顛覆過往資安防禦架構
可視可控一把抓

詹鴻基 Jason
資安顧問

paloalto NETWORKS

Gartner Magic Quadrant - 企業級防火牆領導品牌廠商

1. 連續八年位於企業級防火牆領導地位

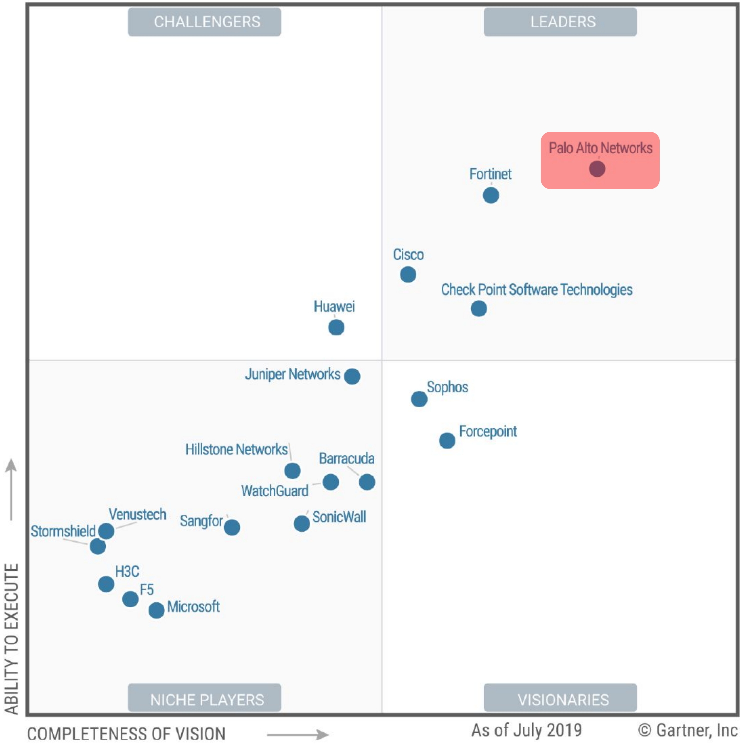
2. 持續引領其他友商真實地反應防火牆市場的需求，同時也引領著企業級防火牆系統的市場與技術繼續向前邁進

3. 相對於其他廠商，Palo Alto Networks是純粹的安全供應商，是所有行業中企業防火牆候選名單的優先選項

4. 客戶對於第七層應用程式識別度滿意度高

5. 網路資訊安全市佔率 #1

Figure 1. Magic Quadrant for Network Firewalls



As of July 2019 © Gartner, Inc

Gartner, Magic Quadrant for Enterprise Network Firewalls, Adam Hils, Jeremy D'Hoinne, Rajpreet Kaur, 4 October 2018

This graphic was published by Gartner, Inc. as part of a larger research document and should be evaluated in the context of the entire document. The Gartner document is available upon request from Palo Alto Networks. Gartner does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner's research organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose. GARTNER is a registered trademark and service mark of Gartner, Inc. and/or its affiliates in the U.S. and internationally, and is used herein with permission. All rights reserved.

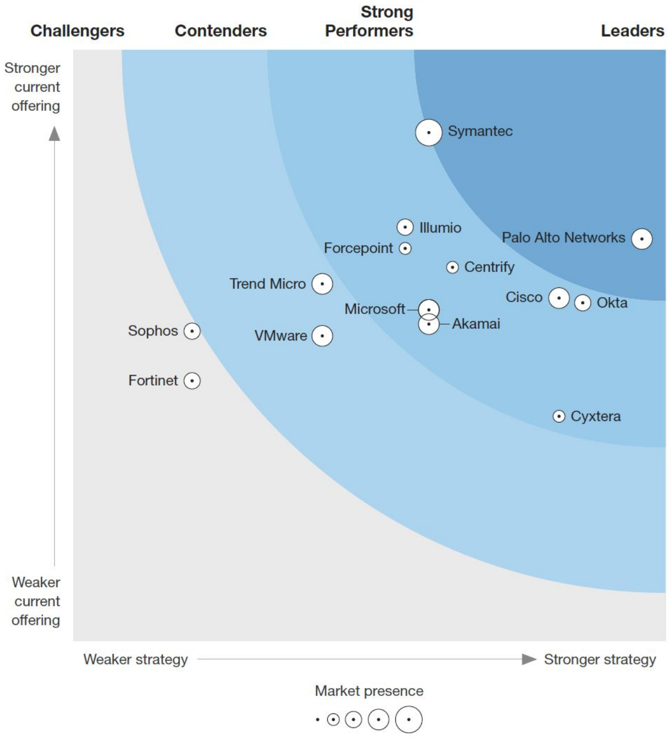
零信任平台領導者

- Forrester’s Zero Trust eXtended (ZTX) Wave rating helps you move toward pragmatic implementations of Zero Trust
- We received the highest score in the strategy category
- In our view, our position validates the Security Operating Platform as an integrated platform that customers can use to implement Zero Trust and prevent successful cyberattacks

THE FORRESTER WAVE™

Zero Trust eXtended (ZTX) Ecosystem Providers

Q4 2018



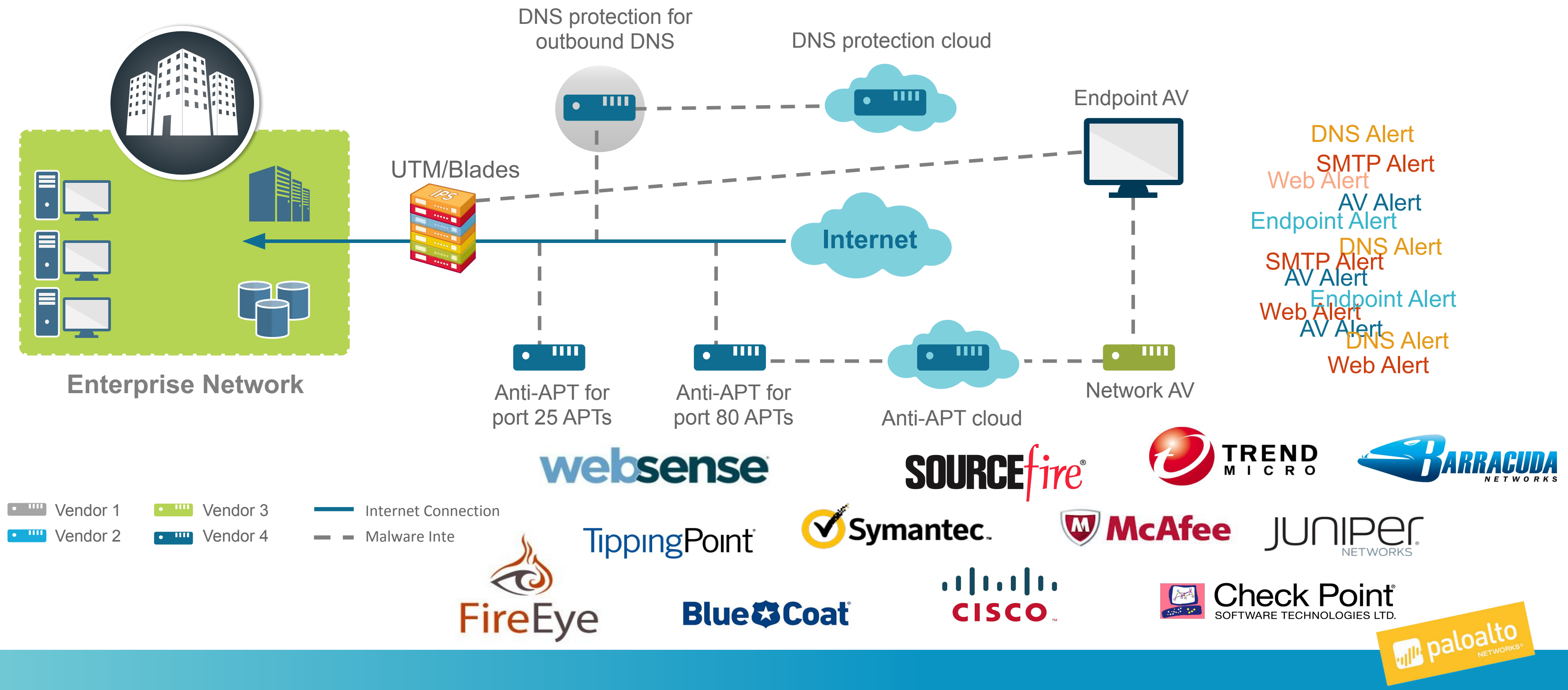
The Forrester Wave™ is copyrighted by Forrester Research, Inc. Forrester and Forrester Wave™ are trademarks of Forrester Research, Inc. The Forrester Wave™ is a graphical representation of Forrester's call on a market and is plotted using a detailed spreadsheet with exposed scores, weightings, and comments. Forrester does not endorse any vendor, product, or service depicted in the Forrester Wave™. Information is based on best available resources. Opinions reflect judgment at the time and are subject to change.

傳統資安架構防護機制的困境

有限的可視化程度

無關聯性

人工手動設定

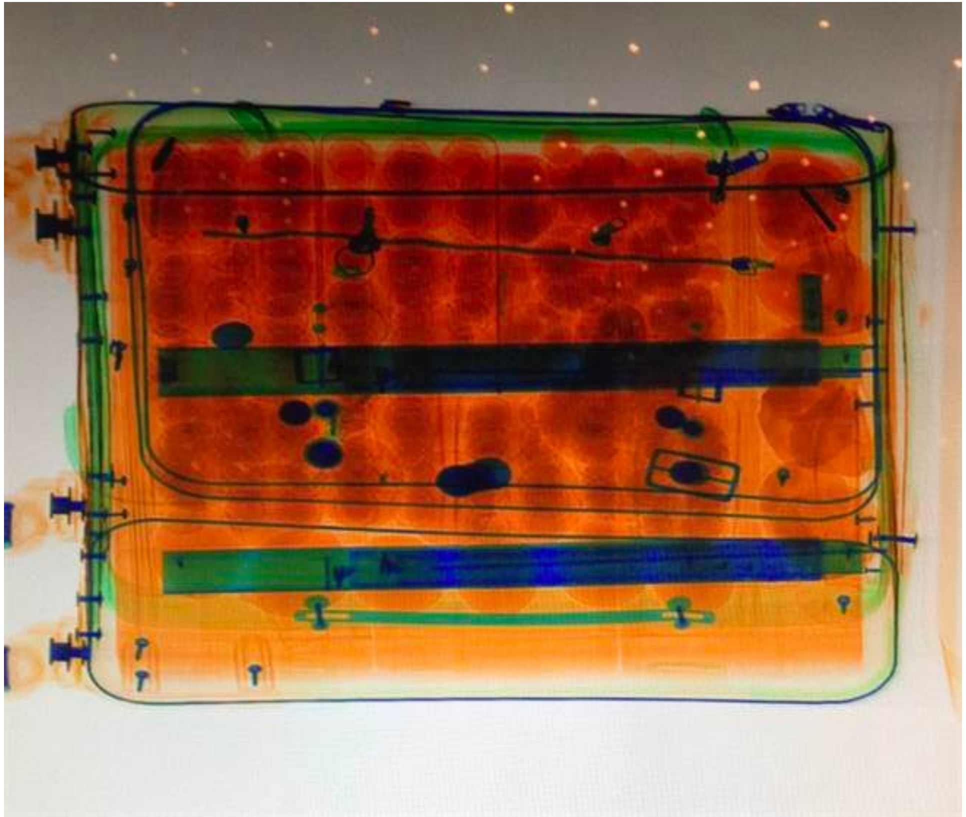


HOW?

Visibility
可視性

L4 Security

L7 Security



Layer 4與Layer 7差異

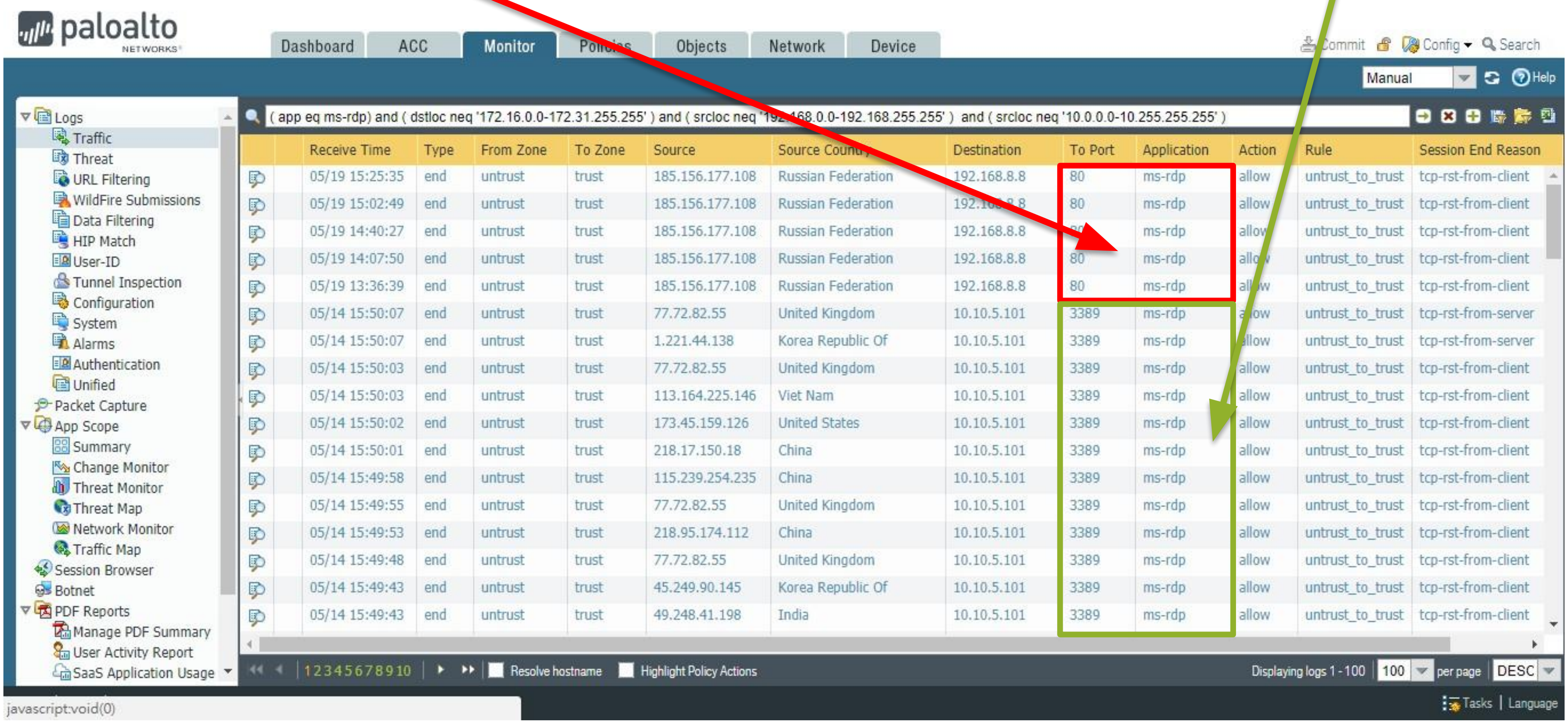
- Layer 4的有侷限性, 僅能針對**Port**來控管, 但無法辨識**應用程式**, 這樣會有被偷渡的風險, 在允許的Port上面運行不正確的應用程式。

- Ms-rdp是跑在3389 port上面, 但下頁圖明顯看出想偷渡在80 Port上, 僅有Layer 7的防火牆在一開始就能夠辨識出來並阻擋。

- Layer 7並非是單純的IPS, 掃毒或是網頁過濾等等資安掃描, Palo Alto Networks的Layer 7是從網路開始辨識**應用程式**, 可以做到**特定Port就跑特定應用程式。**

正確的Port+不正確的應用程式 = “不合法”的存取

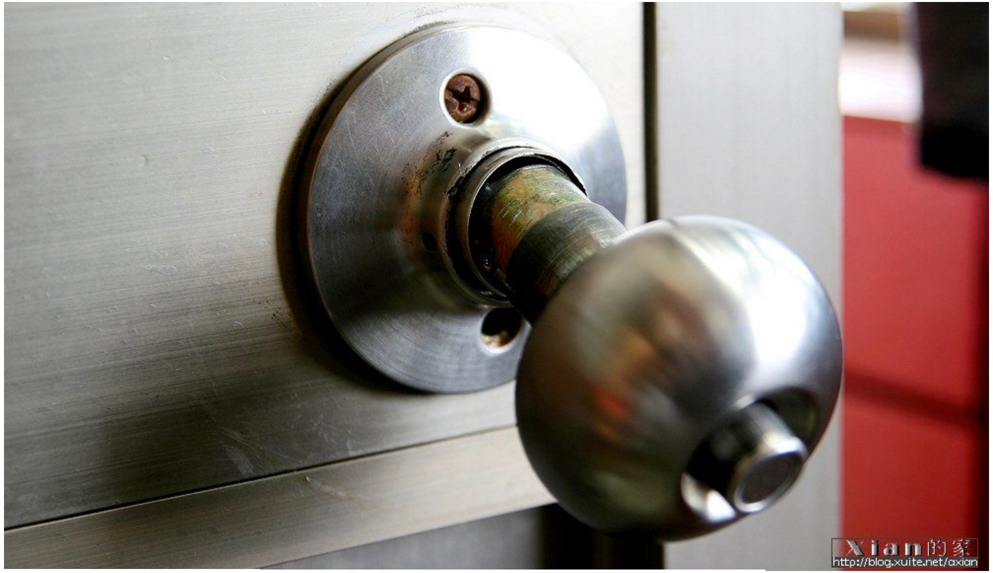
正確的Port+正確的應用程式 = 合法的存取

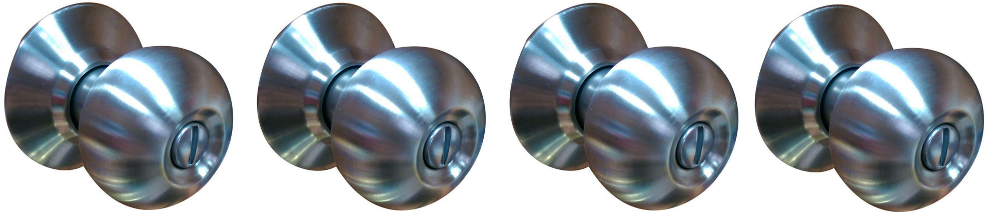


(app eq ms-rdp) and (dstloc neq '172.16.0.0-172.31.255.255') and (srcloc neq '192.168.0.0-192.168.255.255') and (srcloc neq '10.0.0.0-10.255.255.255')

Receive Time	Type	From Zone	To Zone	Source	Source Country	Destination	To Port	Application	Action	Rule	Session End Reason
05/19 15:25:35	end	untrust	trust	185.156.177.108	Russian Federation	192.168.8.8	80	ms-rdp	allow	untrust_to_trust	tcp-rst-from-client
05/19 15:02:49	end	untrust	trust	185.156.177.108	Russian Federation	192.168.8.8	80	ms-rdp	allow	untrust_to_trust	tcp-rst-from-client
05/19 14:40:27	end	untrust	trust	185.156.177.108	Russian Federation	192.168.8.8	80	ms-rdp	allow	untrust_to_trust	tcp-rst-from-client
05/19 14:07:50	end	untrust	trust	185.156.177.108	Russian Federation	192.168.8.8	80	ms-rdp	allow	untrust_to_trust	tcp-rst-from-client
05/19 13:36:39	end	untrust	trust	185.156.177.108	Russian Federation	192.168.8.8	80	ms-rdp	allow	untrust_to_trust	tcp-rst-from-client
05/14 15:50:07	end	untrust	trust	77.72.82.55	United Kingdom	10.10.5.101	3389	ms-rdp	allow	untrust_to_trust	tcp-rst-from-server
05/14 15:50:07	end	untrust	trust	1.221.44.138	Korea Republic Of	10.10.5.101	3389	ms-rdp	allow	untrust_to_trust	tcp-rst-from-server
05/14 15:50:03	end	untrust	trust	77.72.82.55	United Kingdom	10.10.5.101	3389	ms-rdp	allow	untrust_to_trust	tcp-rst-from-client
05/14 15:50:03	end	untrust	trust	113.164.225.146	Viet Nam	10.10.5.101	3389	ms-rdp	allow	untrust_to_trust	tcp-rst-from-client
05/14 15:50:02	end	untrust	trust	173.45.159.126	United States	10.10.5.101	3389	ms-rdp	allow	untrust_to_trust	tcp-rst-from-client
05/14 15:50:01	end	untrust	trust	218.17.150.18	China	10.10.5.101	3389	ms-rdp	allow	untrust_to_trust	tcp-rst-from-client
05/14 15:49:58	end	untrust	trust	115.239.254.235	China	10.10.5.101	3389	ms-rdp	allow	untrust_to_trust	tcp-rst-from-client
05/14 15:49:55	end	untrust	trust	77.72.82.55	United Kingdom	10.10.5.101	3389	ms-rdp	allow	untrust_to_trust	tcp-rst-from-client
05/14 15:49:53	end	untrust	trust	218.95.174.112	China	10.10.5.101	3389	ms-rdp	allow	untrust_to_trust	tcp-rst-from-client
05/14 15:49:48	end	untrust	trust	77.72.82.55	United Kingdom	10.10.5.101	3389	ms-rdp	allow	untrust_to_trust	tcp-rst-from-client
05/14 15:49:43	end	untrust	trust	45.249.90.145	Korea Republic Of	10.10.5.101	3389	ms-rdp	allow	untrust_to_trust	tcp-rst-from-client
05/14 15:49:43	end	untrust	trust	49.248.41.198	India	10.10.5.101	3389	ms-rdp	allow	untrust_to_trust	tcp-rst-from-client

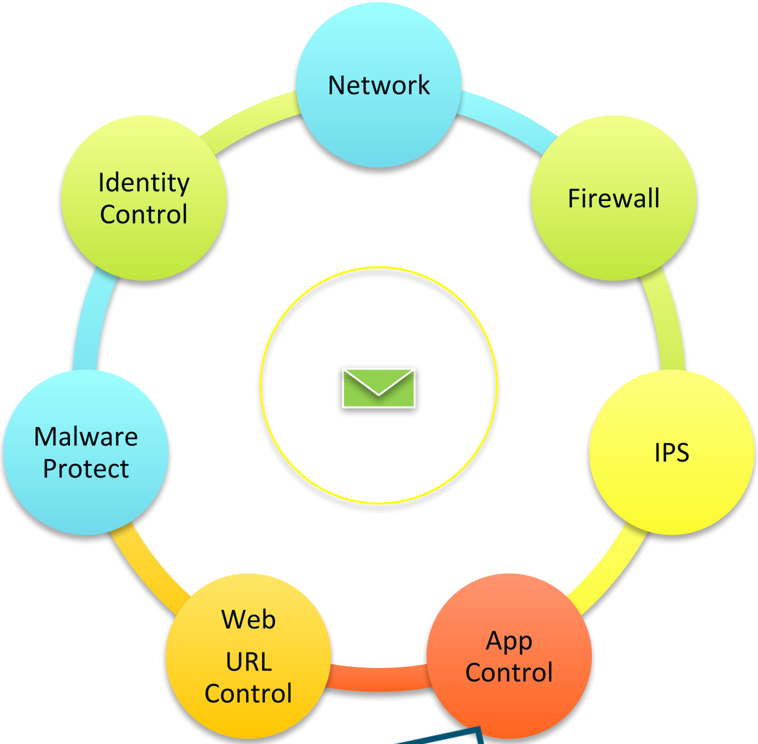
Displaying logs 1 - 100 | 100 per page | DESC

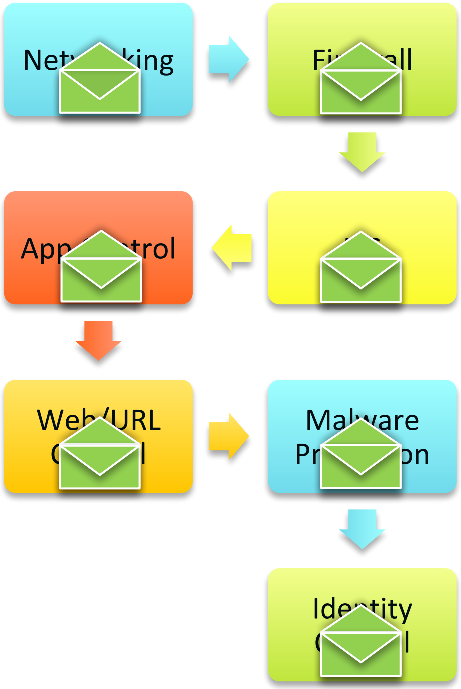

Xian的家
http://blog.xuite.net/axian



12:42
1 2 3
4 5 6
7 8 9
* 0 #

Palo Alto Networks 原生平行處理
vs. 傳統 & UTM & NGFW 防火牆非原生的序列式處理



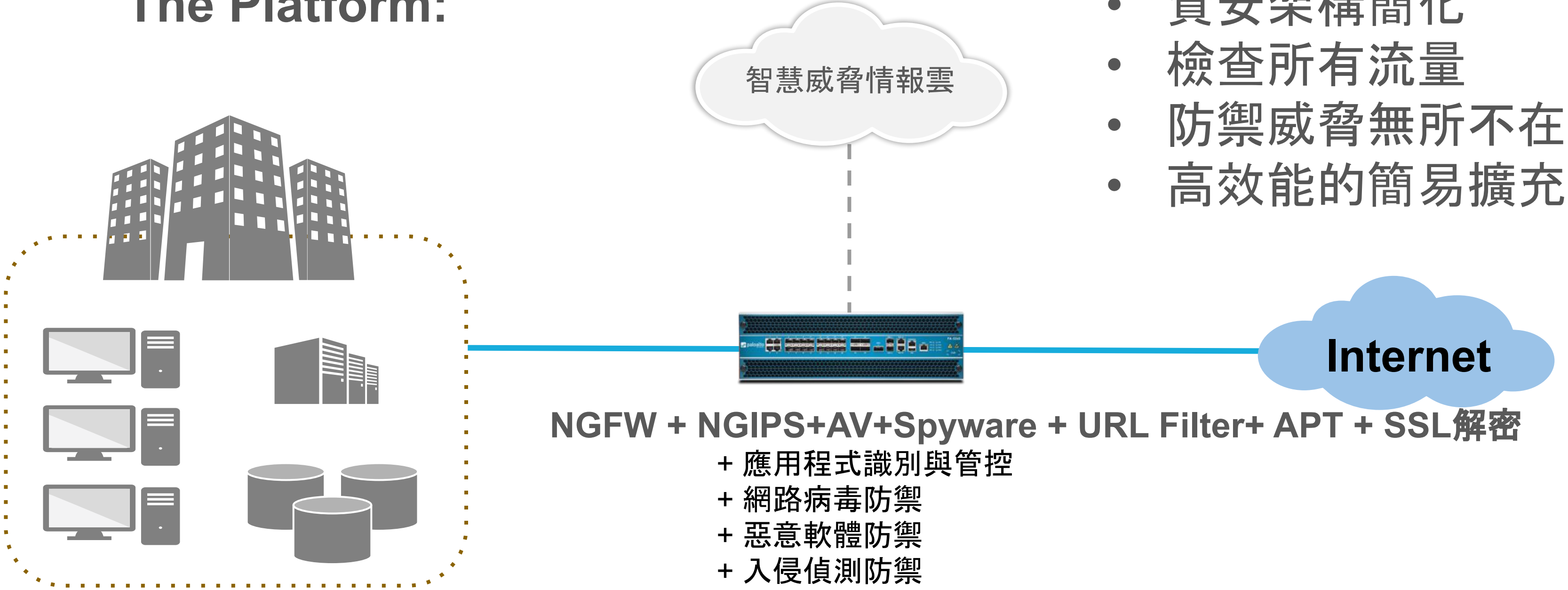


傳統 & UTM & NGFW防火牆
(非原生的序列式處理)

單一資安平臺，全面性防護

The Platform:

- 資安架構簡化
- 檢查所有流量
- 防禦威脅無所不在
- 高效能的簡易擴充彈性



NGFW + NGIPS+AV+Spyware + URL Filter+ APT + SSL解密

+ 應用程式識別與管控
+ 網路病毒防禦
+ 惡意軟體防禦
+ 入侵偵測防禦
+ DNS 防禦
+ SSL 加解密
+ 網址/網頁內容過濾
+ 多功能沙箱分析
+ 智慧化關聯分析報表與管理

資安政策規則優化
POLICY OPTIMIZER

傳統資安政策規則存在於漏洞

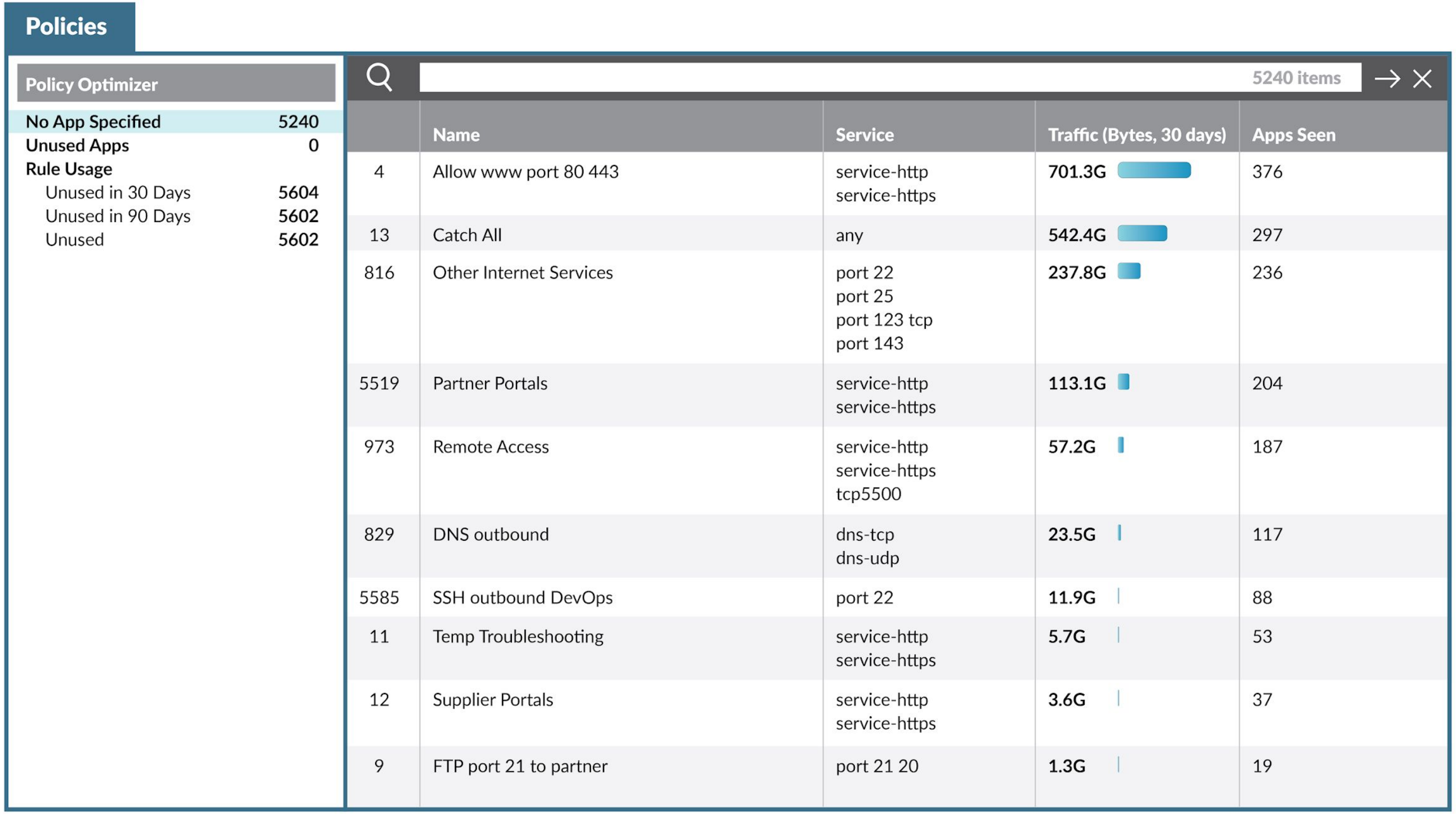
應用程式基礎的資安規則

強化安全:
使用App-ID縮小差距

最小化人為誤設:
違規的主要原因

節省時間
使用直觀的規則

您的舊規則在策略優化器中



Policies

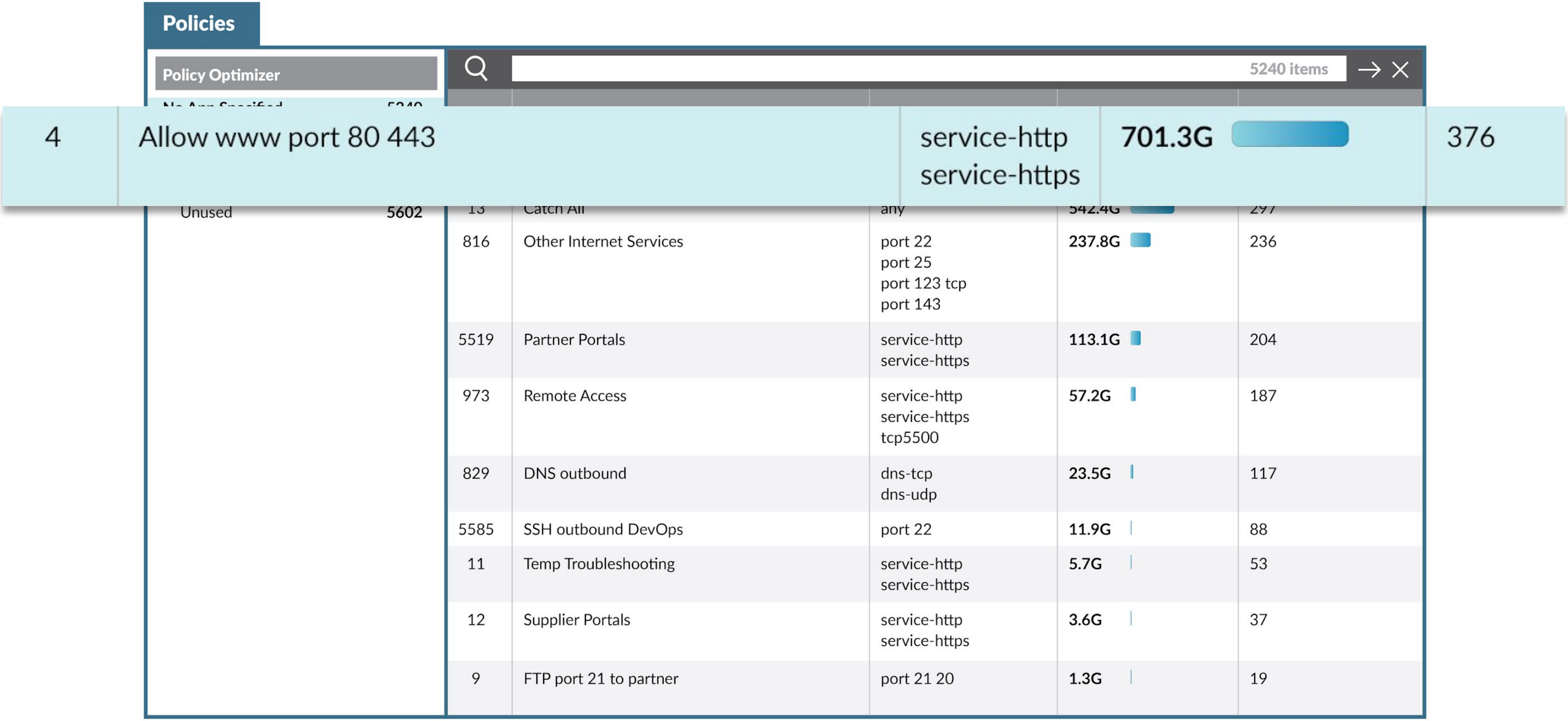
Policy Optimizer

No App Specified	5240
Unused Apps	0
Rule Usage	
Unused in 30 Days	5604
Unused in 90 Days	5602
Unused	5602

5240 items

	Name	Service	Traffic (Bytes, 30 days)	Apps Seen
4	Allow www port 80 443	service-http service-https	701.3G	376
13	Catch All	any	542.4G	297
816	Other Internet Services	port 22 port 25 port 123 tcp port 143	237.8G	236
5519	Partner Portals	service-http service-https	113.1G	204
973	Remote Access	service-http service-https tcp5500	57.2G	187
829	DNS outbound	dns-tcp dns-udp	23.5G	117
5585	SSH outbound DevOps	port 22	11.9G	88
11	Temp Troubleshooting	service-http service-https	5.7G	53
12	Supplier Portals	service-http service-https	3.6G	37
9	FTP port 21 to partner	port 21 20	1.3G	19

第1步：選擇一個優化的傳統規則



Policies

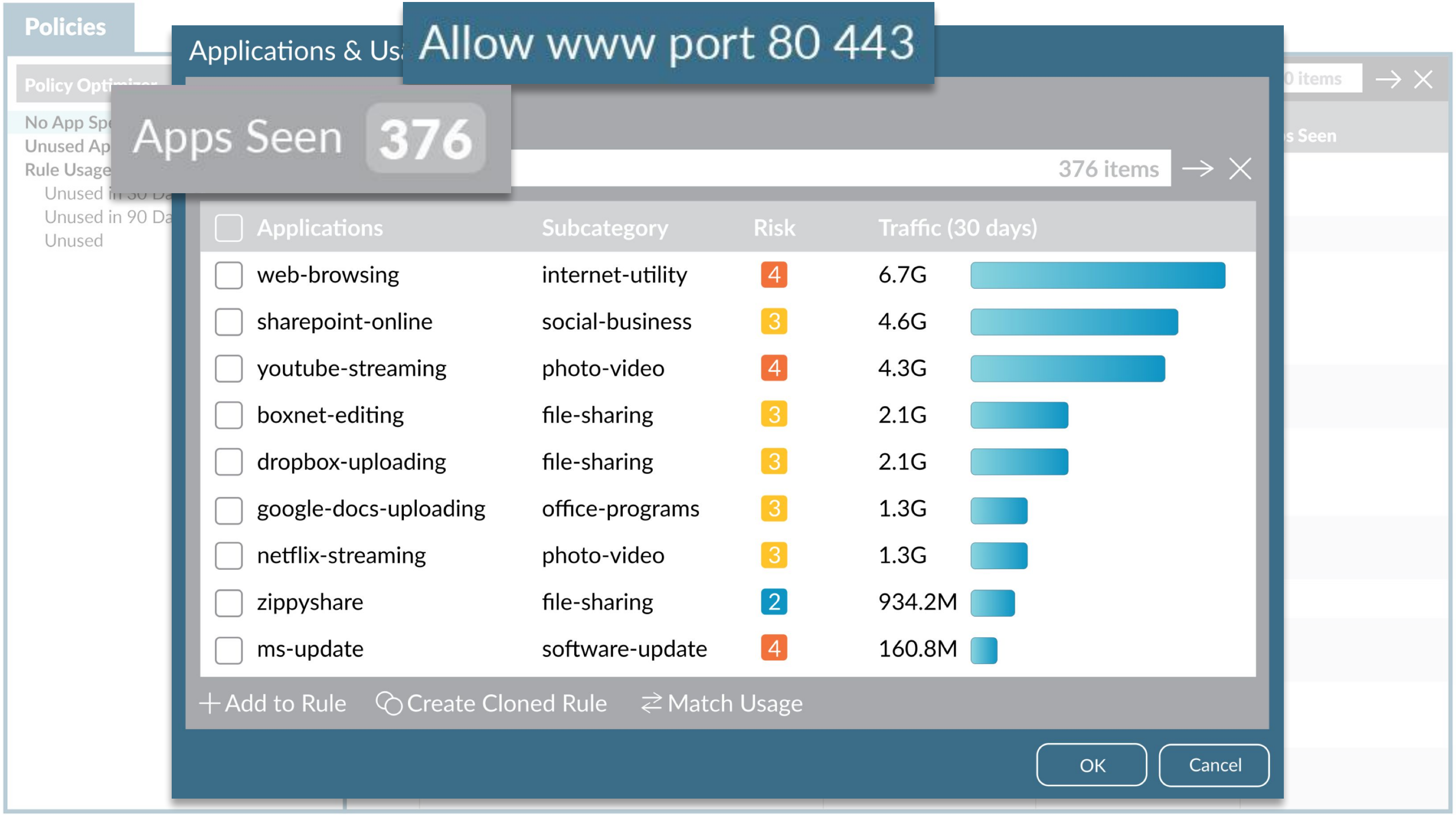
Policy Optimizer

No App Specified	5240
Unused	5602

5240 items

4	Allow www port 80 443	service-http service-https	701.3G	376
13	Catch All	any	542.4G	297
816	Other Internet Services	port 22 port 25 port 123 tcp port 143	237.8G	236
5519	Partner Portals	service-http service-https	113.1G	204
973	Remote Access	service-http service-https tcp5500	57.2G	187
829	DNS outbound	dns-tcp dns-udp	23.5G	117
5585	SSH outbound DevOps	port 22	11.9G	88
11	Temp Troubleshooting	service-http service-https	5.7G	53
12	Supplier Portals	service-http service-https	3.6G	37
9	FTP port 21 to partner	port 21 20	1.3G	19

第2步：查看與規則匹配的所有應用程式



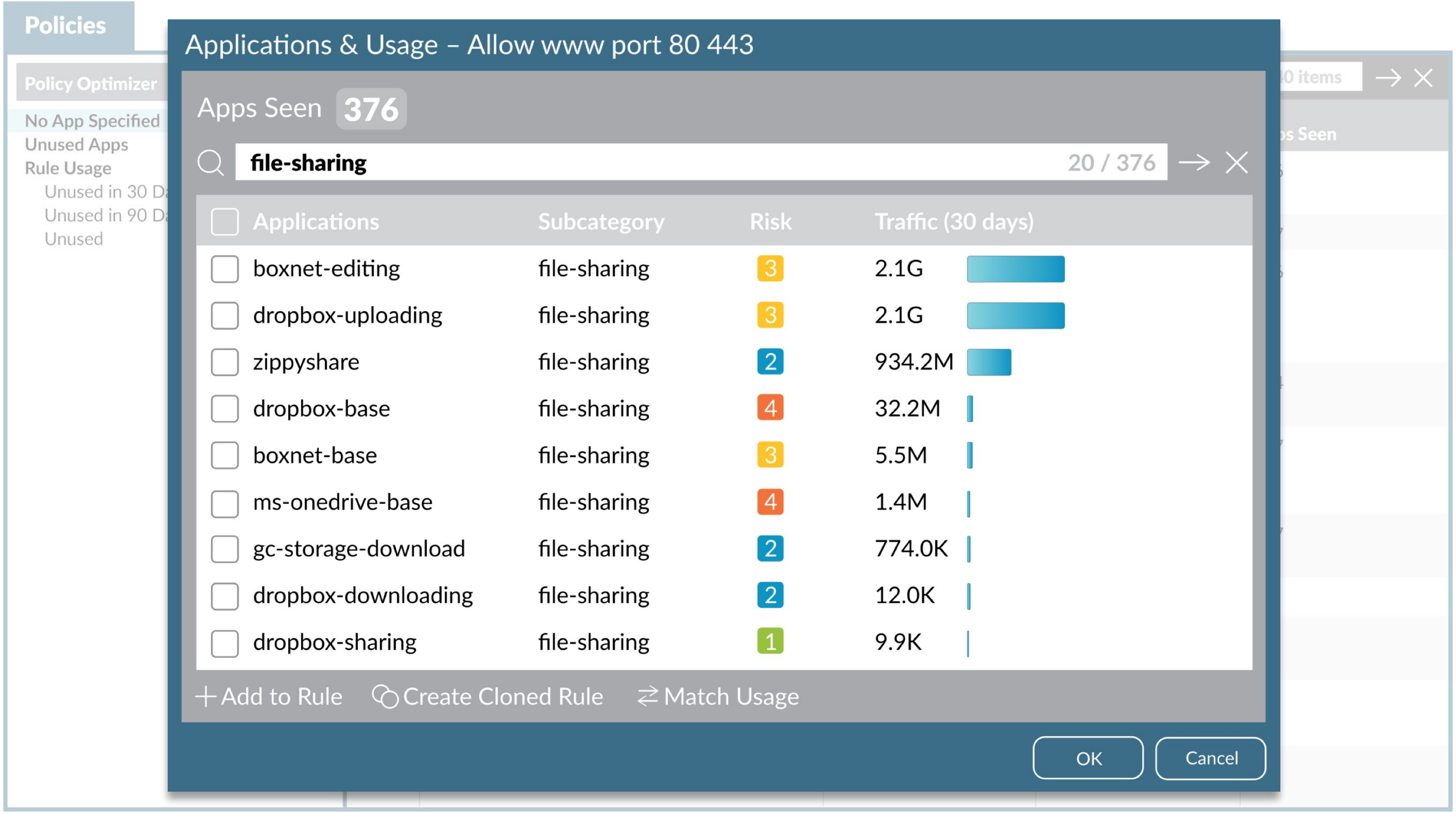
Allow www port 80 443

Apps Seen 376

376 items

□ Applications	Subcategory	Risk	Traffic (30 days)
□ web-browsing	internet-utility	4	6.7G
□ sharepoint-online	social-business	3	4.6G
□ youtube-streaming	photo-video	4	4.3G
□ boxnet-editing	file-sharing	3	2.1G
□ dropbox-uploading	file-sharing	3	2.1G
□ google-docs-uploading	office-programs	3	1.3G
□ netflix-streaming	photo-video	3	1.3G
□ zippyshare	file-sharing	2	934.2M
□ ms-update	software-update	4	160.8M

第3步：篩選file-sharing應用程式



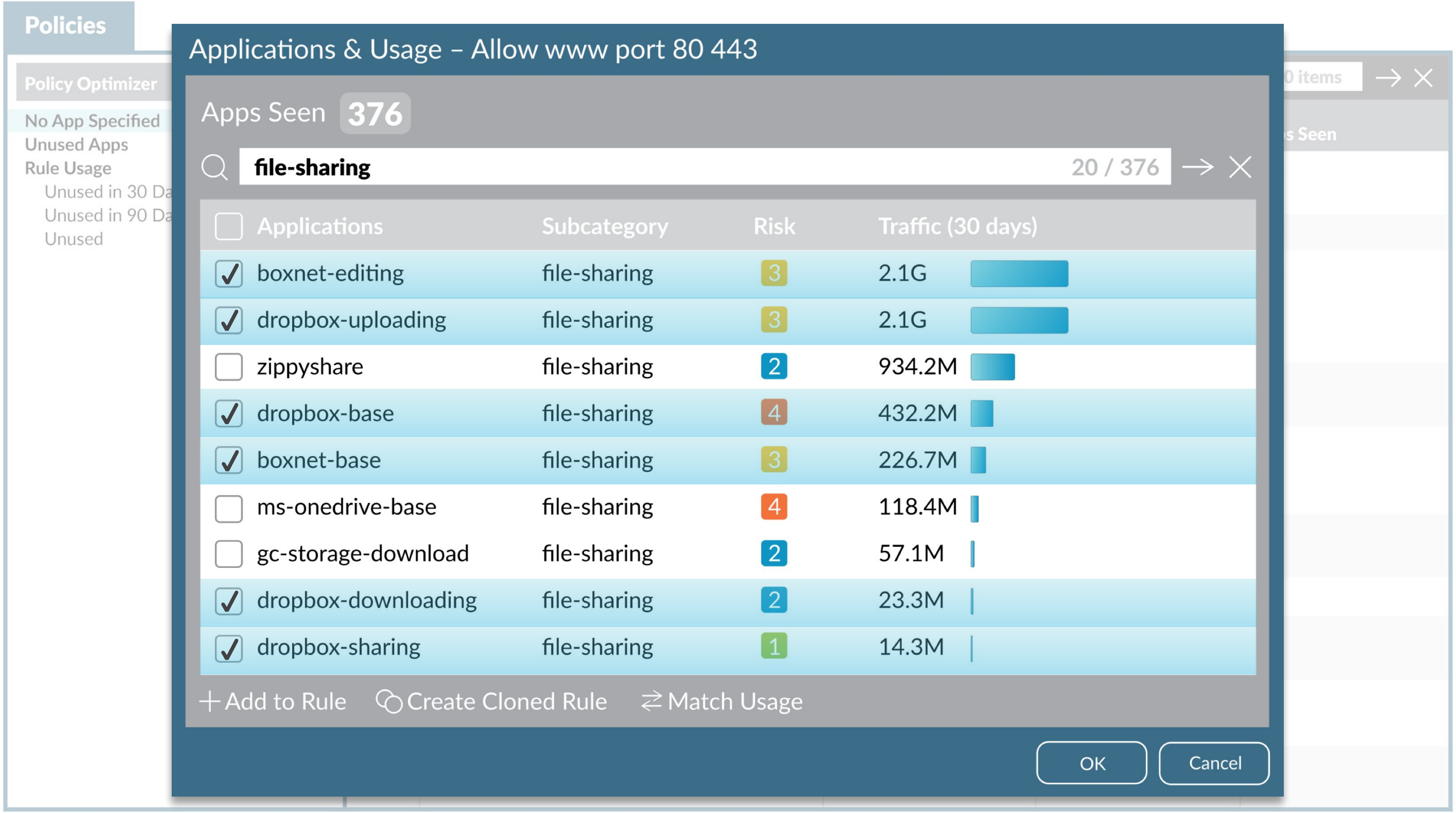
Applications & Usage – Allow www port 80 443

Apps Seen 376

file-sharing 20 / 376

□ Applications	Subcategory	Risk	Traffic (30 days)
□ boxnet-editing	file-sharing	3	2.1G
□ dropbox-uploading	file-sharing	3	2.1G
□ zippyshare	file-sharing	2	934.2M
□ dropbox-base	file-sharing	4	32.2M
□ boxnet-base	file-sharing	3	5.5M
□ ms-onedrive-base	file-sharing	4	1.4M
□ gc-storage-download	file-sharing	2	774.0K
□ dropbox-downloading	file-sharing	2	12.0K
□ dropbox-sharing	file-sharing	1	9.9K

第4步：選擇允許使用的應用程式



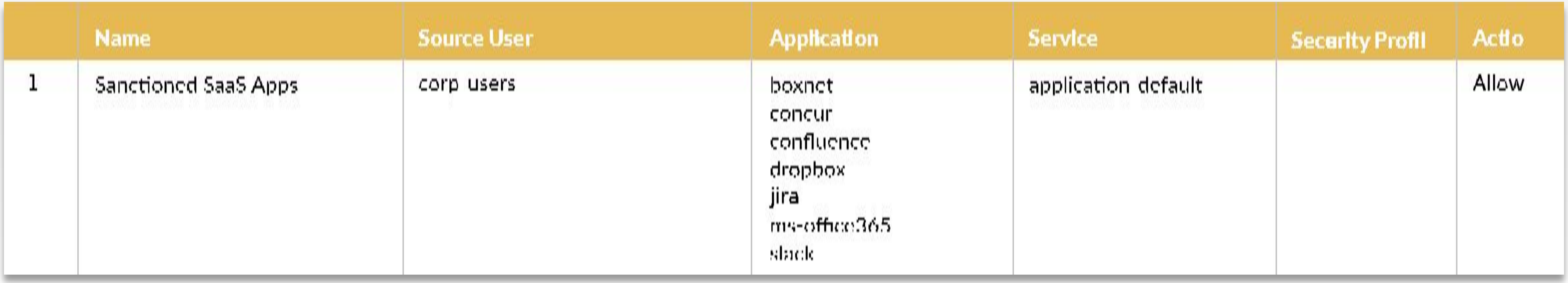
Applications & Usage – Allow www port 80 443

Apps Seen 376

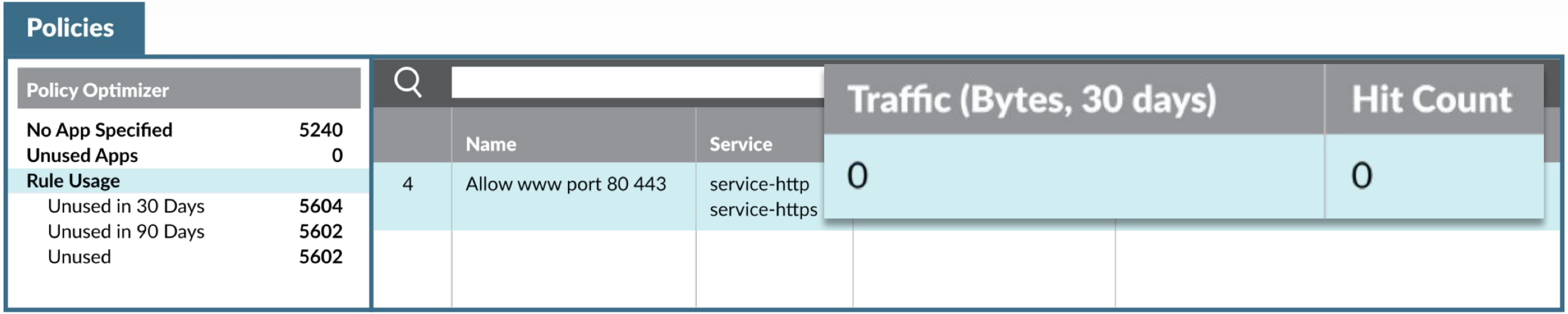
file-sharing 20 / 376

□ Applications	Subcategory	Risk	Traffic (30 days)
☑ boxnet-editing	file-sharing	3	2.1G
☑ dropbox-uploading	file-sharing	3	2.1G
□ zippyshare	file-sharing	2	934.2M
☑ dropbox-base	file-sharing	4	432.2M
☑ boxnet-base	file-sharing	3	226.7M
□ ms-onedrive-base	file-sharing	4	118.4M
□ gc-storage-download	file-sharing	2	57.1M
☑ dropbox-downloading	file-sharing	2	23.3M
☑ dropbox-sharing	file-sharing	1	14.3M

基於APP的規則結果



	Name	Source User	Application	Service	Security Profil	Actio
1	Sanctioned SaaS Apps	corp users	boxnet concur confluence dropbox jira ms-office365 slack	application default		Allow

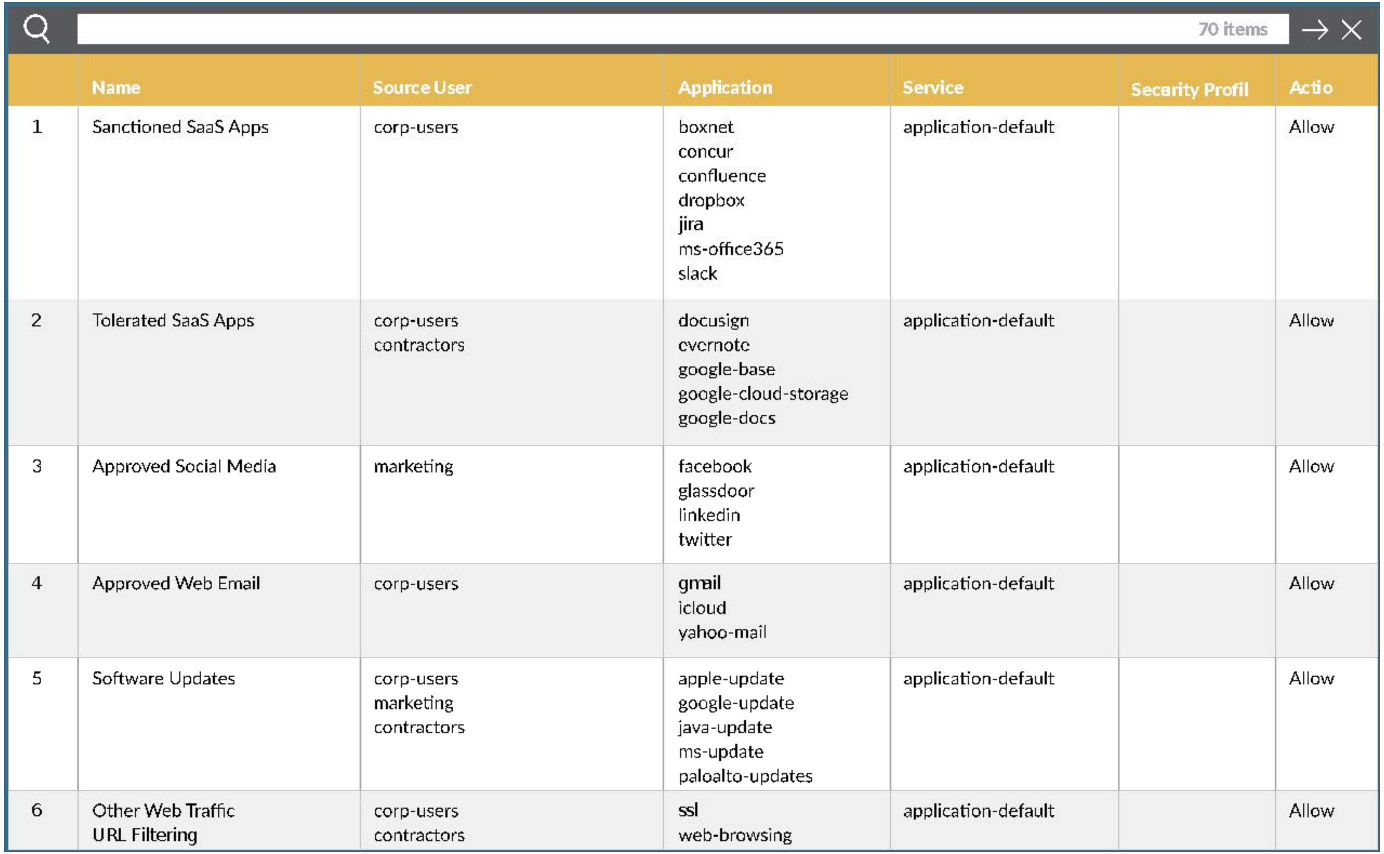


Policies

Policy Optimizer	
No App Specified	5240
Unused Apps	0
Rule Usage	
Unused in 30 Days	5604
Unused in 90 Days	5602
Unused	5602

	Name	Service	Traffic (Bytes, 30 days)	Hit Count
4	Allow www port 80 443	service-http service-https	0	0

最終結果：基於APP的規則避免了策略疏漏



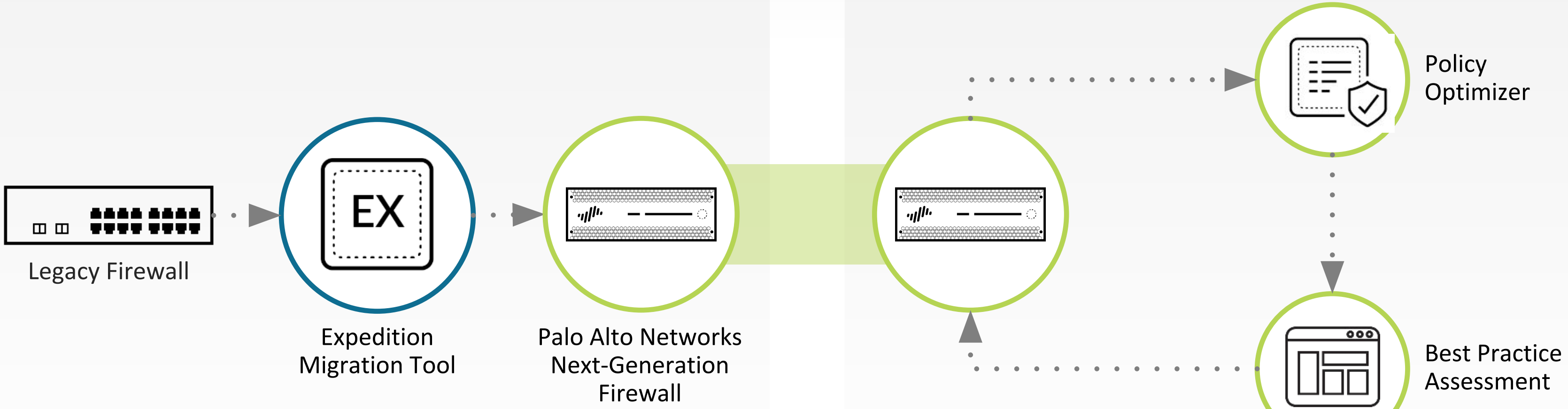
70 items

	Name	Source User	Application	Service	Security Profil	Actio
1	Sanctioned SaaS Apps	corp-users	boxnet concur confluence dropbox jira ms-office365 slack	application-default		Allow
2	Tolerated SaaS Apps	corp-users contractors	docusign evernote google-base google-cloud-storage google-docs	application-default		Allow
3	Approved Social Media	marketing	facebook glassdoor linkedin twitter	application-default		Allow
4	Approved Web Email	corp-users	gmail icloud yahoo-mail	application-default		Allow
5	Software Updates	corp-users marketing contractors	apple-update google-update java-update ms-update paloalto-updates	application-default		Allow
6	Other Web Traffic URL Filtering	corp-users contractors	ssl web-browsing	application-default		Allow

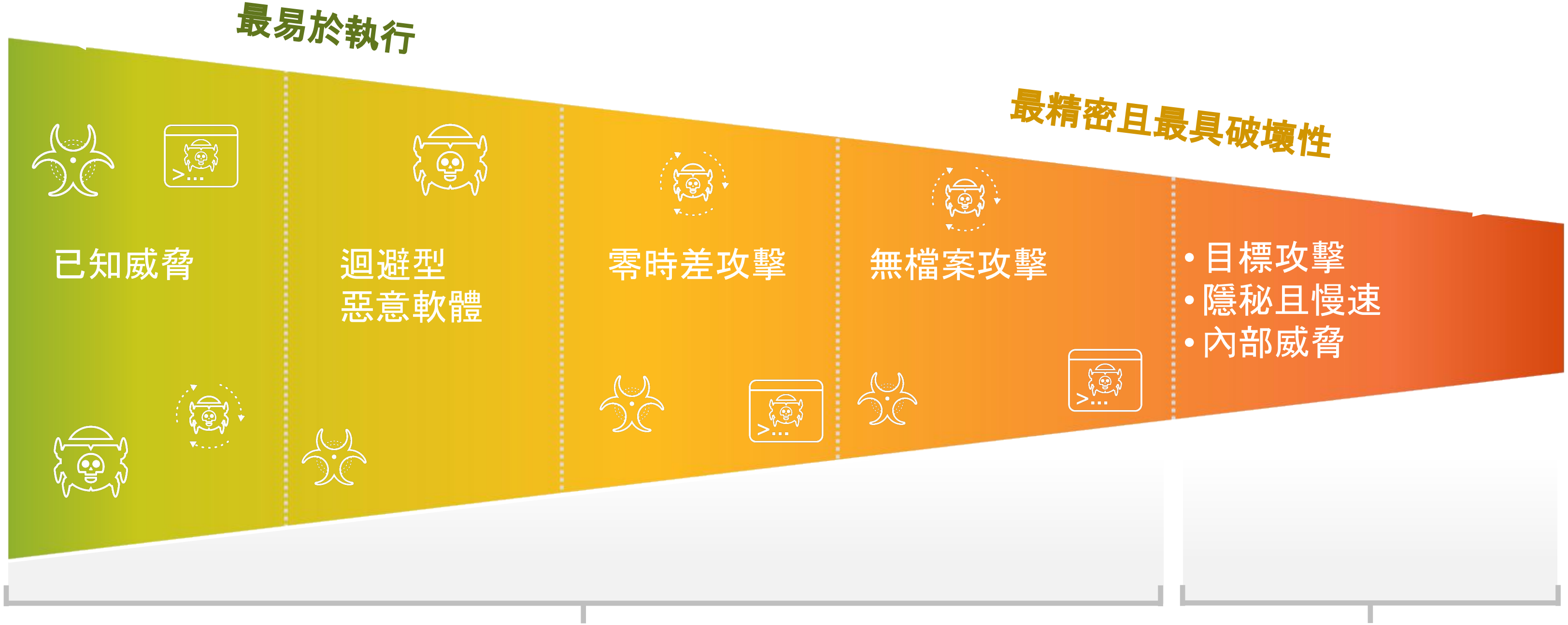
從基於舊的埠資安規則轉換到應用程式資安規則

1. 使用Expedition 遷移工具將規則從舊版 FW遷移到我們的NGFW

2. 使用策略優化器和最佳實踐評估的持續優化過程


Legacy Firewall
EX
Expedition Migration Tool
Palo Alto Networks Next-Generation Firewall
Policy Optimizer
Best Practice Assessment

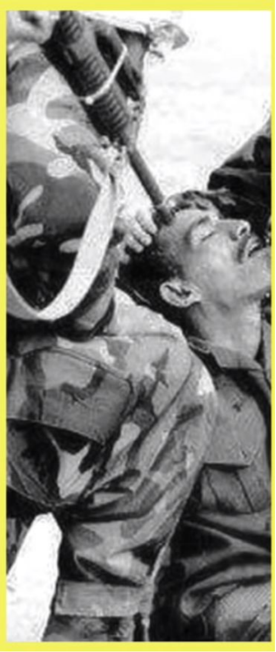
針對進階攻擊需要採用偵測與回應 (雪中送炭? 錦上添花?)

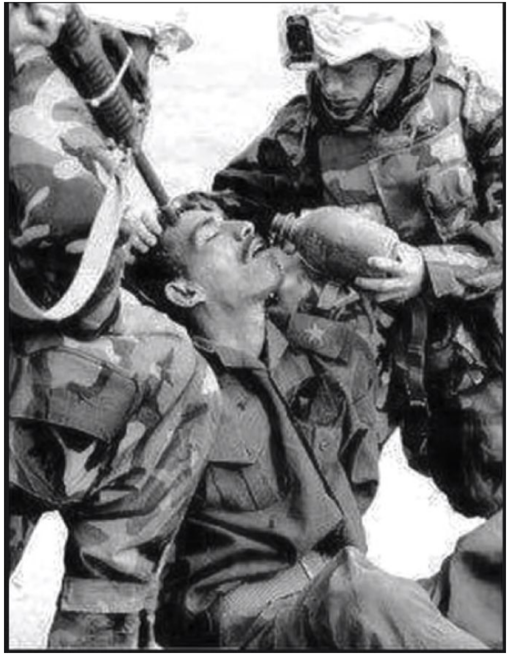


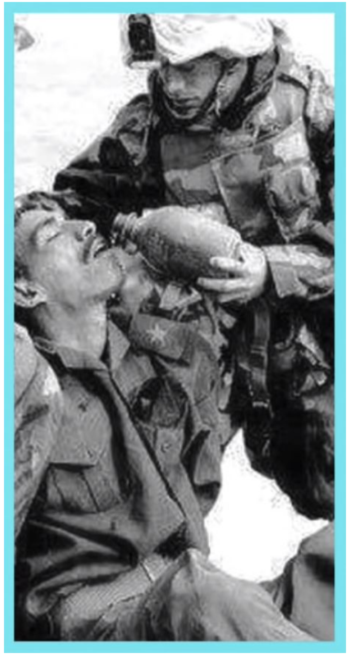
99% 以上的攻擊可透過
正確的工具來防禦

少於 1% 需要採用機器學習,
長時間進行跨層分析

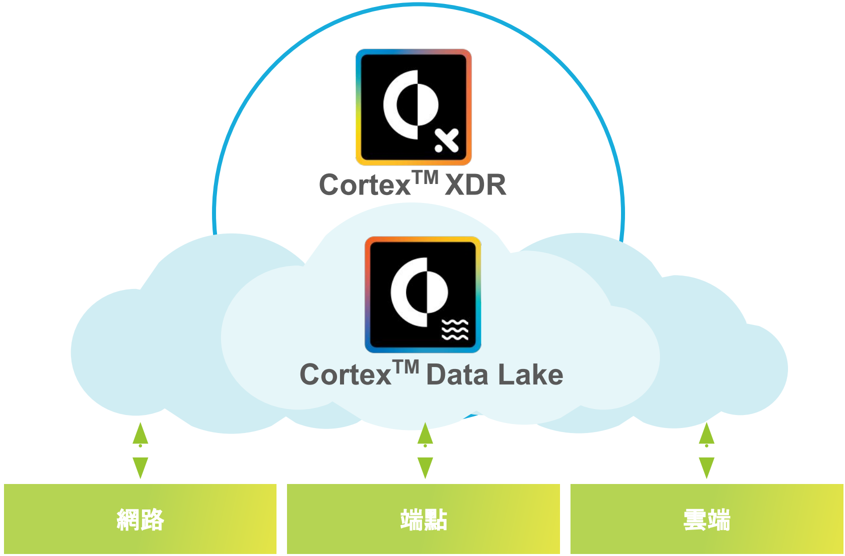
帶風向 >>>>>> 查證 = 浪費時間







跨越網路、端點和雲端的偵測與回應

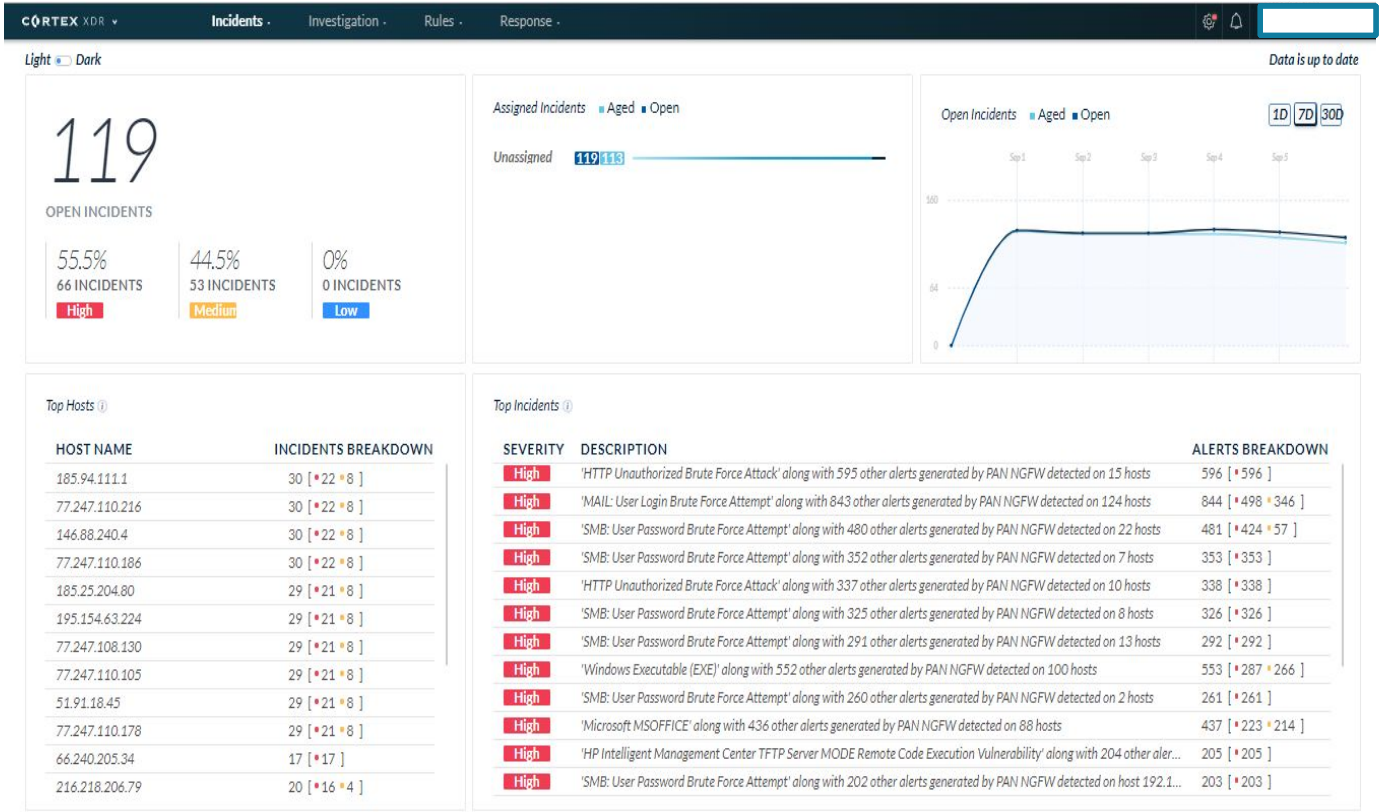


使用豐富的數據與雲端行為分析來自動偵測攻擊

整合數據來找出根本原因以加速調查

與執行點緊密整合以阻止威脅並調整防禦措施

案例分享 - 縮限問題範圍與查找



119

OPEN INCIDENTS

55.5%	44.5%	0%
66 INCIDENTS	53 INCIDENTS	0 INCIDENTS
High	Medium	Low

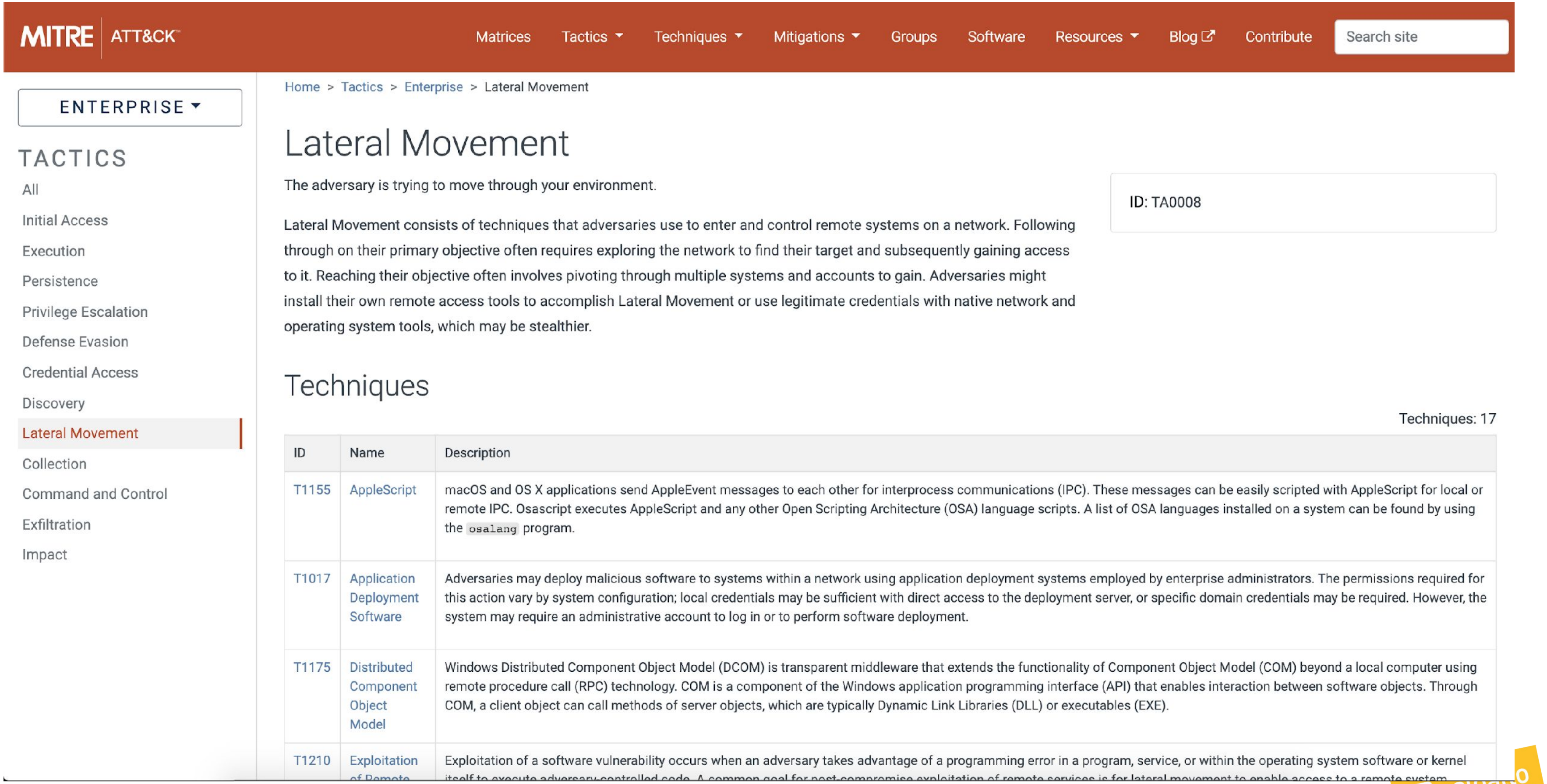
Top Hosts

HOST NAME	INCIDENTS BREAKDOWN
185.94.111.1	30 [•22 •8]
77.247.110.216	30 [•22 •8]
146.88.240.4	30 [•22 •8]
77.247.110.186	30 [•22 •8]
185.25.204.80	29 [•21 •8]
195.154.63.224	29 [•21 •8]
77.247.108.130	29 [•21 •8]
77.247.110.105	29 [•21 •8]
51.91.18.45	29 [•21 •8]
77.247.110.178	29 [•21 •8]
66.240.205.34	17 [•17]
216.218.206.79	20 [•16 •4]

Top Incidents

SEVERITY	DESCRIPTION	ALERTS BREAKDOWN
High	'HTTP Unauthorized Brute Force Attack' along with 595 other alerts generated by PAN NGFW detected on 15 hosts	596 [•596]
High	'MAIL: User Login Brute Force Attempt' along with 843 other alerts generated by PAN NGFW detected on 124 hosts	844 [•498 •346]
High	'SMB: User Password Brute Force Attempt' along with 480 other alerts generated by PAN NGFW detected on 22 hosts	481 [•424 •57]
High	'SMB: User Password Brute Force Attempt' along with 352 other alerts generated by PAN NGFW detected on 7 hosts	353 [•353]
High	'HTTP Unauthorized Brute Force Attack' along with 337 other alerts generated by PAN NGFW detected on 10 hosts	338 [•338]
High	'SMB: User Password Brute Force Attempt' along with 325 other alerts generated by PAN NGFW detected on 8 hosts	326 [•326]
High	'SMB: User Password Brute Force Attempt' along with 291 other alerts generated by PAN NGFW detected on 13 hosts	292 [•292]
High	'Windows Executable (EXE)' along with 552 other alerts generated by PAN NGFW detected on 100 hosts	553 [•287 •266]
High	'SMB: User Password Brute Force Attempt' along with 260 other alerts generated by PAN NGFW detected on 2 hosts	261 [•261]
High	'Microsoft MSOFFICE' along with 436 other alerts generated by PAN NGFW detected on 88 hosts	437 [•223 •214]
High	'HP Intelligent Management Center TFTP Server MODE Remote Code Execution Vulnerability' along with 204 other aler...	205 [•205]
High	'SMB: User Password Brute Force Attempt' along with 202 other alerts generated by PAN NGFW detected on host 192.1...	203 [•203]

縮限問題範圍與查找 - 1



Lateral Movement

The adversary is trying to move through your environment.

Lateral Movement consists of techniques that adversaries use to enter and control remote systems on a network. Following through on their primary objective often requires exploring the network to find their target and subsequently gaining access to it. Reaching their objective often involves pivoting through multiple systems and accounts to gain. Adversaries might install their own remote access tools to accomplish Lateral Movement or use legitimate credentials with native network and operating system tools, which may be stealthier.

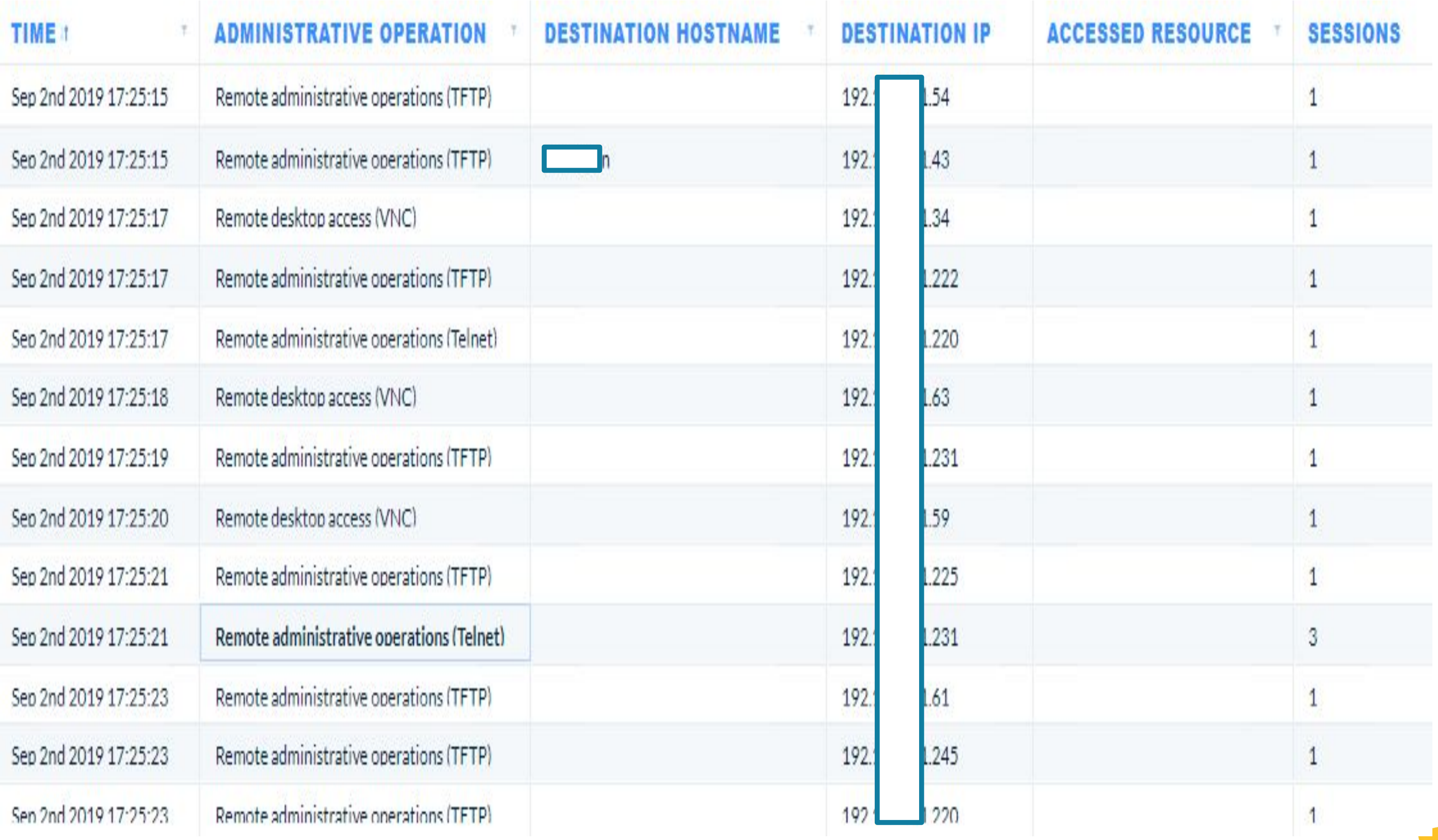
ID: TA0008

Techniques

Techniques: 17

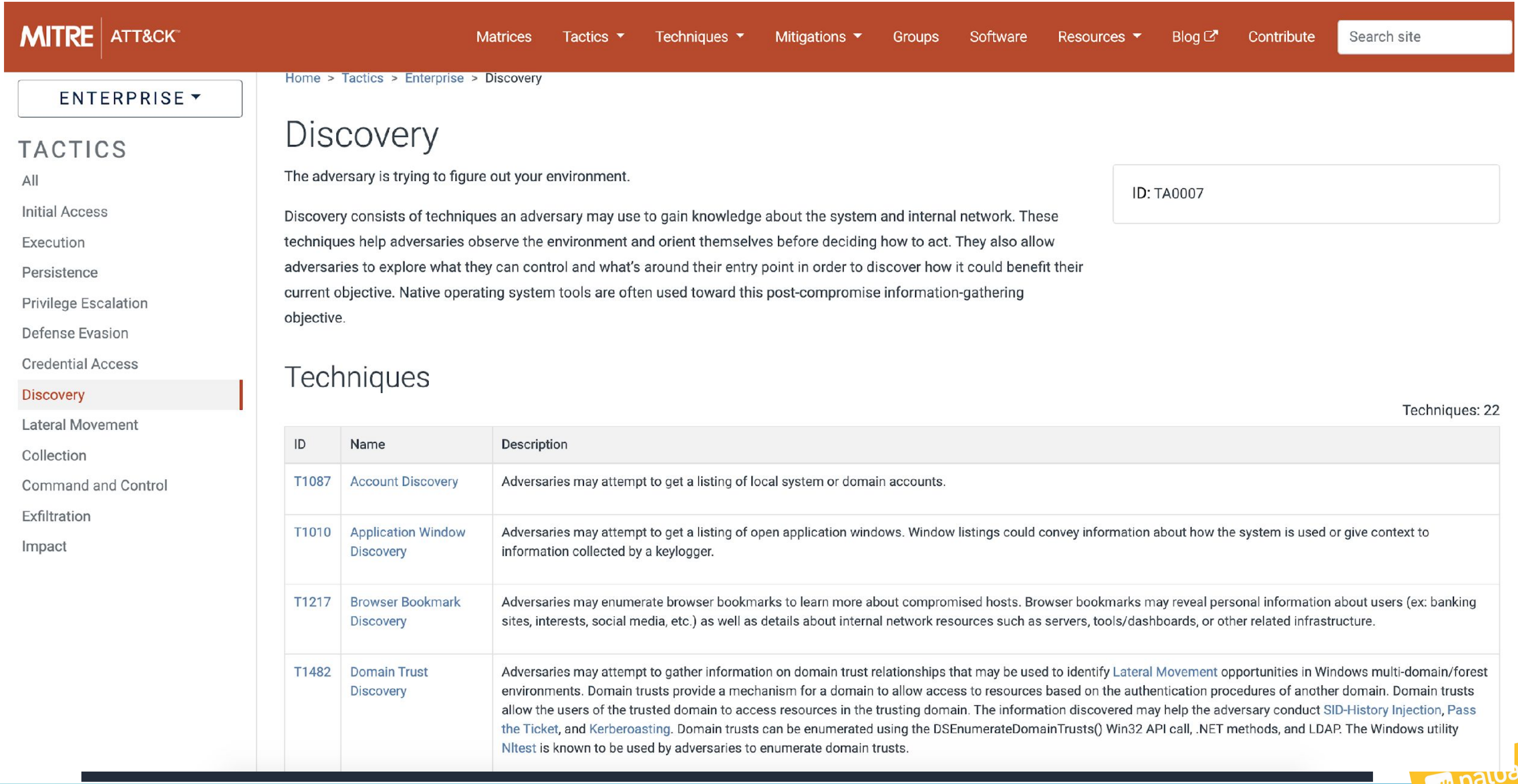
ID	Name	Description
T1155	AppleScript	macOS and OS X applications send AppleEvent messages to each other for interprocess communications (IPC). These messages can be easily scripted with AppleScript for local or remote IPC. Osascript executes AppleScript and any other Open Scripting Architecture (OSA) language scripts. A list of OSA languages installed on a system can be found by using the `osalang` program.
T1017	Application Deployment Software	Adversaries may deploy malicious software to systems within a network using application deployment systems employed by enterprise administrators. The permissions required for this action vary by system configuration; local credentials may be sufficient with direct access to the deployment server, or specific domain credentials may be required. However, the system may require an administrative account to log in or to perform software deployment.
T1175	Distributed Component Object Model	Windows Distributed Component Object Model (DCOM) is transparent middleware that extends the functionality of Component Object Model (COM) beyond a local computer using remote procedure call (RPC) technology. COM is a component of the Windows application programming interface (API) that enables interaction between software objects. Through COM, a client object can call methods of server objects, which are typically Dynamic Link Libraries (DLL) or executables (EXE).
T1210	Exploitation of Remote	Exploitation of a software vulnerability occurs when an adversary takes advantage of a programming error in a program, service, or within the operating system software or kernel itself to execute adversary-controlled code. A common goal for post-compromise exploitation of remote services is for lateral movement to enable access to a remote system.

縮限問題範圍與查找 - 1



TIME	ADMINISTRATIVE OPERATION	DESTINATION HOSTNAME	DESTINATION IP	ACCESSED RESOURCE	SESSIONS
Sep 2nd 2019 17:25:15	Remote administrative operations (TFTP)		192.[redacted].54		1
Sep 2nd 2019 17:25:15	Remote administrative operations (TFTP)	[redacted]	192.[redacted].43		1
Sep 2nd 2019 17:25:17	Remote desktop access (VNC)		192.[redacted].34		1
Sep 2nd 2019 17:25:17	Remote administrative operations (TFTP)		192.[redacted].222		1
Sep 2nd 2019 17:25:17	Remote administrative operations (Telnet)		192.[redacted].220		1
Sep 2nd 2019 17:25:18	Remote desktop access (VNC)		192.[redacted].63		1
Sep 2nd 2019 17:25:19	Remote administrative operations (TFTP)		192.[redacted].231		1
Sep 2nd 2019 17:25:20	Remote desktop access (VNC)		192.[redacted].59		1
Sep 2nd 2019 17:25:21	Remote administrative operations (TFTP)		192.[redacted].225		1
Sep 2nd 2019 17:25:21	Remote administrative operations (Telnet)		192.[redacted].231		3
Sep 2nd 2019 17:25:23	Remote administrative operations (TFTP)		192.[redacted].61		1
Sep 2nd 2019 17:25:23	Remote administrative operations (TFTP)		192.[redacted].245		1
Sep 2nd 2019 17:25:23	Remote administrative operations (TFTP)		192.[redacted].220		1

縮限問題範圍與查找 - 2



Discovery

The adversary is trying to figure out your environment.

Discovery consists of techniques an adversary may use to gain knowledge about the system and internal network. These techniques help adversaries observe the environment and orient themselves before deciding how to act. They also allow adversaries to explore what they can control and what's around their entry point in order to discover how it could benefit their current objective. Native operating system tools are often used toward this post-compromise information-gathering objective.

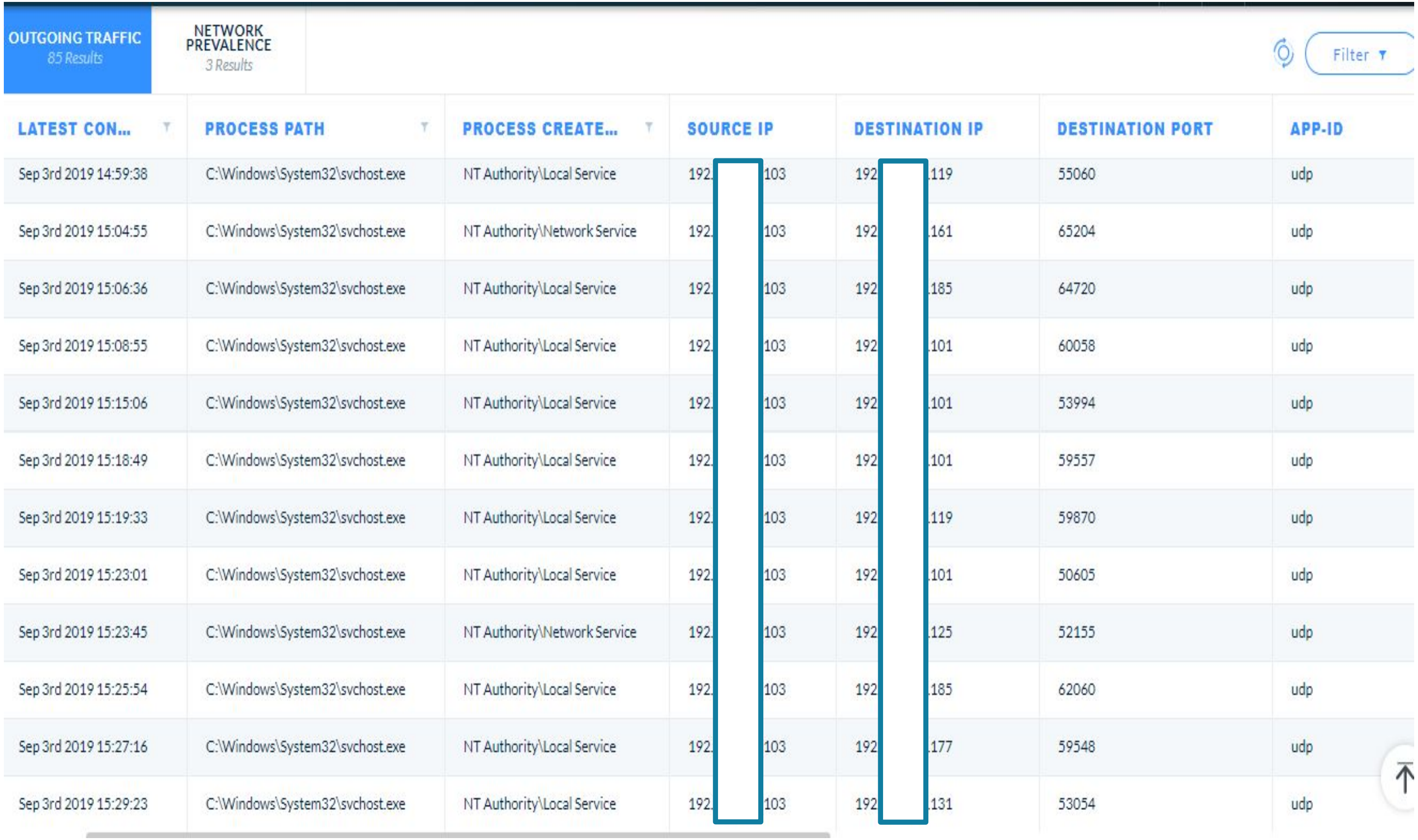
ID: TA0007

Techniques

Techniques: 22

ID	Name	Description
T1087	Account Discovery	Adversaries may attempt to get a listing of local system or domain accounts.
T1010	Application Window Discovery	Adversaries may attempt to get a listing of open application windows. Window listings could convey information about how the system is used or give context to information collected by a keylogger.
T1217	Browser Bookmark Discovery	Adversaries may enumerate browser bookmarks to learn more about compromised hosts. Browser bookmarks may reveal personal information about users (ex: banking sites, interests, social media, etc.) as well as details about internal network resources such as servers, tools/dashboards, or other related infrastructure.
T1482	Domain Trust Discovery	Adversaries may attempt to gather information on domain trust relationships that may be used to identify Lateral Movement opportunities in Windows multi-domain/forest environments. Domain trusts provide a mechanism for a domain to allow access to resources based on the authentication procedures of another domain. Domain trusts allow the users of the trusted domain to access resources in the trusting domain. The information discovered may help the adversary conduct SID-History Injection, Pass the Ticket, and Kerberoasting. Domain trusts can be enumerated using the DSEnumerateDomainTrusts() Win32 API call, .NET methods, and LDAP. The Windows utility Nltest is known to be used by adversaries to enumerate domain trusts.

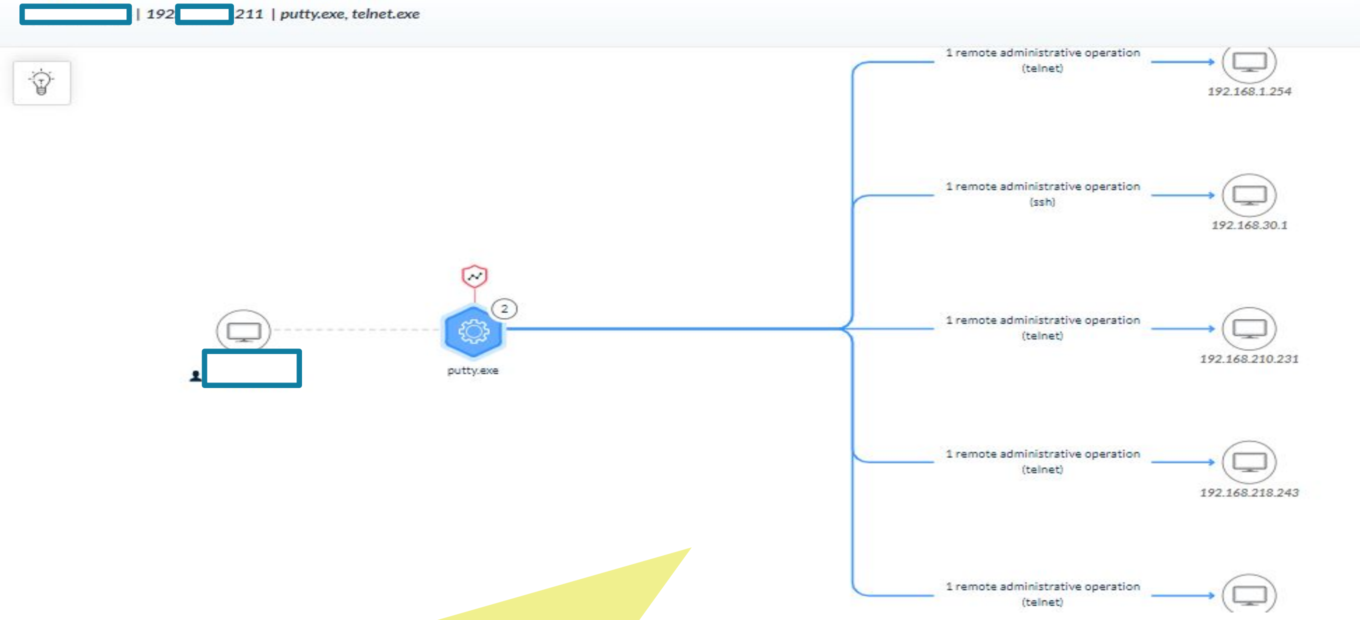
縮限問題範圍與查找 - 2



LATEST CON...	PROCESS PATH	PROCESS CREATE...	SOURCE IP	DESTINATION IP	DESTINATION PORT	APP-ID
Sep 3rd 2019 14:59:38	C:\Windows\System32\svchost.exe	NT Authority\Local Service	192.[redacted]103	192[redacted].119	55060	udp
Sep 3rd 2019 15:04:55	C:\Windows\System32\svchost.exe	NT Authority\Network Service	192.[redacted]103	192[redacted].161	65204	udp
Sep 3rd 2019 15:06:36	C:\Windows\System32\svchost.exe	NT Authority\Local Service	192.[redacted]103	192[redacted].185	64720	udp
Sep 3rd 2019 15:08:55	C:\Windows\System32\svchost.exe	NT Authority\Local Service	192.[redacted]103	192[redacted].101	60058	udp
Sep 3rd 2019 15:15:06	C:\Windows\System32\svchost.exe	NT Authority\Local Service	192.[redacted]103	192[redacted].101	53994	udp
Sep 3rd 2019 15:18:49	C:\Windows\System32\svchost.exe	NT Authority\Local Service	192.[redacted]103	192[redacted].101	59557	udp
Sep 3rd 2019 15:19:33	C:\Windows\System32\svchost.exe	NT Authority\Local Service	192.[redacted]103	192[redacted].119	59870	udp
Sep 3rd 2019 15:23:01	C:\Windows\System32\svchost.exe	NT Authority\Local Service	192.[redacted]103	192[redacted].101	50605	udp
Sep 3rd 2019 15:23:45	C:\Windows\System32\svchost.exe	NT Authority\Network Service	192.[redacted]103	192[redacted].125	52155	udp
Sep 3rd 2019 15:25:54	C:\Windows\System32\svchost.exe	NT Authority\Local Service	192.[redacted]103	192[redacted].185	62060	udp
Sep 3rd 2019 15:27:16	C:\Windows\System32\svchost.exe	NT Authority\Local Service	192.[redacted]103	192[redacted].177	59548	udp
Sep 3rd 2019 15:29:23	C:\Windows\System32\svchost.exe	NT Authority\Local Service	192.[redacted]103	192[redacted].131	53054	udp

行為剖析 – 適當工具 適合的使用者

內網-連線行為



[redacted] | 192[redacted]211 | putty.exe, telnet.exe

[redacted]
putty.exe
2
1 remote administrative operation (telnet)
192.168.1.254
1 remote administrative operation (ssh)
192.168.30.1
1 remote administrative operation (telnet)
192.168.210.231
1 remote administrative operation (telnet)
192.168.218.243
1 remote administrative operation (telnet)

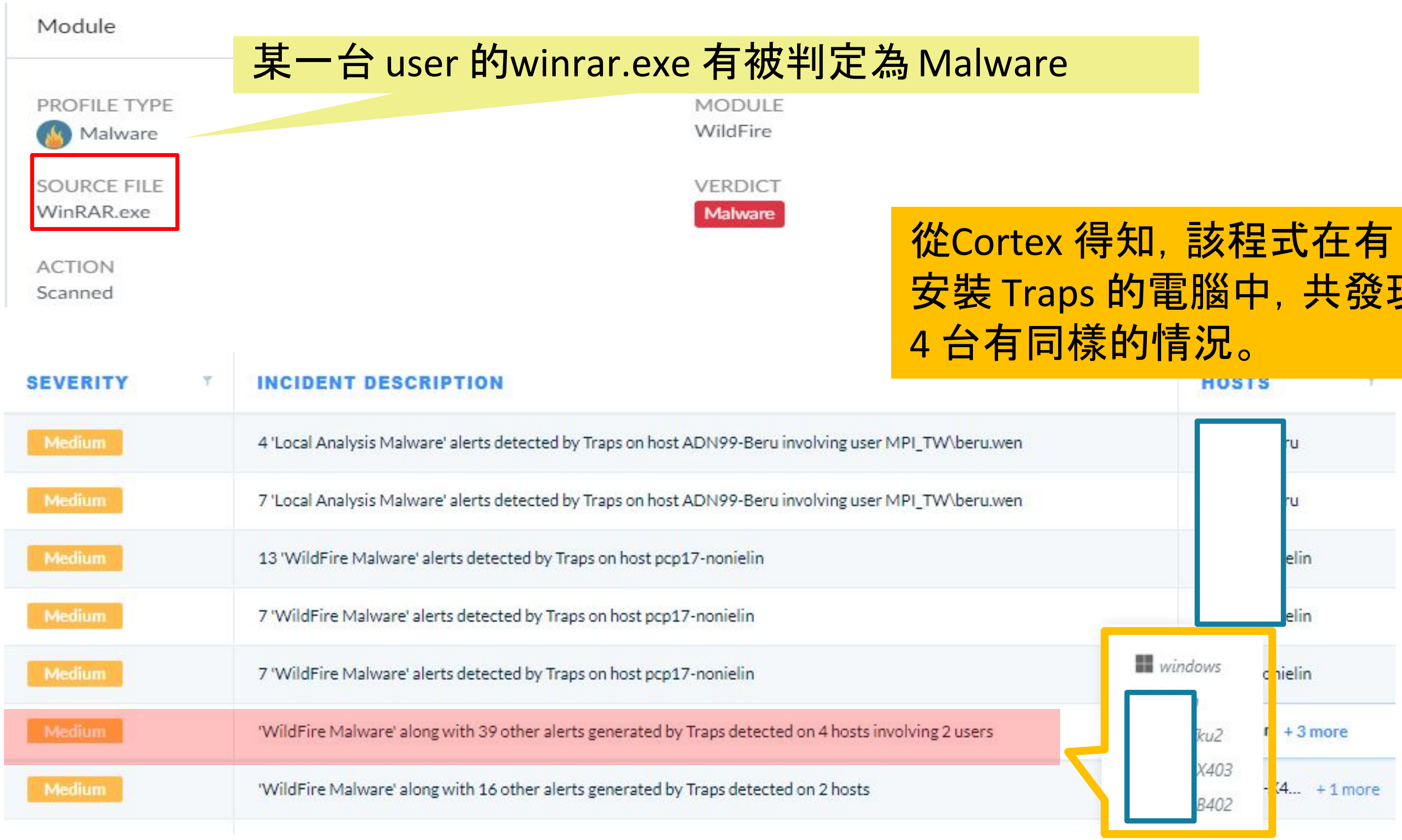
Alert Description

The device [redacted]rformed 5 new administrative operations on 5 hosts

New behavior: Remote administrative operations (SSH), Remote administrative operations (Telnet)

The device [redacted]s first seen on Aug 10th 2019 08:00:00

分析查找



某一台 user 的winrar.exe 有被判定為 Malware

從Cortex 得知，該程式在有安裝 Traps 的電腦中，共發現 4 台有同樣的情況。

Module

PROFILE TYPE
Malware

SOURCE FILE
WinRAR.exe

ACTION
Scanned

MODULE
WildFire

VERDICT
Malware

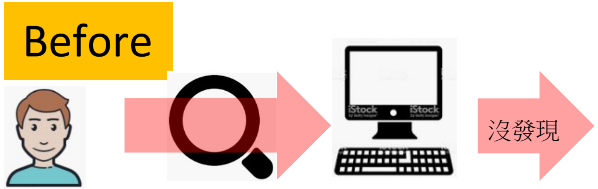
SEVERITY	INCIDENT DESCRIPTION	HOSTS
Medium	4 'Local Analysis Malware' alerts detected by Traps on host ADN99-Beru involving user MPI_TW\beru.wen	[redacted]ru
Medium	7 'Local Analysis Malware' alerts detected by Traps on host ADN99-Beru involving user MPI_TW\beru.wen	[redacted]ru
Medium	13 'WildFire Malware' alerts detected by Traps on host pcp17-nonielin	[redacted]elin
Medium	7 'WildFire Malware' alerts detected by Traps on host pcp17-nonielin	[redacted]elin
Medium	7 'WildFire Malware' alerts detected by Traps on host pcp17-nonielin	onielin
Medium	'WildFire Malware' along with 39 other alerts generated by Traps detected on 4 hosts involving 2 users	r + 3 more
Medium	'WildFire Malware' along with 16 other alerts generated by Traps detected on 2 hosts	-X4... + 1 more

windows
[redacted]
ku2
X403
B402

效益改善

項目	描述
縮小問題的範圍	例:54667 中的 5 個告警
查找問題更明確	直接說明是哪個檔案造成;例: explorer.exe，avastsvc.exe)
列出使用者可疑行為	大檔傳送、橫向連接
節省問題處理時間	直接處理異常程式或行為

Before



<u>標準檢查流程</u>
(約 0.5H)

1. 上網歷程記錄
2. 近期安裝檔案
3. 事件
4. 登錄檔
5. 排程
6. 檢查系統管理員
7. Netstat 查連線

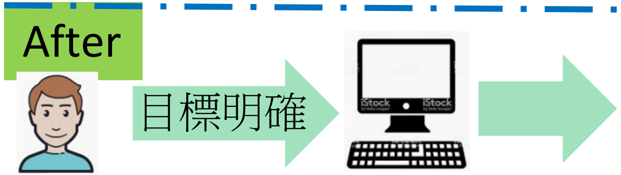
- 基本處理 (約0.5H)
- 重灌(持續發生時)
  - 安裝與設定:約1H
  - 資料移轉:約6H

A. 檢查與基本處理: 約1H
B. 包含重灌: 約8H

MIS:8H ; User:8H

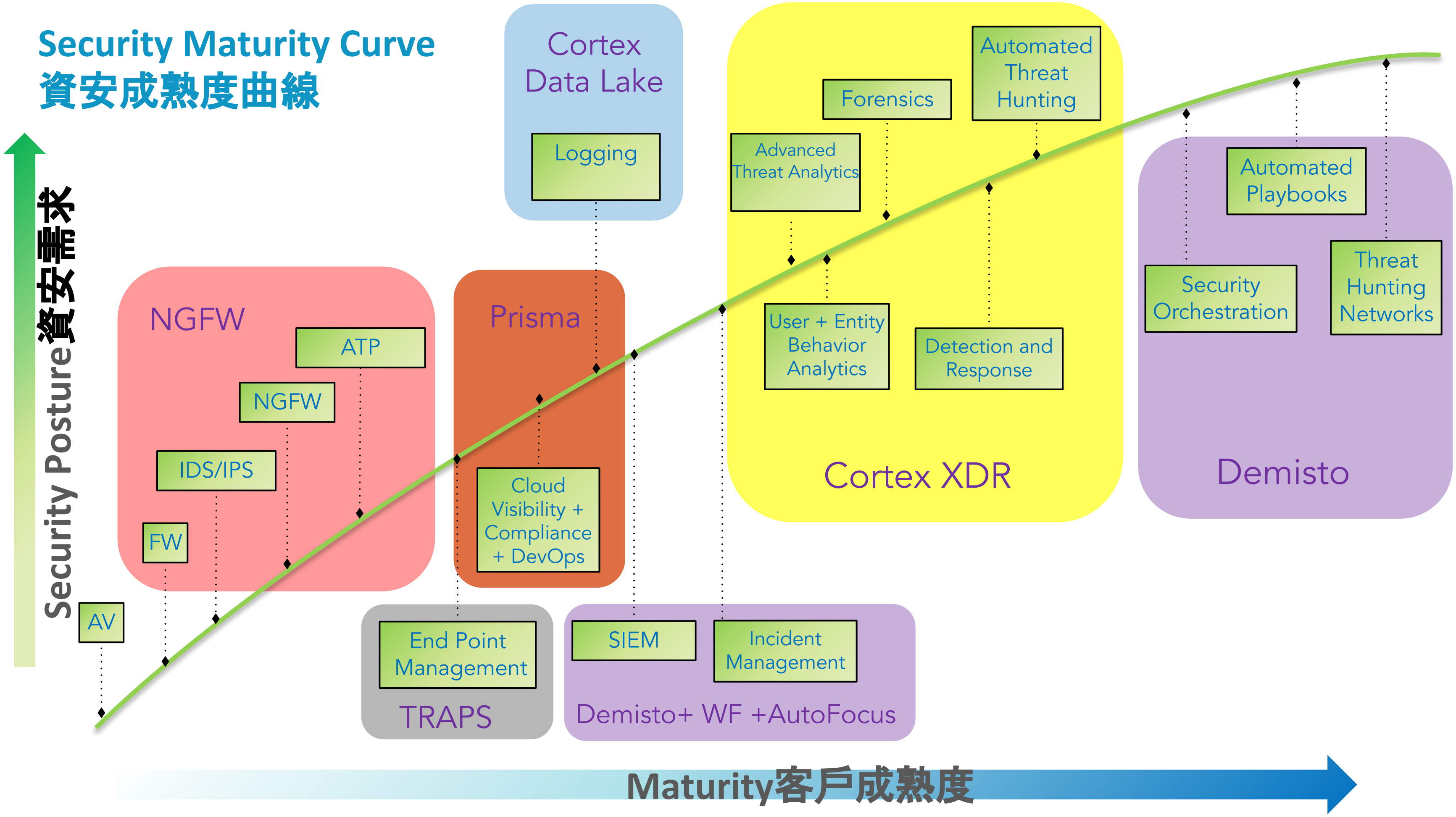
<u>提報次數統計:</u>
2018/11~2019/8共約 70 件

After



移除檔案 (約10m)

Security Maturity Curve
資安成熟度曲線



Securing Your Transformed Enterprise

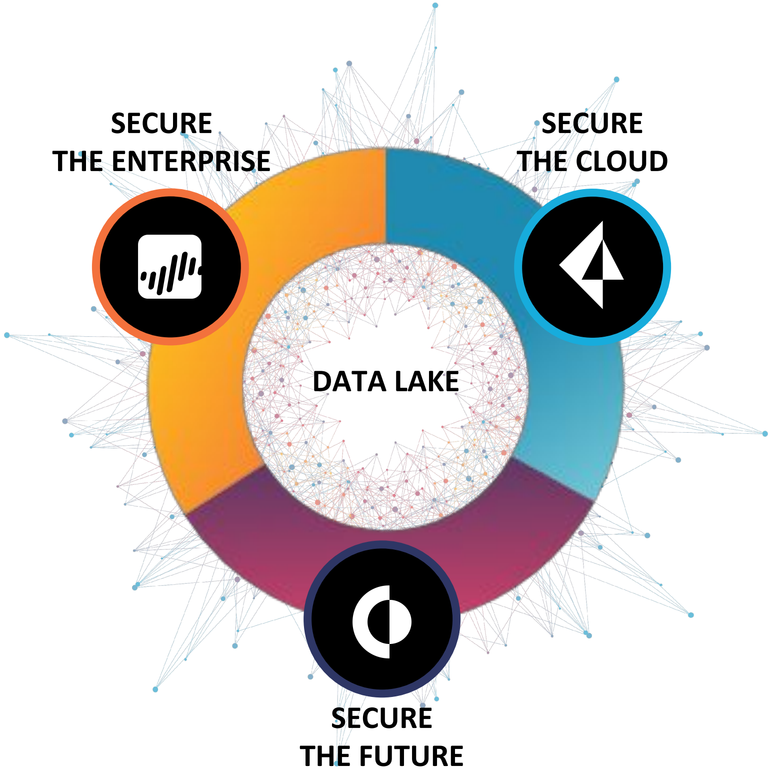
Hybrid data center

Internet Perimeter

Branch & mobile

5G & IoT

Endpoint



Secure access

SaaS

Public cloud

Detection & response

Automation & orchestration

Network traffic & behavioral analytics

Threat intelligence

THANK YOU

Email: jchan@paloaltonetworks.com I Twitter: @PaloAltoNtwks