Solution Brief

CipherTrust DSPM(Data Security Posture Management)

基本となる5つの重要な問いとその答え

cpl.thalesgroup.com

THALES
Building a future we can all trust

DSPMを重視する動きは、データセキュリティの考え方が境界ベースの防御からデータ中心のアプローチへと大きくシフトしていることを示しています。データがハイブリッドなマルチクラウド環境で増加し分散し続ける中、機密情報を保護し信頼を維持するために、データセキュリティポスチャ（態勢）を動的に管理することがますます重要になっています。

DSPM（Data Security Posture Management）とは?

DSPM（Data Security Posture Management；データセキュリティポスチャ管理）は、機密データの所在やアクセス権限、使用状況、保存されているデータやアプリケーションのセキュリティ態勢を可視化して管理するための手法です。

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

DSPM（Data Security Posture Management）とは、組織がインフラストラクチャ全体で機密データを保護するためのツールや手法を指します。DSPMソリューションは、データの検出、分類、保護、リスク評価を自動化し、機密データの所在やアクセス権限を可視化することで把握しやすくします。これらのツールは、脆弱性を特定し、アラートを発し、データセキュリティリスクに対処するための是正ガイダンスを提供します。また、他のセキュリティシステムと統合してコンプライアンスレポートの作成を可能にすることで、組織が強固なデータセキュリティポスチャを維持して規制要件を満たせるよう支援します。

Gartnerによると、DSPMツールは、オンプレミス、クラウド、マルチクラウド環境、ハイブリッドクラウドなど、さまざまなデータストアタイプにわたる非構造化データと構造化データの検出、分類、リスク分析を自動化します。これらのツールは、機密データの所在、アクセス権限、既存の保護措置を継続的に把握するために役立ちます。また、DSPMソリューションは多くの場合、特定されたリスクを是正するための推奨事項や自動化機能を提供し、データセキュリティ戦略を規制要件に沿わせることで、ガバナンスとコンプライアンスを確保します。

今日のデータ環境におけるDSPMの重要性

近年、テクノロジーと社会の変化によりデータセキュリティは大きく変容しており、全体的かつ包括的なDSPM（Data Security Posture Management）戦略の必要性が高まっています。

DSPMを重視する動きは、データセキュリティの考え方が**境界ベースの防御からデータ中心のアプローチへと**大きくシフトしていることを示しています。データがハイブリッドなマルチクラウド環境で増加し分散し続ける中、機密情報を保護し信頼を維持するために、データセキュリティポスチャ（態勢）を動的に管理することがますます重要になっています。

包括的なDSPM戦略には、構造化データと非構造化データの両方が含まれ、かつ、クラウド環境全体に保存されているデータを考慮する必要があります。データストレージが多様化し複雑化する中で、堅牢なDSPMソリューションの必要性も高まっています。これらのソリューションは、オペレーションの整合性と規制コンプライアンスをサポートし、最新のサイバー防御戦略の基盤を形成して、進化し続ける脅威の状況から機密データを保護します。今日のDSPMには、絶えず変化するリスクに対応し、効果的にデータを保護することが求められています。

データセキュリティ ライフサイクルの可視性の欠如:
今日の複雑なデータ環境では、構造化データと非構造化データの場所と相互作用を把握することが極めて重要です。しかし、クラウド、データレイク、オンプレミスシステムにデータが分散しているため、データを正確に特定し分類することが困難になっています。「Cloud Security Alliance: Understanding Data Security Risk 2025」レポートによると、回答者の80%がリスクの高いデータソースを特定する自信がないと回答しています。さらに、データは簡単に移動・共有されてしまうため、データの所在を管理することが難しくなっています。ユーザーが適切なセキュリティ対策を講じずにデータを共有した場合、機密情報が不明な場所や外部の場所に保管される可能性があり、データ流出攻撃に対する脆弱性が高まります。

認証情報の拡散（スプロール）:
クラウドコンピューティングの急速な拡大により、多くの組織がますます機密データをオンラインに保存するようになりました。この変化により、新たな脆弱性が生じ、システム構成が複雑化することで、従来のセキュリティ対策だけでは対応が困難になっています。クラウドサービス、コンテナ、DevOpsの急速な導入により、鍵やシークレットが複数のプラットフォーム、リポジトリ、コードベースに分散しており、このような無秩序な拡散が攻撃対象領域を拡大しています。多くのセキュリティ侵害は、認証情報の漏洩や管理不備に起因しています。Verizonの「2024年度データ漏洩／侵害調査報告書」によると、データ漏洩／侵害の80%が盗まれた認証情報に関連しています。機密性の高い認証情報を保護し、不正アクセスを防止するには、厳格な監視と一貫したセキュリティ対策が不可欠です。

認証情報セキュリティに対するAI主導のリスク:
AIを活用した攻撃(フィッシングキャンペーンなど)は、巧妙で拡張性があり検出困難なため、認証情報の侵害リスクが増大しています。多要素認証(MFA)は必要不可欠ですが、それだけでは不十分です。異常なアクセス時間、ログイン場所、予期せぬデータのダウンロードを追跡する監視機能を追加することで、AI主導の高度な脅威に対抗する多層防御が実現します。Sapios ResearchとDeep Instinctのレポートによると、調査に回答したセキュリティ専門家の75%が、過去1年で攻撃の増加を実感しています。その85%は、原因として生成AIを悪用する攻撃者の存在を挙げています。こうした進化し続ける脅威の状況によって、あらゆる環境で組織のデータを保護するためには効果的なDSPM戦略の導入が不可欠であることを、再認識させられています。

耐量子暗号のリスク:
MicrosoftのMajorana 1チップのような最近の開発動向は、量子コンピューティングが近い将来、RSAやECCなどの非対称アルゴリズムを破るレベルに到達する可能性を示唆しています。Shorのようなアルゴリズムを実行する量子コンピュータによって、これらの暗号方式が破られ、機密データが漏洩するリスクがあります。2025年タレス データ脅威レポートでは、回答者の70%がポスト量子コンピューティングにおける最大の懸念としてHNDL(Harvest now, decrypt later)攻撃を挙げています。つまり、サイバー犯罪者は現時点で暗号化されたデータを収集しておき、将来的に量子コンピューティングが利用可能になった際に解読しようとしているのです。この脅威に備えるには、今のうちに耐量子アルゴリズムを導入し、暗号アジリティを確保する必要があります。

リスクのプロアクティブな検知:
内部脅威(情報漏洩や妨害行為など)はますます巧妙化し、検出が困難になっています。2025年タレス データ脅威レポートでは、外部からの不正アクセスと同等に、従業員による情報漏洩が懸念されています。従来の境界セキュリティでは不十分であるため、強力な監視による効果的なリスク管理が侵害防止には不可欠です。

データガバナンス:
世界のデータ保護規制ではコンプライアンス違反に厳しい罰則が設けられています。機密データの侵害を未然に防ぐためには、行動変化を把握して早期に脅威を特定することが極めて重要となっています。新たな脆弱性や攻撃ベクトルに対処するために、DSPMのような手法を活用し、セキュリティ戦略を進化させる必要があります。

DSPM(Data Security Posture Management)の基本となる5つの重要な問いに対する答え

機密データはどこにあるのか?

機密データの所在を把握することは、データ保護の第一歩です。これには、データベースやスプレッドシートに含まれる構造化データと、メール、文書、マルチメディアファイルなどの非構造化データの両方を特定することが含まれます。これらのデータは多くの場合、オンプレミスのサーバーや複数のクラウドプラットフォーム(AWS、Azure、Google Cloudなど)を含む、さまざまなストレージ環境に分散しています。

重要性

- **適切なセキュリティ対策の実施:**データの種類に応じて、規制要件やビジネスニーズに適合したセキュリティ対策が必要です。
- **データの拡散管理:**データの量が増加し、ハイブリッド環境やマルチクラウド環境に広がる中で、機密データがどこに保存されているかを把握することは、より困難かつ重要な課題となっています。
- **規制遵守:**データ保護法(GDPR、CCPA、HIPAAなど)の遵守には通常、対象データの保存場所を詳細に把握する必要があります。

多くの組織は、自社の機密データがどこにあるのか、あるいは危険な状態にさらされているかどうかを把握できていません。こうした盲点がセキュリティリスクにつながり、不注意なミスを招いたり、隠れた脆弱性や設定ミスのあるデータベースの存在に気付かないまま攻撃者に悪用される機会を生んだりする可能性があります。

今日の多くの企業が、オンプレミスサーバー、複数のパブリック/プライベートクラウド環境、SaaSプラットフォームなど、多様なストレージソリューションを利用しています。これにより、機密データが広範囲に分散し、包括的な追跡と管理が複雑になっています。

また、現在の組織は、構造化データ(データベースなど)と非構造化データ(メールや文書など)を含む膨大なデータを高速なペースで生成、処理しています。こうしたデータのリアルタイムの所在を継続的に監視することは、大きな課題となっています。

さらに、組織内のデータは動的であり、さまざまなアプリケーションやユーザーによって定期的に移動、処理、アクセスされています。このようなデータの絶え間ない移動により、特定の時点での正確なデータの所在を把握することは、高度な監視ツールなしには困難です。

オンプレミス、クラウド、マルチクラウド、ハイブリッド環境にわたるデータエステート全体で、構造化・非構造化データを問わず、すべてのデータストアを自動検出するためには、データ検出と分類の活用が極めて重要です。自動化された検出と分類は、新規または変更されたデータストアを日常的に一貫して検出し分類する唯一の方法です。

誰が機密データにアクセスできるのか?

機密データの不正使用やデータ漏洩を防ぐには、その機密データにアクセス可能なユーザーを制御し監視する必要があります。これには、社内の従業員だけでなく、外部パートナーや関係者のアクセス権限の管理も含まれます。

重要性

- **データ漏洩の防止:**機密データへのアクセスを業務上必要なユーザーに限定することで、内部脅威や外部からの攻撃リスクを低減できます。
- **コンプライアンスのサポート:**多くの法規制では、データへの厳格なアクセス制御が義務付けられています。アクセス可能なユーザーを把握することで、こうした規制へのコンプライアンスを維持するために役立ちます。
- **データ管理の強化:**データへのアクセス状況を監視することで、セキュリティ強化や業務効率の向上に不可欠な監査や使用パターンの追跡が可能になります。

多くの組織では、包括的なツールの不足でデータアクセスの可視性と監視が制限されています。さまざまなシステムやプラットフォームにまたがるアクセスデータを集約して分析する効果的な手段がなければ、機密データへのアクセス状況を正確に把握することは困難です。

現在の企業では通常、RBAC(ロールベースアクセス制御)、ABAC(属性ベースアクセス制御)、その他のモデルなど、複雑かつ階層化されたアクセス構造を採用しています。こうした複雑な仕組みにより、誰が、どのデータに、どのような条件でアクセスできるかを正確に把握することが難しくなっています。さらに、大規模な組織では、部門や部署ごとにそれぞれのITリソースを独自に管理していることが多く、アクセス制御やポリシーに一貫性がありません。このような分散化は、組織全体のデータアクセスの追跡を複雑にし、誰が機密情報にアクセスできるかの可視性をさらに低下させます。

すべてのデータベースにわたってユーザーとその権限をデータベースオブジェクトにマッピングし、セキュリティポスチャを把握するためには、各データストアをスキャンして付与されたユーザー権限を確認し、ユーザー権限に関するさまざまな詳細を可視化する必要があります。

認証情報はどの程度保護されているか?

暗号化されたデータの解読・使用を可能にするメタデータや認証情報(暗号鍵やシークレットなど)に対して適切な保護策を講じることが、極めて重要です。これには、現在だけでなく将来的にもデータを保護できる暗号技術の採用が含まれます。量子コンピューティングにより、悪意のある復号技術の進化が加速すると予想されるためです。

重要性

- **関連メタデータの保護:**暗号化されたデータとは別に、暗号鍵やシークレットを一元管理することで、機密データのセキュリティを一層強化できます。
- **ポスト量子時代への備え:**クリプトアジャイルな製品を導入することで、ポスト量子暗号(PQC)アルゴリズムや暗号鍵の利用が可能になります。
- **認証情報の拡散を防ぐ:**認証情報を保護し、暗号鍵やシークレットの無秩序な拡散を阻止することは、攻撃対象領域の縮小と不正なデータアクセスの防止に不可欠です。

多くの組織がデータ保護の基本的な手段として暗号化を活用していますが、暗号化されたデータを解読し使用するための暗号鍵やシークレットを保護する必要性については見落とされがちです。暗号化されたデータの近くに暗号鍵やシークレットを保管することは、ドアマットの下に家の鍵を置くのと同じように、脆弱性を高めます。

多くの組織は複数のクラウドプロバイダー(CSP)を利用してデータを保管しているため、鍵の作成、管理、ローテーションのプロセスはCSPごとに異なります。導入する暗号化ソリューションの数が増え続けるにつれ、一貫性のないポリシーや異なる保護レベルを管理することになり、コストは増大します。このような複雑な状況を抜け出すための最善の方法は、一元化された暗号鍵管理システムに移行することです。

暗号鍵やシークレットの生成、保管、ローテーション、バックアップ、リカバリ、失効、終了といったライフサイクル全体を一元管理することで、職務分掌を効果的に実現できます。これにより、鍵の作成・管理を行う担当者が保護対象のデータにアクセスできない仕組みが確立され、重要なタスクに関する責任を分担することでリスクが軽減されます。

機密データはどのように使用されているのか?

データのアクセス状況や使用状況を継続的に追跡することは、セキュリティとコンプライアンスの確保に不可欠です。これには、データへのアクセスや変更の背景を理解し、セキュリティ上の脅威を示唆する異常なパターンを検出することも含まれます。

重要性

- **異常検知:**不審なアクセスパターンや予期せぬデータ変更は、データ侵害の初期兆候の可能性があります。
- **監査およびフォレンジック分析:**データの使用状況を包括的に記録することは監査に必要なだけでなく、セキュリティインシデント後のフォレンジック調査においても極めて重要です。
- **データアクセス制御の最適化:**データの使用状況を把握することで、実際のビジネスニーズやセキュリティ要件により適したアクセス制御を実施できます。

効果的なデータ使用状況の追跡には、すべてのデータ操作の詳細かつ正確な記録を提供する、高度な監視・ログ記録ツールが必要です。しかし、多くの企業ではこうしたツールを保有していないか、システム全体で十分に統合されていないため、データ使用状況の可視性にギャップが生じています。

今日の企業は、オンプレミスシステム、複数のクラウドプラットフォーム、さまざまなエンドユーザーデバイスにまたがる、非常に複雑なデータ環境で動いています。それぞれの環境は異なる方式でデータを処理し保管するため、組織全体でデータのアクセス状況や使用状況を正確に把握することが困難になっています。

また、GDPRやHIPAAなどの各種規制では、データアクセスや使用状況の詳細なログ記録が義務付けられています。複数の法域にまたがる規制を遵守することは、機密データの使用状況の追跡をさらに難しくする要因の1つです。

データ保護には、強固なコンプライアンスとセキュリティが不可欠であり、それによってデータの使用状況、脆弱性、アクセス権の可視性を確保します。デジタル経済の発展とともにデータ量が急速に増大する中で、企業はコンプライアンス違反や侵害のリスクを減らすために、データ中心のコンプライアンスとセキュリティソリューションを導入する必要があります。ワークフローの自動化と適切な推奨アクションの提供により、プロセスを効率化し、データリスクが顕在化する前にセキュリティチームがそれを特定できるようになります。

データストアのセキュリティポスチャ(データセキュリティの現状など)はどうなっているのか?

データストアのセキュリティポスチャを評価するには、導入済みのセキュリティ対策の有効性を評価し、脆弱性を特定し、潜在的な脅威の影響を理解する必要があります。

重要性

- **防御の強化:**データセキュリティの脆弱性とギャップを特定することで、積極的な改善策を講じ、侵害の防止につなげることができます。
- **セキュリティリソースの効率的な管理:**セキュリティのどこが最も脆弱なのかを把握することで、リソースを最も必要な場所に効果的に配分できます。
- **レジリエンス(回復力)の確保:**セキュリティポスチャを定期的に評価することで、進化する脅威やビジネス慣行の変化に対応した防御を確保します。

効果的なポスチャ管理には、最新の脆弱性定義を定期的に更新し、それを活用したスキャンを通じて、リソースの評価、脆弱性の特定、リスクの分析を行う必要があります。CISおよびDISA STIGベンチマークに基づく事前定義された脆弱性テストでデータベースをスキャンすることにより、最新の脅威にさらされているデータベースを把握できます。これらのスキャンではCVSSを使用し、ネットワークやデータに発見された脆弱性に基づくリスクを提示し、リスクスコアを割り当てます。CVSSは、「ITの脆弱性の特性と影響を伝えるためのオープンフレームワーク」であり、米国国立標準技術研究所(NIST)がセキュリティコンテンツ自動化プロトコル(SCAP)フレームワークの一環として管理しています。CVSSによる脆弱性のスコアリングは、発見された脆弱性に内在するリスクを測定し、対応の優先順位を決めるための正確なモデルを提供します。

監視は、データ管理ライフサイクルの重要なフェーズであり、リアルタイムの情報を提供します。これには、システムイベント、アラート、違反、ブロックされたソース、ゲートウェイとエージェントのステータス、システム警告、データベース監査情報、ファイルサーバー監査情報、アーカイブ情報などが含まれます。

監視対象のイベント、アラート、違反には、さまざまな側面があります。特定の実装によっては、異なる役割や関連するセキュリティポリシーを持つ複数のタイプのユーザーが存在する可能性があります。事前設定された深刻度評価を使用するか、ポリシーをカスタマイズしてイベントの解釈を微調整し、アラートが誤検知なのか攻撃なのか、それとも別の問題なのかを判断することができます。

リスクを超えてデータを安全に保つ単一のプラットフォーム

データは最も貴重な資産であり、スケールメリットを生み出します。AIのような最新イノベーションを導入すると、これまで以上に膨大なデータが生成されるようになります。データとデータリポジトリの飛躍的な増加は、データの盲点を増やし、情報を危険にさらす脆弱性を拡大させます。データを保護すると同時にその膨大な可能性を活用するためには、機密データを効果的に特定し、そのセキュリティ、ガバナンス、コンプライアンスを強化することが不可欠です。

データエステートを把握する

CipherTrust DSPMは、オンプレミス、クラウド、マルチクラウド、ハイブリッドクラウド環境を含む幅広いデータストアにわたり、構造化データと非構造化データの検出と分類を自動化します。

- **データのスキャンと特定:**CipherTrust DSPMは、オンプレミス、クラウドを問わず、データ環境を体系的にスキャンし、データリポジトリを検出します。これにはデータベース、ビッグデータプラットフォーム、クラウドストレージ、ファイルシステムが含まれます。
- **データの分類:**CipherTrust DSPMはデータを検出後、その種類や機密度に基づいて分類します。この自動分類により、企業は保有するデータを把握し、適切にセキュリティの優先順位を決定することができます。
- **ユーザーアクセスの把握:**CipherTrust DSPMは、ユーザー権限管理を提供し、データアクセスや特権ユーザーのアクティビティを監視することで、過剰な権限、不適切な権限、未使用の権限を特定します。また、セキュリティチームやIT部門に対し、データが組織内でどのようにアクセス、使用、移動されているかの完全な可視性を提供します。

データセキュリティポスチャを強化する

DSPM(Data Security Posture Management)には、包括的なデータ保護戦略が不可欠ですが、軽視されがちです。強固なデータセキュリティポスチャを維持するためには、暗号化と効果的な認証情報管理を通じてデータ保護の強固な基盤を確立することが重要です。CipherTrust DSPMは機密データを特定し、業界をリードする技術を活用して保護します。これにより、認証情報とメタデータの安全性を確保し、ユーザーやアプリケーションによる不正アクセスを阻止し、組織全体のデータセキュリティとコンプライアンスの枠組みを強化します。

- **機密データの保護:**暗号化、データマスキング、トークナイゼーションなどの主要なデータ保護を実装することで、クレジットカード情報、知的財産、個人識別情報(PII)などの機密情報を保護しながら、許可されたアプリケーションや担当者のみが機密データを使用できるようにします。
- **暗号化データを解読するためのメタデータの保護:**暗号化とデータマスキングはデータ保護の第一歩です。しかし、保護されたデータを復号する鍵とシークレットを、一元的な鍵管理を活用して保護することも同様に重要です。これを効果的に行うには、ハイブリッドクラウド環境全体で鍵やシークレットを検出し、インベントリ化する必要があります。
- **ポスト量子時代への備え:**量子コンピュータは、現在一般的に使用されている暗号方式を破る能力を持つため、サイバーセキュリティ上の重大な脅威となります。これは、データ侵害／漏洩、通信の侵害、ブロックチェーンと認証プロトコルの脆弱性につながる可能性があります。この脅威を軽減するためには、耐量子暗号への移行を進め、プロアクティブなセキュリティ対策を講じる必要があります。
- **認証情報の拡散の阻止:**暗号化、トークナイゼーション、データマスキングにより、認証情報が許可された対象者以外に共有されないように保護します。これらの手法はデータの読み取りや使用を不可能にし、機密データを含んだ不正なデータストアの作成を防ぎます。

強固なデータ保護基盤を確立すると、CipherTrust DSPMを通じて、プロアクティブなリスク分析を実施し、管理データに関連するリスクを効果的に特定し、優先順位をつけることができるようになります。このインテリジェントなリスク分析により、脆弱性がどこに存在するかを迅速に特定するための有益な洞察が得られます。この知見を活用することで、リスクを軽減するための戦略計画を実施し、データセキュリティポスチャを大幅に強化し、最も貴重な資産であるデータの安全を確保できます。

- **リスク評価:** CipherTrust DSPMは、データがどのように保存、アクセス、共有されているかを評価することで、データ侵害につながる可能性のある脆弱性、危険な構成、不適切なアクセス制御を特定できます。CipherTrust DSPM はすべての環境にわたるデータセキュリティリスクの一元的なビューを提供するため、機密データの所在、保護レベル、保護方法を確認できるだけでなく、内部脅威の兆候となる鍵やシークレットの不正使用を特定できます。

- **行動変化の特定:**ユーザーとエンティティの行動の変化は、リスクや潜在的な環境脅威の重要な兆候です。AIを活用した脅威が出現する中で、行動分析は、微細な変化を捉えて、最新のフィッシング手口やその他のローアンドスロー攻撃を特定する有効なツールであることが証明されています。
- **AIに起因するリスクの特定:**従業員の業務を支援するためAIの利用が進む一方で、組織は新たなタイプのリスクと向き合う必要があります。未承認のシャドーAIの利用を特定し、AIによる機密データの漏洩を防ぎ、AIの異常行動を検知して対応できるようにすることが極めて重要です。
- **インシデントの関係性の把握:**AI分析を活用し、ユーザーの行動とアプリケーションやデータのコンテキストを統合することで、外部・内部の脅威を理解し、「ローアンドスロー」攻撃に対処します。
- **重点領域の優先順位付け:**カスタマイズ可能なリスクスコアにより、単にリスクを特定するだけでなく、深刻度と影響度に基づいて優先的に対処すべき領域を判断できます。これにより、セキュリティポスチャの改善に最も効果のある分野に効率的に投資することが可能になります。

データセキュリティ運用の継続的な改善

リスクが特定されたら、迅速かつ効果的に対処して是正することが極めて重要です。CipherTrust DSPMはリスクを特定するだけでなく、その緩和方法に関する推奨事項も提示します。プレイブックを通じて、データセキュリティのために、リスクのある行動を示すユーザーの隔離や調査のための脅威チケットの発行といった自動アクションを確立できます。

- **セキュリティ強化の提案:**CipherTrust DSPMは、リスク評価に基づいて、特に強化が求められる領域に対して実行可能な洞察と推奨事項を提供するため、セキュリティ制御を強化できます。
- **セキュリティポリシーの自動化:**CipherTrust DSPMは、複数のプラットフォームにわたるセキュリティポリシーの適用を自動化し、データ資産の保護に必要な手作業を削減します。
- **インシデントの深刻度に応じた優先順位の引き上げ:**CipherTrust DSPMは、システムへの影響とポリシー違反の深刻度を迅速に特定することで、効率的なインシデント管理と問題解決を促進します。

データガバナンスとコンプライアンスの取り組みによって、組織のデータライフサイクル全体を通じて、品質、セキュリティ、可用性を確保するためのポリシーとプロセスが確立されます。CipherTrust DSPMは、データへのアクセス、使用、転送状況の可視性を提供することで、組織がデータセキュリティ戦略とガバナンス／コンプライアンスの整合性を図れるようにします。

- **コンプライアンス対応のサポート:**GDPR、HIPAA、CCPAなどのコンプライアンス規制を満たすためには、機密データが適切に保護され、アクセス制御が正しく実装されていることを保証する必要があります。新たなコンプライアンス要件に対応するには、組織は鍵やシークレットの使用状況を監査できなければなりません。
- **レポートの生成:** CipherTrust DSPMは、監査人やその他のステークホルダーに対するコンプライアンスの証明に使用できる詳細なレポートを提供します。

DSPM ソリューションは機密データを包括的に保護することを目指す組織にとって極めて重要です。これらのソリューションは、効果的なデータセキュリティ戦略を支える基本となる5つの重要な問いに対する答えを提供します。

CipherTrust DSPM: DSPMに不可欠な主要技術の統合

データ検出
CipherTrust DSPMは、オンプレミスからクラウドまで多様な環境にわたる機密データの検出に優れており、重要な情報の特定とマッピングを自動化します。これにより、コンプライアンス管理と侵害防止が強化されます。

データ分類
CipherTrust DSPMは、データを機密性や規制要件に基づいて厳密に分類することで、最適なセキュリティ対策の適用とデータ保護の優先順位付けを実現します。

データ暗号化、マスキング、トークナイゼーション
CipherTrust DSPMは、ITエコシステム全体にわたる保存データと移動中データの保護、匿名化、暗号化を可能にします。また、そのデータを解読する鍵を、完全に管理下に置いて保護することができます。

静的リスク分析
システムの静的リスク分析は、データインフラストラクチャ内の脆弱性を事前に特定するため、攻撃者に悪用される前に潜在的な脅威に対処できます。

評価と漏洩リスクの特定
CipherTrust DSPMは、データアクセスポイントと公開範囲レベルを継続的に監視し、不正アクセスやデータ漏洩を迅速に検出して軽減し、機密情報の完全性を維持します。

高リスクの脆弱性に関するアラート
リアルタイムのアラートシステムが深刻な脆弱性を警告し、潜在的な影響に基づいて問題を優先順位付けすることで、迅速かつ効果的な組織対応を可能にします。

リスクレポートとアセスメント
この機能は詳細なリスクアセスメントとカスタマイズ可能なレポートを提供します。これによりセキュリティポスチャを理解し、脆弱性を特定して事前に緩和対策を講じることができます。

是正ガイダンス
CipherTrust DSPMは、特定されたセキュリティ上の脆弱性に対する是正策を提案し、ベストプラクティスと業界標準に沿った実践的で実行可能なガイダンスを提供します。

エンタープライズ対応
拡張可能なアーキテクチャで設計されたCipherTrust DSPMは、既存の企業システムと円滑に統合し、複雑なデータ環境をサポートしながら、組織の進化するニーズに適応します。

セキュリティおよびオーケストレーションサービスとの統合
CipherTrust DSPMをセキュリティおよびオーケストレーションサービスと統合することでセキュリティ運用を改善し、さまざまなセキュリティツールの同期管理を容易にし、運用効率を高めます。

プレイブックの自動化
CipherTrust DSPM は、プレイブックの自動化を活用し、一般的なセキュリティインシデントに対する標準化された対応を提供します。これにより、脅威管理を効率化し、対応時間と被害を最小限に抑えます。

コンプライアンス監査とレポート
CipherTrust DSPMは、アクセスログからリスク評価まで、データセキュリティ管理のあらゆる側面を文書化する詳細なレポートを提供し、コンプライアンス対応と監査プロセスをサポートします。

タレスについて

今日の企業は、決定的な意思決定を行うために、クラウド、データ、ソフトウェアに依存しています。そのため、世界で評判の高いブランドや最大手の組織は、クラウドやデータセンターからデバイス、ネットワーク全体に至るまで、作成、共有、保存場所を問わず機密情報やソフトウェアを保護し、それらへのアクセスを安全に確保するために、タレスに信頼を寄せています。当社のソリューションは、企業がクラウドに安全に移行し、自信を持ってコンプライアンスを達成し、何百万人もの消費者が毎日利用するデバイスやサービスにおいて、ソフトウェアからより大きな価値を生み出すことを可能にします。