



# 建立強韌防護 - 確保現代教網應用安全

## F5 雙層式 WAAP 治理架構，制敵機先阻絕攻擊於邊境

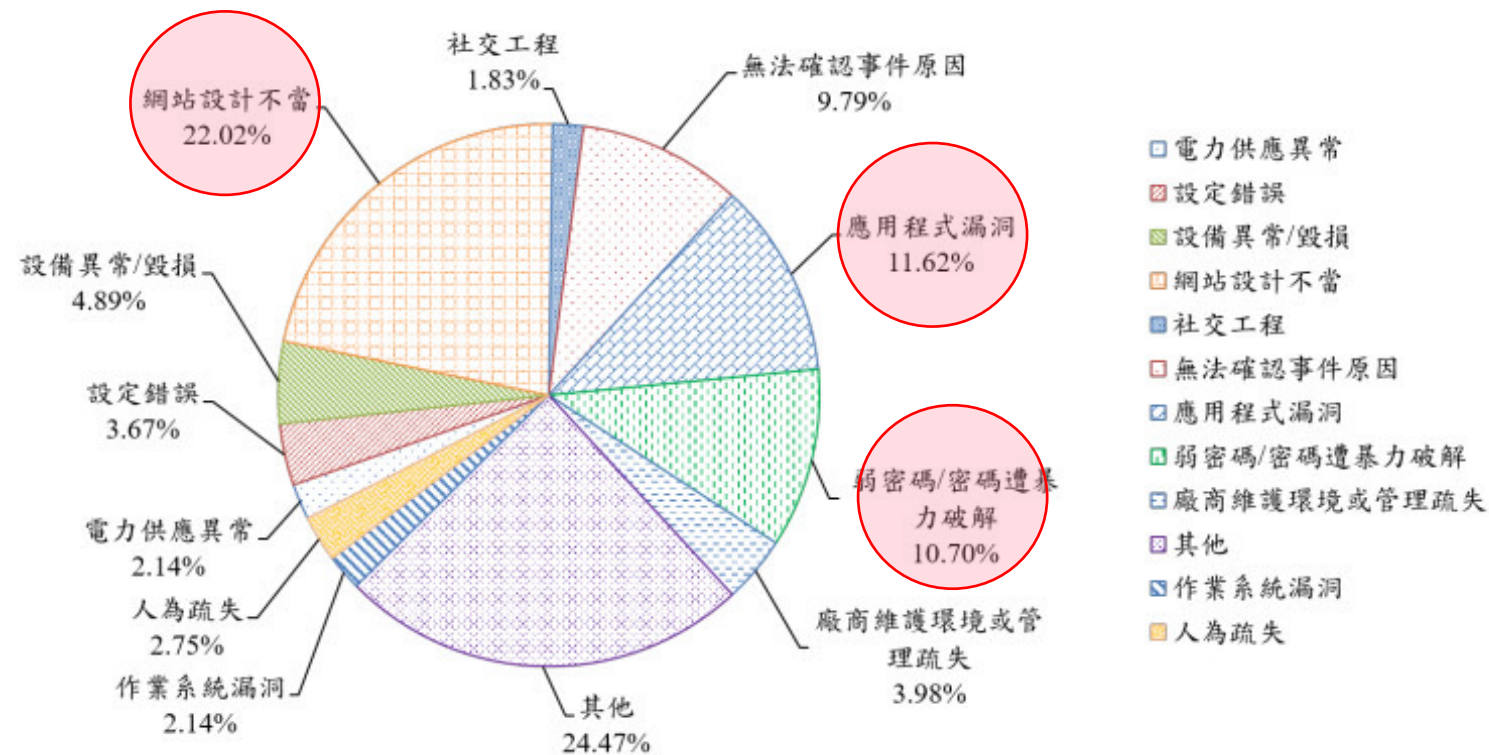
F5, Inc.

Solutions Engineer

Joshua 范茗閱

# 既有的資安威脅

<https://www.ithome.com.tw/news/154164>



我國推動政府資安落實，最近有了新的成效浮現，從行政院國家資通安全會報技術服務中心（以下簡稱技服中心）發布的第三季資通安全技術報告，可以看到具體轉變。在這份11月7日公開的政府資安防護態勢回顧中指出，過往分析通報事件發生原因時，公部門無法確認事件原因的比例居高不下，這將導致難以防範類似事件再發生，如今，這樣的比例正呈現逐漸下降的趨勢，能見度提升，有助於更快處理與及早預防資安問題。

.....

## 強調事件記錄保存，無法確認事件原因降低

近年來，我國政府不斷強調資安事件通報的重要性，使得重大資安事件看似越來越多，但這也代表機關守法、願意回報他們所面臨的資安事故，而非抱持著息事寧人的心態、不願或不敢通報，導致政府被蒙在鼓裡、無法及時控制損害範圍與應變。現在當各個機關都變得更勇於通報之後，下一步重點就會是如何從通報事件找出根因，才能杜絕再次發生。

.....

## 重大資安事件通報二級事件增加，網頁攻擊與DDoS比例增

除了資安事故能見度提升，但隨著國內外情勢趨於警張，大家都很擔憂政府資安威脅現況是否隨之惡化，因為裴洛西訪臺而衍生國內遭到多起網路攻擊的事件，正是發生在8月，包括分散式阻斷服務（DDoS）攻擊、內容置換（Deface），以及幾可亂真的假訊息等。

# 既有的資安威脅

**iThome** 新聞 產品&技術 專題 AI Cloud 醫療IT 資安 研討會 社群 IT EXPL

新聞

## 中國駭客RedHotel針對包括臺灣在內的17個國家，進路攻擊行動

根據資安業者Recorded Future的調查，中國支持的駭客組織RedHotel從2019年起，便滲透臺灣、美國與東南亞等地的政府與民間組織竊取政經情資，也會利用受害組織的憑證與基礎設施發動攻擊

文/ 陳曉莉 | 2023-08-15 發表 讚 55 分享



圖片來源: Nemanja Jeremic on unsplash

CYBER THREAT ANALYSIS CHINA

**Recorded Future®**

By Insikt Group®  
August 8, 2023



### RedHotel: A Prolific, Chinese State-Sponsored Group Operating at a Global Scale

<https://go.recordedfuture.com/hubfs/reports/cta-2023-0808.pdf>

# 應注意而未規範於資通安全法

## DNS 攻擊

全球預警情報網 Security & news

事件通告：網軍針對政府機關發動地毯式DNS攻擊，請自建DNS客戶提高警覺

風險等級：高度威脅  
摘要：  
【弱點說明】  
事件通告：網軍針對政府機關發動地毯式DNS攻擊，請自建DNS客戶提高警覺  
【影響範圍】  
• 自建DNS用戶，  
【細節描述】  
1. 近期DDoS事件讓SOC難以發現，作攻擊。(2) 攻擊藉以癱瘓客戶自建響：消耗DNS伺服器  
【建議措施】  
(1) 申請DNS Host  
(2) 針對DNS服務於advance-ddos

衛生福利部食品藥物管理署  
FDA Taiwan Food and Drug Administration

請輸入關鍵字 站台 站外 搜尋 進階搜尋  
熱門關鍵字：食品添加物 營養標示 非登不可 基因改造

公告資訊 機關介紹 業務專區 法規資訊 便民服務 出版品 政府資訊公開 個人化服務

目前位置：首頁 > 公告資訊 > 本署新聞

公告資訊

本署公告

本署新聞

維護公告

活動訊息

預告法規沿革區

食藥關謠專區

食藥膨風廣告專區

食藥署成功抵禦DNS DDoS攻擊，已恢復正常運行  
| 發布日期：2023-03-24 | 更新日期：2023-03-24

一、 食品藥物管理署名稱解析伺服器今日遭受分散式阻斷服務攻擊，在發現異常流量後，本署立即啟動了緊急應對措施，與電信業者通力合作，減緩攻擊影響，現已正常提供服務。

二、 本日攻擊事件係攻擊者針對本署網域名稱系統(DNS)進行分散式阻斷服務(DDoS)，導致網際網路使用者無法經由網址解析取得本署網站服務IP。

三、 為應對未來可能出現的類似事件，我們將加強網路安全措施，提高應對此類攻擊的能力。

# 地端防禦的架構是根本之道

## 地端資料中心防禦

### F5 BIG IP

白名單

(File Type, URL)

SSL offload

API Security Gateway

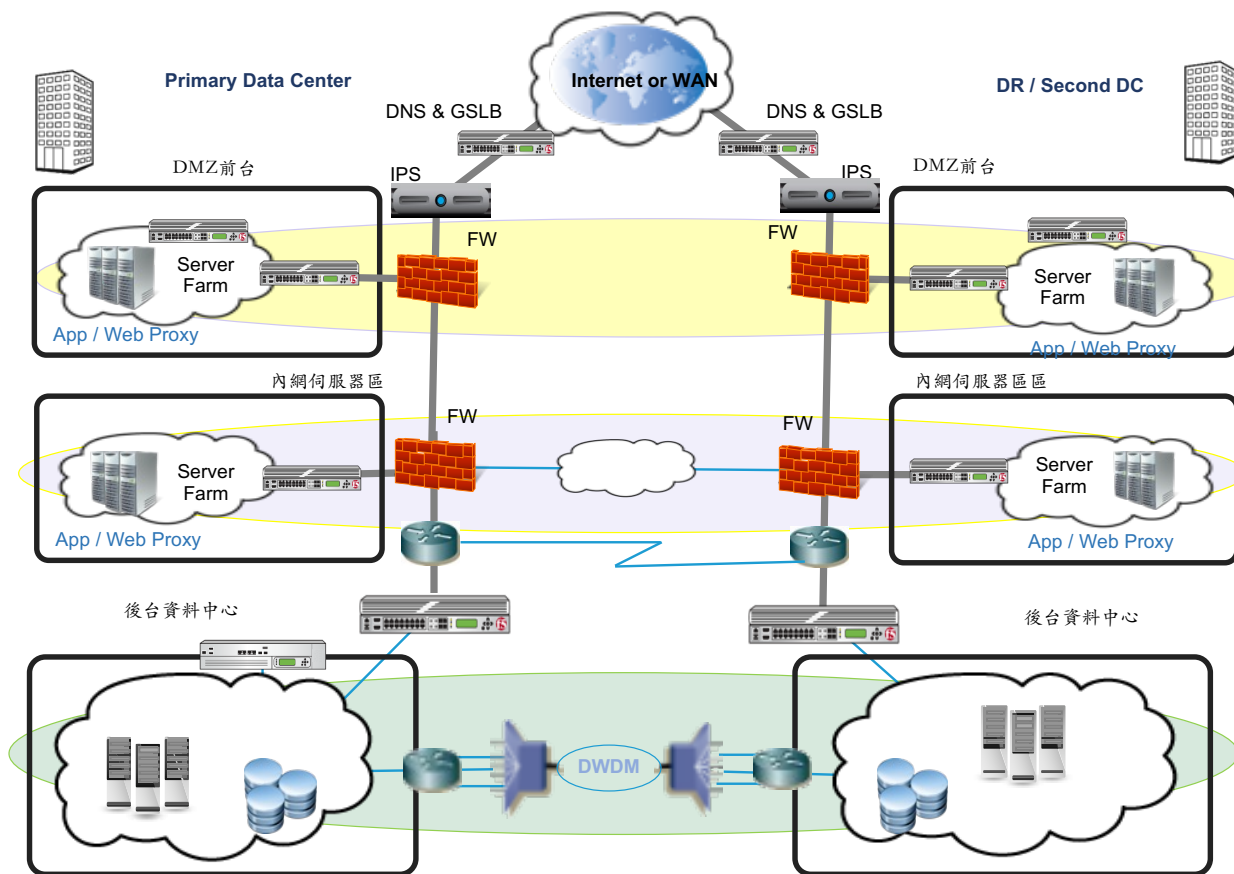
L7 DDOS

Advanced Feature

黑名單(OWASP Top 10)



AWAF



- 無法應付 DNS 攻擊
- 無法應付海量 DDoS 攻擊
- 無法應付日趨成熟的機器人攻擊
- 無法保護當應用臨時部署公有雲
- 無法適應混合雲架構
- 無法建立數位資安韌性
- 資安資源需要重新配置

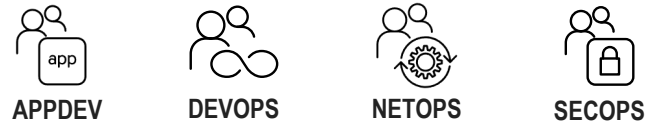
# F5 豐富的應用網路和安全解決方案



## Multi-Cloud Application Security and Delivery Technologies

# F5 Distributed Cloud - WAAP-as-a-Service

多層、高效的現代應用程式安全性，彙集了 F5 應用程式安全的精華



Integration with Critical Automation, Git Ops and Dev Tools



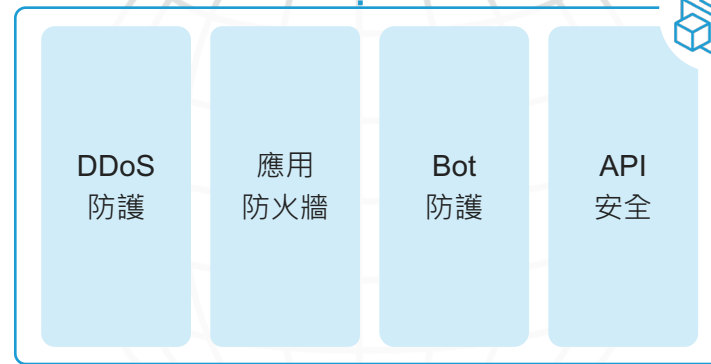
Integration with SIEM, Logging and Alerting Platforms



F5 Distributed Cloud Console – Centralized control plane



Public Cloud



F5 Global Network



Private Cloud / Data Center



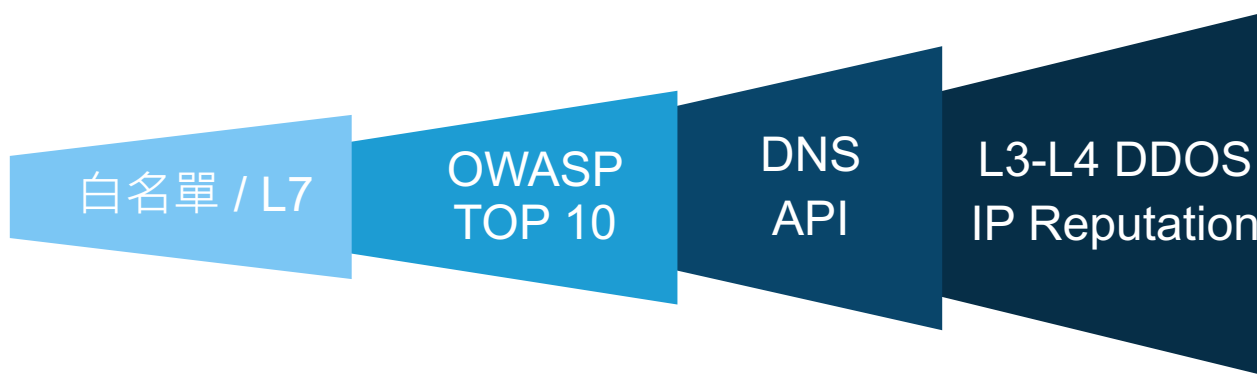
Branch/Customer Edge



Distributed Cloud Services



# 雙層式 WAAP 治理架構：XC WAAP + BIG-IP AWAf



- > 既有運行的應用系統 (3-tiering)
- > 新開發的容器化應用服務 (k8s)
- > 數據中台服務 (data fabric)

# 緩解大型的攻擊防禦，建議利用雲資安強大的邊緣運算能力

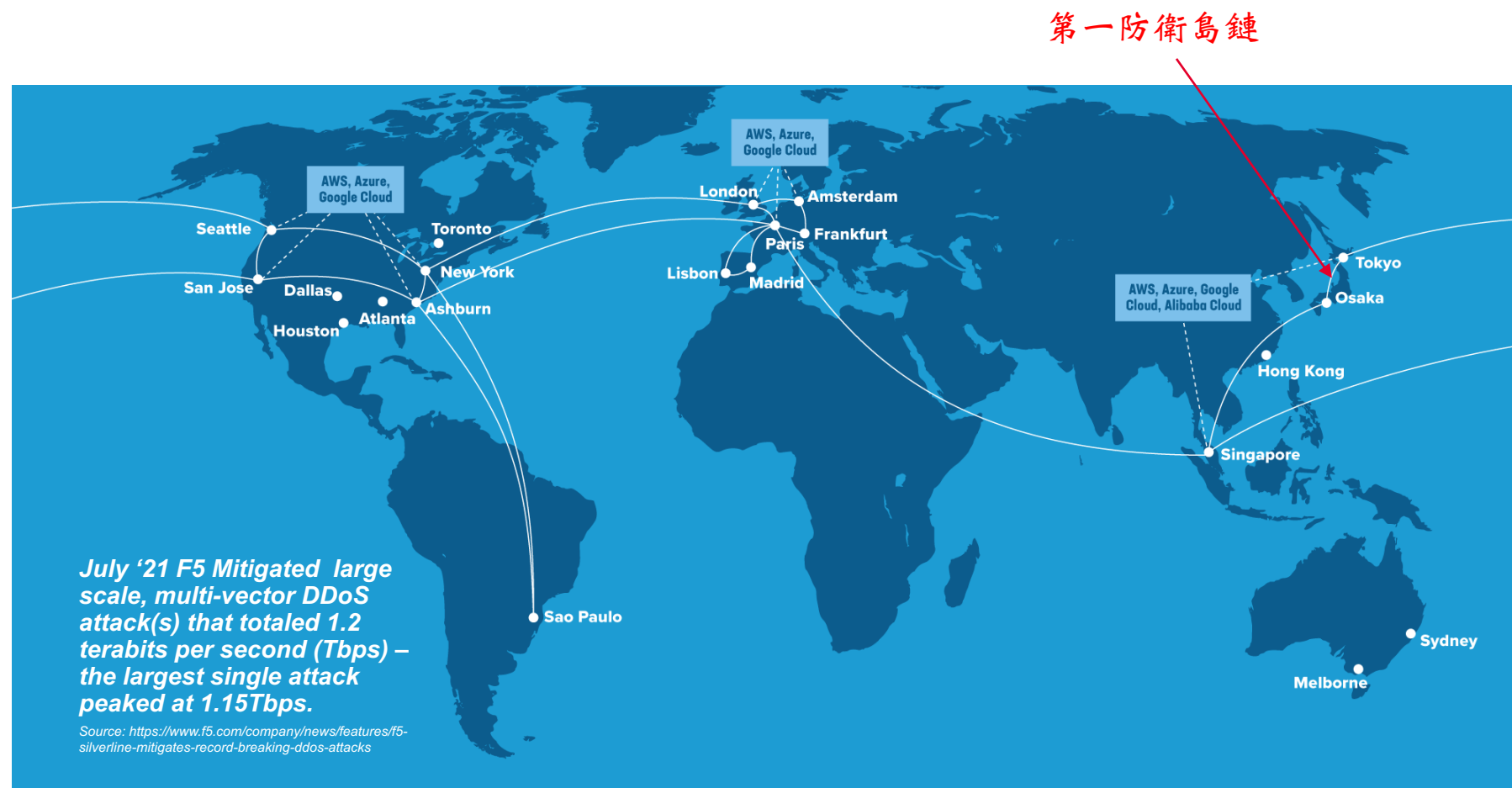
遠離關鍵應用服務和基礎設施，防禦決戰於邊境

世界級的全球安全運營中心  
全球26 PoP清洗端點

全球 DDoS 保護網絡  
具有 17+ TB 清理能力。

靈活的服務選項  
包括 Always Available 或 Always On 部署

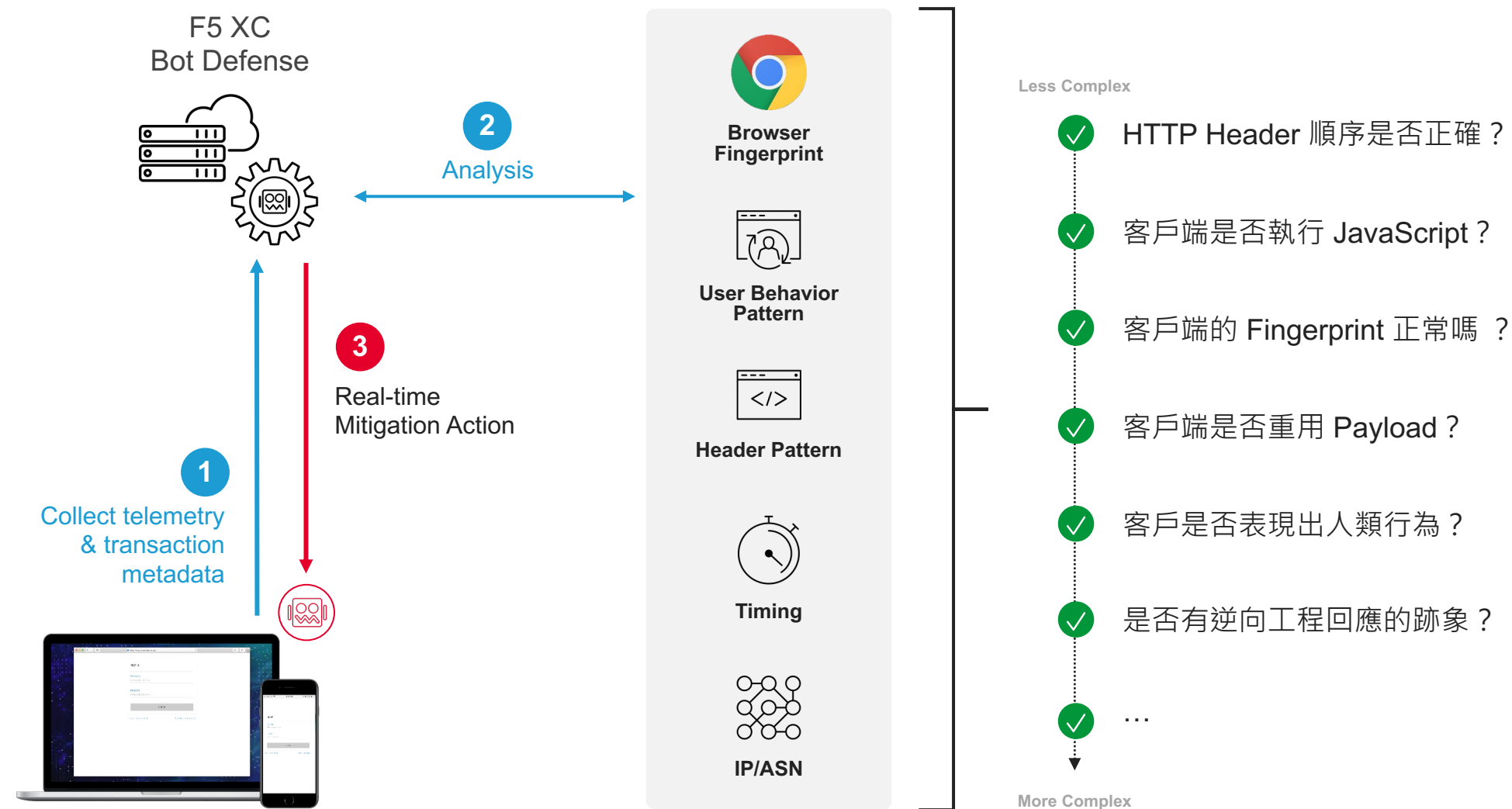
連接您需要的方式和地點  
使用基於 BGP 的流量重定向和直接連接、對等互連或 GRE 隧道。



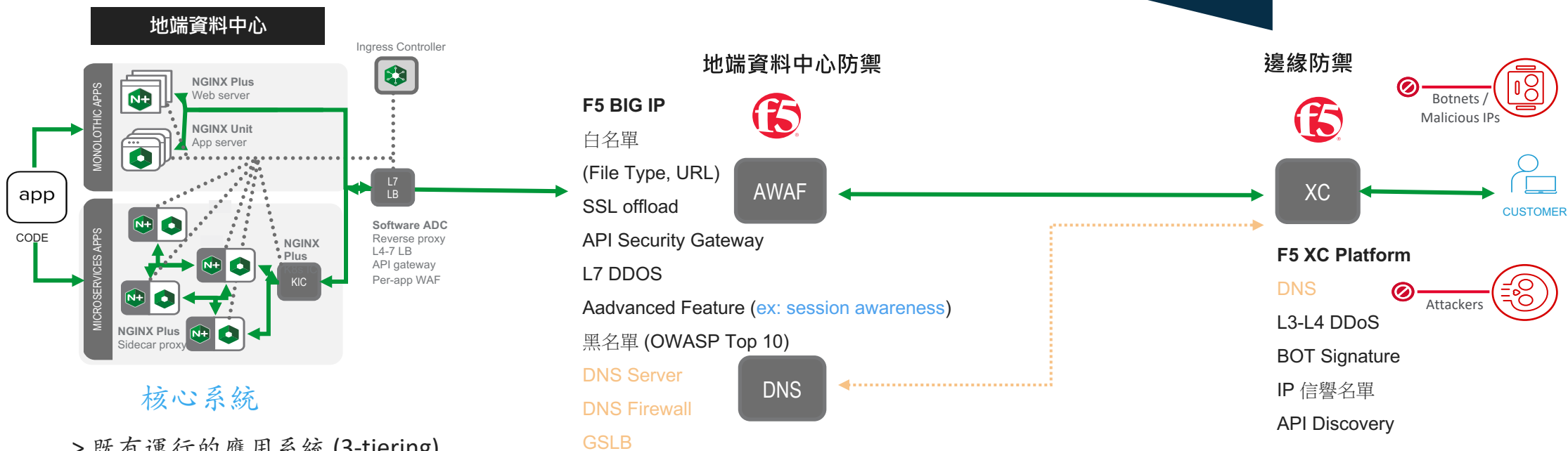
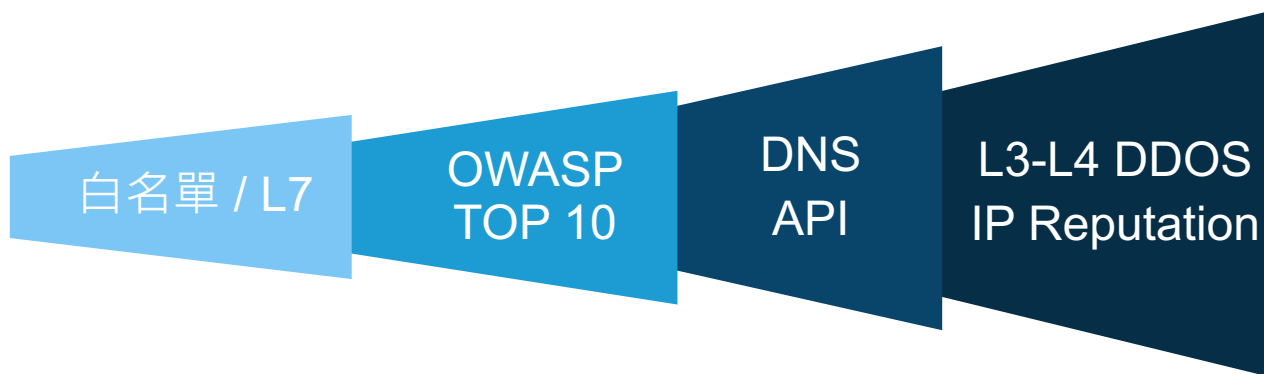
Note: Network PoPs without network lines are planned.  
Standard DDoS Service offering MSA specifies a 15 Minute Response SLA.

# 打造動態安全防禦架構，迎戰自動化攻擊時代

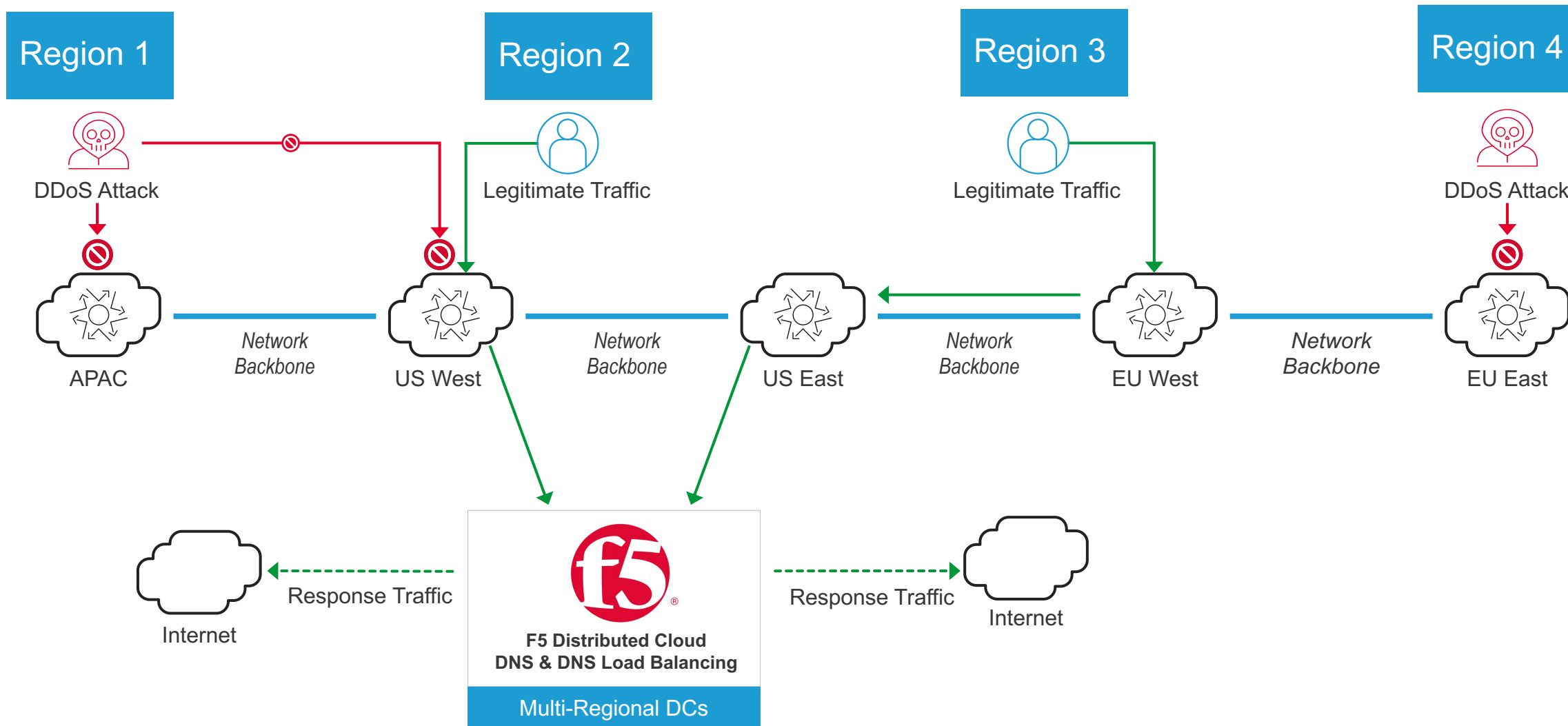
高效的實時檢測通知緩解措施



# 域名解析服務延伸：XC DNS + BIG-IP DNS

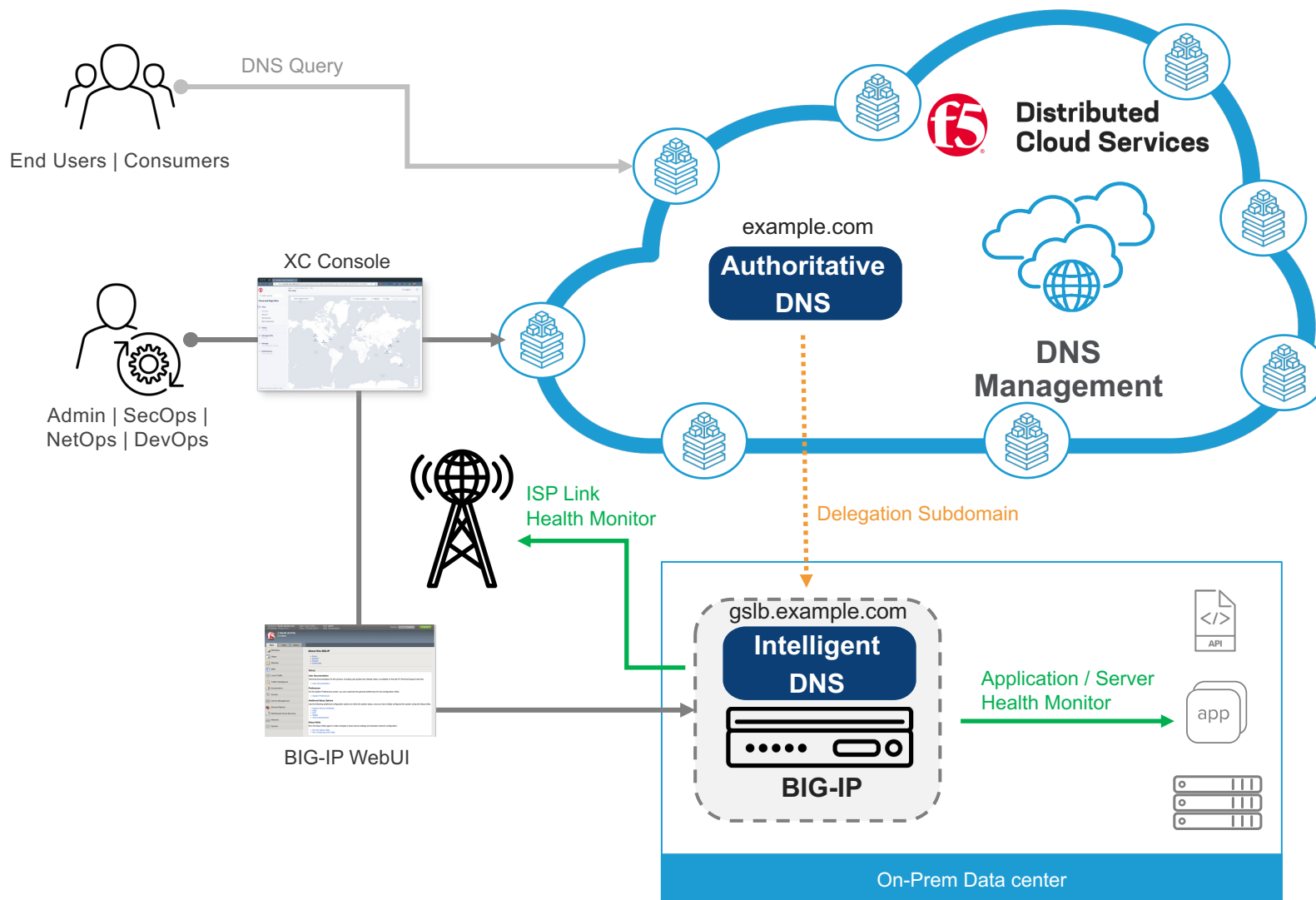


# 將 DNS 服務延伸結合強大的韌性架構

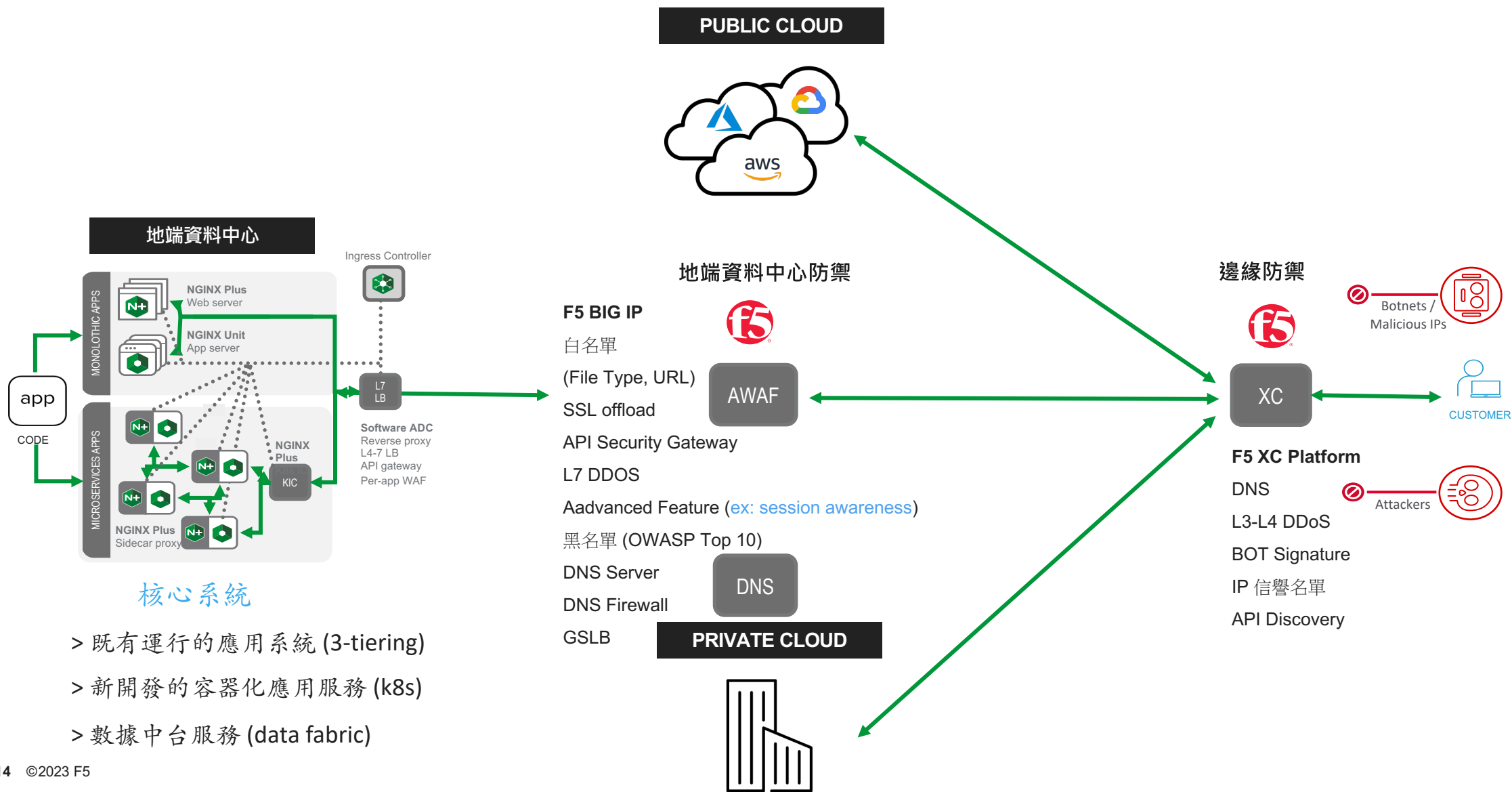


# XC DNS + BIG-IP DNS

- **F5 Distributed Cloud (XC)** 提供代管權威 DNS 服務
- **F5 BIG-IP** 作為智能 DNS 解析探測結點。能針對應用以及線路進行細緻的可用性探測
- 可將需要智能解析的記錄委派至 **F5 BIG-IP**，同時其他 DNS 記錄由 **F5 XC** 進行解析。這樣提供了更靈活和智能的 DNS 發布能力
- 不論是 **XC (DNSaaS)** 還是 **BIG-IP (DNS Express)**，都是高效能的名稱解析伺服器，同時具備對抗 **DNS DDoS** 攻擊的防護能力
- 所有控制平台均提供 **API** 介面，方便進行自動化工作整合



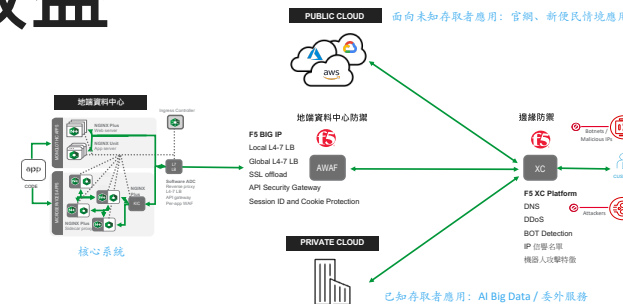
# 靈活彈性的安全架構，保護任何場景中的應用服務



- > 既有運行的應用系統 (3-tiering)
- > 新開發的容器化應用服務 (k8s)
- > 數據中台服務 (data fabric)

# 雙層式 WAAP/DNS 治理數位資安韌性架構效益

## F5 BIG-IP AWAFF + XC WAAP Security Platform



### 效益 1

#### 良好的資安縱深防禦

完整的縱深防禦策略將幫助您應對多樣化的資安挑戰。透過 **BIG-IP AWAFF** 和 **XC WAAP** 安全平台，建立多層次的防護，包括強化網路和應用的安全，采用先進的分析技術來檢測異常行為，以建立數位資安韌性，您將能夠更好地應對和減輕不同類型的攻擊。同時，確保資安資源的適當配置，以確保最大程度的保護和回應能力。

### 效益 2

#### 地端 DNS 延伸並整合安全

**DNS** 扮演機關單位網路門牌號碼的關鍵角色，是使用者在數位服務中存取機關應用服務的第一步，透過 **XC platform Secondary DNS** 與地端 **Primary DNS** 整合式的架構，不僅可以抵擋駭客發動對 **DNS** 各種攻擊，並可以維持現有 **DNS** 維運的方式，地雲整合 **DNS** 實現資安強大韌性，並延伸地端既有之管理效益。

### 效益 3

#### 阻絕 DDoS 攻擊於邊境

駭客偶發性的攻擊具有二個特性，火大強大以及針對性，透過世界級的骨幹資安防禦邊緣運算架構，將駭客攻擊的戰場拉至邊境，阻絕 **L3-L7 DDoS** 攻擊，將駭客阻擋在第一層邊境，透過地雲整合實現了機關善用智慧前瞻科技主動抵禦潛在威脅的目標，達成制敵先機阻絕攻擊於邊境的具體措施，並建構資安政策分層治理的管理框架。

