F5 Distributed Cloud Service - WAAP
隨雲而生的F5 WAAP安全方案

Solution Consultant, F5 Inc.

Jeffrey Ou


應用服務正在發展並變得
越來越複雜….
Security & Attack
Is Changing….

如今，應用服務已成為我們日常生活方面不可或缺的...

應用影響著我們的

吃飯方式

應用影響著我們的

出行方式

應用影響著我們的

溝通方式

新冠疫情更是提升了應用的重要性

應用影響著我們的

工作方式

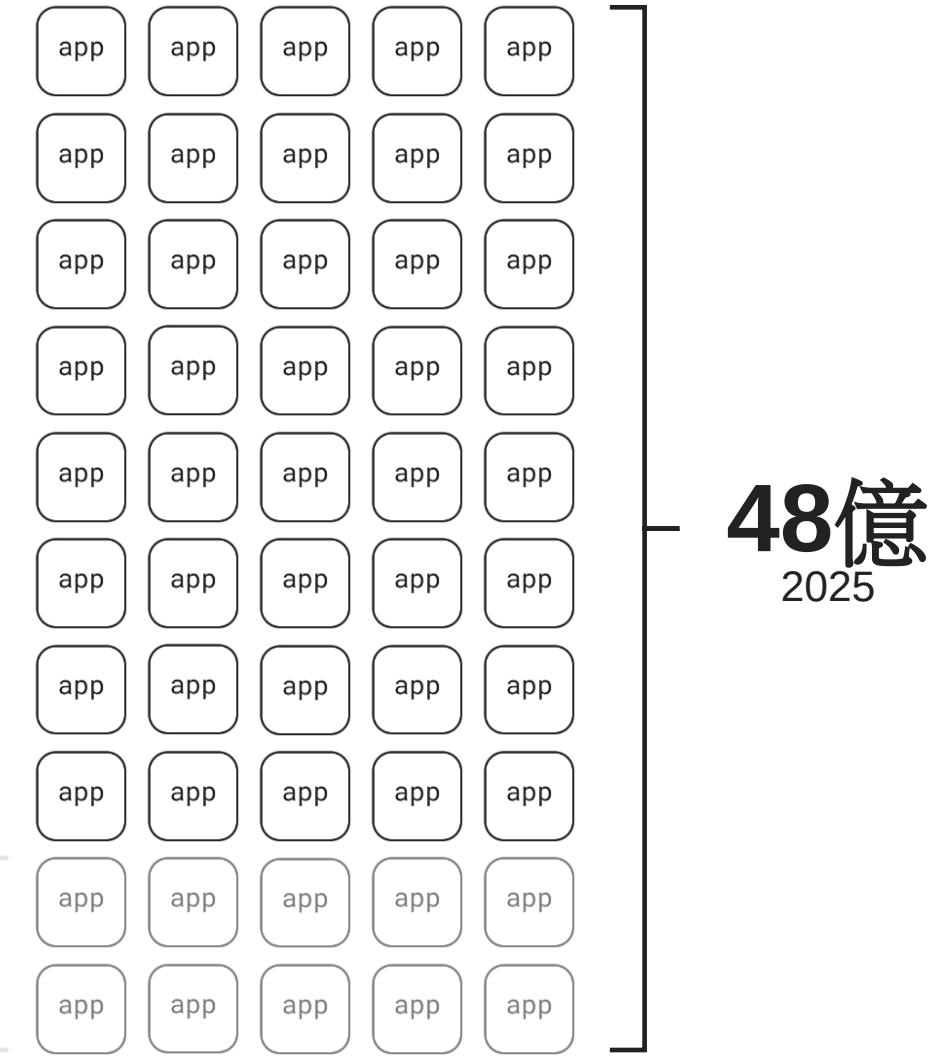
應用影響著我們的

支付方式

應用影響著我們的

娛樂方式

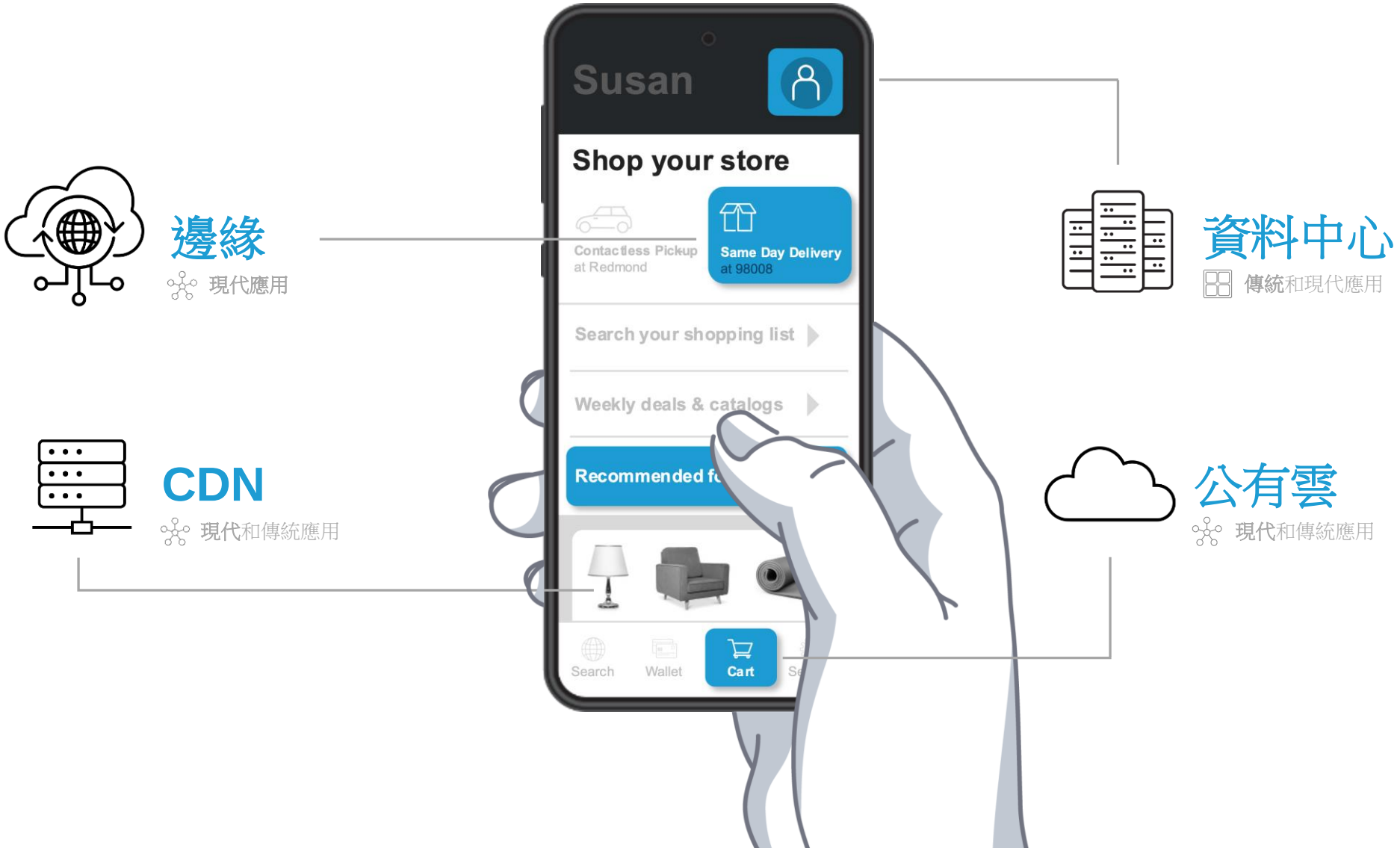
應用服務的數量在**爆炸式增長**



5x
迅速增長

引用來源：IDC, 2021

由傳統和現代應用所組成的數位體驗中，涉及到了多個橫跨本地到邊緣的應用資源..



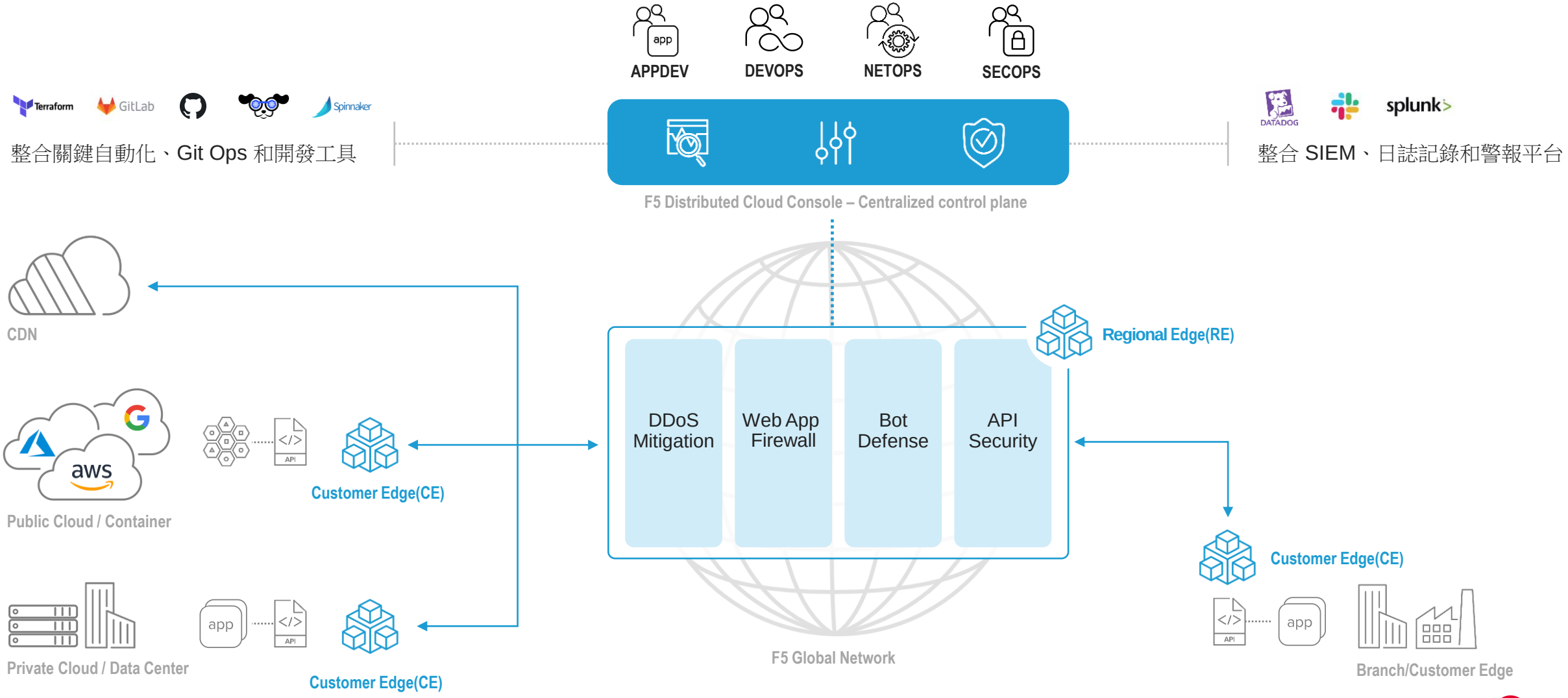
在這些數位化應用服務體驗的背後，有一個易遭受大規模的安全性漏洞的系統...

碎片化　不一致　難以擴展　流動受阻的資料　易於遭受攻擊

This graphic is illustrative and not meant to be an exhaustive list of all providers

隨雲而生的F5 Distributed Cloud Platform - WAAP安全方案

安全政策集中控制，K8S PaaS平台微服務安全靈活部署F5 Distributed Cloud(RE / CE)



緩解大型、複雜的 DoS 攻擊

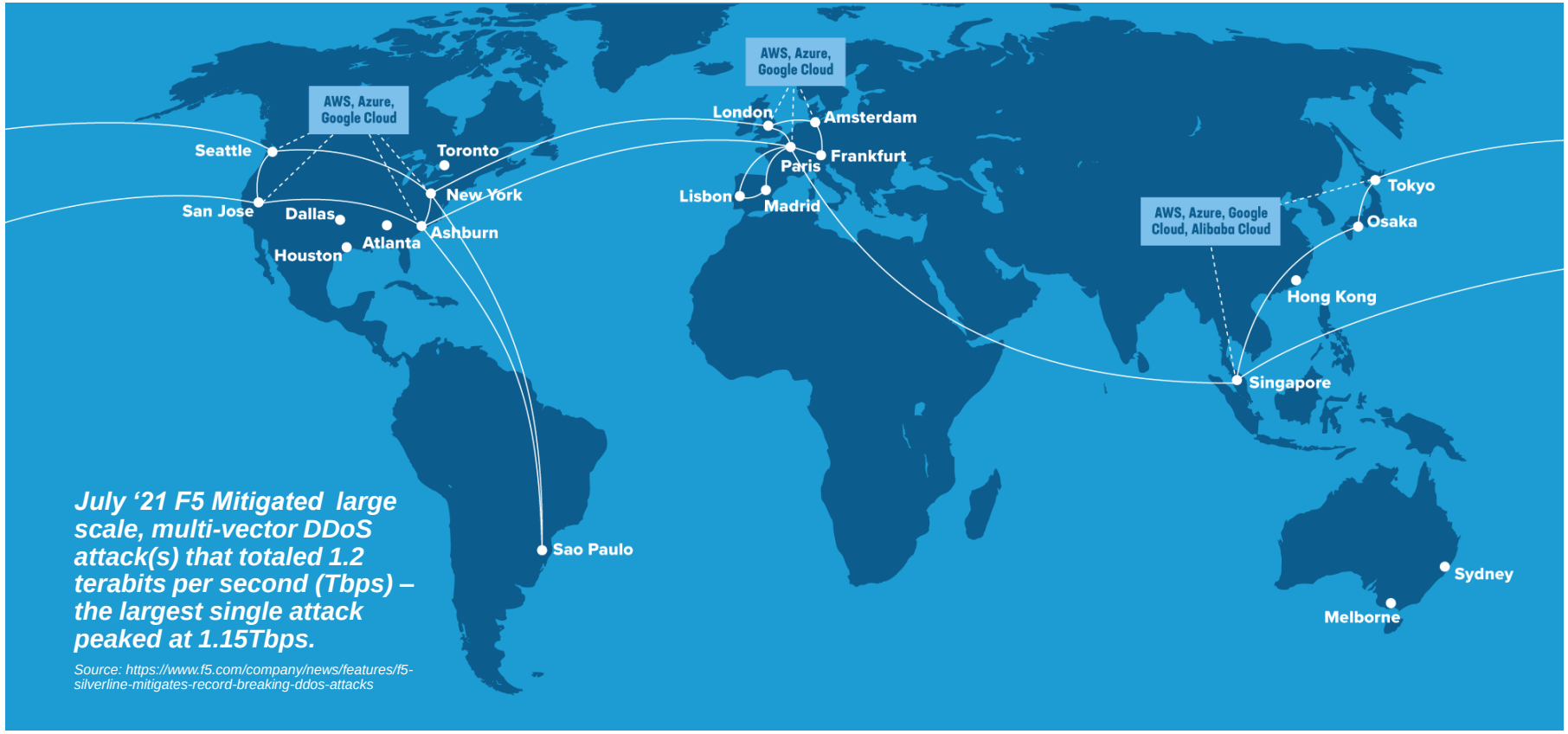
遠離關鍵應用服務和基礎設施，防禦更接近攻擊源頭

世界級的全球安全運營中心
平均在不到 2 分鐘的時間響應DDoS攻擊

全球 DDoS 保護網絡
具有 12+ 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。

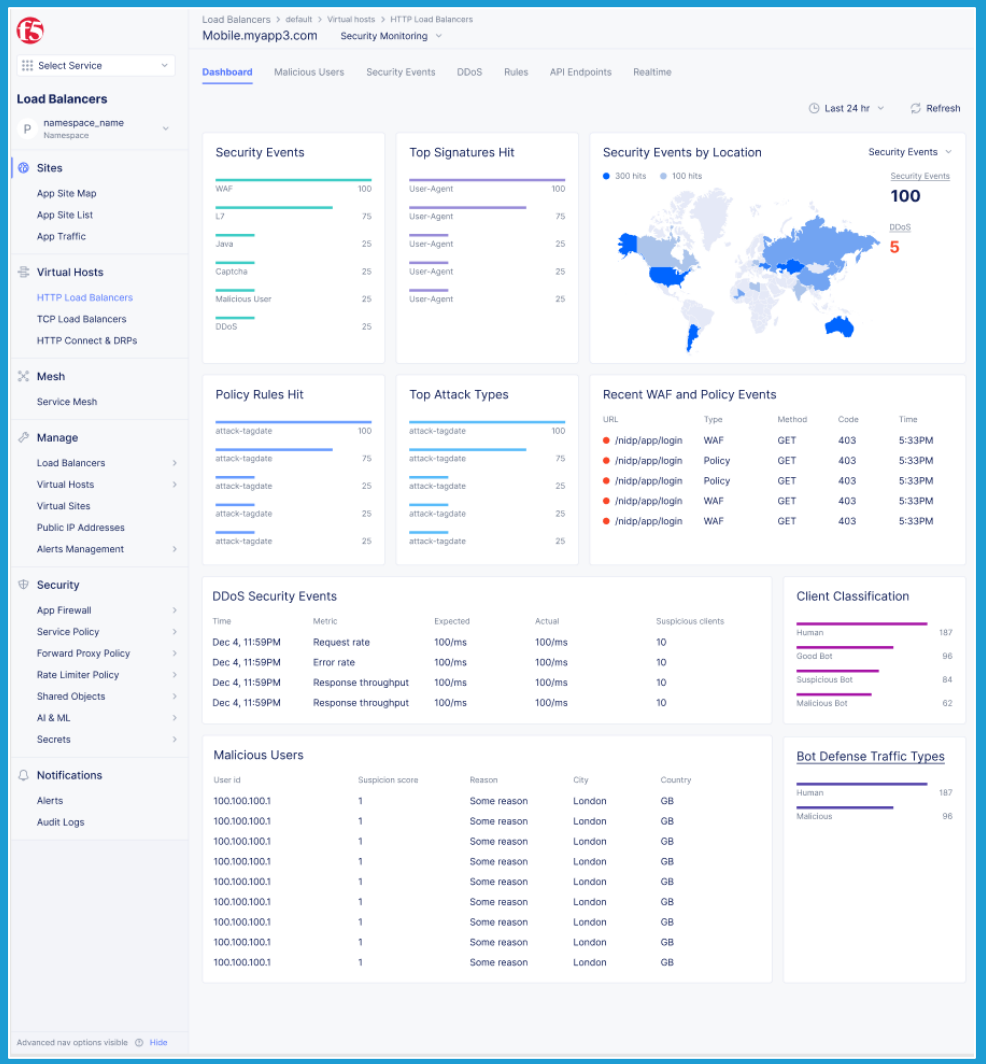


Note: Network PoPs without network lines are planned.
Standard DDoS Service offering MSA specifies a 15 Minute Response SLA.

A Next Gen WAF
新世代應用服務防火牆

提供高效安全性、低誤判

- 通過簡單的 UI 簡化設置和管理，或通過 API 實現自動化，包括最佳實踐保護機制和創建自定義規則的靈活性
- 強大的特徵資料庫引擎包含超過 7,000 個 CVE 簽名，用於 F5 Lab 支持的已知漏洞/技術
- 高級行為檢查引擎，了解特定客戶端與其他客戶端的比較，分析 WAF 規則命中的數量、禁止訪問嘗試、登錄失敗、請求和錯誤率等。
- 強大的安全服務策略引擎，帶有 IP 信譽資料庫和允許/拒絕列表，允許配置阻止來自可疑國家、ASN 等的具有已知錯誤 TLS Fingerprint 的客戶端IP。
- 自動攻擊特徵調整用於確定特徵識別的攻擊是否真的是威脅，有助於減少誤報



Better visibility for security events and traffic with drilldown

Bot 惡意自動化攻擊部署

- 支持全站點保護
- 支持針對特定URL的Bot擴展防禦安全性

用戶行為分析和基於特徵的機器人檢測

Good

- 包含在 **WAF** 服務中
- 通過匹配特徵或識別異常行為來識別機器人
- 利用機器學習/人工智能引擎
- 保護 **Web** 內容和 **API**

Bot Defense

Best

- 針對特定自動化攻擊行為提供進階配置選項
- 旨在保護網站或 API 的高度敏感部分，例如登入頁面
- 更豐富的特定威脅檢測集，可識別諸如爬蟲抓取、ATO 、撞庫等攻擊
- 已知特定威脅的重點惡意活動數據庫

F5 Distributed Cloud API Security
簡化操作自動探索和安全策略管理

OWASP API 完整涵蓋

全面涵蓋 OWASP API 前 10 名漏洞利用，
在發現新漏洞時自動更新。

Automated Discovery

API 經常更改。 在使用 API 時，系統會確定正常行為、使用量、存取方法並檢測異常值，幫助您檢測 API服務。

Importing Swagger

在 API 更新時與 CI/CD 管道整合。 WAAP 將確切知道哪些端點、方法和有效負載是有效的，從而加強安全性以防止濫用。

Determine the Response

根據使用 API 的客戶端其構成的威脅級別進行允許、限制或拒絕。 並允許對可疑和惡意流量進行深入取證。

Response Analysis

WAAP 將分析伺服器如何回應查詢，識別接收錯誤回應代碼但持續發送錯誤請求的異常值。

Behavior and Time

通過分析使用哪些端點、以順序和頻率，
API 保護可以識別不遵守正常行為和行為異常的用戶端。

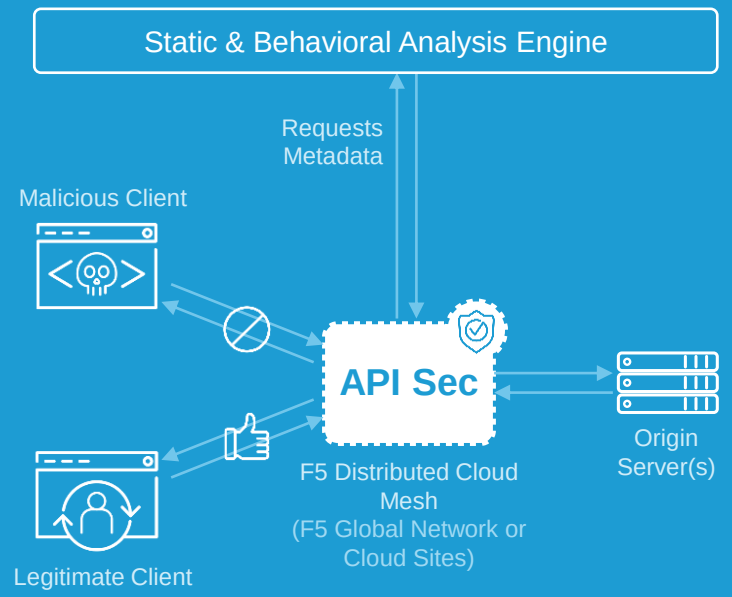
Forensics 追蹤取證

一旦識別出惡意行為者，追踪惡意行為者的歷史行為，並檢視試圖利用的手法與行動。

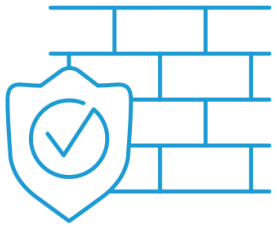
Visualize API Usage

識別 API 的使用模式，關聯好的和壞的使用者活動
以優化 API 以獲得更好的客戶體驗。

Automated API Protection



F5 Distributed Cloud WAAP 重點適用案例



跨多雲/混合環境簡化 應用服務與微服務K8S的安全性

- 管理 Web 應用服務漏洞
- 跨環境的有限的可見性
- 在全球範圍內擴展安全性
- 敏感性資訊洩露
- 保持合規性
- 應用程服務效能低下
- 降低誤判
- 微服務K8S安全性難以統一

消除惡意自動化行為、欺詐和濫用

- 惡意自動流量
- 增加頻寬成本
- Denial of service (DoS)
- 付款欺詐
- Account takeover
- 爬蟲
- Token破解
- 廣告欺詐

管理和保護 API

- 身份和訪問管理
- API 濫用
- 識別Shadow API
- 信息洩露
- 保持API合規性

簡化敏捷應用服務開發的安全性

- 缺乏可編程性/自動化
- 與開發工具的整合有限或困難
- 減緩開發週期和發布
- 應用服務性能低下
- 可擴展性的限制