1

# 賽門鐵克端點防護最新版 SEP 14
# Symantec Endpoint Protection V14

保安資訊有限公司-賽門鐵克解決方案專家

# 相關術語

**攻擊鏈**

攻擊鏈(Attack Chain)，有時也被稱為殺傷鏈(Kill Chain)，基本上是攻擊的生命週期或是描述網路攻擊階段的框架，從早期的偵察到最終的數據滲透的目標。

**機器學習**

機器學習：端點上的多面向機器學習可防止新型和未知的威脅，減少對病毒特徵的依賴。使用全球情報網上數以兆計的好壞檔案樣本來訓練機器學習，以大幅降低誤報率。"

**記憶體攻擊緩解**

賽門鐵克技術術語可攔截常用軟體（例如Internet Explorer，Adobe Acrobat，Microsoft Office）中的已知漏洞，以保護常用的應用程式和作業系統免受威脅。

**端點檢測與回應(EDR)**

端點偵測與回應(Endpoint Detection and Response，EDR)。一種新興技術。該術語定義了這類工具和解決方案，專注於檢測，調查和減輕主機和端點（如Symantec ATP或Blue Coat安全網頁閘道）的可疑活動和問題。


**零日(Zero-Day)攻擊**

所謂零時差攻擊(Zero-day Attack，又稱作零日攻擊)，指的是採用新發現、尚未被公開的電腦系統、應用軟體、外掛程式等弱點所進行的攻擊。由於該弱點尚未被揭露，所以也沒有任何修補或修正程式提供，因此零時差攻擊發生時，往往會造成比一般性漏洞更大的危害。.


**未知威脅**

威脅顯示為異常，它是可疑的，並且可能最近被看到，但是沒有已知的簽名或標識符。

# 企業組織希望能專注在核心事業

## 無庸置疑，端點防護扮演非常重要的角色

- 不要發生資料外洩
- 不要有過多的誤報警示造成業務中斷
- 扮演策略IT的重要決策，而不僅僅是突發狀況的通報者
- 不會造成IT人員的負擔，保持最高生產力
- 支援分散式作業環境以及不同多元的IT環境
- 符合法規遵循與政府法令
- 維持企業形象與聲譽以及顧客的信任度

# 複雜、不斷演變的威脅態勢

## 端點防護必須能夠偵測與攔阻端點攻擊鏈的每個環節並提供更深入的保護

**430M**

**全新惡意程式變種**

**2015年+36%**

**125%**

**零時差漏洞增加**

(2014-24)/(2015-54)

**35%**

**加密型勒索軟體**

**總數增加-2015年**

**55%**

**魚叉式網路釣**

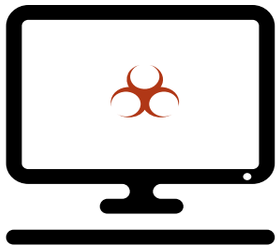
**魚活動增加-2015年**


**入埠流量** → **酬載(Payload)傳遞** → **酬載(Payload)執行** → **離埠流量**

資料來源: Symantec ISTR 2016

# 今天的端點安全比以前更加困難

## 不斷攀升的威脅態勢與不合適的端點防護造成重大業務中斷事件



**80%**

安全工作人員感覺管理端點安全比2年前更加困難。

***– ESG Endpoint Security Report***

**難上加難**

*31% 以應對新的惡意軟體為首要任務*

**損失生產力**

*38% 安全工作人員，花費許多時間在處理突發狀況*

**更高的成本**

*每起資料外洩事件的平均成本為400萬美元*

# Symantec Endpoint Protection

> 在整年度的所有網路間諜活動中，惡意軟體被利用率高達90%，不管是經由電子郵件、網頁順道下載、直接或遠端安裝，保護端點至關重要。

*Verizon 2016 資料外洩調查報告*


| 優異的防護 | 卓越的效能 | 妥善安排的<br>應變措施 |
|---|---|---|

# 2

# 產品概述/解決方案

# SEP 12.1 防護技術集

## 防火牆與入侵預防

- 在惡意程式擴散到電腦並控制流量前，加以攔截。

**攔截網路威脅**

## 防毒

- 在惡意程式感染系統之前，加以掃描並且根除。

**檔案**

## 信譽

- 運用社群的智慧，判斷檔案和網站的安全性。

**信譽分析**

## 行為

- 監控並攔截出現可疑行為的檔案。

**行為監控**

## 清除大師

- 積極矯正難以移除的感染情形。

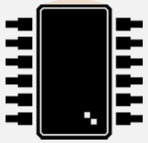
**修復**

**核心防護技術集**

## 應用程式控管

- 監控應用程式行為:自動化系統鎖定以及黑名單與白名單等等..

**精細的政策控制**



## 裝置控管

- 阻擋經由USB裝置的感染，協助預防資料外洩，SEP 14 新增支援 MAC 作業系統。

**USB 儲存裝置**

## 主機完整性

- 隔離與偵測未經授權的變更，進行損害評估，並確保遵循法規。

**保護以及法規遵循**

**依需求自行調整的安全政策**

# SEP 14 次世代防護技術集與現有防護技術優化

## 採用現有SEP 12.1防護技術優化+ SEP 14 新增全新技術

### 機器學習

- 處理程序處於預先執行階段，即能偵測得到能阻止大量已知與未知惡意程式。

業界最低誤攔率

### 應用程式保護

- 保護常被利用於記憶體攻擊型態的應用程式(Office、Acrobat、Internet Explorer、Java ..。

保護程式漏洞、錯誤

### 模擬器

- 反藏匿技術，可偵測隱藏的惡意程式。

強而有力的反藏匿技術

### 智慧型威脅雲端

- 即時雲端查詢，約可降低端點70%的病毒定義檔大小。

每日的更新下載量減少70%

### 效能強化

- 更快的即時病毒偵測/掃描。

更快速、更輕盈的代理程式

### 輕鬆整合

- 可程式化的REST APIs
- 可輕鬆整合 Blue Coat 網頁安全閘道以及Symantec ATP。

輕鬆整合

### 自動化應變

- 也能經由自動化更新機制-LiveUpdate 更新Windows 用戶端代理程式的安全性修正。

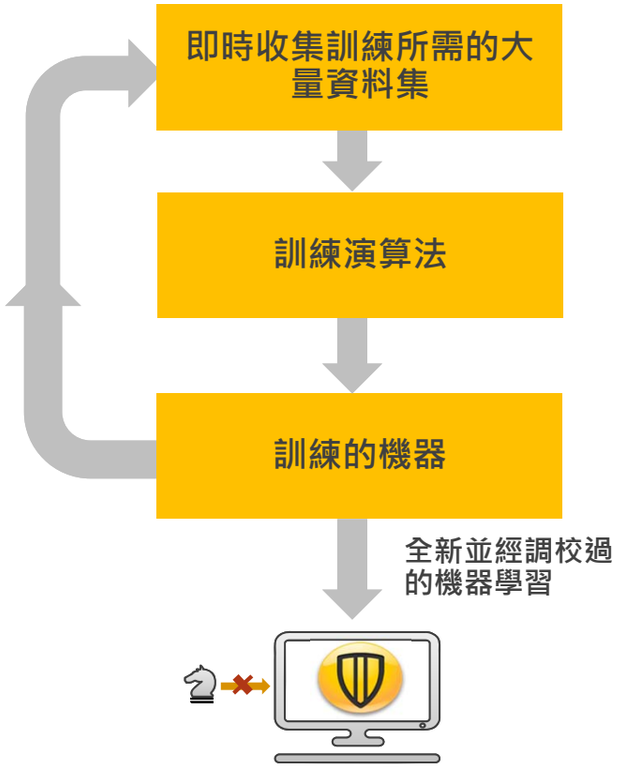
自動化運行

**優異的防護** | **卓越的效能** | **妥善安排的應變措施**

# 重要效益 #1: 優異的防護

## *惡意程序執行之前即能偵測: 進階機器學習*

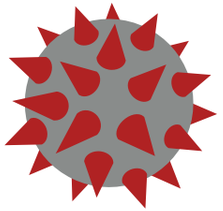
### 在端點電腦上運作的進階機器學習引擎




端點利用進階機器學習技術偵測

針對同一家族的零時差攻擊變種特別有效


可以利用**最低誤攔率**偵測大量類別的惡意程式



與病毒定義檔無關、無須密集更新

# 全球規模最大的民間威脅情報網路

## 最多樣性的大數據，進階的演算法，技術高超的威脅研究專家

**1億7千5百萬**
消費者以及企業端點
採用賽門鐵克解決方案

2015年 發現
**4億3,000萬**
全新獨特的惡意程式

**20億**
電子郵件每日掃描

**9** 威脅回應中心

**5,700萬**
攻擊偵測器
橫跨 **157** 國家

**12,000+**
雲端應用程式受保護

**1億8千2百萬**
去年攔截到的網路攻擊數量

**10億**
網頁請求每日分類

**全球規模最大的網路情報網 之一**
**3.7 兆筆安全相關資料**

# 重要效益 #1:優異的防護

## *惡意程序執行之前即能偵測: 記憶體攻擊緩解*

## 攔截零時差記憶體攻擊，阻止其攻擊常用軟體的弱點

### *沒有採用記憶體攻擊緩解:*

情況危急:
- Java 漏洞被公佈
- 尚無修補程式可用

已有修補程式:
- 使用者仍須安排時間安裝修補程式

**Day 0:** 漏洞被公佈 → **Day 1:** 漏洞已可被偵測 → **Day 2:** 岌岌可危，等待修補程式 → **Day 3:** 需使用者採取行動

利用此技術在攻擊者發攻擊之前，就阻止

### *有採用記憶體攻擊緩解:*

情況危機:
- 漏洞利用試圖停用 Java Security Manager
- Symantec 攔阻此漏洞利用



無論任何瑕疵、程式錯誤或漏洞，這項非病毒特徵型技術都能發揮效用。

# 重要效益 #1:優異的防護
## *惡意程式執行當下:模擬工具*
### 快速與精準偵測隱藏的惡意程式

**無 模擬**

惡意軟體同時被
多種包裝技術
藏匿起來

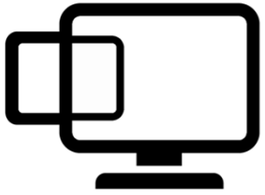

**被包裝, 無法確認**

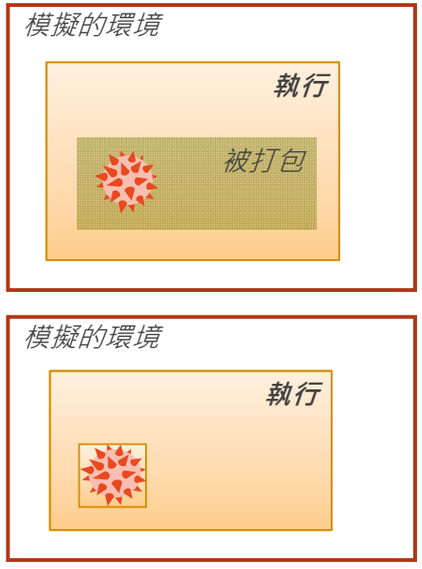
模擬檔案被執行就能偵測到自訂包裝(Pack)中隱藏的惡
意軟體。

---

**有 模擬**

模擬工具提供虛擬環境‘拆解’並執行被包裝的惡意軟體






**酬載(Payload)確認**

掃描程式會在輕量型虛擬機器上，以毫秒的速度掃描每個檔案，使威脅無所遁形，同時協助改善偵測率和效能。

# 重要效益 #2: 卓越的效能

## *未執行前即偵測:智慧型威脅雲端的快速掃描功能*

獲得專利的即時雲端查詢技巧，掃描所有可疑檔案

利用最新的即時雲端情報掃描可疑的檔案

採用專用進階技術，可提供更快15%掃描速度

開機速度更快

# 重要效益 # 3: 輕鬆整合與自動化

## *可程式化的API 與SEP 管理 (SEPM) 主控台溝通*

### 輕鬆與其它安全基礎架構整合

**SEMP :SEP 管理主控台**

用戶端管理

應用程式以及裝置控管

政策控制

報告與分析

**REST API's**

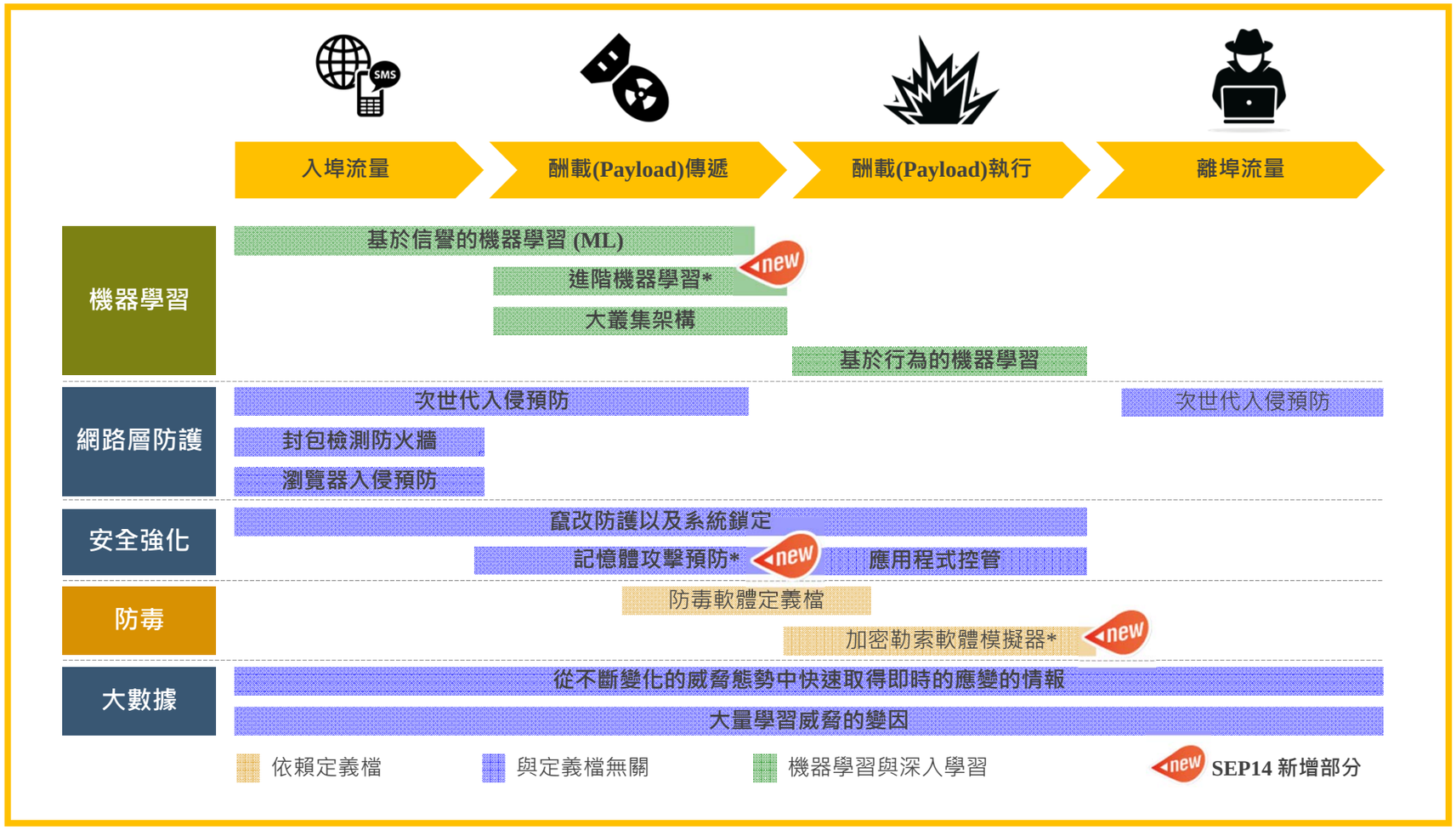
| SEP14 - API's |
| --- |
| 登入/登出 SEPM |
| 取得群組清單 |
| 擷取 SEPM 版本資訊 |

可由其它應用程式及腳本，協調/自動化 SEPM 採取適當的應變動作

連接到第三方平台以便與端點進行控制或與網絡平台整合

# 全方位的進階保護，延伸涵蓋至端點攻擊鏈的每個環節

## 避免單點失效，全軍覆沒



# Symantec Endpoint Protection 14

## 有效防護大規模增加的惡意軟體、針對性攻擊和新興威脅，同時不影響使用者及IT人員生產力。

### 優異的防護

賽門鐵克以全球最大民間威脅情報網路為後盾，採用多層次的核心及次世代防護技術，可跨越攻擊鏈的每個環節，提供極具效益的防護。

### 卓越的效能

經由統一的中央主控台以及可在單一代理程式中支援機器學習、記憶體攻擊預防、端點偵測和回應 (EDR)、防惡意程式與應用程式控制功能等所有端點防護技術，讓企業得以享有高效能又輕量化的解決方案。

### 妥善安排的應變措施

在端點上輕鬆整合現有的安全防護機制，以自動化的機制提供最高等級的防護，並採取妥善協調的應變措施。

# 為何有 370,000 企業，信賴 Symantec Endpoint Protection

## SYMANTEC ENDPOINT PROTECTION

- 整合全方位防護技術在一個輕量型代理程式，能夠完整防護**進階攻擊鏈**的每個環節
- 透過開放式的API，整合第三方產品的**自動化應變**工作流程，迅速阻止感染擴散
- **優化內容更新機制並降低掃描時間**
- 持續 **超越競爭對手** 在針對防護能力與效能影響的第三方公正單位評比
- 始終提供 **領先業界的產品，長期扮演產業領頭羊角色，** 也是端點防護的市佔率第一名
- 提供 **單一管理主控台，統一集中管理 Windows, Macs, Linux 以及虛擬機器**
- 提供精細的 **政策控管** 功能
- 支援 **Windows** 嵌入式作業系統

# 升級途徑:由 SEP 12.x 升級到 SEP 14


**最佳實務:經由SEP 14管理主控台，部署SEP 14 用戶端**

# 由 SEP 12 升級至SEP 14 有哪些效益?

- 單一代理程式涵蓋整個端點攻擊鏈所需的全方位防護技術，運用最新一代的機器學習技術、智慧型威脅雲端以及與全球安全情報網-從 157 個國家、1.75 億個端點及 5,700 萬個攻擊偵測器收集而來的資料做關連、比對與查詢，獲得最好的偵測與攔截以及業界最低的誤報率。
- 端點採用無須特徵更新而且誤報率極低的人工智慧進階機器學習技術為後盾，遏止目標式攻擊、進階威脅以及未知的威脅。
- 記憶體攻擊緩解措施可攔截常用軟體中的漏洞。
- 端點偵測和回應：新的可程式化 REST API 實現了與第三方產品整合的可能 (包括 Secure Web Gateway)，並可在端點上協調的應變動作，迅速阻止感染散佈。
- 安全性更新-獲得擴充的 LiveUpdate 功能，可支援自我安全修補程式(self-updating)。
- 卓越的效能 -輕量化代理程式以及智慧型威脅雲端的快速掃描功能，使用多項先進技術 (例如pipelining、信任推演與批次詢問)，因此不須將所有病毒特徵定義檔下載至端點，即可維持高水準的成效。因此，它只會下載最新的威脅資訊，使病毒特徵定義檔案的大小減少70%，連帶也能減少頻寬使用量。
- 更快的掃描速度:新一代技術充分利用獲得專利的即時雲端查詢技巧，可快速存取全球規模最大的民間威脅情報網路，提供比前一版本快15%的掃描速度。
- 降低IT 人員工作負擔:利用可程式化的API與SEP管理(SEPM)主控台溝通，並協調適當的應變動作，利用應用程式控管將新發現的惡意應用程式加入黑名單中。這些低誤報、自動化流程和政策，能進一步降低IT人員的負擔。

# Symantec Endpoint Protection 在端點防護領域始終維持領導者地位

## 新版一上市，來自第三方公正評比，佳評如潮


**通過 A/V Test4，在 18 個月間 100% 抵禦零時差攻擊**

SE Labs

**屢屢獲得 SE Labs 給予的 AAA 等級評價 (最高評分)。**

**SEP 14**

SC MAGAZINE

**Recommended Product**
"Verdict: **we love this product**."

Gartner
A Magic Quadrant Leader for Endpoint Protection Platforms

**過去 14 年在 Gartner 神奇象限中始終維持領導者評等**

black hat USA 2015

**Unhacked at 'Capture the Flag'**

MSExchange.org READERS' CHOICE WINNER 1

# SEP 14 :核心防護+新創科技+雲端大數據調校的精準機器學習

優異的防護力、卓越的效能以及妥善安排的應變措施

## 感謝聆聽

保安資訊有限公司-賽門鐵克解決方案專家

http://www.savetime.com.tw

We keep info. Safe,Secure & Save you Time,Cost