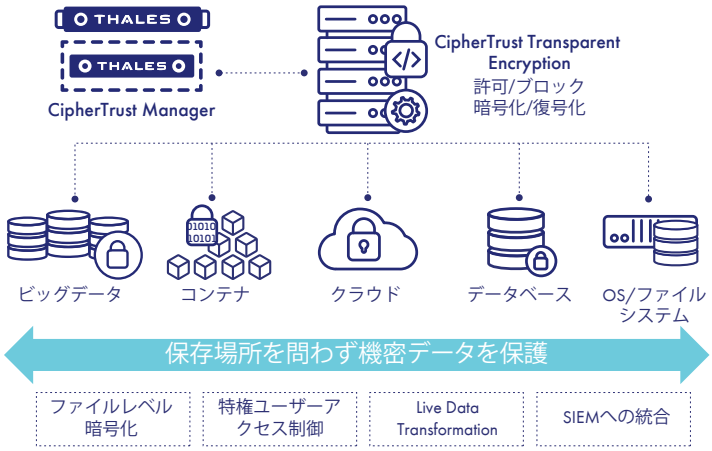
cpl.thalesgroup.com

THALES
Building a future we can all trust

CipherTrust Transparent Encryptionで様々な場所に保管されているデータを保護すべき１０の理由

企業が使用し、保存しているデータの量は、この1年間だけでも大幅に増加していると考えられます。また、各地域や国のさまざまなプライバシーに関する法律や規制を遵守することは、より複雑で困難になっています。毎日のように新たなデータ侵害が報告されており、評判や収益が損なわれています。データ保護のために使用可能なオプションは数多くあります。特に展開を急ぐべき理由がある場合には、機密資産を保護するためにアプリケーションの変更を必要としない、シームレスなアプローチを見つけることが極めて重要です。理想的には、合理的なワークフローで機密データを検出し自動保護することです。

CipherTrust Transparent Encryption なデータアクセス監査ロギングを備えた保存データ暗号化を提供します。これにより、データがオンプレミス、マルチクラウド、ビッグデータ内、コンテナ環境のいずれに保存されていても、データは保護されます。展開はシンプルでスケーラブルかつ迅速に行われます。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インストールされ、その上で実行されるすべてのアプリケーションに対して暗号化と復号化が透過的に実行されます。CipherTrust Transparent Encryptionは、最小限の中断、労力、コストで、データセキュリティのコンプライアンス要件とベストプラクティス要件に対応します。タレスのデータ検出と分類ソリューションとシームレスに連携するように設定でき、1ステップで検出と保護の統合を可能にし、迅速なコンプライアンス対応とリスク軽減を実現します。タレスが提供するソリューションの利点をより理解しやすくするため、CipherTrust Transparent Encryptionを使用すべき理由トップ10をまとめました。



透過的な動作

1 バックグラウンドでシームレスに動作

どのようなデータ保護システムも、展開と使用が容易でなければ、組織にとって望ましくない（そして潜在的にコストのかかる）邪魔な存在となってしまいます。

CipherTrust Transparent Encryptionを展開してファイルやフォルダ内のデータを暗号化するために、アプリケーションに変更を加える必要はありません。CipherTrust Transparent Encryptionは、保存データに対する高速で透過的なファイルレベルの暗号化を提供します。迅速かつシームレスに動作し、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または復号化プロセスが透過的に実行されます。重要なのは、ビジネスプロセス、ユーザータスク、管理ワークフローを妨げないということです。

2 あらゆる場所でデータを保護

データは多様な形式でさまざまな場所に存在する可能性があり、データフットプリント全体の一部だけを保護しても、データ侵害から身を守ることはできません。

CipherTrust Transparent Encryptionを使用すると、データがどこに保存されていても暗号化できます。オンプレミス、クラウド、ビッグデータ、コンテナ環境をサポートし、広範囲にわたる構造化データと非構造化データに対応できます。重要なものが保護機能の範囲外に置かれることはありません。

セキュリティの強化

3 ランサムウェア攻撃の軽減

ランサムウェアとは悪意のあるマルウェアの一種で、サイバー犯罪者は被害者が身代金を支払うまで、ビジネスクリティカルなファイル、データベース、またはコンピュータシステム全体にアクセスできないようにします。これは、サイバー恐喝の一種です。

アクセスポリシーを定義して、「信頼できる」アプリケーションのホワイトリストを作成し、信頼できないバイナリ（ランサムウェアなど）がCipherTrust Transparent Encryptionで保護されたデータストアにアクセスすることを防ぎ、また特権ユーザーがファイルやデータベースのユーザーデータにアクセスすることを防止できます。これらのアクセスポリシーにより、侵入者がそのバイナリの実行権限と、ビジネスクリティカルなデータを含むターゲットファイルの読み取り/書き込み権限を持っていても、不正なバイナリによるファイル/データベース/デバイスの暗号化を阻止できます。CipherTrust Transparent Encryptionは、保護されたフォルダ/ファイル/デバイスを管理者が読み書きできないようにすることで、権限昇格攻撃を阻止できます。

4 不正なデータアクセスの防止

データを暗号化すればそれで終わりというわけではありません。権限のある個人に、データにアクセスして読み取りできるアクセス権を提供する必要があります。

そこで、CipherTrust Transparent Encryptionの中核にあるロールベースのアクセスポリシーが役立ちます。ロールベースのアクセスポリシーにより、誰が、どこで、いつ、どのように、どのデータにアクセスできるかを制御できます。アクセス制御は、システムレベルのユーザーやグループのほか、LDAP、Active Directory、Hadoop、コンテナのユーザーやグループが利用できます。特権ユーザーアクセス制御を容易に実装できるため、管理者の通常業務を妨げずに、データへの脅威となる可能性があるユーザーやグループからデータを保護できます。

容易な展開

5 システムのダウンタイムの回避

データを保護するためとはいえ、何時間も何日もシステムをオフラインにするわけにはいきません。

CipherTrust Transparent Encryptionは、暗号化操作にエージェントを利用します。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インストールされます。これは非常にスケーラブルで透過的なプロセスであり、システムやアプリケーション（パフォーマンスを含む）に影響を与えることなくバックグラウンドで実行されます。インストールプロセス中に何もオフラインにする必要はありません。選択したデータの暗号化を開始する準備ができると、ダウンタイムなしのデータ変換機能が計り知れない価値を発揮します。Live Data Transformationオプションを使用することで、初期暗号化操作時のシステムのダウンタイムが完全になくなるため、チームの通常業務を妨げずに、サイズに関係なくデータを保護できます。

6 主要なプラットフォームとオペレーティングシステムをすべてカバー

組織で使用しているさまざまなプラットフォームすべてにわたってデータを保護できるようにすることは、暗号化ソリューションを選択する上で重要な検討事項です。

CipherTrust Transparent Encryptionは、特定のオペレーティングシステムカーネルごとに緊密な統合と最適化を提供します。AMD、Intel、IBMの一部の最新CPUに組み込まれた暗号化機能を利用することで、ハードウェアアクセラレーションによる暗号化を活用し、パフォーマンスを向上させます。BYOE（Bring Your Own Encryption）は、このソリューションと合わせて容易に導入できます。Amazon S3バケットやAzure Disk and File Storageなどの最新のクラウドアプローチに加え、主要なプラットフォームやオペレーティングシステムをすべてサポートしています。CipherTrust Transparent Encryptionコネクタの一連の拡張機能（Live Data Transformation、SAP HANA、Efficient Storage、Teradata Protection を含む）は、すでに使用または検討されている特定のプラットフォームや構成に対して最適化された暗号化サポートを提供します。

7 内部と外部の両方の鍵を組み込み

他のシステムのすでに存在する暗号鍵や、サードパーティから提供された暗号鍵を使用しなければならない場合があります。選択したデータ暗号化ソリューションに柔軟性がなければ、重大な問題が発生する可能性があります。

CipherTrust Transparent Encryptionは、可能な限り柔軟に設計されています。なにより、すべての鍵をCipherTrustプラットフォームで作成する必要がありません。自社（または信頼できるサードパーティ）がCipherTrust Data Security Platformの外部で生成した鍵も利用できます。そうした鍵をインポートして、プラットフォームで生成された鍵の代わりに使用できます。最終的な結果は同じです。高速で透過的かつ安全なデータ保護が可能です。

迅速なコンプライアンス対応

8 統合された検出と保護の促進

機密データは、検出後に迅速に保護できなければ脆弱なままとなり、データプライバシーに関する法律違反や規制違反となる可能性があります。異なるベンダーのデータ検出と保護ツールを組み合わせて使用すると、複雑さが増し、多くの場合、運用コストが高くなります。

CipherTrustプラットフォームは、CipherTrust Data Discovery and ClassificationとCipherTrust Transparent Encryptionを緊密に統合した、インテリジェントな保護を提供します。これにより、手動で介入することなく、1ステップで自動的にデータを検出して保護することができます。CipherTrust Managerを使用して検出コネクタと保護コネクタの両方を構成および管理するこのプラットフォーム機能は、CipherTrust Intelligent Protectionとして知られており、データを保護しリスクを軽減する実証済みのソリューションです。

9 コンプライアンスレポートの簡素化

データの取り扱いがさまざまな法律や規制に準拠していると証明することは、特に手動のアドホックなアプローチを採用している場合、負担の大きい作業となります。

ご想像のとおり、CipherTrust Transparent Encryptionは、データがコンプライアンスに準拠していることを証明する必要がある場合に、その作業を容易にするさまざまな機能を備えています。コンプライアンス規制の一環として監査人から求められるレポートの作成を支援します。暗号化ソリューションで生成されたログファイルを、選択したSIEM（System Information and Event Management）ソリューションにエクスポートできます。syslog、CEF（Common Event Format）、LEEF（Log Event Extended Format）など、標準的なログフォーマットをサポートしています。すべてのアクセスと暗号化の試行（成功または失敗）がログに記録されるため、必要に応じて内部および外部の監査人に全体像を提示できます。

10 ビジネス継続性の支援

日々のビジネスの妨げとなるような暗号化ソリューションが、大幅に採用されることは考えられません。

CipherTrust Transparent Encryptionを展開することで、ビジネスを中断することなく機能を継続できるようになります。たとえば、このソリューションは、メタデータを平文のままにしてファイルを暗号化するように設定できます。プライバシーとセキュリティの要件に違反することなく、管理者とシステムレベルのユーザーのビジネス継続性をサポートします。幅広いアクセス制御ポリシー設定により、すべてのデータユーザーの特定のニーズに対応するために、きめ細かなアプローチを実装できます。タレスのソリューションを使用することで、データの完全性、セキュリティ、可用性が保証されます。

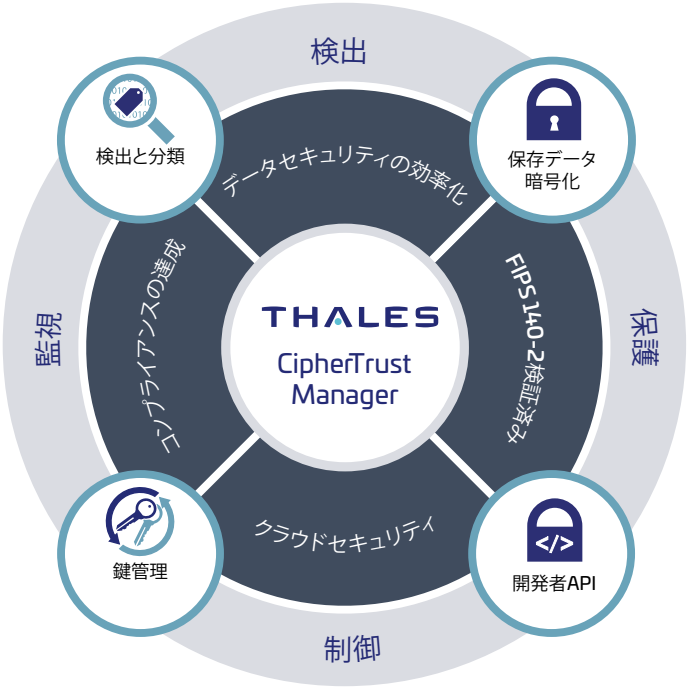
CipherTrust Data Security Platform

CipherTrust Transparent Encryptionは、CipherTrust Data Security Platform の一部です。CipherTrustプラットフォームは、データ検出、分類、データ保護を統合して、これまでにないきめ細かなアクセス制御を提供し、一元的に鍵管理が行えます。これにより、データセキュリティの運用効率化、迅速なコンプライアンス準拠、クラウド移行の保護、ビジネス全体のリスク軽減が可能になります。

タレスについて

皆様がプライバシー保護を信頼して任せている相手は、そのデータを保護するためにタレスに頼っています。データセキュリティに関しては、組織が直面する決定的な局面は次々と増え続けています。その局面が暗号化戦略の策定、クラウドへの移行、コンプライアンス要件の順守のいずれであっても、デジタルトランスフォーメーションを保護するためにタレスに頼ることができます。

決断の瞬間のための、確実なテクノロジー。



THALES

Building a future we can all trust

お問い合わせ

すべてのオフィスの所在地と連絡先情報につきましては、
cpl.thalesgroup.com/ja/contact-us をご覧ください。

> cpl.thalesgroup.com/ja <