Case Study

Secrets Management を導入した3社の事例

cpl.thalesgroup.com

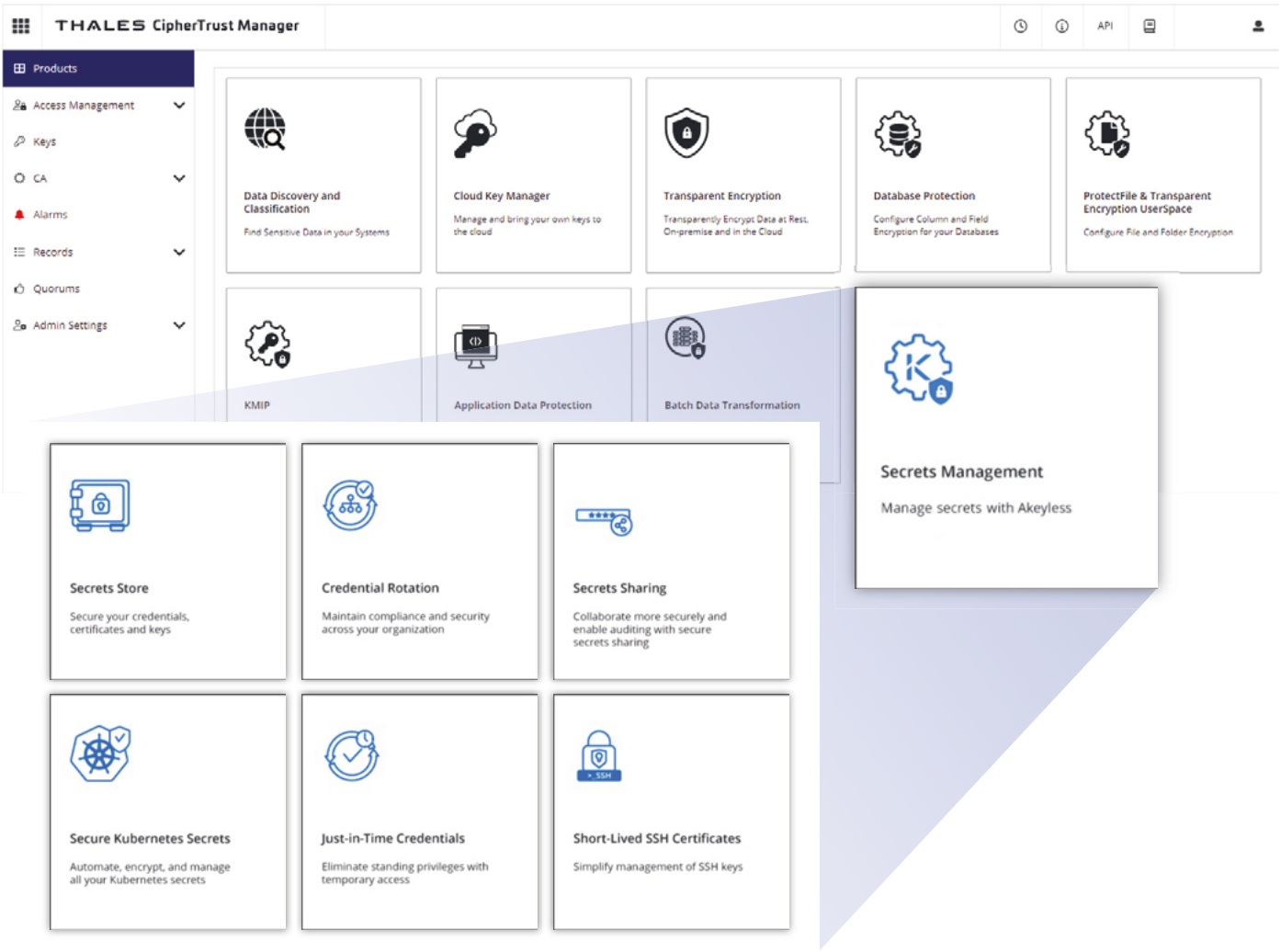
THALES
Building a future we can all trust

THALES
Building a future we can all trust

Powered by
AKEYLESS

CipherTrust Secrets Management（CSM）は、Akeylessが搭載された最先端のシークレット管理ソリューションです。CSMは、シークレット、資格情報、証明書、API鍵、トークンなど、DevOpsツールやクラウドワークロード全体にわたってミッションクリティカルなシークレットへのアクセスを保護および自動化します。この機能によりCipherTrust Data Security Platformの性能を強化することで、セキュリティおよびガバナンスチームは、業務全体のセキュリティプロセスを合理化してリスクを低減できます。

エンタープライズ対応のシークレット管理は、シークレットの作成、保存、ローテーション、削除の自動プロセスを提供します。このケーススタディでは、消費財製造、フィンテック、ビジネスアプリケーションソフトウェア業界の3社が、Akeyless搭載のシークレット管理コンポーネントを活用し、組織全体で一貫したセキュリティポリシーを適用することに成功した事例を紹介します。



包括的なデータ保護とシークレット管理を1つのツールで実現

効率的なシークレット管理をエンタープライズ規模で実現

組織について

世界中に12,000人の従業員と13の子会社を擁する多国籍消費財メーカーは、大きな課題に直面していました。大規模な運用をサポートするために、同社は、世界中に分散したセキュリティチームにセキュリティサービスを提供する小規模な中央チームによって実装できる、信頼できる価値の高いシークレット管理サービスを必要としていました。この中央チームの目的は、MSSP（マネージドセキュリティサービスプロバイダー）として各地のセキュリティチームをサポートすることです。MSSPチームは、セキュリティサービスを見つけて購入し、それを世界中に分散したセキュリティチームに提供します。ベンダーとの関係を管理し、サポートを提供することで、各地のチームが適切なセキュリティ対策を容易に実現できるようにすることが目標です。

課題

しかし、同社は、自社インフラの準備と管理に関連するコストに加え、プロバイダーからの多額のライセンスコストに直面していました。さらに、何かが正しく機能していない場合にすぐに発見できるように、監視機能を設定する必要もありました。また、問題の発生時にチームが24時間365日対応できるようにするには、かなりのコストと労力がかかり、高い総所有コスト（TCO）につながります。

チームは、ドキュメントやオンボーディングリソースの提供に懸命に取り組みましたが、それでもシークレット管理ツールを理解し、使いこなすのに苦労していました。現在のプロバイダーが提供するソリューションの信頼性、可用性、期待どおりに機能するという保証に対しての不満は蓄積していきました。導入率が低く、信頼性に疑問があり、TCOは桁外れに高いため、変更を検討する時期が来ていました。

ソリューション

同社には、迅速に導入できてメンテナンスも最小限に抑えられるシークレット管理ソリューションが必要でした。同社は、ツールセットを問わず、アウトオブボックス統合を可能にするAPI駆動機能を備えたクラウドネイティブソリューションを探し求めました。

メリット

- 迅速な導入
- API駆動機能
- アウトオブボックス統合
- セキュリティの強化とリスク軽減

導入率の向上

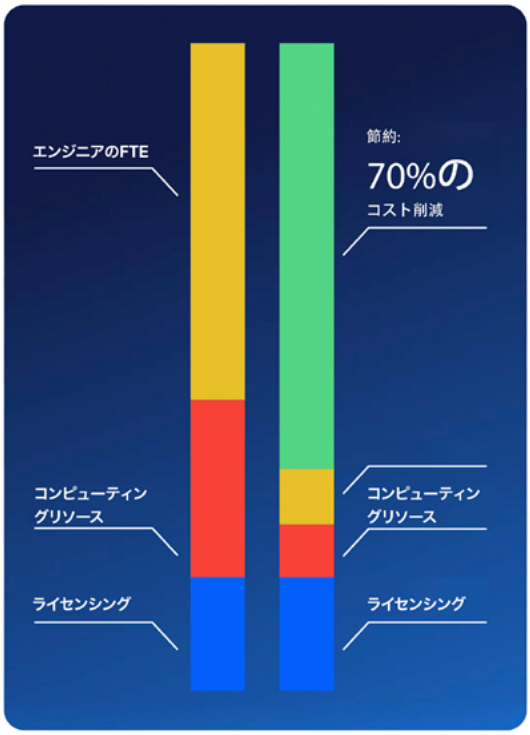
MSSPチームは、各地のセキュリティチームによる導入率が以前のプロバイダーと比較して270%も上昇したことを確認しました。セキュリティチームは特定のツールの使用を義務付けられたわけではありません——単純にそのツールが使いやすいと感じたのです。

機能性の向上

データベースユーザーの一時的な資格情報の使用や、オンプレミスマシンの資格情報のローテーションなど、以前のプロバイダーにはなかった、あるいは実装が困難だった機能を使用できるようになりました。

TCOの削減

エンジニアリングリソースとコンピューティングリソースの両方を含め、以前のプロバイダーと比較して全体でコストが70%減少しました。



導入前と導入後の実際の比較ビュー

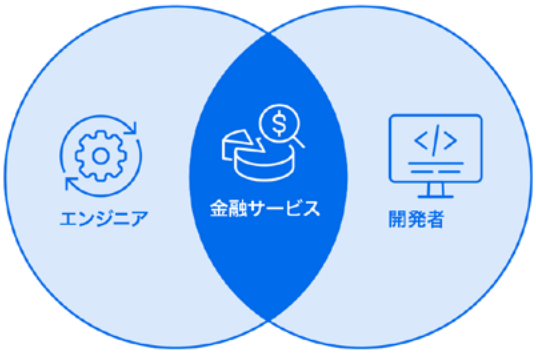
セキュリティの強化とDevOpsワークフローの加速化を実現

組織について

規制が厳しく、ペースの速いフィンテック企業は、競争優位性を維持する革新的な金融サービスを生み出すために、何百人もの開発者やエンジニアを雇用しています。クラウドファーストの理念のもと、サービスをより早く市場に投入するには、自動化されたワークロードオーケストレーションと継続的インテグレーション(CI)パイプラインが必要でした。

課題

PCI-DSSなどの多くの規制を守り続けるという課題は困難でした。同社のソフトウェア開発者チームとエンジニアリングチームが拡大するにつれ、Kubernetes環境内のシークレットの数は大幅に増加しました。シークレット管理は開発者が心配すべきものではありません。開発者は、会社の成長に貢献するような、競合他社をしのぐインパクトのあるソリューションを開発することに集中する必要があります。



ソリューション

リスクを減らしコンプライアンスへの取り組みを支援するため、同社はVPNリモートアクセスとシークレット管理ソリューションの強化を検討していました。Akeyless搭載のシークレット管理コンポーネントはゼロナレッジアプローチを採用しており、完全にセキュアな暗号鍵保管を提供するため、保護されたデータにアクセスできるのは同社のみであるという点が高く評価されました。このソリューションにより、同社はジャストインタイムアクセスのシナリオを使用して、エンジニアリングチームの拡張とDevOpsワークフローの効率化を実現できました。

メリット:

- **完全にセキュアな暗号鍵保管**
- **Kubernetesとのアウトオブボックス統合**
- **ワークフローの簡素**

SaaSベースのシークレット管理ソリューションを使用することで、シークレット管理インフラ、高可用性、ディザスタリカバリ、バックアップの導入と管理に伴う運用上のオーバーヘッドを排除しました。このソリューションは、オープンソースベースのVPNソリューションに取って代わり、人からマシンへのアクセスのユースケースに対応しました。また、統合プラットフォームが包括的な機能を提供するため、シークレット管理と特権アクセス管理(Privileged Access Management; PAM)の両方のニーズを満たすことができました。

結果:

- **厳しい個人情報保護法に準拠**
- **数百人のエンジニアと開発者に対しシームレスにスケーリング**
- **CISOに安心を提供**
  - **ディザスタリカバリ**
  - **高可用性**
  - **バックアップ**

ハイブリッドマルチクラウド戦略のサポート

組織について

世界16カ国に2,100人の従業員を擁するビジネスアプリケーションソフトウェア会社は、ビジネスアプリケーションを作成および展開するためのソフトウェアを提供しています。組織的には、同社はさまざまな部門に分かれており、アプリケーション、デジタルエクスペリエンス、また開発者向けのツールやモジュールの作成など、各部門がそれぞれ責任を担っています。

課題

一連の買収と各部門の継続的な成長により、開発者チームには多くの異種ツールが混在していました。その結果、シークレットの使用量や、必要なAPIへのアクセス、ワークロードが急速に増加しました。それに伴い、シークレットの拡散や資格情報の漏洩リスクも高まりました。しかし、同社のマルチクラウド戦略には、ツールの運用と保守に多大な時間とコストをかけることなく、ビジネスチームが簡単に利用できる一元的なソリューションが必要でした。

ソリューション

同社は、既存のクラウドサービスやDevOpsツールのための幅広いアウトオブボックス統合機能を備えた、各チームが容易に導入できるシークレット管理プラットフォームを必要としていました。そのため、次のようなソリューションが必要でした。

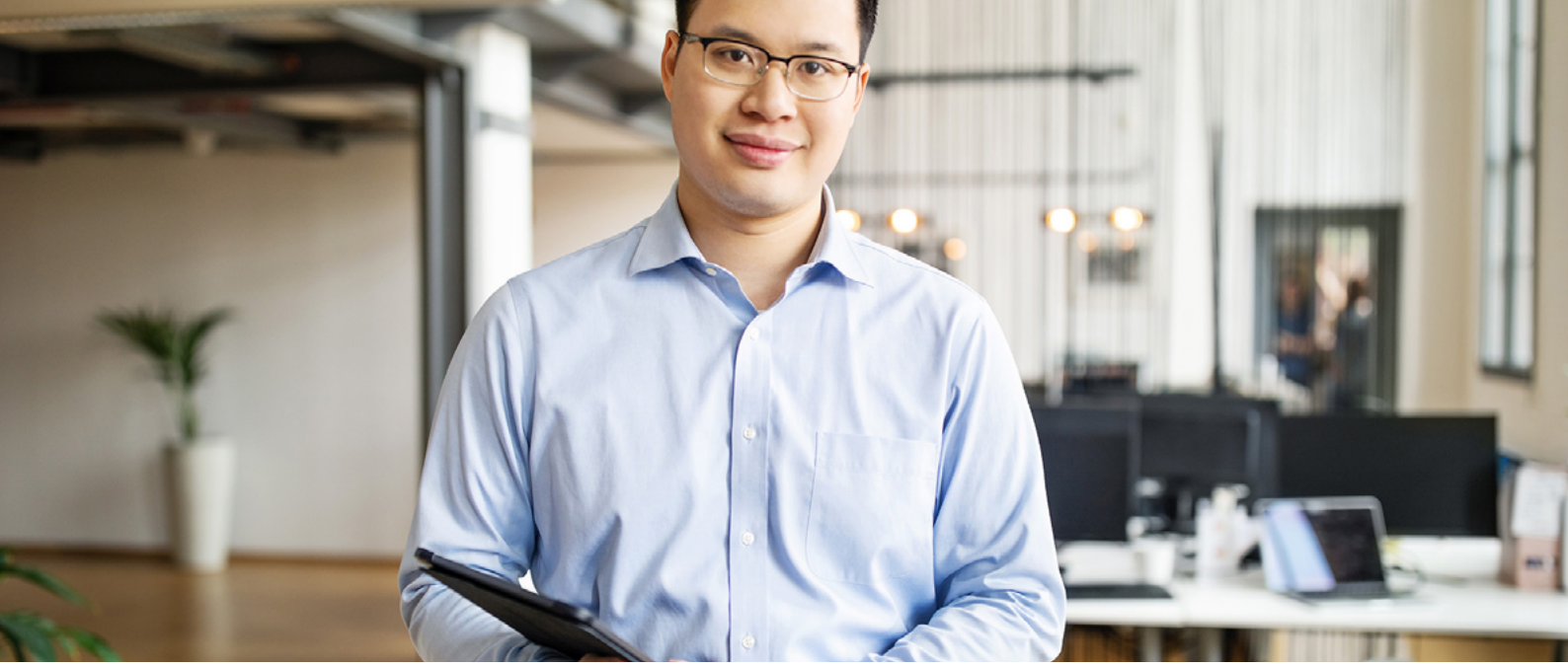
- 多様な開発者チームが、セキュリティを気にすることなく、イノベーションとソフトウェア開発に集中できるようにする。
- AWS、Azure、Google Cloud の利用に関係なく、スタッフやワークロードがどこに存在していても、利用可能な一元化されたシークレット管理システムにチームがアクセスできるようにする。
- 高可用性、高パフォーマンス、スケーラビリティを提供しながら、マルチリージョンに対応したマルチクラウドアーキテクチャにより、新たな信頼をもたらす。
- 暗号鍵の排他的な所有権を維持する。クラウドプロバイダ`ーのVaultや仮想化されたVaultインスタンスでは、ユーザーはマスター鍵を放棄しなければなりません。しかし、新しいシークレット管理ソリューションでは、組織は暗号鍵の所有権を維持できます。これにより、暗号鍵や暗号鍵で保護されたデータが、不正な管理者やハッカーによってアクセスされたり、CLOUD Ac（t クラウド法）を通じて政府に引き渡されたりすることを避けられるため、リスクが軽減されました。

結果:

- **オーバーヘッドを60%～70%削減**
- **チームはソフトウェアの保守やパッチ適用の無駄なサイクルを排除**
- **開発者のワークフローが向上**

Akeyless搭載のシークレット管理コンポーネントを活用することで、同社は以下を実現しました。

- オーバーヘッドを60%～70%削減し、生産性の維持とビジネス推進のために必要なリソースへの従業員のアクセス許可に関連するワークフローを簡素化。
- 従来のシークレット管理ツールにありがちな、複雑な基盤インフラの保守やソフトウェアのパッチ適用の無駄なサイクルを排除。
- 開発者ワークフローの効率とセキュリティの向上。



CipherTrust Secrets Management

AkeylessがCipherTrust Secrets Managementは、迅速に導入でき、エンタープライズ対応であるため、シークレット管理を簡素化し、開発者の効率を向上させることができます。 CipherTrust Secrets ManagementはCipherTrust Data Security Platformの一部であり、クラウド、オンプレミス、ハイブリッド環境にわたって組織が機密データを検出、保護、制御できるようにするデータ中心のセキュリティ製品の統合スイートです。 CipherTrust Platformは、緊急の要件を満たすことを可能にし、次のセキュリティ課題やコンプライス要件の発生時に組織が機敏に対応できるように準備します。CipherTrust Platform の詳細についてはこちらをご覧ください。

リソース

現在のシークレット管理方法を改善する計画を立てましょう。

- 無料相談についてタレスに問い合わせる
- 無料デモ/POCを予約する
- 90日間の無料トライアルを開始する
- デモを視聴する
- シークレット管理ソリューションの選び方を学ぶ

他社ソリューションとの違い:

- **すべてのシークレットタイプに対する一元管理**
- **DevSecOpsのための使いやすい自動化機能**
- **ハイブリッドおよびマルチクラウド環境に対応するSaaS(Software as a Service)のスケーラビリティ**

Akeylessについて

Akeylessの革新的なテクノロジーとクラウドネイティブアーキテクチャの独自の組み合わせにより、企業はコンプライアンスと規制の要件を満たしながら、DevOps、クラウドワークロード、レガシー環境を迅速に保護できます。

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。

cpl.thalesgroup.com

お問い合わせ先 – Email: 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。