

# Forrester Wave™：2016 年第四季防止資料外洩套件報告

工具和技術：資料安全和隱私保護策略計畫書

撰寫者：Heidi Shey

2016 年 11 月 8 日

## 閱讀本報告的理由

在我們針對防止資料外洩套件供應商所進行的 30 項標準評估中，我們評選出七家最重要的供應商，分別是 Clearswift、DeviceLock、Digital Guardian、Forcepoint、GTB Technologies、Intel Security 和 Symantec，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

### Symantec、Digital Guardian 和 Forcepoint 領先群倫

Forrester 的研究發現，Symantec、Digital Guardian 和 Forcepoint 在市場上領先群倫。Intel Security、GTB Technologies 和 Clearswift 提供具競爭力的選項。DeviceLock 則落在最後。

### 安全性和風險管理專業人員正在尋找健全、一致的資料保護政策落實執行方法

DLP 套件市場持續成長，因為有更多的安全性和風險管理專業人員將 DLP 套件視為落實執行合規、隱私保護和智慧財產保護政策的方法。此市場成長的主因是 DLP 套件能透過單一主控台提供能防堵所有資料外洩管道的 DLP 功能，以套用一致的政策。

### 智慧財產保護、資訊管理，以及端點能見度與控制功能是關鍵差異點

隨著 DLP 套件持續進步，更好的智慧財產保護、資訊管理，以及端點能見度與控制功能將決定哪些供應商更能滿足不斷改變的企業需求。加密資料和資訊流檢查之類的功能持續重要。能提供這類功能的供應商將能提供超越傳統 DLP 技術的全面資料保護套件。

# Forrester Wave™：2016 年第四季防止資料外洩套件報告

工具和技術：資料安全和隱私保護策略計畫書



撰寫者 [Heidi Shey](#)

共同撰寫者：[Stephanie Balaouras](#)、[Alexander Spiliotes](#) 和 [Peggy Dostie](#)

2016 年 11 月 8 日

## 目錄

### 2 資料使用和處理政策需要有一套能落實執行這些政策的方法

防止資料外洩 (DLP) 套件提供落實執行、資料外洩管道全面防堵以及其他更多功能

### 2 DLP 套件評估概觀

受評估廠商和納入標準

### 4 廠商背景資料

領先廠商不但符合嚴格的企業要求，更大力著重創新

表現強勁的廠商提供技術成熟完整且有獨特功能的產品項目

競爭廠商不但符合企業要求，而且發展出在特定領域不容小覷的實力

### 10 補充資訊

## 重要事項與資源

Forrester 在 2016 年 9 月進行了產品評估，並專訪了下列七家主要防止資料外洩 (DLP) 套件廠商：Clearswift、DeviceLock、Digital Guardian、Forcepoint、GTB Technologies、Intel Security 和 Symantec。

## 相關研究文件

[市場概觀：防止資料外洩解決方案](#)

[《運用 Forrester 的 DLP 技術成熟度方格表重新思考防止資料外洩流程》\(Rethinking Data Loss Prevention With Forrester's DLP Maturity Grid\)](#)

[《廠商競爭態勢：防止資料外洩解決方案》\(Vendor Landscape: Data Loss Prevention Solutions\)](#)

## 資料使用和處理政策需要有一套能落實執行這些政策的方法

達到監管合規、隱私保護和智慧財產保護要求的資料使用和處理政策如果沒有落實執行的方法，只會流於無效的紙上談兵。<sup>1</sup> Forrester 對防止資料外洩 (DLP) 的定義如下：

*能偵測出並防止違反敏感資料使用、儲存和傳送相關企業政策的功能。其目的在於落實執行政策，以防止不當的敏感資訊散播。*

### 防止資料外洩 (DLP) 套件提供落實執行、資料外洩管道全面防堵以及其他更多功能

DLP 套件是指能保護待用、移動中和使用中資料的解決方案。<sup>2</sup> 這類產品能防堵多種資料外洩管道 (例如電子郵件、端點、網路、雲端、行動裝置)，並幫助落實 DLP 政策的集中管理。除了能落實執行政策並防止資料不慎外洩之外，這類解決方案的技術也不斷進步，不僅能提供 DLP 功能，更發展成為整合式安全性解決方案，兼具防範、內部威脅偵測和回應能力。

在 2015 年，有 44% 的北美和歐洲企業決策者已實作全面 DLP 解決方案和套件或正在實作過程中，同時另有 15% 的決策者表示已規劃擴大現有實作規模，以及另有 19% 的決策者已規劃在未來 12 個月內進行實作。<sup>3</sup> 在 2016 年，有 63% 的北美和歐洲企業已實作 DLP 解決方案和套件或正在實作過程中。<sup>4</sup>

## DLP 套件評估概觀

為了評定 DLP 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 DLP 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 16 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。**這部分包括廠商的資料外洩管道 (電子郵件、網路和網頁、雲端、端點，以及行動裝置) 防堵技術能力評估標準；專門保護智慧財產的功能；可顯示故障模式；資訊管理功能，例如報告、資料探索、資料分類，以及與資訊生命週期相關技術 (例如 eDiscovery 或法務相關資料保留、記錄管理或企業內容管理、企業 / 認知搜尋，以及權利管理) 整合功能；突發事件管理 (上報以及案例管理)、(使用者以及管理員) 生產力管理；加密技術支援；端點能見度與控制；以及其他功能，例如多語支援，以及員工和各國隱私保護合規功能。
- ▶ **策略。**這部分包括廠商已規劃 DLP 套件增強功能的評估標準；整體安全性產品組合願景，以及客戶滿意度。我們對客戶滿意度的評估是根據多項廠商客戶推薦專訪、一項客戶推薦調查，加上 Forrester 在 2016 年一整年期間詢問客戶以及與客戶互動的綜合結果。
- ▶ **市佔率。**這部分包括廠商現有客群的評估標準；財務狀況；以及人員配置和相關資源。現有客戶群評估標準在於評估廠商的客戶數 (依個別企業標誌計算)；在全球、業界和企業的佔有率；銷售滲透率；以及部署滲透率。

**Forrester Wave™：2016 年第四季防止資料外洩套件報告**  
工具和技術：資料安全和隱私保護策略計畫書

### 受評估廠商和納入標準

Forrester 在此評估中納入了 7 家廠商：Clearswift、DeviceLock、Digital Guardian、Forcepoint、GTB Technologies、Intel Security 和 Symantec。其中每家廠商均有 (詳見圖 1)：

- › 一套能防堵每種資料外洩管道的 DLP 套件。資料外洩管道包括電子郵件、端點、網路、網頁，以及雲端，涵蓋移動中、使用中和待用資料。所有受評估的套件均有這類 DLP 功能：能檢查內容和管道資訊流、能偵測出違反公司資料處理政策的活動，以及提供突發事件補救方法選項。
- › 至少有 300 家客戶 (依個別企業標誌計算)。我們用這項限制條件，以確保 Forrester 最大的客戶能有信心，獲選的這些供應商均有幫助解決企業目前所面臨挑戰的經驗。
- › 受評估套件產品版本均在 2016 年 8 月 12 日之前已普遍可購得。我們僅評估截至此截止日期已發行且普遍可用的套件功能。

DLP 套件持續發展，超越 DLP 技術範圍，並成為兼具防範、內部威脅偵測和因應能力的整合式安全性解決方案。

**Forrester Wave™：2016 年第四季防止資料外洩套件報告**  
 工具和技術：資料安全和隱私保護策略計畫書

圖 1 受評估廠商：套件資訊和選擇標準

廠商	產品名稱
Clearswift	Aneesya Platform
DeviceLock	DeviceLock DLP
Digital Guardian	Digital Guardian for Data Loss Prevention
Forcepoint	Triton AP-DATA
GTB Technologies	Enterprise DLP that Works Platform
Intel Security	McAfee DLP
Symantec	Symantec DLP

#### 廠商納入標準

廠商必須提供一套能防堵每種資料外洩管道（電子郵件、端點、網路、網頁、雲端，而且涵蓋移動中、使用中及待用資料）的 DLP 套件。所有受評估的套件均有這類 DLP 功能：能檢查內容和管道資訊流、能偵測出違反公司資料處理政策的活動，以及提供多種事件補救方法選項。

廠商必須至少有 300 家客戶（依個別企業標誌計算）。我們用這項限制條件，以確保 Forrester 最大家的客戶能有信心，獲選的這些供應商均有幫助解決企業目前所面臨挑戰的經驗。

受評估套件產品版本均在 2016 年 8 月 12 日之前已發行且普遍可購得。

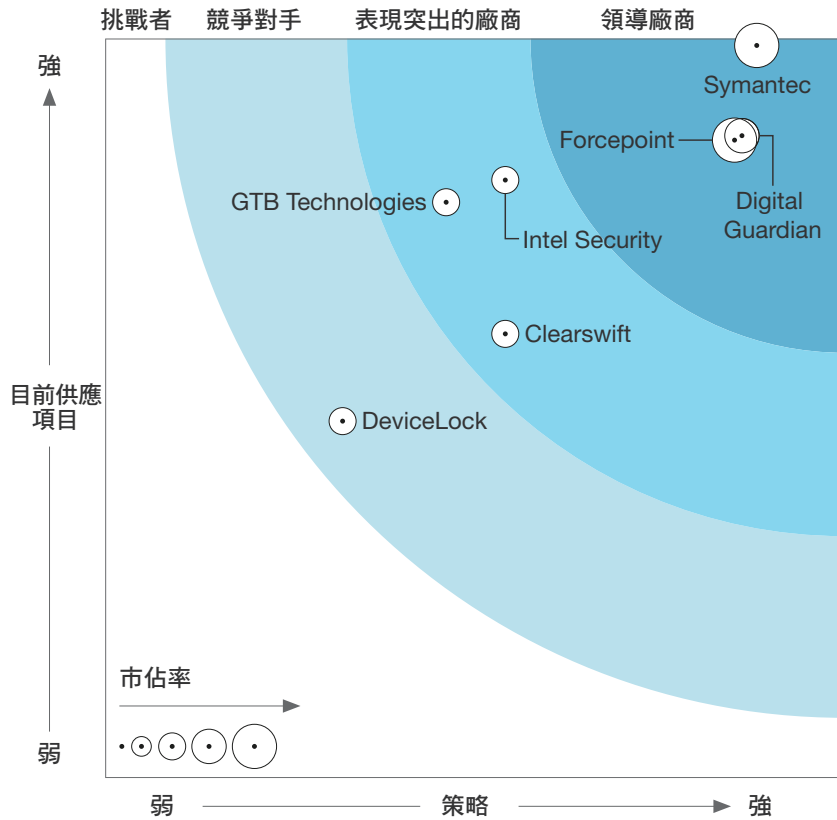
## 廠商背景資料

本 DLP 套件評估的目的只是提供一個起點。我們建議客戶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 2）。

Forrester Wave™：2016 年第四季防止資料外洩套件報告

工具和技術：資料安全和隱私保護策略計畫書

圖 2 Forrester Wave™：2016 年第四季防止資料外洩套件報告



**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](http://Forrester.com) 下載 Forrester Wave 工具。

## Forrester Wave™：2016 年第四季防止資料外洩套件報告

工具和技術：資料安全和隱私保護策略計畫書

圖 2 Forrester Wave™：2016 年第四季防止資料外洩套件報告 (續)

	Forrester 加權比重	Clearswift	DeviceLock	Digital Guardian	Forcepoint	GTB Technologies	Intel Security	Symantec
<b>目前供應項目</b>	50%	3.00	2.41	4.34	4.31	3.89	4.04	4.95
資料外洩管道防堵	15%	2.40	3.30	4.10	3.45	3.25	3.70	4.85
智慧財產保護	14%	3.00	3.00	5.00	5.00	5.00	4.00	5.00
可顯示故障模式	10%	3.50	3.00	3.50	5.00	4.0	5.00	5.00
資訊管理	10%	2.15	2.25	3.50	5.00	4.40	4.10	5.00
突發事件管理	10%	3.50	1.50	4.50	4.50	4.00	5.00	5.00
生產力管理	13%	4.50	3.00	5.00	4.00	4.00	3.00	5.00
加密技術支援	10%	4.0	0.50	5.00	4.50	3.50	4.50	5.00
端點能見度與控制	10%	1.00	2.00	4.00	3.00	3.00	3.00	5.00
其他功能	8%	2.70	2.30	4.00	4.70	3.60	4.70	4.70
<b>策略</b>	50%	2.70	1.60	4.30	4.25	2.30	2.70	4.40
已規劃的增強功能	30%	3.00	1.00	5.00	5.00	2.00	3.00	4.00
安全性產品組合願景	40%	3.00	1.00	4.00	5.00	2.00	3.00	5.00
成本	0%							
客戶滿意度	30%	2.00	3.00	4.00	2.50	3.00	2.00	4.00
<b>市佔率</b>	0%	2.42	2.28	3.18	4.18	2.30	2.62	4.68
現有客戶群	40%	3.05	2.70	2.70	4.45	3.50	2.05	4.20
財務狀況	30%	2.00	1.00	3.00	4.00	2.00	4.00	5.00
人員配置和相關資源	30%	2.00	3.00	4.00	4.00	1.00	2.00	5.00

所有分數均以 0 (弱) 到 5 (強) 的評量尺為計分基礎。

## 領先廠商不但符合嚴格的企業要求，更大力著重創新

領先廠商不僅在他們的目前供應項目中提供能符合最嚴格企業要求的健全功能，而且已規劃強大前瞻的增強功能，並在整體安全性產品組合方面已有願景，這些均將幫助他們符合未來的企業需求。

- › **Symantec**。Symantec 提供一套全面 DLP 套件，具備健全的功能，包括智慧財產保護、資訊管理、突發事件管理，以及加密技術支援。也提供豐富的功能組合，幫助公司符合隱私保護要求。Symantec 有最多的 DLP 專責人員和專用資源，優於此項 Forrester Wave 評估的所有其他受評估廠商。Symantec 持續在此領域創新，而且在 DLP 市場上擁有高品牌認知度。

雖然許多安全性和風險管理專業人員可能將 DLP 與 Symantec 畫上等號（這歸功於 Symantec 在多年前收購了 Vontu！），但還是應該依照您的需求和要求進行評估，以確保從技術和策略角度來看，Symantec 均良好適配。畢竟並非每個人都需要一台超跑，尤其當車子只在交通尖峰時段用於上班通勤時，更是不需要。需要有先進智慧財產保護功能的大企業和大公司應考慮選用 Symantec。

- › **Digital Guardian**。Digital Guardian 將目前普遍需要的兩種企業安全功能整合在一起：DLP 以及端點能見度與控制功能。對策略夥伴關係的極大重視持續增強該公司的資訊管理技術能力。該公司也有一項受歡迎的 DLP 即代管服務項目，目前包含在英國和歐盟境內代管服務選項。此服務選項也讓 Digital Guardian 不但能為大型企業提供服務選項，還能服務中小型市場上的公司（例如安裝機座在 10 個以下）。

Digital Guardian 是此項 Forrester Wave 評估中，受評估廠商套件中客群最小的套件，而且在行動裝置 DLP 功能發展方面還有改善空間。此套件將持續發展其平台，在功能上超越 DLP 範圍，並包括其他重點功能領域，例如先進的防威脅保護。公司如果有涵蓋 Windows、Mac 和 Linux 作業系統的 DLP 功能，或是有興趣採用 DLP 即代管服務，應考慮選用 Digital Guardian。

- › **Forcepoint**。Forcepoint 將 DLP、安全分析和內部威脅偵測整合在其套件內。這套解決方案有一個操作順暢的使用者介面儀表板，而且提供最令人驚艷的報告功能，優於此項 Forrester Wave 評估中其他受評估的競爭廠商。Forcepoint 擷取並顯示豐富的資訊給安全性分析人員和突發事件因應人員，包括詳細的風險評分、突發事件相關性，以及端點活動視訊播放等這類功能。Forcepoint 也提供 DLP 做為多種獨立產品的內建功能，並透過策略合作夥伴提供 DLP 即代管服務。

Forcepoint 的語言支援能力有限，只提供英文版管理員使用者介面。但是，在其面向端點使用者的對話部分，確實有強大的當地語言轉換功能。有充足資源和人員能充分利用此套件功能的公司，將最能從 Forcepoint 受惠。需要有健全智慧財產保護和資訊管理功能的大企業，以及已有成熟安全計畫的公司，應考慮選用 Forcepoint。



## 表現強勁的廠商提供技術成熟完整且有獨特功能的產品項目

表現強勁廠商的目前供應項目均有符合企業核心 DLP 要求的健全功能。其中每家廠商的套件均有與眾不同的差異點，而且所提供的功能讓套件成為能滿足目前企業特定 DLP 需求的理想解決方案，同時也有一項創新策略，幫助發展能滿足未來需求的功能。

- › **Intel Security**。Intel Security 提供一套功能齊全的 DLP 套件，具備健全功能，包括資料探索和分類、突發事件管理，以及加密技術支援。此套件提供豐富的功能組合，幫助公司符合隱私保護要求，並保護智慧財產。此套件的訓練影片和使用者群組也是實用的資源。Intel Security 與客戶協同合作，幫助客戶在實作 DLP 技術控制之前，先了解自家公司的資料和政策，並建議專業服務，以奠定 DLP 技術基礎。

過去幾年來 Intel Security 的成果豐碩！<sup>5</sup> 但該公司在完全實現其 DLP 技術願景上（發展一套端點安全性、資料保護、雲端基礎架構安全性以及統一工作流程的整合式系統），仍有改善空間，同時為順利達到這項成果，也持續地投資。企業如果正在找能與 Intel Security 其他解決方案（例如加密或端點安全性）整合的技術成熟完整 DLP 套件，應考慮選用 Intel Security。

- › **GTB Technologies**。GTB Technologies 以一個容易管理且極具價格競爭力的解決方案形式，提供一套功能齊全的 DLP 套件。此套件有健全的資料探索功能，讓使用者能依索引進行跨端點搜尋，而且已與 Seclore 的資訊權利管理解決方案完全整合。其管理員使用者介面和使用者訊息當地語系化的語言選項，在此項 Forrester Wave 評估的受評估廠商套件中選項種類最多。

雖然 GTB Technologies 配置給人員和銷售業務的專用資源最少，不及此項 Forrester Wave 評估中其他受評估競爭廠商，但其技術仍讓該公司能遠端支援為數眾多的客戶和潛在客戶。其解決方案設計為容易部署，而且技術協助通常是透過網路會議、畫面分享和遠端存取等方式。GTB Technologies 的客群涵蓋中小企業和大型企業，其中大多數客戶 Forrester 會將其歸類為中小企業。公司如果需要有一套容易管理、技術成熟完整、以 DLP 為主的 DLP 套件，應考慮選用 GTB Technologies。

- › **Clearswift**。Clearswift 提供一套容易管理且管理負擔小的解決方案。其套件具備健全的 DLP 和加密功能。Clearswift 的雙向資料編校功能也值得一提。Clearswift 的解決方案不僅提供常見的資料外洩使用案例防範功能，還提供傳入資料濾清功能（這是能有效濾除勒索軟體之類威脅的因應方法）。從資料外洩途徑的角度來看，這項結構化濾清功能非常實用，有助於將文件屬性或使用中內容（例如巨集或指令碼）從可能是分析重要依據的試算表中移除。

Clearswift 的資訊生命週期和權利管理，以及案例管理等功能則較不健全。雖然資料探索和分類功能還有改善空間，但目前的這些功能已足以滿足常見的企業使用案例所需。Clearswift 的客群涵蓋各種規模的企業。公司如果希望受惠於雙向資料編校功能，而且需要有一套容易管理、不會影響員工生產力的解決方案，應考慮選用 Clearswift。

**Forrester Wave™：2016 年第四季防止資料外洩套件報告**  
工具和技術：資料安全和隱私保護策略計畫書

### 競爭廠商不但符合企業要求，而且發展出在特定領域不容小覷的實力

這項 Forrester Wave 評估中唯一競爭廠商的目前供應項目，具備符合大多數企業要求的強大功能以及特定層面的健全功能，最適合在這些層面有特定要求的企業。這家廠商採行別出心裁的方法和策略，凸顯其解決方案技術專長，並著重發展有別於競爭對手的層面。

- › **DeviceLock**。DeviceLock 提供一套延展性極高的解決方案，而且如其名稱能精確控制公司筆記型電腦或桌上型電腦透過電話到印表機等多種類型裝置的進出資料動向。事實上，DeviceLock 的核心技術發展重點向來是裝置通訊端口控制。也著重在幫助客戶透過多種自助式資源（說明文件、影片、線上協助、客戶討論區）快速獲致成功，所以對於希望不透過專業服務協助部署 DLP 套件，以及希望快速部署 DLP 套件的公司而言，是很有吸引力的選項。

DeviceLock 的資料分類、資訊生命週期和權利管理、突發事件管理，以及加密技術支援等功能則較不健全。但是，這些功能通常是大型企業才需要。DeviceLock 的客群在此項 Forrester Wave 評估的所有受評估廠商中最為多樣，而且同時包含中小企業和大型企業。公司如果想要找一套主要提供強大端點控制功能的 DLP 套件，應考慮採用 DeviceLock。

## 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 2 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。

### 本 Forrester Wave 中所用的資料來源

Forrester 使用四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 8 月 12 日前提供給我們的資料。

- ▶ **廠商資格預審調查。** 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。
- ▶ **Wave 評估廠商問卷。** Forrester 評估了每家廠商在一份詳細調查問卷上的回答，以評定每家廠商符合 Forrester Wave 評估標準的程度。

**Forrester Wave™：2016 年第四季防止資料外洩套件報告**  
工具和技術：資料安全和隱私保護策略計畫書

- › **產品示範。**為了在齊平的標準下評估每家廠商和其套件，我們也請廠商依照評估項目特定功能相關指示，進行其產品的功能性示範。我們利用在這些產品示範中的觀察結果，確認每家廠商的產品功能明細與他們在 Forrester Wave 問卷上回答時的描述相符，這些描述包括管理員和使用者經驗。
- › **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>。

**Forrester Wave™：2016 年第四季防止資料外洩套件報告**  
工具和技術：資料安全和隱私保護策略計畫書

## 頁尾註解

- <sup>1</sup> DLP 工具能幫助落實執行政策，但並非一勞永逸的靈丹妙藥。要確保成功，必須經過五個關鍵流程階段。詳見《[運用 Forrester 的 DLP 技術成熟度方格表重新思考防止資料外洩流程](#)》(Rethinking Data Loss Prevention With Forrester's DLP Maturity Grid) Forrester 報告。
- <sup>2</sup> 本報告指出不同的資料外洩管道，並探討廠商目前分別以單一元件、獨立解決方案或套件提供 DLP 功能的不同競爭態勢。詳見《[廠商競爭態勢：防止資料外洩解決方案](#)》(Vendor Landscape: Data Loss Prevention Solutions) Forrester 報告。
- <sup>3</sup> 本報告也探討了導致企業再度重視 DLP 的因素、DLP 套件採用現況，以及不同 DLP 功能企業實作方法的優缺點。詳見《[市場概觀：防止資料外洩](#)》(Market Overview: Data Loss Prevention) Forrester 報告。
- <sup>4</sup> 資料來源：《Forrester 2016 年 Global Business Technographics® 安全性調查》(Forrester's Global Business Technographics® Security Survey, 2016)。
- <sup>5</sup> 在 2016 年 9 月 7 日，Intel 同意將 Intel Security 改回老酒新裝的舊名 McAfee。詳見《[要訊速覽：基於多方協力未能奏效，Intel 再度打出 McAfee](#)》(Quick Take: Intel Spins Off McAfee As Synergies Fail To Materialize) Forrester 報告。

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 或 +1 617-613-5730 或寄電子郵件至 [clientsupport@forrester.com](mailto: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。