

大手国際金融サービス企業

Voltage と SDM によってメインフレームと Azure 間で安全にデータをやり取りできるようにすることで、規制への準拠とデータ分析をわずか 8 週間で実現しました。



PSD2 コンプライアンスによって複雑になるデータ管理

ヨーロッパのすべての銀行と同様に、この大手企業も新たなオープンバンキング時代の中でビジネスを行っています。オープンバンキングによって、欧州経済地域全体で第三者が銀行情報を利用できるようになります。その目的は、銀行業務を最適化し、顧客が自身の財務データをよりきめ細かく管理できるようにすることです。顧客は特定の同意を与えることで、自身の財務データを第三者と自由に共有できます。一方、銀行では、顧客に合わせてよりきめ細かくパーソナライズされた新しいサービスを提供できるようになります。オープンバンキングを保護するために、ヨーロッパのすべての銀行が決済サービス指令 2 (PSD2) に準拠する必要があります。これにより、オンライン決済のセキュリティが強化され、銀行の競争力が高まることで顧客にメリットがもたらされます。また、顧客はアカウントへのアクセス権を持つユーザーや、アカウントへのアクセス方法を制御することもできます。

「Voltage と SDM はわずか 8 週間で実装され、すぐにメリットを実感できました。Micro Focus (現在は OpenText の傘下) には独自の革新的なサイバーセキュリティソリューションがあるため、機密データを Azure クラウド環境にシームレスに複製し、必要に応じていつでも活用して分析できます」

シニアプログラムマネージングアーキテクト
大手国際金融サービス企業

金融データの安全なやり取りはすべての銀行が直面している課題です。この金融サービス企業のデータセキュリティエンジニアは次のように説明しています。「大規模な銀行であるため、20TB を超えるアカウントデータを保有しています。その多くは非常に機密性が高いものです。さまざまなデータセンターでホストされているメインフレーム環境にこうしたデータが保存されています。PSD2 で定められているすべてのデータをメインフレームから公開しようとしたが、持続可能な方法でこのデータを共有するための効果的かつ安全な方法はありませんでした」

さらに次のように続けます。「メインフレームといえば、誰もが非常に堅牢なデータセキュリティを想像します。これは事実ですが、規制や新しい働き方に対応するには、データを安全に転送する必要があります。これが閉じられたメインフレーム環境の問題となっています。Microsoft とのパートナーシップをきっかけに、データセンターから毎日レプリケーションを行う Azure のクラウドアプローチを採用しました。Azure にはいくつかのセキュリティ機能があります。ただ、転送中の機密データやデータ分析のためにクラウドで使用しているデータにはこれでは不十分だと考えていました。そこで、Microsoft と、コンサルタントパートナーである Accenture と協力してソリューションを探しました」

Voltage の強固な暗号化と Azure のクラウド統合

データの爆発的な増加、そして一般データ保護規則 (GDPR)、Payment Card Industry Data Security Standard (PCI DSS)、PSD2 などの規制圧力により、各社は情報ライフサイクル全体にわたって確固たるポリシーと手順を実施することを強いられています。Voltage

概要

業種

金融

所在地

スペイン

課題

メインフレームに保存されているデータを安全に活用することで、オープンバンキング業界規制に準拠し、より柔軟なレポート作成機能とデータ分析機能を実現する

製品とサービス

Voltage SecureData Enterprise
Structured Data Manager

成功ポイント

- レポート作成機能とデータ分析機能の大幅な強化
- 堅牢な暗号化アルゴリズムを使用したシームレスなクラウド統合
- PSD2、PCI、GDPR の各規制への完全準拠
- 実装期間はわずか 8 週間

「Voltage と SDM を組み合わせることで、データをオンザフライで安全に復号化できます。これは、当行のシナリオで非常に役立ちます。高い柔軟性により、レポート作成と分析の実行がはるかに容易になりました。おかげで、組織の将来の成功に不可欠なデータ主導の意思決定も可能になりました」

シニアプログラムマネージングアーキテクト
大手国際金融サービス企業

お問い合わせ

www.opentext.com



SecureData by OpenText Enterprise では、オンプレミス、クラウド、ビッグデータ分析プラットフォームのどこに機密データが転送されても安全を確保できます。Accenture と Microsoft は、Voltage が Azure の機能と SecureData の統合によってもたらす強固なデータ保護を高く評価しました。同行のチームは自社のアーキテクチャに Voltage を加えるメリットは大きいと感じ、OpenText™ と Microsoft の共同契約によってソリューションを実装しました。

「Voltage の暗号化と仮名化の機能が特に気に入っています」と、同行のシニアプログラムマネージングアーキテクトは述べます。「他のソリューションでは、転送中のデータを暗号化することはできますが、これを簡単に元に戻すことはできません。これでは、分析目的でデータが必要な場合に役に立ちません。Voltage の仮名化により、個人識別情報 (PII) フィールドが1つ以上の人工識別子 (仮名) に置き換えられるため、安全に復元可能な双方向データ変換を実現できます」

Voltage+SDM = チームに成功をもたらす

パフォーマンスを損なうことなく、信頼性の高いプロセスと分析で大量のデータを管理するために、同行のチームは Structured Data Manager (SDM) by OpenText を選択しました。これにより、GDPR、PCI DSS、PSD2 などの最新のコンプライアンスおよび保護要件に従ってデータを保護できます。SDM

と Voltage SecureData が連携することで、フォーマット保持型暗号 (FPE) を使用して、使用中またはアーカイブ中の機密データが自動的に暗号化されます。FPE を使用すると、データレベルの暗号化を従来のビジネスアプリケーションに統合できます。これが成功の鍵となります。FPE を使用しない場合、企業のデータアナリストはカスタムクエリとアルゴリズム、および手動プロセスを開発する必要があります。

メインフレームから企業のデータレイクである Azure Big Data への、夜間実施される増分データレプリケーションは、Voltage と SDM によって管理されます。必要なデータ変換はすべて Azure Databricks によって実行されます。つまり、姓と名のフィールドから氏名が作成された後、データが企業の Azure SQL データベースに保存されます。サードパーティプロバイダーは、クラウド API コネクタを介してこのデータを使用するため、隙のないデータセキュリティを維持できます。

SDM の使用範囲を拡張して、企業が見落としている可能性がある機密データを特定できます。使用可能なすべてのデータをスキャンすることで、SDM でデータを検出、分析、分類できます。その後、承認済みアルゴリズムによって、Voltage の暗号化プロセスを通じてこのデータを保護することも、データが冗長である場合はアーカイブ対象か削除対象として推奨することもできます。こ

うした自動化プロセスにより、コストを大幅に削減し、安全なデータの削除によってさらにリスクを軽減することが可能になります。同行ではこれらについて今後検討する予定です。

完全な分析と柔軟なレポート機能をわずか 8 週間で実現

「Voltage と SDM の統合により、データをオンザフライで安全に復号化できます。これは、当行のシナリオで非常に役立ちます」と同行のシニアプログラムマネージングアーキテクトは述べます。「高い柔軟性により、レポートを安全に作成し、クラウドサービスで分析を実行することがはるかに容易になりました。おかげで、組織の将来の成功に不可欠なデータ主導の意思決定も可能になりました」

彼はこのように締めくくります。「Voltage と SDM はわずか 8 週間で実装され、すぐにメリットを実感できました。Micro Focus (現在は OpenText の傘下) には独自の革新的なサイバーセキュリティソリューションがあるため、機密データを Azure クラウド環境にシームレスに複製し、必要に応じていつでも安全に使用して分析できます」

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。