企業數位轉型-資安瞻前顧後

Palo Alto Networks
台灣解決方案架構師 林揚城(Brook Lin)

May 2021

回顧2020年

回顧: 2020年

我們對2020年亞太地區的預測

現在的4G問題為5G奠定基礎

- 最大的5G基礎設施項目將在未來10年內著手進行，迄今為止只有少數試驗成功。儘管5G將與4G網路一起發展，但5G時代尚未完全到來。

人才短缺並非您所想的那樣

- 資安需求仍將持續超過供給，除非觀念上發生根本的改變。將需要兩個互補的方式—採用自動化和探索替代人才來源，來面對2020年的這一項挑戰。

探索物聯網將成為每個人的地雷區

- 許多亞洲經濟體重要支柱的製造業發生重大變化。製造商希望透過部署感應器、可穿戴設備和自動化系統來簡化生產、物流和員工管理。因此，需要不斷改進、更新這些相互連接的設備以確保安全。

資料隱私界線變得模糊

- 為了解決這一個日益嚴重的問題並保護資料，監管機構展開實施更嚴格的個資法，例如建議公民在其原國籍國存放資料的法律。

雲端未來已經到來：不要在動盪中迷失方向

- 儘管將資料遷移到雲端是趨勢，但對於將關鍵資訊放上雲端仍存有擔憂。

2021年預測

2021年 預測 1

懷念旅行嗎？做好更多必須分享個資的準備

旅行泡泡和互惠的綠色通道將會放大個資的爭論

儘管個資的爭論已經持續多年，追蹤接觸史是真正使個人開始在意數據隱私的原因。

由政府主導嚴格的接觸者追蹤計劃和準確數據的存取是在許多東亞國家幫助“拉平曲線”的關鍵因素，這些數據也很快的轉變成數位工具。隨著感染率再次飆升，Future Market Insights的研究顯示，在許多國家的反覆感染浪潮的推動下，新的接觸者追蹤應用程式每年將增加15%。

未來許多國家實施的**旅行泡泡**或**互惠綠色通道**對所有旅客是有效率且安全的方式，個資將需要透過正確的安全控制措施跨境共享，並以透明訊息交流並表明如何處理和儲存此類數據。

在2021年，政府共享COVID-19測試獲得的醫學數據，結合所有守法公民和政府拒絕名單的持續追蹤和簽到，是否會使旅客在休閒旅行恢復時，更審慎地看待其共享的訊息呢？

2021年 預測 2

對於那些已經做好準備的人而言，5G的等待已經結束

隨著政府現在全力以赴因應COVID-19和經濟復甦，私人企業現在已準備好接手5G競賽

iPhone 12的推出可能會造成首次大規模採用支持5G的裝置的現象，從而加速了越來越多國家/地區的網路的部署。

毫無疑問的，隨著電信公司部署提供消費者以及政府新的數位服務機會以幫助2021年的經濟復甦，將會加速越來越多國家5G網路的部署。

隨著政府現在全力以赴因應COVID-19和經濟復甦，私人企業現在已準備好接手5G競賽。由於5G需要安裝的**節點數量非常多**，使5G的部署更具挑戰性，大大增加了網路攻擊的可能性。

私人企業部門**負擔不起與4G相同部署與的設計和實施方法**，將無法免除其在3G和4G時代所遭受的類似攻擊。

2021年 預測 3

在家工作變得更聰明，更安全

資安將被推向邊緣及簡易化

2020年教會企業如何使**整個公司能夠進行遠距工作**。2021年也為企業提供了一個機會，讓它們規劃出一條新的道路，並思考如何在**不同情境下完成工作**。

隨著雲端工具的採用以及虛擬的桌上型電腦越來越多，企業可以改為為員工提供更簡單的連接設備，使員工可以在線儲存他們所需的程式和資源時，可以直接將工作交付給他們，從而保護公司的重要資產。

資安將會需要以邊緣的方式來交付，這將使諸如安全存取服務邊界（SASE；secure access service edge）之類的解決方案因其靈活性，簡單性和可見性而成為新的網路安全規範。

2021年 預測 4

重新整頓的一年

IT團隊回歸到井然有序的思考模式，藍天般有創意地思考將完全消失

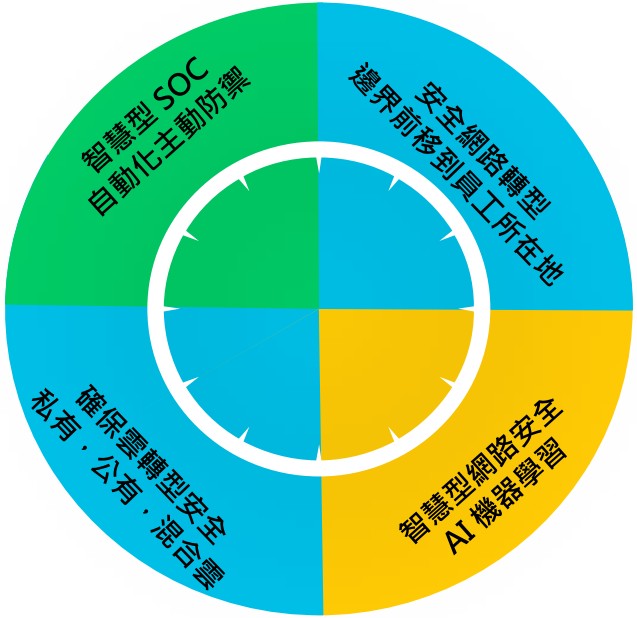
除了電子郵件之類的輕觸功能將移至更廣泛的雲端，在2021年也將看到更多的工作被虛擬化，迫使許多公司檢視現有雲端環境的安全性。

隨著企業繼續擴展現有的雲端規模，現在企業需要一層身份和存取管理（IAM；Identity and Access Management）的治理。今年，Palo Alto Networks Unit 42的研究人員觀察到，單個IAM配置錯誤可以使攻擊者攻陷整個雲端環境並繞過幾乎所有安全控制措施。

隨著疫情帶動IT團隊必須解決更多問題，到2021年，可能會有更多的企業將重點轉移到如何使井然有序的思考模式，而面對基本的問題上，將優先考慮到企業雲端環境建立的彈性。

依舊存在的問題

- 邊界安全問題依舊存在
  - SSL VPN 問題持續發酵
  - Exchange 漏洞（Pwn2Own 再度被攻陷 ）
- 供應鏈安全問題
  - SolarWinds 事件帶來的省思
- 勒索事件與資料外洩依然是焦點
- 雲安全的顧慮
- 資訊安全人力/經驗依然有提升空間



迎向數位轉型
(Digital Transformation)

數位轉型所面臨的風險

- **Changing Landscape**
  Companies and increased customer expectations are driving traditional companies to themselves. Business has become a **digital industry** with new innovative products, services & competitors.

- **Increased Attack Surface**
  With a continuous increasing attack surface due to digital initiatives to support your company' s strategy are directly accessible from anywhere at any time. The interconnectedness between systems further increases the attack surface. This makes your industry an **ideal target for cyber attacks**.

- **Impact to the Business**
  A security-by-design approach is essential to reduce the risk of a severe cyber breach and to **safeguard business continuity**. Disruption of digital services can have a significant impact on the brand image & financial results of the company.

We Create A Transformation Strategy To Realize Portfolio Value
不執著於單一面向進而採用全面完整的轉型策略

中期-Tactical: 1-2 Year

- Executive Alignment Across Businesses
- Zero Trust Implementation And Reporting
- Complete SSL Decryption
- Continuous App-ID, User-ID improvement
- Implement MFA for internal applications
- Implement Credential Theft Protection
- Validate and Maintain IPS Enforcement
- Improve SaaS visibility and operationalization

長期-Strategic: 2-3 Year

- Cross-Functional Security Ownership
- Transition to a positive enforcement model
- Access Management (User-ID, MFA)
- Automated Behavior Analytics Integration
- Automated and integrated SecOps

短期-Quick Wins: 10 Months

- Regular Executive Threat Exposure Reviews
- Enterprise Security Assessment and Gap Analysis
- Zero Trust Protect Surface Roadmap
- Webinars and Workshops
- Team Alignment Across Workcenters

資安道路上總會遇到困難 - But all of it creates greater risks.

More remote users, devices and data

mean more targets for cyber attacks.

3x

increase in the number of endpoints by 2023

COVID-19形成 The New Normal(新常態)

Rapid cloud deployments

are accelerating faster than digital enterprises' security.

43%

Struggle to deliver consistent security across data centers and the cloud

COVID-19促使 Total Experience(全面體驗)

Advanced cybercriminals

are taking advantage of world events and advanced technology.

68.9%

increase in phishing attacks leaders are experiencing since the coronavirus outbreak

COVID-19加速 Cybersecurity Mesh (網絡安全網狀運作)

Source: Gartner, ESG Global, Accenture

Gartner 2021 戰略科技趨勢
Three Themes

- People centricity: Despite the pandemic changing how many people work and interact with organizations, people are still at the center of all business — and they need digitalized processes to function in today’ s environment.

- Location independence: COVID-19 has shifted where employees, customers, suppliers and organizational ecosystems physically exist. Location independence requires a technology shift to support this new version of business.

- Resilient delivery: Whether a pandemic or a recession, volatility exists in the world.

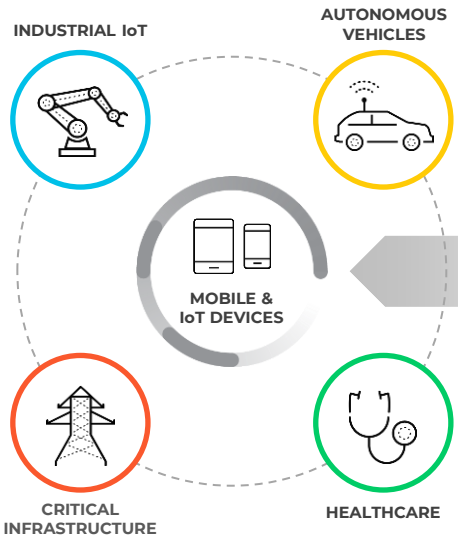
We help you … 5大方向

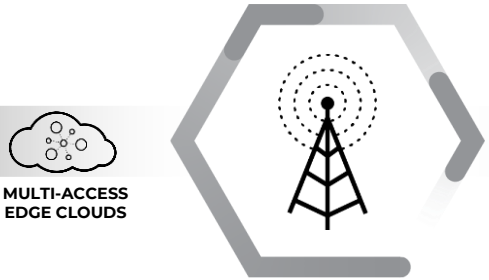
- Use AI and ML to intelligently secure the network and proactively prevent threats across network and IOT devices including 5G security
- Secure your remote workforce with simple, scalable cloud-delivered security
- Elevate branch performance and ROI with secure SD-WAN that is autonomous, app-defined, and cloud delivered
- Transform security operations using the most advanced AI and automation to detect, investigate, automate and respond to threats
- Deliver consistent cloud security by protecting data and applications across the lifecycle in and across any cloud

5G帶來了什麼改變

近一步擴大的用戶基數

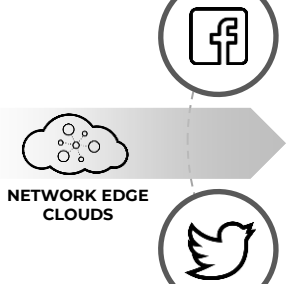
關鍵行業關鍵應用的緊密集成5G





網路核心、應用和服務

遷移到邊境雲

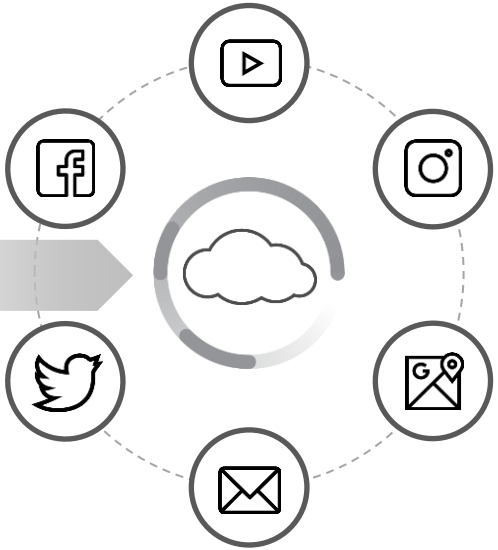


OTT的應用和服務

4G LTE

電信商作為傳輸通道

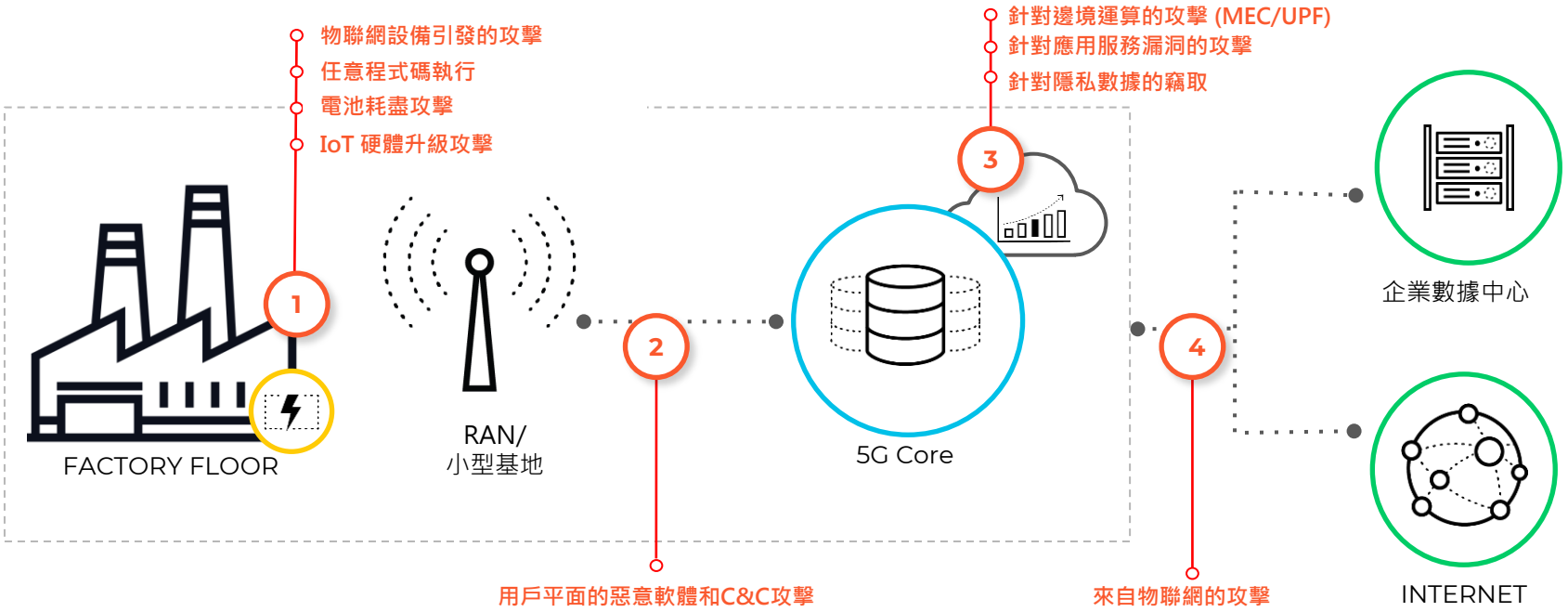
盡力而為的傳輸模式



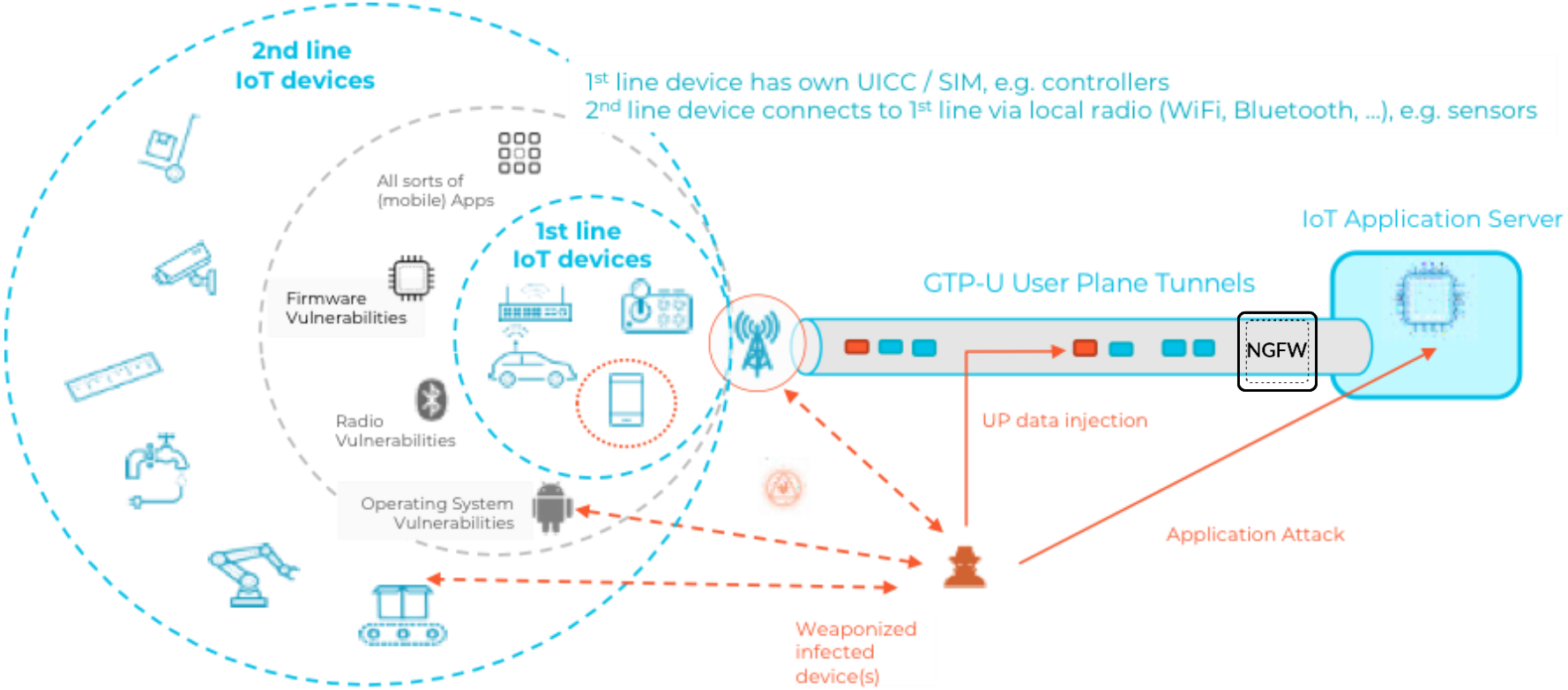
4G/LTE安全和5G安全的區別

	4G/LTE安全	5G 安全
User	• 4G/LTE網路主要提供2C服務 • 作為管道，SP沒有動力提供客户安全保障	• 5G網路更多面向行業服務 • 企業客户需要企業級安全性和SLA • 為服務提供商提供安全增值服務的創造收入
Device Type	• 設備级别的攻擊面僅限於幾種設備類型，包括智慧型手機或者LTE路由器	• 隨著更多數量和類型的設備連接到5G網路，5G的攻擊面將大大增加
Protocol	• 專有3GPP協議相對安全	• SBA HTTP/2取代了大多數專有3GPP協議 • IP的HTTP/2比專有協議更容易受到IT協議棧漏洞的攻擊
HW vs SW	• 選定供應商提供的網路功能主要是在封閉環境中以硬體形式提供的	• 在5G中，網路功能已轉移到軟體(VM或者容器)中，開放的環境和應用更容易受到攻擊
SP View	• 傳統的觀點是使用GI FW和IDS / IPS部署外圍安全來處理採樣流量。 • 更多惡意軟體/流量可能會給營運商帶來更多收入	• 惡意軟體導致企業客戶滿意度的下降 • 需要在5G網路中的多個位置部署先進的威脅檢測和預防

5G 網路使用者面對潛在威脅 – 企業視角



5G企業應用安全 - IoT Chain安全



智能製造
工業4.0


保護關鍵資產
• 可行的安全情報（用戶/設備ID/威脅關聯）
• 對M2M / IoT行為模式的可見性
保護關鍵服務
• 未修補的舊版操作系統中安全地連接5G物聯網
• 識別並阻斷已知/未知惡意威脅
• 訊息和數據平面漏洞防護
數據安全
• 避免專有信息，知識產權資產和
• 商業機密的數據洩露
• 數據隱私與合規

It's Time for a New Approach

Cloud-first businesses need comprehensive cloud-delivered security that:

Protects All Application Traffic

Provide access to all applications and secure them against all threats, not just web-based apps and threats

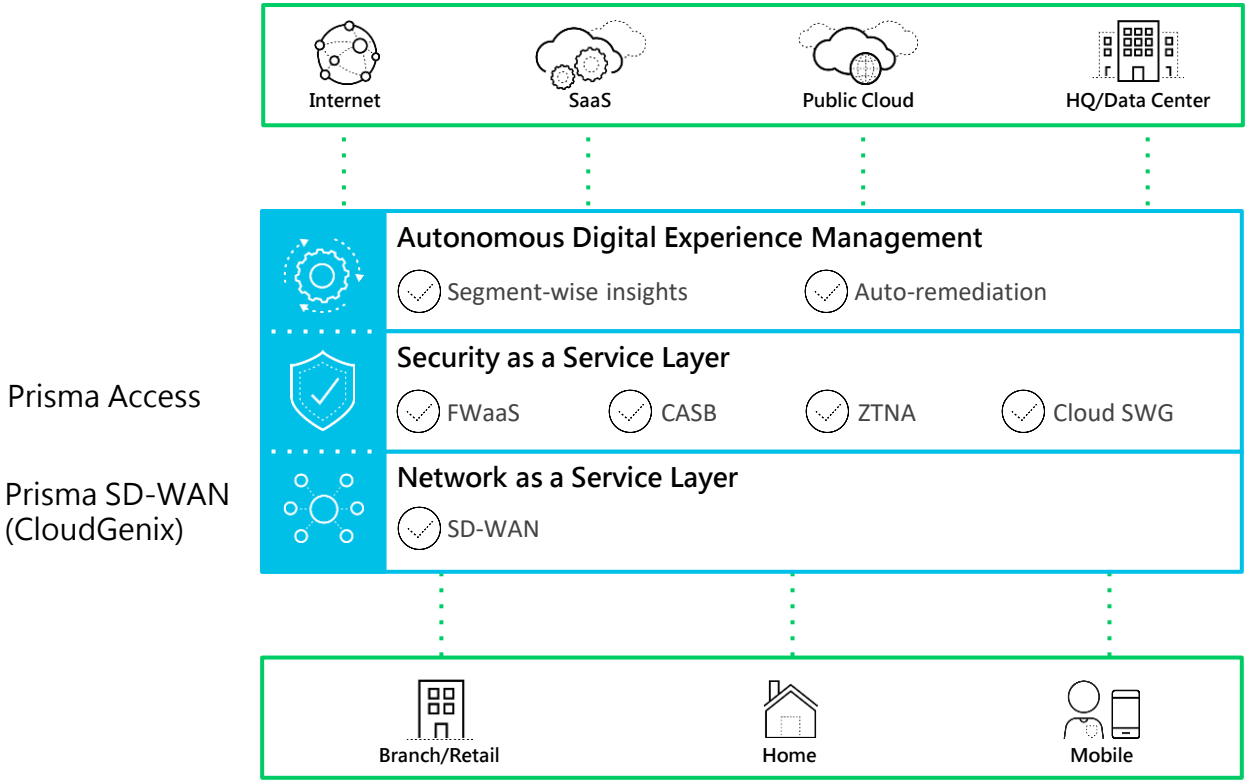
Provides Complete Best-in-class Security

Deliver industry-leading capabilities converged into a single cloud-delivered platform

Delivers an Exceptional User Experience

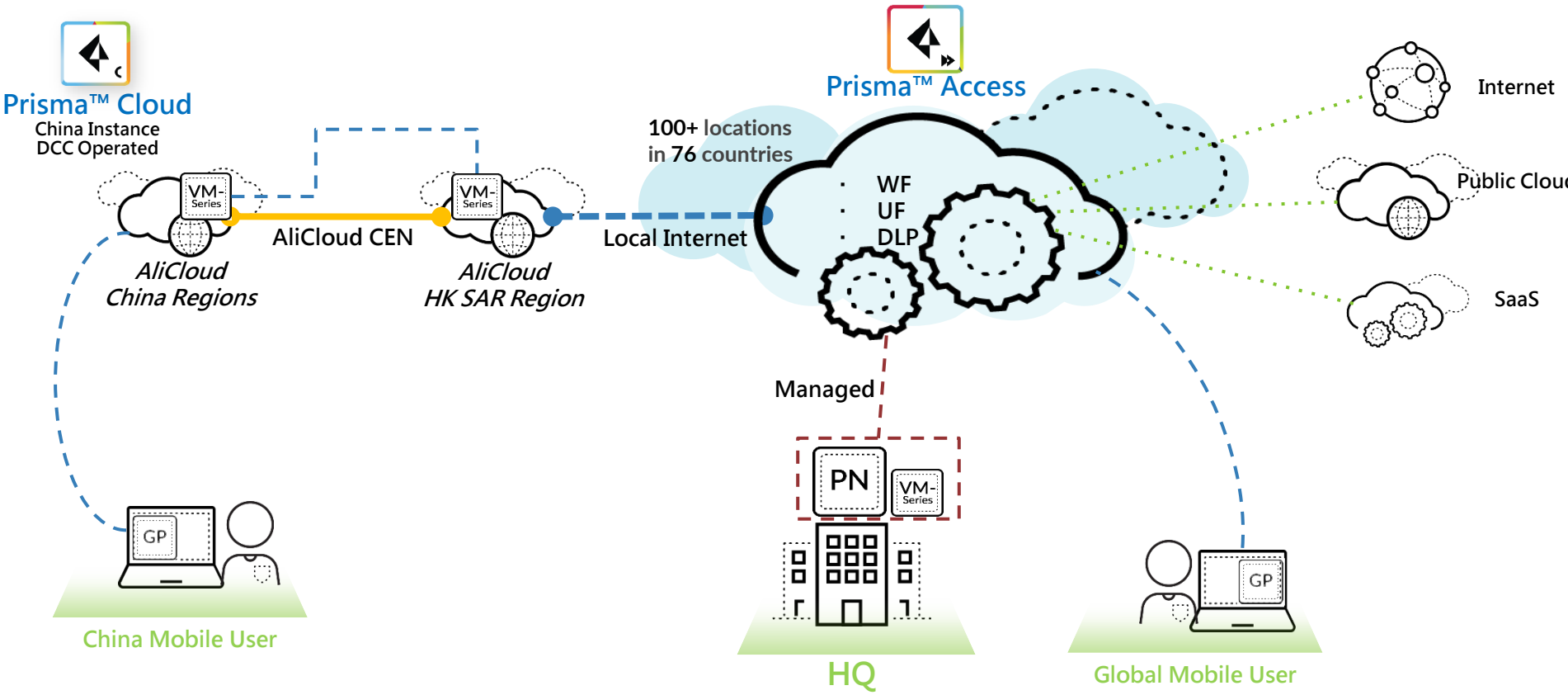
Optimize the user experience, with guaranteed performance across a massively scalable network

The Industry’s Most Complete SASE Solution



- Protects All App Traffic
- Complete, Best-in-Class Security
- Exceptional User Experience

Prisma Access flexible design – Your imagine We did it



謝謝