解決方案簡介



THALES
CYBERSECURITY

CipherTrust 資料安全態勢管理

識別風險、確定行動優先順序、降低風險。

cpl.thalesgroup.com

THALES

CYBERSECURITY

資料規模與複雜度已超越傳統資安防護

機感資料如今已成爲現代企業的核心資產。它支撐著客戶信任、數位化營運、資料分析和人工智慧創新。然而，這些資料日益分散在雲端平台、SaaS 應用、協作工具、分析環境、文件共享和傳統系統中。

隨著環境的不斷擴展，許多企業無法自信地回答以下三個關鍵問題：

- 機敏資料目前位於何處？
- 誰有權限存取這些資料？他們是否應該擁有存取權限？
- 哪些風險漏洞會造成最大的業務風險？

傳統資安工具的設計，已無法因應現今資料大量分散與營運環境高度複雜化的挑戰。

CipherTrust 資料安全態勢管理 (DSPM)，透過持續發現、智慧風險分析、內建保護和集中式治理，協助企業重新掌控資料安全。

大多數企業已經擁有視覺化工具。他們現在需要的是控制權。

爲何資料安全必須改變：

我們正處於網路安全新時代

資安風險環境的變化速度，已超越許多企業既有的資安營運模式。

- AI 正加速資料風險：代理型 AI（Agentic AI）與 AI 驅動的分析應用，正快速複製、轉換並產生新的機敏資料儲存環境。若企業無法確保資料生命週期的可信度與有效控管，就無法眞正信任建立在這些資料之上的 AI 結果。
- 機敏資料無所不在：關鍵資訊不再只存在於資料庫中。它散佈儲存在雲端、SaaS 平台、協作工具、資料湖和非託管儲存庫中。
- 董事會重視可量化的成果：資安主管日益被要求證明可量化的風險降低成效，而不只是展現工具的部署與導入。
- 法規與資料主權日益受到重視：全球各地的隱私法規、資料在地化要求，以及特定產業的監管規範持續增加。
- 工具氾濫導致營運效率低落：許多企業依賴各自獨立的工具來進行發現、存取治理、加密、合規性和態勢管理。

結果

只有可視性，沒有行動；只有警示，沒有補救；只有風險，卻沒有人負責。

安全領導者面臨的五大挑戰

許多企業面臨的並非可視性問題，而是控制問題。

1. 未知機敏資料：機敏資料存在於安全團隊未監控的位置，造成盲點和隱藏風險。AI 和 Agentic AI 系統的快速普及加劇了這項挑戰，因爲它們會在雲端、SaaS、協作和人工智慧環境中產生、複製和使用機敏資料。
2. 過度的存取權限：過多使用者、第三方及服務帳戶，在超出業務所需的情況下，仍持續保有敏感資訊的存取權限。
3. 風險優先排序有限：團隊收到大量發現，但對造成實際業務的風險，無法做優先排序。
4. 人工合規負擔：稽核準備工作往往需要花費數週，從多個彼此分散、未整合的系統中蒐集佐證資料。
5. 保護漏洞：即使識別出風險，應用加密、遮罩、代碼化或策略變更，也可能需要不同的團隊和工具做修護。

資料安全新營運模式

CipherTrust DSPM

發現 | 分析 | 保護 | 控制

發現：在惡意行爲者之前發現關鍵訊息

持續發現並分類雲端、SaaS、資料庫、文件共享和本地環境中的結構化和非結構化機敏資料，確保所有關鍵資訊都清晰可見。您將獲得：

- 機敏資料的完整即時清單
- 發現、分類和關聯影子資料
- 掌握關鍵資料的儲存位置與移動路徑
- 了解不同環境中的資料訪客

消除盲點，掌握關鍵資料的儲存位置。

分析：聚焦關鍵風險

關聯資料敏感度、存取風險、漏洞、行爲和業務背景，確定哪些因素會造成眞正的企業風險。您將獲得：

清楚排序具最高潛在影響的風險，並優先處理

- 能夠追蹤人爲、非人爲以及特定代理的活動，例如過度共享、資料外洩和異常存取模式
- 深入了解過度存取、配置錯誤和攻擊路徑
- 更快地識別並回應安全漏洞
- 更有效地利用有限的安全資源

減少干擾，將資源集中在潛在影響最大的風險。

保護：從風險偵測到即時防護

直接從平台套用加密、代碼化、遮罩和基於策略的修復措施，更快降低資料暴露的風險。您將獲得：

- 更快修復高風險
- 整合調查和取證工具，支援快速事件回應和資料安全事件的根本原因分析
- 在最關鍵的地方應用保護措施
- 自動化執行（需審核）工作流程
- 降低風險暴露和洩漏的影響

更快地、有效地降低風險暴露，並減少洩漏事件的影響。

掌控：透過持續治理保持掌控

透過單一控制平台，跨混合環境管理存取權限、策略、金鑰、機密資訊和合規性證據。您將獲得：

- 確保只有授權使用者才能存取資料
- 資料所在位置的策略執行一致性
- 雲端和本地集中控制
- 隨時可供查核的存取和保護可視性

隨著資料和環境的演變，持續保持控制。

企業爲何選擇 CipherTrust DSPM

CipherTrust DSPM 內建風險修復功能，將風險視覺性轉化爲實際行動，使安全團隊不僅能夠識別風險，還能快速降低風險，無需依賴分散的工具或手動流程。

CipherTrust DSPM 提供貫穿資料生命週期的全面保護，從風險發現到風險修復，並提供必要的治理機制，進而彌補傳統單點解決方案的不足，確保機敏資料在不同環境傳輸時始終安全無虞。 CipherTrust 分析資料互動以識別風險，並對其進行優先排序，引導企業將時間和資源投入最有可能造成重大影響的風險。

CipherTrust DSPM 在強化資料安全的同時，不影響企業業務運作，透過自動化的加密、代碼化與存取控制降低資料曝險風險，同時維持資料在分析、AI 與日常營運上的可用性。例如，CipherTrust DSPM 可以找到未加密或加密強度不足的資料，並允許企業使用自動化控制來應用適當的加密強度。

此外，CipherTrust DSPM 透過持續維持稽核就緒狀態，簡化合規管理，讓企業即時掌握敏感資料的所在位置、保護方式，以及具備存取權限的人員。 CipherTrust DSPM 提供審計日誌和報告，使企業能夠隨時獲取所需的合規資訊，並始終做好查核準備。

最後，它使企業能夠在混合雲和多雲環境中實現一致的控制，無論資料儲存在何處，都能強制執行策略、降低風險暴露並維護治理。

整合到您的資料安全與回應體系中。

CipherTrust DSPM 可與既有的資安與事件回應生態系整合，包括 SIEM 平台及 ServiceNow 等工單系統，將資料風險洞察轉化爲實際的資安行動。透過將發現、風險分析和修復工作流程直接串接到客戶的安全架構，企業可以加快事件回應速度，自動化修復流程，並縮短在混合雲和多雲環境中，識別和解決關鍵資料外洩所需的時間。

適用情境

- 發現混合資產中未知的機敏資料
- 減少對關鍵資料的過度存取
- 加強稽核和監管準備
- 確保代理型 AI 與 AI 驅動的分析資料安全
- 保護高價值的監管資料和關鍵業務資料

部署靈活，效能毫不妥協

在不放棄控制權的前提下，實現安全現代化。

SaaS 部署

快速實現價值、降低營運負擔、持續創新、全球可擴展。

本地部署/混合部署

維護主權、滿足內部信任和監管要求，並在各種部署模式下保持一致的功能。

爲什麼選擇 Thales

CipherTrust DSPM 傳承 Thales 數十年來在保護全球關鍵系統、資料與基礎架構方面的領導地位。

從全球銀行和醫療保健機構到政府部門、製造業以及受嚴格監管的企業，各企業機構在不容許絲毫差錯的情境下都信賴 Thales。

唯有 Thales 將新一代 DSPM 創新技術，與在加密、金鑰管理、代碼化，以及活動監控與風險分析領域深厚且經驗成熟的技術優勢相結合，協助企業降低資料風險，同時維持對機敏資訊的掌控。

憑藉支援全球大型企業的規模，以及因應資料主權、資料在地化與法規要求的彈性，Thales 打造值得信賴的平台，協助企業因應今日日益複雜的全球 IT 環境。

Thales 優勢

大多數 DSPM 供應商都能協助您了解風險	CipherTrust DSPM 助您降低風險
• 著重於定期發現與分類	• 持續發現與分類
• 事件列表，未進行優先排序	• 基於情報的優先排序
• 警報過多	• 內建保護
• 需要手動修復	• 集中式治理
• 需要單獨的防護工具	• 建構於經驗成熟的 Thales 資料安全平台之上

結論

CipherTrust DSPM 幫助企業擺脫碎片化工具和僅提供態勢資訊的儀錶板，實現可衡量的風險降低。

它結合了持續發現、優先智慧排序、內建保護和集中控制，使安全主管能夠全面掌控跨雲端、SaaS、AI 和混合環境的機敏資料。

大多數供應商都能協助您了解資料風險。
Thales 能協助你規避風險。

藉助 CipherTrust DSPM 重新控制機敏資料。

關於 Thales

Thales 是網路安全領域的全球領導者，致力於幫助企業、政府和全球最值得信賴的組織，以最高的投資報酬率，大規模地保護關鍵應用程式、機敏資料、身分和軟體。我們擁有超過 30,000 家客戶，其中包括 58% 的《財富》世界 500 強企業，我們的解決方案已部署在全球 148 個國家。透過我們創新的服務和整合平台，Thales 幫助客戶更了解風險、抵禦網路威脅、彌補合規漏洞，並每天爲數十億消費者提供值得信賴的數位化體驗。

© Thales - May 2026 • AC v2