FortiMail / FortiMail Cloud
郵件閘道 – 更有效快速地回應未知威脅

郵件是駭客發動攻擊的起源

傳統的安全郵件防護已不足以對抗瞬息萬變、層出不窮的 BEC 金融詐騙、勒索軟體、進階持續性滲透攻擊 (APT) 的新型態郵件攻擊

郵件防護 1.0

- 基於內容的電子郵件威脅防禦
  - ☑ 垃圾郵件
  - ☑ 灰色郵件

郵件防護 2.0

- 基於附件的電子郵件威脅防禦
  - ☑ 惡意軟體
  - ☑ 網路釣魚
  - ☑ 深度檔案清洗 (CDR)
  - ☑ 連動沙箱，引爆可疑內容

郵件防護 3.0

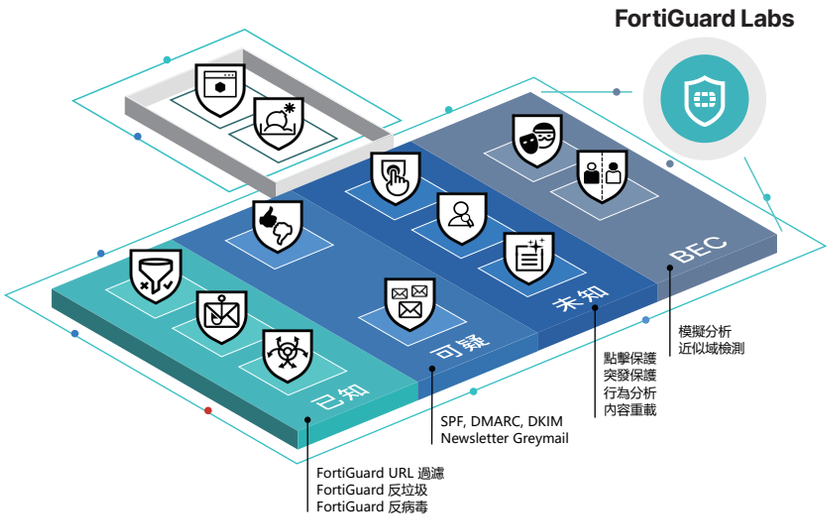
- 基於惡意連結及商務的電子郵件威脅防禦
  - ☑ 惡意網站
  - ☑ 勒索病毒
  - ☑ 利用 Web 作為傳染
  - ☑ 媒介 URL 即時點擊保護 (URL Click Protection)

郵件防護完全體

- 基於整合及連動的電子郵件全面性威脅防禦
  - ☑ FortiIsolator
  - ☑ FortiNDR
  - ☑ 透過 API 介接 Microsoft 365 及 Google Workspace

進階多層式安全防禦

- 已知威脅
- 可疑威脅
- 未知威脅 / 0-Days
- 仿冒嘗試
- 商業郵件洩漏



Fortimail 進階郵件保護機制

- Phishing & Malware
- 沙箱偵測處理
- URL 連結保護
- QR Code 偵測檢查
- 商務郵件檢查
- Community Intelligence – FortiMail Plugin
- 內容偵測 Unwanted Content – Content Analyzer

全方位資安整合功能 & 情境分析

Case 1 員工資安意識薄弱，該如何教育郵件資安意識

FortiPhishing

1. 可以提供社交工程演練機制，製作擬真的釣魚郵件
2. 提供不同等級的釣魚郵件及不同模板，多樣化釣魚郵件測試
3. 統計員工點選率，找出資安意識最薄弱的風險者
4. 可提供及時提醒，達到教育的意義

Case 2 員工不小心點選了惡意郵件，怎麼避免後續問題

FortiIsolator

1. 網頁隔離獨立瀏覽
2. 點選惡意連結不影響本機
3. 檔案預覽，避免下載惡意檔案

FortiSandbox

1. 惡意檔案下載前丟入沙箱分析
2. 提供地端或雲端方案
3. 提供多種底層模擬

Case 3 FortiMail 可與其他資安方案怎麼整合

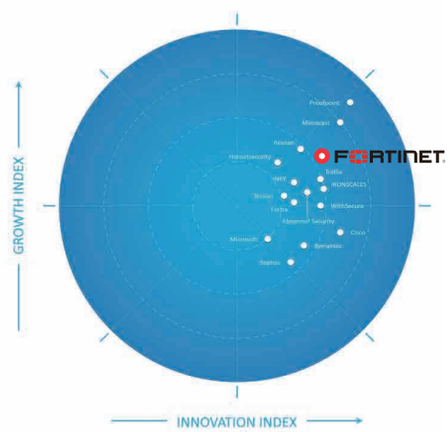
FortiSASE FortiZTNA
零信任方案

1. 整合零信任聯防
2. 全域性的防禦
3. 檔案預覽，避免下載惡意檔案

Fortigate

1. 整合既有 Fortigate
2. 無痛整合既有方案
3. 無需額外程式，即可聯防

選擇 FortiMail : Email Security 領域的領跑者



Frost Radar™: Email Security

SE Labs AAA June 2022 Email Security Services ESS Protection

97% 綜合偵測評比
94% 保護和合規
95% 偵測正確性

vb VERIFIED SPAM + virusbtn.com March 2022

99.97% 垃圾郵件抓捕

vb 100 VIRUS virusbtn.com

100% 病毒偵測

FORTINET®
Fortinet.com/tw

官方網站 | LINE@ | Facebook | YouTube | 與我們聯絡