

CipherTrust Transparent Encryption (通過的暗号化)

高度な保存データ暗号化、強力なアクセス制御、詳細なデータアクセス監査ログにより、機密データを確実に保護します。信頼性の高いハードウェアアクセラレーション暗号化ソリューションによって、物理環境、仮想環境、クラウド環境全体でファイル、ボリューム、接続されたクラウドストレージを保護し、コンプライアンスを達成してベストプラクティスに準拠できます。

課題：変化する環境と増大する脅威の中で機密データを保護する

機密データを保護するには、データセンターのオンプレミス環境にあるデータベースやファイルを保護するだけでは不十分です。現在の一般的な企業は、3社以上のIaaSまたはPaaSプロバイダー、50以上のSaaSアプリケーション、ビッグデータ環境、コンテナ技術、自社の仮想環境やプライベートクラウドを利用しています。

問題をさらに複雑にしているのは、サイバー攻撃が高度化し、攻撃力も増していることです。さらに、機密情報の保護に関する新たなコンプライアンスや規制要件が次々と導入され、既存の規制もさらに厳しくなっています。

ソリューション：CipherTrust Transparent Encryption

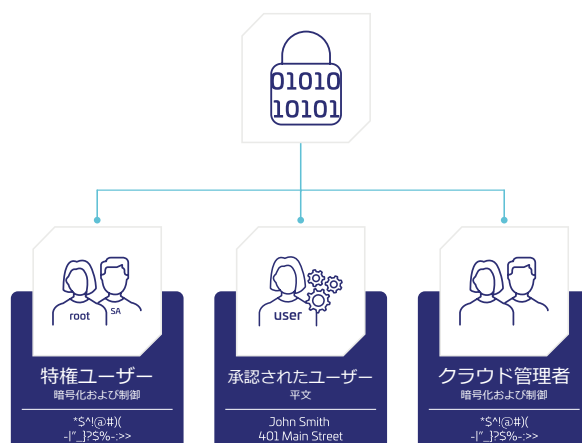
FIPS 140-3 L1 認証を取得したCipherTrust Transparent Encryptionエージェントは、オペレーティングファイルシステムまたはデバイス層に常駐し、その上で動作するすべてのアプリケーションに対して暗号化と復号化を透過的に実行します。CipherTrust Transparent Encryptionは、充実したアクセス制御機能を備えており、誰が、いつ、どのような権限でデータにアクセスできるかを細かく制御できます。

機密性の高い保存データを保護するための主要要件：

- **コンプライアンスとベストプラクティスに準拠：**実績のあるハードウェアアクセラレーション暗号化ソリューションにより、暗号化、アクセス制御、データアクセスログに関する要件を満たします。物理環境、仮想環境、クラウド環境全体でファイル、ボリューム、接続されたクラウドストレージを保護しつつ、詳細なアクセス制御と監査ログを実現します。
- **シンプルかつスケーラブルな導入：**複数のクラウド、オンプレミス、ビッグデータ、コンテナ環境にわたって容易にスケールするソリューションを迅速に導入できます。一元的な鍵管理、暗号化、アクセスポリシーにより、運用が効率化されます。
- **特権ユーザーアクセス制御：**管理者の通常業務を妨げずに、ユーザーやグループ内の潜在的な脅威による不正アクセスを防ぎ、機密データを保護します。
- **実用的なセキュリティインサイト：**詳細で実用的なセキュリティイベントログを活用することで、ファイルアクセスの状況を把握できる有益なインサイトを得られるため、潜在的な脅威を迅速に検知して阻止できます。

CipherTrust Transparent Encryptionエージェント

特権ユーザーアクセス制御を提供



- **幅広いプラットフォームのサポート：**Linux、FreeBSD、AIX、Windowsシステムにわたり、構造化データと非構造化データの両方を保護します。S3バケットに保存されたデータにも透過的な暗号化とアクセス制御を拡張できます。
- **暗号化や鍵の再生成時のダウンタイムなし：**Live Data Transformationコネクタを使用することで、初期暗号化や鍵の再生成時のダウンタイムがなくなります。これは、他のソリューションにはない独自の機能です。

主な特長

透過的なデータ保護：アプリケーション、インフラ、システム管理タスク、ビジネスプラクティスを変更することなく、ファイルレベルの暗号化を継続的に適用することでユーザーやプロセスによる不正アクセスからデータを保護します。すべてのアクティビティについて、詳細なデータアクセス監査ログを作成します。

シームレスかつ容易な導入：CipherTrust Transparent Encryptionエージェントは、サーバーのファイルシステムまたはボリュームレベルに導入され、ローカルディスクに加えてAmazon S3やAzure Filesなどのクラウドストレージ環境もサポートします。

きめ細かなアクセス制御の定義：きめの細かな最小権限のユーザーアクセスポリシーを適用することで、外部からの攻撃や特権ユーザーによる不正使用からデータを保護します。システム、LDAP/Active Directory、Hadoop、コンテナ内のユーザーやグループに対して、個別にポリシーを適用できます。また、プロセス、ファイルタイプ、時間帯、その他のパラメータに基づくアクセス制御にも対応します。

高性能なハードウェアアクセラレーション暗号化: CipherTrust Transparent Encryptionは、データ暗号化用のAES(Advanced Encryption Standard)や鍵交換用のECC(楕円曲線暗号)など、標準ベースの強力な暗号化プロトコルを採用しています。最新のCPUに搭載されたAESハードウェア暗号化機能を活用して、暗号化のオーバーヘッドを最小限に抑えています。また、CTEは安全な通信を実現するため、ポスト量子暗号(ML-KEM)にも対応しています。

包括的なセキュリティインテリジェンス: コンプライアンス要件を満たすだけでなく、データセキュリティ分析にも利用できる詳細なデータアクセス監査ログにより、脅威を迅速に検知して阻止します。さらに、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出します。

幅広いシステムと環境のサポート: Windows、Linux、AIXなど多様なプラットフォームに対応しています。基盤となるストレージ技術に関係なく、物理、仮想、クラウド、Kubernetes、ビッグデータ環境で使用できます。

高度なセキュリティ機能

クラウドおよびコンテナ環境との統合: 動的なクラウドおよびコンテナ環境のデータを保護します。

鍵ローテーション: 暗号化鍵を自動的にローテーションし、セキュリティを強化します。

データ消去: 不要になった機密データを確実に完全消去します。

ゼロダウンタイムのデータ変換: Live Data Transformation オプションにより、初期暗号化や定期的な鍵再生成時のダウンタイムがなくなります。この特許技術により、アプリケーションをオフラインにすることなく、データ使用中にデータベースやファイルを暗号化したり、新しい暗号鍵で再暗号化したりすることができます。

SAP HANAおよびTeradata認定: CipherTrust Transparent Encryptionは、SAP HANAとTeradata データベースについて、SAPおよびTeradataの認定を受けており、データ暗号化、鍵管理、特権ユーザーアクセス制御、きめ細かなファイルアクセス監査ログを提供します。

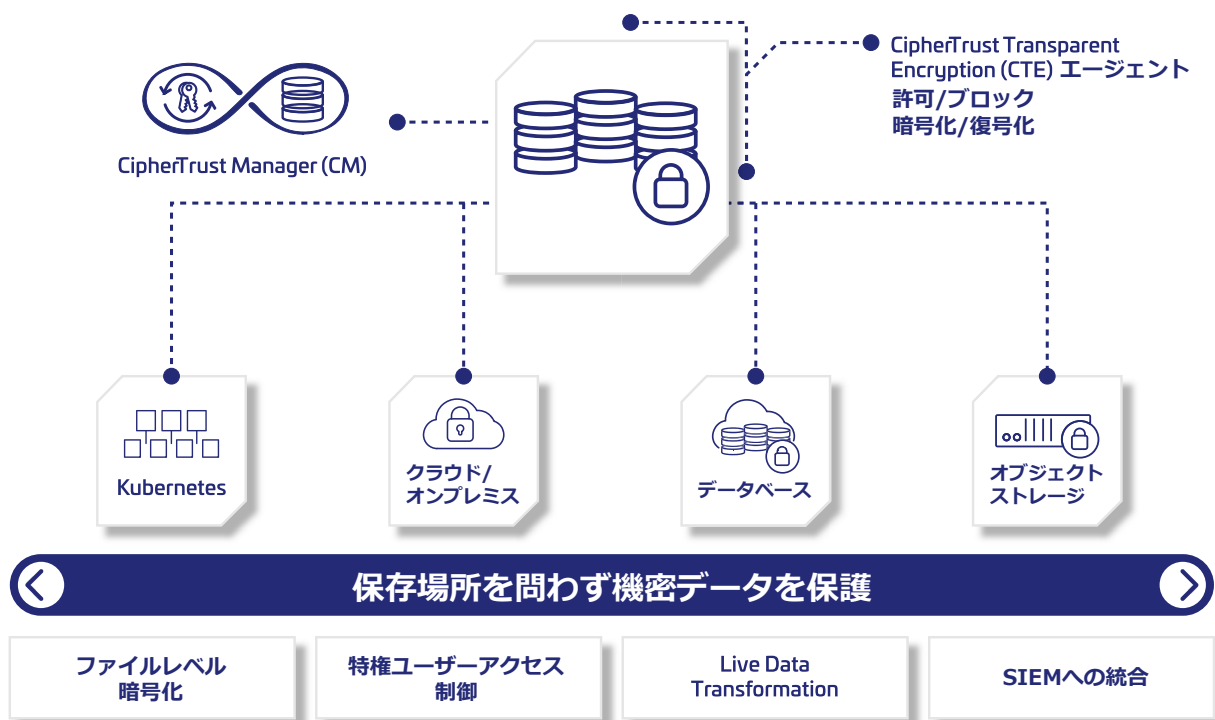
CipherTrust Transparent Encryption Userspace: Linux FUSEを基盤としたスケーラブルで強力なファイル暗号化ソリューションを提供し、Linuxサーバーのカーネルアップグレードの影響を受けません。

AIセキュリティ: CipherTrust Transparent Encryptionは、AIおよびLLMアプリケーションの機密データを保護し、AIワークフロー全体でのコンプライアンス維持を支援します。

ソリューションアーキテクチャ

このアーキテクチャは、CipherTrust Transparent Encryption コネクタとCipherTrust Managerアプライアンスで構成されています。ポリシーと鍵は、CipherTrust Managerで一元管理されます。CipherTrust Managerは、FIPS 140-2 Level 1、またはHSMを備えFIPS 140-2 Level 3に準拠したアプライアンスとして利用可能です。

あらゆる場所に存在する保存データを保護



CipherTrust Transparent Encryption のメリット:

データセキュリティの強化:

保存データ暗号化: 基盤となるストレージが侵害された場合でも、機密データを不正アクセスから保護します。

鍵の一元管理: 暗号鍵を安全に一元管理し、鍵の漏えいリスクを低減します。

特権ユーザーアクセス制御: 特権ユーザーであっても暗号化データへのアクセスを制御し、データの機密性を確保します。

コンプライアンスの強化:

詳細なデータアクセス監査ログ: 包括的な監査証拠を提供し、PCI DSS、HIPAA/HITECH、GDPRなどのコンプライアンス要件の遵守を支援します。

強力なデータ保護: 全体的なデータセキュリティ態勢を強化し、データ侵害や規制罰金のリスクを低減します。

運用効率の向上:

透過的な暗号化: アプリケーションやユーザーのワークフローを変更することなくデータを暗号化し、業務への影響を最小限に抑えます。

スケーラビリティ: 多様な環境にわたる大量のデータを保護するために容易に拡張でき、管理を簡素化します。

柔軟な導入オプション: さまざまなユースケースに対応できる柔軟な導入形態をサポートします。

その他のメリット:

クラウドおよびコンテナ環境との統合: 動的なクラウドおよびコンテナ環境のデータを保護します。

鍵ローテーション: 暗号鍵を自動的にローテーションし、セキュリティを強化します。

データ消去: 不要になった機密データを確実に完全消去します。

これらのメリットを活用することで、CipherTrust Transparent Encryptionは、組織が機密データを保護し、コンプライアンス要件を満たし、運用効率を維持できるよう支援します。

CipherTrust Data Security Platform

CipherTrust Transparent Encryptionは、CipherTrust Data Security Platformの一部です。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の複雑さを解消し、コンプライアンス達成までの時間を短縮し、クラウド移行を安全に実現する、データ中心のソリューションを包括的に統合したプラットフォームです。

CipherTrust Platformは、データの検出・分類・保護、また鍵とシークレットの一元管理を、単一のプラットフォームに統合します。これにより、セキュリティ運用に必要なリソースを削減し、全社的に一貫したコンプライアンス管理を実現して、ビジネス全体のリスクを大幅に低減します。

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。