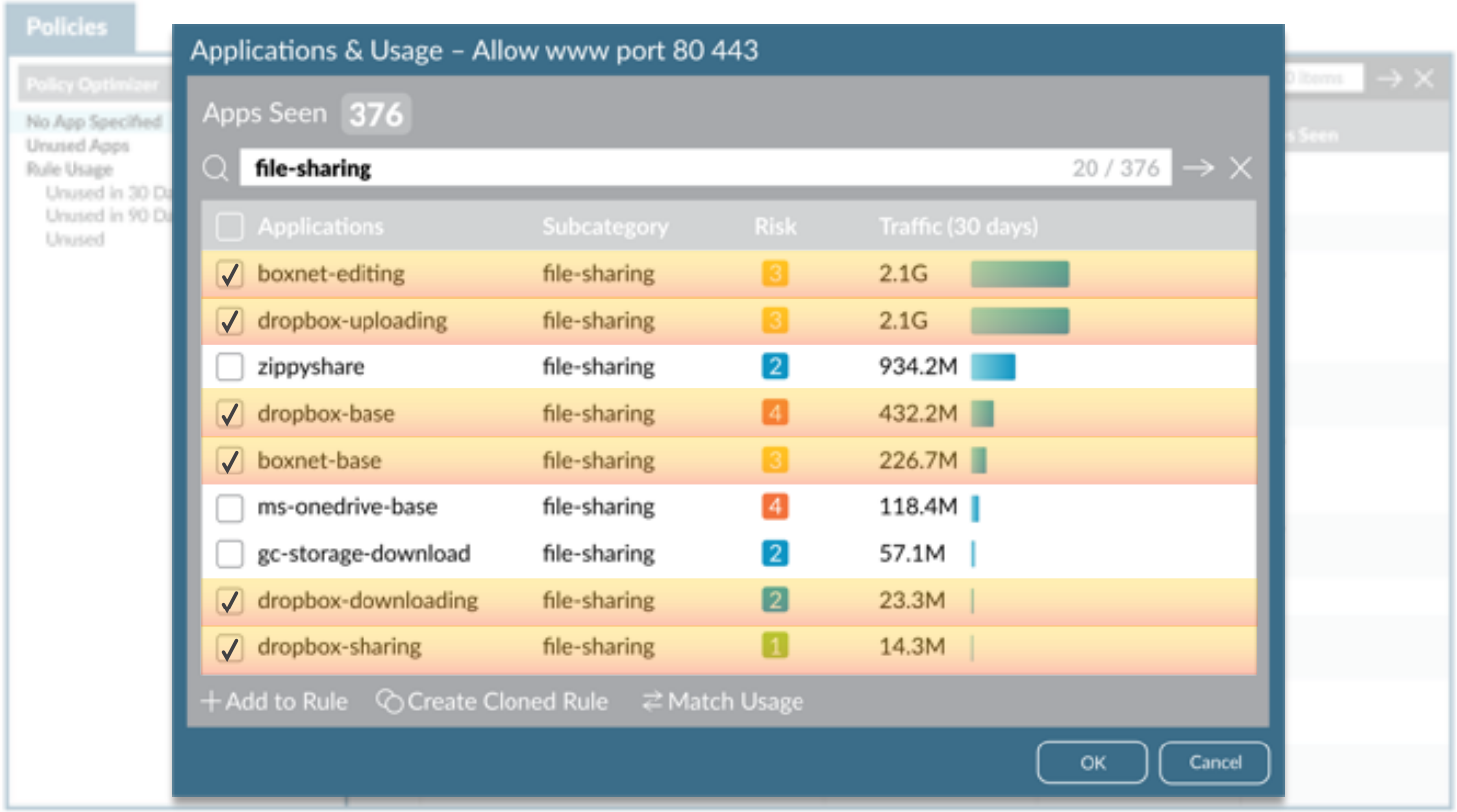
第二步：查看與規則匹配的所有應用程式



第3步：篩選file-sharing應用程式

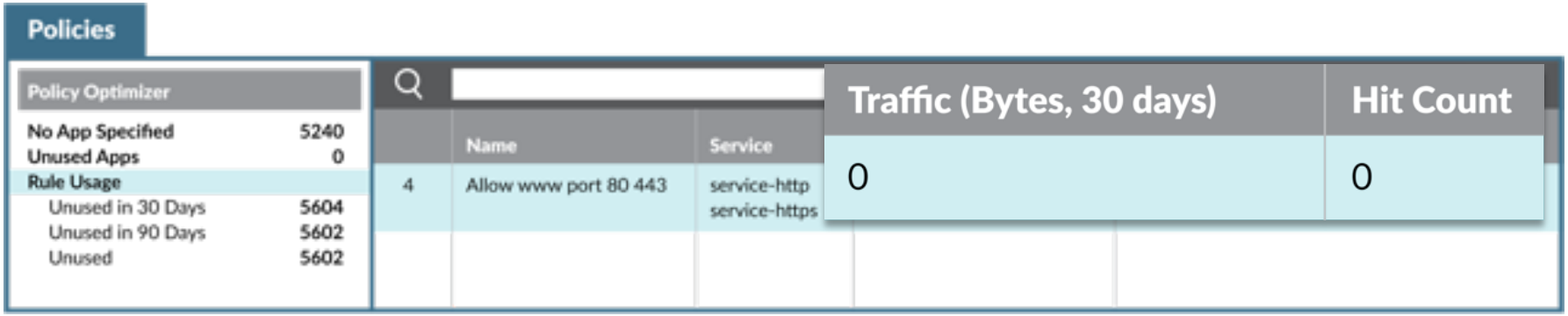


第4步：選擇允許使用的應用程式



基於應用程式定義的防火牆規則結果

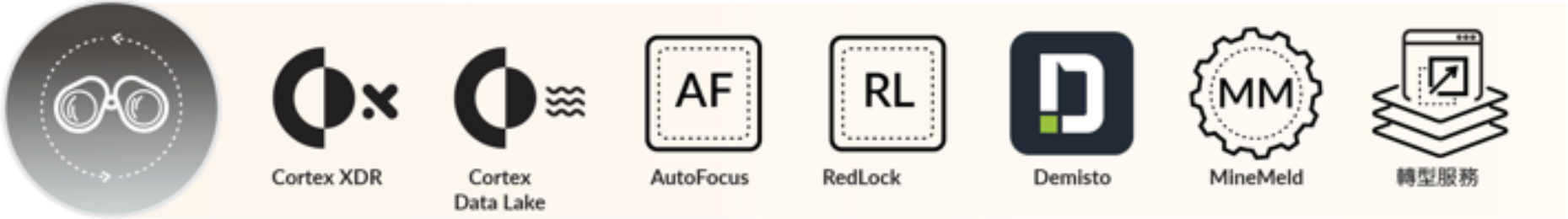
	Name	Source User	Application	Service	Security Profile	Action
1	Sanctioned SaaS Apps	corp-users	boxnet concur confluence dropbox jira ms-office365 slack	application-default		Allow



監控與維護網路

- 疊代程序中的最後一個步驟是監控與維護網路。也就是說，透過第七層持續查看所有內部和外部日誌，並將重點放在零信任的操作層面。檢查並記錄網路上的所有流量是零信任的重要面向。

- 向系統發送盡可能多的環境相關遙測數據非常重要。此數據能讓您掌握新的洞察，瞭解如何持續改善零信任網路。而網路受到的攻擊越多，就可以更深入地瞭解如何使政策更加安全，功能也會變得更加強大。



Thank you