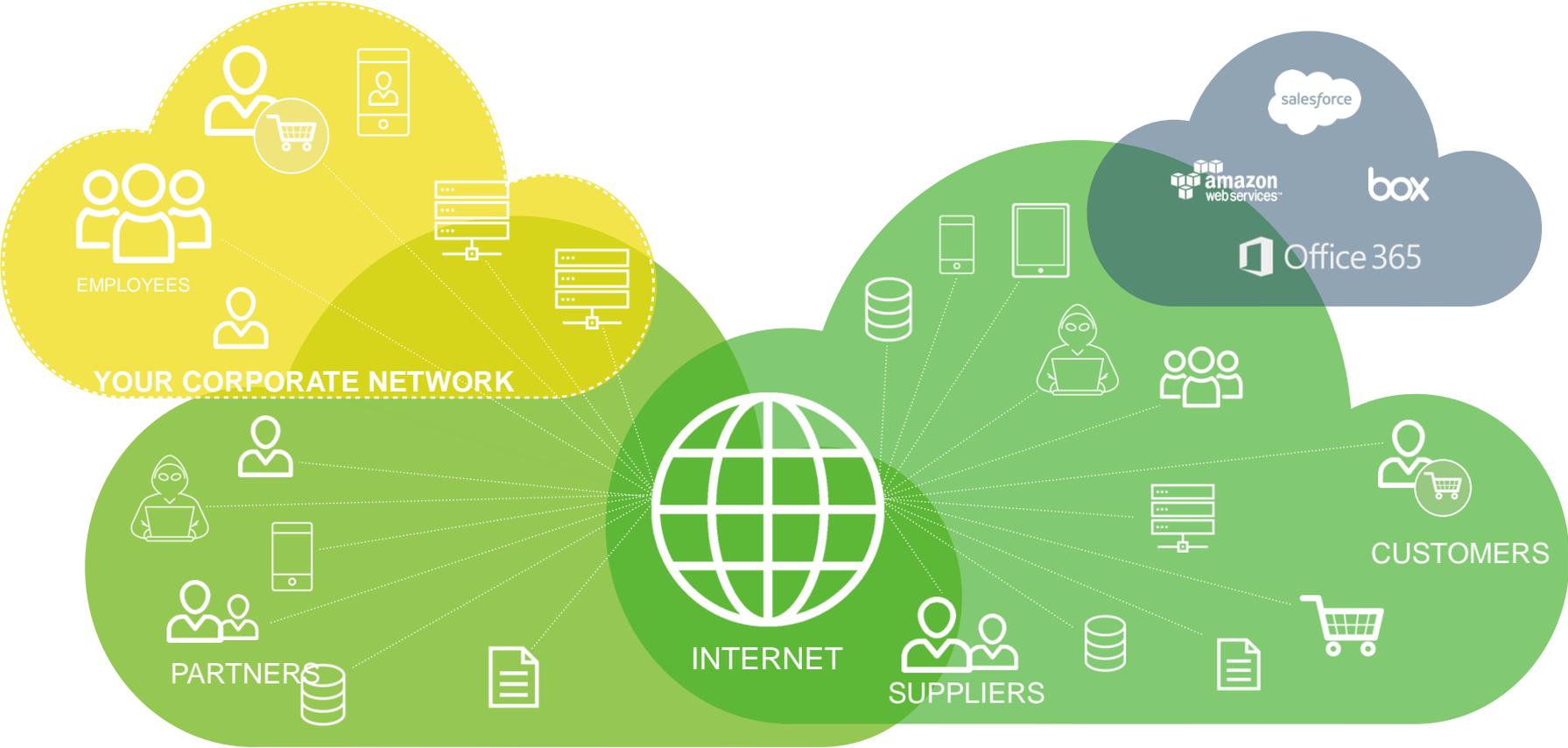




資安威脅狂潮來襲， 為您的企業穿上資安鐵布衫

陳志遠 Mark Chen
FORCEPOINT 台灣區技術經理

資訊安全戰場不僅只在企業內部網路



資訊安全挑戰只會越來越嚴峻

到處都有公司的重要資料(包含不是我能管理與掌控的系統) 而且隨處可得

我們公司內部有各式各樣的資訊安全系統

每天太多的資安警告事件，我沒辦法分辨什麼是真正需要關注的

等我理出頭緒要採取行動，通常為時已晚

YOUR CORPORATE NETWORK

3rd party 雲端服務
增加11倍
從 2014-16

一般企業平均使用
30-75
各類型資安系統

超過一半的資安主管需
面對的資安事件量
>5000 筆/每天

平均得花費 **46 天**
才能發現並阻止潛伏
攻擊

PARTNERS

INTERNET

SUPPLIERS

salesforce

amazon





重新思考

資訊安全

 **FORCEPOINT**
POWERED BY Raytheon

Protecting the human point.

傳統資安防護策略

數位活動



威脅導向的防護方式

- ▶ 依賴預先設定好的資安政策
- ▶ 事發當下判斷好與壞
- ▶ 阻擋已經的惡意威脅，允許合法行為

必要的防護方式
卻不足以應付內部威脅

行為導向的資安防護策略

提供行為的脈絡與
自動化分析，協助
判斷真實威脅

數位活動

“GOOD”

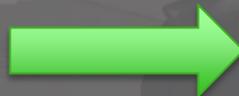
行為導向的防護方式

- ▶ 透過自動化行為分析偵測潛在高風險使用者
- ▶ 快速了解可能潛在的風險與背後的原因
- ▶ 由使用者如何使用機敏資料來分辨好壞
- ▶ 持續地自動學習與觀察，找出正常中的異常

早期發覺內部的潛在風險

“BAD”

為特定目的而成立的公司 → 以HUMAN POINT為核心價值



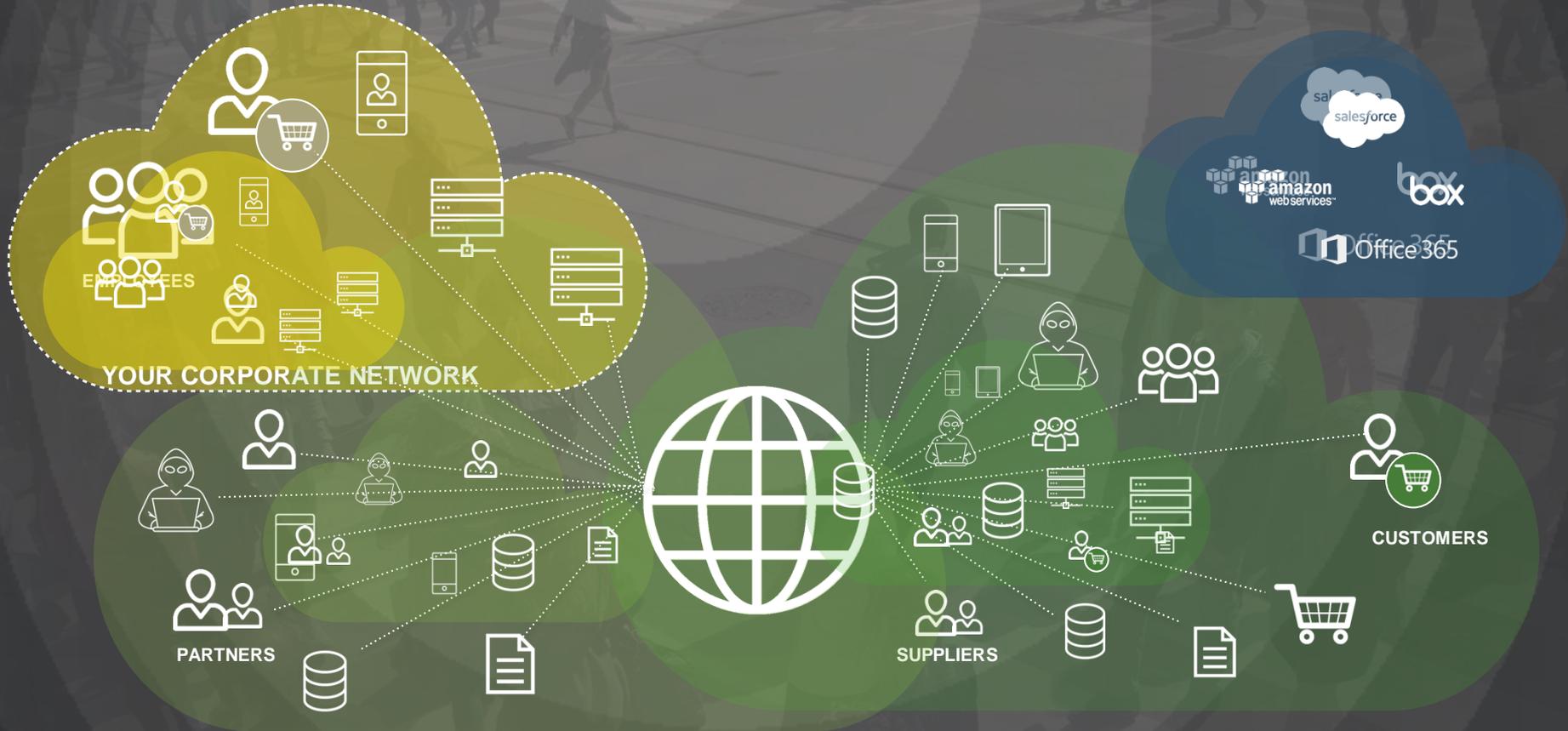
FORCEPOINT

POWERED BY Raytheon

Protecting the human point.

- ▶ One of the largest private cybersecurity companies in the world, with thousands of enterprise and government customers in more than 150 countries.
- ▶ Created by Raytheon in 2016 to **commercialize defense-grade technologies** for the enterprise security market.
- ▶ Supporting global governments, defense and intelligence communities to ensure success of the world's most high-consequence missions.

翻轉思維，關注恆定的核心因素



翻轉思維，關注恆定的核心因素

THE HUMAN POINT

PEOPLE



DATA



了解人與資料的互動過程

salesforce

amazon
webservices

box

Office 365



THE HUMAN POINT SYSTEM

THE HUMAN POINT SYSTEM



進階分析

簡化管理

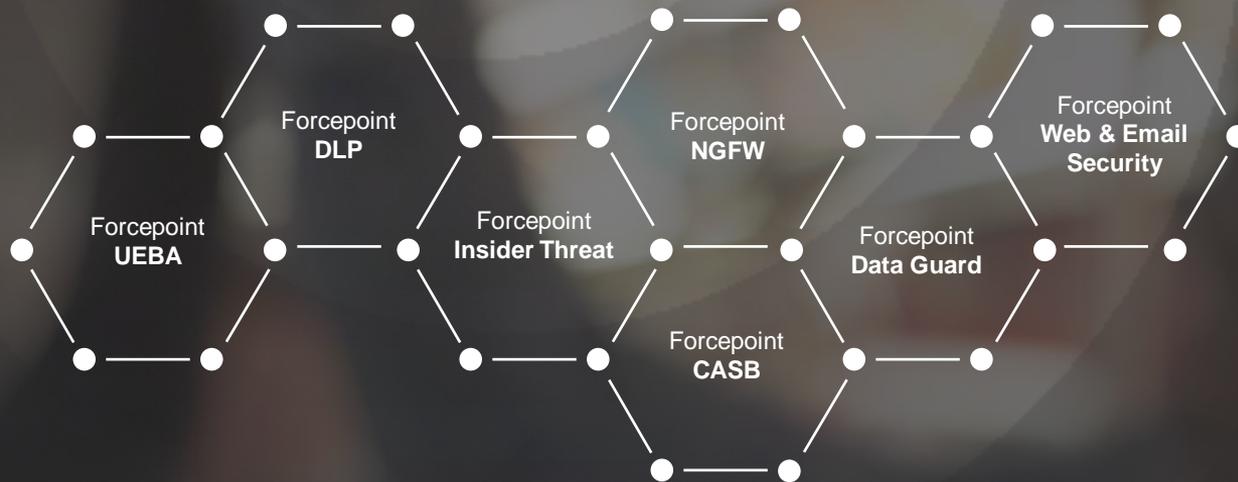
完整防護

THE HUMAN POINT SYSTEM 設計理念

每個元件具備特色:

- ▶ 領先業界的進階技術
- ▶ 可從任何一個元件開始
- ▶ 可整合為一致性的系統以簡化管理與政策
- ▶ 可快速與您的現有系統整合





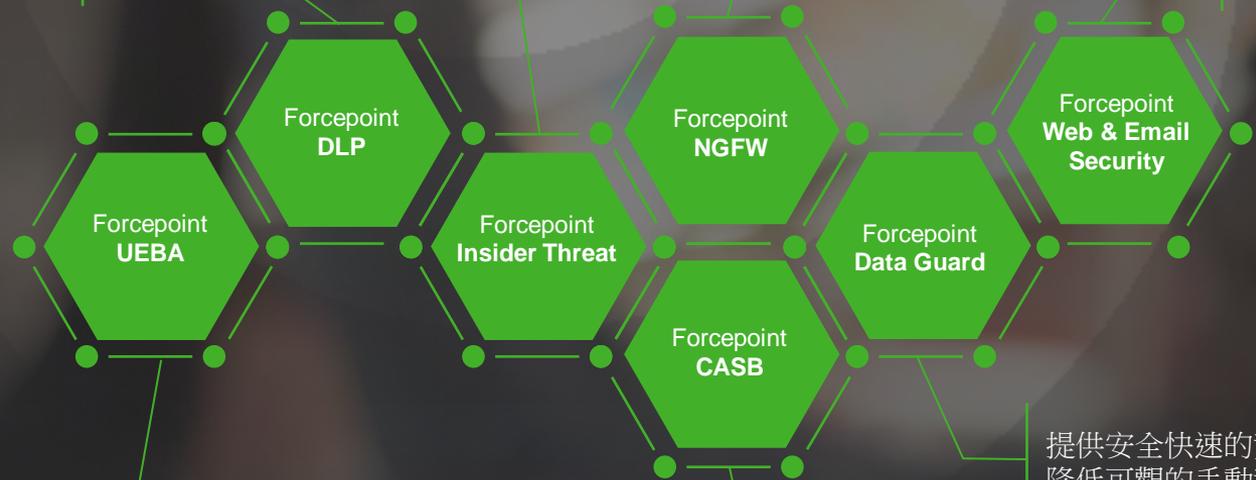
領先業界的進階技術

來自雷神
最完整的使用者行為與內部威脅分析系統
超過100萬的端點部署規模

2017NSS labs排名第1的NGFW與NGIPS
可降低50%的網路費用
降低86%的網路攻擊
減少73%的事件回應時間

來自Websense
先進Web與email
APT防護技術

Gartner連續9年DLP領導象限



業界領先的
資訊安全風險分析平台
提供可行動的分析結果

提供安全快速的資料傳輸防護
降低可觀的手動資料轉移費用

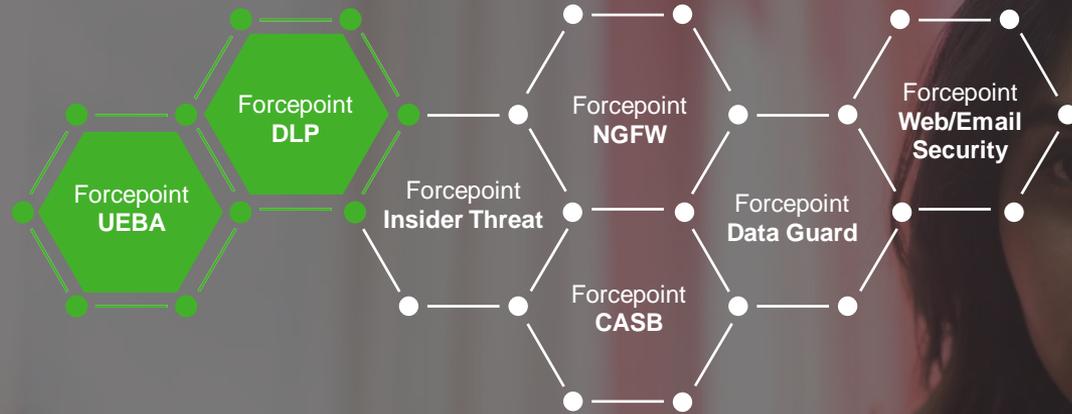
支援最多的雲端應用服務
提供特有的使用者行為風險分析管理
同時可結合**FORCEPOINT DLP**在雲端保護最重要的資料



隨時加入
THE HUMAN POINT SYSTEM

應用情境

在雲端服務(如Office 365)上，分析可能導致資料外洩的異常行為
延伸公司內部既有的DLP政策至雲端服務，保護重要資料



start with

Forcepoint UEBA



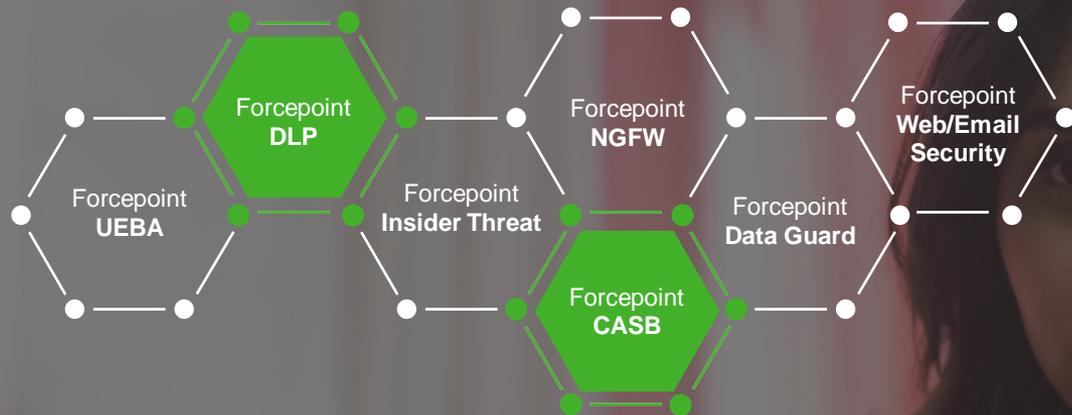
add

Forcepoint DLP

應用情境

保護重要的智慧財產與機敏資料

盤點並保護雲端上的重要資料並且管理雲端服務的使用



start with

Forcepoint DLP



add

Forcepoint CASB

次世代的資訊安全防護

到處都有公司的重要資料
而且隨處可得

我們公司內部有各式各樣的資訊安全系統

每天太多的資安警告事件
我沒辦法分辨什麼是真正需要關注的

等我理出頭緒要採取行動，通常為時已晚



打開能見度

- ▶ Forcepoint DLP 與 Forcepoint Insider Threat 結合可提供強大有力的調查分析能力，包含錄影紀錄
- ▶ Forcepoint NGFW 為分散式的防護系統提供集中化的資安管理能力



系統整合

- ▶ Forcepoint 的 Human Point System 提供整合的平台，可統合雲端與第三方系統與使用者
- ▶ Forcepoint 的系統可簡化管理於單一地點



有效的警示

- ▶ Forcepoint UEBA 提供統合風險分析結果，有效降低事件雜訊
- ▶ Forcepoint DLP 的 Incident Risk Ranking 可自動分析並關聯高風險資料外洩事件，凸顯關注重點。



即時分析與
保護

- ▶ Forcepoint UEBA 統合各應用安全系統的資訊，提供使用者行為的情境，協助您從眾多事件中快速辨識異常違規行為。
- ▶ Forcepoint DLP 即時阻止機敏資料外洩，防止公司信譽損害。

請開始加入我們的旅程

安全防護效益



威脅導向

資料導向

風險管理導向



FORCEPOINT NGFW

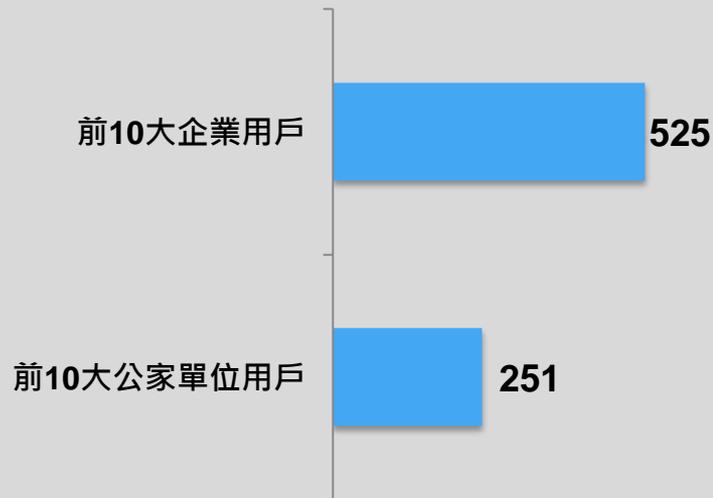
FORCEPOINT NGFW OVERVIEW

超過**20**年以上的創新歷史(**STONESOFT**)

- ▶ 大型集中化管理能力
- ▶ 高效能與穩定性
- ▶ 高可用性與彈性
- ▶ 業界最高安全性
- ▶ 進階規避防護技術

解決企業網路全球化，雲端服務，大型政府組織等分散式部署管理負擔

平均部署規模



需要大型集中化管理能力
以解決維運問題

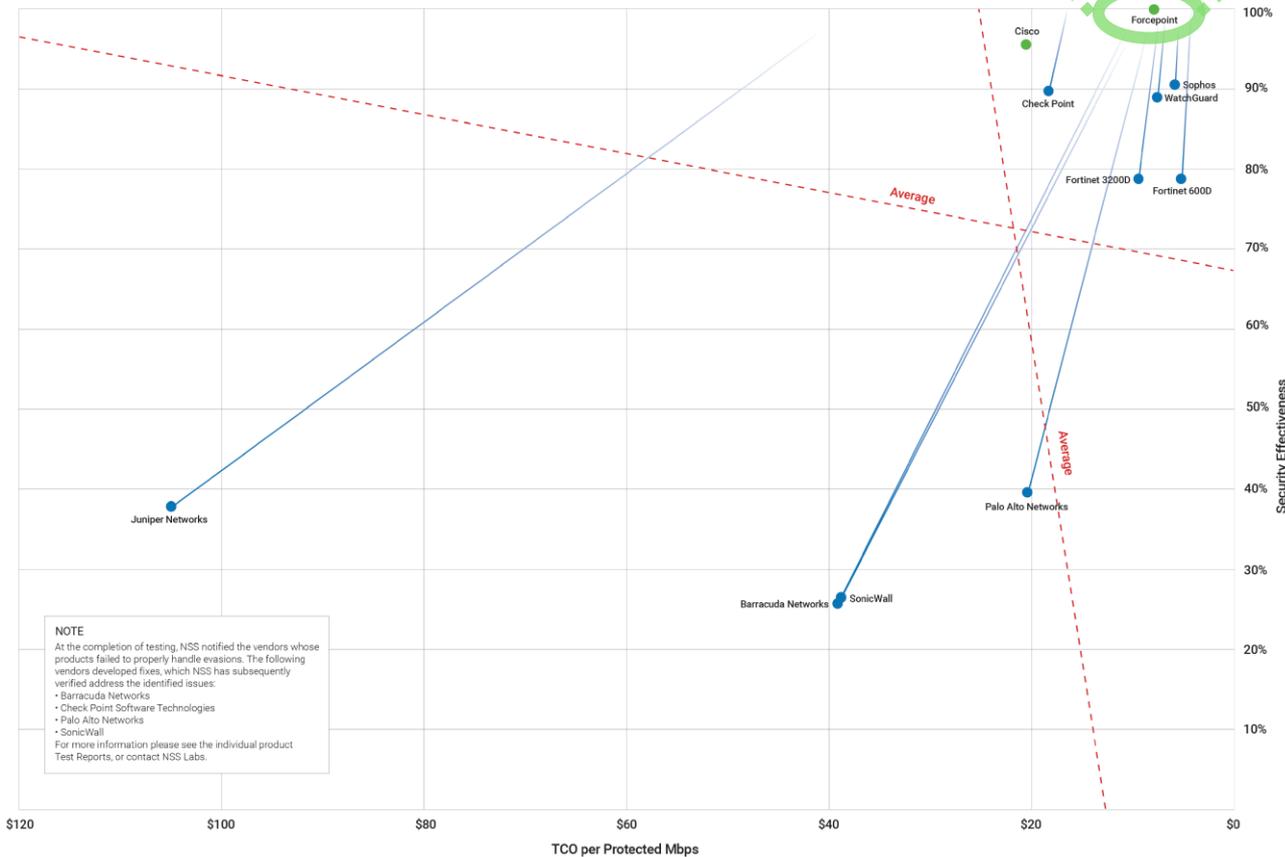
FORCEPOINT連續多年獲得防火牆權威報告NSS LABS NGFW與NGIPS的肯定

- 連續**5年**獲得NSS Labs推薦NGFW
- NSS Labs 2017 NGFW **100%**
- NSS Labs 2017 NGIPS **99.91% (No.1)**
- 專利AET技術 **100%**防止進階規避攻擊



	2012	2013	2014	2016	2017
覆蓋範圍	94%	96%	96.5%	97.5%	100%
防規避	100%	100%	100%	100%	100%
評等					

2017 NSS LABS NGFW 評比#1

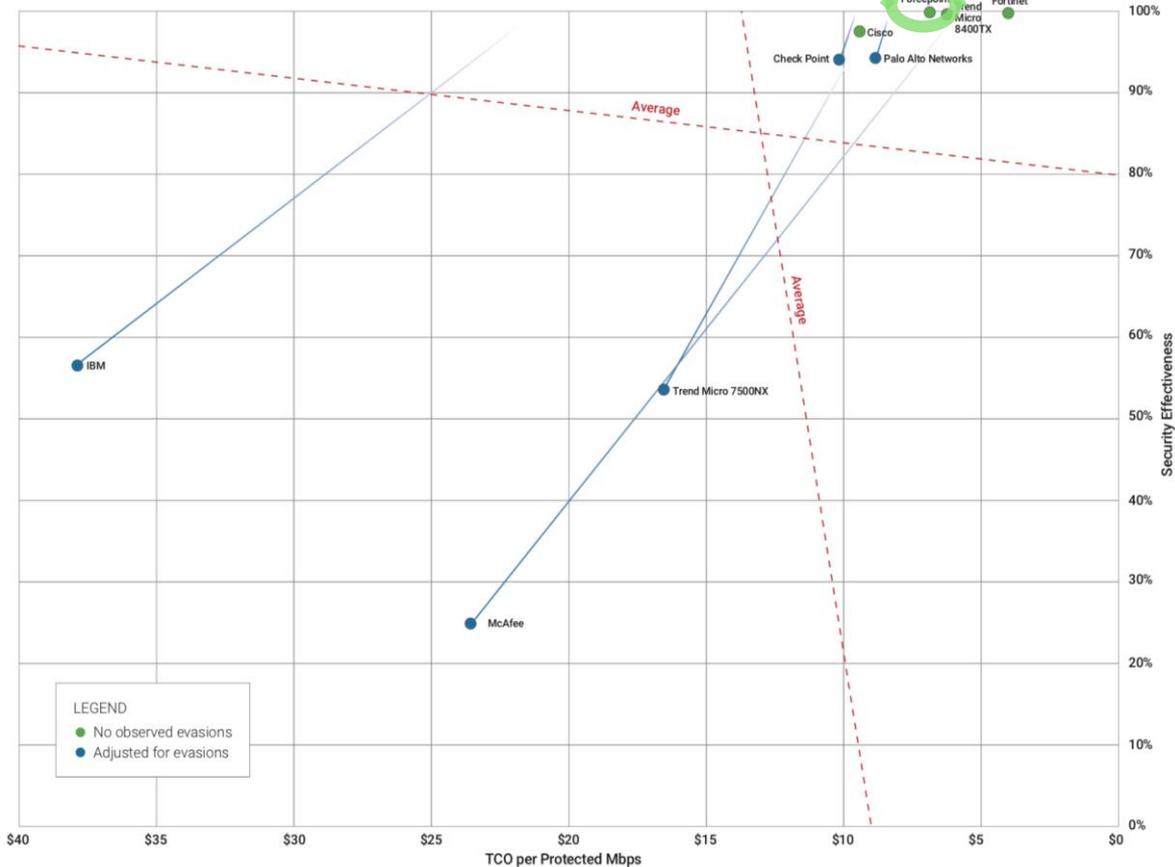


NOTE
 At the completion of testing, NSS notified the vendors whose products failed to properly handle evasions. The following vendors developed fixes, which NSS has subsequently verified address the identified issues:

- Barracuda Networks
- Check Point Software Technologies
- Palo Alto Networks
- SonicWall

For more information please see the individual product Test Reports, or contact NSS Labs.

2017 NSS LABS NGIPS 評比#1



NSS Labs連續五年的防禦率紀錄分析

■ 持續**5年**的高水準防護，防禦率逐年攀高，提供資料中心最佳安全防護需求

Device	2012	2013	2014	2016	2017
PaloAlto	79	91	60	96	39
Juniper	27,5	95	N/A	97,5	38
Cisco ASA	N/A	N/A	N/A	96	N/A
Forcepoint	94	96	96,5	97,5	100
Checkpoint	66	98	97	99	89
Fortinet	73	92	94	99	78,5
Huawei	N/A	N/A	N/A	97,5	N/A
SonicWall	94	98	97,5	98	26
Cisco Firepower	N/A	98	99	96	95
Cyberroam	N/A	N/A	88	58	N/A
Barracuda	N/A	N/A	89	92,5	25
WatchGuard	N/A	28	97,5	N/A	88,5
Hillstone	98	N/A	N/A	98	N/A
Sophos	N/A	N/A	N/A	N/A	91

NSS Labs Cyber Advanced Warning System 真實漏洞攻擊測試結果

■ **NSS Labs** 每月持續透過真實漏洞攻擊測試各家防火牆防護能力。
FORCEPOINT 長久以來被證實具有最佳防禦能力

廠商	被穿透的攻擊統計
Cisco	322
Juniper	288
Sophos	245
Barracuda	104
Check Point	31
WatchGuard	27
Palo Alto	17
Fortinet	11
SonicWall	11
Forcepoint	5

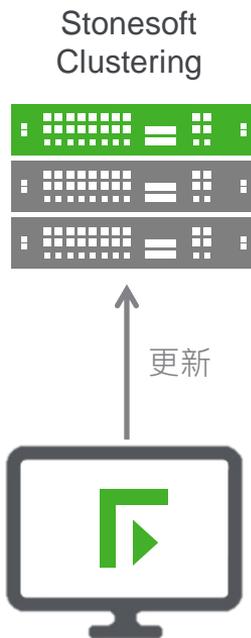


獨特的Clustering功能：

- ▶ 不同的韌體版本
- ▶ 不同的設備型號
- ▶ 可軟體硬體混合
- ▶ 支援多達16個節點的AA Cluster
- ▶ 支援IPv6 AA Cluster

運作優點：

- ▶ 可在無中斷連線情況下完成防火牆HA系統**升級和更新**，提高SLA
- ▶ 大幅減少系統升級時所需前置作業時間
- ▶ 客戶可彈性規劃配置，符合各種業務環境成長需求
- ▶ 提供業界最佳防火牆Clustering效能



v5.8



節點 1: NGF-3206

v5.7



節點 2: NGF-1402



節點 3: 軟體

v5.6

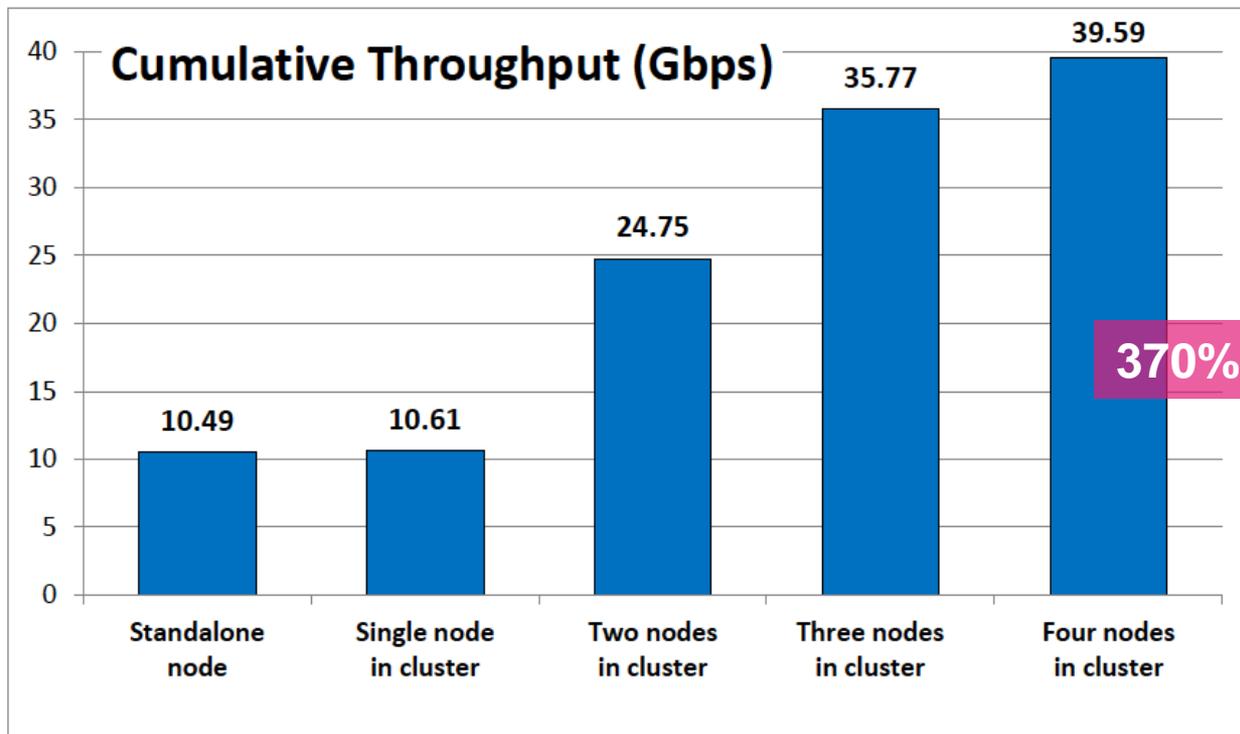


節點 4: NGF-325



節點 5: 軟體

真正的Active-Active!無與倫比的Cluster效能



Throughput and Scalability Report Stonesoft NGFW 5206, Miercom, October 2014

STONESOFT MULTI-LINK 技術，提供最大連線彈性與效能

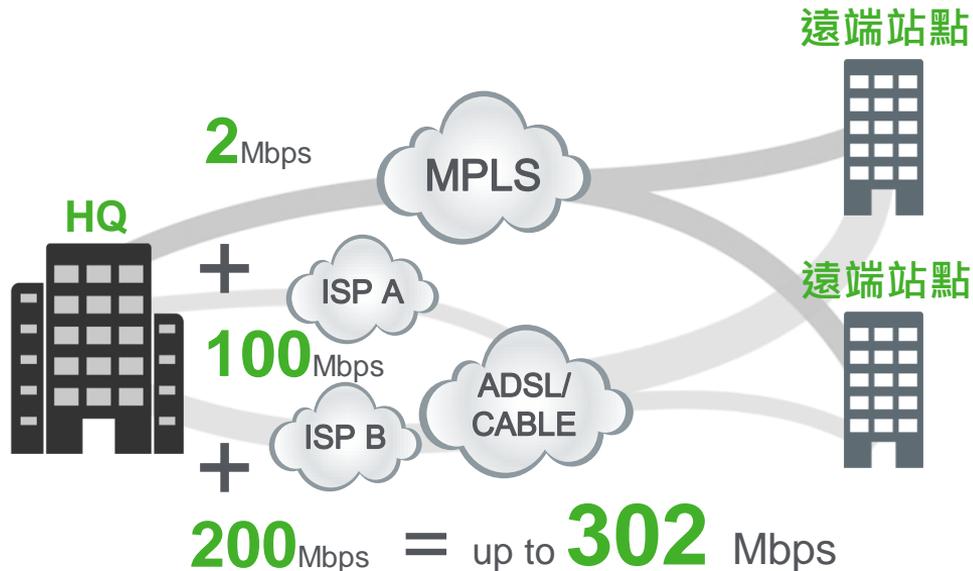
支援 **Site to Site VPN**

支援 **Outbound ISP Load balancing**

支援 **Inbound Server Load Balancing**

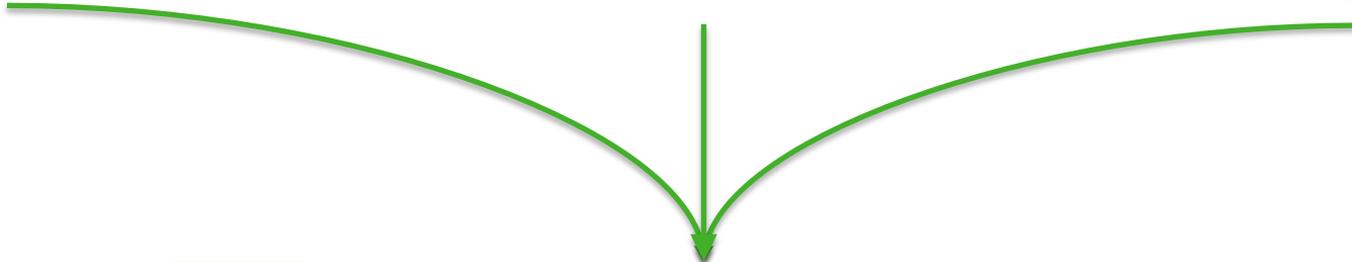
可結合 **QoS 頻寬與連線管理**

- ▶ 分配網路應用服務優先權
- ▶ 當某線路有問題時,可將交易類流量自動轉移自另一條線路.非交易類流量可選擇是否轉移至其他線路



websense

STONESOFT



FORCEPOINT

POWERED BY **Raytheon**

結合SIDEWINDER SECURITY PROXIES，提供軍規等級安全防護

▶ 重要通訊協定的安全代理:

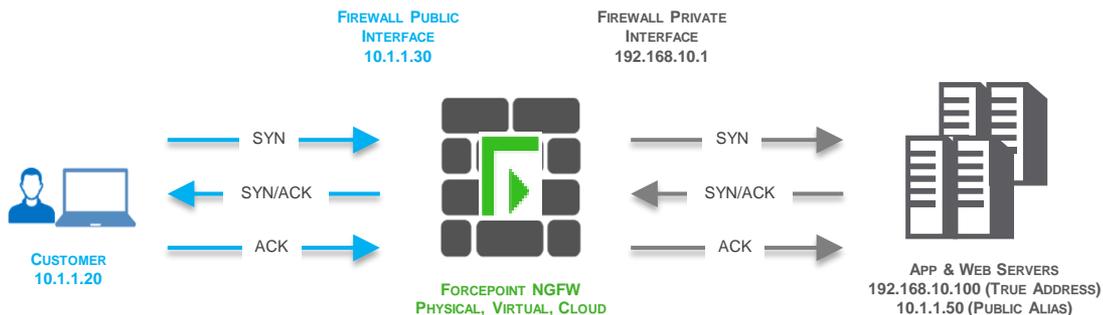
- UDP
- TCP
- HTTP / HTTPS
- SSH / SFTP

▶ 可改寫通訊協定Header

- 可去識別化減少外洩資訊
- 避免重要訊息外洩

▶ 提供更多精細的控制:

- 通訊協定版本
- 認證方式
- 允許執行的指令



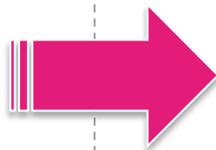
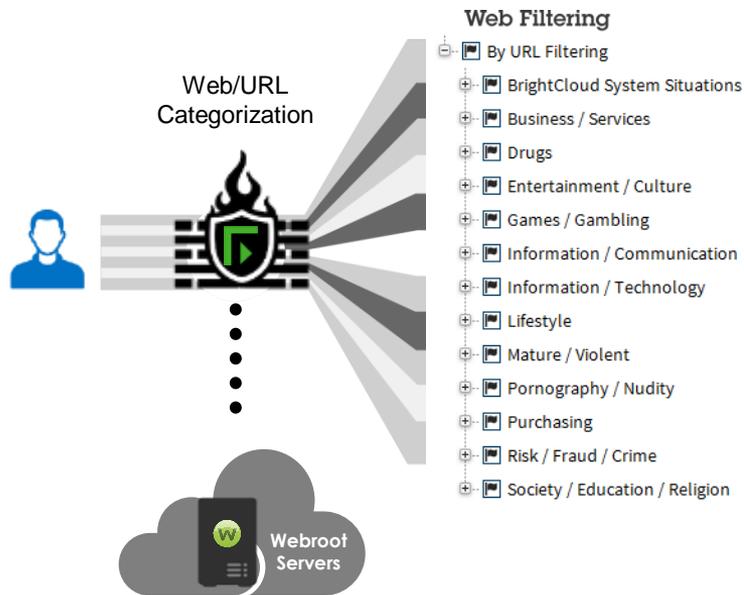
The top screenshot shows the SMC configuration interface for the 'HQ-FW-policy (modified) (ED)'. The table below is a representation of the rules shown in the interface:

ID	Source	Destin...	Service	Action	Comment
5.5.1	± ANY	± ANY	DMZ access rule	Allow	
			Internet access rule		
5.5.5	internal-net1	± ANY	SSM SSH	Allow	
5.5.6	internal-net1	± ANY	SSM SSH	Allow	
			Discard all		

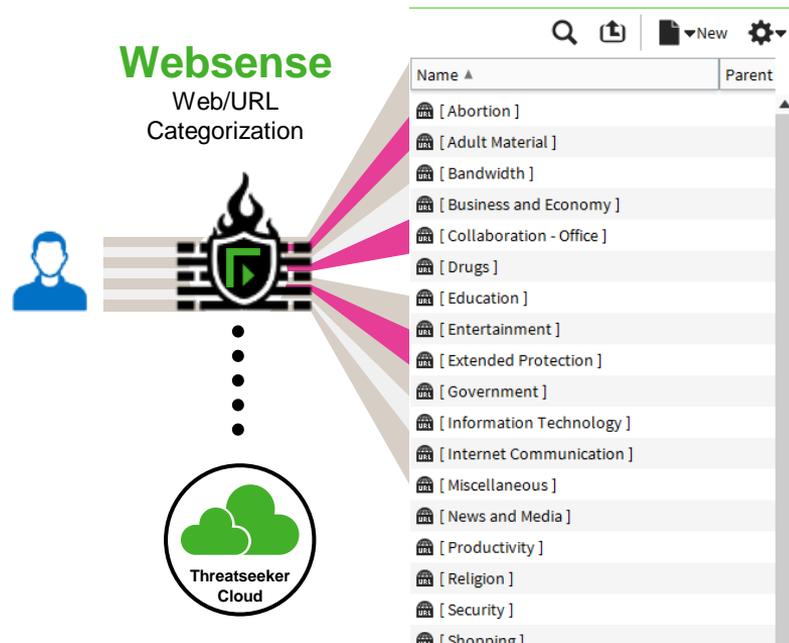
The bottom screenshot shows the 'SSM SSH for HQ - Properties' dialog box. The 'SFTP Commands' section is expanded, showing a list of allowed commands. The 'Read directories on the server' and 'Read files on the server' options are checked.

結合WEBSense THREATSEEKER 全球智能威脅情資(URL分類資料庫)

以前



現在



← → Menu **FORCEPOINT** Stonesoft Management Center

Multiple Elements × +

Engines ⚙️ ▼

Organize by: By Type ▼

Search

- ⊖ Firewalls (20)
 - 🟢 Algiers FW
 - 🟢 Atlanta FW
 - 🟢 Beijing FW
 - 🟢 Dubai Virtual FW 1
 - 🟢 Dubai Virtual FW 2
 - 🟢 Dubai Virtual FW 3
 - 🟢 Dubai Virtual FW 4
 - 🟢 Dubai Virtual FW 5
 - 🟢 Helsinki FW
 - HQ Site
 - London FW
 - Madrid FW
 - 🟢 Mexico FW
 - 🟢 Milan FW
 - 🟢 Moscow FW
 - 🟢 Paris FW
 - 🟢 Plano FW
 - 🟢 Riyadh FW
 - 🟢 Saint Paul FW
 - 🟢 Santa Clara FW
 - 🟢 Tunis FW
- ⊖ IPS (4)
 - 🟢 Atlanta IPS
 - 🟢 Dubai Virtual IPS 1
 - 🟢 Dubai Virtual IPS 2
 - 🟢 Helsinki IPS
- ⊖ Layer 2 Firewalls (2)
 - 🟢 Atlanta L2 FW
 - 🟡 Helsinki L2 FW
- ⊖ Master Engines (2)
 - 🟡 Dubai Master FW
 - 🟢 Dubai Master IPS

🏠 Home
Security Engines

Algiers FW	Atlanta FW	Atlanta IPS	Atlanta L2 FW	Beijing FW	
Dubai Master FW	Dubai Master IPS	Dubai Virtual F...	Dubai Virtual F...	Dubai Virtual F...	
Dubai Virtual F...	Dubai Virtual F...	Dubai Virtual IP...	Dubai Virtual IP...	Helsinki FW	
Helsinki IPS	Helsinki L2 FW	London FW	Madrid FW	Mexico FW	
Milan FW	Moscow FW	Paris FW	Plano FW	Riyadh FW	
Saint Paul FW	Santa Clara FW	Tunis FW			

VPNs

Corporate VPN
Gateways: 13/13
Tunnels: 12/12

Route-Based VPN
Gateways: 4/4
Tunnels: 6/6

Others

Log Server

Management Server

Web Portal Server

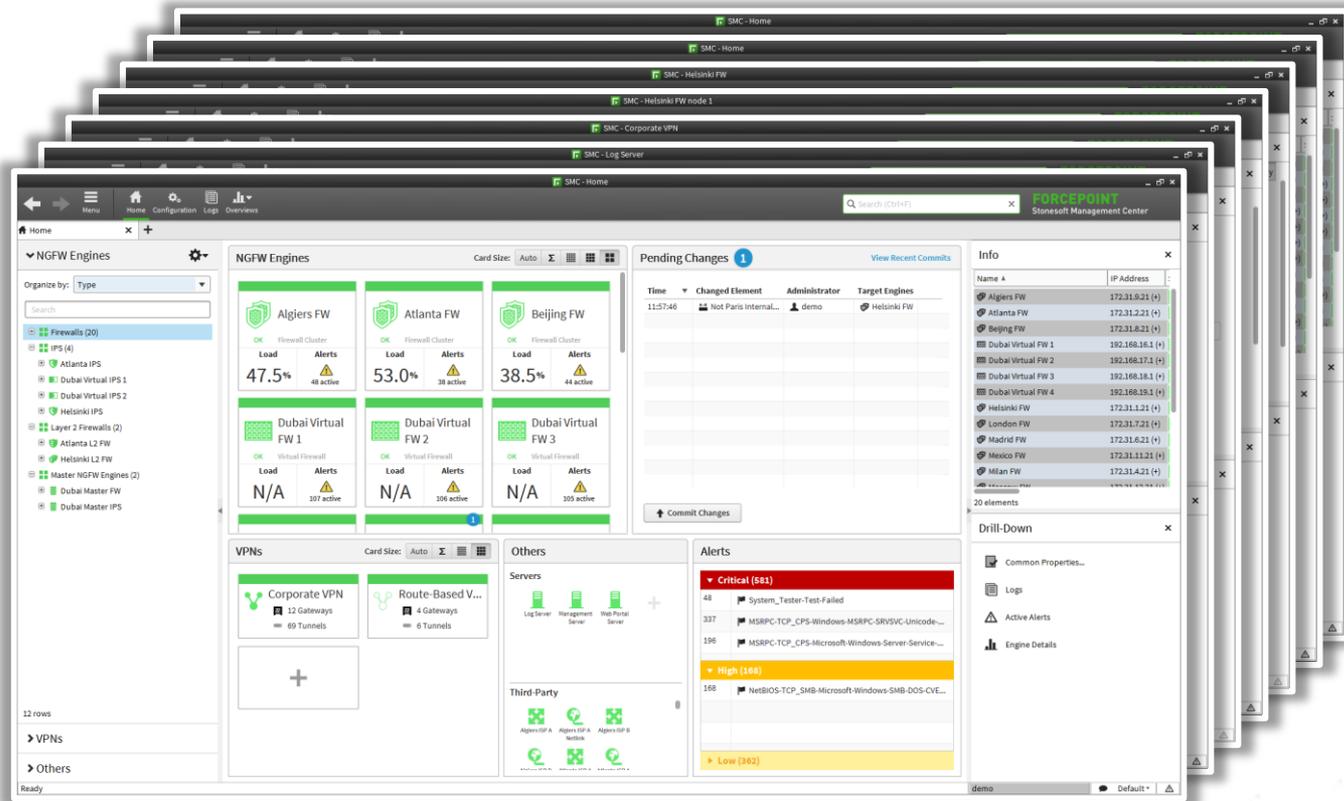
Alerts

▼ Critical (2030)

Count	Situation
136	System_Tester-Test-Failed
1137	MSRPC-TCP_CPS-Windows-MSRPC-SRV SVC-Unicode-Buffer...
1	Alert Server: Active alert queue full
756	MSRPC-TCP_CPS-Microsoft-Windows-Server-Service-Buffer...

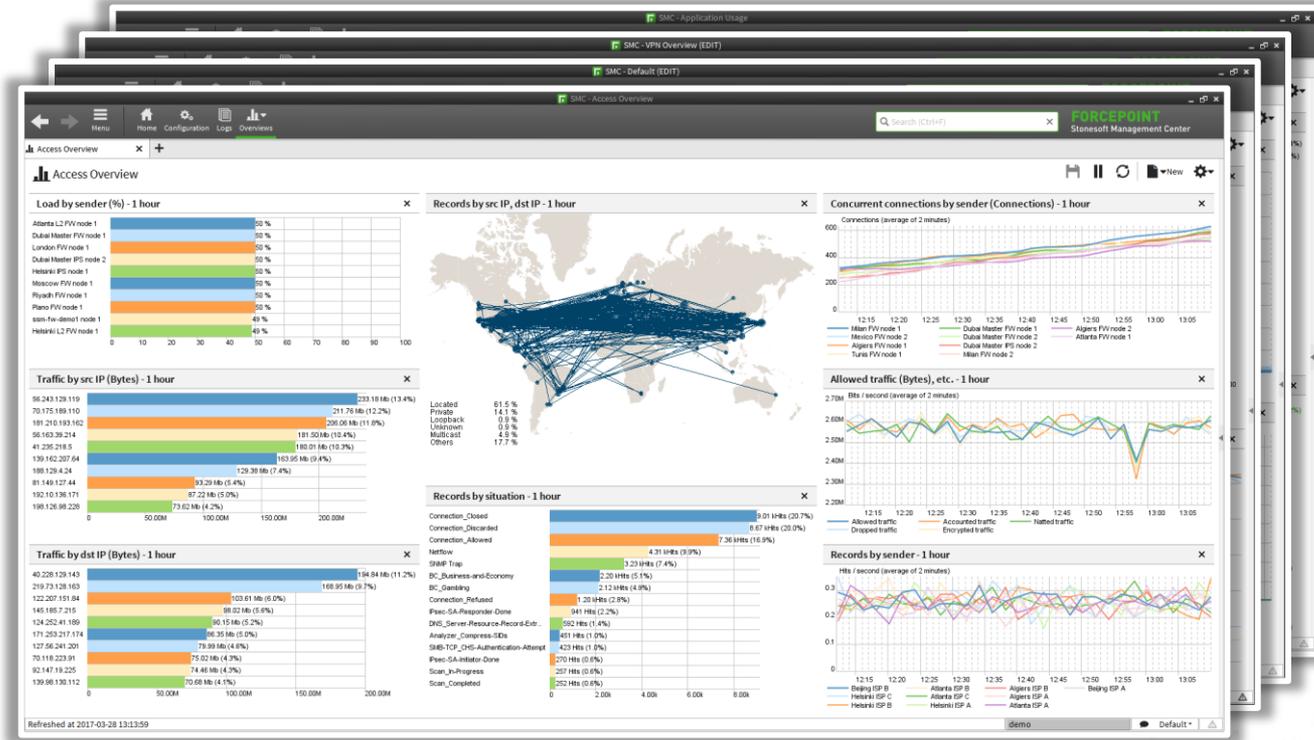
完整的防火牆系統健康監控能力

- ▶ 多種監控狀態供快速分析與深入調查
- ▶ 一目瞭然的系統健康資訊



即時的視覺化報表分析體驗

- ▶ 可自由客製化的儀表板
- ▶ 超過百種的分析資料



提供政策變更管理機制

- ▶ 內建政策變更管理機制
- ▶ 政策設定完佈署前可指定人員覆核
- ▶ 有效管理政策變更與留下完整稽核記錄

Pending Changes 2 [View Recent Commits](#)

Time	Changed Ele...	Adminis...	Target ...	✓
13:08:55	BR	admin	BR	
13:08:55	HQ	admin	HQ	

[↑ Commit Changes](#) [Approve All](#)

Pending Changes 2 [View Recent Commits](#)

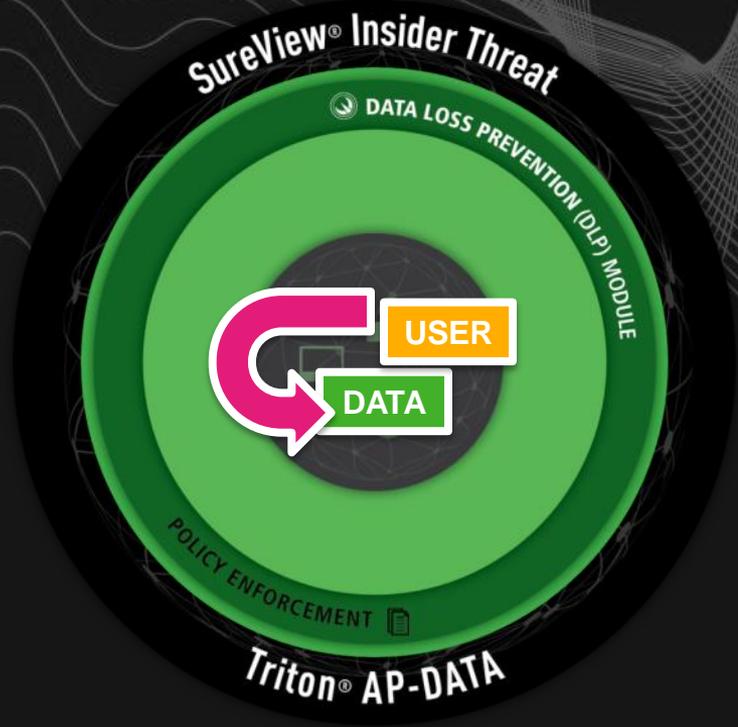
Time	Changed Ele...	Adminis...	Target ...	✓
13:08:55	BR	admin	BR	✓
13:08:55	HQ	admin	HQ	✓

[↑ Commit Changes](#) [Approve All](#)



FORCEPOINT Insider Threat

現今主流營業秘密與機敏資料保護策略



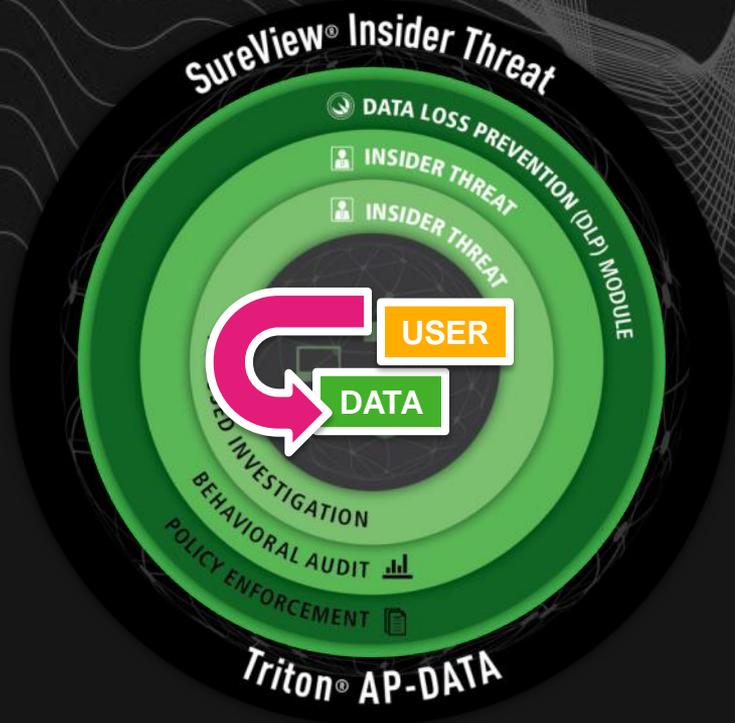
機敏資料傳輸分析與保護(DLP)

- 資料內容分析
- 基於資料傳輸事件的風險解析
- 監控與保護個資或智慧財產

DLP由內容感知技術提供資料分析與處理能力



營業秘密與機敏資料保護策略—結合使用者情境分析



DLP 資料分析與保護

- 資料內容分析
- 基於資料傳輸事件的風險解析
- 監控與保護個資或智慧財產

Insider Threat 使用者行為稽核分析

- 自動學習並建立使用者行為基準
- 辨識潛在的異常行為
- 基於使用者行為的風險分析

Insider Threat 聚焦事件調查，找出真正內部威脅

- 全面整合多種資料收集來源，包含AP-DATA
- 提供使用者行為的詳細記錄與完整情境
- 使用者行為錄影監控
- 協助找出高風險使用者

如果我們可以早一步知道...



粗心大意的內部員工

散漫高風險的網路行為



不遵守公司程序



準備離職，心生不滿的員工，瀏覽人力銀行網站，蒐羅公司內部資料



具有犯罪意圖的員工、商業間諜



惡意軟體感染，異常的提權行為



密碼遭到竊取，奇怪的網路存取嘗試，異常存取時間



神鬼駭客-史諾登...

其實這些威脅可以更早被發現

內部行為威脅指標

⚠️ 在夏威夷，下班時間約聘人員的異常登入行為

⚠️ 異常的內部橫向網路傳輸

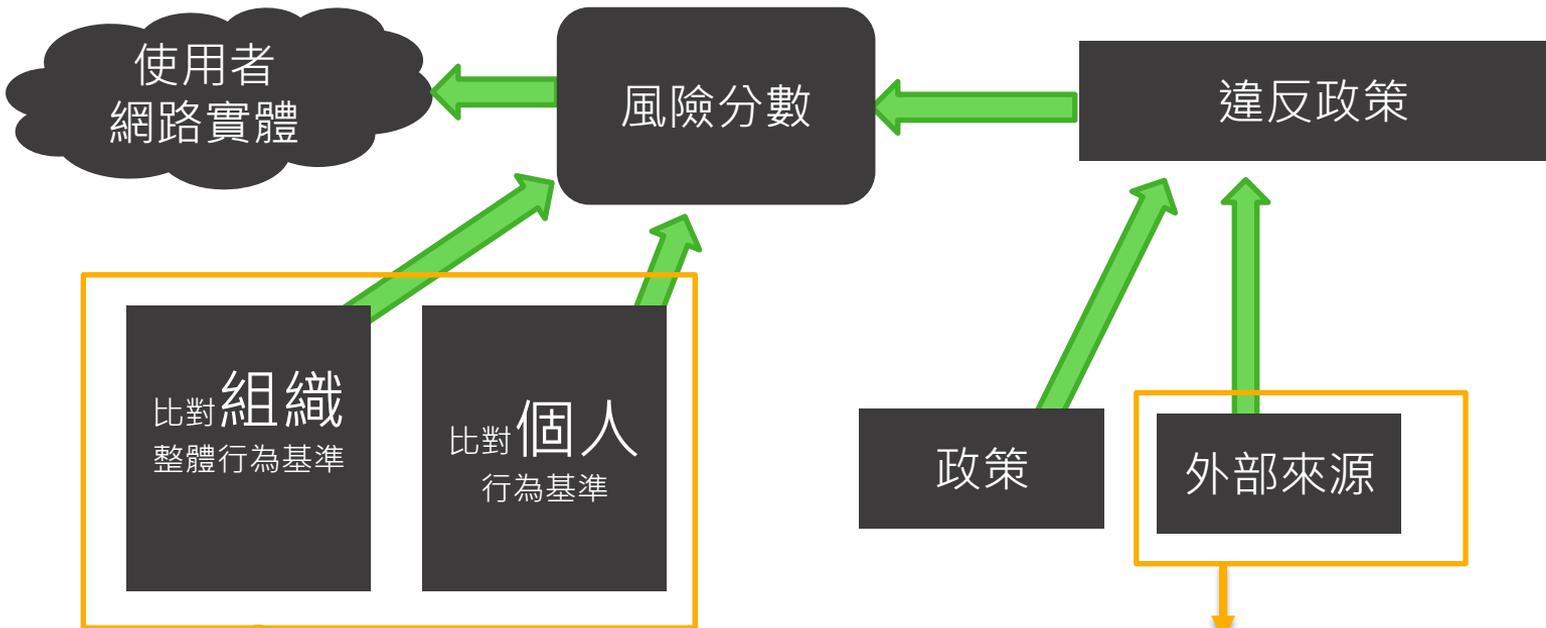
⚠️ 大量檔案傳輸至USB

⚠️ 20-25個員工帳號存取活動，都來自於史諾登的IP位址

⚠️ 異常的管理者權限行為

如何有效分析數以萬計的使用者行為事件以了解風險？

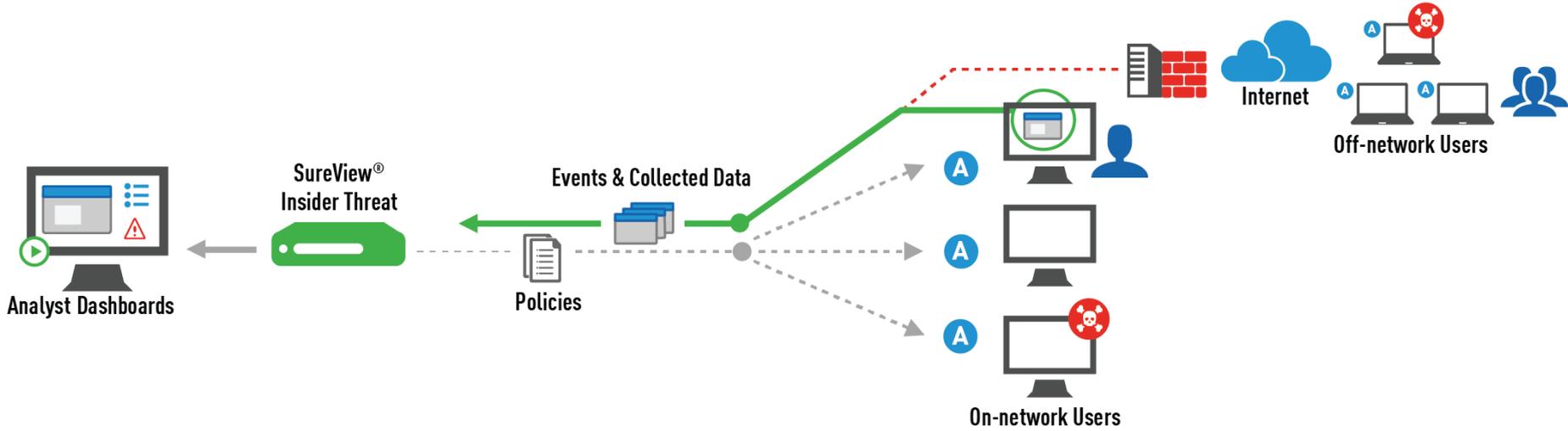
ADVANCED Scoring Engines



自動學習並與組織或個人使用行為比對

- 可整合DLP匯入風險評級
- 可指示FIT Agent收集事件證據

必須具備完整的使用者行為能見度



Application
General



Clipboard



Email



File



Keyboard



Logon



Printer



Process



System Info



Video



Web



Web URL

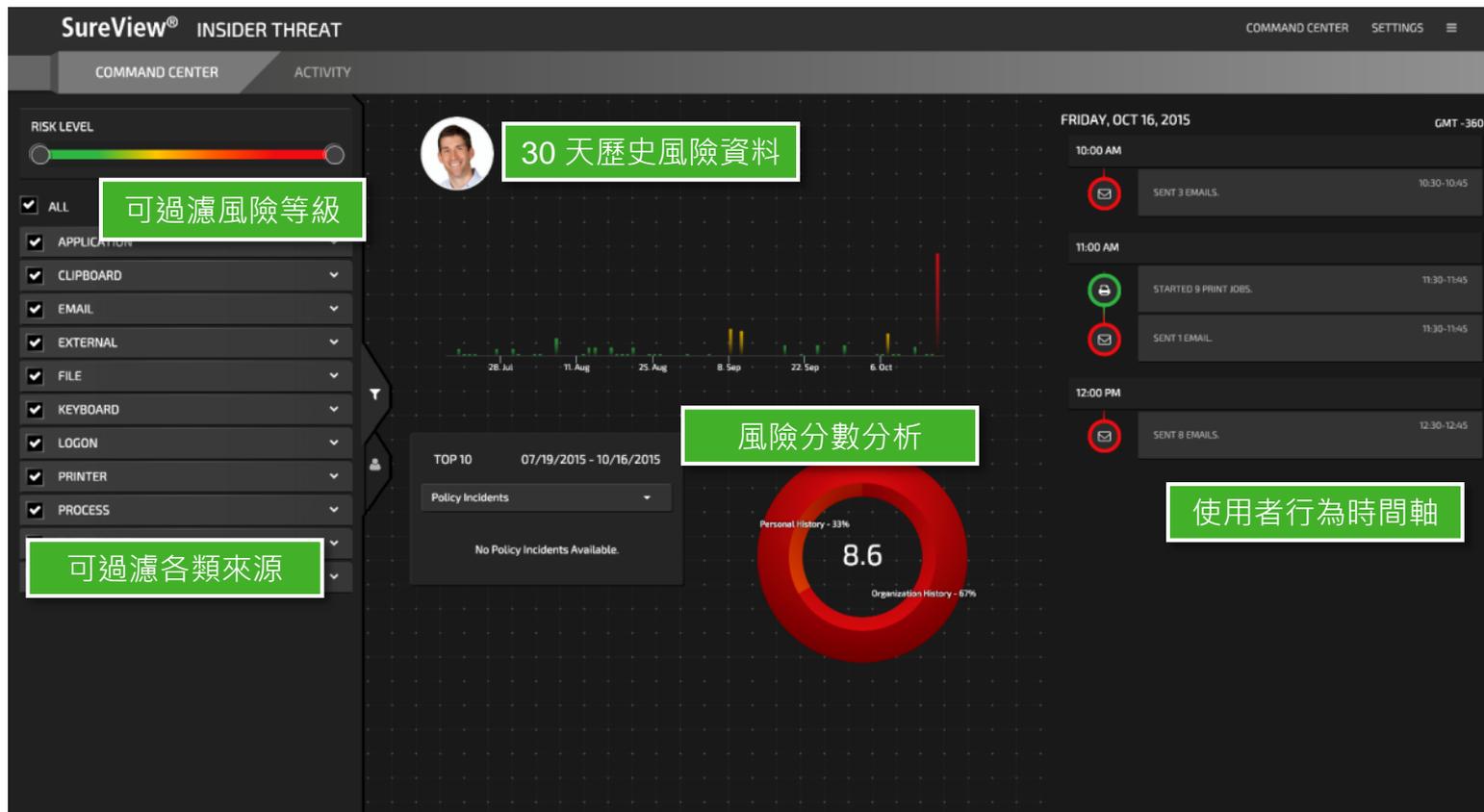


Webmail
(Gmail, Yahoo,
Outlook)

簡單易懂的風險儀表板，清楚呈現組織高風險使用者，降低管理者負擔



使用者風險分析與管理

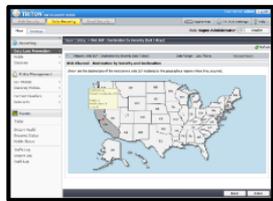


必須具備完整的取證與調查資訊



桌面錄影取證

提供事件觸發
事前、事中、
事後桌面操作
錄影取證，真
實還原原始情
境



網頁內容擷取

包含網頁圖片、
影像、音訊、
文字、檔案、
表單等完整網
頁內容資訊。



原始檔案

提供原始檔案
證據保留，以
作為事件調查
證據佐證



鍵盤側錄

提供原始鍵盤
按鍵與輸出文
字監控與側
錄，便於監控
分析特殊高命
令與敏感對話
內容



Meta Data

包含檔案、磁
碟、網頁、鍵
盤、應用程式
等各式原始元
資訊

提供事件觸發時之**事前**與**事後**錄影

The screenshot displays the Forcepoint Investigator Workbench Video Replay interface. The main window shows a Gmail interface with a red box highlighting a warning message: "A protected file is being attached to an email". The email details panel on the right shows the following information:

- Event - Email Sent**
- User: REALWORLD2008/CWAT
- Agent: JEACWARD
- Policy: Webmail with Attachment
- Category: Targeted User
- Group: Engineer Group A
- Priority: High
- Time: Jan 27 14:58:09
- GUID: {8EC982A-58E7-4C5F-A288-68729330FAE}
- Version: 6.3
- Rule: [Warning icon]
- Policy Violation info. [Warning icon]

The email details panel also shows the following information:

- Email Sent**
- Subject: Information
- From: carolyn.ward.1444@gmail.com
- To: mjessicasimmons@gmail.com
- Sent: [Warning icon]
- Protected File info. [Warning icon]
- Body (94 B) / FlyFishing.zip (20K)
- Joe Radoni
- Sr. Systems Engineer
- (80)831-1182
- Additional Properties
- Property: Encrypted: true
- Collection Start Time: Jan 27 14:58:09
- GUID: {DDE1E0D-6102-4972-63EA-03C20728950}

The Video Replay Window Displays user activities in context. The Video Replay Toolbar is visible at the bottom.



Thanks

