FORRESTER®

適用於安全及風險管理專業人員

Forrester Wave™：2016 年第四季端點安全性套件

最舉足輕重的 15 家供應商和優缺點比較

撰寫者：Chris Sherman

2016 年 10 月 19 日

閱讀本報告的理由

在我們的端點安全性套件供應商 25 項標準評估中，我們選出 15 家最重要的供應商，分別是 Bromium、Carbon Black、CrowdStrike、Cylance、ESET、IBM、Intel Security、Invincea、Kaspersky Lab、Landesk、Palo Alto Networks、SentinelOne、Sophos、Symantec 和 Trend Micro，並針對這些供應商進行了研究、分析和評分。本報告指出每家供應商的比較結果，以幫助安全性和風險管理專業人員選用適切的產品。

關鍵重點

Trend Micro、Sophos 和 Symantec 領先群倫

Forrester 的研究發現，Trend Micro、Sophos、Symantec、Kaspersky Lab、Intel Security 和 Carbon Black 是市場上的領導廠商。Cylance、Landesk、CrowdStrike、ESET、Palo Alto Networks、IBM、SentinelOne 和 Invincea 提供具競爭力的選項。Bromium 則落在最後。

安全性專業人員尋求威脅防範和偵測功能比重平衡的產品

端點安全性產品市場不斷擴大，是因為有越來越多的安全性專業人員將端點安全性套件廠商視為幫助他們解決最大挑戰的救星。此外，安全性專業人員也越來越信任這個技術領域的供應商，將其視為策略合作夥伴，能為他們提供端點安全性最重要決策的相關建議。

威脅分析和自動遏制功能是關鍵差異點

隨著傳統端點安全性方法已過時且成效不佳，更優越的威脅偵測準確性和自動遏制力將決定哪家供應商能領先群倫。

Forrester Wave™：2016 年第四季端點安全性套件

最舉足輕重的 15 家供應商和優缺點比較

撰寫者：Chris Sherman
以及 Christopher McClean、Salvatore Schiano 和 Peggy Dostie
2016 年 10 月 19 日

目錄

重要事項與資源

在本評估中，Forrester 只評估截至 2016 年 7 月 15 日為止普遍可購得的產品。我們專訪了 15 家廠商和 45 家以上使用他們產品的公司客戶。受訪廠商包括 Bromium、Carbon Black、CrowdStrike、Cylance、ESET、IBM、Intel Security、Invincea、Kaspersky Lab、Landesk、Palo Alto Networks、SentinelOne、Sophos、Symantec 和 Trend Micro。

相關研究文件

《2016 年端點安全性產品採用現況》(The 2016 State Of Endpoint Security Adoption)

《調查簡報：端點安全性技術創新持續強化》(Brief: Endpoint Security Innovation Is Intensifying)

《TechRadar™：2016 年第一季行動安全性》(TechRadar™ : Mobile Security, Q1 2016)

FORRESTER®

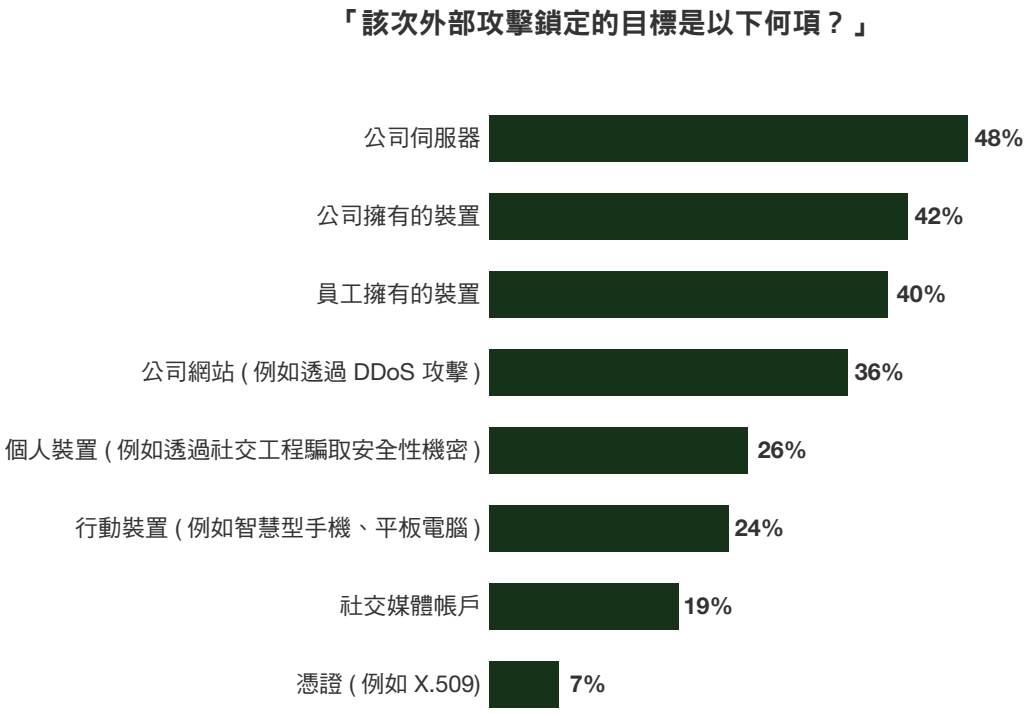
Forrester Research, Inc., 60 Acorn Park Drive, Cambridge, MA 02140 USA
+1 617-613-6000 | 傳真：+1 617-613-5000 | forrester.com

選用適切的端點安全性解決方案，否則將可能面臨安全風險

端點安全性是您防範網路攻擊的第一道防線。系統遭入侵已成為企業經常遇到的頭痛問題，而員工端點和伺服器是最常成為攻擊目標的資產類型 (詳見圖 1)。這類安全性缺口可能產生損害嚴重的影響，導致企業損失營收、失去在市場上的商譽和競爭力。[1] 更雪上加霜的是，端點安全性不足會導致門戶大開，容易遭受透過不同伎倆和工具所發動的攻擊，包括散佈惡意程式、惡意探索軟體，以及透過社交媒體騙取安全性機密。所以，設置適切的端點保護在目前更是絕對必要。

安全性預算在過去幾年來已大幅增加，而且端點安全性預算在 2016 年平均佔 IT 安全性總預算的 10%。[2] 但儘管有預算能投資新技術，安全性專業人員依然不確定該如何找到適切的工具，以保護因員工裝置而不斷擴大的易受攻擊面。

圖 1 公司內部端點是最容易成為攻擊目標的資產群組



調查對象：其公司 (員工人數 1,000 人以上) 在過去 12 個月內曾遭受一次外部安全入侵的 192 位網路安全性決策者
資料來源：《Forrester 2016 年 Global Business Technographics® 安全性調查》(Forrester's Global Business Technographics® Security Survey, 2016)

端點安全性產品買家正面臨嚴重分化的市場

隨著新惡意程式變型和混淆系統的方法數目增加，防毒技術在保護員工端點和伺服器上的效果已不大如前。因此，有眾多競爭技術廠商興起，目標鎖定在接管停滯的防毒技術市場。但是，許多傳統防毒技術廠商面對這波攻勢也主動出擊，而不是毫無還擊。其中一些廠商為了順應新趨勢，已建置或收購新技術，這些技術均不仰賴舊式依照封鎖清單的防惡意程式保護模式。有些廠商則擴增他們的防惡意程式引擎，增加了多種分析功能，不只是靜態列出封鎖清單而已。上述情況導致了市場嚴重分化，有許多不同的端點安全性方法，每種方法都各有利弊。

端點安全性套件必須能滿足核心買家的需求

要一眼洞悉市場混淆情況，可以將廠商技術功能分成三大核心需求類別：攻擊防範、偵測和修復 (詳見圖 2)。單點產品一般只能滿足上述一種需求，而端點安全性套件則能滿足上述兩種或全部三種需求，因為端點安全性套件能針對每種需求提供不同程度的自動原則強制執行。所以，在購買新產品之前，請先考量廠商滿足上述每種需求的技術能力，具體來說就是以下方面技術能力的優越性：

- **預防惡意程式和惡意探索執行。**在功能上，端點安全性套件應能建立一種作業環境，讓惡意程式無法載入記憶體，或惡意探索無法利用執行中的流程。也應能透過系統強化和應用程式控制等措施，縮小易受攻擊面，以此防範威脅。
- **偵測攻擊執行後的惡意活動。**有鑑於攻擊者終將突破控制防線，最新端點安全性套件也會監控執行中的記憶體，以便在惡意程式和惡意探索得逞之前先發現。有些解決方案只著重監控流程行為，但大多數先進的解決方案也會分析使用者行為，以確立情境，全面監控。
- **修復並遏制惡意活動和潛在漏洞。**一旦最新端點安全性套件發現端點上有惡意活動或潛在漏洞之後，應能夠不需要管理員太多介入，就立即啟動自動化修復程序。修復功能包括可執行檔 / 檔案隔離、設定回復，以及目標式流程 / 使用者行為封鎖等。漏洞修復技術 (例如修補程式部署) 也包含在內；這類技術通常會擴增防範措施。

圖 2 最新端點安全性套件具備比重平衡的威脅防範、偵測和修復功能

端點安全性評估概觀

為了評定端點安全性套件市場的現況，並了解廠商彼此相較的技術能力水平，Forrester 評估了端點安全性套件頂尖廠商的技術優缺點。在檢閱過往的研究、使用者需求評估以及廠商和專家訪談後，我們開發出一套完整的評估標準。我們根據 25 項標準對廠商進行評估，並將這些標準分成三個主要類別：

- **目前供應項目。**針對每個端點安全性解決方案，我們評估了以下項目：1) 防範功能，包括惡意程式執行防範、系統強化和應用程式控制；2) 偵測功能，包括攻擊偵測和威脅情資智慧；3) 修復功能，包括攻擊後修復和漏洞修復；4) 其他安全功能，包括端點安全性輔助功能和行動安全性；5) 架構，包括一般架構、作業系統支援、自動化和協調統合，以及擴充性和彈性；以及 6) 客戶意見，包括客戶對於產品對端點使用者經驗的影響、防範效果、偵測效果和廠商支援品質的回饋意見。
- **策略。**我們評估了廠商的以下項目：1) 成本和授權模式；2) 產品發展藍圖和 3) 上市策略，包括管道與合作夥伴佔有率。
- **市佔率。**我們評估了廠商的以下項目：1) 企業客戶佔有率和 2) 授權合作夥伴計畫。

受評估廠商和納入標準

Forrester 在此評估中納入了 15 家廠商：Bromium、Carbon Black、CrowdStrike、Cylance、ESET、IBM、Intel Security、Invincea、Kaspersky Lab、Landesk、Palo Alto Networks、SentinelOne、Sophos、Symantec 和 Trend Micro。其中每家廠商均有 (詳見圖 3)：

- **一套端點安全性套件，能防範、偵測端點威脅，並進行修復。**我們將只提供上述其中一項功能的解決方案視為單點產品，而非套件。
- **企業市場地位。**我們只納入符合下列其中一項標準的廠商：管理至少 100 個企業客戶帳戶或至少 150 萬個使用者機座。
- **企業買家表達高度興趣。**我們只納入 Forrester 客戶對其產品有高度興趣的廠商。客戶應在 Forrester 向其詢問以及互動時，在沒有提示的情況下主動提及廠商名稱 (「我們曾考量以下廠商的端點安全性產品」)。

圖 3 受評估廠商：產品資訊和選擇標準

廠商	受評估產品
Bromium	Bromium Endpoint Protection
Carbon Black	Cb Response & Cb Protection
CrowdStrike	Falcon Host
Cylance	CylancePROTECT
ESET	ESET Endpoint Security
IBM	IBM BigFix & MaaS360
Intel Security	McAfee Complete Endpoint Protection Enterprise
Invincea	X by Invincea
Kaspersky Lab	Kaspersky Endpoint Security for Business
Landesk	Landesk Security Suite
Palo Alto Networks	Palo Alto Networks Traps
SentinelOne	SentinelOne Endpoint Protection Platform
Sophos	Sophos Endpoint Protection
Symantec	Symantec Endpoint Protection
Trend Micro	Trend Micro Smart Protection Suite

納入標準

廠商必須在 2016 年 7 月 15 日當天或之前有：

一套端點安全性套件，能防範、偵測端點威脅，並進行修復。我們將只提供上述其中一項功能的解決方案視為單點產品，而非套件。

企業市場地位。我們只納入符合下列其中一項標準的廠商：管理至少 100 個企業客戶帳戶或至少 150 萬個使用者機座。

企業買家表達高度興趣。我們只納入 Forrester 客戶對其產品有高度興趣的廠商。客戶應在 Forrester 向其詢問以及互動時，在沒有提示的情況下主動提及廠商名稱 (「我們曾考量以下廠商的端點安全性產品」)。

未符合標準的相關廠商

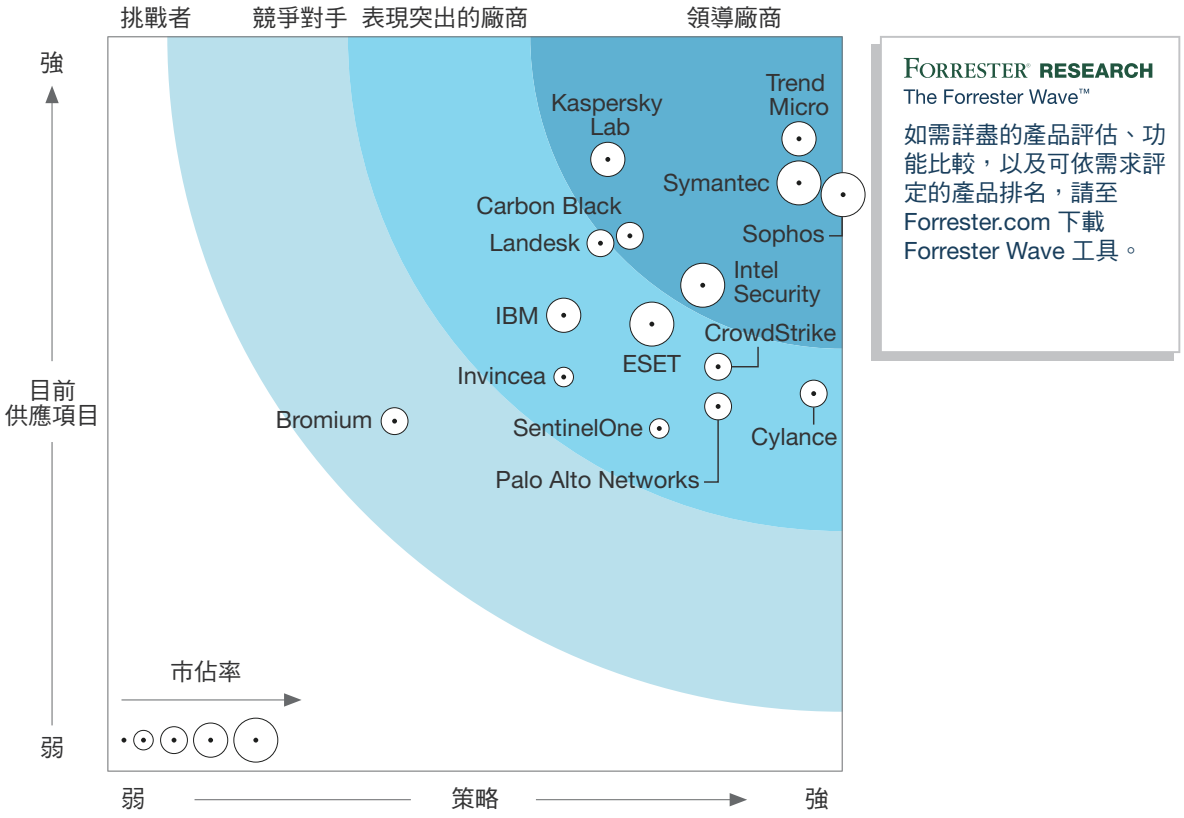
有許多端點安全性產品廠商未被我們納入本評估，但在合適的情況下，這些廠商中的每一家都有值得考量的技術功能：

- **Microsoft 目前提供原生端點安全功能。**有鑑於 Windows 10 安全性的先進功能，許多組織在規劃改用其他技術時，也正評估這項產品是不是可行的端點安全性產品選項。由於這項評估流程與典型端點安全性套件的評估流程極為不同，所以 Forrester 計畫在 2017 年晚期另外發表一項專門針對 Microsoft Windows 10 端點安全功能的研究報告。
- **有些端點安全性產品供應商的鎖定對象為消費者和小型企業。**這類供應商包括 AVG Technologies、Malwarebytes 和許多其他供應商。由於本評估是針對企業市場，所以我們未納入任何這類供應商。
- **其他鎖定企業的廠商則未符合標準。**提供端點安全性產品給企業的其他知名廠商包括 Bitdefender、Check Point Software、Cisco Systems、Cybereason、Digital Guardian 和 Webroot。這些供應商未符合至少一項的評估對象納入標準。

廠商背景資料

本端點安全性套件評估的目的只是提供一個起點。我們建議讀者參閱詳細的產品評估報告，並利用 Forrester Wave 的 Excel 廠商比較工具調整加權比重，以符合各自需求 (詳見圖 4)。

圖 4 Forrester Wave™：2016 年第四季端點安全性套件



FORRESTER® **RESEARCH**
The Forrester Wave™

如需詳盡的產品評估、功能比較，以及可依需求評定的產品排名，請至 Forrester.com 下載 Forrester Wave 工具。

圖 4 Forrester Wave™：2016 年第四季端點安全性套件 (續)

	Forrester 加權比重	Bromium	Carbon Black	CrowdStrike	Cylance	ESET	IBM	Intel Security	Invincea	Kaspersky Lab	Landesk	Palo Alto Networks	SentinelOne	Sophos	Symantec	Trend Micro
目前供應項目	50%	2.38	3.64	2.75	2.54	3.04	3.10	3.29	2.68	4.16	3.59	2.48	2.33	3.92	4.00	4.30
防範功能	17%	1.88	4.52	2.04	3.44	2.32	2.00	3.88	3.52	4.12	3.24	2.60	1.36	3.76	3.16	3.76
偵測功能	16%	3.60	5.00	5.00	3.20	3.40	3.00	3.60	4.60	4.00	3.00	4.40	4.60	3.40	4.40	5.00
修復功能	20%	1.50	3.50	2.50	2.00	2.50	4.00	2.50	1.50	4.50	4.50	2.00	2.00	3.50	4.50	4.00
其他安全功能	20%	1.75	1.50	0.00	0.00	2.75	3.25	3.00	0.00	4.75	4.00	1.00	0.00	5.00	5.00	4.25
架構	15%	3.55	4.00	4.05	3.65	3.95	3.10	3.95	3.40	3.60	2.85	2.00	3.55	4.50	3.30	4.70
客戶回饋意見	12%	2.50	3.90	4.10	4.10	3.80	3.00	3.00	4.50	3.60	3.60	3.60	3.60	3.00	3.00	4.20
策略	50%	1.95	3.55	4.15	4.80	3.70	3.10	4.05	3.10	3.40	3.35	4.15	3.75	5.00	4.70	4.70
成本和授權模式	15%	3.00	1.00	5.00	5.00	5.00	1.00	3.00	5.00	3.00	1.00	5.00	5.00	5.00	3.00	3.00
產品發展藍圖	65%	2.00	4.00	4.00	5.00	3.00	3.00	4.00	3.00	3.00	4.00	4.00	4.00	5.00	5.00	5.00
上市策略	20%	1.00	4.00	4.00	4.00	5.00	5.00	5.00	2.00	5.00	3.00	4.00	2.00	5.00	5.00	5.00
市佔率	0%	2.25	2.75	2.25	2.25	4.25	3.50	5.00	1.75	3.75	3.00	2.25	1.50	4.50	5.00	4.00
企業客戶佔有率	75%	2.00	2.00	2.00	2.00	4.00	3.00	5.00	2.00	4.00	3.00	2.00	1.00	5.00	5.00	5.00
授權合作夥伴	25%	3.00	5.00	3.00	3.00	5.00	5.00	5.00	1.00	3.00	3.00	3.00	3.00	3.00	5.00	1.00

所有分數均以 0 (弱) 到 5 (強) 的評量尺為計分基礎。

領導廠商

› **Trend Micro 提供市場上技術功能屬一屬二的產品。**Trend Micro 提供一套功能完整且有彈性的端點安全性套件，能內部部署或透過受管理軟體即服務供應項目，部署在類型廣泛的企業環境內。該公司目前的供應項目提供比重平衡性極佳的防範和偵測功能，但缺點在於缺少修補程式部署功能，以及以偵測為主的功能是透過另一項產品 (Endpoint Sensor) 提供。

Trend Micro 的客戶給予該公司這項產品在威脅防範保護效果上的評分，是本項 Forrester Wave 評估中所有套件所獲最高的同項評分之一，而且這項產品對端點使用者經驗的負面影響也低於平均程度。整體而言，Trend Micro 目前的產品組合以及短期和長期發展藍圖，均非常符合企業買家目前和未來 (可能會有) 的需求。

› **Sophos 提供最方便企業使用的軟體即服務端點安全性套件。**Sophos 提供一套緊密整合端點安全功能的套件，而且先進的威脅防範、偵測和自動化修復功能比重平衡性良好。買家會喜歡此套件的直覺式管理介面，以及多數企業部署均需要的彈性和擴充性，無論規模大小為何。Sophos 也是本項 Forrester Wave 評估中少數其中一家端點安全性套件廠商，能提供功能完整、可選擇內部部署或透過軟體即服務型的服務部署的套件。但是，這套解決方案缺少提供給員工裝置的修補程式管理，以及彈性的應用程式預設 - 拒絕允許清單選項，這對某些企業買家而言可能會是一個問題。

整體而言，客戶對於這項產品的效果，以及對端點使用者經驗最小程度的負面影響，均表示高度滿意。在新舊端點安全性技術多不勝舉的領域中，Sophos 的發展藍圖著重開發強大且無需簽名的防範和偵測功能 (包括新的 Intercept X 產品，在本項 Forrester Wave 評估規定的產品推出截止日期之後、在本報告發佈之前已推出)，這應會讓這項產品具有長期競爭力。

› **Symantec 提供市場上功能最完整的端點安全性套件。**Symantec 深厚的端點安全性技術涵蓋種類廣泛的防範、偵測和修復功能。買家只要利用這套產品組合的完整功能範圍，就幾乎涵蓋了每個可能的易受攻擊面。但是，客戶需要購買多種產品才能獲得所有這些功能，而且其中一些關鍵元件缺少整合。因此，客戶對於管理員使用者經驗，以及對端點效能的中度負面影響，均表示低度滿意。但隨著該公司轉而採取無需簽名的防範技術策略 (預定將在這項產品的短期發展藍圖上實行，將從即將推出的 Symantec Endpoint Protection 14 更新版開始實行)，這表示對這項產品前幾代版本的倚賴將減少，所以客戶的滿意度可能會改變。

隨著該公司持續開發先進的入侵後偵測技術，以及與最近所收購 Blue Coat Systems 的技術整合，應能在未來 6 到 12 個月內改善功能效果，並推出一項更有競爭力的產品項目。

› **Kaspersky Lab 以一套緊密整合的套件滿足最多的企業需求。**Kaspersky Lab 擁有市場上功能最完整的端點安全性解決方案之一，具備強大的防範、偵測和修復功能。該公司是內部自行開發其中每種功能，所以不同元件間的整合功能強大且有其用意。

企業如果希望獲得深入的威脅探查功能，應考量其他供應商的產品，不過該公司在短期發展藍圖上已規劃透過 KATA 2.0 (預定在 2017 年第一季推出)，往這個領域擴展。整體而言，客戶對於該公司產品的惡意程式和惡意探究防範功能，以及可靠的執行後偵測功能，均給予高成效的評價。

› **Intel Security 的擴充性技術讓該公司的產品特別適合極大型企業。**Intel Security 提供目前市場上功能最強大的管理平台之一：McAfee ePolicy Orchestrator (ePO)。這項產品是該公司所有安全性產品的底層管理工具，提供企業買家需要的強大技術和彈性。安全功能廣泛，是透過一個通用原則引擎緊密整合，而且資料情報串流涵蓋多種防範、偵測和修復功能。不過這也導致一項缺點，許多客戶表示，使用者介面過於複雜，很難操作。

這項產品的多項效果評分都相當不錯，但買家應留意，客戶表示這項產品對較舊型機器上的使用者經驗產生高於平均程度的負面影響。此外，也有一些顯著的功能差距，最明顯的是缺少修補程式管理和行動安全功能。但是，假設該公司達成其目前短期和長期發展藍圖的目標 (例如提供先進的依行為偵測和遏制措施)，這套解決方案應會重獲其競爭優勢，並將是持續多年的主力產品。

› **Carbon Black 持續以先進的偵測技術，讓產品的功能不僅限於應用程式控制。**Carbon Black 提供比重平衡性極佳的防範、偵測和修復功能，而且不需倚賴簽名確認的封鎖清單。這主要是因為該公司之前還是 Bit9 時，以其同級最佳、依據攻擊後鑑識調查的允許清單技術聞名已久。雖然應用程式控制技術持續是該公司的核心供應項目之一，但該公司在 2014 年收購 Carbon Black 之後，也提供功能強大的偵測和因應功能。隨著該公司於 2016 年最新收購 Confer，該公司展現出決心，要發展出上述功能與防範和偵測功能的比重更加平衡的產品組合。

客戶對這項產品的評價為防範功能優越，且偵測效果極佳，但缺點是對使用者經驗的負面影響高於平均程度。Forrester 預期，隨著 Confer 代理程式和 Carbon Black 技術之間的整合開始展現成效，以及這項產品對預設 - 拒絕模式的倚賴減少，使用者經驗應會改善。

表現突出的廠商

› **Cylance 提供無需使用簽名的強大惡意程式防範功能。**Cylance 是另一家過去幾年來廣獲青睞且高度成長的新秀廠商。該公司提供目前市場上少數的端點安全性單點產品之一，展現出不需網際網路連線或頻頻更新封鎖清單 / 允許清單的強大惡意程式執行防範功能。這項產品能達到如此的效能，是透過情報人工智慧引擎，掃描在端點上啟動的每個可執行檔，以預測其行為。

整體而言，這項產品贏得客戶的高度滿意，而且對員工端點操作經驗的負面影響程度小。雖然目前提供的這項產品缺少在競爭產品中可看到的一些執行後偵測元件，但該公司已規劃在 2016 年晚期推出的發行版本中，擴充這項產品的偵測功能。買家也應留意，Cylance Protect 可能需要買家額外投資購買端點安全性 / 管理輔助技術，才能彌補其不足之處。

› **Landesk 的目標是成為端點安全性技術領域的下一個主要供應商。**許多安全性產品買家將 Landesk 視為以系統管理技術為主的公司，但過去幾年來，這一點顯然已經改變。透過收購和內部開發雙管齊下，Landesk 目前提供多種強大的安全性技術，讓該公司躋身於端點安全性套件頂尖供應商之列。這些技術包括完整的應用程式控制功能 (透過收購 AppSense)、同級最佳的修補程式管理技術 (透過收購 Shavlik)、可靠的行動安全功能 (透過收購 LetMobile)，以及內部開發的端點偵測功能。雖然這些不同元件尚未完全整合，但技術整合已列入該公司的短期發展藍圖上。

客戶對於 Landesk 的防範和偵測功能表示高度滿意，但也指出其產品對端點使用者經驗產生中度的負面影響。隨著該公司持續整合不同的安全功能，使用者經驗應會改善。

› **CrowdStrike 正努力發展端點防範惡意程式套件的取代技術。**CrowdStrike 自 2012 年推出其第一套發行版本以來，已有極大發展，擴大建置了多項不需倚賴管理員介入或監督的防範功能和自動化修復功能。雖然這項產品最初著重在擴增企業既有端點安全性產品的功能上，但目前也可以在特定環境內用於取代惡意程式防範工具。但是，這項產品的重點依然是在攻擊偵測；Falcon Host 的雲端架構和「威脅圖形顯示」(Threat Graph) 讓管理員能輕鬆看出其公司內端點活動的關聯性，並比較全域的運作狀況。

買家對於 CrowdStrike 的防範技術能力，以及特別是偵測其環境所面臨威脅的技術能力，表示高度滿意，而且其產品對端點使用者經驗產生的負面影響程度極小。雖然這項產品還不是功能完整的套件，但該公司的 2017 年發展藍圖著重在擴大建置企業級功能上，包括加密、裝置控制和使用者行為分析 (UBA) 等模組，這些將讓這項產品更能與端點安全性套件領先廠商的產品競爭。

› **ESET 以一套輕量型套裝軟體提供強大的防惡意程式保護。**ESET 向來著重在消費者和中小企業市場上，但過去幾年來，已推出更多讓其端點安全性套件具備彈性和技術廣度的功能，而彈性和技術廣度正是企業買家通常尋求的優點。這包括比重平衡性穩固的端點防範和自動化修復功能，並有多種端點安全性輔助技術支援，例如端點加密、媒體控制和行動安全性。

ESET 的產品在防範效果方面獲得極高評分，而且對端點使用者經驗產生的負面影響程度極小。但是，缺乏彈性的應用程式控制和漏洞修復功能，可能讓某些企業買家卻步，所以如果該公司希望這項產品維持競爭力，需要在這項產品的未來迭代版本中解決此問題。

› **Palo Alto Networks 提供強大的惡意程式防範和惡意探索封鎖功能。**Palo Alto Networks 的 Traps 產品透過其雲端式惡意程式執行前的分析引擎 WildFire，提供攻擊防範功能，並透過其 Traps 核心引擎提供惡意探索執行後的封鎖功能。但買家應留意，不明惡意程式封鎖功能需要透過網際網路連上 WildFire 的伺服器才能執行；如果因為無法上網而無法立即取得 WildFire 的判定，管理員可以設定原則將不明可執行檔封鎖，但這可能會對端點使用者經驗產生負面影響，而且只有高風險或靜態端點才可能接受這樣的影響。

使用者表示，執行這項產品的全面保護模式時 (執行雲端分析和行為封鎖功能)，會對端點使用者經驗產生高於平均程度的負面影響。但是，這項產品的最新版本 (Traps v3.4，本項 Forrester Wave 未評估，但此版本在本報告發佈前推出) 會透過對端點的靜態分析解決這個問題。整體而言，這項產品雖然缺少端點能見度和控制這項專門功能，但其防範和偵測功能均獲得高評分。

› **對於已設置威脅偵測技術的企業而言，IBM 的產品是可靠的選擇。**IBM 的端點安全性產品組合涵蓋端點管理和漏洞修復功能 (透過 BigFix 的技術)、簽名確認的惡意程式防範功能 (透過 Trend Micro 的技術授權)，以及透過其 Apex 技術的無需簽名應用程式完整性保護功能。客戶給予這項產品的惡意程式防範效果極高的評分，並表示這項產品對使用者經驗的負面影響程度相當小。

企業買家會喜歡 Apex 和 BigFix 技術整合的優點；但該公司依然仰賴與 Carbon Black 的產品整合，才能提供威脅偵測功能。這雖然是 IBM 端點安全性產品組合的一大缺點，但有鑑於 IBM X-Force 事業部的威脅研究專業能力，以及 IBM 在巨量資料分析上的專業能力，IBM 應能將這項缺點化為一大轉機。整體而言，IBM 目前的客戶以及已經有 Carbon Black (或另一項端點偵測技術) 的客戶，會從 IBM 的端點安全性產品組合獲得最大效益。

› **SentinelOne 著重在入侵開始產生影響時立即予以遏止。**SentinelOne 的公司規模和年資雖然屬中等，但仍受到高度矚目。這是因為其核心產品使用的是行為偵測方法，而非倚賴簽名 (雖然還是可以在威脅執行前強制執行基本封鎖清單功能，以遏止不明威脅)，因此對端點使用者經驗的負面影響程度小。但是，相較於本評估中著重防範的其他解決方案，SentinelOne 的執行前防範功能和易受攻擊面縮小技術均屬中等；該公司真正鎖定的目標是在惡意程式或惡意探索開始侵入記憶體之前，封鎖惡意活動。因此，這項產品的偵測效果獲得高評分，但防範效果只獲得中等評分。

雖然該公司已為這項產品規劃許多增強功能，讓這項產品能與功能完整的端點安全性套件 (尤其是端點上無需簽名的惡意程式執行防範功能) 齊頭競爭，但買家應留意，SentinelOne 的這項產品可能需要買家額外投資購買端點安全性 / 管理輔助技術，才能彌補其技術的不足之處。

› **Invincea 並非只是另一個著重沙箱功能的安全性單點產品。**Invincea 是唯一一家提供分段保護措施的受評估廠商，這些措施包括無需簽名的保護、應用程式遏制和依行為的偵測。依照應用程式的風險等級，某些應用程式可以在使用者模式的沙箱內執行，沙箱會提供保護，阻止惡意探索和惡意程式逃脫，而且由於結合列出封鎖清單的惡意程式防範和先進的保護措施，所以保護範圍涵蓋更廣泛的端點環境。不過也因此會對使用者經驗產生負面影響，影響程度差異極大，端賴客戶的設定和環境而定 (例如是否啟用應用程式沙箱功能)。

雖然 Invincea 缺少許多企業套件買家需要的端點安全性輔助技術，但這項產品的整體效果仍獲得高評分。雖然 Invincea 有強大的防範和偵測功能，但較適合已設置安全性技術 (資料安全性、媒體控制、設定管理) 的企業，以及作業環境屬於高風險，需要更多威脅防範功能的企業。

競爭對手

› **Bromium 雖然走在時代先端，但著重在威脅防範。**Bromium 用硬體虛擬化技術，防範惡意程式和惡意探索入侵端點。這項技術會在虛擬機內執行檔案和可執行檔，並在邏輯邊界上強制執行依行為的控制，以侷限惡意探索可能對端點產生的影響。Bromium 提供不需使用簽名或應用程式允許清單的高度保護。

但是，買家應留意，如果端點上的 RAM 或 CPU 未達最低處理能力要求，這項產品可能對端點上的使用者經驗產生負面影響。整體而言 如果組織的硬體已有技術支援 不需要功能完整的端點安全性套件，Bromium 會是可靠的選擇。

聘請分析師

與 Forrester 的思維領導者共同合作，將我們的研究結果套用到您獨特的業務和技術計畫中，將讓您對自己的決策更有信心。

詢問分析師

為了幫助您將研究結果應用在實務上，請聯繫分析師，在 30 分鐘電話會議中討論您的問題，或選擇透過電子郵件回覆。

深入了解。

諮詢分析師建議

歡迎聘請分析師透過依需求設計的策略諮商會、研習會或演講，協助您將研究結果化為行動。

深入了解。

線上研討會

歡迎加入我們的線上研討會，了解對您的業務有影響的最新研究。每次連線均包含分析師回答問題時段和簡報投影片，而且可隨選連線。

深入了解。

Forrester 的 iPhone® 和 iPad® 研究應用程式
讓您無論身在何處，都能比競爭對手更快洞察先機。

補充資訊

線上資源

圖 4 的線上版本是 Excel 架構的廠商比較工具，能提供詳盡的產品評估和依需求評定的排名。

調查方法

Forrester 2016 年 Global Business Technographics® 安全性調查是在 2016 年 3 月至 5 月期間實地進行。這項線上調查包括 3,588 位受訪者，分別來自澳洲、巴西、加拿大、中國、法國、德國、印度、紐西蘭、英國和美國，均隸屬員工人數在兩人以上的企業。

Forrester 的 Business Technographics 會確保最終調查對象只包含在業務以及技術產品和服務的規劃、預算編列和採購上參與程度高的人員。

本 Forrester Wave 中所用的資料來源

Forrester 使用三種資料來源的組合來評估每種解決方案的優缺點。我們在評估參與本項 Forrester Wave 的廠商時，部分使用他們在 2016 年 9 月 20 日前提供給我們的資料。

- **廠商調查。**Forrester 根據與評估標準的關係來調查廠商的功能。一旦分析過完成的廠商調查後，我們就視需要拜訪廠商，以收集關於廠商資格的詳細資料。
- **產品示範。**我們請廠商進行各自產品的功能示範。並使用這些產品示範的結果來驗證每家廠商產品功能的詳細資料。
- **電訪客戶取得參考資訊。**為了驗證產品與廠商的資格，Forrester 向每家廠商現有的三家客戶進行電訪，以取得參考資訊。

Forrester Wave 研究方法

我們先進行主要的研究，在此市場中找出符合我們標準的廠商並據此擬出一份廠商清單。從這份初始廠商名單開始，再進一步縮減為最後的清單。廠商是根據以下條件選出：1) 產品的適用性；2) 客戶的成功應用；以及 3) Forrester 客戶的需求。我們會將不具有足夠的客戶推薦或不符合本項評估範疇的廠商加以排除。

在檢閱過往的研究、使用者需求評估以及廠商和專家訪談後，我們開發出初始評估標準。為了依照我們的標準集來評估廠商及其產品，我們透過實驗室評估、問卷、示範和 / 或與客戶推薦討論的組合，收集關於產品資格的詳細資料。我們將評估傳送給廠商檢閱，然後再調整評估，以針對廠商的產品及策略提供最正確的看法。

我們設定了預設加權比重，以反映我們對大型使用者公司需求的分析和 / 或 Forrester Wave 評估中列出的其他案例，然後根據清楚定義的尺度為廠商評分。我們預設這些加權比重的目的僅是為了提供起點，並建議讀者透過 Excel 工具調整加權比重，以符合各自需求。最後的分數會根據目前的產品、策略及市佔率產生市場的圖形描述。Forrester 打算跟著產品功能和廠商策略的進展，定期更新廠商評估。如需關於各項 Forrester Wave 評估所依循方法的詳細資訊，請參閱 http://www.forrester.com/marketing/policies/forrester-wave-methodology.html。

誠信政策

我們所有研究 (包括 Forrester Wave 評估) 的進行方式均依照我們的誠信政策。如需詳細資訊，請參閱 http://www.forrester.com/marketing/policies/integrity-policy.html。

尾註

[1] 網路犯罪份子正使用更精密的鎖定目標式攻擊，以竊取無所不包的資訊，包括寶貴的智慧財產以及您的客戶、合作夥伴和員工的敏感個人資訊。他們的動機從謀財到報復皆有。只要有足夠的時間和財力，他們就能突破甚至是最大型企業的安全防線。您不可能一一阻止每項網路攻擊。但是，您的客戶確實期望您快速適切因應。因為遏制入侵的能力差，加上拙劣的因應，可能導致動輒數百萬美元的業務和商機損失，並毀掉您公司的商譽。如需詳細資訊，請參閱《做好防患未然規劃：如何在遭入侵後持續營運》(Planning for Failure: How To Survive A Breach) Forrester 報告。

[2] 已請安全性技術決策者將他們的預算劃分給 10 個安全性技術層面。客戶威脅管理平均佔支出的 10%。資料來源：《Forrester 2016 年 Global Business Technographics 安全性調查》(Forrester's Global Business Technographics Security Survey, 2016)。

每年 Forrester 均調查數千位來自全球多個產業和不同規模組織的安全性技術決策者和資訊人員。本報告提出從這些調查中所整理出與端點安全性最相關的資料，而且特別著重在影響中小企業和大型企業的趨勢。當您在檢討您的 2016 年安全性技術預算時，請用本報告，幫助比較您公司和同業的支出模式與優先順序，同時留意整個安全性技術環境中影響端點安全性技術的目前趨勢。要深入了解，請參閱《2016 年端點安全性技術採用現況》(The 2016 State Of Endpoint Security Adoption) Forrester 報告。

FORRESTER®
CHALLENGE THINKING. LEAD CHANGE.

我們與業務和技術領導者共同合作，以發展出心繫客戶且帶動成長的策略。

產品和服務

- 核心研究和工具
- 資料和分析
- 同業合作
- 分析師聘請
- 諮詢
- 事件

Forrester 的研究和見解是專門針對您的職位和關鍵業務計畫而量身打造。

我們服務的對象

行銷和策略專業人員
行銷長
企業對企業 (B2B) 行銷
企業對消費者 (B2C) 行銷
客戶體驗
客戶洞察
電子商務和管道策略

技術管理專業人員
資訊長
應用程式開發和交付
企業架構
基礎架構和作業
- 安全性和風險管理

採購和廠商管理

科技產業專業人員
分析師關係

客戶支援

如需有關文件紙本或電子版翻印的資訊，請聯絡客戶支援部門：+1 866-367-7378、+1 617-613-5730，或寄電子郵件至 clientsupport@forrester.com。本公司提供數量折扣和特殊優惠價給學術和非營利單位。