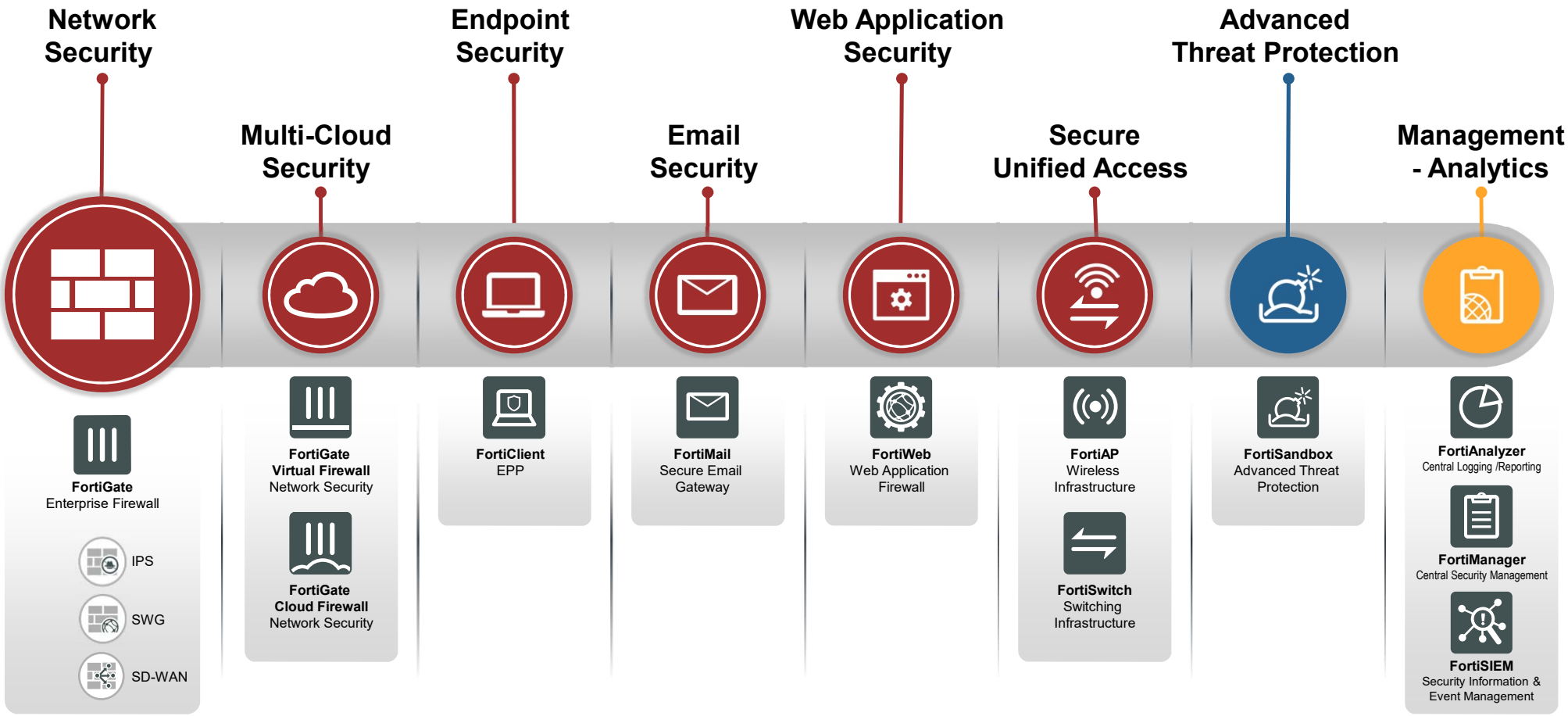
FORTINET

企業全面性的內外網防禦

Security Fabric



Security Is About Securing People

Location

Mobile Device

Port

VLAN

Fortinet 2017年 資安趨勢預測

- 從聰明變得更聰明：自動而人性化的攻擊，將需要更多智慧型的防護
- 物聯網製造商將必須為安全漏洞負責
- 200億個物聯網設備是雲端架構中最弱的一環
- 攻擊者將會開始轉向攻擊智慧城市
- **勒索軟體將導入規模經濟**
- 技術必須彌補重要網路技能的短缺

請參閱：2017 Threat Predictions - by Derek Manky

請參閱： Fortinet預測2017為網路安全引爆年 安全威脅將會更具智能、自主性，而且比以往更難偵測

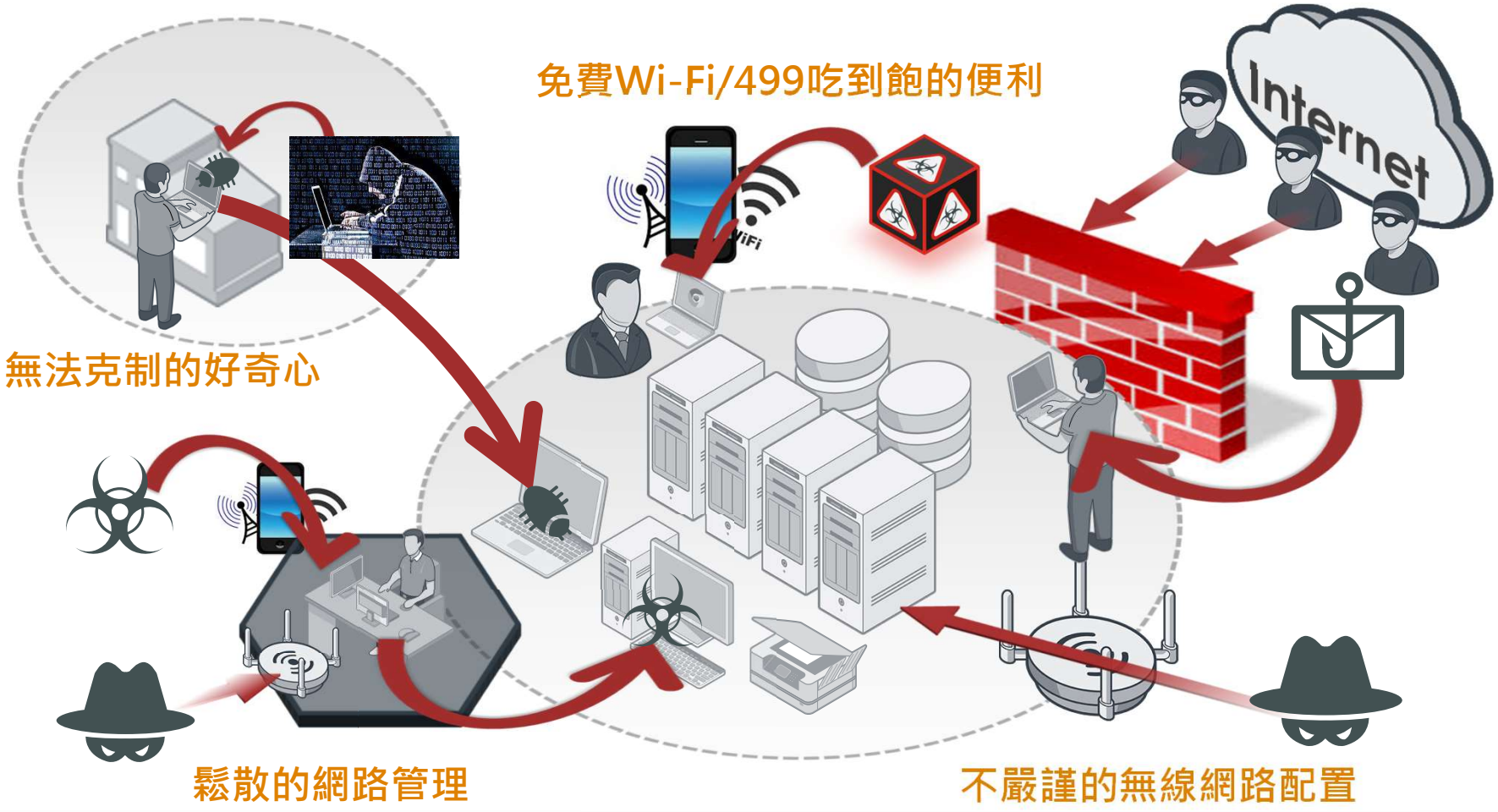
Fortinet 2018年 資安趨勢預測

- 自我學習的Hivenet和Swarmbot威脅的興起
- 綁架雲端商用平台所帶來的商機
- 新世代型態的惡意軟體
- 關鍵基礎架構網路的前端隱憂
- 地下網路與網路犯罪經濟體系將採用 AI 自動化提供服務

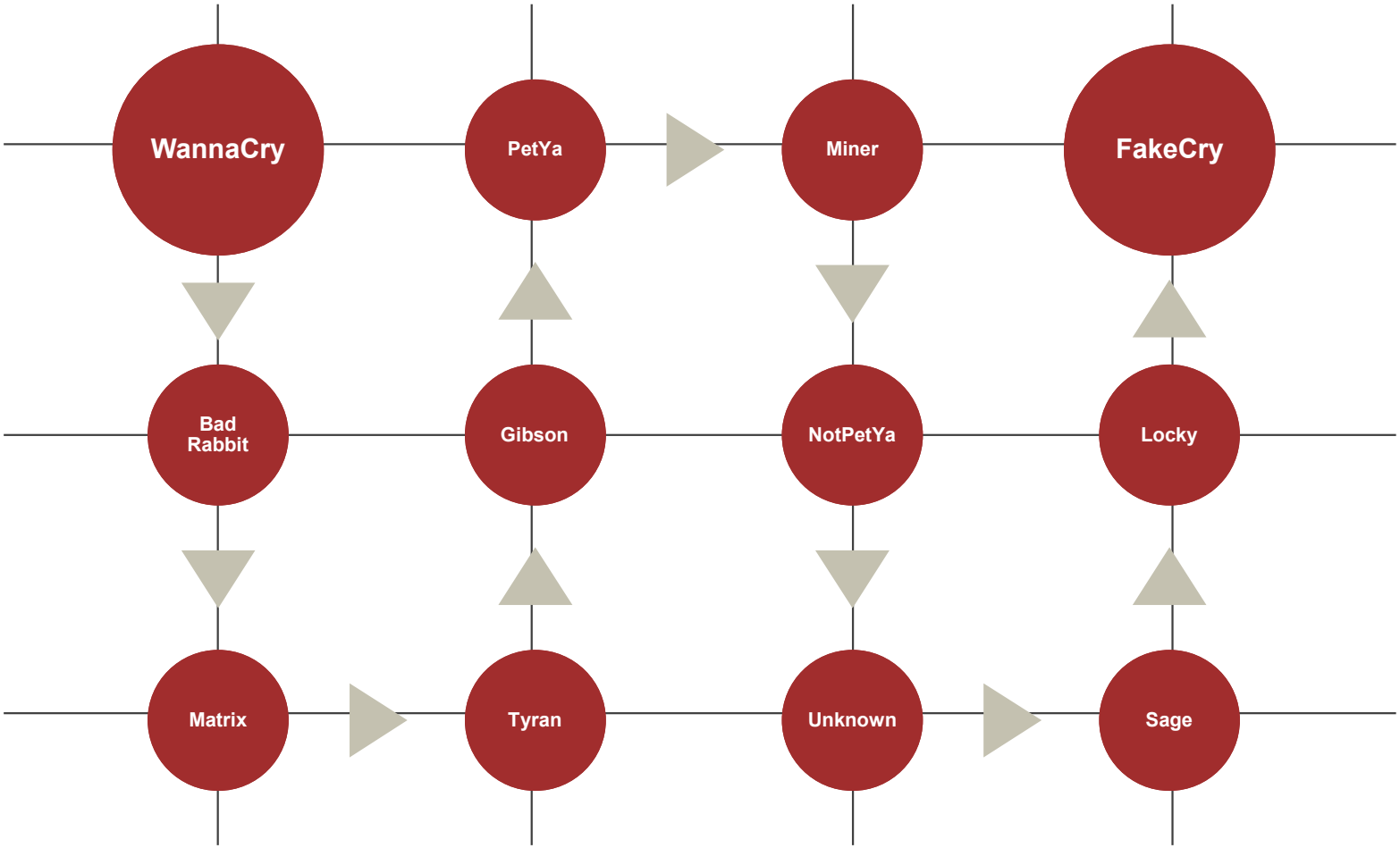
請參閱：2018 Threat Predictions - by Derek Manky

Mid-year 2017 Predictions Update

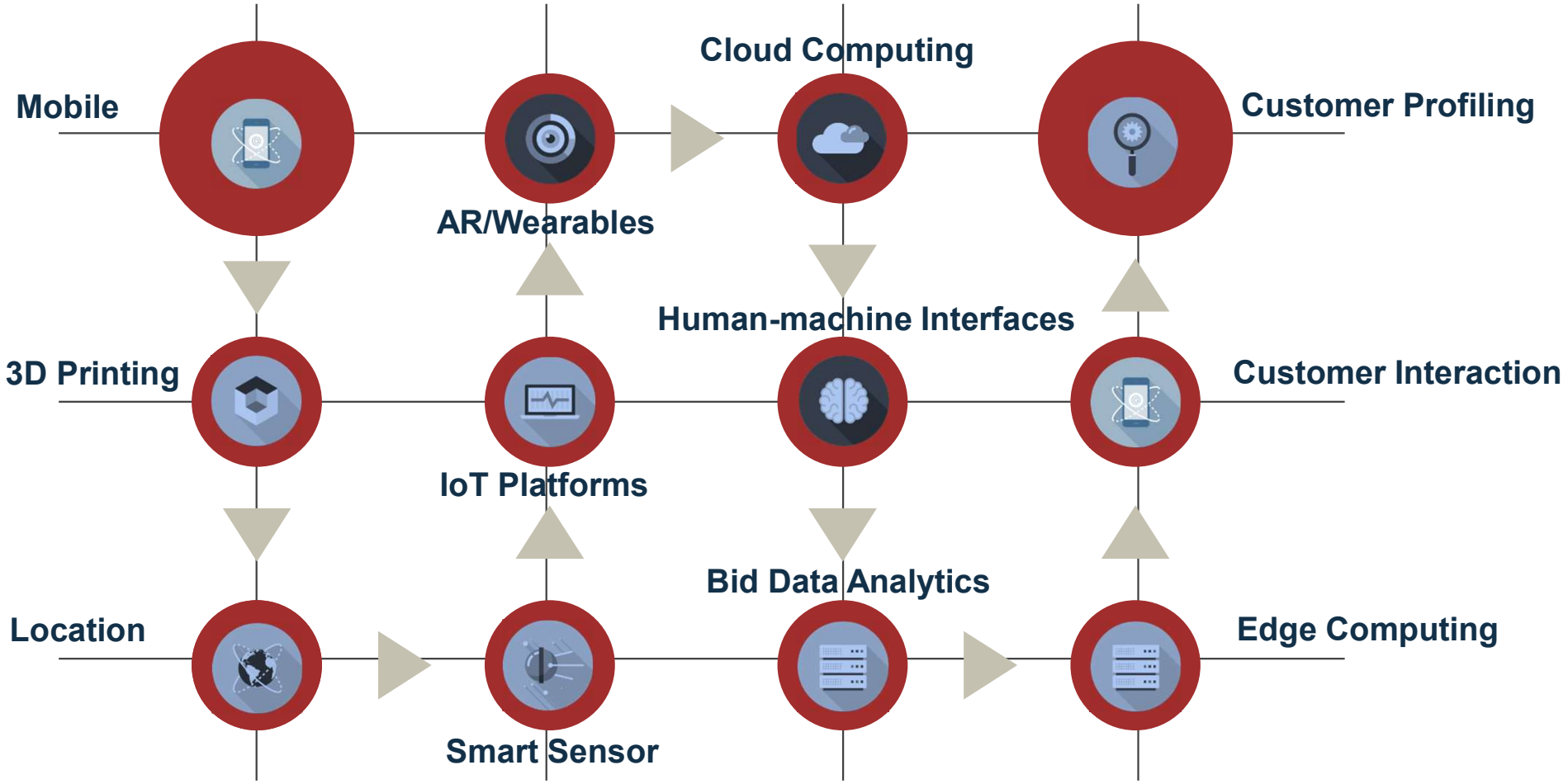
內網安全存取的必要性?



威脅的橫向擴散

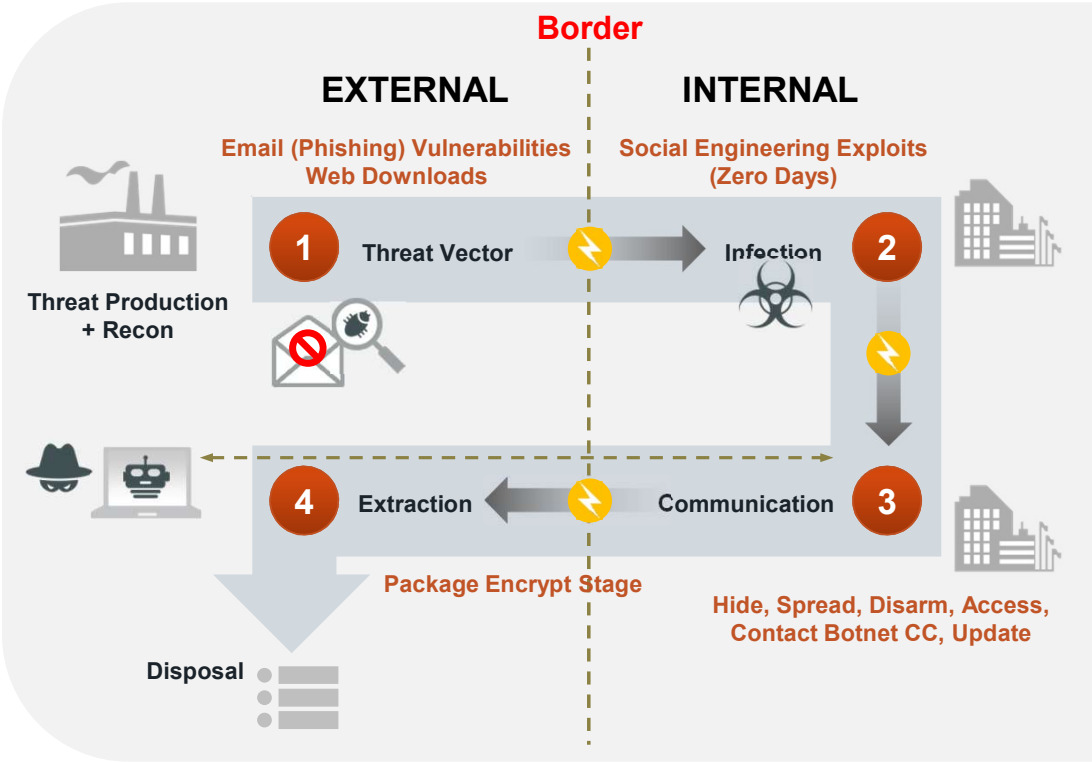

WannaCry
PetYa
Miner
FakeCry
Bad Rabbit
Gibson
NotPetYa
Locky
Matrix
Tyran
Unknown
Sage

橫向擴散的傳播與攻擊不容小覷

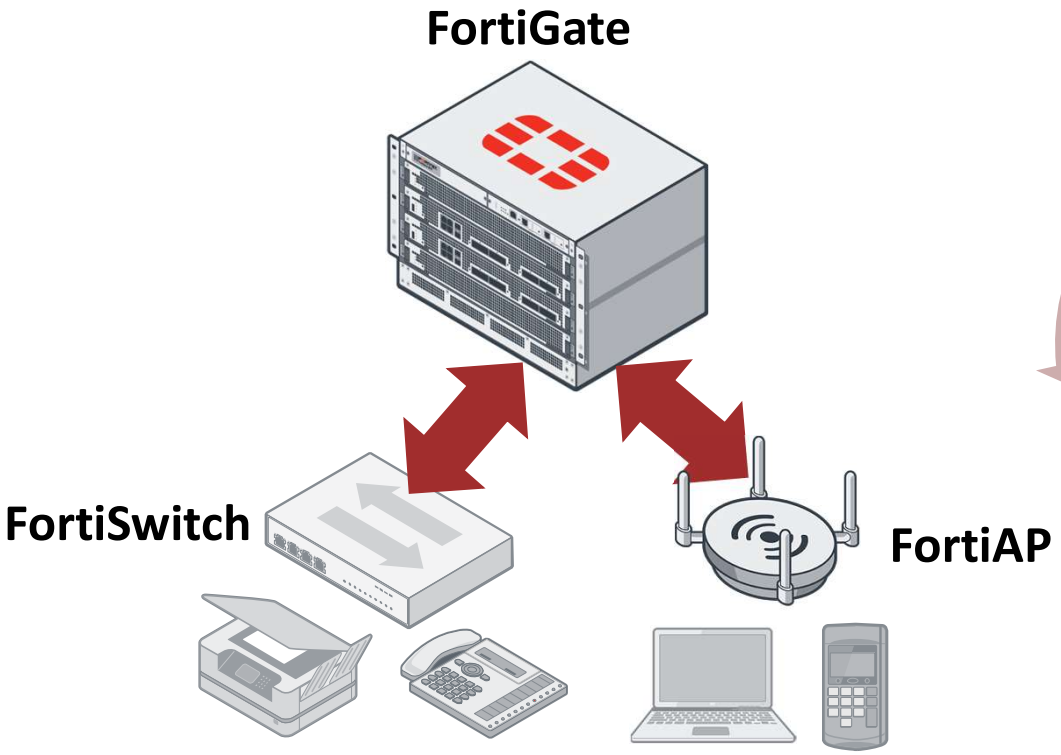


為何邊界防火牆無法提供完整的保護.....

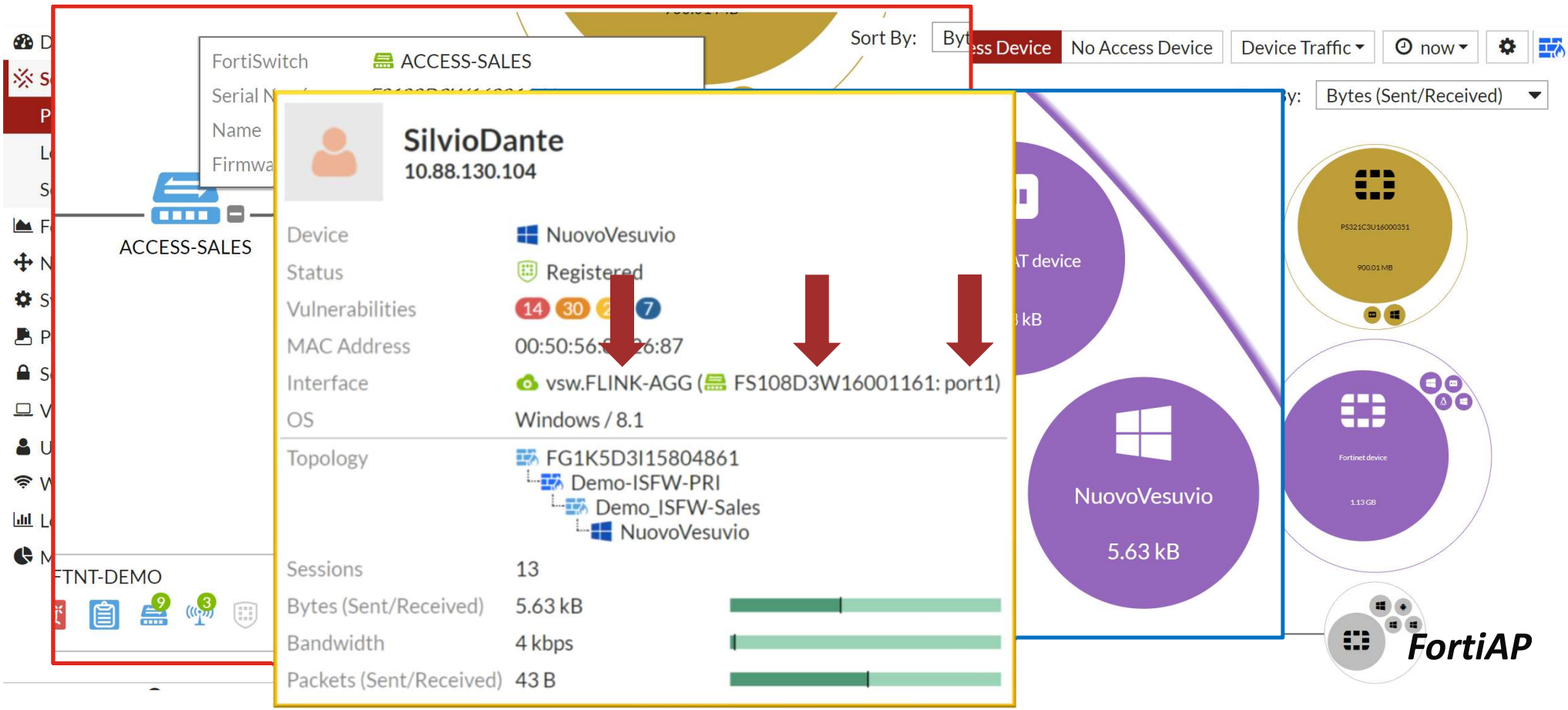
- 既有的的防火牆專注在邊界防護上
- 區域內網已經不再是安全可信任的
- 有太多的方式可以入侵到內部
- 一旦威脅入侵成功，從內部可以快速的散播



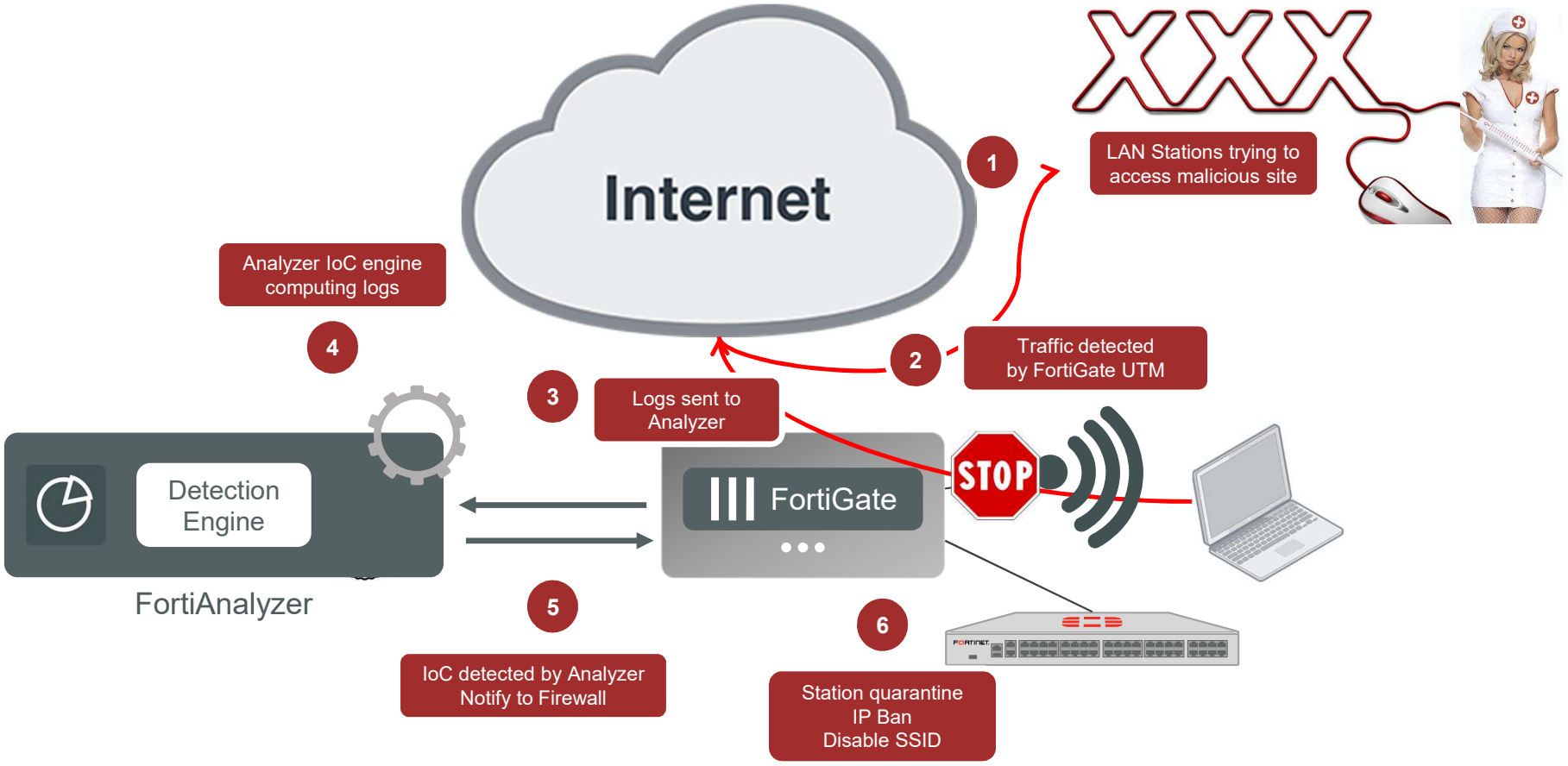
全面性內外網防禦的運作主軸



Visibility: 清楚呈現網路拓樸結構

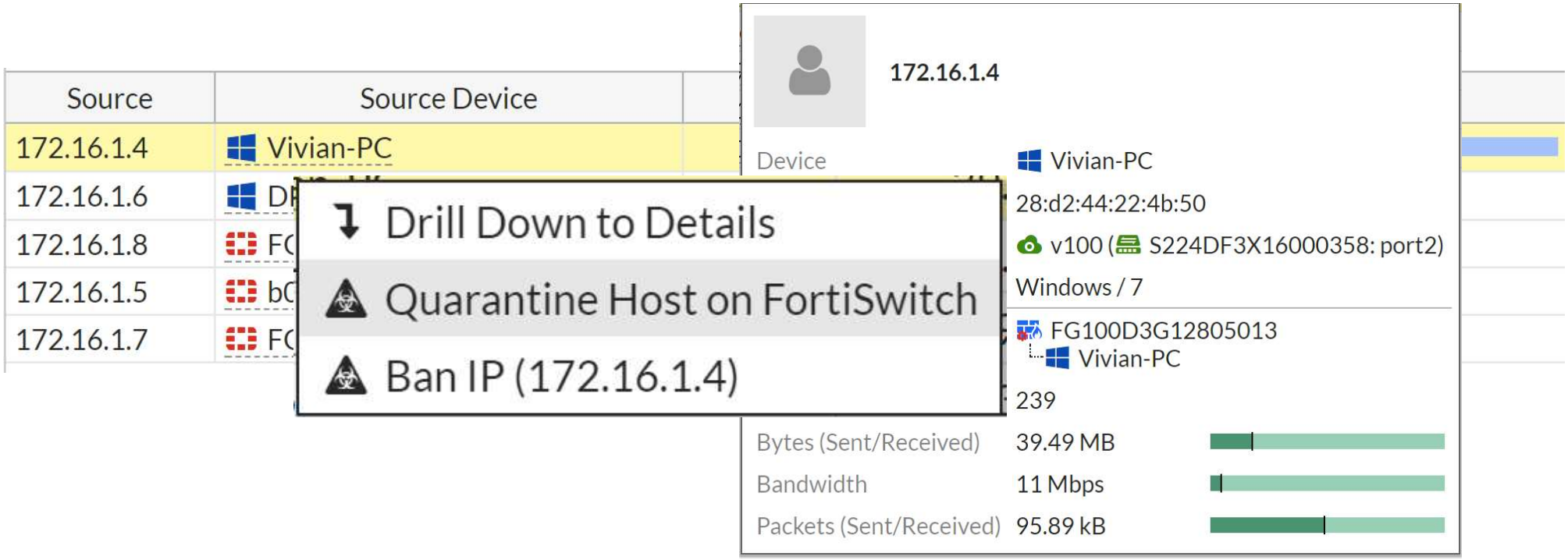


Analysis: 分析網路應用與流量



Action: 將問題隔離在接入層

- 在網路交換器上隔離主機 (隔離 VLAN)
- 在防火牆介面上封鎖主機 IP



安全 vs 易用

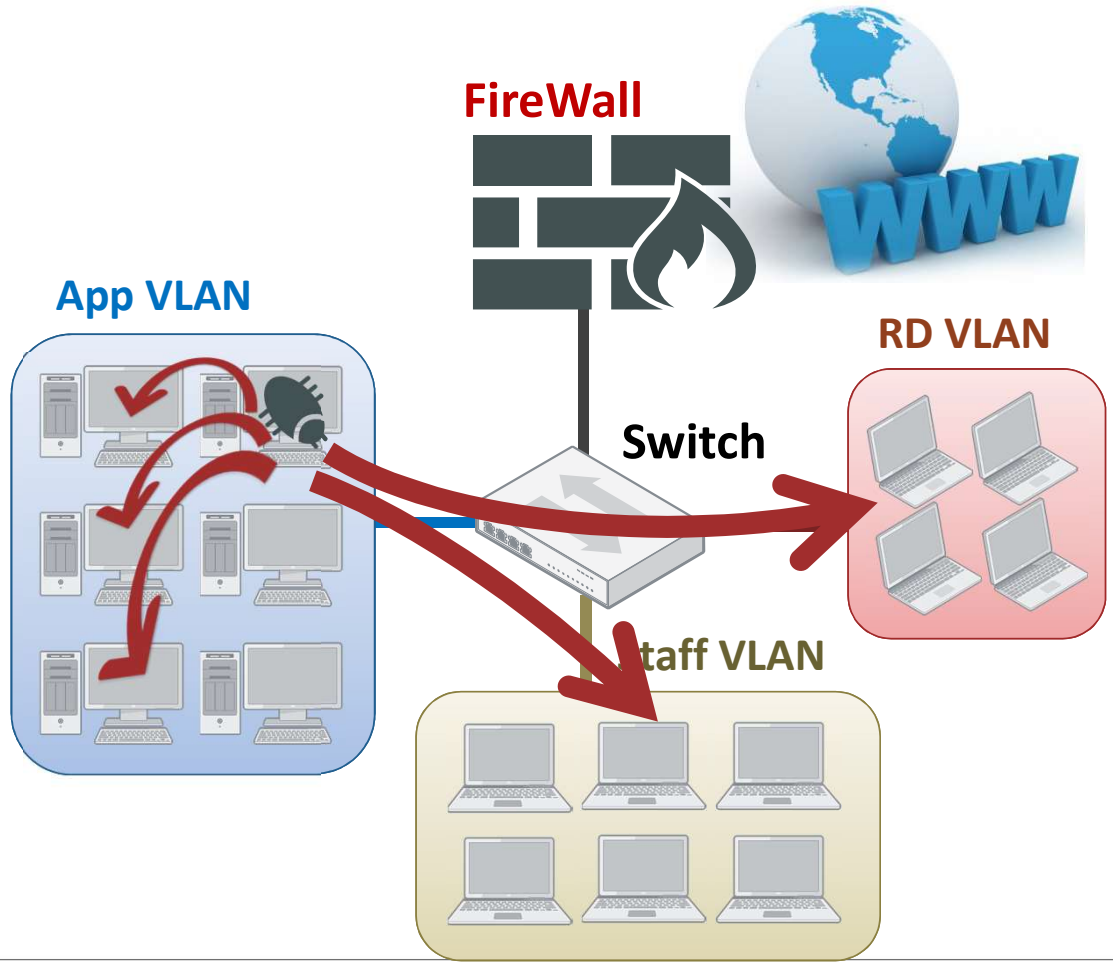
網路的安全性

用户易用性及
IT管理的簡易性

內網防禦的及時性?

當內網遭受威脅攻擊時~

- 既有有線及無線設備無攻擊記錄
- 不知道攻擊者電腦在哪裡
- 網路交換器無法防堵攻擊
- 無法立即進行封鎖阻擋

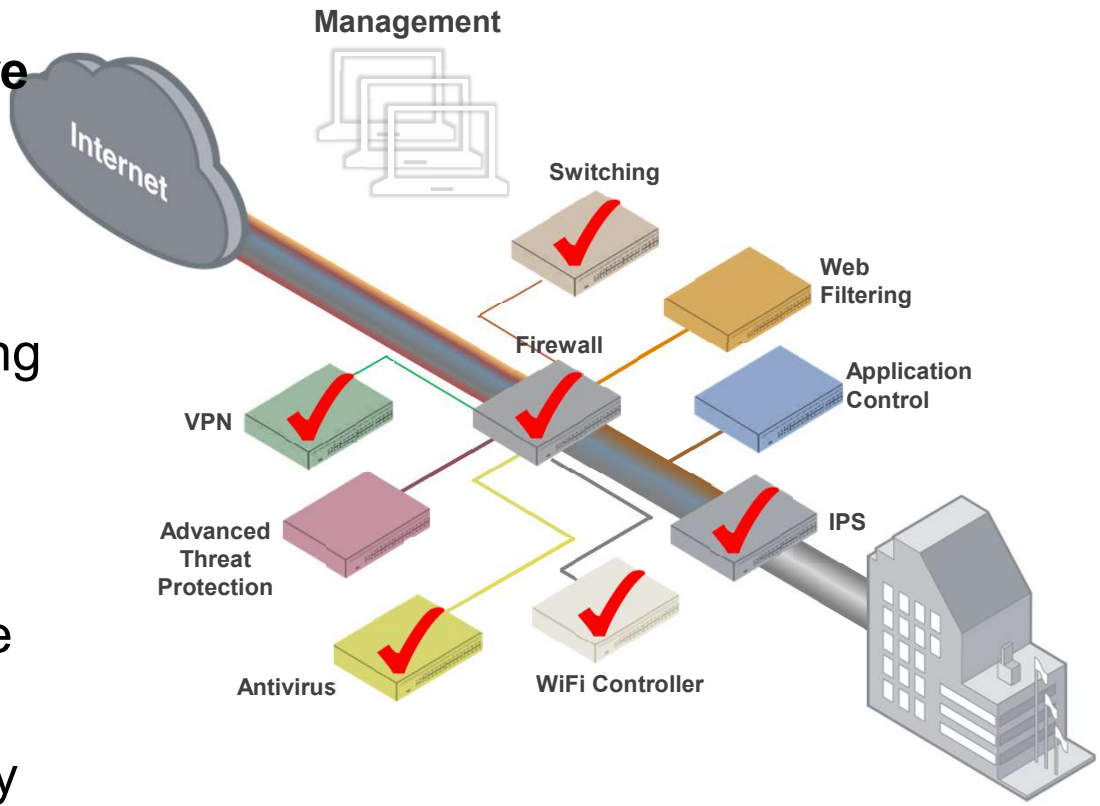


基礎架構管理的簡易性?

Complexity in your infrastructure

- Multiple point solutions
- Multiple platforms
- Multiple management consoles
- Inconsistent policy and networking
- Varying upgrade cycles

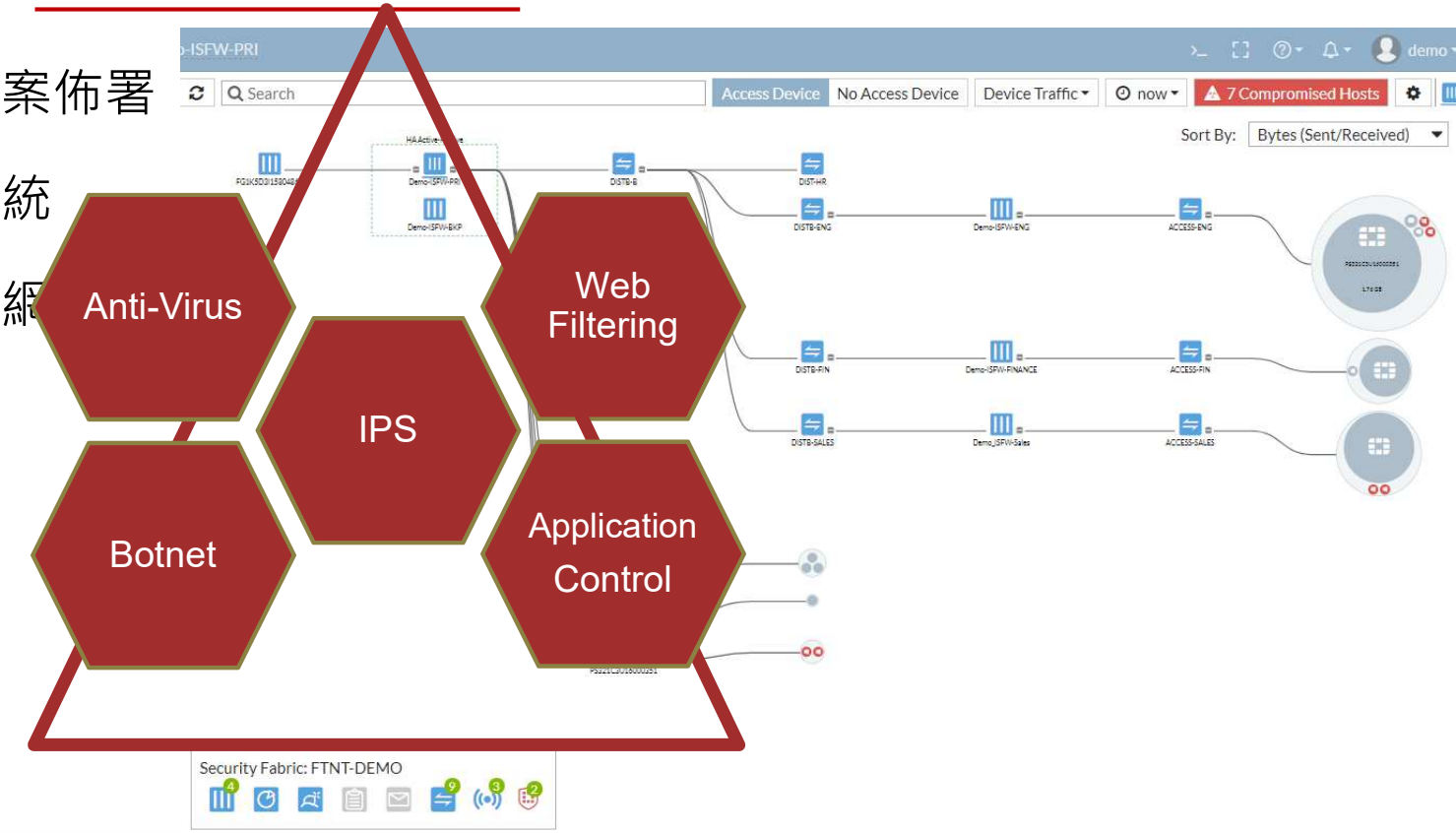
- Slow and porous threat response
- Resources strained to maintain
- Prone to configuration complexity



基礎架構管理的簡易性?

多品牌複雜的架構增加維運困難度

- **單一品牌**的解決方案佈署
- **單一集中**的管理系統
- **可**快速分辨與因應網



Protect the Network from Advanced Threats

Start with Edge and Extend to Internal Network Segments

Why is Internal Segmentation Important?

- Disrupts the flat network design
- Increases visibility, control and mitigation capabilities
- Reduces the spread of damage caused by security breaches
- Increased security across all attack vectors

結論

未來...

- 新世代的防護方案需提供高**可視度**與**防護性**來涵蓋來自**多面向**的資訊威脅
- 整合多樣化的技術用以防護偵測進階威脅的入侵攻擊
- 整合式的智能系統，經由持續性的自動化檢測評估，確保資安系統自身維持最優化配置


thank you!
FORTINET®