



建構高校能e化校園資訊安全網路

劉 乙 Jim Liu

Fortinet Taiwan SE Director

© Copyright Fortinet Inc. All rights reserved.

代理商 逸盈科技 | (02)66368889 | www.netfos.com.tw

News. SONY洩密 專家警告駭客恐導致公司倒閉 (連續三次被駭, 超過上億個資外洩)



臉書創辦人薩克柏成了自家網站漏洞受害者，被雞的照片曝光。翻攝網路



薩克柏和愛犬相處的生活照，都因被「檢舉」全都

被駭的過程尚未完全解密，但後果卻值得擔憂和警惕。

國際新聞 > 臉書出包 薩克柏祕照曝光 >

點閱(33657) 轉寄(0) 引用(3)

字級: A A A 分享: p f t

臉書出包 薩克柏祕照曝光 「檢舉」功能有漏洞 生活照全都錄

2011年 12月08日 f 讚 205 +1 1

【莊蕙嘉／綜合外電報導】「臉書」安全性又出包！用來防止不雅照片的「檢舉」功能有漏洞，用戶只要檢舉他人的大頭貼，便能跳過隱私設定，瀏覽被檢舉者的照片。這回創辦人薩克柏成了受害者，他和女友的14張生活照被上傳網路，被自家產品漏洞捅一刀，雖已修復但仍顏面無光。

首先披露此漏洞的是一個健身網站論壇，該站張貼多張薩克柏（Mark Zuckerberg）照片，包括他和女友普莉希拉陳（Priscilla Chan）合影、他和愛犬「野獸」（Beast）互動等生活照。

稱僅少數受影響

雖然目前只有少數用戶的資料被洩露，但問題在於，如果漏洞持續存在，未來可能會影響到更多的用戶。



賓拉登

SECURITY 已然改變



32

億

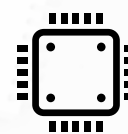
網路用戶



13

億

智慧型手機銷售



30

億

物連網設備，
每年生產量將
持續至2020



10,000x

資安事件增長

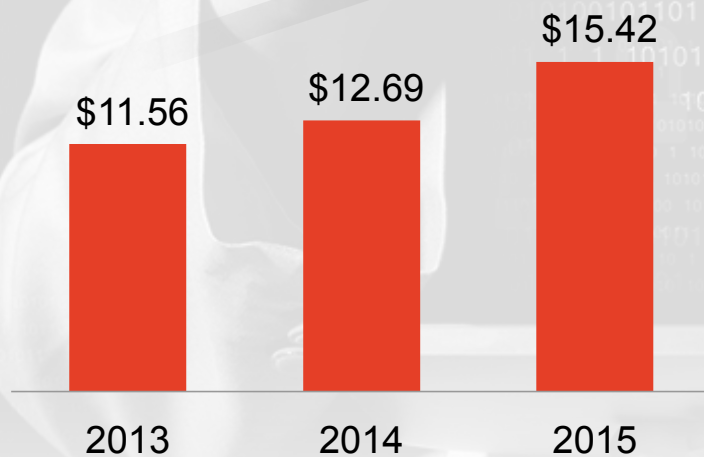


雲端市場市值評估直指

\$1910 億

RISKS 價值難以估計 ...

在美國平均單一資安事件的損失價值
Dollars (Millions)



“

Sony security spends \$22M per year. Sony Breach...direct cost of \$35M for one year....cost to reputation \$100B+

Kowsik Guruswamy, CTO of Menlo Security

”



過時的傳統標準作法 已不合時宜



過於著重死守法規遵循

Enterprises spend too much on checking boxes down a list.



太過於針對已經知威脅

Taking a reactive approach only addresses known threats, not the new unknowns.



過於分散的解決方案

Too many different security vendors whose products do not communicate with one another.

嶄新的解決方案

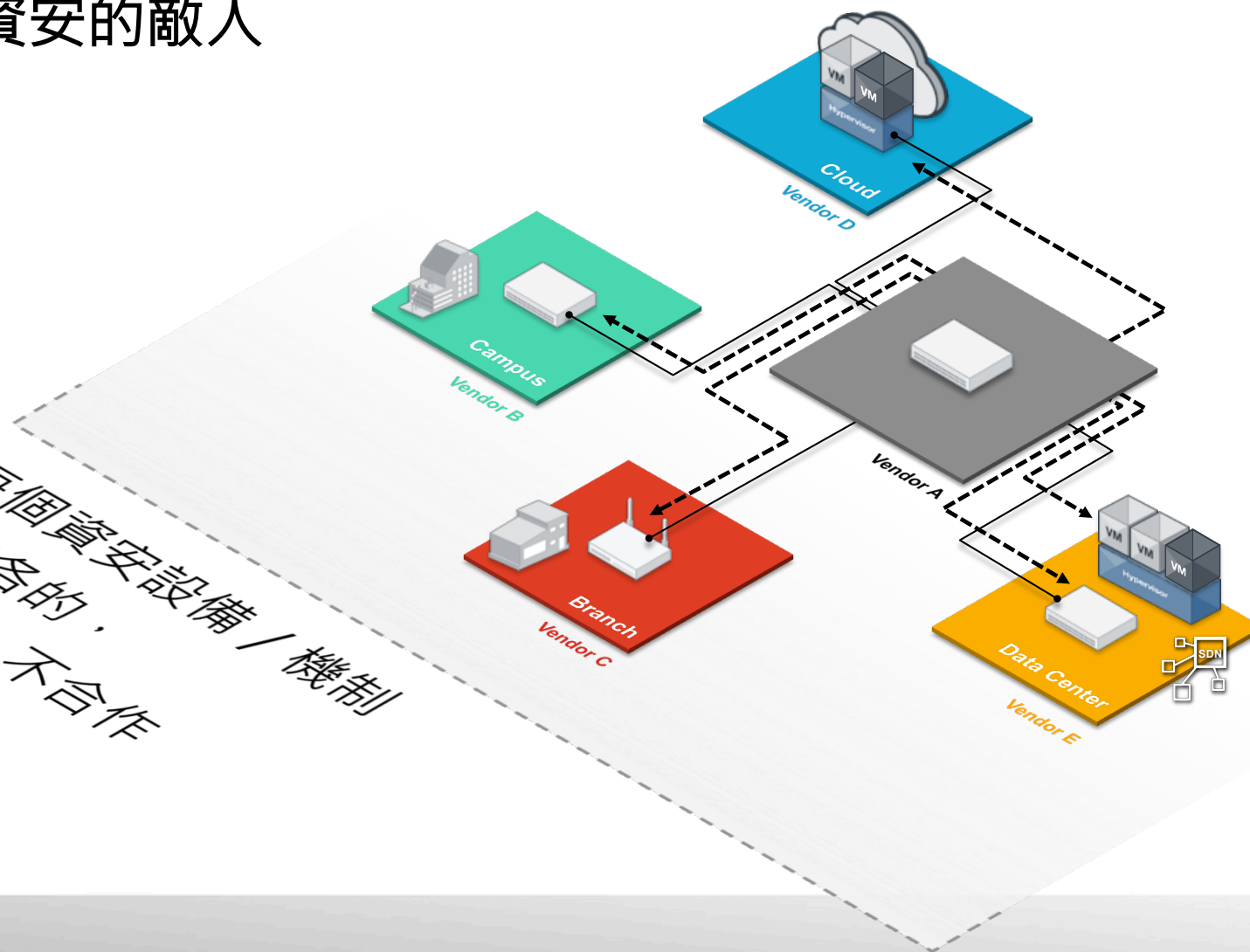
The background of the slide is a detailed, grayscale circuit board pattern with various electronic components and traces.

RULE#1

「複雜」 是資安的敵人
是駭客的朋友

「複雜」是資安的敵人

每個資安設備 / 機制
各管各的，
不交談，不合作



The background of the slide is a detailed, grayscale circuit board pattern with various electronic components and traces.

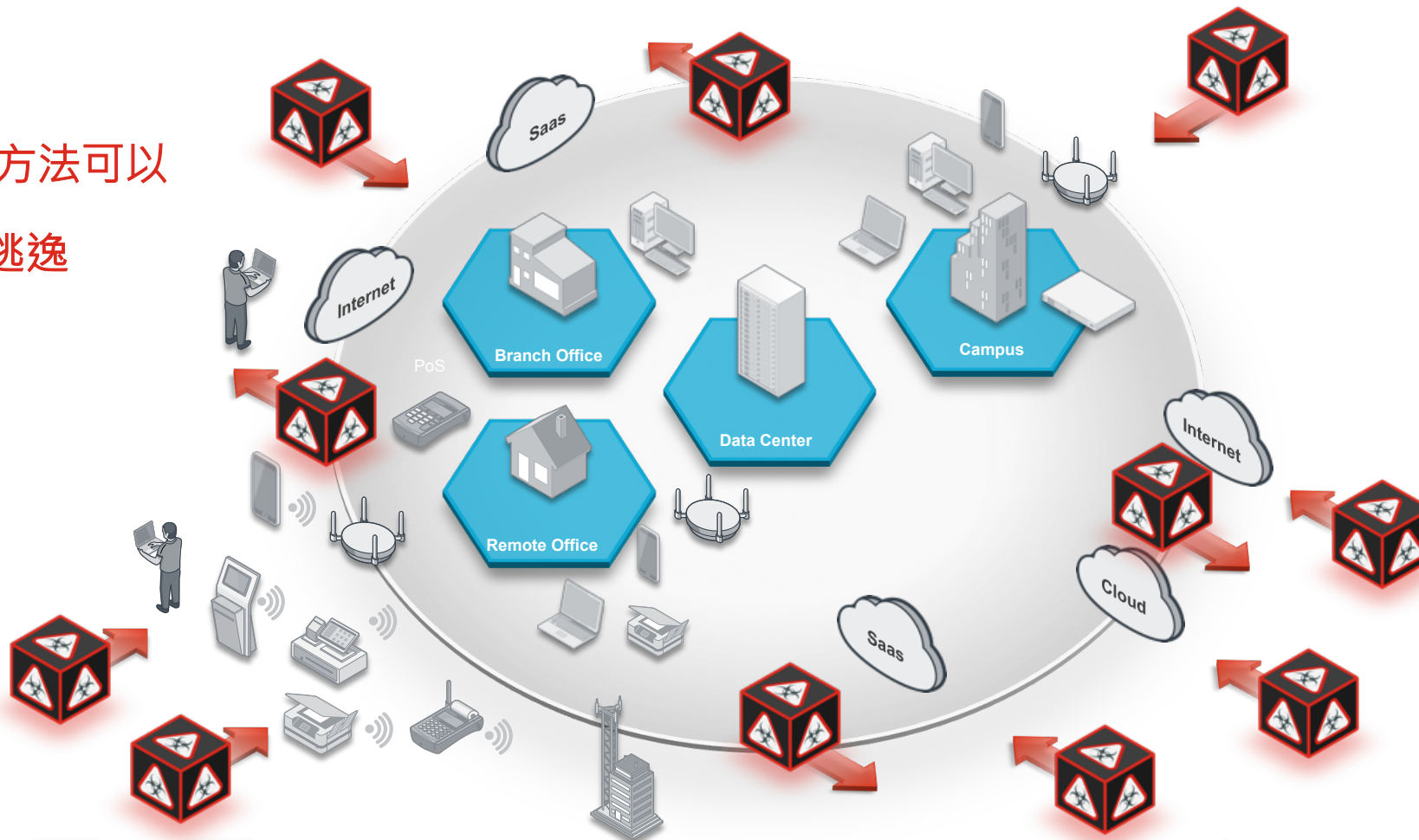
RULE#2

ZERO-TRUST (零信任)

今日的資安不再有邊界

你，我都已處在 無邊界的攻擊環境

有更多的方法可以
入侵 / 逃逸



The background of the slide is a detailed, grayscale image of a circuit board. It features a complex network of white lines representing traces, with various electronic components like capacitors, resistors, and integrated circuits scattered throughout. The overall aesthetic is technical and high-tech.

RULE#3

SPEED

速度是資安決戰關鍵



10G OR **100G** 的骨幹網路



Business Security

Infrastructure Speed

資安和高速網路間無止盡的拉扯

FORTINET.

定義新一代資安世界 嶄新的解決方法

Security demands
efficiency without compromise

全球資安領域領導廠商

Fortinet Quick Facts

- 2000 年成立, **2002** 第一個產品入市, IPO **2009**
- **HQ:** Sunnyvale... **100+** 分公司分部全球
- 員工: **3900+**
- **255,000+** 客戶
- 已銷售超過 **2** 百萬 設備
- **#1** 全球資安設備量佔有率 (IDC)
- 市場領導技術... **257** 專利, **228** 申請中。。



Custom **ASIC-based**
scalable architecture
FortiASIC



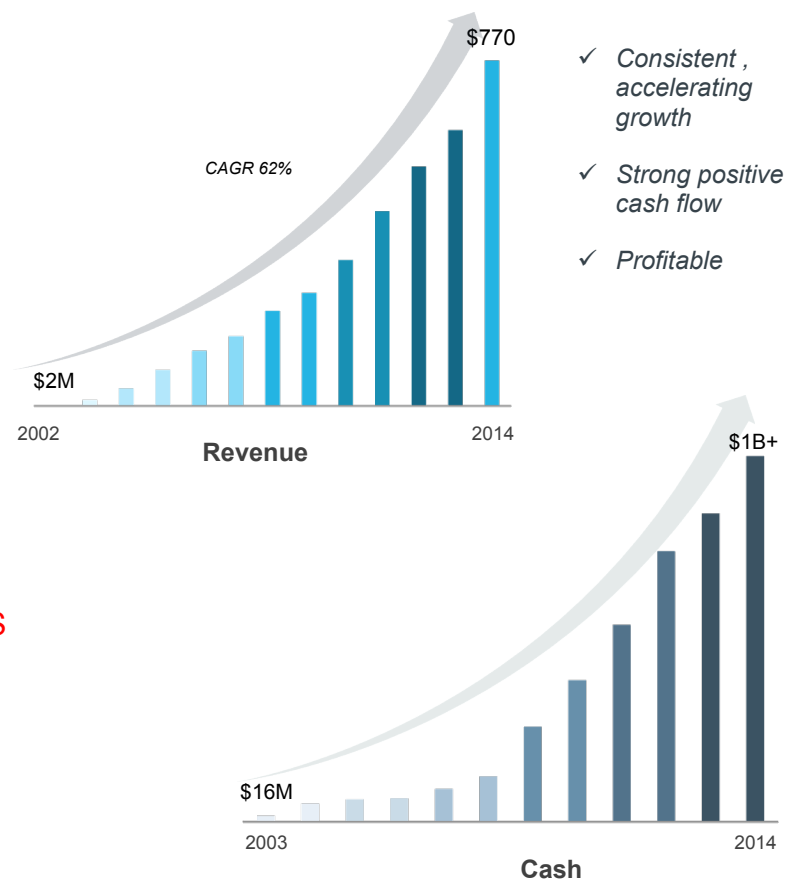
Custom, converged
Networking + **Security OS**
FortiOS



Industry-leading, validated
Threat Research
FortiGuard



Global **Infrastructure & Support**
FortiCare



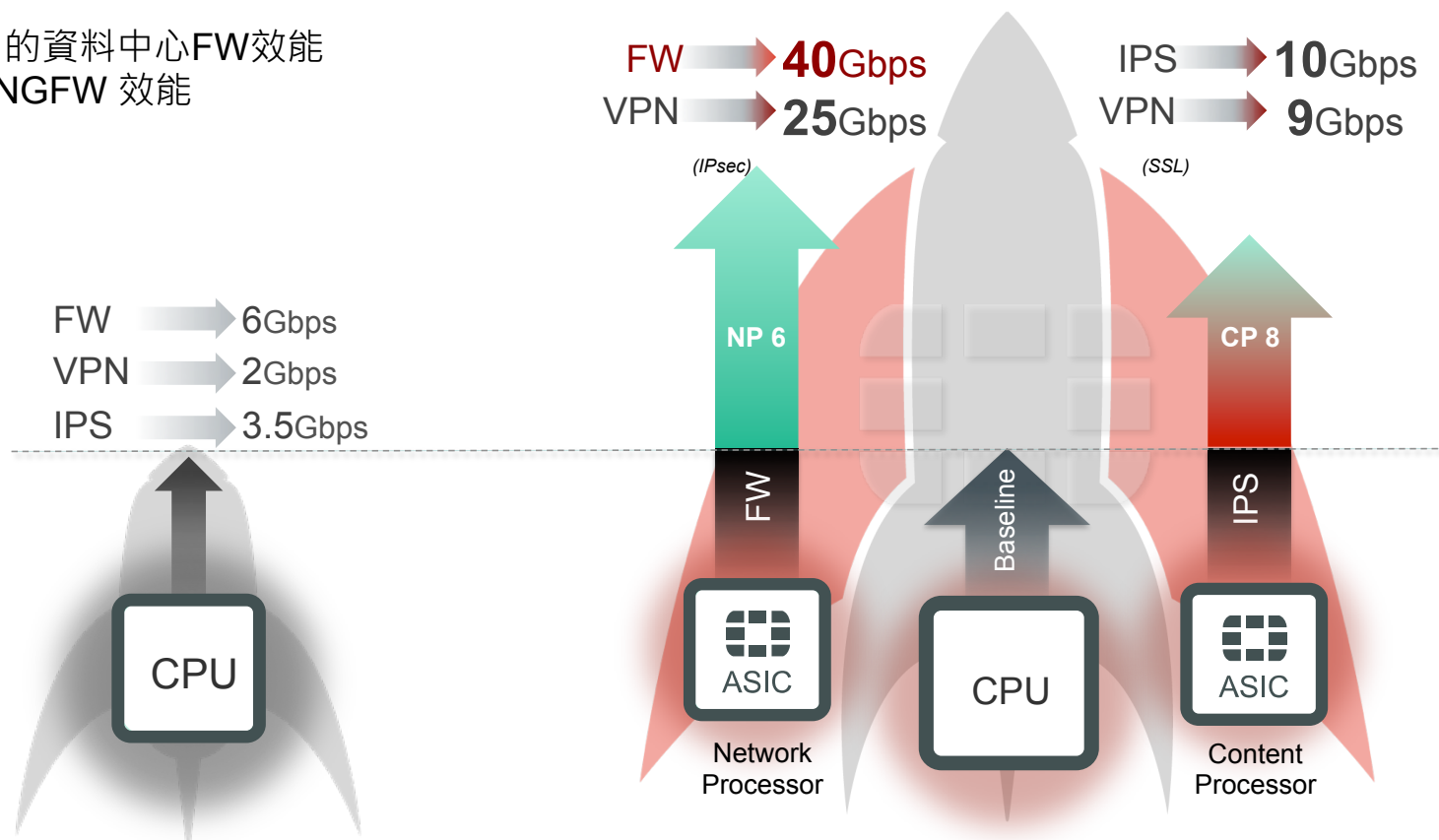
永不妥協 - 不再需要與效能妥協的資安新世界



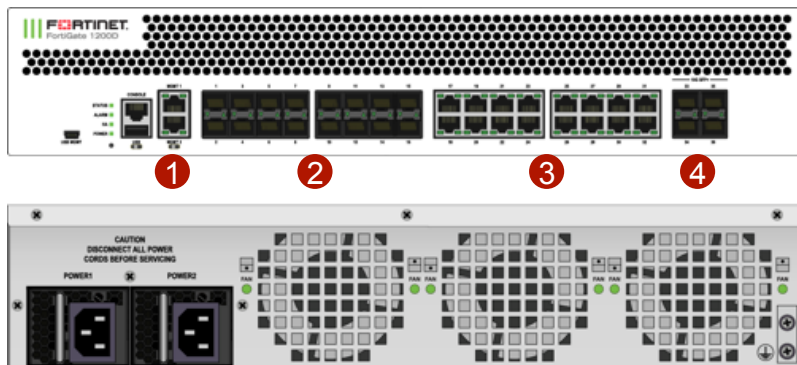
永不妥協助 - 資安 V.S. 效能 -

彈性, 高效能的晶片加速 (ASIC) 資訊安全

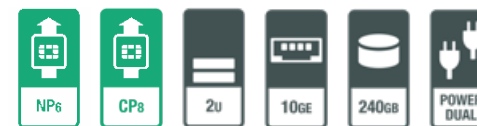
- 提高近 **10X** 的資料中心FW效能
- 提高近 **5X** NGFW 效能



FortiGate 1200D



- ① 2x GE RJ45 Management Ports
- ② 16x GE SFP Slots
- ③ 16x GE RJ45 Ports
- ④ 4x 10GE SPF/+ Slots



72 Gbps
Firewall throughput

11 Million
Concurrent Sessions

290,000
New Sessions/Sec



11 Gbps
IPS Throughput

6 Gbps
SSL Inspection (IPS) Throughput



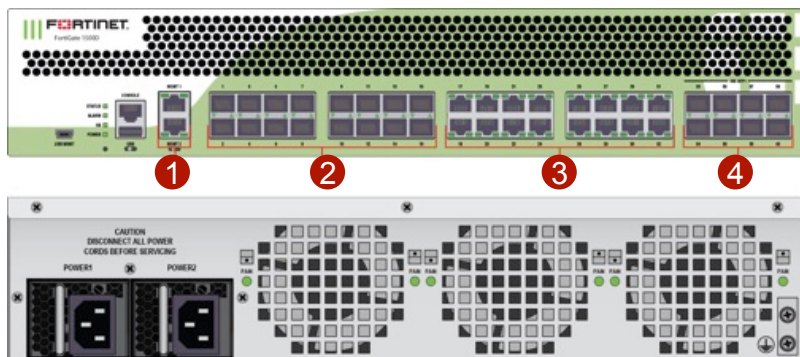
2.4 Gbps
NGFW Throughput



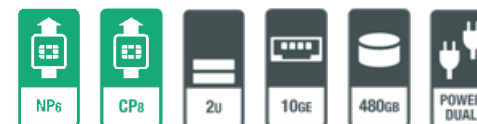
Large Enterprise / Data Center
NGFW / ISFW / DCFW



FortiGate 1500D



- ① 2x GE RJ45 Management Ports
- ② 16x GE SFP Slots
- ③ 16x GE RJ45 Ports
- ④ 8x 10GE SFP/+ Slots



80 Gbps
Firewall throughput

12 Million
Concurrent Sessions

300,000
New Sessions/Sec



15 Gbps
IPS Throughput

10.5 Gbps
SSL Inspection (IPS) Throughput



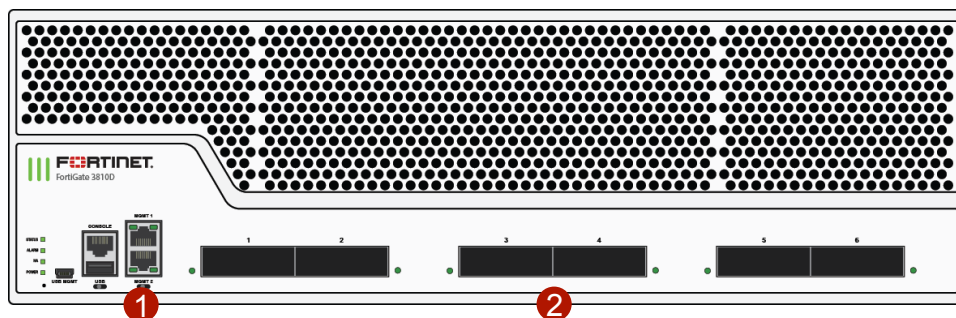
4.5 Gbps
NGFW Throughput



Large Enterprise / Data Center
NGFW / ISFW / DCFW



FortiGate 3810D



- ① 2 x GE RJ45 Management Ports
- ② 6 x 100GE CFP2 Slots



320 Gbps
Firewall throughput

95 Million
Concurrent Sessions

480,000
New Sessions/Sec



30 Gbps
IPS Throughput

15 Gbps
SSL Inspection (IPS) Throughput



12 Gbps
NGFW Throughput



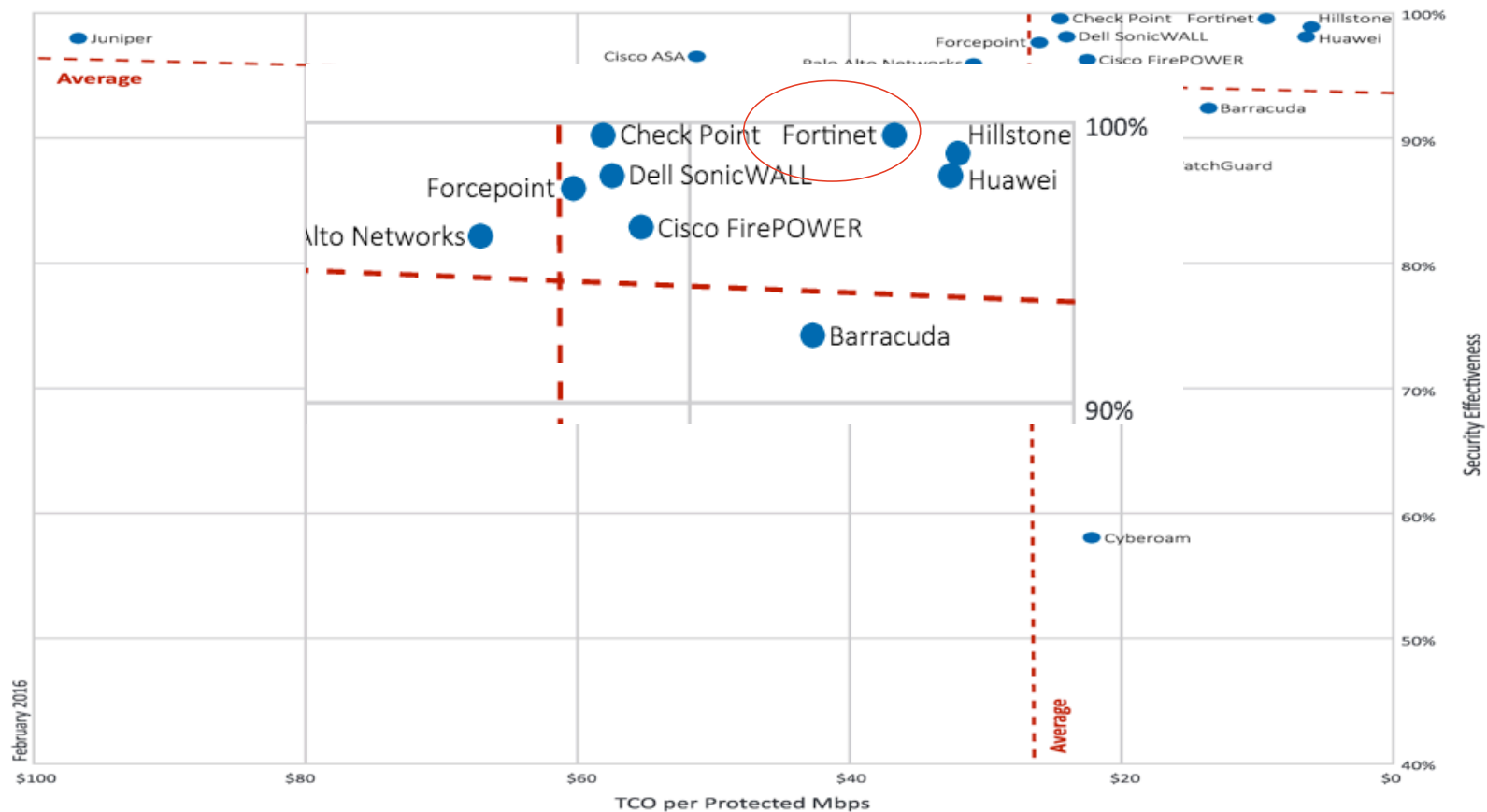
**Large Enterprise / Data Center /
Service Provider**
NGFW / ISFW / DCFW / CCFW



NSS Lab 指引的明燈

- 2016 NSS NGFW 最佳推薦產品

Next Generation Firewall (NGFW) Security Value Map™



如何快速有效率解決 您的資安問題？

Security demands
efficiency without compromise

強化認證機制

強化認證機制

資安完全視覺化

強化網站資訊安



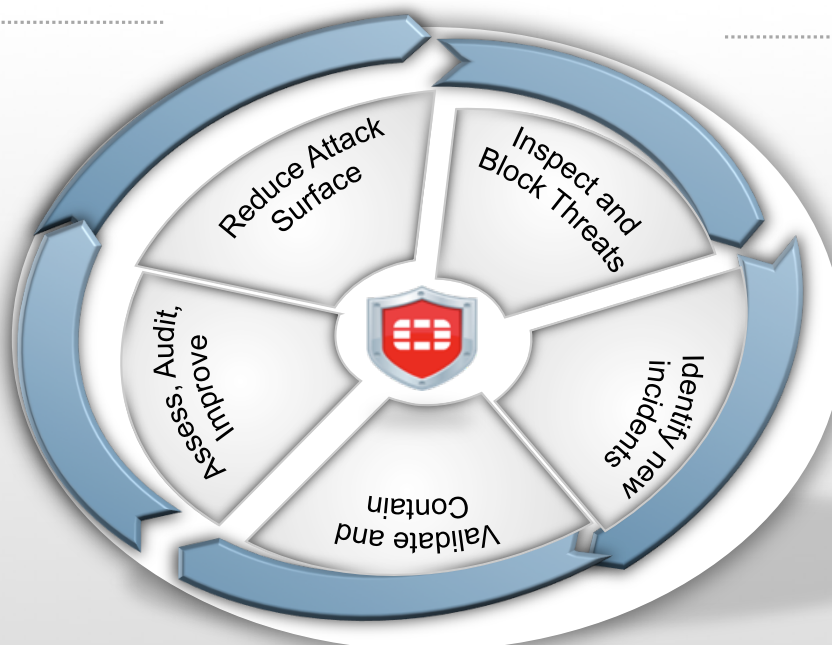
Fortinet's 進階威脅防護架構 (已知 + 未知 威脅)

存取控管

- 防火牆 (FortiGate) + FortiAP
- 2 factor authentication / OTP (一次性密碼) (FortiAuthenticator/ FortiToken)
- 弱點管理

持續的監控

- 報表功能 (Fortianalyzer)
- FortiGuard research
- SIEM/Log Mgt/Intelligence



事件回應

- FortiGuard Services - Device Quarantine - FortiGuard Updates

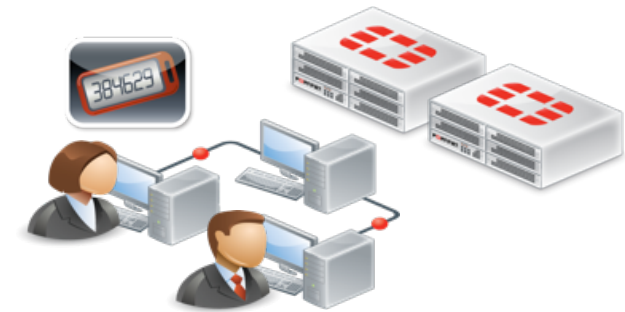
已知威脅防禦

- NG Firewall (FortiGate)
- IPS, App Control
- Deep Flow Antimalware
- Email/Web Filter
- Antibot
- DDoS (FortiDDoS)

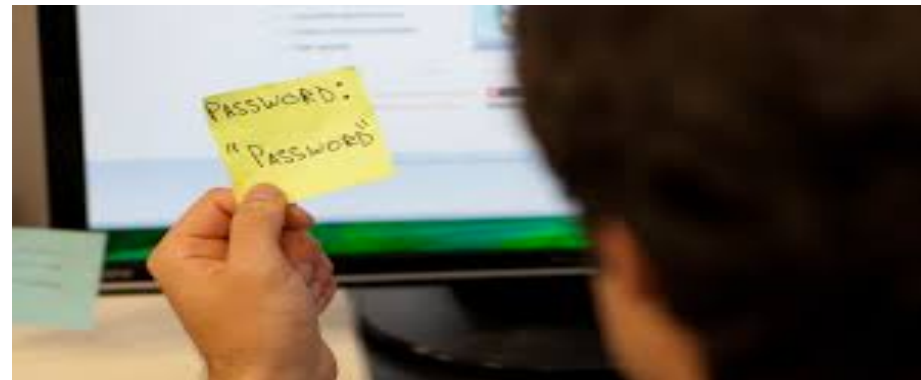
潛在威脅偵測

- Sandbox (沙箱) (FortiSandbox / FortiCloud)
- Network behavioral analysis
- Client reputation
- Botnet reporting

Password is dead – FortiGate也可以扮演 Token Server



資安也要合乎人性

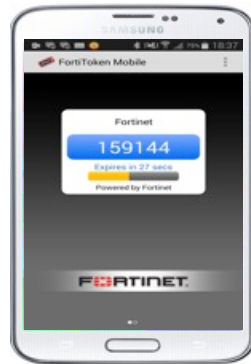
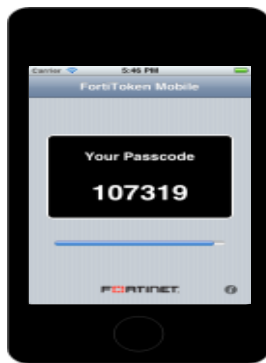


FortiGate 也可以扮演 OTP Sever



Two-Factor Authentication

免除硬體購置與維護

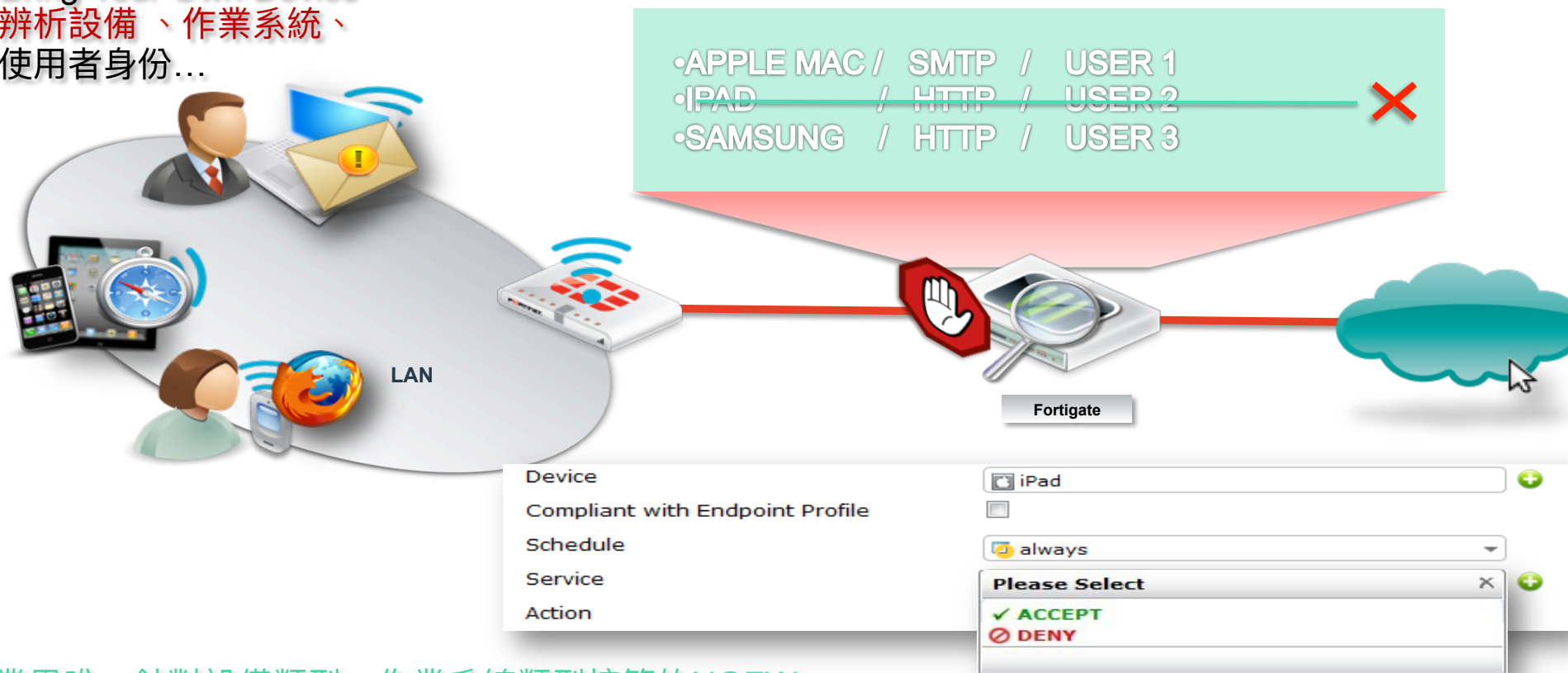


FortiToken Mobile

- 支援 Android 與 iOS
- 免費下載安裝, 並支援其他標準OATH系統 例如 : Google, Dropbox, Amazon
- 支援 QR Code 驗證啟用
- 強化式密碼保護
- 單一次永久授權, 無資產管理負擔可自由重覆指派使用
- 內建二支 OTP , 強化系統管理安

獨步業界 -- FortiGate 也可扮演 無線網路控制器
同時整合無線/有線的資安細緻威脅控管

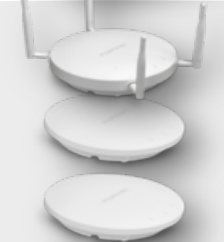
Bring Your Own Device
辨析設備、作業系統、
使用者身份...



業界唯一針對設備類型，作業系統類型控管的NGFW

FortiAP Family – 802.11n and 802.11ac



3x3:3 Resiliency and Versatility	Dual Radio Dual Band			FAP-320C		
				FAP-320B		
2x2:2 Performance			FAP-222C	FAP-223B		
			FAP-222B	FAP-221B		
				FAP-221C		
1x1:1 Value	Single Radio	FAP-28C			FAP-210B	
		FAP-14C FAP-11C		FAP-112B		
		Remote	Outdoor	Indoor		

快速有效的整合打擊已知威脅



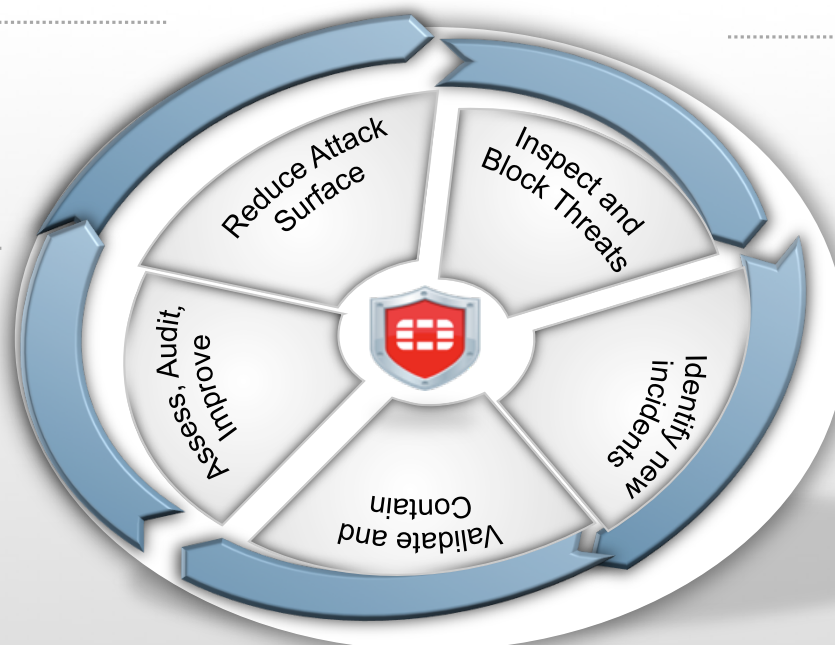
Fortinet's 進階威脅防護架構 (已知 + 未知 威脅)

存取控管

- 防火牆 (FortiGate) + FortiAP
- 2 factor authentication / OTP (一次性密碼) (FortiAuthenticator/ FortiToken)
- 弱點管理

持續的監控

- 報表功能 (Fortianalyzer)
- FortiGuard research
- SIEM/Log Mgt/Intelligence



事件回應

- FortiGuard Services - Device Quarantine - FortiGuard Updates

已知威脅防禦

- NG Firewall (FortiGate)
- IPS, App Control
- Deep Flow Antimalware
- Email/Web Filter
- Antibot
- DDoS (FortiDDoS)

潛在威脅偵測

- Sandbox (沙箱) (FortiSandbox / FortiCloud)
- Network behavioral analysis
- Client reputation
- Botnet reporting

資安完全視覺化

APT 進階攻擊

資安完全視覺化

整合性的單一監控平台



有效可分析的 資安智能



動態圖形數據可視化



FortiView 可視圖形

有效的圖形視別 – 依據類別數量, 動態產生不同大小的氣泡圖

地理資安威脅氣溫圖



Bubble Chart



Country Map

簡單的操作介面 – 一鍵檢視不當網路活動

System

- Dashboard
- Status
- FortiView
- Sources
- Applications
- Destinations
- All Sessions
- Network
- Config
- Admin
- Certificates
- Monitor

Router

- Policy & Objects
- Security Profiles
- VPN
- User & Device
- WAN Opt. & Cache
- WiFi & Switch Controller
- Log & Report

Policy ID: [Search]

now 5 minutes 1 hour 24 hours

Destination	Application	Sessions	Bytes (Sent/Received)
172.30.1.106	DNS	105	
216.115.107.207	HTTP.BROWSER_Chrome	8	
216.115.107.206	HTTP.BROWSER_Chrome, SSL	4	
pagead2.googlesyndic.com (74.125.239.141)	HTTP.BROWSER_Chrome	4	156.82 K
ne	SSL, HTTP.BROWSER_Chrome		16.99 K
pa	HTTP.BROWSER_Chrome		16.66 K
cc	HTTP.BROWSER_Chrome		118.35 K
de	Unknown, Skype		744 I
a.	HTTP.BROWSER_Chrome		9.48 K
ww	HTTP.BROWSER_Chrome		7.84 K
chart.googleapis.com (74.125.28.95)	HTTP.BROWSER_Chrome		43.49 K
111.221.74.37	Skype	2	1.07 K
111.221.74.27	Skype	2	1.23 K
r.openx.net (173.241.250.7)	HTTP.BROWSER_Chrome	2	16.56 K
213.146.168.254	Unknown	1	1.78 K
d7.zedo.com (23.4.217)	HTTP		
dsn6.skype-dsn.akadns.net (213.199.179.175)	Unkr		
157.55.235.173	SSL		
111.221.77.173	Unkr		
157.55.56.173	Unkr		
64.4.23.173	Unkr		
157.55.130.172	Unkr		
157.55.56.172	Unkr		
dsn13.d.skype.net (157.55.130.171)	Unkr		

容易使用並且自動幫你過濾收尋條件

選擇你要的目標並且使用 drill down 功能

以大量Session來進行排序

即時或歷史紀錄

Dashboard Tables

- 列出各Session統計資料，並以不同時間區分
 - 使用智能搜索和列表方式篩選項目
 - 排序並顯示前100名（預設=Session）
 - 由選擇的條件來做Drill down 分析

身份辨識 / 使用設備種類 一目瞭然

Filter Sessions...

now 5 minutes 1 hour 24 hours

滑鼠移動到物件上就會有預覽視窗

#	Date/Time	Source	Destination	Application Name	Security Action	Threat
1	15:28:27	rliao (10.200.10.2)		Skype	✓	
2	15:28:24	rliao (10.200.10.2)		BitTorrent	✓	
3	15:28:23	rliao (10.200.10.2)		BitTorrent	✓	
4	15:28:23	rliao (10.200.10.2)		BitTorrent	✓	
5	15:28:23	rliao (10.200.10.2)		BitTorrent	✓	
6	15:28:23	rliao (10.200.10.2)		BitTorrent	✓	
7	15:28:23	rliao (10.200.10.2)		BitTorrent	✓	
8	15:28:23	rliao (10.200.10.2)		BitTorrent	✓	
9	15:28:23	rliao (10.200.10.2)		Unknown		
10	15:28:23	rliao (10.200.10.2)		Unknown		
11	15:28:23	rliao (10.200.10.2)		BitTorrent	✓	
12	15:28:23	rliao (10.200.10.2)				
13	15:28:23	rliao (10.200.10.2)				
14	15:28:23	rliao (10.200.10.2)				
15	15:28:23	rliao (10.200.10.2)				
16	15:28:23	rliao (10.200.10.2)				
17	15:28:20	rliao (10.200.10.2)				
18	15:28:20	rliao (10.200.10.2)				

Set filter: Application Name=BitTorrent

物件即可成為過濾條件

完整的Session詳細資訊

客製化的預覽條件

Session viewer

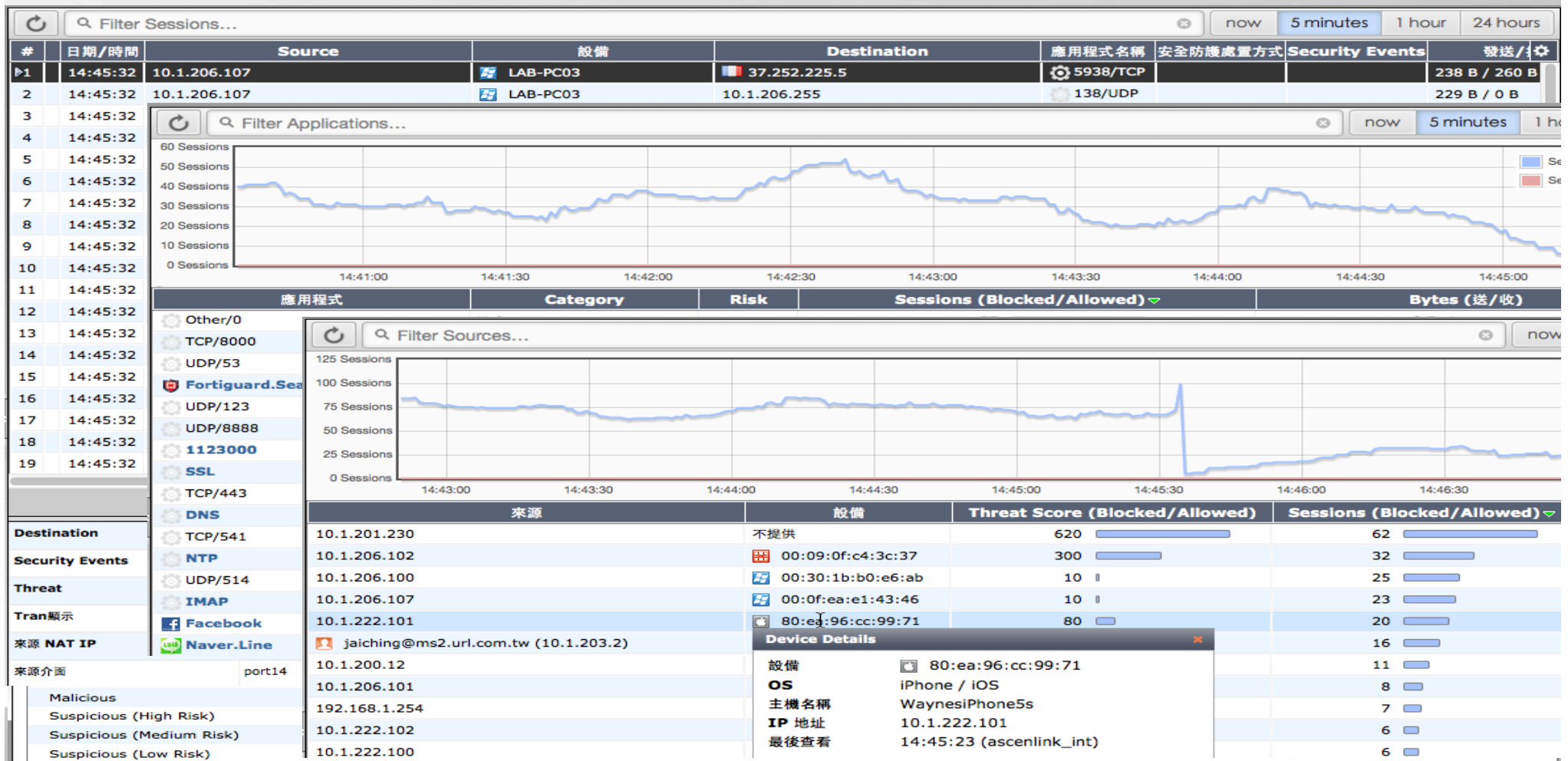
- 過濾後的Session詳細列表
- 提供連結到相關的log資訊

Application Category	P2P
Application Control List	default
Application Name	BitTorrent

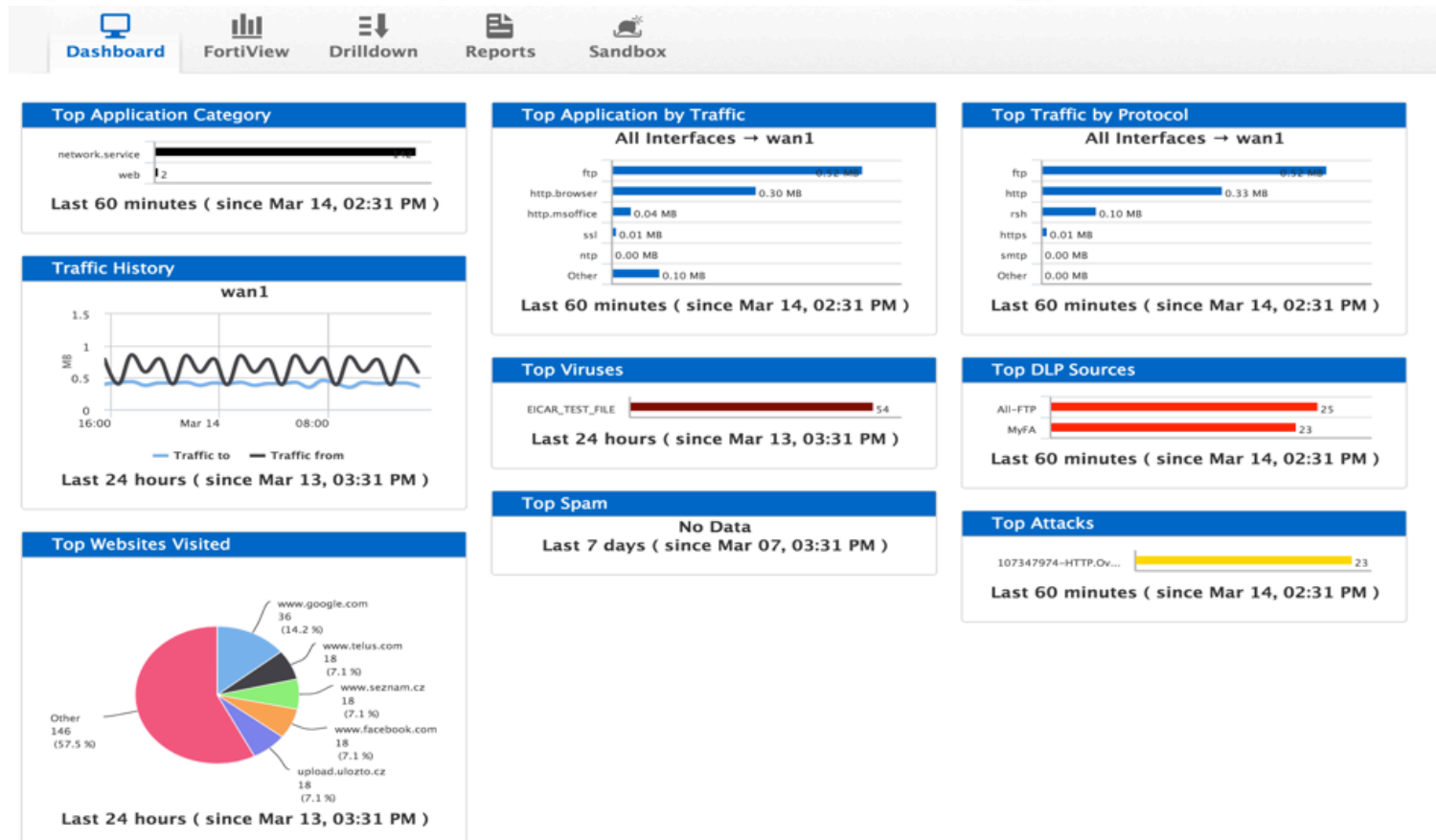
Application Control Action	detected
Application ID	6
Reputation Action	1048576

[Total: 21894]

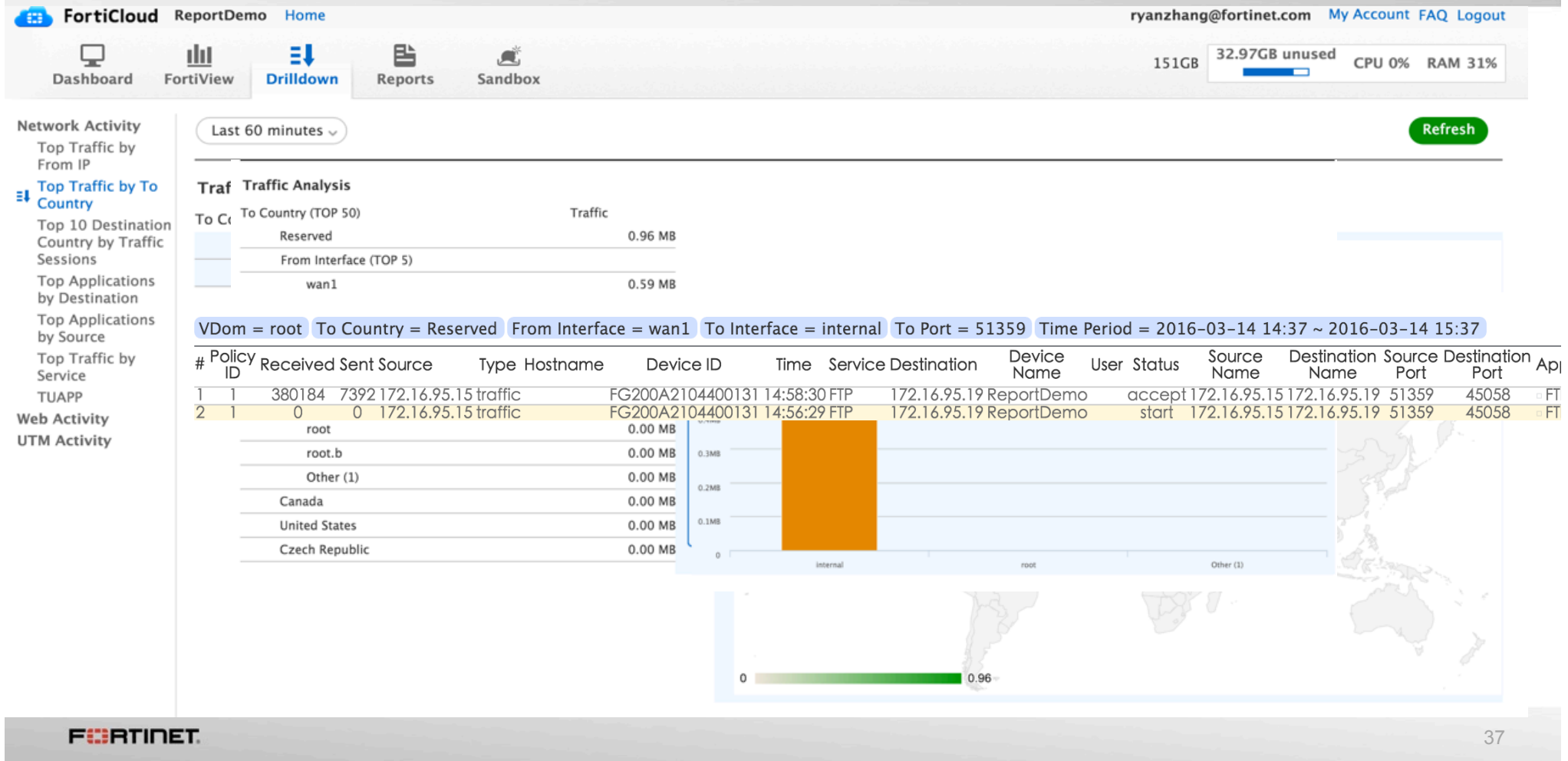
全中文操作介面 – 詳盡的分析資訊



單一管理視覺介面



Drill Down - 深入追踪



整合性的單一監控平台

APT 進階攻擊

資安完全視覺化

整合性的單一監控平台



資安完全視覺化

強化認證機制

資安完全視覺化

強化網站資訊安



後資訊E化的...



為保障個人隱私權；所有臉部均已做過特殊處理

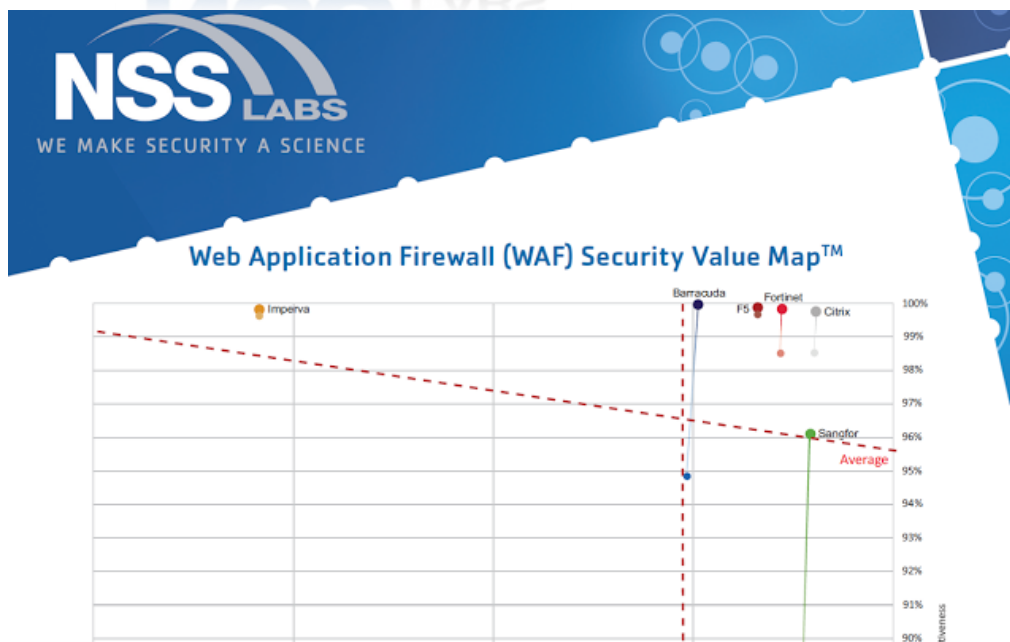
NSS Labs WAF產品報告分析與比較



NSS-LABS

主要是在協助客戶選擇**CP值最好**的產品

1.WAF效能達到一定的水準 2.價錢要合理



FortiWeb



FORTIWEB-1000D	
Hardware	
10/100/1000 Interfaces (RJ-45 ports)	6 (4 bypass)
1000Base-SX Bypass Interfaces	2x SFP QSE ports (non-bypass)
USB Interfaces	2
Storage	2x 2 TB
Form Factor	2U
Power Supply	2U Hot Swap Redundant
System Performance	
Throughput	750 Mbps
Latency	Sub-ms
High Availability	Active/Passive
Application Licenses	Unlimited
All performance values are "up to" and vary depending on the system configuration.	



FortiWeb 產品特色與優勢 (全方位的網站防護--前中後)



- 4種運作模式最完整
- 網頁防置換/防惡意程式植入(不需要License)
- 內建弱點掃描(不需要License)
- 可整合Acunetix掃描結果
- NSS Labs推薦WAF產品
- 內建SSL加速晶片與Bypass模組
- 可整合FortiSandbox, FortiAnalyzer
- FortiGuard 整合服務
- TTP mode可解DHE加密演算法
- 內建L7 負載平衡功能
- GUI介面簡單易上手
- 全中文化介面



- Automatic behavior-based scanning
- Auto setup/learning mode
- Layer 7 DDoS protection
- FortiGuard antivirus, IP reputation and signatures
- Transparent, reverse and non-inline deployment options
- Central Management/ADOMs
- REST API
- Virtual Patching/Third-Party support
- Advanced real-time reporting
- SSL offloading/compression
- SSO/Authentication
- Layer 7 load balancing

FortiWeb 網頁遮罩功能: 可針對網頁機敏性資料& 報表資料做遮罩

FortiWeb VM

Help Logout FORTINET

System
User
Policy
Server Objects
Application Delivery
Web Protection
Known Attacks
Signatures
Custom Signature Group
Custom Signature
Advanced Protection
Input Validation
Protocol
Access
Web Anti-Defacement
DoS Protection
IP Reputation
Auto Learn
Web Vulnerability Scan
Log&Report

Edit Custom Signature

Name: test signautre
Direction: ☐ Request ☒ Response
Case Sensitive: ☐
Expression: price
Action: Alert & Erase
Block Period: 60 (1~3600)(Seconds)
Severity: High
Trigger Action: Please Select

設定字串及後續處理動作

OK Cancel

Add Target Delete

ID	Target
1	RESPONSE_STATUS
2	RESPONSE_BODY
3	RESPONSE_HEADER

整合弱點掃描工具(黑箱)

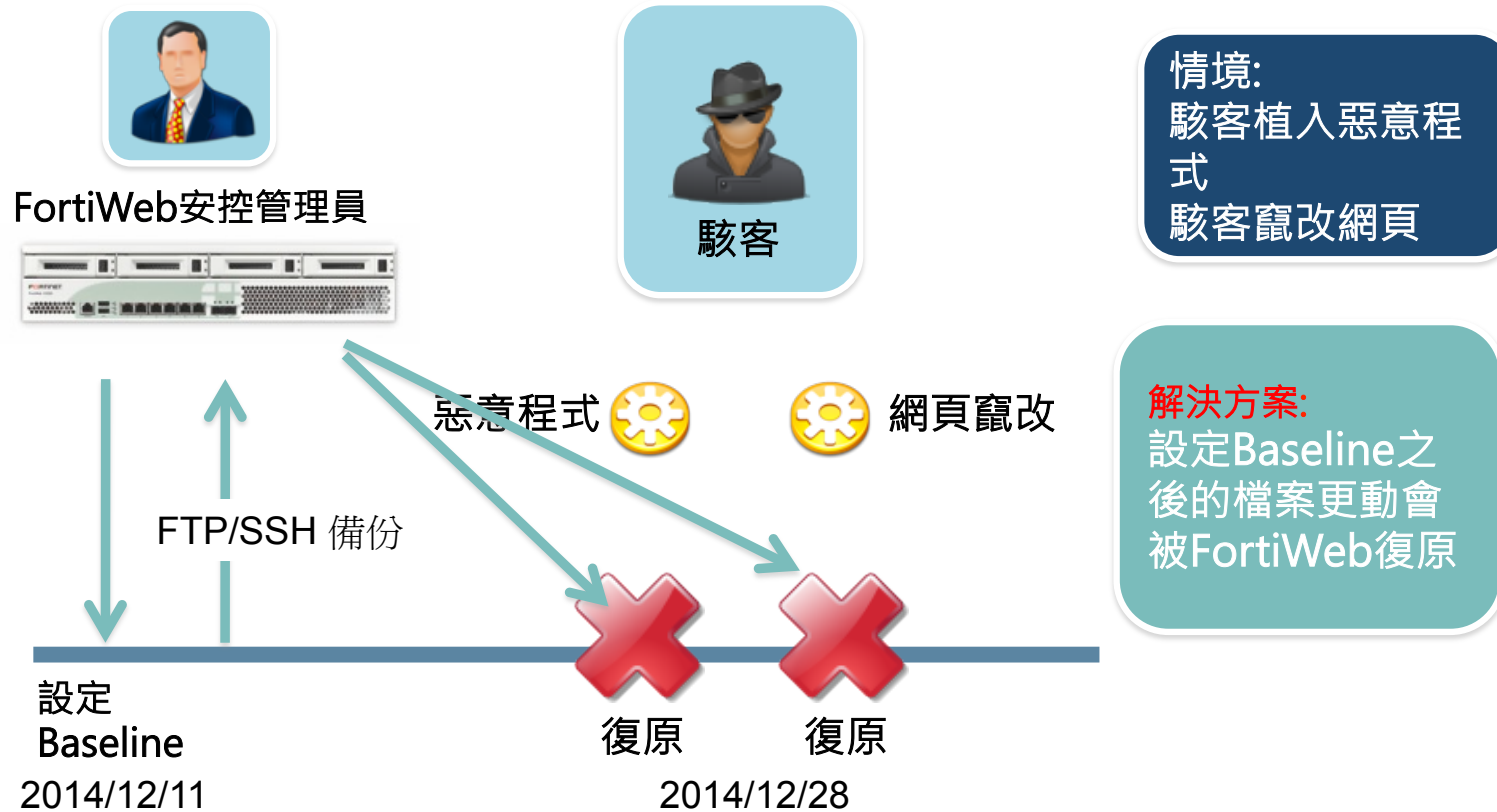
不用再為應用程式弱點尚未修補傷腦筋



- FortiWeb can import scan results and instantly create mitigation policies
- Eliminated payment processors' emergency fix and test cycles

零天攻擊的利器

- FortiWeb 網站防置換運作原理(自動Recover模式)



偵測到網站程式被更動(非自動Recover)

進行改變確認程序

點選 Acknowledge

#	File Path	Scan Time	Result	File Size	File Time	Prev Size	Prev Time	Return
1	/asf-logo-wide.gif	2015-05-14 22:23:47	Added	5866	2015-03-30 00:00:00	0		
2	/asf-logo.png	2015-05-14 22:23:47	Added	17811	2015-03-30 00:00:00	0		
3	/bg-button.png	2015-05-14 22:23:47	Added	713	2015-03-30 00:00:00	0		
4	/bg-middle.png	2015-05-14 22:23:47	Added	1918	2015-03-30 00:00:00	0		
5	/bg-nav-item.png	2015-05-14 22:23:47	Added	1392	2015-03-30 00:00:00	0		
6	/bg-nav.png	2015-05-14 22:23:47	Added	1401	2015-03-30 00:00:00	0		
7	/bg-upper.png	2015-05-14 22:23:47	Added	3103	2015-03-30 00:00:00	0		
8	/build.xml	2015-05-14 22:23:47	Added	3469	2015-03-30 00:00:00	0		
9	/favicon.ico	2015-05-14 22:23:47	Changed	21630	2015-03-30 00:00:00	3638	2015-01-14 00:00:00	
10	/hidden_test.jsp	2015-05-14 22:23:47	Added	920	2015-03-30 00:00:00	0		
11	/index.jsp	2015-05-14 22:23:47	Added	12530	2015-03-30 00:00:00	0		
12	/RELEASE-NOTES.txt	2015-05-14 22:23:47	Added	9054	2015-03-30 00:00:00	0		
13	/Thumbs.db	2015-05-14 22:23:47	Added	30720	2015-03-30 00:00:00	0		
14	/tomcat-power.gif	2015-05-14 22:23:47	Added	2376	2015-03-30 00:00:00	0		
15	/tomcat.css	2015-05-14 22:23:47	Added	5926	2015-03-30 00:00:00	0		
16	/tomcat.gif	2015-05-14 22:23:47	Added	2066	2015-03-30 00:00:00	0		

選擇確認改變

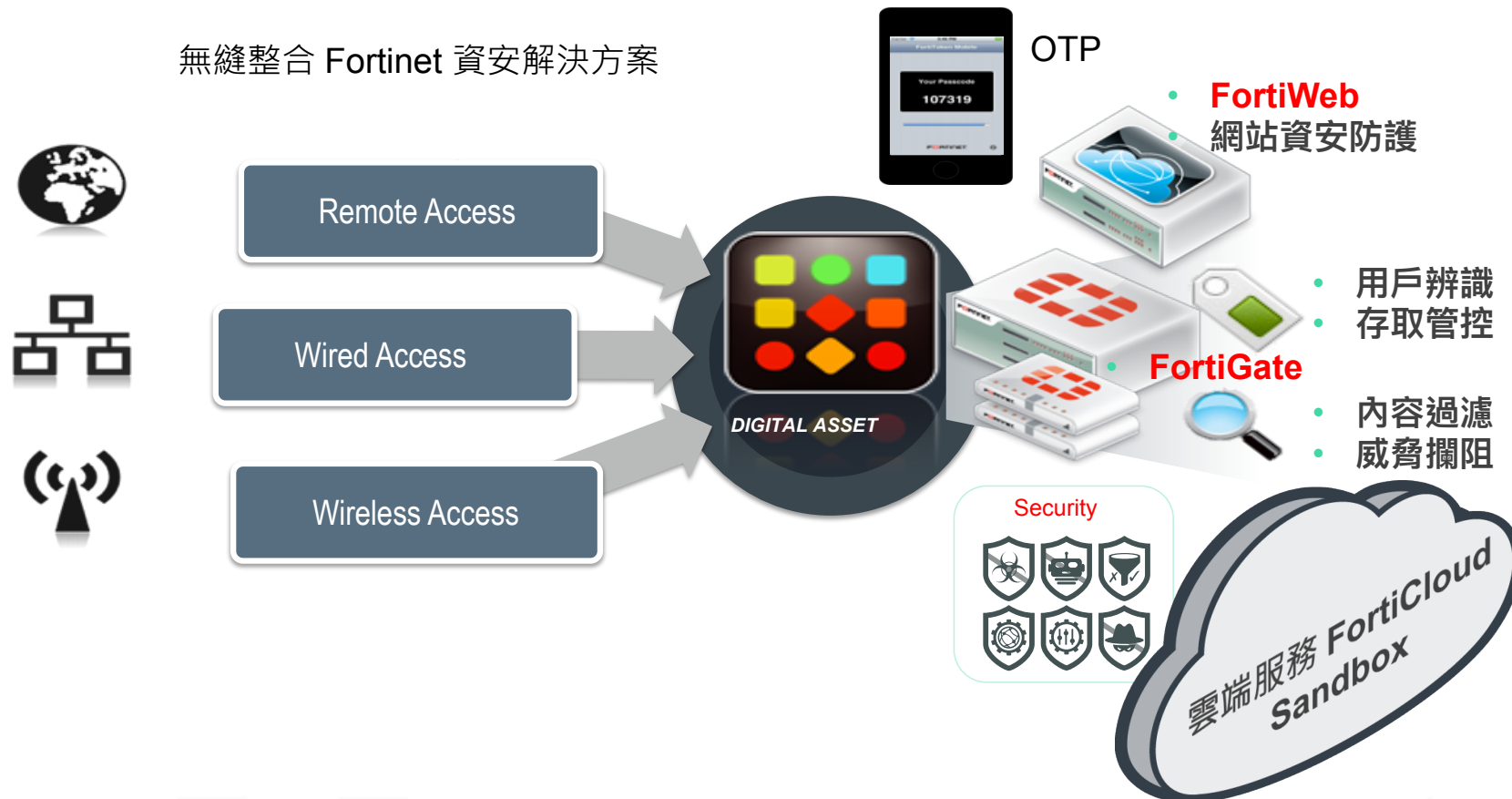


**NEW WORLD.
NEW RULES.
NO COMPROMISES.**

提供一個完整且安全的企業網路環境



無縫整合 Fortinet 資安解決方案



FORTINET®