

Twister5

2025▲

全域視角的威脅預測： AI與資安在數位未來的聯防方案

Twister5 design

極風雲創 林佑儒 Tom Lin

Twister5

2022-2024 年 資安大事件

Twister5 design



●●● DDoS 頻繁攻擊

2022-2024 年資安事件分析

資安事件總覽

- **112 件** 資安事件，於2022-2024 年間。
- **42%** 為網路攻擊，其中多數來自 外部駭客。
- **36%** 為資料侵害
(如個資外洩、勒索軟體)，顯示企業需加強 內部控制與資料保護。

2024 資安事件

- 截至 2024 年 11 月，重大資安事件已達 72 件，超過 2022-2023 年總計 40 件。
- **9-10 月 DDoS 攻擊增加：**
NoName057 親俄駭客團體發動大規模 DDoS 攻擊，導致 **DDoS** 相關事件比例升至 10%。

資安威脅對企業影響

資料外洩頻率增加，對企業 訂單與營收造成衝擊。企業需加強 內部資安管理，以降低資安風險。

傳統地端防禦架構面臨的挑戰



- 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

● ● ● 攻擊手法日新月異，單一地端防禦架構略顯不足

各行各業都是駭客攻擊的目標，常見的安全威脅：

現代企業服務需採用
多層防護機制來確保安全。

DDoS攻擊

DDoS攻擊影響網路服務可用性

Zero Day攻擊

未知漏洞或是新型態攻擊行為



DNS DDoS攻擊

攻擊者攻擊企業DNS服務，造成服務癱瘓

WAF、API、Bot 威脅

不同面向的攻擊行為



如何補強地端 地端 WAF 防禦

Twister5 design



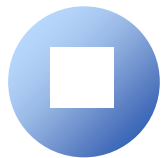
●●● 目前地端 WAF 的侷限性

傳統地端 WAF 雖然能提供應用層防護，但仍有以下弱點：



靜態規則：

WAF 主要依賴手動設定的靜態規則，無法即時適應新型攻擊。



流量擴展性

當遭受大規模 DDoS 攻擊時，仍可能成為瓶頸。



API 安全保護有限

需手動維護 API 安全規則，無法即時發現未授權 API 存取



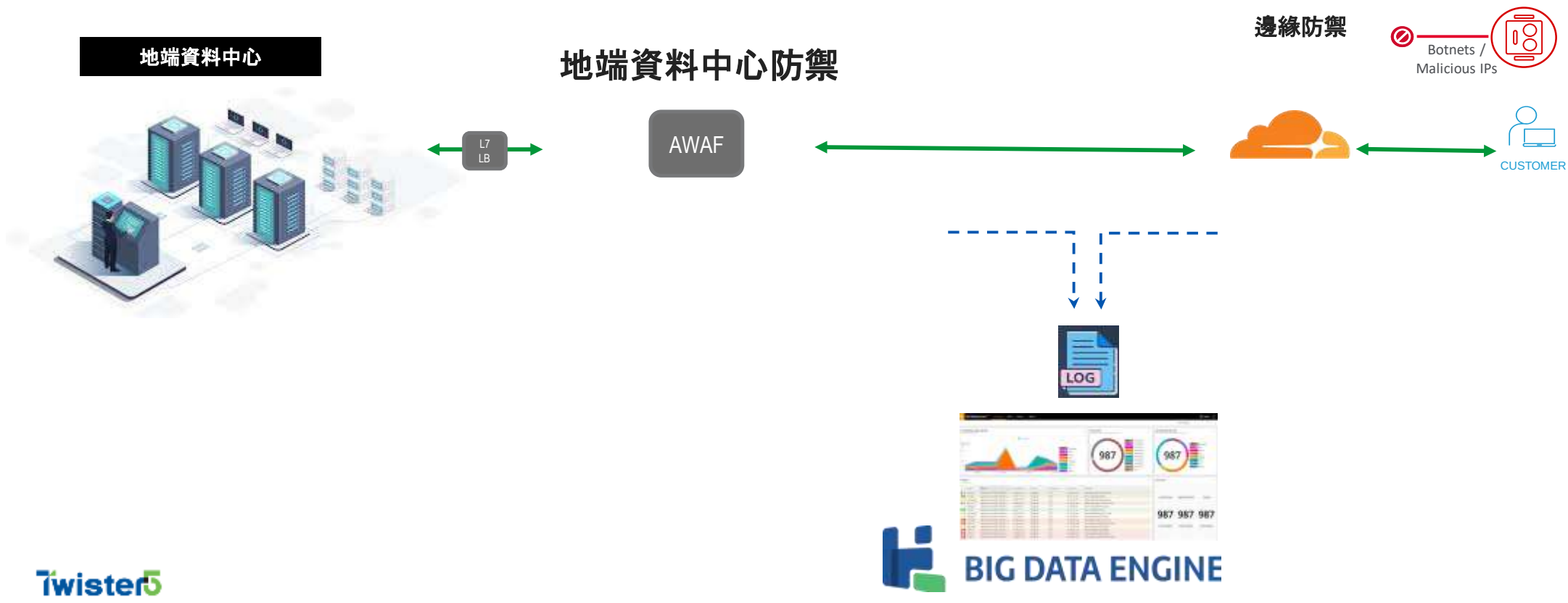
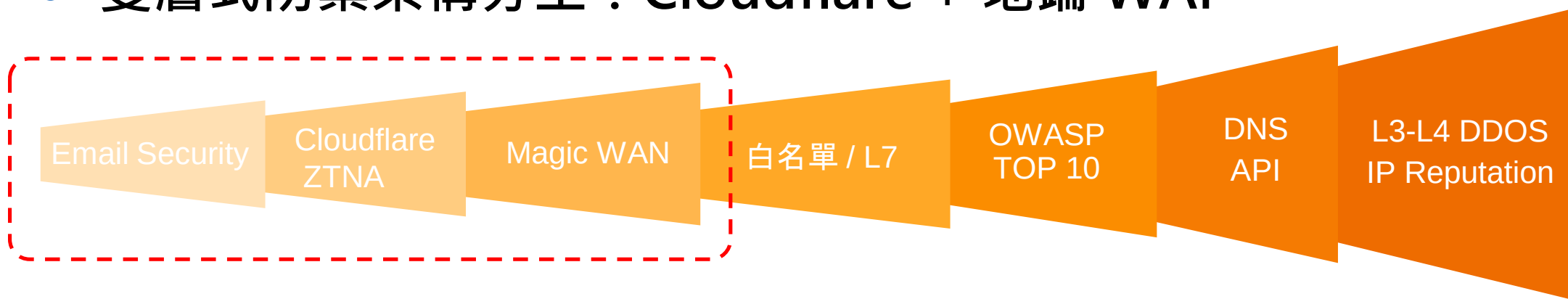
Bot 防禦較弱

難以區分合法使用者與惡意 Bot，易受自動化攻擊影響。

因此，企業需要更靈活、智慧及自動化的防禦機制。



● ● ● 雙層式防禦架構分工：Cloudflare + 地端 WAF



●●● Cloudflare 提供第一層防禦

Cloudflare 提供雲端 AI 驅動的安全防護，成為資安第一防線

智慧型 WAF

自動更新防禦規則（涵蓋 OWASP Top 10），並透過機器學習偵測異常流量。

DNS DDoS 安全保護

採取 Anycast 架構防禦 DNS 服務被中斷，並持續監測 DNS 流量，以提升整體網路安全性。

01

02

03

04

DDoS 防禦能力

全球 Anycast 網路可吸收超過 300 Tbps 的攻擊流量。

API、Bot 防禦

自動發掘 API，防止 API 濫用與未授權存取
精準區分人類與 Bot，阻擋惡意流量

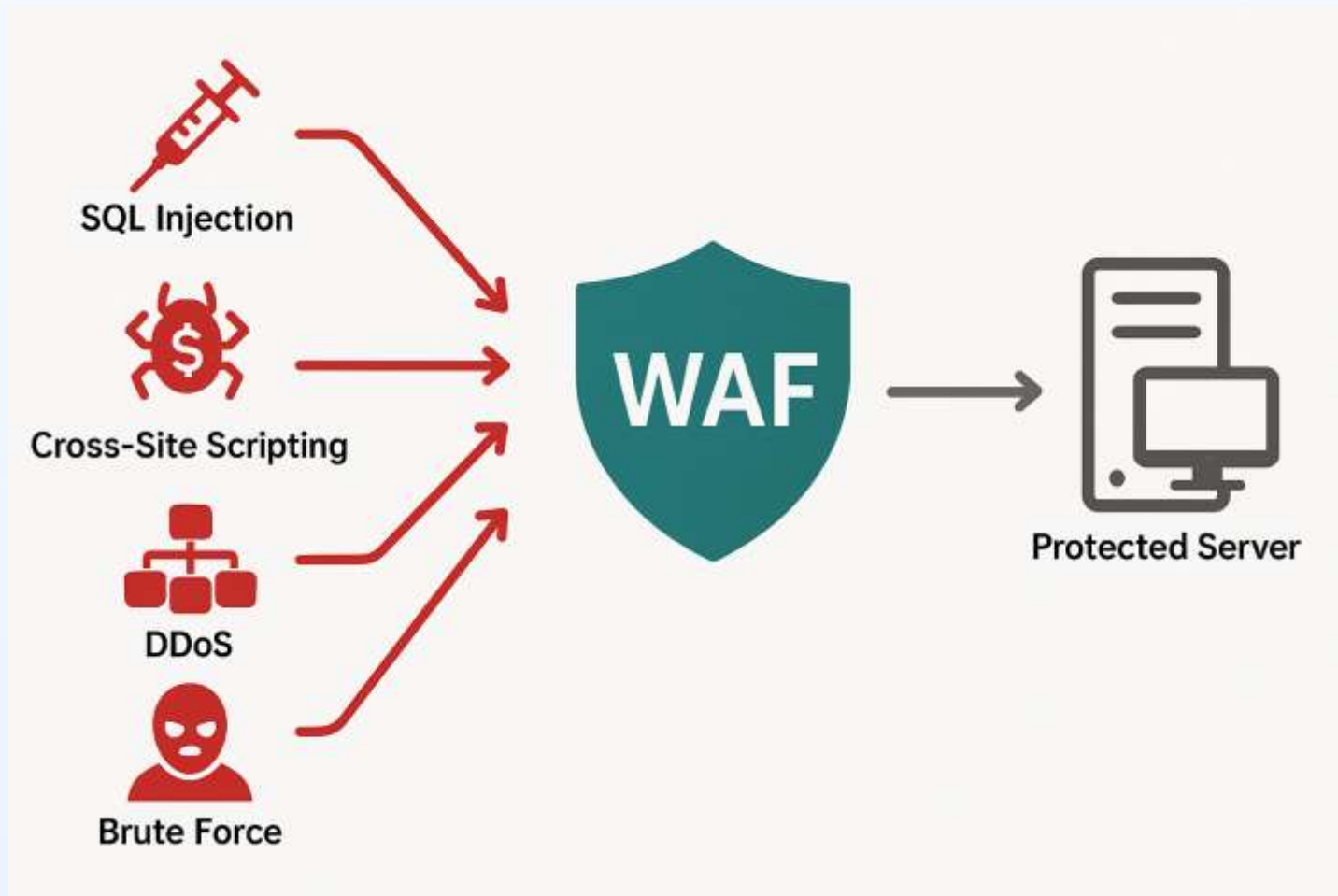


Twister5

極風雲創 應用資安解決方案

Twister5 design

●●● 全台**首家(唯一)**應用資安防禦訂閱制提供商



Cloud WAF 是雲端網頁應用 防火牆服務：

雲端訂閱制，用多少付多少

不須採購任何設備

不改變既有環境

無需安裝任何程式

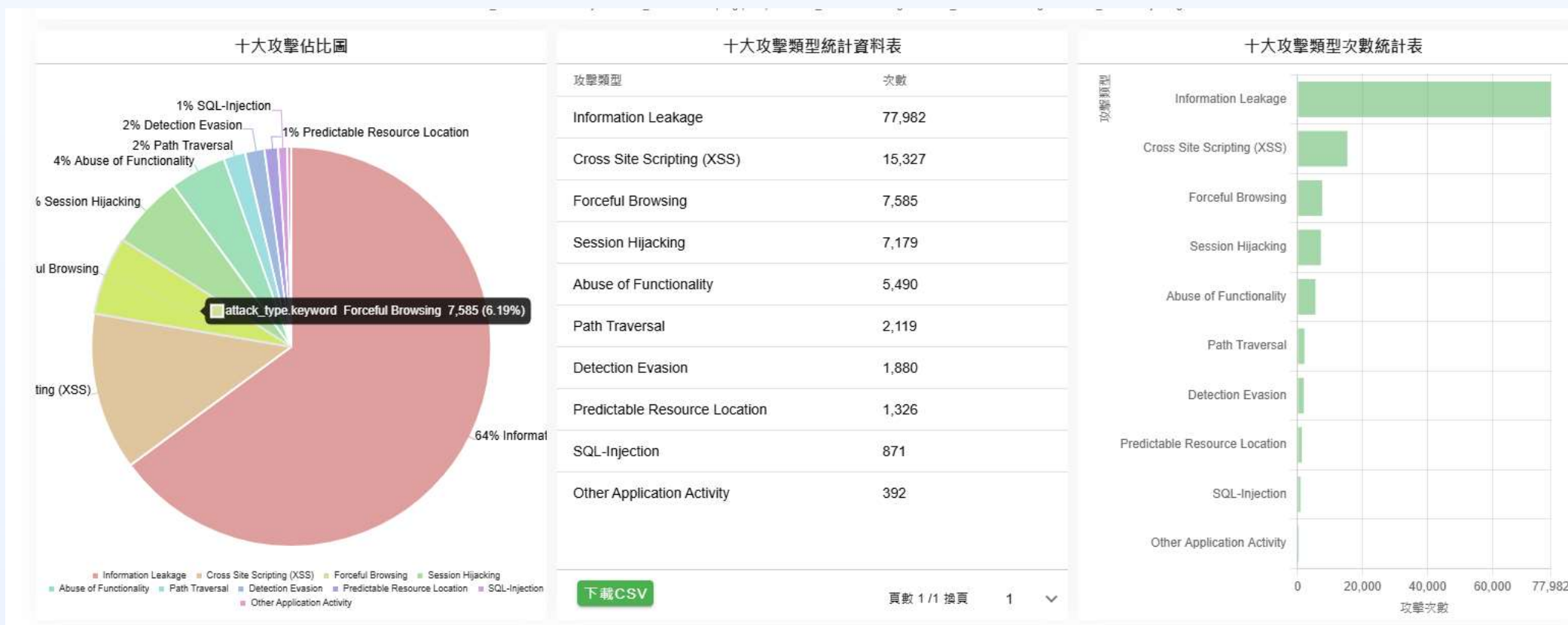
不須更改既有網站

即可享有網站防護服務

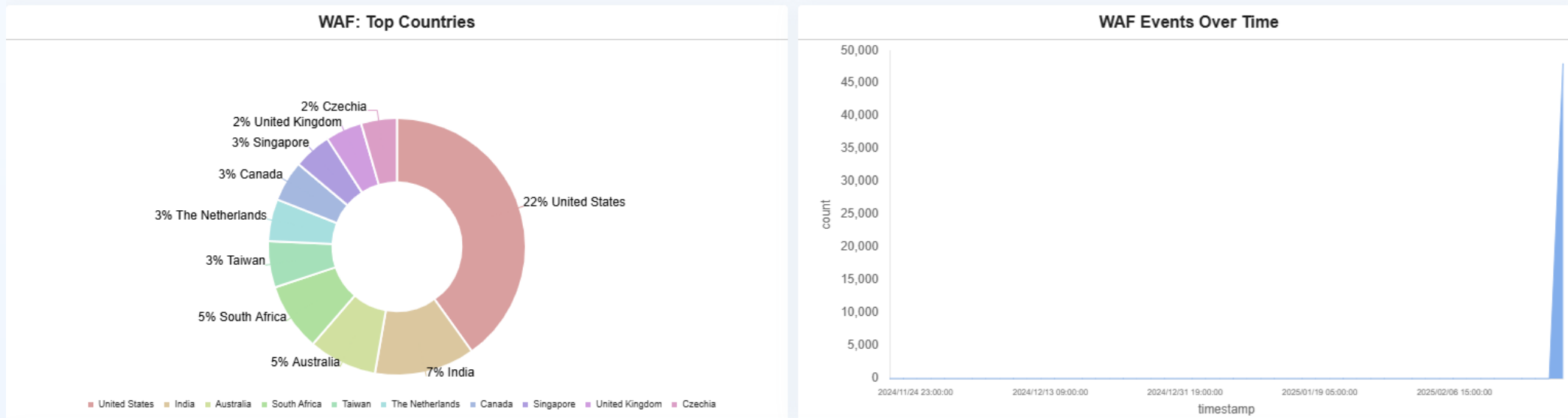
●●● 獨家整合式地/雲 log 監控模組-發現攻擊樣態

BDE可以提供地端WAF設備發現的攻擊樣態

以作為未來Cloudflare資安政策調整或是模組採購之依據



獨家整合式地/雲 log 監控模組-發現攻擊樣態



HOST	IP	Port	次數 ↓
erp.twister5.cf	2402:7500:477:e1cb:e1ab:7c48:cae2:7156	57872	244
erp.twister5.cf	1.163.231.21	57086	87
aichat.twister5.cf	1.34.61.17	13759	22
aichat.twister5.cf	185.213.155.171	53190	18
aichat.twister5.cf	104.253.203.35	14056	18
nuxt5.twister5.cf	54.188.190.47	54214	18
aichat.twister5.cf	119.13.223.92	36407	18
aichat.twister5.cf	205.169.39.53	33132	16

●●● 獨家整合式地/雲 log監控模組-整合告警平台

新增頻率告警規則

規則名稱

惡意自動化程式

觸發事件量

10

觸發時間區間

1

觸發條件欄位

邏輯判斷

×

bot_signature_categor

!=

+ 增加條件

重新告警頻率

1

告警對象Email

可設定多組Email，請用逗號(,)分隔



2020/3/25 (週三) 下午 05:45

wafreport@twister5.com.tw

ElastAlert: a5e308b0-2602-46a6-a195-9b9964e0e2d2

收件者 ivan.tsai@twister5.com.tw

a5e308b0-2602-46a6-a195-9b9964e0e2d2

At least 20 events occurred between 2020-03-25 13:44 CST and 2020-03-25 17:44 CST

@timestamp: 2020-03-25T09:44:49Z

@version: 1

_id: kI4UEXEBBpJwfhxzhKGI

_index: logstash-asm-index-2020.03.25

_type: asm-log

attack_type: Forceful Browsing

client_ip: 10.10.10.1

client_port: 49402

dest_ip: 10.10.10.100

dest_port: 80

geo_location: N/A

您可以定義事件、頻率、關鍵字、門檻值等項目的政策以觸發告警機制。

- 日誌量頻率超標
- 特殊事件告警
- 設備狀態異常告警
- 事件連續觸發告警
- 支援E-Mail、Line
- 依權限進行告警配置

●●● 獨家整合式地/雲 log 監控模組-長時間保存週期



Cloudflare提供有限的Log保存週期

BDE可以提供3年甚至更久週期log的保存





資安智能平台即服務 生成式AI應用願景

Twister5 design



●●● 資安智能平台即服務 - 激發人類想象力的全新高度

◆ 辨識使用者操作行為是核心優勢

- 匯集各種網站的訪問類型、使用者的操作行為、連線頻率等資訊。
- 收集的資訊經正規及去識別化後，可以代表一個環境領域的現況與趨勢。

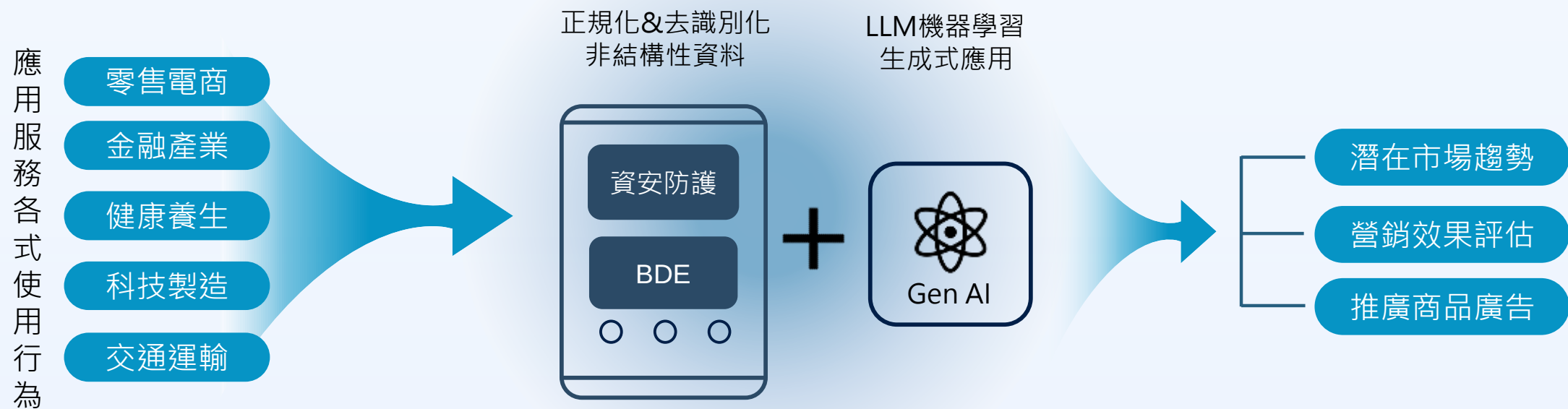
◆ AI 讓大數據不再只是垃圾

- 快速分析大量數據，辨識出難以察覺的模式和趨勢，提供更具深度的洞察力。
- 透過機器學習和深度學習演算法，根據歷史數據進行預測，幫助管理者提前做出資安決策。
- 大數據轉化為個性化的建議和方案，提升使用者體驗。

◆ 生成式 AI 讓未來應用有無限可能

- 生成式 AI 結合創造力與技術，能生成文本、圖像、音樂等內容，突破傳統應用框架。從個性化設計到智能創作，為未來教育、娛樂、醫療等領域都能帶來無限可能。
- 從品質管控、營運管理、產品包裝、銷售預測、行銷推廣、績效評估、加值服務到第三方廣告銷售等應用領域，將可以透過 BDE.ai 創造更不同面向的價值。

資安智能平台即服務 生成式應用願景



資安智能平台即服務 - 生成式應用示意 I

E-Commerce

Apple Pay

1,738

769.00%

Google Pay

1,544

129.08%

Samsung Pay

824

-7.62%

街口支付

928

2.32%

Line Pay

441

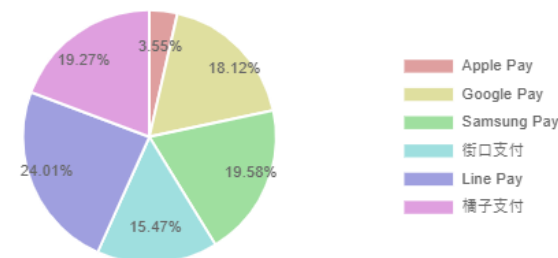
-78.83%

橘子支付

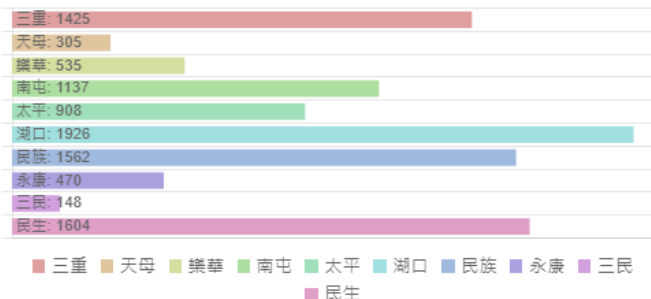
1,912

90.25%

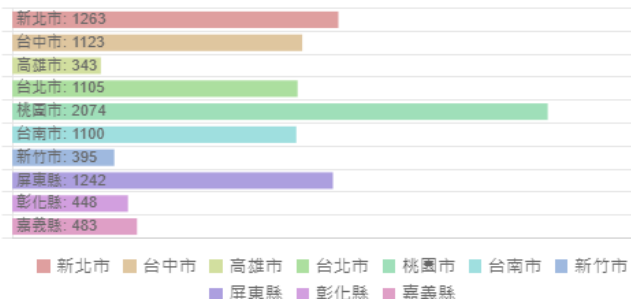
API Dashboard Calls by Server



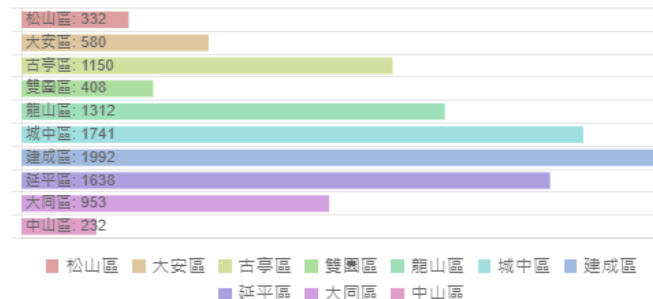
交易金額



城市 TOP 10



區域 TOP 10



會員編號	城市	地區	支付方式	支付金額	支付交易碼	商店名稱
yn-bg6DdZF	新竹市	松山區	Apple Pay	3658	HHYZ8_WODJxU3-G	藝奇
_hg_g51ael	新竹市	中山區	橘子支付	4497	aLG3cKwXOt8nn7d	夏慕尼
ehDwx7_XiU	新竹市	雙園區	街口支付	1373	-0QTICnhVagWjOj	石二鍋
9tfLKbj564	台南市	雙園區	街口支付	2505	LukN3f1Kt3v5Vdz	藝奇

●●● 資安智能平台即服務 - 生成式應用示意 II

CXO

交易金額

1,464

-39.14%

交易筆數

1,102

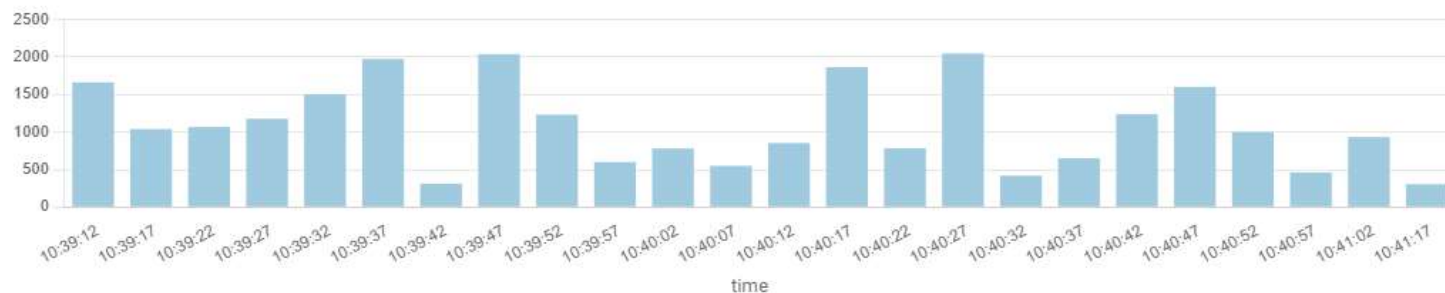
11.16%

在線人數

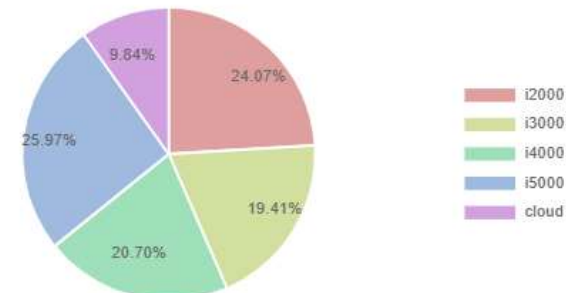
1,543

58.13%

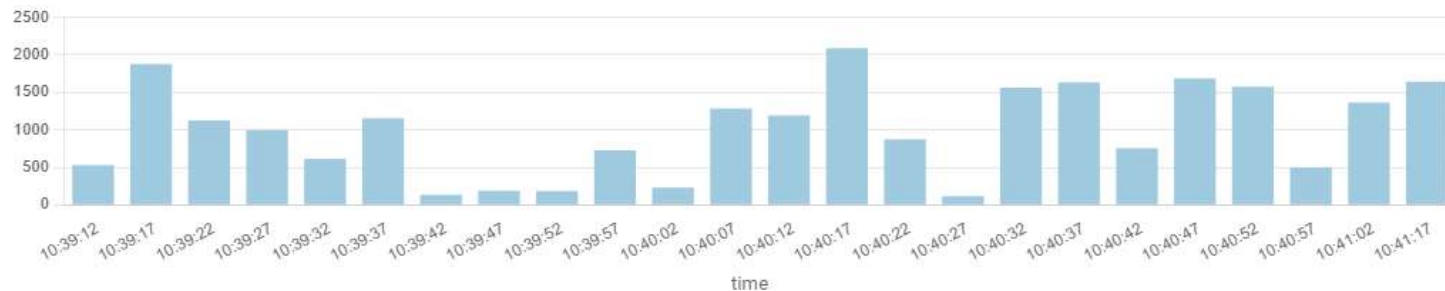
今日交易時序/品項



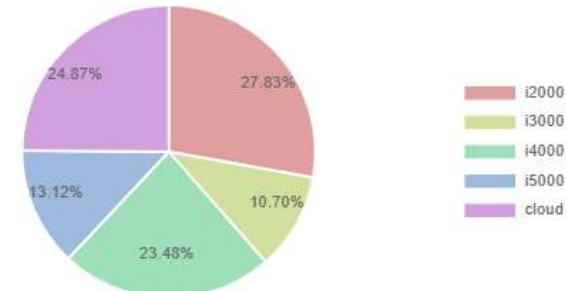
今日交易比例/品項



今日交易時序/品項



今日交易比例/品項



Twister5

2025▲

THNAK YOU

Twister5 design

極風雲創股份有限公司 (股票代號7826)