解決方案簡介

CipherTrust Data Security Posture Management

需要提問和回答的五個基本問題

cpl.thalesgroup.com

THALES
Building a future we can all trust

THALES
Building a future we can all trust

對 DSPM 的重視反映了資料安全從基於邊界防禦向以資料為中心方法的更廣泛轉變。隨著資料在混合多雲環境中持續擴散和分散，動態管理資料安全狀態對於旨在保護敏感資訊並維護信任的企業而言愈發關鍵。

什麼是資料安全狀態管理？

資料安全狀態管理（DSPM）提供對機敏資料位置、存取者、使用方式以及所儲存資料或應用程式安全狀態的可見性。

來源: https://www.gartner.com/reviews/market/data-security-posture-management

根據 Gartner 的定義，DSPM 工具可自動發現、分類和分析各類資料儲存中的非結構化和結構化資料風險，包括本地、雲端、多雲和混合雲環境中儲存的資料。這些工具有助於持續識別機敏資料的位置、可存取性及現有保護措施。DSPM 解決方案通常提供建議或自動化功能以修復已識別的風險，並透過使資料安全策略與法規要求保持一致來確保治理與合規。

根據 Gartner 的定義，DSPM 工具可自動發現、分類和分析各類資料儲存中的非結構化和結構化資料風險，包括本地、雲端、多雲和混合雲環境中儲存的資料。這些工具有助於持續識別機敏資料的位置、可存取性及現有保護措施。DSPM 解決方案通常提供建議或自動化功能以修復已識別的風險，並透過使資料安全策略與法規要求保持一致來確保治理與合規。

DSPM 在當今資料環境中的重要性

由於技術和社會變革，資料安全近年來發生了重大轉變，凸顯了制定全面綜合的資料安全狀態管理 （DSPM） 策略的必要性。

對 DSPM 的重視反映了資料安全從基於邊界防禦向以資料為中心方法的更廣泛轉變。隨著資料在混合多雲環境中持續擴散和分散，動態管理資料安全狀態對於旨在保護敏感資訊並維護信任的企業而言愈發關鍵。

全面的 DSPM 策略必須涵蓋結構化和非結構化資料，並考慮跨雲環境儲存的資料。隨著資料儲存日趨多樣化和複雜化，對強大 DSPM 解決方案的需求也在增長。這些解決方案不僅支援運營完整性和法規合規，更是任何現代網路防禦策略的支柱，能夠保護敏感資訊免受不斷演變的威脅。如今，DSPM 必須應對新興風險，以有效保護資料。

缺乏資料安全生命週期可見性：

在當今複雜的資料環境中，了解結構化和非結構化資料的位置與互動至關重要。然而，隨著資料分散在雲端、資料湖和本地系統中，準確識別和分類資料已變得頗具挑戰。據”雲端安全聯盟：了解資料安全風險 2025”報告顯示，80% 的受訪者對識別高風險資料來源缺乏信心。此外，資料易於移動和共享，削弱了對其位置的控制。當使用者在缺乏適當安全措施的情況下共享資料時，敏感資訊可能流向未知或外部位置，加大了資料外洩攻擊的風險。

憑證蔓延：

雲端運算的快速擴張使眾多企業在線上儲存了越來越多的機敏資料，這也使其面臨傳統安全措施無法充分應對的新型漏洞和複雜設定。雲端服務、容器和 DevOps 的迅速普及使金鑰和機密散落於各平台、儲存庫和程式碼庫中。這種不受控的擴散增大了攻擊面，眾多洩露事件與暴露或管理不當的憑證有關。2024 年 Verizon 資料洩露調查報告顯示，80% 的資料洩露涉及被盜憑證。強有力的監管和一致的安全措施對於保護敏感憑證、防止未授權存取至關

AI 驅動的憑證安全風險：
AI 產生的攻擊（如網路釣魚活動）更具說服力、可擴展性更強且更難檢測，增大了憑證洩露風險。雖然多因素驗證（MFA）必不可少，但仍不夠充分。增加行為監控——追蹤異常存取時間、登入位置和意外資料下載——可提供對抗複雜 AI 驅動威脅的分層防禦。Sapios 研究和 Deep Instinct 的報告顯示，75% 的受訪安全專業人員表示在過去一年中攻擊有所增加，85% 將上升歸因於不法分子使用生成式 AI。這一不斷演變的形勢凸顯了在所有環境中部署有效 DSPM 策略以保障組織資料安全的重要性。

後量子密碼學風險：
近期發展（如微軟的 Majorana 1 晶片）表明，量子運算可能很快達到能夠破解 RSA 和 ECC 等非對稱演算法的水平。執行 Shor 演算法的量子電腦可能破解這些加密方法，暴露敏感資料。2025 年 Thales 資料威脅報告顯示，「先收穫後解密」攻擊（70%）是後量子運算領域最受關注的威脅，網路犯罪分子正在收集當前加密資料，以待量子運算可用時解密。這凸顯了組織現在就需透過採用抗量子演算法和擁抱加密敏捷性來做好準備。

主動偵測風險：
內部威脅（包括洩露和破壞）正變得日益複雜，難以偵測。2025 年 Thales 資料威脅報告強調，受訪者對員工造成的資料暴露風險與外部未授權存取的擔憂程度相當。透過強而有力的監控進行有效風險管理對於防止洩露至關重要，因為傳統邊界安全已不足以應對。

資料治理：
全球資料保護法規對違規行為規定了嚴厲處罰，凸顯了識別行為變化以在機敏資料受損前發現威脅的重要性。安全策略必須不斷演進，融入 DSPM 等方法來應對新出現漏洞和攻擊途徑。

回答資料安全狀態管理的五個基本問題

我的機敏資料在哪裡？

了解機敏資料的位置是保護資料的第一步。這包括識別結構化資料（如資料庫和電子表格中的資料）和非結構化資料（如電子郵件、文件和多媒體檔案）。這些資料類型通常分散在各種儲存環境中，包括本地伺服器和多個雲端平台（如 AWS、Azure 或 Google Cloud）。

重要性

- 實施適當的安全控制：特定類型的資料可能需要基於法規要求或業務需求的特定安全措施。
- 管理資料擴散：隨著資料量增長並分散到混合和多雲環境中，追蹤機敏資料的儲存位置變得更具挑戰性，也更為關鍵。
- 遵從法規：遵守資料保護法律（GDPR、CCPA、HIPAA 等）通常需要詳細了解特定類型資料的儲存位置。

許多企業不知道其機敏資料在哪裡，也不知道資料是否處於危險暴露狀態。這些盲點會造成安全風險，可能導致疏忽錯誤或為攻擊者創造可利用的機會，往往透過您可能甚至不知道存在的隱藏漏洞或設定錯誤的資料庫加以利用。

如今，企業通常採用多種儲存解決方案，例如本地伺服器、多個雲端環境（公有雲和私有雲）以及 SaaS 平台。這種多樣性使機敏資料分散在眾多位置，使全面追蹤和管理變得複雜。

現代企業以極快的速度產生和處理大量資料，涵蓋結構化資料（如資料庫）和非結構化資料（如電子郵件和文件）。持續監控所有這些資料的即時位置面臨重大挑戰。

此外，企業內的資料是動態的；它定期被各種應用程式和使用者移動、處理和存取。這種持續的移動使得在沒有先進監控工具的情況下，確定任何特定時間資料的精確位置變得十分複雜。

關鍵在於利用資料發現和分類功能，自動發現資料資產中的所有資料儲存——從結構化到非結構化——跨越本地、雲端、多雲和混合環境。自動化發現和分類是例行、一致地發現和分類新增或修改資料儲存的唯一方式。

誰有權存取我的機敏資料？

控制和監控誰有權存取機敏資料對於防止未授權使用和潛在資料洩露至關重要。這包括管理內部員工和外部合作夥伴的權限。

重要性

- 防止資料洩露：透過將機敏資料的存取權限限制在工作需要的人員範圍內，組織可以降低內部威脅和外部攻擊的風險。
- 支援合規：許多法規框架要求嚴格控制資料存取。了解存取權限有助於維持對這些法規的合規。
- 增強資料管理：監控資料存取情況有助於稽核和追蹤使用模式，這對安全和運營效率至關重要。

許多企業由於缺乏全面的工具，在資料存取的可見性和監管方面存在局限。在沒有有效手段跨各系統和平台彙總和分析存取資料的情況下，確定當前誰有權存取機敏資料變得十分困難。

現代企業通常採用複雜的分層存取結構，包括基於角色的存取控制（RBAC）、基於屬性的存取控制（ABAC）及其他模型。這些複雜的系統使得精確了解誰在何種條件下可存取哪些資料變得困難。此外，在大型企業中，不同部門或分支機構往往獨立管理各自的 IT 資源，導致存取控制和策略不一致。這種去中心化使得追蹤整個企業的資料存取變得複雜，進一步降低了對誰可以存取敏感資訊的可見性。

掃描資料儲存位置以獲取已授予的使用者權限，並顯示有關使用者權限的各種詳細資訊，對於透過跨所有資料庫將使用者和權限對應到資料庫物件來了解資料狀態至關重要。

憑證的保護程度如何？

對具備解鎖加密資料能力的元資料和憑證（如加密金鑰和機密）進行保護至關重要。這包括使用支援當前資料保護和未來量子運算將加速惡意解密技術環境下資料保護的密碼學。

重要性

- 保護相關元資料：將金鑰和機密與加密資料分開集中管理，為保護機敏資料增加了額外的安全層。
- 為後量子現實做好準備：部署加密敏捷產品，使組織今天就能使用後量子運算（PQC）演算法和金鑰。
- 阻止憑證蔓延：保護憑證並阻止金鑰和機密的不受控擴散，對於減少攻擊面和防止未授權資料存取至

許多企業將加密作為保護資料的基本工具，但往往忽視了保護使加密資料可讀和可用的金鑰和機密的必要性。就像把房子的鑰匙放在門墊下一樣，將加密金鑰和機密儲存在加密資料附近會使其容易受到攻擊。

許多企業利用多個雲端服務供應商儲存資料，這意味著金鑰建立、管理和輪換流程因雲端服務供應商而異。隨著企業部署越來越多的加密解決方案，他們發現自己需要管理不一致的策略和不同層級的保護，並承受不斷上升的成本。走出這一迷局的最佳方式通常是過渡到集中式加密金鑰管理系統。

集中化金鑰和機密管理（涵蓋金鑰產生、儲存、輪換、備份、復原、撤銷和終止）可有效實現職責分離，確保建立和管理金鑰的人員無法存取受保護的資料，透過分配關鍵任務的相關職責來降低風險。

我的機敏資料是如何被使用的？

追蹤資料隨時間的存取和使用情況對安全和合規至關重要。這包括了解資料存取和修改的背景，並偵測可能表明安全威脅的異常模式。

重要性

- 偵測異常：異常的存取模式或意外的資料修改可能是資料洩露的早期跡象。
- 稽核和鑑識分析：全面的資料使用日誌對稽核至關重要，在安全事件發生後的鑑識調查中也彌足珍貴。
- 最佳化資料存取控制：透過了解資料的使用方式，企業可以改進存取控制，以更好地符合實際業務需求和安全要求。

有效的資料使用追蹤需要先進的監控和日誌工具，以提供所有資料互動的詳細準確記錄。許多企業缺乏這些工具，或未將其完全整合到所有系統中，導致資料使用可見性存在差距。

各類法規要求對資料存取和使用進行詳細記錄（如 GDPR、HIPAA）。在不同司法管轄區遵守這些法規，為追蹤機敏資料的使用方式增加了又一層難度。

強大的合規和安全性對於資料保護至關重要，可確保對使用情況、漏洞和存取權限的可見性。隨著數位經濟驅動資料指數級增長，企業需要以資料為中心的合規和安全解決方案來降低不合規和洩露風險。自動化工作流程並提供建議操作可簡化流程，協助安全團隊在資料風險升級之前識別它們。

我們資料儲存的安全狀態（即資料安全的當前狀態）如何?

評估資料儲存的安全狀態涉及評估已實施安全措施的有效性、識別漏洞以及了解潛在威脅的影響。

重要性

- 加強防禦：識別資料安全中的漏洞和差距，能夠主動改進並協助防止洩露。
- 有效管理安全資源：透過了解安全最薄弱的地方，企業可以將資源更有效地分配到最需要的地方。
- 確保韌性：定期評估安全狀態確保防禦措施與不斷演變的威脅和變化的業務實踐保持同步。

有效的狀態管理需要定期更新的最新漏洞定義，並透過掃描加以利用，以評估資源、搜尋漏洞並確定風險。透過使用基於 CIS 和 DISA STIG 基準的預定義漏洞測試掃描資料庫，使企業能夠及時了解易受最新威脅影響的資料庫。這些掃描利用 CVSS 按網路和資料中發現的漏洞呈現風險並分配風險評分。CVSS 是「一個用於傳達 IT 漏洞特徵和影響的開放框架」，由美國國家標準與技術研究院（NIST）作為安全內容自動化協議（SCAP）框架的一部分進行維護。使用 CVSS 對漏洞評分提供了一種準確的模型，用於衡量已發現漏洞中固有的風險並確定其修復優先順序。

監控是資料管理生命週期中的關鍵階段，可提供即時資訊，包括系統事件、告警、違規、被封鎖來源、閘道和代理狀態、系統警告、資料庫稽核資訊、檔案伺服器稽核資訊、封存資訊等。

監控事件、告警和違規可涉及多個方面。根據您的具體實施情況，可能存在多種類型的使用者，具有不同的角色和相關安全策略。您可以使用預設定的嚴重性評級或自訂策略，以微調事件的解讀方式，從而判斷告警是誤報、攻擊還是其他情況。

超越風險識別、保障資料安全的一體化平台

資料安全狀態管理（DSPM）是指協助企業保護其整個基礎架構中機敏資料的工具與實踐。DSPM 解決方案自動化資料發現、分類、保護與風險評估，提供對機敏資料儲存位置及存取者的可見性。這些工具可識別漏洞、產生告警並提供修復指導，以應對資料安全風險。透過與其他安全系統整合並支援合規報告，DSPM 協助企業維持強大的資料安全狀態並符合法規要求 。

了解您的資料資產

CipherTrust DSPM 在各類資料儲存中自動發現和分類結構化和非結構化資料，包括本地、雲端、多雲和混合雲環境。

- 掃描和識別資料：CipherTrust DSPM 系統地掃描資料環境——無論是本地還是雲端——以發現資料儲存庫。這包括資料庫、大數據平台、雲端儲存和檔案系統。
- 資料分類：在發現之後，CipherTrust DSPM 根據資料的類型和敏感性對其進行分類。這種自動化分類協助企業了解其持有的資料，並相應地確定安全優先順序。
- 了解使用者存取：CipherTrust DSPM 提供使用者權限管理，監控資料存取和特權使用者的活動，以識別過度、不當或未使用的權限。它還為安全和 IT 團隊提供對資料如何在組織內被存取、使用和移動的完整可見性。

強化您的資料安全狀態

全面的資料保護策略對資料安全狀態管理（DSPM）至關重要，但往往被忽視。透過加密和有效的憑證管理建立堅實的資料保護基礎，對維持強大的資料安全狀態至關重要。CipherTrust DSPM 識別機敏資料並使用業界領先的技術加以保護。它確保憑證和元資料的安全，阻止使用者和應用程式的未授權存取，並強化企業的整體資料安全和合規框架。

- 保護機敏資料：實施加密、資料遮罩和權杖化等關鍵資料保護措施，確保機敏資料只能被授權的應用程式和人員使用，同時保護信用卡資訊、智慧財產權或個人識別資訊（PII）等敏感資訊。
- 保護解鎖加密資料的元資料：加密和資料遮罩是保護資料的第一步。然而，同等重要的是要保護解鎖受保護資料的金鑰和機密，利用集中化金鑰管理。為有效做到這一點，應在混合雲環境中偵測和清點金鑰與機密。
- 為後量子現實做好準備：量子電腦因其能夠破解常用加密方法而構成重大網路安全威脅。這可能導致資料洩露、通訊受損，以及區塊鏈和驗證協議中的漏洞。企業需要過渡到抗量子密碼學並採取主動安全措施來降低這一威脅。
- 阻止憑證蔓延：加密、權杖化和資料遮罩保護憑證，使其不會被分享給授權受眾以外的人。這些技術使資料保持不可讀或不可用狀態，防止建立包含機敏資料的非正規資料儲存。

建立強大的資料保護基礎後，CipherTrust DSPM 使企業能夠進行主動風險分析，有效識別和優先處理與其管理資料相關的風險。這種智慧型風險分析提供關鍵洞見，使企業能夠迅速定位漏洞所在。憑藉這些知識，他們可以制定策略計畫來降低這些風險，顯著增強其資料安全狀態，並確保其最寶貴資產——資料的安全。

- 評估風險：透過評估資料的儲存、存取和共享方式，CipherTrust DSPM 可以識別可能導致資料洩露的漏洞、高風險設定和不當存取控制。CipherTrust DSPM 提供跨所有環境的資料安全風險集中視圖，使企業能夠了解機敏資料的位置、保護層級及保護方式，同時識別表明內部威脅的金鑰或機密濫用。

- 識別行為變化：使用者和實體行為的變化是風險和潛在環境威脅的關鍵指標。隨著 AI 驅動威脅的出現，行為分析已被證明是識別現代網路釣魚策略或其他低速緩慢攻擊中細微變化的有效工具。
- 識別人工智慧帶來的風險：隨著人工智慧被越來越多地用於賦能員工，企業必須應對新一代風險。識別影子 AI 服務、防止 AI 造成的機敏資料洩露，以及偵測和回應異常 AI 行為至關重要。
- 理解事件關係：利用 AI 分析將使用者行為與應用程式和資料上下文相結合，以理解外部和內部威脅，並應對「低速緩慢」攻擊。
- 確定重點領域：透過可自訂的風險評分，企業不僅可以識別風險，還可以根據嚴重性和影響確定哪些領域需要最多關注。這使他們能夠將投資有效集中在最能改善安全狀態的領域。

持續改善資料安全運營

識別風險後，迅速有效地進行修復至關重要。CipherTrust DSPM 不僅識別風險，還提供如何降低風險的建議。透過劇本，企業可以建立代表資料安全採取行動的自動化操作，無論是隔離表現出風險行為的使用者，還是開啟待調查的威脅工單。

- 提出安全增強建議：基於風險評估， CipherTrust DSPM 提供可操作的洞見和建議，以加強最需要的地方的安全控制。
- 自動化安全策略：CipherTrust DSPM 可以在不同平台上自動執行安全策略，減少保護資料資產所需的手動工作量。
- 升級事件優先順序：CipherTrust DSPM 透過快速識別受影響系統和策略違規的嚴重性，促進高效的事件管理和問題解決

資料治理和合規舉措建立政策和流程，以確保企業資料在其整個生命週期中的品質、安全和可用性。CipherTrust DSPM 透過提供對資料存取、使用和傳輸的可見性，協助企業將其資料安全策略與治理和合規保持一致。

- 支援合規舉措：透過確保機敏感資料得到充分保護且存取控制得到正確實施，滿足 GDPR、HIPAA、CCPA 等合規法規的要求。為滿足新興合規要求，企業必須能夠稽核金鑰和機密的使用情況。
- 產生報告：CipherTrust DSPM 提供可用於向稽核人員和其他利害關係人展示合規性的詳細報告 。

DSPM 解決方案對於旨在全面保護機敏資料的企業至關重要。這些解決方案回答了支撐有效資料安全策略的五個基本問題。

CipherTrust DSPM：整合 DSPM 必要關鍵技術

資料發現

CipherTrust DSPM 擅長在從本地到雲端的各種環境中發現機敏資料，自動識別和對應關鍵資訊。這有助於增強合規管理和洩露保護。

資料分類

借助 CipherTrust DSPM，資料根據其敏感性和法規需求進行精細分類，從而能夠精確應用安全措施並確定資料保護的優先順序。

資料加密、遮罩和權杖化

CipherTrust DSPM 允許您在整個 IT 生態系統中對靜態和動態資料進行保護、匿名化和加密，並確保資料金鑰受到保護且只在您的控制之下。

靜態風險分析

系統的靜態風險分析預先識別資料基礎架構中的漏洞，使企業能夠在漏洞被利用之前解決潛在威脅。

評估和暴露風險識別

CipherTrust DSPM 持續監控資料存取點和暴露層級，以迅速偵測和緩解未授權存取或資料洩露，保護敏感資訊的完整性。

高危漏洞告警

即時告警系統對嚴重漏洞發出警告，根據其潛在影響確定問題優先順序，使企業能夠快速有效地回應。

風險報告和評估

該功能提供深度風險評估和可自訂報告，協助企業了解其安全狀態並識別漏洞以進行主動緩解。

修復指導

就已識別的安全漏洞提供糾正措施建議，提供符合最佳實踐和行業標準的實用、可操作指導。

企業就緒性

憑藉可擴展的架構設計，CipherTrust DSPM 與現有企業系統無縫整合，支援複雜資料環境並適應不斷變化的企業需求 。

與安全和協調服務的整合

透過將 CipherTrust DSPM 與安全和協調服務整合來改善安全運營，促進各種安全工具的協調管理並提高運營效率。

劇本自動化

CipherTrust DSPM 利用劇本自動化為常見安全事件提供標準化回應，簡化威脅管理並最小化回應時間和損失。

合規稽核和報告

CipherTrust DSPM 透過詳細記錄資料安全管理各方面（從存取日誌到風險評估）的報告，支援合規和稽核流程。

關於 Thales

Thales 是網路安全領域的全球領導者，協助企業、政府和世界上最受信賴的組織在任何地方、大規模保護關鍵應用程式、機敏資料、身份驗證和軟體——並以最高的投資報酬率實現。我們擁有超過 30,000 名客戶，其中包括全球財富 500 強中的 58%，我們的解決方案部署在全球 148 個國家和地區。透過我們的創新服務和整合平台，Thales 協助客戶更好地了解風險、抵禦網路威脅、彌補合規差距，並每天為數十億消費者提供可信賴的數位體驗。