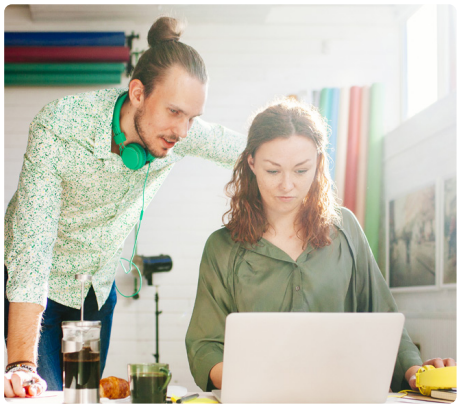
opentext™ | Cybersecurity

お客様事例

多国籍小売企業

Voltage SecureData Enterprise が、700 万件を超えるクラウド上の顧客レコードのデータセキュリティを包括的に確保することによって、デジタルトランスフォーメーションをサポート。



データ中心のセキュリティとサイロ型のアプローチ

12,000 店以上の実店舗をグローバルに展開しているこの企業は、デジタルトランスフォーメーションにも重点的に取り組んでおり、マルチチャネルアプローチを採用して成功を収めています。

従来の IT モデルでは、組織は階層型またはサイロ型のアプローチでセキュリティ管理を行います。このようなモデルでは、複数のアプリケーション、ネットワーク層、データベース、ファイルシステム、データセンターのストレージシステムなどの間を機密データが移動します。データはそれぞれのレベルで保護されますが、インフラストラクチャ内でデータが移動するため、異なるレイヤーの間でセキュリティギャップが生じることは避けられません。同社の CISO オフィスのプロジェクトマネージャーは、この問題について次のように説明しています。「レイヤー内ではすべてのデータが暗号化されていましたが、特権ユーザーアカウントが不正使用されたら、データ漏洩が生じる可能性がありました。データフローの保護には SFTP を使用していましたが、交換されるファイルにはプレーンテキストデータも含まれており、送信元から宛先までのさまざまな段階で保存されるため、これもリスク要因でした。また、階層型のアプローチにはコストがかかるという課題もありました。レイヤーごとに別々のセキュリティソリューションが必要で、それぞれに異なる専門知識が求められるため、リソースの調達が複雑になるためです。Azure と Google Cloud を活用したクラウドへの全社的な移行に伴い、当社は安心して任せられる包括的なデータセキュリティを求めていました。セキュリティモデルをデータ中心のアプローチに転換することで、こうした問題は解決できるだろうと考えました」

「当社は平均して 2 週間ごとに、新しいアプリケーションを Voltage に導入しています。データはデフォルトで暗号化されており、必要なときにしか開示されません。これにより、リスクとコンプライアンスの体制が大幅に強化されました」

プロジェクトマネージャー
CISO オフィス
大規模小売企業

Voltage：「プライバシー・バイ・デフォルト」

システムベースのセキュリティ統合を必要とする単機能ソリューションとは異なり、データ中心のセキュリティでは、信頼できない環境間でも信頼できる形でデータを移動できます。データがストレージから移動してアプリケーション内で使用されるまでのどの段階においても、完全なデータセキュリティを実現し、一貫して暗号化形式のままで使用できます。同社は、市場に存在するいくつかの選択肢を評価した結果、Voltage SecureData Enterprise by OpenText™ を導入し、データセキュリティの確保を通じてビジネス価値の向上に成功しました。

「プライバシー・バイ・デフォルト」を社内のセキュリティアーキテクチャの中心に据えたことにより、データはシステムに入った瞬間から、完全に暗号化された状態のままとなります。データ形式と整合性は、検証ルールも含めて、Voltage の Format-Preserving Encryption (FPE) by OpenText™ を通じて保証されます。標準的な暗号化では、暗号化された形式で元の形式より多くのフィールドが使用されるため、

概要

業種

小売

所在地

グローバル

課題

お客様がコアビジネスに集中できるようにし、ハードウェアとメンテナンスへの投資を削減できるようにしながら、お客様のデジタルトランスフォーメーションをサポートする

製品とサービス

Voltage SecureData Enterprise

主な成功要因

- 700 万件を超える顧客レコードの包括的保護
- Google Cloud と Azure によるクラウド導入
- チーム間の連携の改善とデータ知識の共有
- 変化を続けるビジネス要件に対応するための市場投入期間の短縮
- リスクとガバナンスの体制強化

「Micro Focus (現在は OpenText™ の傘下) と連携することで、製品ライフサイクルの特定のタスクで必要なデータ知識の共有が進み、セキュリティ、開発、運用、プロジェクトの各チーム間のコラボレーションを強化できました」

プロジェクトマネージャー
CISO オフィス
大規模小売企業

お問い合わせ
www.opentext.com

データが肥大化する可能性があります。その結果、システムパフォーマンスの問題が発生し、保守やサポートで必要以上の経費がかかる可能性があります。Voltage FPE を使用すると、フィールドは部分的にまたは全体的に暗号化されますが、フィールドのサイズと形式は変わりません。同社のプロジェクトマネージャーは、このことの重要性について次のようにコメントしています。「クラウド上に保存された顧客レコードが 700 万件以上あり、それぞれに最大 10 個の暗号化フィールドが含まれています。Voltage FPE は、ほぼすべてのデータ型とデータ形式をサポートしており、データプロセスとアプリケーションの操作性や参照整合性を維持するためにデータベーススキーマを更新する必要はありません。たとえば、マーケティングキャンペーン中に電子メールを送信するために必要なフィールドだけを復号化するなど、フィールドを特定して復号化することができます」

GDPR に完全準拠しながら市場投入までの時間を短縮

従来、復号化キーの管理には手間がかかり、コストがかかります。組織はキーデータベースを維持する必要があり、それに加えて、データベースを継続的に保護するために必要なハードウェア、ソフトウェア、IT プロセスも維持しなければなりません。通常は、サイト間でキーを複製またはバックアップすることも必要です。Voltage Stateless Key Management by OpenText™ を使用すれば、そのような必要はなくなります。一元管理されたポリシーに従って、アプリケーションとそのユーザーが適切に認証され権限が確認されれば、アプリケーションに必要なキーがその場でセキュアな形で生成されます。キーは必要になった時点で生成されるため、保存しておく必要がありません。そのため、運用や障害復旧の作業が楽に行えます。

市場投入までの時間を短縮することは非常に重要で、サービスデリバリーの改善は企業にとって重要な成功要因です。同社のプロジェクトマネージャーによれば、最近の経緯を振り返ってみると、IT アーキテクチャの中心に「セキュリティ・バイ・デザイン」を据えることが非常に重要だったと述べています。「当社のマーケティング部門は、革新的なゲーム会社との協業によって、ポイントカードを持つ顧客を引き付ける素晴らしいアイデアを生み出しました。当社は、お客様が楽しんでいる間に、そのお客様に関する有用な知見を別途得ることができます。通常であれば当社は、アプリケーションの動作の仕組みとそのアプリケーションが機密データを管理する方法を、データフローを含めて完全に理解する必要がありました。しかし、Voltage を基盤として導入していることで、当社はサードパーティアプリケーションを迅速に統合することが容易にできるようになっていました。そうしたアプリケーションは、非常にアジャイルなスタートアップ企業の製品であることが多く、データセキュリティが重要視されていない場合があります。当社はデータアクセスを自社で制御できるため、GDPR やその他の関連するデータプライバシー規制に完全に準拠しながら、全体のプロセスをスピードアップできます。当社はビジネスを加速させますが、それは完全にセキュアな手段によって行っています」

ビッグデータとデータレイクの保護

すべてのデータは Hadoop データレイクに収集され、その中で暗号化された状態に保たれます。データを使用するアプリケーションはそこからデータを取得し、復号化する必要があれば、Voltage が各データオブジェクトに格納されているキー識別子を介して認証を処理します。データサイエンスチームとビジネスインテリジェンスチームは、Google Big Query を用いてデータの相関関係を処理し、データ主導の意思決定に利用します。エンドツーエンドのライフサイクルを通じて明確にデータが保護される一方、さまざまな環境、クライアント、プラットフォームとの統合が可能であることから、ビジネスアナリストは好んで業務に Voltage を用います。

アプリケーション導入を加速しチーム間連携を改善

同社の銀行および金融部門は、機密性の高い顧客の財務データを抱えています。Voltage のデータ中心のセキュリティ原則を中心に据えれば、企業は個々のプライバシー影響評価 (PIA) にかかる時間とコストを節約できます。監査当局がデータセキュリティのプロセスを完全に把握できるからです。

同社のプロジェクトマネージャーはそのメリットを認めています。「データ中心のセキュリティモデルとして Voltage を実装した結果、当社の俊敏性が向上し、絶えず変化するビジネス要件により迅速に対応できるようになりました。当社は平均して 2 週間ごとに、新しいアプリケーションを Voltage に導入しています。データはデフォルトで暗号化されており、必要なときにしか開示されません。これにより、リスクとコンプライアンスの体制が大幅に強化されました」

同氏は結論として次のように述べています。「Micro Focus (現在は OpenText™ の傘下) と連携することで、製品ライフサイクルの特定のタスクで必要なデータ知識の共有が進み、セキュリティ、開発、運用、プロジェクトの各チーム間のコラボレーションを強化できました。当社は今、自信を持ってブランドイメージを語ることができます。『お客様のデータはすべて暗号化されており、安全に保管されます』と」

opentext™ | Cybersecurity

OpenText Cybersecurity は、あらゆる規模の企業とパートナー様を対象に、包括的なセキュリティソリューションを提供しています。予防から検出、復旧対応、調査、コンプライアンスに至るエンドツーエンドの統合プラットフォームにより、包括的なセキュリティポートフォリオを通じてサイバーレジリエンスの構築をサポートします。コンテキストに基づくリアルタイムの脅威インテリジェンスから得られた実用的なインサイトを活用できるため、OpenText Cybersecurity のお客様は、優れた製品、コンプライアンスが確保されたエクスペリエンス、簡素化されたセキュリティというメリットによって、ビジネスリスクを管理できます。

768-JA0015-003 | O | 12/23