全新 Symantec ATP (Advanced Threat Protection)

從最高偵測率到最快應變力，全面掌握進階式威脅

Agenda

1	現狀威脅分析
2	賽門鐵克 APT 安全防護架構
3	防護功能說明
4	結論

Agenda

1 現狀威脅分析

2 賽門鐵克ATP防護架構

3 防護功能說明

4 結論

In 2009 there were

2,361,414

new piece of malware created.

In 2015 that number was

430,555,582

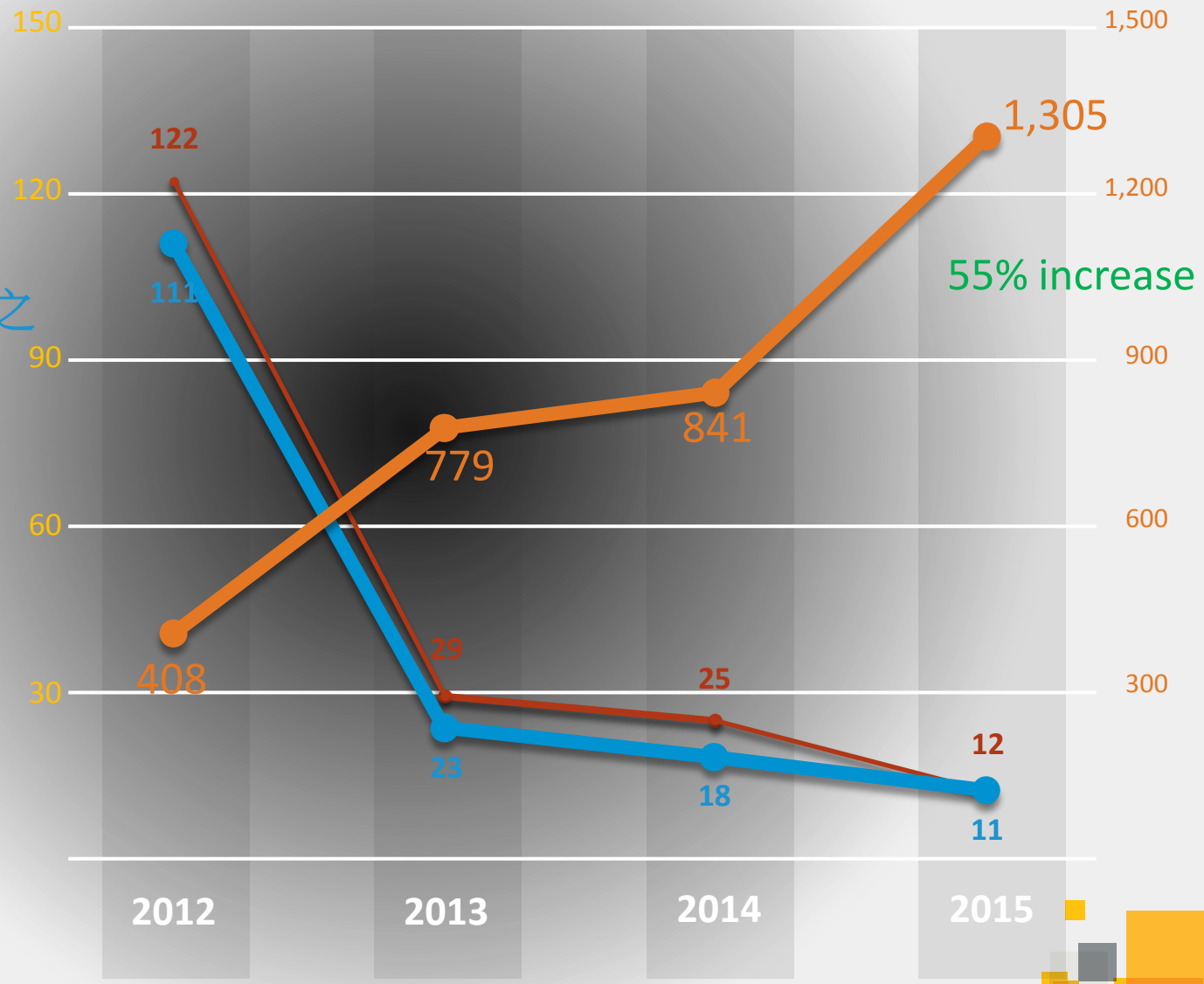
That's

1 Million 179 Thousand

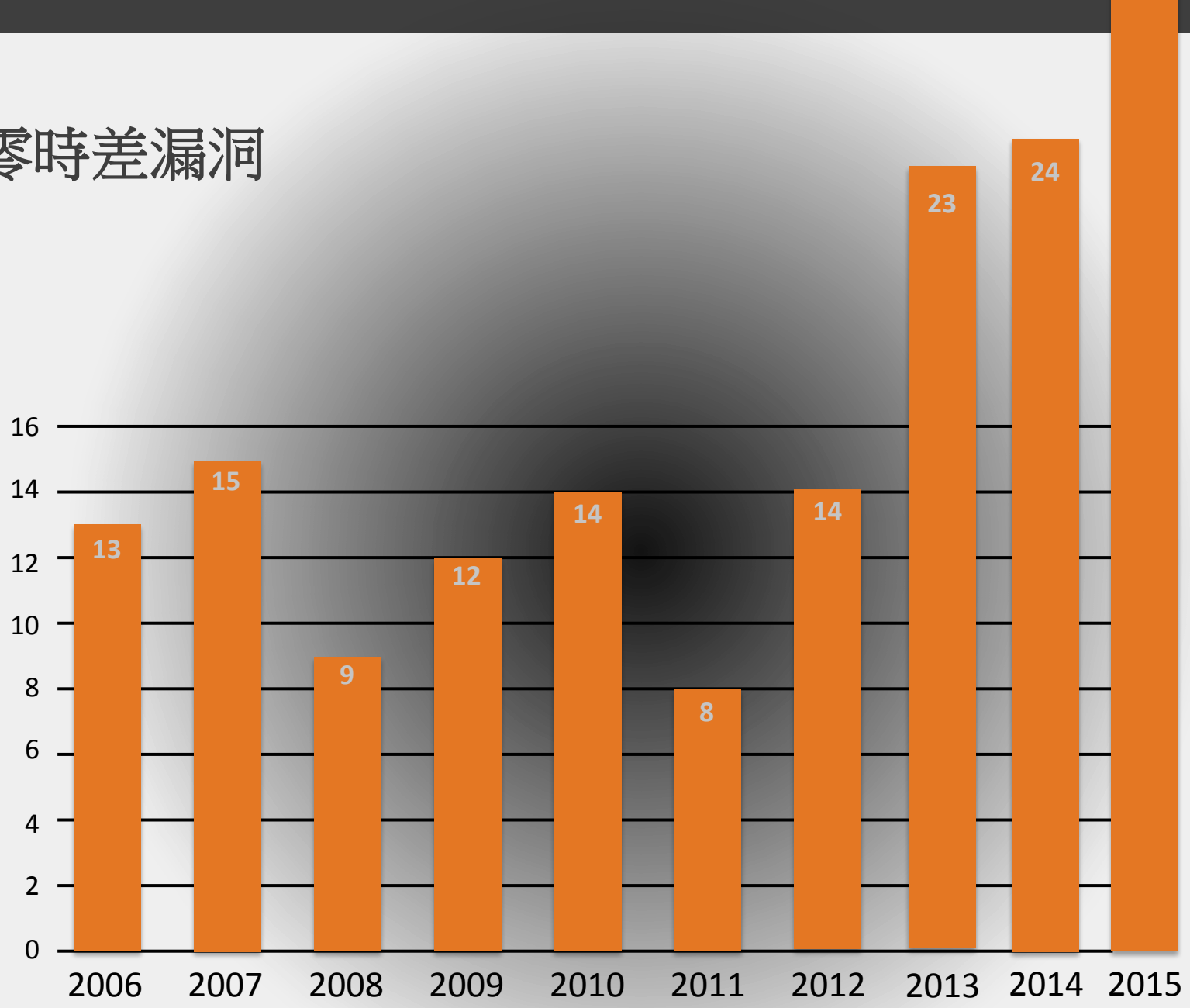
a day.

針對性攻擊活動趨勢統計

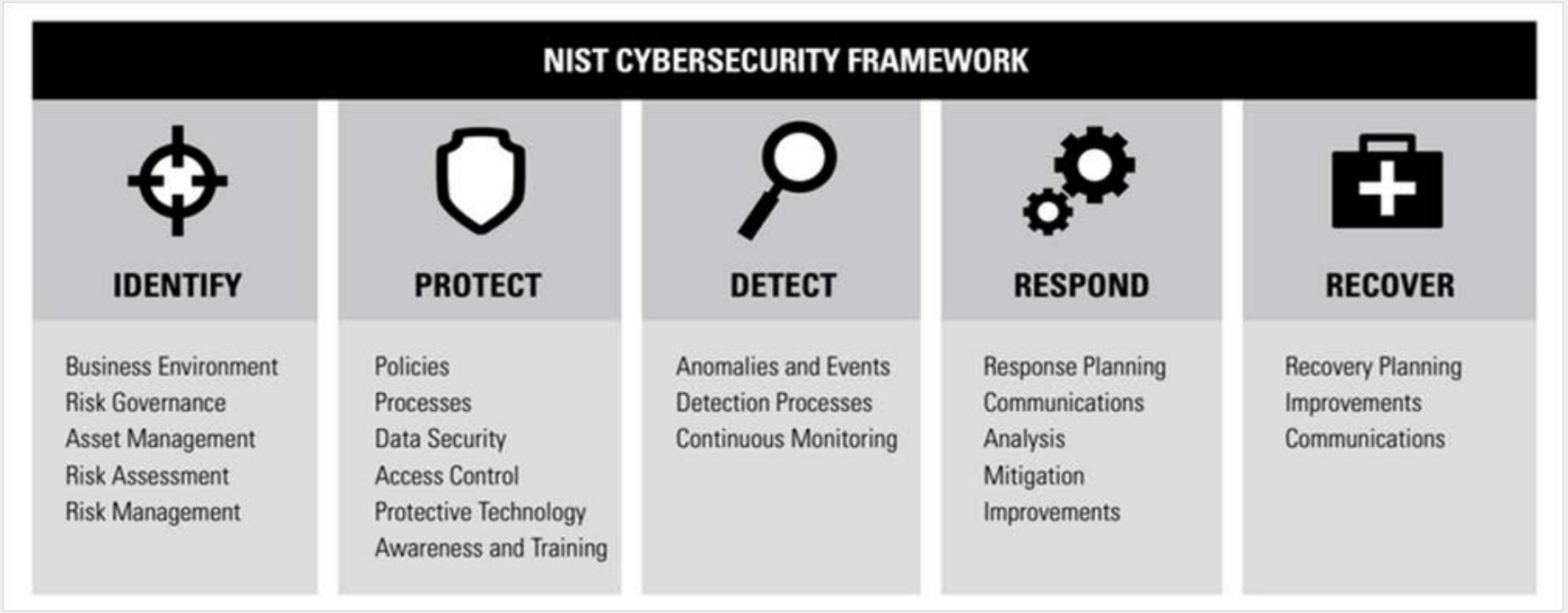
- 平均電子郵件病毒攻擊數量
- 每次攻擊活動之收件者人數
- 針對式攻擊活動數量



零時差漏洞


54
16
14
12
10
8
6
4
2
0
13
15
9
12
14
8
14
23
24
2006
2007
2008
2009
2010
2011
2012
2013
2014
2015

NIST Cybersecurity Framework



What Is Symantec™ Advanced Threat Protection?

阻擋

阻擋攻擊

偵測

找出入侵管道

回應

遏制並修復問題

Symantec Endpoint Protection

- SONAR
- Insight
- Firewall
- IPS
- App Control
- Media Control

Symantec Email Security.cloud

- DKIM email authentication
- Skeptic malware detection
- Traffic Shaping and reputation based protection.
- Aggressive SLA

Symantec™ Advanced Threat Protection

ATP Endpoint
HW or VM appliance adds EDR to SEP

ATP Network
HW or VM Network Appliance

ATP Email
Add-on for Email Security.cloud

Agenda

1 現狀威脅分析

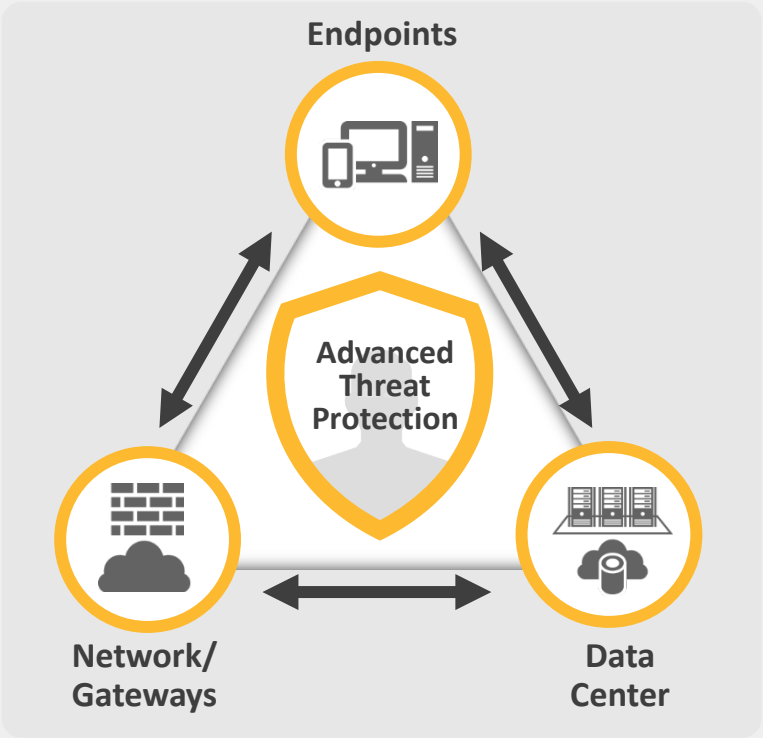
2 賽門鐵克 APT 安全防護架構

3 防護功能說明

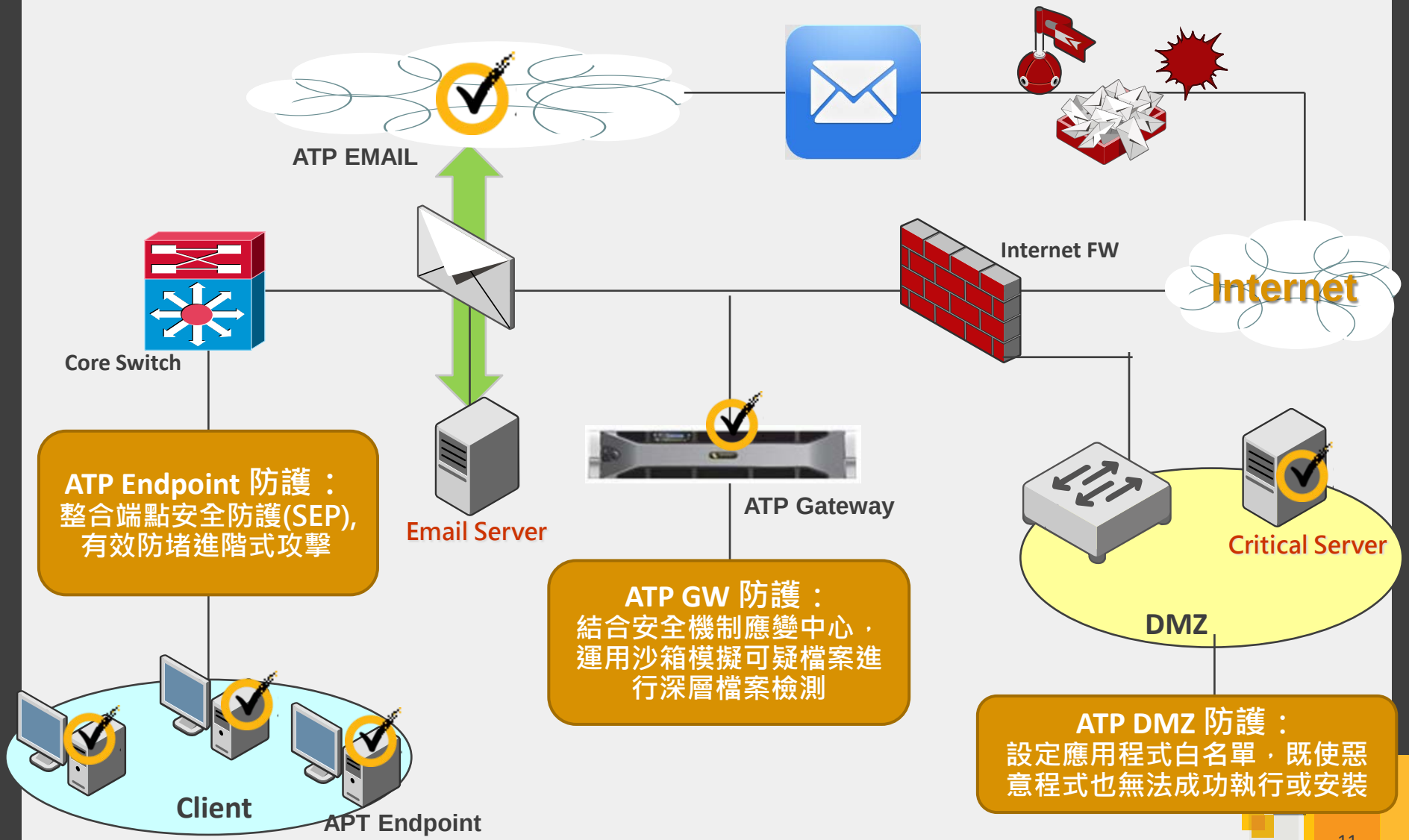
4 結論

賽門鐵克 進階威脅防護策略

- 針對進階式攻擊提供一個全方位防護架構
- 在每一個控制點上，提供事件分析與矯正能力
- 可以保護內部資料中心、虛擬化或是雲端，並實現流程化的管理平台
- 雲端管理平台可以可以同時管理端點、伺服器與閘道端



賽門鐵克 ATP 全方位防護架構示意圖



Agenda

1 現狀威脅分析

2 賽門鐵克 APT 安全防護架構

3 防護功能說明

4 結論

賽門鐵克 ATP 之獨家技術

更智慧 | 更好的偵測及更快速回應 | 關聯所有控制點 | 整合 SEP

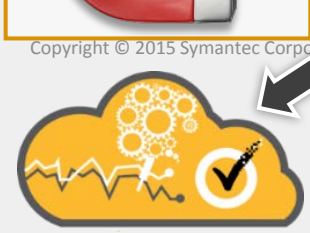
SYMANTEC CYNIC™

NEW: 雲端 PAYLOAD 誘發技術

全面性涵蓋：包含有 Office docs, PDF, HTML, Java, containers, 及可執行檔

更有效偵測：模擬使用者在真實環境中操作。並同時運行於虛擬與實體環境中

雲端優勢：創新技術。例如最新惡意程式變種更新，即時擴展以符合需求



SYMANTEC SYNAPSE™

NEW: 關聯分析與優先等級排序

優先等級排序：根據已經感染或是已經被阻隔進行事件優先權分級

事件的分析調查：關聯所有控制點

容易使用：提供視覺化感染路徑圖形顯示

賽門鐵克 ATP 模組簡介

 **ATP:** Endpoint	 **ATP:** Network	 **ATP:** Email
• 提高端點惡意威脅能見度 • 端點異常，可疑檔案及威脅矯正 • 整合現有 SEP – 需不要額外安裝其他程式	• 檢視分析所有裝置與網路協定 • 除檔案沙箱進階分析還可以針對網頁攻擊與 C&C 惡意連線進行偵測 • 可以安裝於實體機器、虛擬環境， 支持 In-Line 與 TAP 部屬	• Email 內容進階分析 (依然是 APT 攻擊重要關鍵通道) • 電子郵件提供豐富的有針對性的攻擊的報告，透過 Cynic 與 Synapse 關聯分析更清楚知道威脅來源 • 可以透過Symantec. Cloud 來提供

賽門鐵克 ATP 網路模組概述

ADVANCED THREAT PROTECTION: NETWORK

- **網路裝置**
  - 硬體 (8840, 8880) 或 Virtual (VMWare ESXi 5.1, 5.5)
- **部署架構**
  - **TAP/SPAN – Monitoring** 或 **In-line – Blocking mode**
- 監控內部 inbound 與 outbound 連外流量
- 可以檢測所有的裝置與所有通訊協定(protocols)
- 自動沙箱, 網站攻擊 & 殭屍網路偵測
- **Agentless** 整合包含 Email Security.cloud 與 Symantec Endpoint Protection

INCLUDES THE CORE PLATFORM

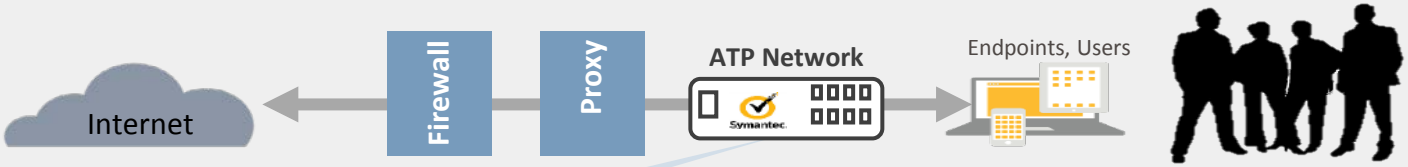
SYMANTEC CYNIC™

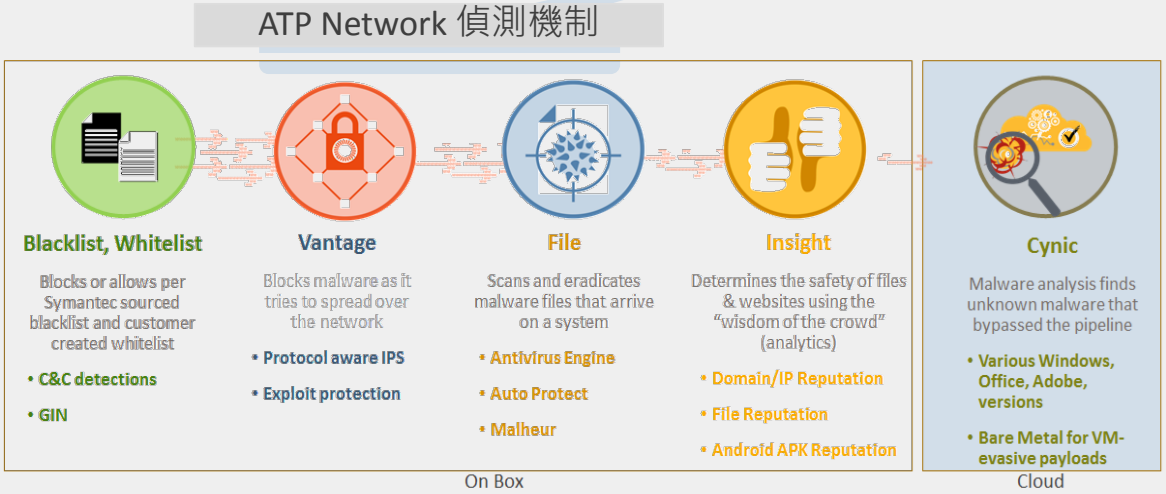
雲端沙箱
惡意檔案分析平臺

SYMANTEC SYNAPSE™

單一資安事件關聯

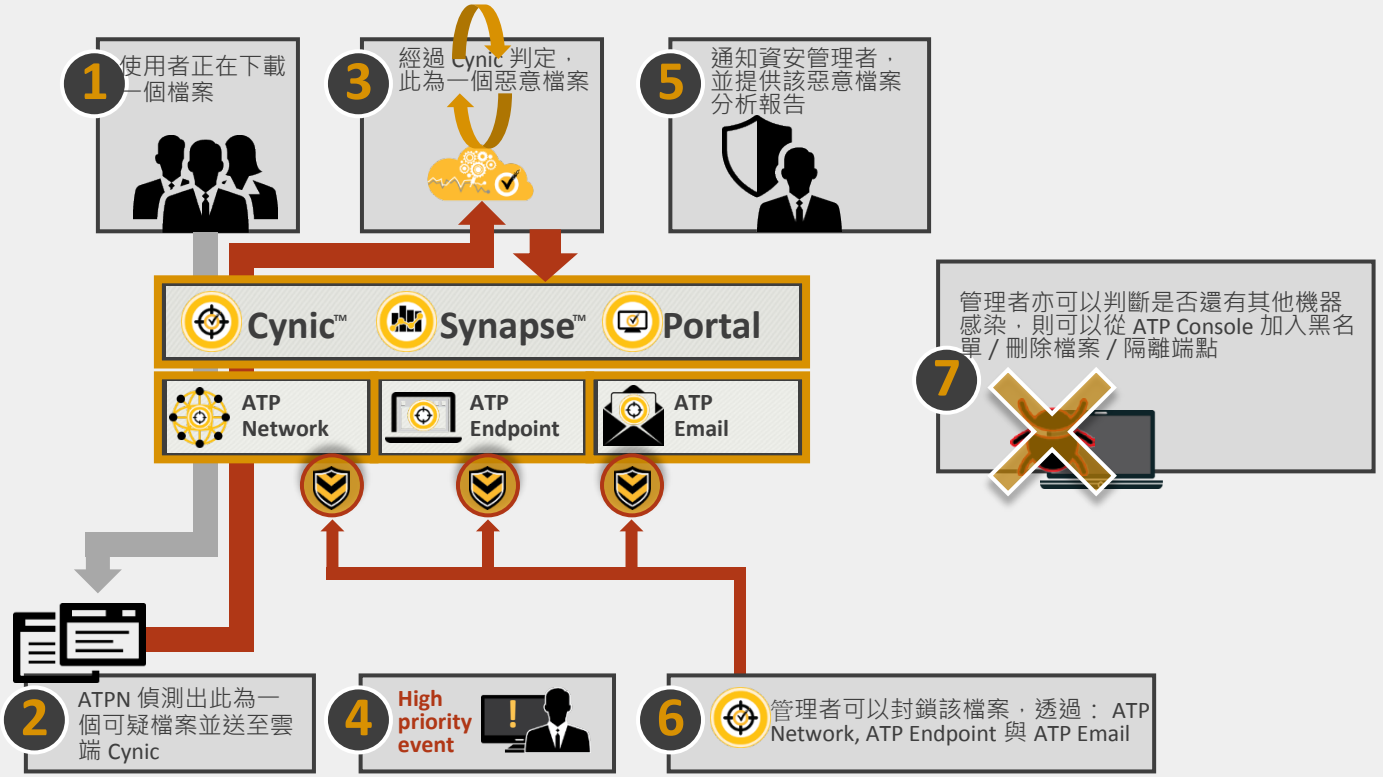
完整的偵測機制:Advanced Threat Protection -Network





- **虛擬與實體 Appliance**
  - 2 款硬體裝置
    - 8840 network throughput 500 Mbps
    - 8880: network throughput 2Gbps
  - 3 種部署模式
    - TAP, In-line Block, In-line Monitor
  - 集中式管理：最高可以支援 50 台 Scanner Nodes
- **檢測所有 inbound 與 outbound 網路流量**
- **透過賽門鐵克雲端進行 Cynic 分析**

ATP in Action
疑似惡意檔案經由網路下載



賽門鐵克 ATP 端點模組概述

ADVANCED THREAT PROTECTION: ENDPOINT

- 無需安裝額外代理程式
- 提供 EDR 端點偵測 (Detection) 與回應 (Response) 能力
- 可以選擇部署於虛擬或是實體環境
- 即時搜尋可疑事件與新威脅
- 可以透過『刪除』，『黑名單』，『隔離』等方式即時事件增加事件處理速度
- 迅速與確實封鎖威脅已判定可疑威脅程式
- 記錄與監控端點平時正常活動，異常時可以透過 IoC (入侵指標)搜尋找出所有相關感染端點

INCLUDES THE CORE PLATFORM

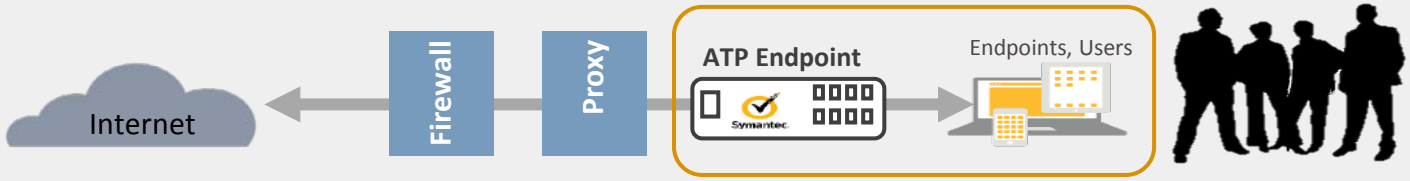
SYMANTEC CYNIC™

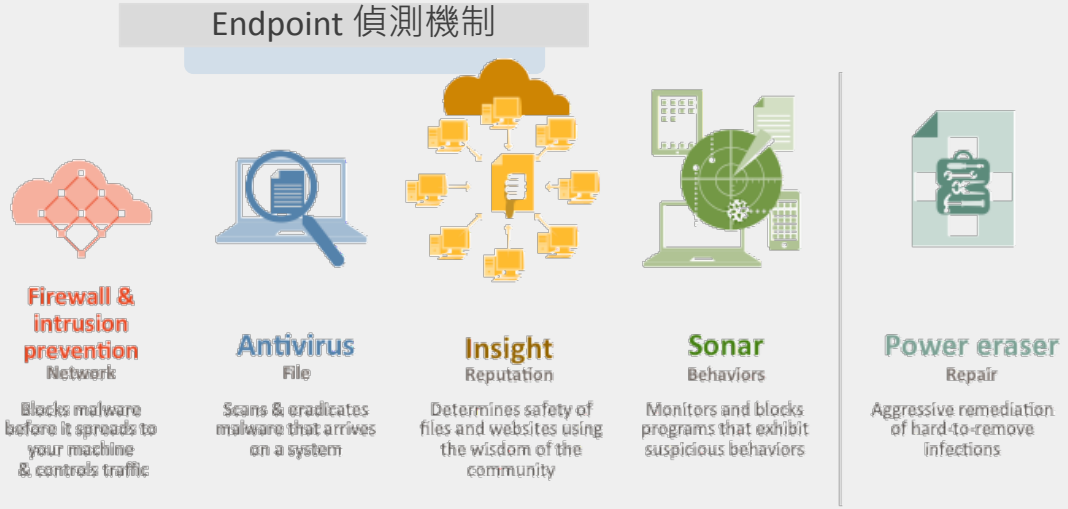
雲端沙箱
惡意檔案分析平臺

SYMANTEC SYNAPSE™

單一資安事件關聯

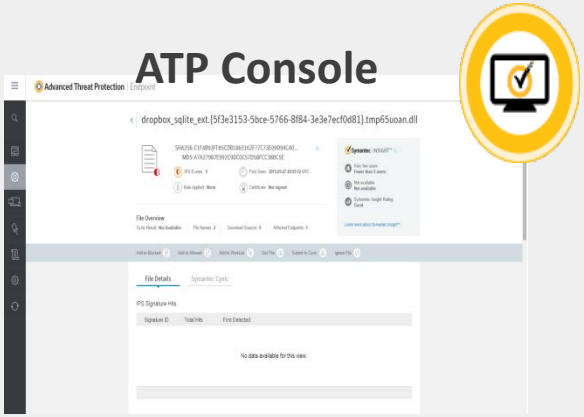
完整的偵測機制:Advanced Threat Protection-Endpoint





- **Virtual appliance**
  - 32 GB RAM, 250 GB hard disk
  - 單一台 Appliance 最高可以支援 25000 使用者
- **整合現行 SEP 之端點**
- **惡意程式威脅搜尋包含： hashs, files, host, domain**
- **透過賽門鐵克雲端進行 Cynic 分析**

ATP 端點模組： 搜尋遭到入侵的跡象指標(IoC)



1 **輸入入侵跡象指標查詢**
管理者在 ATP Console 輸入可疑檔案, 要求用戶端執行掃描動作

SEPM

5 **資料顯示在 ATP**
SEPM 回傳資料直接顯示於 ATP 管理平台上

4 **結果傳回至 SEPM**
掃描結果從用戶端回傳至 SEPM

2 **掃描命令傳送**
等待heartbeat時間, 將掃描命令傳送至用戶端

- 所有的溝通都會經由 **SEPM** 來進行
- 利用 SEP 與 SEPM 定期 heartbeat 溝通來傳送命令
- 立即回覆從 SEP -> SEPM
- 從 ATP <-> SEPM 溝通連線幾乎是即時(1min)

3 **開始搜尋**

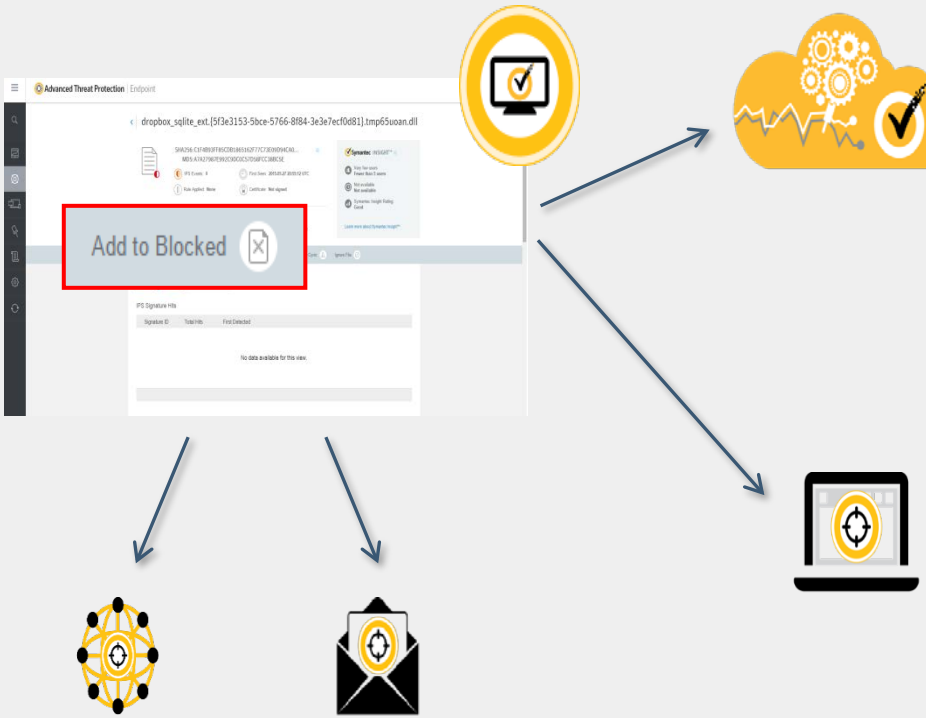
SEP Client 開始搜尋該電腦資訊

掃描條件包含如下(either quick scan or full scan):

- Files by hash (SHA256, SHA1 and MD5) or name
- Folders by name
- Registry keys
- Can use wildcards

SEP

賽門鐵克 APT ： Endpoint 快速回應 -電腦隔離



防範更多交互感染

- Hash is pushed to unified blacklist across all control points (network and Email)

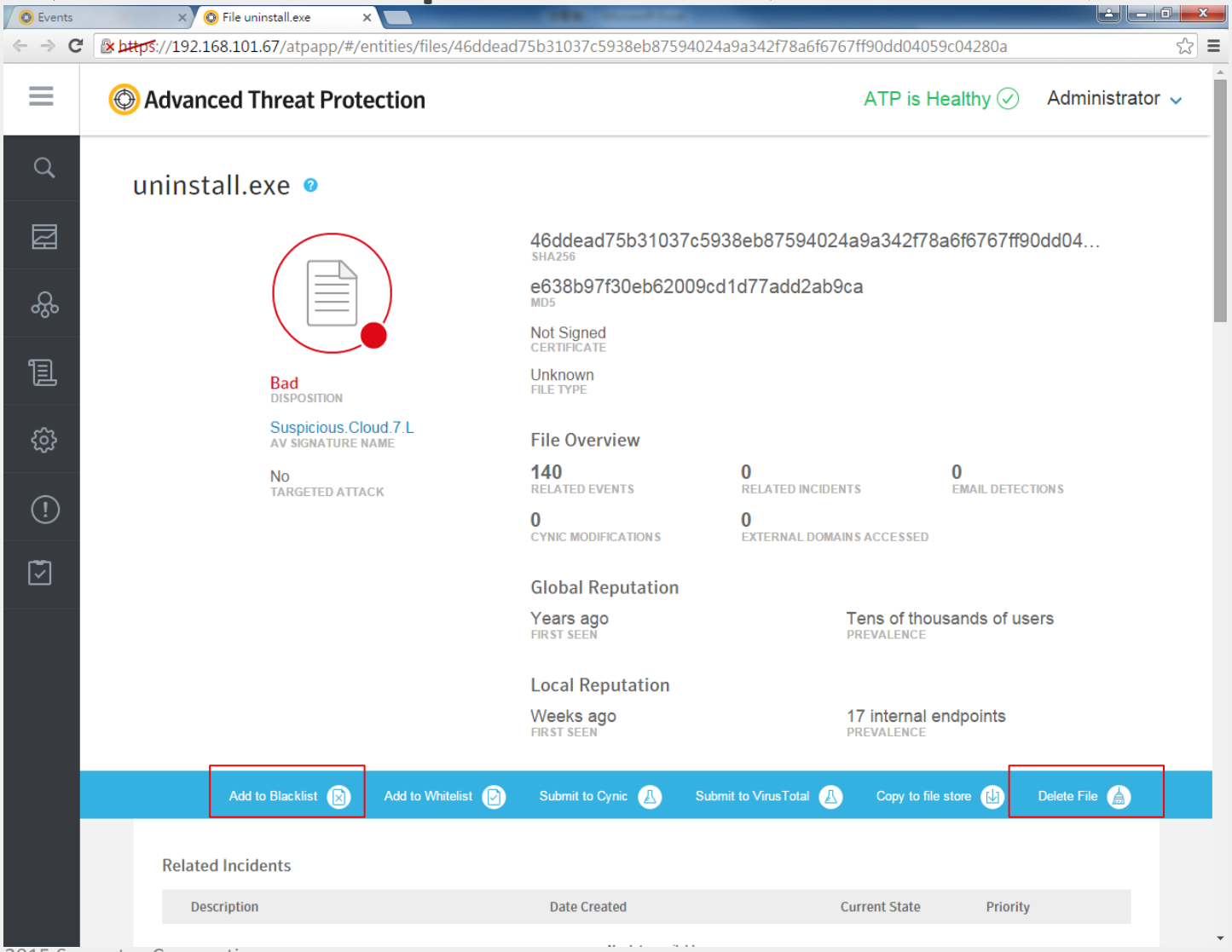
Insight

- File is given Ultra High Bad reputation score in local (ATP appliance based) reputation store
- Now appears as bad in ATP UI
- Next SEP client to call in for reputation will get new score and block the file

受感染檔案與電腦隔離

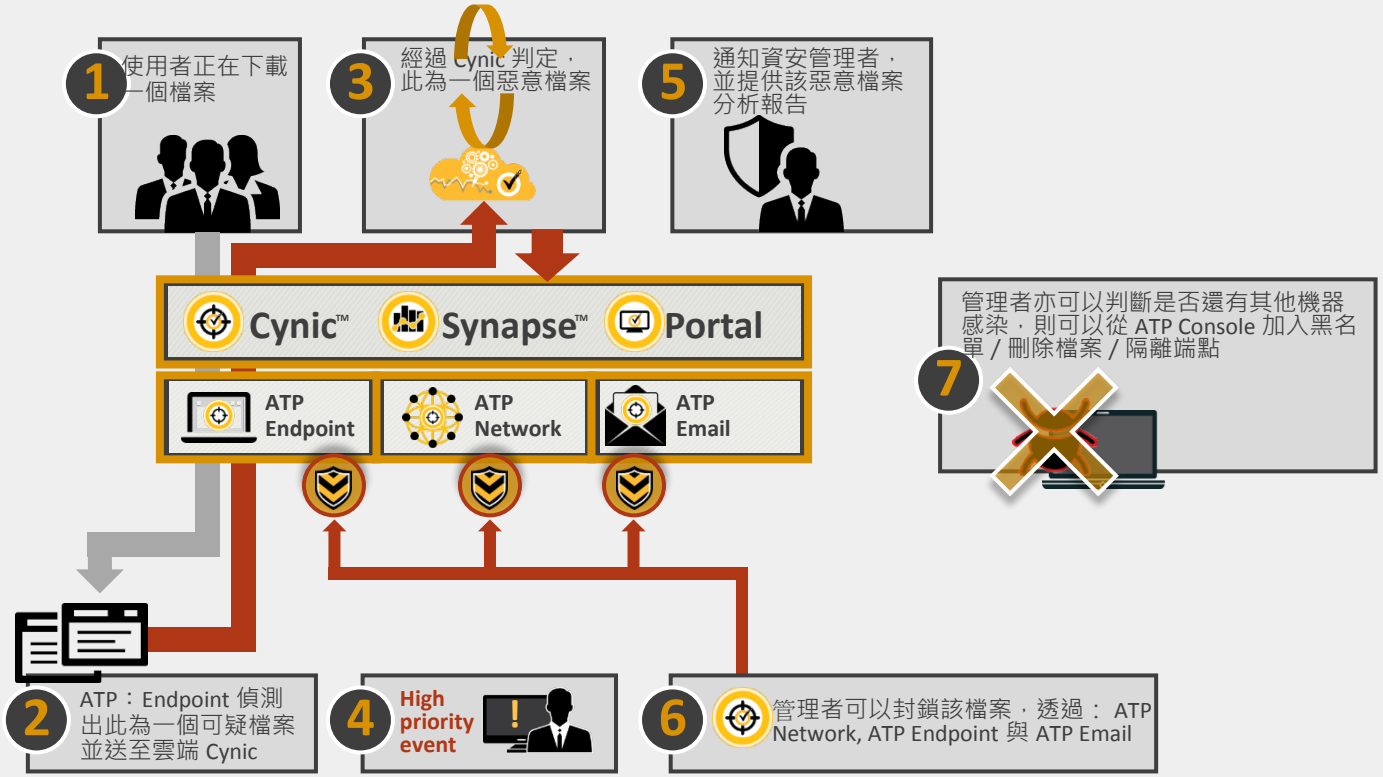
- Hash is pushed to RU6 SEPM and added to System Lockdown blacklist
- Blacklist is propagated to clients on next heartbeat
- Client physically prevents access to the file

賽門鐵克 APT：Endpoint 快速回應 – 遏止與矯正



ATP in Action

疑似惡意檔案經由端點下載



賽門鐵克 ATP 郵件模組概述

ADVANCED THREAT PROTECTION: EMAIL

- 整合至賽門鐵克 Email Security.cloud 服務強化郵件威脅防護
- 增加 Cynic™ 沙箱機制進階式威脅的郵件偵測
- 可以提供詳細 Targeted Attack 報表資料
- 可以針對組織或是個人使用者提供 Identifies targeted attacks 通報
- 可以將ATP 郵件日誌傳送至賽門鐵克 ATP 與 SEP 事件『進行關連分析』
- **容易管理** – 透過賽門鐵克.cloud 整合管理頁面

INTEGRATES WITH THE CORE PLATFORM

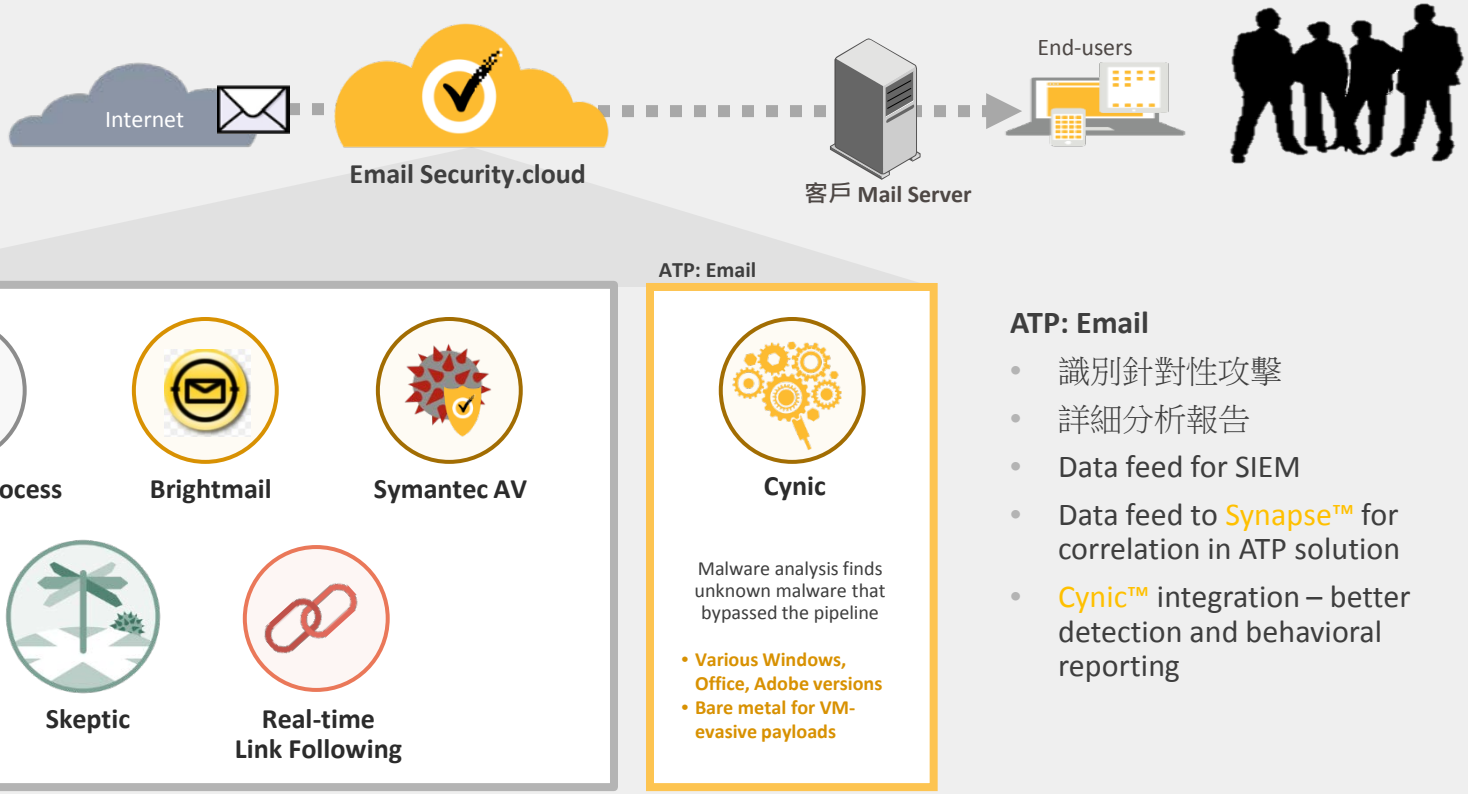
SYMANTEC CYNIC™

雲端沙箱
惡意檔案分析平臺

SYMANTEC SYNAPSE™

單一資安事件關聯

完整偵測機制: Advanced Threat Protection (Email)

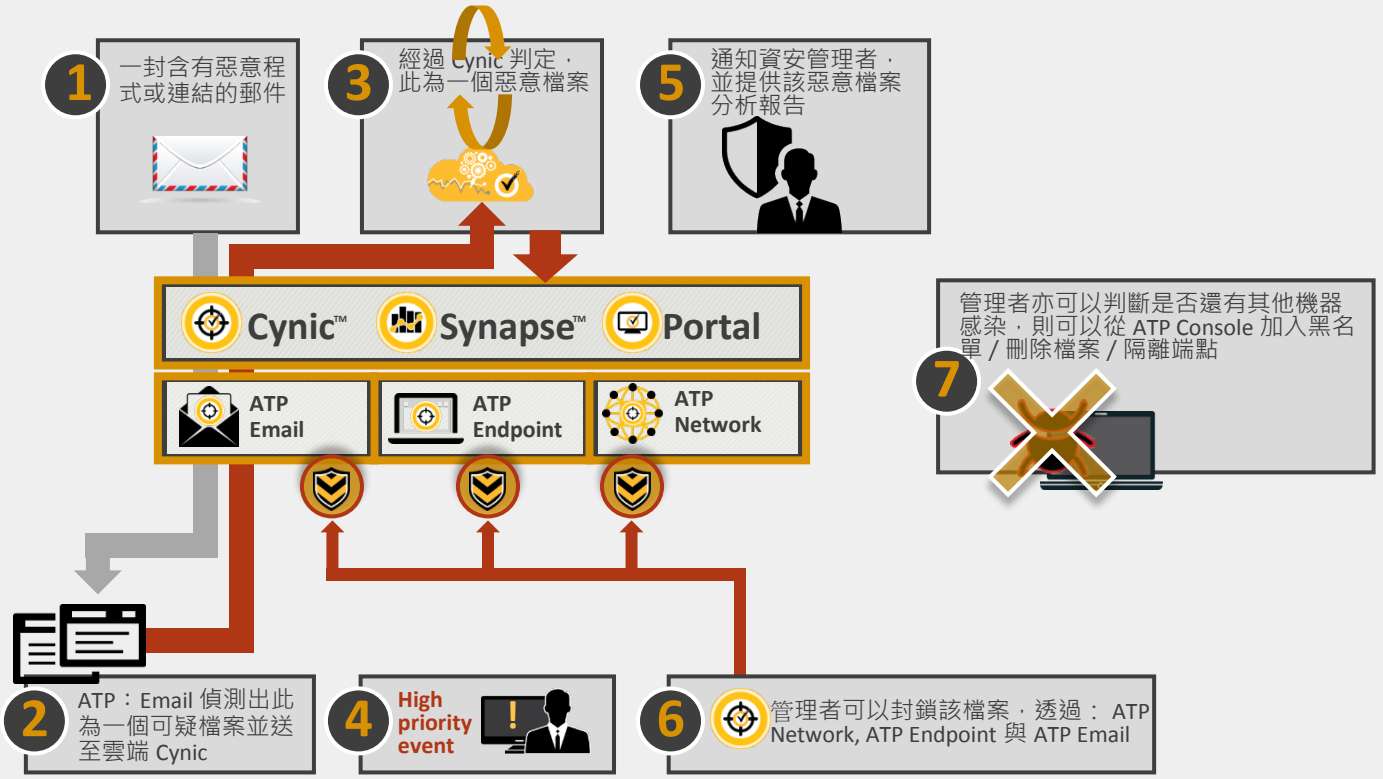


ATP: Email

- 識別針對性攻擊
- 詳細分析報告
- Data feed for SIEM
- Data feed to Synapse™ for correlation in ATP solution
- Cynic™ integration – better detection and behavioral reporting

ATP in Action

疑似惡意檔案經由郵件傳送



Agenda

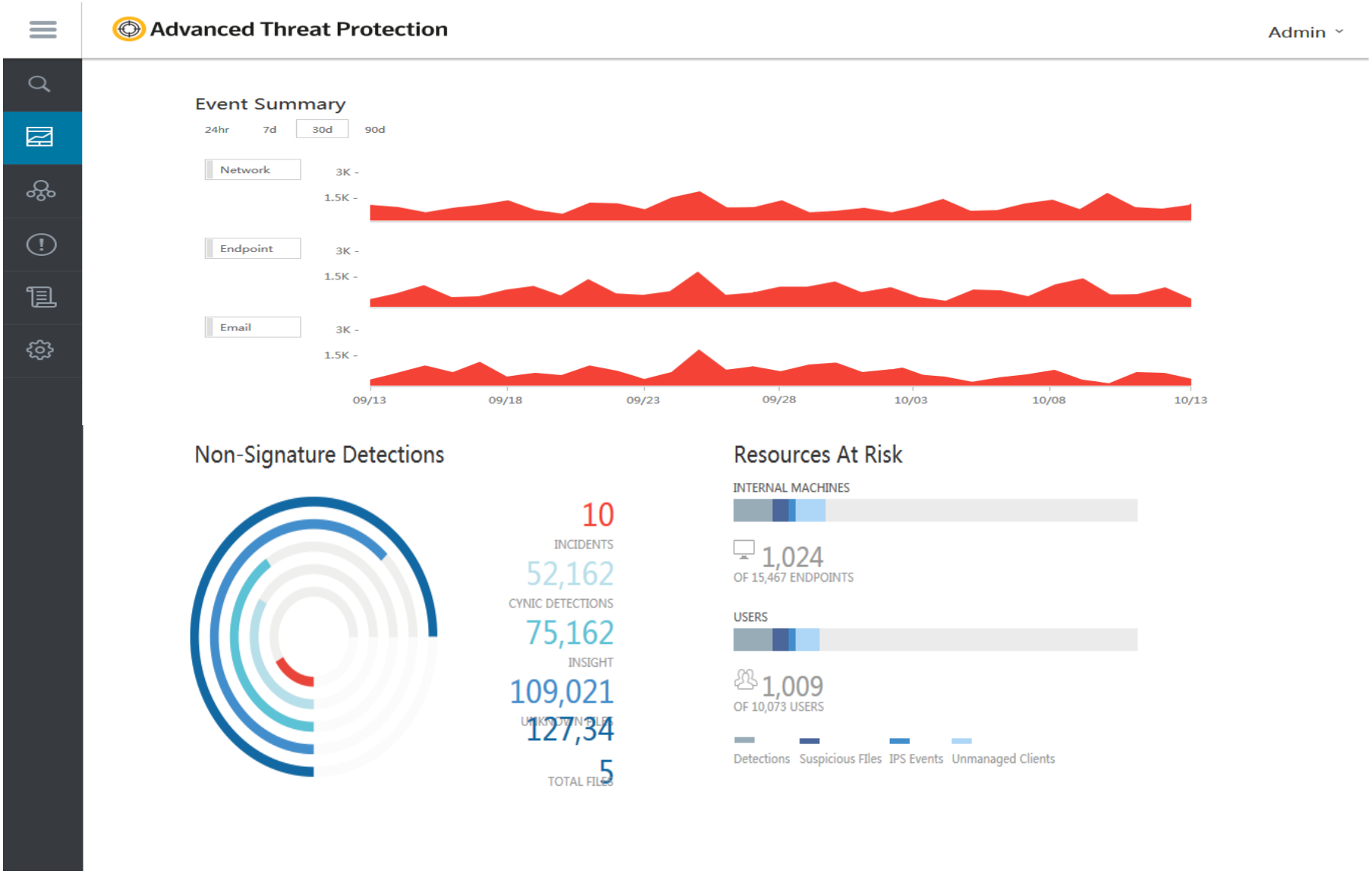
1 現狀威脅分析

2 賽門鐵克 APT 安全防護架構

3 防護功能說明

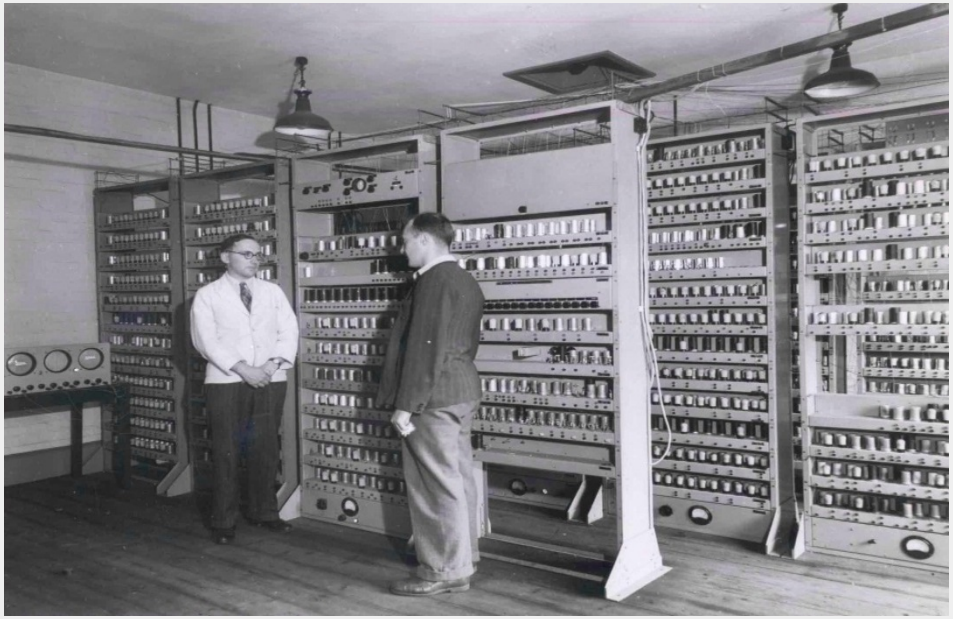
4 **結論**

統一管理介面

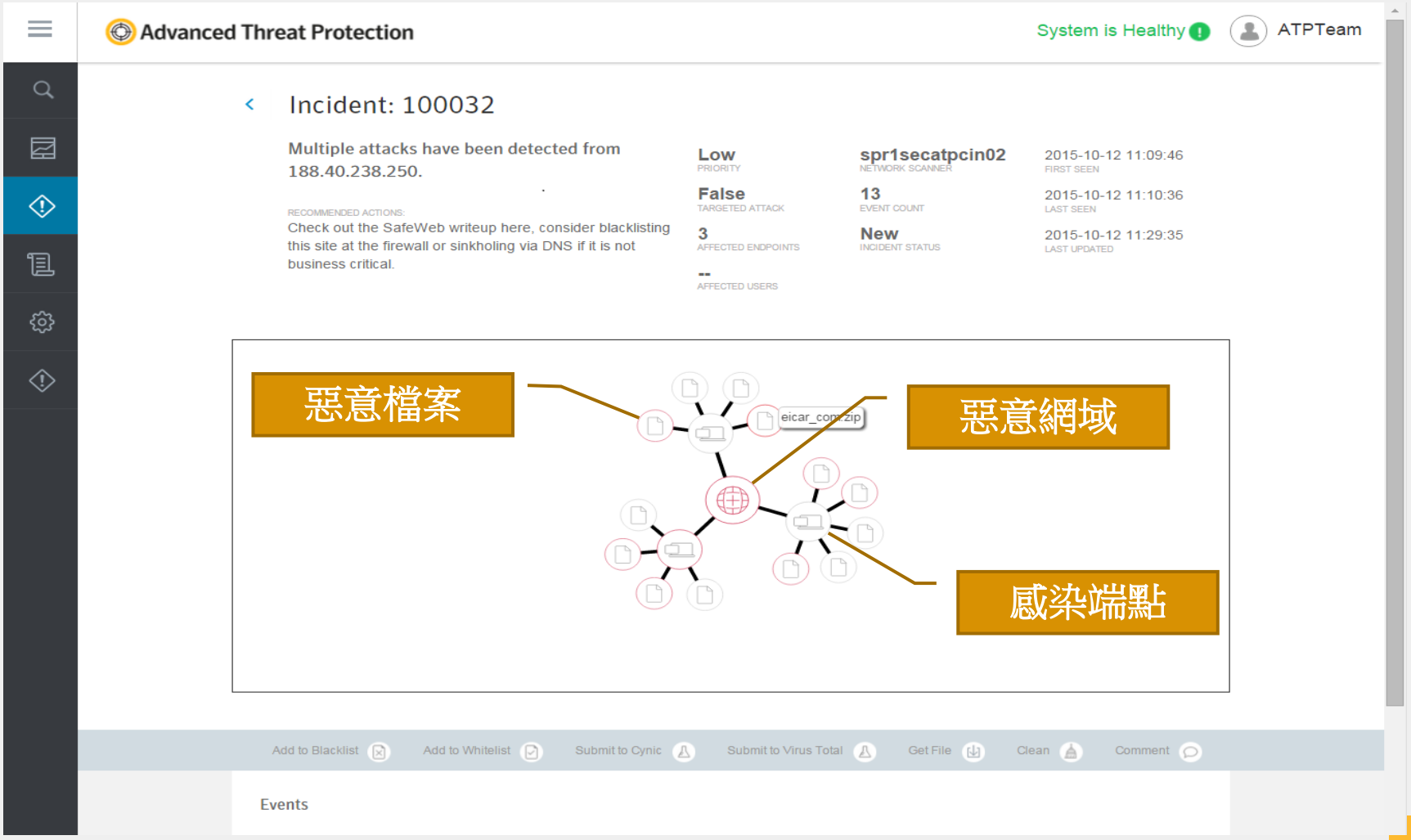

Advanced Threat Protection
Admin
Event Summary
24hr
7d
30d
90d
Network
Endpoint
Email
3K -
1.5K -
09/13
09/18
09/23
09/28
10/03
10/08
10/13
Non-Signature Detections
10
INCIDENTS
52,162
CYNIC DETECTIONS
75,162
INSIGHT
109,021
127,34
5
TOTAL FILES
Resources At Risk
INTERNAL MACHINES
1,024
OF 15,467 ENDPOINTS
USERS
1,009
OF 10,073 USERS
Detections
Suspicious FIles
IPS Events
Unmanaged Clients

Cynic 雲端沙箱 – 虛擬誘發 + 實體誘發

- 如果惡意程式的行為中，分析到有嘗試偵測 VM Driver 的行為，Cynic 會自動將檔案傳送至實體機進行誘發並分析



事件關聯性 – 關聯所有相關威脅



快速回應 – 遏止與矯正

- 加入黑名單
  - 於網路、端點及 Email 進行阻擋
- 刪除端點檔案
- 隔離端點電腦

賽門鐵克 ATP 優勢

最多使用者 & 最多資安情報

- 端點安全: 1億7千5百萬
- 郵件安全: 8億5千萬

最佳的防護

- 持續成為在端點防護與郵件安全的領先者
- 虛擬機及實體機誘發機制
- 結合最新惡意程式威脅情資

全面性偵測

- 全方位進階式安全防護管控 : 端點、郵件及網路
- 偵測範圍包含 : C2 callbacks、行為啟發、信譽評等..等
- 最新技術 : Cynic 雲端沙箱、Synapse 智慧關聯
- IOC 搜尋

最快速回應

- 透過關連事件分析，快速尋找出企業事件中的高風險
- 有效分析調查 : 威脅在哪裡? 如何進來?
- 一鍵矯正

提供最低的資安營運成本

- 關聯並排定優先等級：端點、網路、郵件
- 雲端沙箱
- 整合單一管控介面, 可整合 SIEM 系統

卓越第三方市場評比

"ICSA was **impressed with Symantec ATP** and would recommend it to enterprises"

Product tested	False Positives
Symantec ATP	0%
Trend Deep Discovery	4.9%
Fortinet	3.3%

ICSA Labs, 8th Dec 2015

最低誤判率

26% higher malware protection than **Cisco** and **18%** higher than **FireEye**

"Symantec was observed to have the **highest detection rate** for every category of malware"

Miercom Labs, 18th Dec 2015

Identified **95%** More threats than competing vendors

最高偵測率

"The **most accurate appliance** was Symantec ATP"

Product tested	Detection Score
Symantec ATP	100%
Palo Alto Networks	90%
Cisco Snort	72%
Fortinet	69%

Dennis Technology Labs, 18th Dec 2015

最高正確率

WELLS FARGO

PINNACLEHEALTH

vodacom

EMAAR

TecBan

Inchcape Shipping Services

EURONEXT

مصرف الإنماء alinma bank

بنك الائتمان الكويتي Kuwait Credit Bank

HERSHEY THE HERSHEY COMPANY

PEARSON

Thank you

Q&A

Sean_Wang@symantec.com

ATP 郵件模組 – 目標式攻擊確認

傳送 Email 進行進階分析

乾淨信件傳送至收件者

惡意郵件被 Skeptic, Cynic 與 Link Following 技術偵測及阻擋

Targeted Attack Analysis

Skeptic

Customer Dashboard and Detailed Report updated

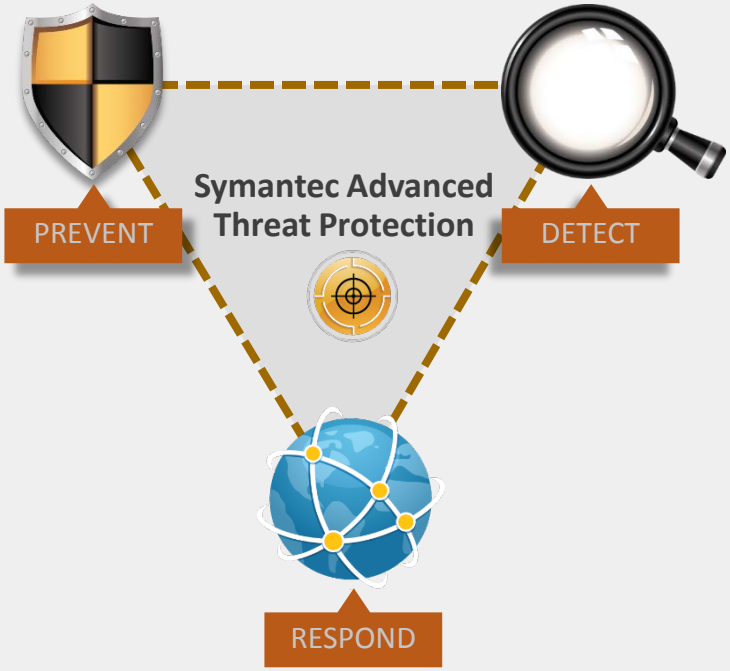
賽門鐵克觀點: APT 攻擊該如何保護呢?

防護、偵測、回應並整合企業內的主要安全控制點

防護
涵蓋所有控制點並即時阻擋威脅

偵測
透過雲端沙箱，進行 Payload 誘發及行為分析，於數分鐘內發現惡意行為及進階威脅

回應
自動化關聯並進行安全事件的優先權排序，資安分析師執行事件調查分析並提供解決修補方案



APT 網路模組：偵測所有通訊協定

7 分鐘

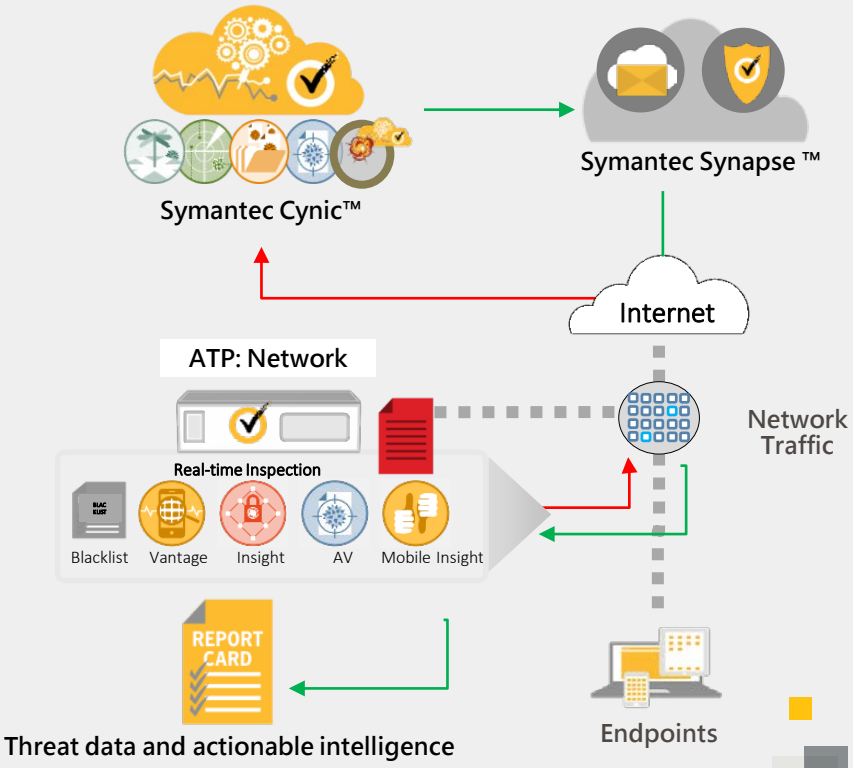
疑似惡意檔案將送回至Cynic 平台進行分析

Cynic 執行與分析該檔案行為透過不同的沙箱同時進行，其中也透過實體機分析以避免VM-aware 惡意程式.

透過 Synapse 把該事件的行為與賽門鐵克智能數據, 郵件, 端點進行關連分析

根據Cynic觀察到行為執行相對應動作，包含事件優先處理等級.

網路型 ATP 提供本機即時檔案檢測與防護技術, 雲端沙箱, 網站攻擊 及 殭屍網路偵測



Thank you!

保安資訊有限公司 –賽門鐵克解決方案專家

www.SaveTime.com.tw　　好記:幫您節省時間.的公司.在台灣

We Keep Info. Safe，Secure & Save you Time，Cost

Thank you!

保安資訊有限公司 –賽門鐵克解決方案專家

www.SaveTime.com.tw　　好記:幫您節省時間.的公司.在台灣

We Keep Info. Safe，Secure & Save you Time，Cost