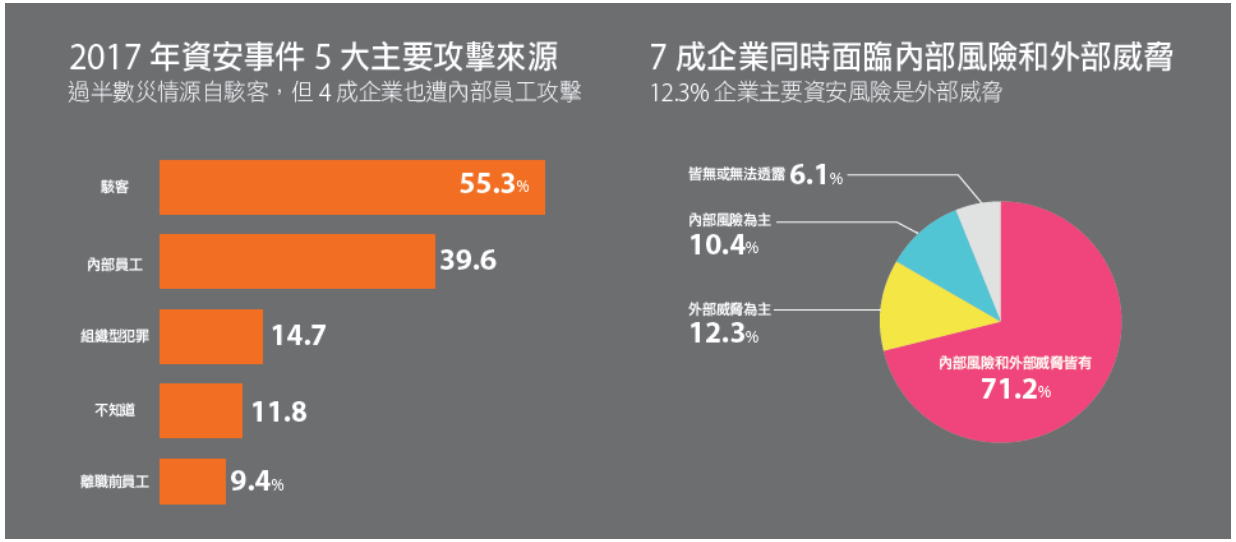
ZERONE
零壹科技

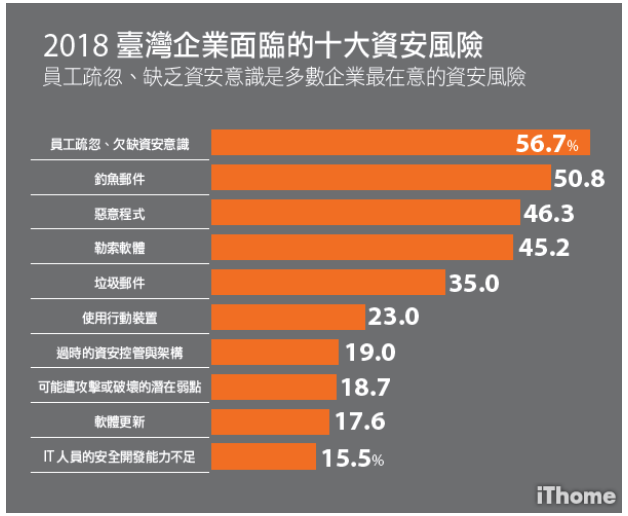
全新資安防禦解決方案
優化網路服務架構新境界

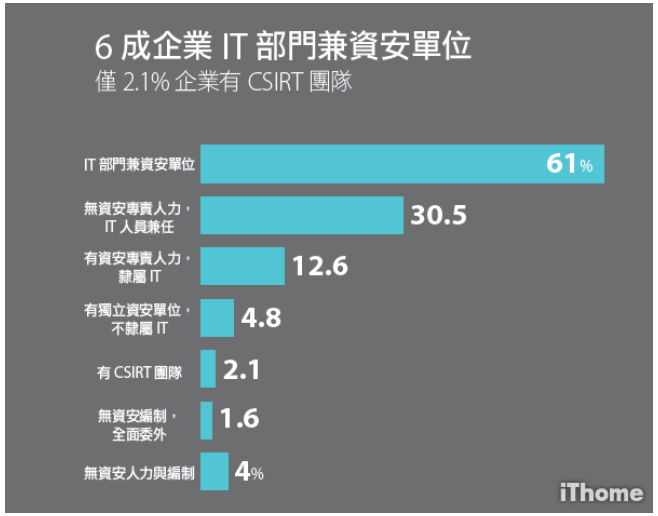
James Wu 資深技術經理

What? Now

該買的資安設備都買了，但資安事件還是不斷發生?!

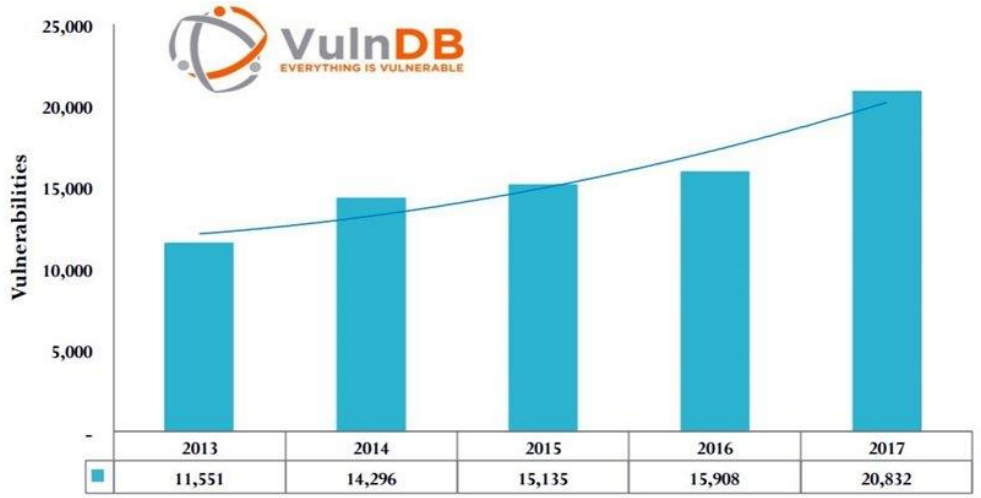






圖片來源 https://goo.gl/4Gjyt6

資安漏洞事件層出不窮，IT人員你今晚睡飽了嗎？



2017年披露的資安漏洞破2萬個再創新高！
只看CVE和NVD，你會漏補7900個無編號漏洞。

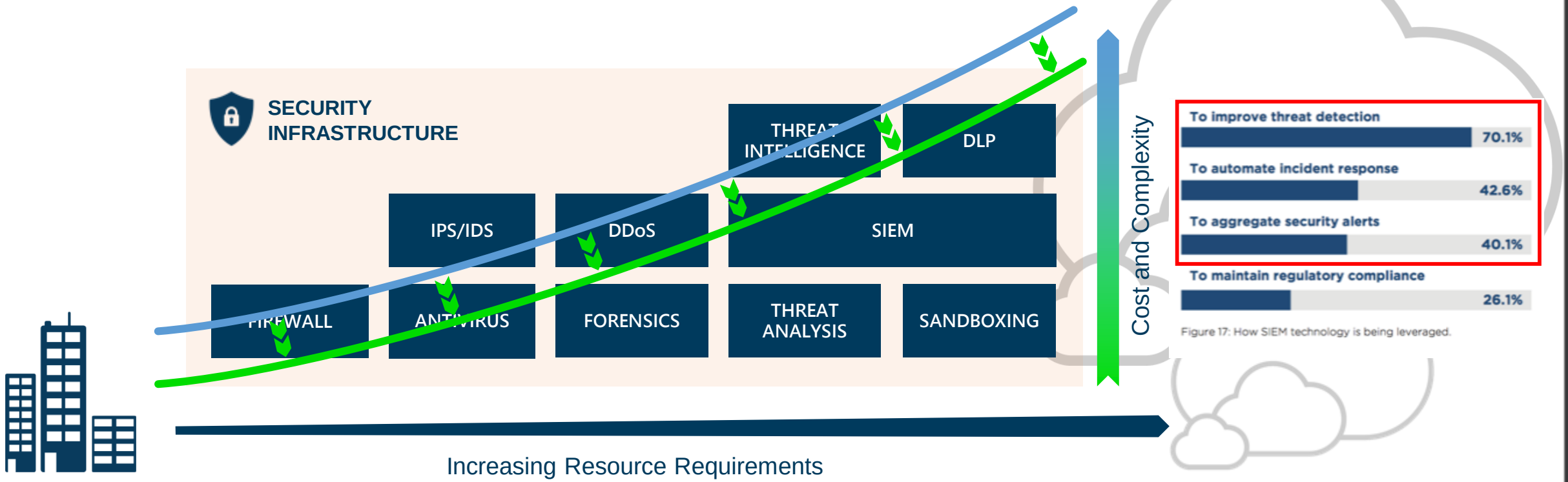
CVSS Score Distribution For Top 50 Vendors By Total Number Of "Distinct" Vulnerabilities

	Vendor Name	Number of Total Vulnerabilities	# Of Vulnerabilities										% Of Total									
			0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9+	Weighted Average	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9+
1	Microsoft	5830	2	92	206	59	806	740	333	1423	26	2043	7.60	0	2	5	1	14	13	6	24	0	35
2	Oracle	5291	2	102	226	418	1516	1383	606	447	23	366	6.10	0	2	4	8	29	26	11	8	0	11
3	Apple	4272	1	53	263	43	722	523	1060	675	15	917	7.00	0	1	6	1	17	12	25	16	0	21
4	IBM	4023	2	61	232	621	1104	684	410	508	28	373	5.90	0	2	6	15	27	17	10	13	1	9
5	Google	3576		9	62	15	664	433	434	933	26	1000	7.50	0	0	2	0	19	12	12	26	1	28
6	Cisco	3532	1	4	51	76	695	814	496	999	42	354	6.90	0	0	1	2	20	23	14	28	1	10
7	Adobe	2571			18	3	230	168	92	131	1	1928	9.00	0	0	1	0	9	7	4	5	0	75
8	Linux	2135	1	91	316	47	654	138	170	585	5	128	5.90	0	4	15	2	31	6	8	27	0	6
9	Mozilla	2047		9	78	11	390	420	237	346	1	955	7.20	0	0	4	1	19	21	12	17	0	27
10	Redhat	1907		46	168	87	390	375	239	426	7	169	6.30	0	2	9	5	20	20	13	22	0	9

選擇知名廠牌，就是安全保障？ 資料來源 https://goo.gl/jYdFe9

傳統的打洞（補丁）方式，
已經無法有效因應資安威脅的快速轉變

隨著企業增長，資安設備只能越換越大？



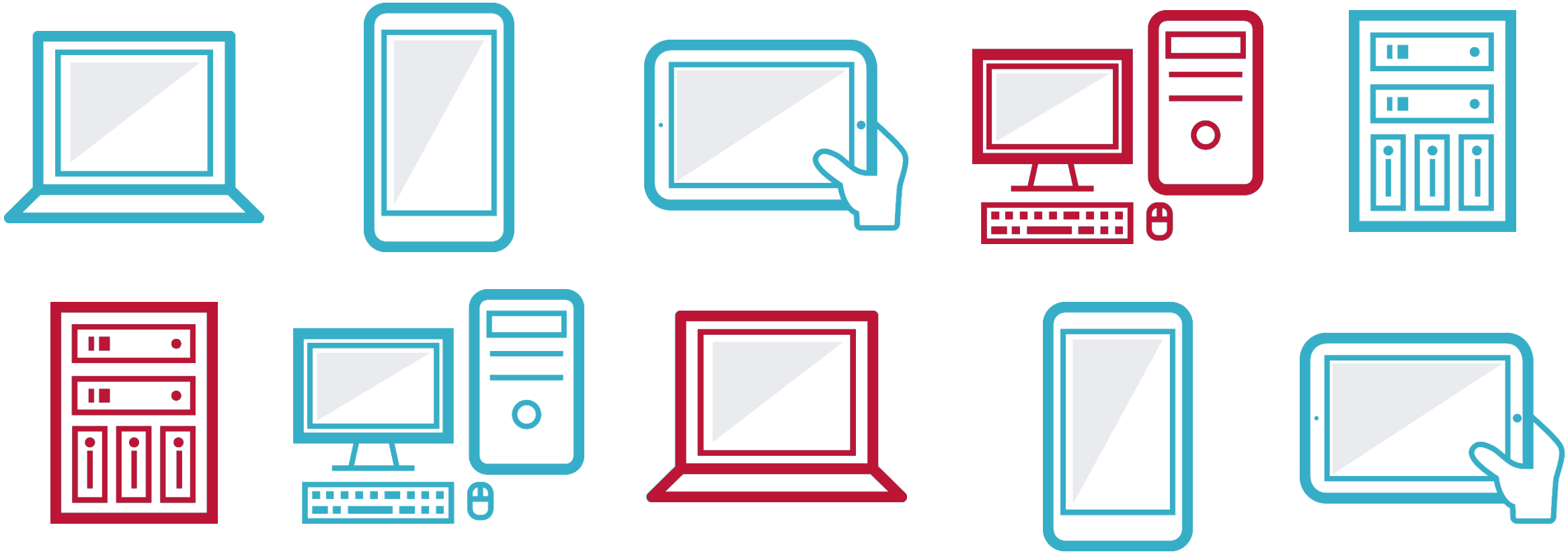
SECURITY INNOVATION TRACKS THREAT INNOVATION.

更多保護. 更為複雜的架構. 更多的維護. 與日俱增的管理負擔.

但如果您可以縮小攻擊來源呢?

較少的	較少的	較小的	資安的基礎建設
ATTACKERS	**SIEM ALERTS**	**ATTACK SURFACE**	可以專注在最重要的防禦需求

過濾惡意來源，讓你的資安設備疲於奔命？



NOW YOU CAN FILTER OUT KNOWN BAD IPs

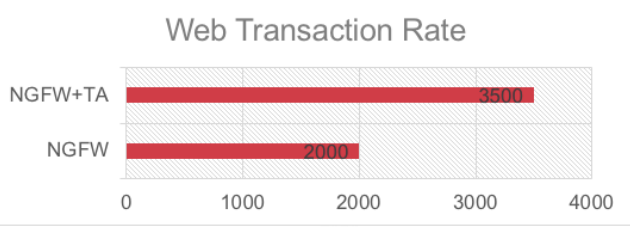
It Time To Stop!

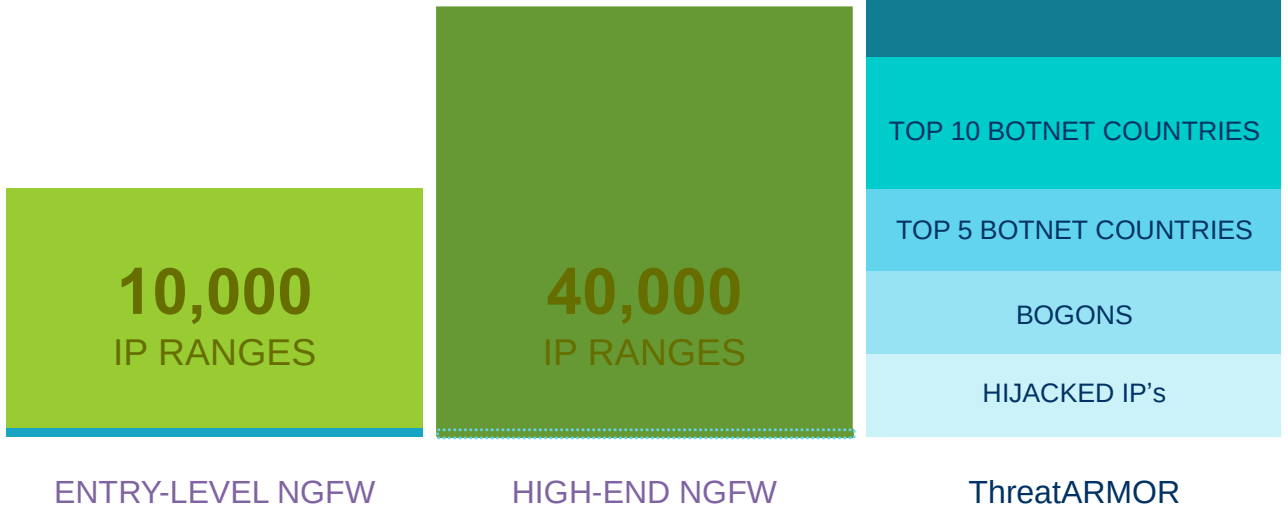
直接過濾已知惡意來源存取，大幅度縮小威脅攻擊面

ixia | ThreatARMOR™

Block up to 80% Malicious Traffic Including Botnets and Ransomware

NGFW產品擁有極佳的DPI探測能力，
可針對應用程式內容進行識別及潛在威脅探測
但對於大規模的惡意IP過濾，則處理能力不佳



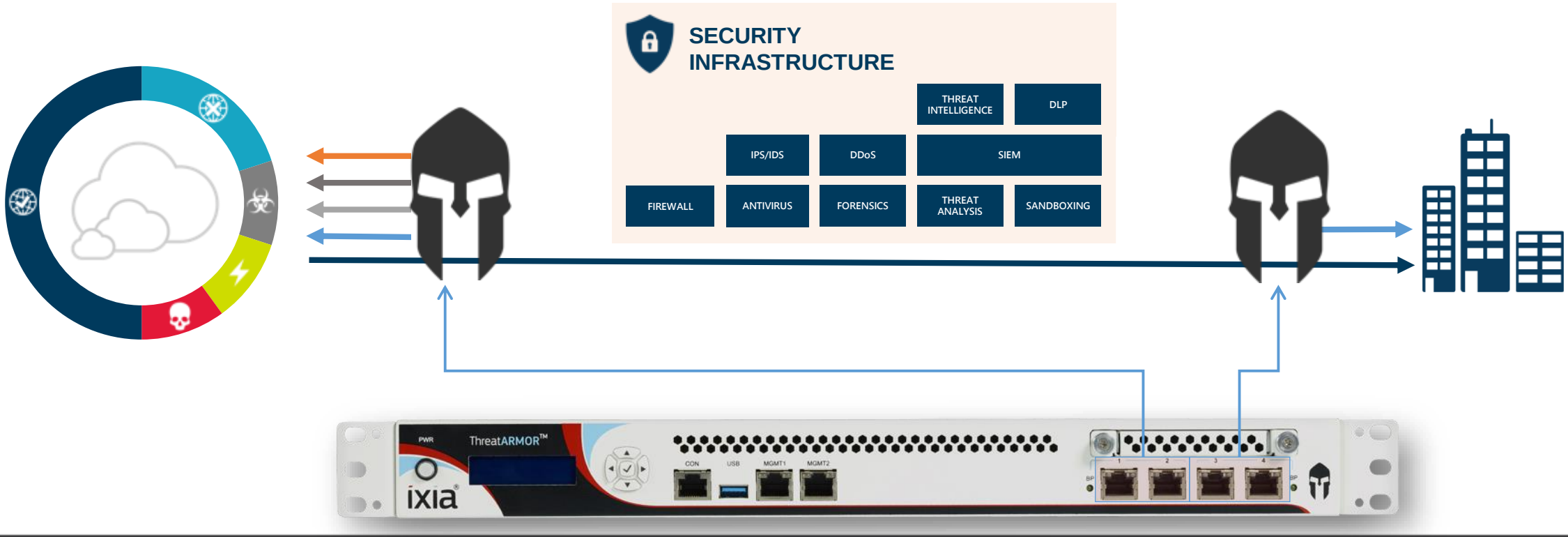


ThreatARMOR™ 部署位置、防護內容說明(內外兼顧)

ThreatARMOR為各種客戶的第一道前端防禦系統

我們封鎖了來自外部的威脅(Botnet,Phishing,Hijacked,Malware,un-Register IPs)

降低了後端防禦設備繁重工作，並且阻斷了自內而外的惡意連線



結合雲端情資，快速因應大規模的攻擊威脅

Analysis

BAD

Whitelist DB Check

BAD

RapSheet Database

情資來源

- Open-source and commercial Threat Intelligence feeds
- Internet Scanning
- Honeypots
- SPAM
- Binary analysis
- Sandboxing

Re-check Daily

Analysis

AV Detection

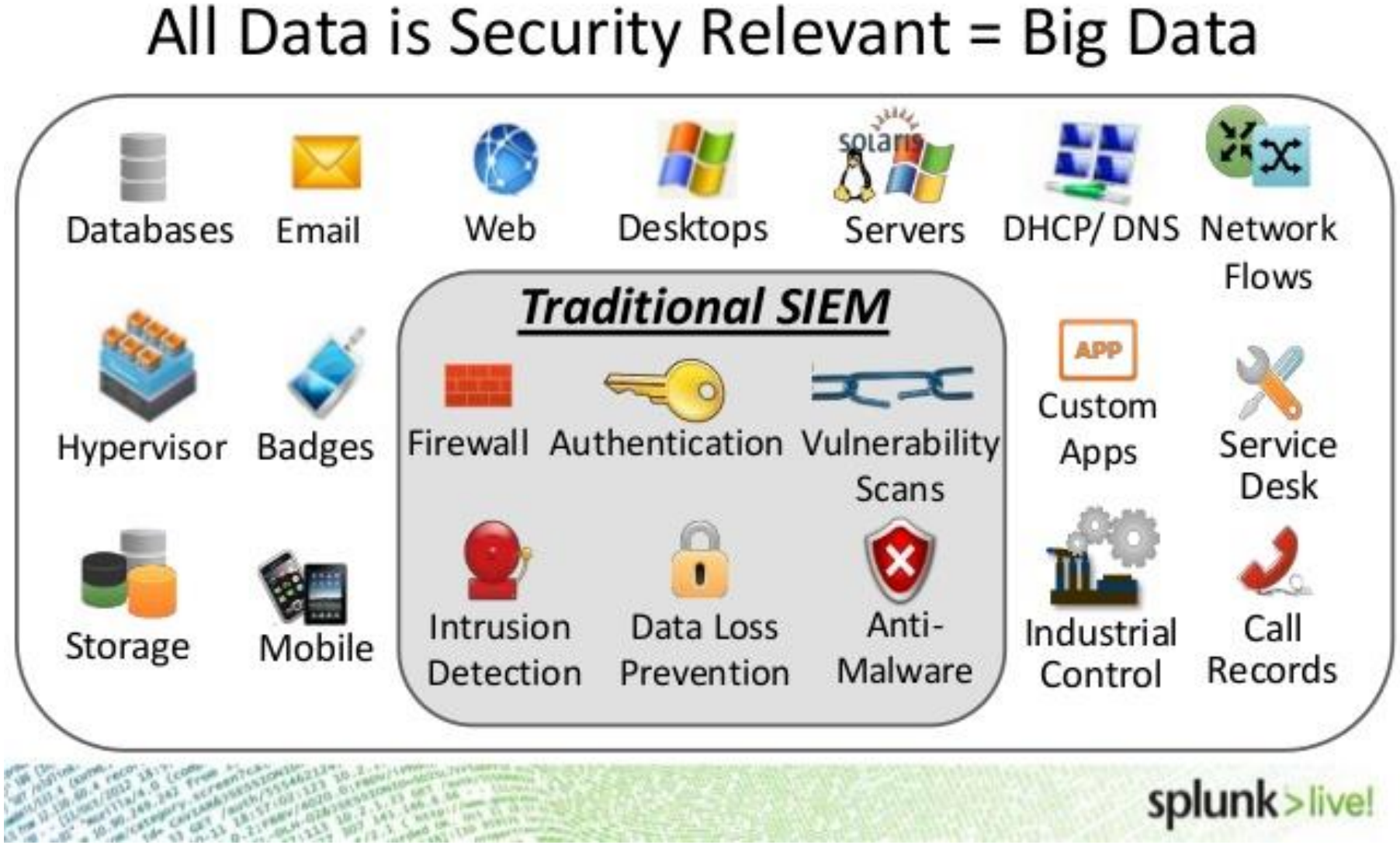
Sandboxes Execution

Phishing Engine

IXIA Signatures

One More Thing!

整合了雲端情資、地端資訊，為何SIEM仍成效不佳？



商業智慧，你分析的是關鍵數據？還是垃圾資訊？

圖片來源 https://goo.gl/xvFt4g

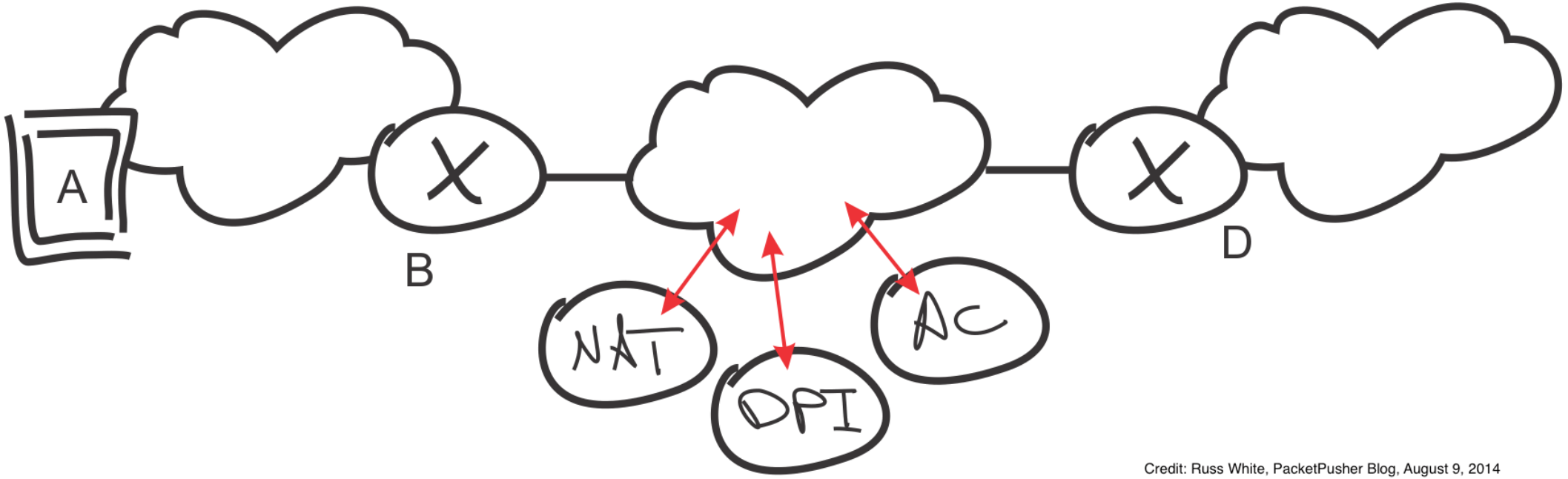
老闆：
馬克！公司剛導入分析系統，弄點什麼來瞧瞧吧！
我想要看最近一個月中國用戶透過手機交易，
針對新產品訂單的分析報告，明早給我！

圖片來源 https://goo.gl/RKFX6c

馬克：
好的! 明早給您。

圖片來源 https://goo.gl/Fai7gZ

設備更新、漏洞修補，讓你忙得要要的？



Credit: Russ White, PacketPusher Blog, August 9, 2014

自定義資安服務鏈架構
無須停機、服務中斷

資安設備機房

圖片來源 https://goo.gl/oedeEK

傳統的封包分析工具，無法處理企業情境式數據包分析

NPB –
App Brokering

Meta Data

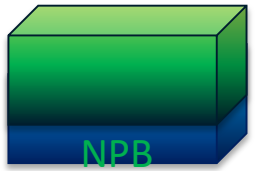
App Filtering

All traffic from Georgia

All voice traffic from HTC
Ones
Someone from S. Africa watching
House of Cards on Netflix on an
iPhone on Vodacom's network

針對應用層
進行進階篩選

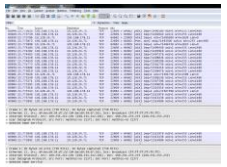
- Netflow分析
- 精確封包萃取



NPB
NPB
Adv. Packet Processing

Hardware AFM
L2-4 Filters

All unique frames going to 10.0.0.0/8
Only 10.0.0.0/8 traffic



Only the first 128 bytes of TCP Port 25 frames
Only TCP Port 25 traffic

去除重複資訊
篩選工具
篩選封包內容
篩選封包內容

Raw Packets

TAP

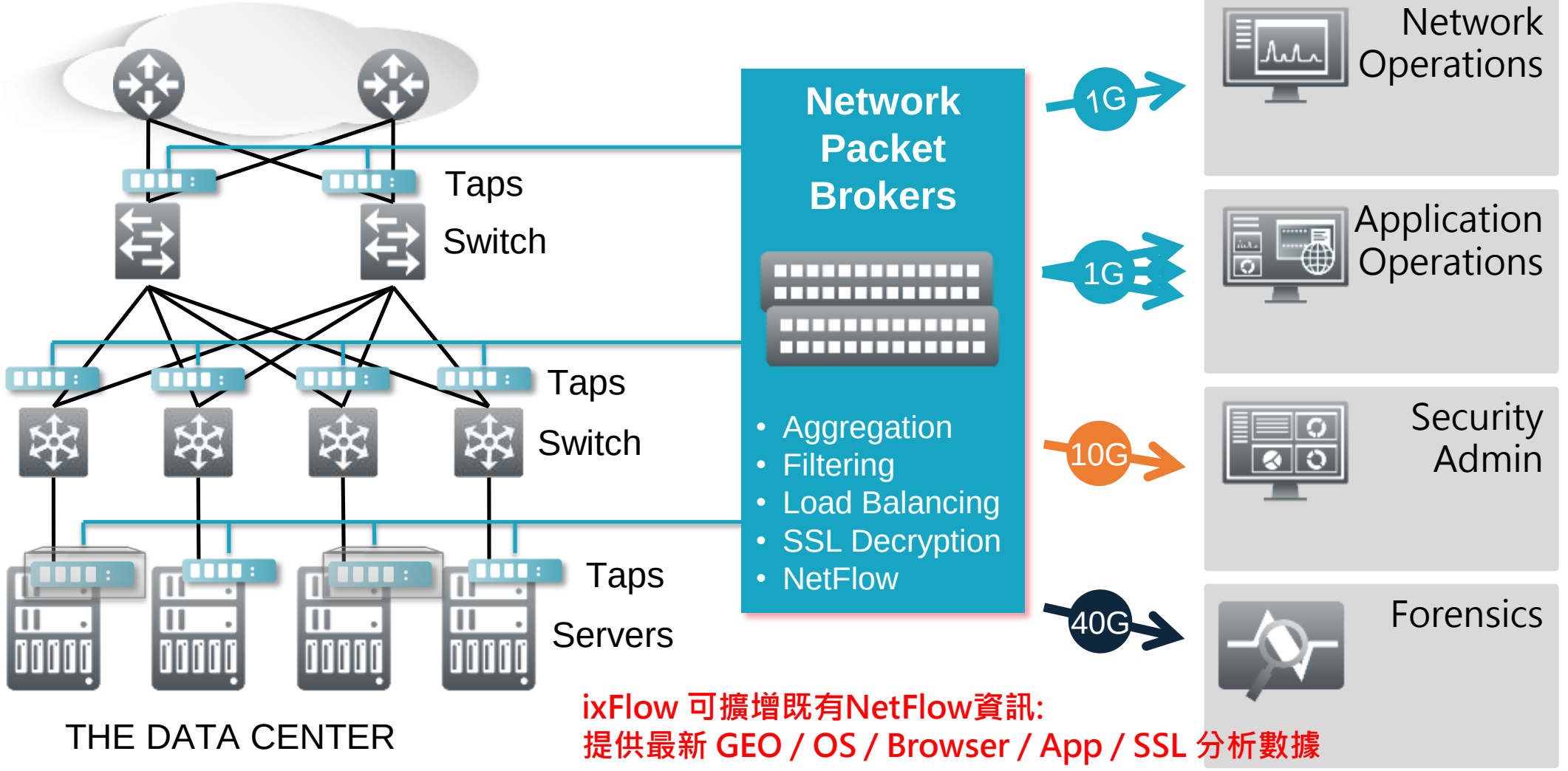
All packets

TAP/SPAN
封包側錄

It Time To Change!

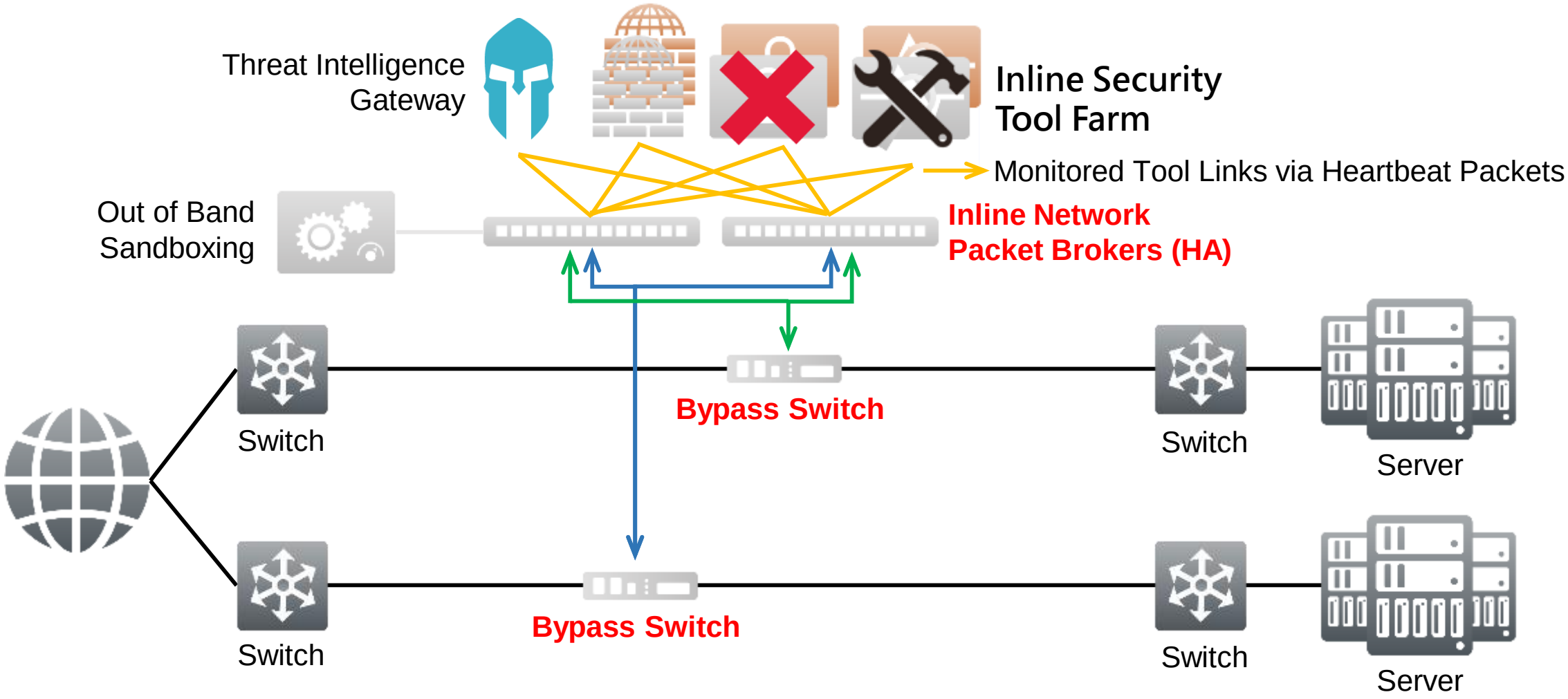
結合最新雲端資源，讓你的數據大聲說話！

- End-to-End Data Access and Distribution



彈性自定義資安服務鏈，不再受限於實體架構限制

- A More Detailed View of a Resilient Security Framework



Summary

圖片來源 https://goo.gl/rr43CE

專業服務 邁向卓越

We Commit To Excellence