Brochure

THALES
CYBERSECURITY

タレスのデータセキュリティ
プラットフォーム

CipherTrust Data Security Platform

cpl.thalesgroup.com

データセキュリティの 課題

セキュリティ侵害が増加し、規制が強化される中、組織はあらゆる場所に存在する機密データを検出、保護、制御、監視することが急務となっています。オンプレミス環境から、ハイブリッド、マルチクラウド環境に至るまで、現代のITエコシステムは複雑化しており、統合的でスケーラブルなデータセキュリティアプローチが求められています。

タレスのCipherTrust Data Securityポートフォリオは、こうした今日のデータ保護の課題に対応するための包括的かつ一元化されたソリューションを提供し、、以下を実現します。あらゆる環境に存在する機密データを検出し、完全な可視性を確保します。リアルタイムのアクティビティ分析により異常を検知し、コンプライアンスを維持します。強力な暗号化とトークナイゼーションによってデータを保護します。きめ細かなポリシーの適用と鍵管理によりアクセスを制御します。

タレスは、データセキュリティ運用を簡素化して統合することで、効率性を高め、コンプライアンス対応を加速し、リスクを大幅に低減します。オンプレミス、クラウドサービスプロバイダー経由、あるいはタレスによる完全マネージドサービスとして、いずれの形態でも導入可能であり、市場をリードする保護機能、完全な制御、暗号鍵の完全な自社保有を実現します。

検出の課題

機密データの特定：

ファイル、データベース、クラウドストレージ環境全体にわたって機密データを検出し分類します。

鍵およびシークレットの検出:

クラウド上の鍵、シークレット、証明書を自動的に特定し検出します。

データリスクの把握：

機密データの所在とアクセス状況を可視化し、リスク評価や保護対策の優先順位付けに活用できます。

コンプライアンスの効率化:

規制対象データを特定して分類し、監査準備やコンプライアンス要件の遵守を支援します。

課題の分析

監査ログの一元管理:

データアクセスやポリシーアクティビティを統合的に可視化し、SIEMを活用した分析をサポートします。

データ可視性の向上:

環境全体にわたる機密データを検出して評価し、実用的なインサイトを提供します。

暗号化アクティビティの監視:

暗号化の使用状況を分析し、異常を検知して潜在的な脅威を特定します。

保護計画の簡素化:

リスクベースのインサイトを活用し、セキュリティ対策やデータ保護戦略の優先順位付けを行います。

保護の課題

保存データの保護:

強力な暗号化により、オンプレミス、クラウド、ハイブリッド環境にわたる機密データを保護します。

透過暗号化:

アプリケーションへの影響を最小限に抑え、コード変更を必要とせずにデータを保護します。

動的なデータ保護:

保存データ、移動中データを問わず、ライフサイクル全体を通じて保護します。

トークナイゼーションとマスキング:

機密データをトークンに置き換えることでリスクを低減し、不正アクセスを防止します。

一元化された鍵管理:

マルチクラウド環境全体の暗号鍵を一元管理します。

ハイブリッド・マルチクラウドプラットフォームの保護:

AWS、Azure、Google Cloudなどのクラウドプロバイダー全体に保護を拡張します。

22%

自社データがどこに保管されているかを特定する自信がほとんどまたはまったくない。

『2025年データ脅威レポート　金融サービス版』

制御の課題

DevOpsへのセキュリティ統合:

イノベーションを損なうことなく、開発ワークフローにセキュリティを組み込み、データを保護します。

開発段階でのデータ保護:

開発、テスト、デプロイメント環境にわたって機密データを保護します。

運用効率の向上:

ポリシー適用を自動化し、環境全体のセキュリティ運用を効率化します。

データセキュリティプラットフォームとは?

データセキュリティプラットフォームとは、組織全体の環境にわたる機密データを保護するために設計された、包括的なテクノロジー群です。データの検出、分析、保護、制御といった機能を統合することで、クラウド、オンプレミス、ハイブリッド環境にまたがるデータリスクを一貫して管理できるようにします。

データセキュリティプラットフォームは、複数のセキュリティ機能を単一の統合フレームワークにまとめて連携させます。個別の分断されたポイントソリューションに依存するのではなく、一貫したポリシーを適用し、セキュリティプロセスを自動化し、システムやアプリケーション全体で機密データの保存・アクセス・利用状況を可視化できます。

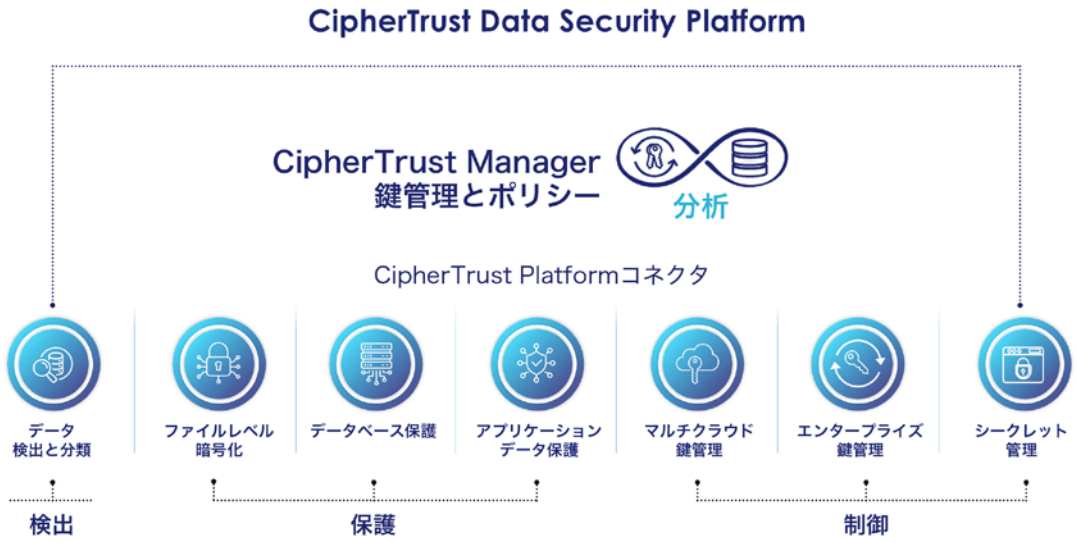
統合的なデータ保護アプローチを提供することで、データセキュリティプラットフォームは、データの所在を問わず、機密情報の検出と適切な分類、保護ポリシーの適用、重要なデータ資産に関するアクティビティの継続的な分析を可能にします。

CipherTrust Data Security Platformとは?

KuppingerColeの2025 Leadership Compass for Data Security Platforms(2025年データセキュリティプラットフォームのリーダーシップコンパス)でリーダーとして認められ、GartnerのMarket Guide to Data Security Platforms(データセキュリティプラットフォームのマーケットガイド)にも掲載されたCipherTrust Data Security Platformは、データセキュリティから複雑さを取り除き、コンプライアンス対応を加速し、クラウドおよびオンプレミス環境を保護するために設計された、包括的で統合されたデータ中心のセキュリティソリューションを提供します。

CipherTrustは、データの検出、分類、保護、分析、そして鍵とシークレットの一元管理を、単一の効率的なプラットフォームに統合します。この統合により、セキュリティチームの運用負荷を大幅に軽減し、一貫したコンプライアンス管理を実現して、組織全体のリスクを最小限に抑えます。

統合されたデータセキュリティアプローチを提供することで、CipherTrust Data Security Platformは、機密データがどこに存在していても、シームレスにそのデータを検出、分類、保護、分析できるようにします。



Data Security Fabricとは?

Data Security Fabricは、複雑で分散した環境全体にわたって機密データを保護するために設計された統合フレームワークです。データがクラウドプラットフォーム、アプリケーション、データセンター、デバイス間を移動する中で、Data Security Fabricはセキュリティ制御、ポリシー、可視性を統一されたアーキテクチャに統合し、データの所在を問わず、一貫したデータ保護を実施できるようにします。

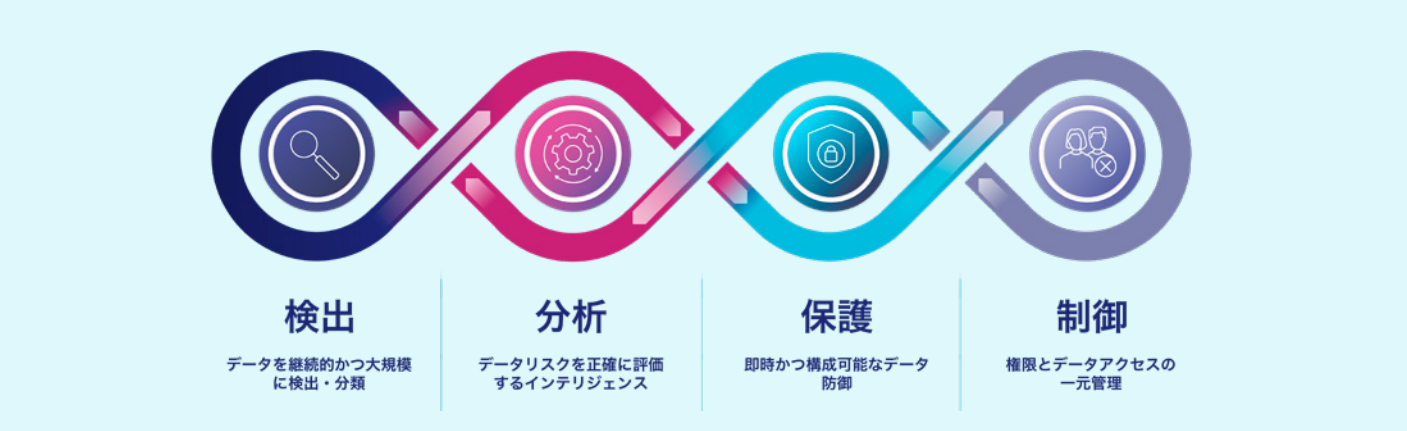
データ検出、分類、暗号化、鍵管理、アクセス制御といった主要な機能を統合することで、Data Security Fabricは、強固なガバナンスとコンプライアンスを維持しながら、データ保護を簡素化します。この統合アプローチにより、運用の複雑さが軽減され、セキュリティチームはハイブリッドおよびマルチクラウド環境全体に一貫した保護を適用できます。

プラットフォーム主導の統合的なデータセキュリティアプローチを通じて、Data Security Fabricは、デジタルエコシステム全体にわたって機密データを検出、分類、保護、監視できるようにし、データの作成、共有、保存、利用の全段階で安全性を確保します。

CipherTrust Data Security Posture Managementとは?

CipherTrust Data Security Posture Management(DSPM)は、機密データの保存場所を問わずその所在を正確に特定することで、データの可視化と保護に向けた包括的かつ統合的なアプローチを提供します。データが複数のクラウド環境、オンプレミスシステム、あるいは増え続けるSaaSアプリケーション内に保存されている場合でも、CipherTrust DSPMは高度なインサイトと制御を提供し、強固なセキュリティ態勢の維持とコンプライアンス要件の遵守を支援します。

業界で実証された長年の専門知識を基盤とするCipherTrust DSPMは、単なるデータ検出にとどまりません。データを継続的に検知して分類しリスクを評価するとともに、高度な保護メカニズムを適用して、最も重要な情報を保護します。強力な監視と分析により、機密データへのアクセス、共有、利用状況を追跡し、潜在的な侵害や不正利用のリスクを低減します。CipherTrust DSPMを活用することで、最も重要な資産であるデータを、ライフサイクル全体を通じて保護するために必要な可視性、インテリジェンス、自動化を実現できます。



Data Discovery and Classification

Data Discovery and Classificationは、セキュリティの強化とコンプライアンス対応の効率化を実現し、コンプライアンス上のギャップやポリシー設定の不備を解消することで、データリスクを最小限に抑えます。単一のソリューションで効率を向上させ、データおよびシークレットの検出とデータ分類を、所在を問わず実行できます。Data Discovery and Classificationは、運用効率の向上、侵害発生時の影響の軽減、開発コストの削減、ツールやストレージにかかるコストの回避を実現します。

Key Management

Key Managementは、暗号鍵の一元管理、きめ細かなアクセス制御、セキュリティポリシーの設定を可能にします。鍵の生成、ローテーション、破棄、インポート、エクスポートといったライフサイクルタスクを管理し、鍵とポリシーに対するロールベースのアクセス制御を提供します。強固な監査とレポート作成をサポートし、開発者向けのREST APIを提供します。また、データ保護コネクタ向けの暗号鍵とポリシーの一元管理を実現します。CipherTrust Managerは、CipherTrust Data Security Platformの中央管理ポイントであり、仮想および物理フォームファクタの両方で提供されます。FIPS 140-2 Level 3まで準拠し、最高レベルの信頼の基点(Root of Trust)のもとで鍵を安全に保管します。

Secrets Management

CipherTrust Secrets Managementは、APIキー、パスワード、証明書、トークンなどのシークレットを安全に保管、アクセス、管理するための一元的なソリューションです。ハードコードされた認証情報を排除し、アクセス制御を適用して、DevOpsおよびクラウドネイティブ環境をサポートします。CipherTrust Data Security Platformと統合されており、ハイブリッドおよびマルチクラウド環境全体で、強固なセキュリティ、監査可能性、スケーラビリティを確保します。

Transparent Encryption

Transparent Encryptionは、保存データの暗号化、特権ユーザーアクセス制御、詳細なデータアクセス監査ログなどの機能を備えています。物理サーバー、仮想サーバー、クラウド、ビッグデータ環境にわたって、Windows、AIX、Linux OS上のファイル、ボリューム、データベース内のデータを保護します。CipherTrust Transparent Encryptionでは、ライブデータ変換(LDT)機能が利用可能であり、システム停止時間ゼロでの暗号化と鍵の再生成を実現します。また、セキュリティインテリジェンスのログとレポートにより、コンプライアンスに関するレポート作成を効率化し、主要なSIEM(セキュリティ情報イベント管理)システムを利用して脅威を迅速に検知します。

Tokenization

Tokenizationは、PCI DSSなどのデータセキュリティ要件への準拠に伴うコストと複雑さを軽減します。ボルトレス型トークナイゼーションにはポリシーベースの動的データマスキングが含まれ、ボルト型トークナイゼーションは環境固有のAPIが追加されています。CipherTrust Data Security PlatformのTokenizationソリューションは、RESTful APIを通じてアプリケーションにトークン化機能を容易に追加できます。

Data Masking

Data Maskingは、データの形式を維持したまま機密情報を難読化することで、コンプライアンス対応を簡素化し、データセキュリティを強化します。静的および動的データマスキングの両方をサポートし、ユーザーの役割に基づいた安全なアクセスを実現します。CipherTrust Data Security Platformと統合されており、ボルトレス型トークナイゼーションとシームレスに連携して動作し、RESTful APIを通じて柔軟なポリシー駆動の保護を実現します。これは、PCI DSSの適用範囲の縮小やデータ漏えいリスクの軽減に有効です。

Database Protection

Database Protectionは、データベースアプリケーションを変更することなく、データベース内の機密フィールドに対するデータ暗号化を、安全で一元化された鍵管理と統合します。CipherTrust Database Protectionソリューションは、Oracle、Microsoft SQL Server、IBM DB2、Teradataデータベースに対応しています。

Application Data Protection

Application Data Protectionは、鍵管理、署名、ハッシュ化、暗号化サービスなどの暗号機能をAPI経由で提供し、開発者がアプリケーションサーバーやビッグデータノードでデータを容易に保護できるようにします。CipherTrust Application Data Protectionは、カスタマイズされたデータセキュリティソリューションの迅速な開発を可能にし、鍵管理の複雑さを開発者の負担から取り除きます。さらに、鍵管理ポリシーをセキュリティ運用部門のみが管理することで、強固な職務分掌を実現します。

File Activity Monitoring

非構造化ファイルのセキュリティは、個人データ、財務情報、企業秘密、知的財産、その他の重要な情報など、機密情報への、権限のない個人や組織によるアクセスを防止するために不可欠です。File Activity Monitoring(FAM)は、さまざまな場所に保存された非構造化データや暗号化データへのアクセスを継続的に監視します。高度な機械学習技術を活用することで、組織はファイル共有やSaaSアプリケーション内の企業データを保護できます。AIデータセキュリティアシスタントは、FAMに統合された生成AI搭載のチャットボットであり、手作業の負荷を大幅に削減し、対応速度を向上させ、複雑なデータアクセス履歴を数秒で明確かつ実用的なインサイトに変換します。この技術により、ユーザーはアクセス権の特定、ファイル権限の確認、機密ファイルの迅速な把握、異常なアクティビティに関する分析やアラートを通じて、インシデント対応やフォレンジック調査を強化できます。

Data Activity Monitoring

タレスは、オンプレミスのデータリポジトリ、ハイブリッド環境、マルチクラウド環境にわたるすべてのデータ資産に対して、Data Activity Monitoring(DAM)を提供します。アプリケーションユーザーや特権ユーザーによる操作を含め、すべてのデータアクティビティをリアルタイムに監視・監査します。この可視性により、誰がいつデータにアクセスし、どのような操作を行ったかを把握できるため、潜在的なセキュリティ脅威を未然に防ぎ、機密データやビジネスクリティカルなシステムに広範なアクセス権を持つ特権ユーザーアカウントをブロックすることが可能になります。

Data Risk Analytics

タレスのリスク分析機能は、データ資産やクラウドサービス全体にわたるセキュリティ脅威や悪意のあるアクティビティを特定するのに役立ちます。これにより、不正アクセス、不審なデータ転送、異常な動作を検知し、その影響を評価して、リスク軽減のための戦略を提示できます。Data Risk Analyticsのポリシーベース検知は、アラートの優先順位付けを行い、ユーザーやアプリケーションによるデータへのさらなるアクセスをブロックします。また、低リスクのイベントをフィルタリングすることで、セキュリティチームが真の脅威に集中できるようにします。

Data Risk Intelligence

タレスのData Risk Intelligenceは、重大度と発生可能性に基づくデータリスクの優先順位付けを可能にします。ユーザー権限、データの脆弱性、暗号化基準、不審なアクティビティを分析し、リスクスコアと実用的なインサイトを提供します。インシデントモデリングとリスク優先順位付けを組み合わせることで、経営層は自社のセキュリティ態勢を把握し、セキュリティ脅威を効果的に管理できます。ML/AI分析を活用し、脆弱性スキャン、権限評価、構成管理から得られるリスク指標を統合することで、ビジネスリーダーは高精度なリスクプロファイルを取得し、セキュリティポリシーの適用やセキュリティギャップの修復を行うことができます。

Data Security Posture Management

データがハイブリッド／マルチクラウド環境全体に広がる中、新たな脆弱性から機密情報を保護するためには、データセキュリティを動的に管理する必要があります。CipherTrust Data Security Posture Management(DSPM)は、データの検出、分類、保護、リスク評価を自動化し、データ保護のベストプラクティスへの準拠を確保するとともに、機密データの所在やアクセス制御の可視性を提供します。DSPMは脆弱性を迅速に特定し、アラートを生成し、データセキュリティリスクに対処するための修復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の統合やコンプライアンス報告の効率化を通じて、強固なデータセキュリティ態勢を維持し、規制要件を満たせるよう支援します。

タレスについて

タレスはデータセキュリティのグローバルリーダーとして、世界中で高い信頼を得ているさまざまな組織が、あらゆる場所で重要なアプリケーション、機密データ、およびIDを包括的に、かつ最高の投資対効果(ROI)で保護できるよう支援しています。フォーチュン・グローバル500企業の58%を含む3万社以上の顧客を抱え、そのソリューションは世界148カ国で導入されています。タレスは、革新的なサービスと統合プラットフォームを通じて、リスクの可視化、サイバー攻撃の防御、そしてコンプライアンスギャップの解消を可能にし、毎日数十億人の消費者に安心で信頼性の高いデジタルエクスペリエンスを提供します。

皆様が信頼を寄せている企業は、タレスの力を活用しています。

- Fortune Global 500企業の58%が採用
- 30,000社以上の顧客
- タレスのソリューションは148カ国で導入
- 世界6,700社以上のリセラー、システムインテグレーター、ディストリビューター、マネージドサービスプロバイダー、テクノロジー企業がタレス アクセラレートパートナー ネットワークに参加

THALES

Building a future we can all trust

お問い合わせ先

連絡先情報につきましては、
cpl.thalesgroup.com/contact-us をご覧ください。

cpl.thalesgroup.com