cpl.thalesgroup.com

THALES

機密データ保護に必用とされる組織の重要な柱とは

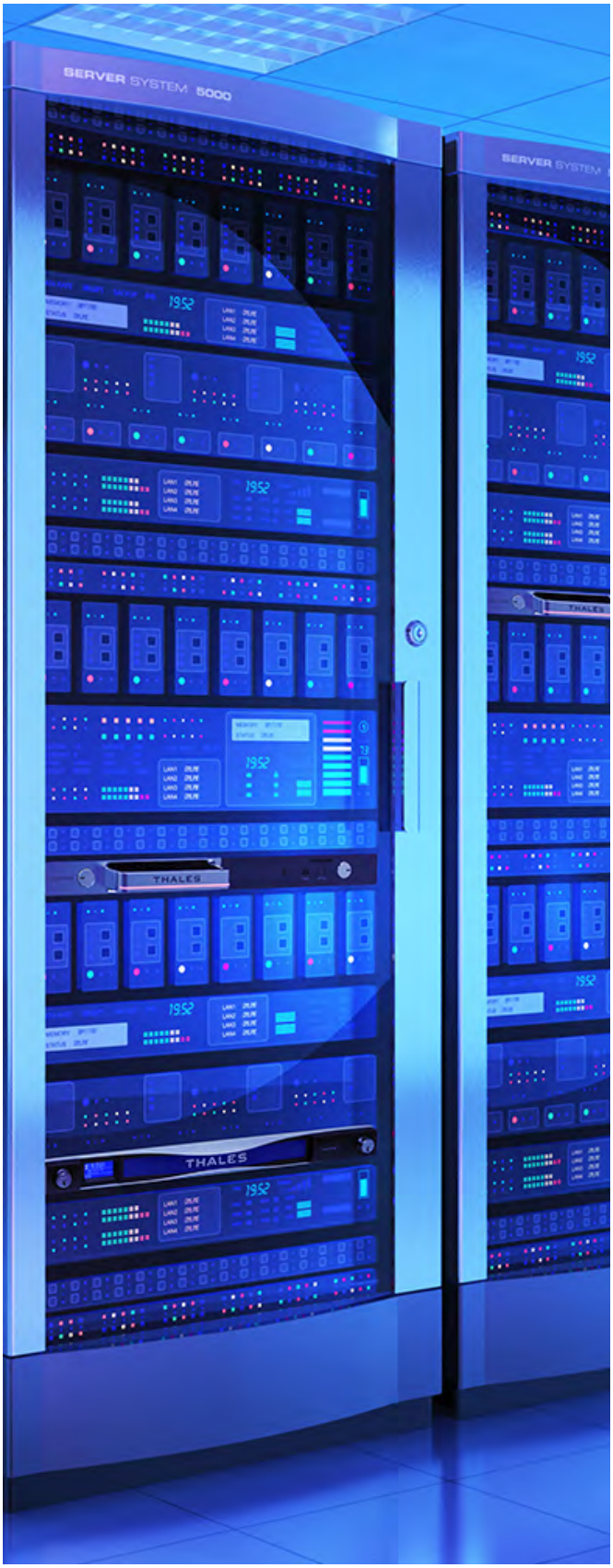
ホワイトペーパー

目次

概要

従来、組織のITセキュリティは主に境界防御に焦点を置き、壁を築くことで外部からの脅威がネットワークに侵入するのを防いでいました。これは依然として重要ではあるものの、十分ではありません。サイバー犯罪者は境界防御を頻繁に突破しており、データはこうした防御の外側のクラウドなどに存在することが多いため、組織は場所を問わずにデータを保護するデータ中心のセキュリティ戦略を適用する必要があります。今日のデータ急増や、世界と地域のプライバシー規制の進化、クラウド導入の拡大、APT（持続的標的型攻撃）などに対応するため、データ中心のセキュリティを適用すれば、場所を問わずにデータを制御して、データ窃盗犯が判読できないようにすることができます。ただし効果を発揮させるには、ユーザーの介入に頼らず自動的にデータが保護されなくてはなりません。

本ホワイトペーパーでは、このデータ急増の時代におけるデータセキュリティの課題について概説します。また、重要なデータを検出および分類し、データ中心のセキュリティを適用する戦略についても説明します。



データの急増、規制の増加、サイバー犯罪者の高度化

従来からある多くのデータセキュリティアーキテクチャは、データがデータセンターに存在し、オンプレミスで利用されることを想定して構築されています。従来のIT環境はエンドツーエンドでIT部門によって制御されていました。IT部門は、インフラストラクチャ、セキュリティ、アプリケーションを所有して運用し、ひいてはデータとユーザーの両方を膨大に把握して制御していました。データやアプリケーションへのすべてのアクセスは、ファイアウォール、次世代ファイアウォール、VPN、アンチウイルス、侵入防止システムといった境界セキュリティの層を通過していました。

本当に重要なものを防御するために境界を越えてセキュリティを展開

従来のデータセキュリティアーキテクチャ

信頼できる境界に基づいたセキュリティ

データ中心のセキュリティアーキテクチャ

場所を問わずデータを保護するセキュリティ

しかし、現代の組織には、このような関所はもはや存在しません。データセンターの周囲の境界がどれほど強力であっても、それによって提供されるセキュリティは概念的なものにすぎません。理由は次のとおりです。

1. 境界セキュリティはデータの移動と急増に未対応

クラウドサービス、ビッグデータ環境、IoTテクノロジーの普及により、膨大な量のデータが非常に高速かつ頻繁にサードパーティのインフラストラクチャやパートナーへと移動しています。これにより、多くの課題が生じています。

- 構造化、半構造化、非構造化データを含む、多様なデータフォーム。
- 境界セキュリティのチョークポイント。これはサービスレベルアグリーメント（SLA）に違反するレイテンシとパフォーマンスのボトルネックを発生させるため、ユーザーは多くの場合、クラウドサービスに直接アクセスします。
- あらゆる場所にいる内部者。内部者はもはや境界の内側にいる従業員ではありません。データは請負業者、サービスプロバイダー、その他のサードパーティの手の中にあります。こうした「内部者」は、自社で検査していない、監視できない、制御下にいない個人です。

2. 運用の複雑さと規制

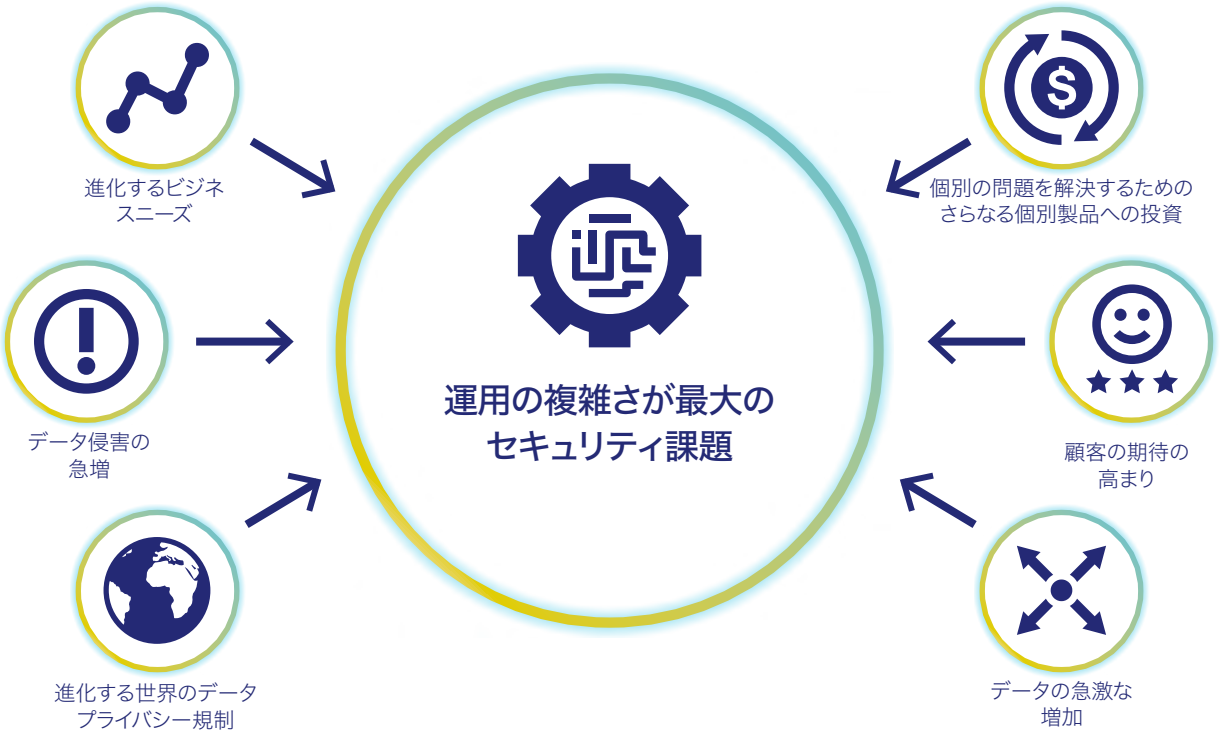
クラウドへのデータ移行、コンテナ、ビッグデータテクノロジー、複数ベンダーのさまざまなツールにより、複雑さが増しています。セキュリティ境界はますます曖昧になっており、分散したITリソースに一貫した統一ポリシーを適用、実装、管理するという課題に組織は直面しています。どの組織にも、古いプラットフォームと新しいプラットフォームが混在しています。

データの急激な増加は、コンプライアンス要件の異なる世界と地域のプライバシー規制の増加によって、さらに複雑になっています。サイロ化された従来のアプローチに依存してデータを保護しても、もはや効果的に準拠することはできません。

こうしたあらゆる要因から、今日のデータ環境はますます複雑化しています。そのため、運用の複雑さがデータセキュリティ導入の最大の障壁であると組織が考えるのも無理はありません。最高情報セキュリティ責任者（CISO）と最高データ責任者（CDO）は、保存場所や使用場所に関係なく機密データの強力な保護を実現する包括的な統合データセキュリティソリューションの必要性を強く認識するようになっています。

従来のデータセキュリティアーキテクチャでは、現代のデータ中心の世界の多くの特性に対応していないため、強硬化する攻撃者による高度なデータ侵害から組織を保護することができません。現代のCISOとCDOは、手段や対策の保守的なサイクルを断ち切りたいのなら、セキュリティに対してまったく新しいアプローチを取る必要があります。

運用の複雑さがデータセキュリティ導入の最大の障壁



機密データ保護戦略の三本柱

従来のセキュリティアーキテクチャは、組織によるデータ処理の古い考えを反映しているため、頻繁に劇的に失敗していました。今日のデータセキュリティは、データが組織の最も貴重な資産であるだけでなく、指数関数的に増え続けることも認識する必要があります。

データ中心のセキュリティは、データが移動するエンドポイント、ネットワーク、アプリケーションだけでなく、データ自体を保護します。したがってデータ自体が安全であるため、リスクを増大させずに必要なだけデータを移動できます。データ中心のセキュリティは、データ急増の進行を遅くして抑制するのではなく、データを保存場所や使用場所に関係なく最大限に活用できるようにします。

このチャートは、データ中心のセキュリティの核となる三本柱を示しています。

データセキュリティの核となる三本柱

#1
機密データの検出と分類
- 機密データを効率的に検出および分類する
- データとそのリスクを明確に理解する

#2
機密データの保護
- 暗号化、アクセス制御、トークン化により機密データを保護する
- データが漏洩または窃取された場合でも、判読不能で役に立たないものにする

#3
暗号鍵の制御
- 鍵管理を一元化する
- 鍵ライフサイクルを管理する
- 統一された鍵管理と暗号化ポリシー

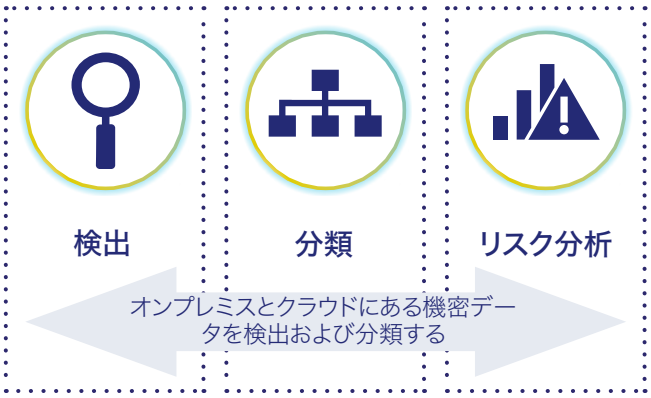
データ中心のセキュリティアプローチを組織のDNAに組み込む必要があります。この包括的なアプローチは、データセキュリティと保護の最前線で何百もの企業のCISO、CDO、CIO、アーキテクトと協働したタレスの経験と、多数の規制や業界標準で要求されるベストプラクティスに基づいています。このアプローチをデータセキュリティに採用するには、次のことを行う必要があります。

1. 機密データを検出および分類する

機密データは、エンタープライズやクラウド、さらにそれ以上に広がっています。通常、データの保存場所とデータにアクセスできる人物の把握には、限界があります。分散データのリスクは、漏洩からコンプライアンス違反までさまざまです。最も機密性の高いデータ資産がオンプレミスデータセンターのどこにあるかを特定することから始め、次に、クラウドやホスティングサービスなどの拡張環境に進みます。まず、ストレージおよびファイルサーバー、アプリケーション、データベース、仮想マシンを検索します。組織全体のあらゆる場所に存在するデータを探し、その機密性と重要性を内部ポリシーと外部規制に基づいて分類します。

機密データの検出、識別、分類は、このプロセスの重要な最初のステップですが、繰り返し可能かつテクノロジーや地理にとらわれないことも重要です。今日のデータ検出および分類ソリューションでは、視覚化されたダッシュボードとドリルダウンが提供されるため、所有している機密データの種類、場所、リスクスコアを明確に把握できます。リスクスコアは、保護レベル、検出された要素の数、場所、機密データの量などのさまざまなパラメータを集計し、これによってファイルやデータベースなどのデータオブジェクトの機密性を識別できます。その後、たとえば改善の優先順位を付けたり、サードパーティデータ共有やクラウド移行について知識に基づく判断を下したりすることで、データを保護し、リスクを軽減することができます。

データ検出と分類は効果的なデータセキュリティの最初のステップ



2. 機密データを保護する

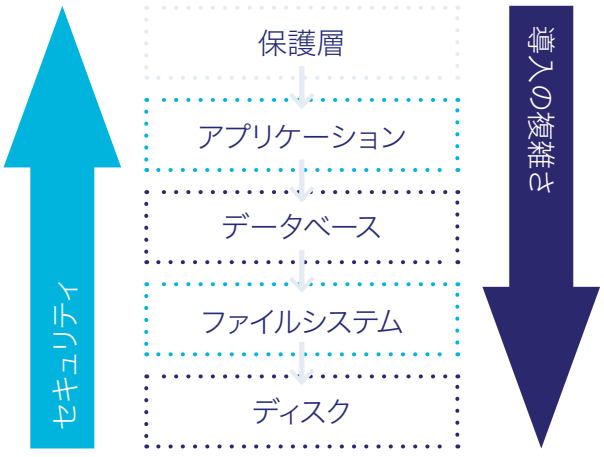
理想としては、機密データ自体を保護するために、組織全体でベースラインとなる暗号化戦略を策定し、それによってデータ漏洩や侵害のリスクを軽減することです。

データが検出および分類されると、各データセットがビジネスに加えるリスクを特定して、アクセス制御および仮名化セキュリティメカニズムの実装方法と実装場所に優先順位を付けることができます。たとえば、ファイルレベルの暗号化ときめ細かいアクセス制御、トークン化と動的データマスキングなどです。つまり、権限のないユーザーによるデータアクセスをより困難にすることや、データが漏洩または窃取された場合でも、データを判読不能で役に立たないものにすることで、データを保護します。

現在、暗号化は、組織で使用されている最も一般的で効果的なデータセキュリティ手法の1つです。データ暗号化はデータを別の形式の暗号テキストに変換するため、許可されたユーザーのみがクリアテキストとしてデータにアクセスできます。暗号化は特定のアルゴリズムを使用してデータを変換しますが、トークン化は機密データを非機密データに置き換えることで保護します。トークン化によって、データは認識不可能なトークン形式になりますが、元のデータのフォーマットは保持されます。トークン化されたデータは、元のデータと同じサイズと形式で保管されます。そのため、トークン化されたデータを保管するためにデータベースのスキーマやプロセスを変更する必要はありません。テキストファイル、PDF、MP3など、保存するデータのタイプが構造化された形式になっていない場合、トークン化は仮名化の形式として適切ではありません。このような場合は、ファイルシステムレベルの暗号化が適しています。ファイルシステムレベルの暗号化では、データの元のブロックが、暗号化されたバージョンに変更されます。

要件に最適なデータ暗号化ソリューションのタイプを決める際には、いくつかの考慮事項があります。高いレベルでは、データ暗号化のタイプはテクノロジースタックのどこで使用されるかによって分類できます。テクノロジースタックには、データ暗号化が一般的に適用される4つのレベルがあります。ディスク、ファイルシステム、データベース、アプリケーションです。通常、スタックの下位に暗号化を適用すると、実装はよりシンプルで手間も減ります。ただし、これらのデータ暗号化アプローチで対処できる脅威の数と種類も少なくなります。一方、スタックの上位に暗号化を適用すると、通常、より高いレベルのセキュリティを実現し、より多くの脅威を軽減できます。

スタックの上位に実装すると、セキュリティは向上するが開発の複雑さも増加



3. 暗号鍵を制御する

暗号化プロセスのセキュリティは、データ暗号化に使用される暗号鍵のセキュリティに依存します。データの暗号化またはトークン化に使用される鍵が、暗号化されたデータまたはトークン化されたデータと一緒に盗まれた場合、データは解読され平文で読めてしまうため、安全ではありません。暗号化とトークン化によって機密データを確実に保護するには、暗号鍵自体をサードパーティやクラウドプロバイダーではなく、組織で保護、管理、制御する必要があります。

組織は、サイロ化された暗号化ソリューションの導入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、増大するコストに対処しなければならないことに気付きます。この迷路を通過する最も簡単な方法は、一元化された鍵管理モデルに移行することです。暗号鍵の管理には、暗号鍵のライフサイクル全体を管理して紛失や悪用から保護することが含まれます。鍵にはライフサイクルがあります。誕生した鍵は、機能を全うし、そして破棄されます。鍵のライフサイクル管理には、鍵の生成、使用、保管、配布、アーカイブ、および削除が含まれます。一元化された鍵管理には次のような利点があります。

- 統一された鍵管理と暗号化ポリシー
- システム全体の鍵失効
- ユーザー権限と管理者権限の設定における人的エラーのリスク軽減
- 高い可用性と拡張性
- セキュアなFIPS 140-2検証
- 自動化によるコスト削減
- 監査情報の統合
- バックアップとリカバリの効率化
- 包括的な職務分掌によるセキュリティの強化

暗号鍵を一元管理する

効果的なデータ中心のセキュリティによるメリット

効果的なデータ中心のセキュリティソリューションを使用すると、データの急増や世界と地域のプライバシー規制の出現によって生じるセキュリティ課題に対処でき、より安全な将来に向けて備えることができます。

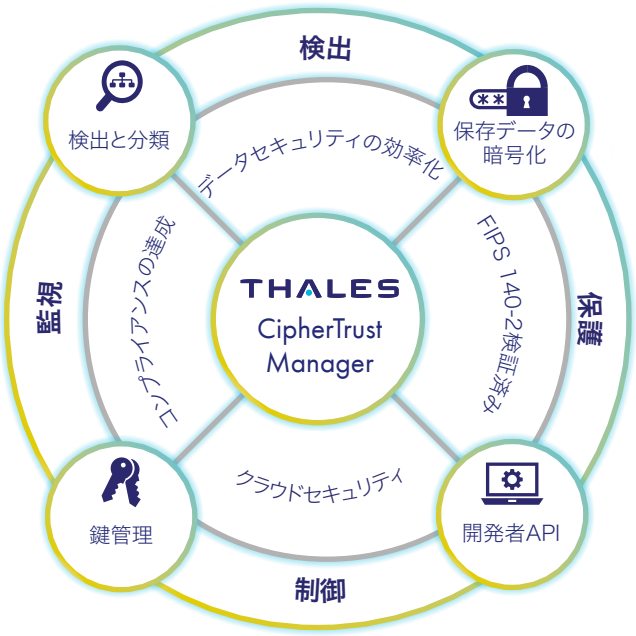
データ中心のセキュリティソリューションを適切に導入した場合:

- リスクを軽減してコストを削減できます。グローバル規模で既存のセキュリティインフラストラクチャを運用し、多大な労力を要する反復的でエラーが生じやすい手動プロセスを減らし、新しいテクノロジーを実現して投資が将来も無駄にならないようにすることで、コストを削減できます。
- すべてのデータ資産の包括的かつ継続的なビューが提供され、セキュリティポリシーと制御のガバナンスが促進されます。
- データとそのリスクを理解して改善の優先順位を付けることができます。
- データを保護するためにデータ保護プロファイルを維持しながら、複数のオンプレミスおよびクラウド環境にわたってデータを安全に移動できます。
- 悪意のあるユーザーや機密情報を盗もうとするAPT(持続的標的型攻撃)からデータを確実に保護します。
- 組織が政府、組織、業界の規制に準拠できるようにして、罰金を軽減します。違反を監視し、レポートの自動作成とセキュリティ手順の監査を行いながらセキュリティポリシーとルールを適用できます。
- データ侵害や監査の課題に対応して、防御可能な法的地位を築きます。

タレスによるセキュリティ戦略の三本柱の実装方法

タレスはデータ保護の世界的リーダーです。タレスは、データ検出と分類、暗号化、高度な鍵管理、トークン化、認証とアクセス管理など、組織がデータやアイデンティティ、知的財産を検出・保護・管理するために必要なあらゆる機能を提供します。タレスのCipherTrust Data Security Platformは、データ検出、分類、データ保護、さらにこれまでにないきめ細かいアクセス制御をすべて単一のプラットフォーム上に統合し、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に割り当てられるリソースが削減され、ユビキタスなコンプライアンス管理が実現し、ビジネス全体のリスクが大幅に軽減されます。

CipherTrust Data Security Platform



CipherTrust Data Security Platformの主な機能

- データ検出と分類
  - データの可視化によるリスク分析
- データ保護技術
  - ファイル、データベース、ビッグデータ、コンテナの透過的な暗号化
  - アプリケーションデータ保護
  - トークン化と動的データマスキング
  - フォーマット保持暗号化(FPE)
  - 静的データマスキング
  - 特権ユーザーアクセス制御
- 一元化されたエンタープライズ鍵管理
  - FIPS 140-2準拠
  - マルチクラウドの鍵管理
  - KMIP統合の比類のないパートナーエコシステム
  - データベース暗号化の鍵管理(Oracle TDE、ビッグデータ、MS SQL、SQL Server Always Encryptedなど)
- 監視とレポート
- 一元管理コンソール

CipherTrust Data Security Platformのメリット

データセキュリティの効率化

次世代の統合データ保護により、場所を問わず機密データを検出、保護、制御します。CipherTrust Data Security Platformは、「single pane of glass（1枚ガラス）」の一元管理コンソールにより、データセキュリティ管理を合理化します。これにより、データがクラウドまたは外部プロバイダーのインフラストラクチャに保存されていても、強力なツールを使用して、機密データの検出および分類、外部からの脅威への対処、内部による悪用からの保護、一貫性のある制御の確立が可能になります。デジタルトランスフォーメーションを実施する前に、プライバシーギャップを簡単に発見して解消し、保護の優先順位を付け、プライバシーとセキュリティ要件について十分な情報に基づく意思決定を行うことができます。

迅速にコンプライアンスを順守

規制当局および監査人は組織に対し、規制対象の機密データを管理し、それを証明するレポートを作成するよう要求します。CipherTrust Data Security Platformのデータ検出と分類、暗号化、アクセス制御、監査ログ、トークン化、鍵管理といった機能は、ユビキタスなデータのセキュリティとプライバシー要件に対応しています。これらの制御は新規展開に対して、または進化するコンプライアンス要件に応じて迅速に追加できます。一元化された拡張可能なプラットフォームの性質により、ライセンスを追加したり、新たなデータ保護要件に応じて必要となるコネクタをスクリプトで展開したりすることで、新たな制御を迅速に追加できます。

セキュアなクラウド移行

CipherTrust Data Security Platformは、機密データをクラウドに安全に保管できる高度な暗号化と一元的な鍵管理ソリューションを提供します。また、高度なマルチクラウドのBYOE（Bring Your Own Encryption; 独自の暗号化）ソリューションを提供することで、クラウドベンダーによる暗号化のロックインを回避してデータの移動性を確保し、暗号鍵の独立した一元管理によって複数のクラウドベンダーにわたるデータを効率的に保護します。独自の暗号化を適用できない組織でも、CipherTrust Cloud Key Managerを使用して外部で鍵を管理することで業界のベストプラクティスを導入できます。 CipherTrust Cloud Key Managerは、複数のクラウドインフラストラクチャとSaaSアプリケーションにまたがるBYOK（Bring Your Own Key; 独自の鍵使用）のユースケースをサポートしています。 CipherTrust Data Security Platformを使用すれば、最も強力な保護手段でクラウド上にある機密データとアプリケーションを保護でき、コンプライアンス要件を満たしつつ、データの作成、使用、保存場所にかかわらず、より細かくデータを制御できるようになります。

総所有コストの削減

CipherTrust Data Security Platformは、データセキュリティを効率化し、迅速にコンプライアンスを順守し、マルチクラウドのセキュリティと制御を実現することで、あらゆる規模の組織のTCOを削減できます。拡張可能なインフラストラクチャをベースに構築されたCipherTrust Data Security Platformを使用すれば、IT組織やセキュリティ組織は、組織全体の保存データを一貫した繰り返し可能な方法で検出、分類、保護できます。従来のアプローチを使用すると、多くの場合、高価な専用の個別製品が必要になり、さらなる統合や、管理のためのスタッフの作業時間が増えるため、コスト削減は見込めません。CipherTrust Data Security Platformで利用可能な多くの製品は、個別にまたは組み合わせて導入できるため、最小限のTCOで次のセキュリティ課題やコンプライアンス要件に備えることができます。データ検出、分類、リスク分析、データ保護、レポート作成を単一のプラットフォームに統合することにより、CipherTrustソリューションは、ITスタッフと予算をより戦略的なタスクに解放し、セキュリティを犠牲にすることなく、現代の組織に必要な風通しの良い、自由なコラボレーションをもたらします。

まとめ

データの価値が高まっていることから、データに対する攻撃はますます巧妙化しています。そのため組織は機密性の高い情報を保護して自社の評判を守る必要があります。データ中心のセキュリティは、今日のサイバーセキュリティの脅威に対する有意義な保護とコンプライアンスの両方を提供する唯一のアプローチです。データ検出と分類、データ保護、一元化された暗号鍵管理の三本柱に基づく、効果的なデータ中心のセキュリティ戦略を実装することで、機密データから安全に価値を抽出し、自信を持ってデジタルトランスフォーメーションテクノロジーを採用できます。

タレスのデータ中心のソリューションを使用すれば、組織全体にわたる機密性の高い構造化データと非構造化データを、コスト効果の高い効率的な方法で保護できます。

THALES

お問い合わせ先
cpl.jpsales@thalesgroup.com
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 <