opentext™ | Cybersecurity

政策方針書

Voltage SecureData Cloud & Analytics

クラウドサービスでの機密データ資産の保護

はじめに

今日のビジネス上の課題により、企業は機動性と柔軟性を持ち、そして新しい市場の顧客に対して迅速にサービスを提供することを迫られています。このような要因が企業のビジネス全体でのクラウド導入を促進している面はあるものの、多くの場合その主な理由は、オンプレミスデータセンターのハードウェアやソフトウェアの保守作業が複雑でコストがかかることにあります。成長に応じてキャパシティの拡大を必要とする企業や、時期によってビジネス活動が急増する企業は、自社でデータセンターのハードウェアおよびソフトウェアを購入、管理、保守するよりも、必要なときに柔軟にキャパシティを利用できるクラウドの方がコスト面で有利であることを認識しています。

企業のセキュリティおよびリスク管理担当者を対象にしたクラウドデータのセキュリティに関する調査によると、クラウドに保管されている企業データの 40% 以上が機密データであり、それらのセキュリティ対策が不十分であることが確認されました[1]。さらに、Ponemon Institute の調査によると、今日の企業はビジネスを遂行するにあたり平均で 27 種類の異なる Software-as-a-Service (SaaS)、Infrastructure-as-a-Service (IaaS)、Platform-as-a-Service (PaaS) ソリューションを使用していて、このことが問題をさらに複雑にしています[2]。

企業のセキュリティおよびリスク管理担当者を対象にしたクラウドデータのセキュリティに関する調査によると、クラウドに保管されている企業データの40%以上が機密データであり、それらのセキュリティ対策が不十分であることが確認されました[1]。

しかし、企業内のさまざまな機能で広くデータが利用されるようになり、モバイルでのデータ利用も増えている今、既存の IT インフラストラクチャに広く組み込まれている従来型のセキュリティ対策は効果を失いつつあることが証明されています。現在、ほとんどの組織で複数のクラウドプロバイダーが使用されていることも、ハイブリッドな IT 環境内を移動する機密データの保護をさらに困難なものにしています。GDPR や CCPA など、さまざまなプライバシー規制が登場して規制環境が複雑化するとともに、データ侵害の発生件数、範囲、規模が広がりを見せるなか、オンプレミス、クラウドのインフラストラクチャやアプリケーション、分析プラットフォームなど、データが流れる場所を問わず機密データを保護できるより効率的な対策が求められています。

以上のようなビジネス上の強い必要性がある一方で、効果の低いセキュリティ対策は変わらないという状態の結果、組織として機密データを保護する対策がないまま機密データがクラウドへと移行される事態が生じています。クラウドネイティブなデータセキュリティ機能が導入されていない、効果が低い、または正しく構成されていないことにより大規模なデータ侵害が発生し、その結果データプライバシー規制のコンプライアンス違反により罰金が科せられる事例が増えています。

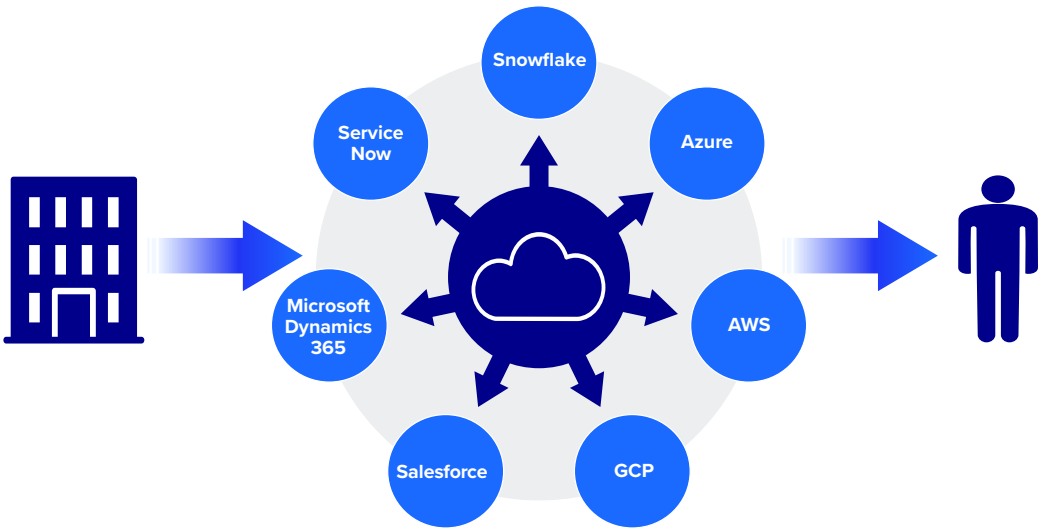
データ中心のセキュリティによるクラウド移行の促進

Voltage SecureData Cloud & Analytics by OpenText™ は、マルチクラウド、ハイブリッド、オンプレミス環境で持続的に機密データを保護します。ハイブリッド IT 全体にデータ中心のセキュリティを組み込み、機密データにまつわるリスクを低減することにより、クラウド環境への安全な移行を促進します。

1. Enterprise Strategy Group (2019) Trends in Cloud Data Security: The Data Perimeter of Hybrid Clouds
2. Ponemon Institute LLC (2018) The 2018 Global Cloud Data Security Study

Voltage SecureData Cloud & Analytics が提供するセキュリティサーバーおよびクライアントにより、アプリケーション、データ、データストアと、オンプレミスおよびクラウド内のサービスとを連携させることができるため、データライフサイクル全体を通したエンドツーエンドの保護を実現できます。Voltage SecureData Enterprise by OpenText™ は FIPS 140-2 と共通基準 (CC) による認証を受けています。z/OS や、Stratus VOS などのトランザクションシステム、Cloudera や MapR などのディストリビューションで動作する Hadoop などのオープンシステム、AWS EMR や Azure HDInsight などのクラウドサービス、OpenText™ Vertica™、Teradata、Snowflake などの高性能分析プラットフォームをはじめ、業界で使用されている幅広いプラットフォームやシステムをサポートします。

ハイブリッド IT：プラットフォームを問わないデータ中心のセキュリティ



Voltage SecureData Enterprise で使用されるトークン化テクノロジーは、柔軟性が高く、あらゆる言語や地域のほとんどすべての構造化データタイプに対して導入してデータを保護できるほか、パフォーマンスとスケーラビリティの高さも実証済みです。

Voltage によりデータの使いやすさを維持して保護

Voltage SecureData Enterprise で使用されるトークン化テクノロジーは、柔軟性が高く、あらゆる言語や地域のほとんどすべての構造化データタイプに対して導入してデータを保護できるほか、パフォーマンスとスケーラビリティの高さも実証済みです。Voltage Format-Preserving Encryption (FPE) by OpenText™、Format-Preserving Hash (FPH) by OpenText™、Voltage Secure Stateless Tokenization (SST) by OpenText™ により機密情報を匿名化します。これにより、データ侵害を無害化しつつ、保護状態にあるデータをアプリケーションや分析プラットフォームで継続して使用することができます。Voltage のトークン化テクノロジーにより、データのコンテキストや意味 (参照関係、ロジック、ビジネス上の意図など) を保持しながらデータを保護された形式に保つことができるため、復号化の必要性を最小限に抑えることができます。また、参照関係の整合性が保たれるため、クロスクラウド分析において保護対象のデータを確実に参照して結合することができます。そのため、電話番号や ID など、異なるデータセット間で共通する識別子を通して重要な知見を入手することができます。

Voltage によるデータの仮名化

AES (Advanced Encryption Standard) の一種である Voltage FPE は、Voltage SecureData Cloud において、データの柔軟な使い勝手を損なうことなく強度の高い堅牢なデータ暗号化を行う、基盤となる革新的なテクノロジーです。NIST SP 800-38G[3] に示されている FF1 方式を導入した Voltage FPE は、データのフィールドおよびサブフィールドレベルでデータプライバシー規制に準拠するために必要な仮名化を行うと同時に、保護されたデータセットに対するビジネスプロセスや分析の実行を可能にする暗号標準です。

Voltage Secure Stateless Tokenization (SST) は特許取得済みの高度なデータセキュリティソリューションです。オンプレミスまたはクラウドにおける支払いカードデータを確実に保護します。Voltage SST では、トークンデータベースが不要で、カード名義人データやその他の機密データを保管する必要がないため、PCI-DSS コンプライアンス監査などの範囲を大きく狭めることができます。プライマリアカウント番号 (PAN) などの各データ値に対して常に一意のランダムなトークンを生成する、あらかじめ作成された静的なテーブルのセットを使用することにより、トークン化プロセスの速度、拡張性、セキュリティ、管理性が向上します。

Voltage によるデータの匿名化

セキュアでコンプライアンスを維持したテストデータ管理を実現するといった特定のユースケースでは、データが復元できると必要以上のリスクが生じることがあるほか、データの復元自体が望ましくない場合もあります。Voltage Format-Preserving Hash (FPH) は、クリックストリーム分析などのいくつかのユースケースにおいて、構造、ロジック、フィールドの一部への適用、使い勝手などの他の Voltage のトークン化テクノロジーが持つメリットはそのままに、データの完全な匿名化を提供します。Voltage FPH は、SHA-256 などの従来の匿名化手法と異なり、フォーマットを保持したまま柔軟な一方向の不可逆変換を行うことによりデータの高性能な操作性を実現します。

Voltage のステートレスキー管理

Voltage のステートレスキー管理 (by OpenText™) は、Voltage のシンプルさと拡張性の土台となるテクノロジーです。キーは必要に応じて動的に取得され、キーデータベースの保管、保護、バックアップの必要はなく、また従来のキー管理ソリューションとの統合も必要ありません。キー、証明書、データベースの管理が不要なため、オンプレミス、オフサイトバックアップ、さらにはクラウドでキーデータベースを継続して保護するためのハードウェアやソフトウェア、IT と人材に必要なプロセスもコストも削減できます。Voltage のステートレスキー管理を使用することにより、暗号化キーを完全に管理すると同時に低コスト、高性能、かつ高可用性のデータ保護を実現できます。またその拡張性により、世界最大手の金融サービス企業、電気通信事業者、支払い処理業者、その他のグローバル企業や政府機関の機密データ保護にも利用されています。

Voltage Format-Preserving Hash (FPH) は、クリックストリーム分析などのいくつかのユースケースにおいて、構造、ロジック、フィールドの一部への適用、使い勝手などの他の Voltage のトークン化テクノロジーが持つメリットはそのままに、データの完全な匿名化を提供します。

3. アメリカ国立標準技術研究所 (2016) Special Publication 800-38G, Recommendation for Block Cipher Modes of Operation: Methods for Format-Preserving Encryption

ハードウェアセキュリティモジュールのクラウド環境に適応した進化

Voltage SecureData Enterprise を使用してストレージやワークロードをクラウドベースの環境に移行する場合は、クラウドにおける HSM ベースの「信頼の基点 (Root of Trust)」が重要になります。認定 Voltage アライアンスパートナーである nCipher Security の nShield as a Service は、機密データとは分離した形で暗号キーデータの生成、アクセス、保護ができる、サブスクリプションベースの FIPS 140-2 認証済み nShield HSM ソリューションで、Voltage のステートレスキー管理をサポートしています。このクラウドホスト型モデルによりデータセンターの HSM を補完または置き換えることができます。

クラウドにおけるデータの保護と分析の実現

低コストのデータストレージ、柔軟に利用できるコンピューティングリソース、ますますサービス範囲を拡大させるデータ分析により、オンプレミスからクラウドへと、ビッグデータ導入環境の移行が進んでいます。しかし、機密データを外部にホスティングすると、セキュリティに関して新たな責任が発生するだけでなく重大なリスクも抱えることになります。責任共有モデルのもとでは、提供するハードウェアおよびソフトウェアサービスのセキュリティについてはクラウドプロバイダーが責任を負う一方、利用者には自身の資産のセキュリティに責任を負うことが求められます。

Voltage SecureData Cloud & Analytics では、クラウドアプリケーションおよびサービスでデータが保護され、保護された形式のままデータを使用することができます。これにより、セキュリティ対策が存在しない、または正しく構成されていないことによりデータ侵害が発生するリスクを除去できるほか、クラウドでの復号化の必要性がないためマルチクラウド環境でも切れ目のないデータ保護モデルを導入できます。データをクラウドに移行する場合、取り込み時、保存中、使用時など、ライフサイクル全体を通して継続的にデータを保護する必要があります。

Voltage SecureData Cloud & Analytics は以下との連携が可能です。

- AWS Glue、Azure Data Factory、Google Data Fusion などのクラウド ETL サービス、および Informatica、Talend、DataStage、Ab Initio などのその他の COTS (商用オフザシェルフ) ETL ツール
- Kafka、NiFi、Storm、Streamsets などのストリーミングプラットフォーム、および AWS Kinesis、Azure EventHubs、Google Dataflow などのクラウドストリーミングサービス
- AWS Simple Storage Service (S3)、Azure Blob Storage、Google Cloud Storage、AWS RedShift、Azure Databricks、Azure SQL Data Warehouse/Synapse Analytics、Google BigQuery、AWS EMR、Azure HDInsight、Google Dataproc、Snowflake などのデータレイクサービス
- AWS RDS、Aurora、DynamoDB、Azure SQL Database、Cosmos DB、Google Cloud SQL などの SQL および NoSQL データベースサービス

他に以下の機能があります。

- AWS Lambda、Azure Functions、Google Cloud Functions、AWS Macie、AWS API Gateway、Google Data Catalogue、Google Apigee、Azure Data Catalogue、API Management などのサーバーレスコンピューティングサービスまたは Functions as a Service (FaaS) における Voltage 変換

Voltage SecureData Cloud & Analytics では、セキュリティ対策が存在しない、または正しく構成されていないことによりデータ侵害が発生するリスクを除去できるほか、クラウドでの復号化の必要性がないためマルチクラウド環境でも切れ目のないデータ保護モデルを導入できます。

クラウドデータウェアハウスのための Voltage SecureData

Voltage SecureData Enterprise を Snowflake、Amazon Redshift、Google BigQuery、Azure Synapse などのクラウドデータウェアハウス (CDW) と連携させることにより、機密性の高いビジネス情報が侵害されるリスクを低減しながらもプライバシー規制を順守するフォーマットが保持されたトークン化データを使用して、クラウドで大規模な分析およびデータサイエンスを安全に実施することができます。

加えて、あらゆる言語の任意の構造化データタイプを必要な量だけ仮名化および匿名化できる Voltage SecureData Enterprise の高度なトークン化テクノロジーにより、異なるテクノロジー間でデータの保護を解除して再度保護する手間をかけずに、スムーズにデータを共有して受け渡すことができます。マルチクラウドエンタープライズ環境では、Voltage SecureData Enterprise により、さまざまな CDW、クラウドサービス、クエリツール、ビジネスインテリジェンスプラットフォーム、SaaS アプリケーション、クラウドサービスプロバイダー間のセキュリティのギャップを解消することができます。

Voltage SecureData Enterprise は、オンプレミスとクラウドのさまざまなデータベース、データウェアハウス、ビッグデータ環境においてデータのプライバシーと保護を提供する強固な機能を備えていますが、クラウドネイティブで強力な統合によりそれらの機能がさらに強化されます。PII、PHI、PCI、および知的財産などのその他のカテゴリの機密データを、AWS S3 バケットや Snowflake 外部ステージなどのクラウドにアップロードする前にオンプレミスで保護することも、アップロード後に保護することも可能です。

Voltage SecureData Enterprise の CDW ソリューションによりこれらの環境のデータの保護および保護の解除を直接管理できるため、機密性の高い結果セットがある場合に、そのうちのどれをデータサイエンティストや分析パートナーに公開するかを制御することができます。また、CDW に用意されているネイティブな役割ベースのアクセスポリシーを使用することで、Voltage SecureData Enterprise ではコードの変更や Voltage API の知識がなくても保護対象データへの透過的なアクセスが可能です。

マルチクラウドエンタープライズ環境では、Voltage SecureData Enterprise により、さまざまな CDW、クラウドサービス、クエリツール、ビジネスインテリジェンスプラットフォーム、SaaS アプリケーション、クラウドサービスプロバイダー間のセキュリティのギャップを解消することができます。

SaaS、COTS、社内アプリケーションのための Voltage SecureData Sentry

Voltage SecureData Sentry by OpenText™ は、クラウドソフトウェアサービスおよびオンプレミスアプリケーションのデータ保護に特化した製品です。Voltage のデータ保護テクノロジーを、Salesforce、ServiceNow、OpenText™ ALM Octane、Microsoft Dynamics 365 などの SaaS アプリケーション、および商用オフザシェルフ (COTS) アプリケーションに拡張することができます。また、Voltage SecureData Sentry により部分的な検索語句やワイルドカードの検索語句をサポートするセキュアなローカルインデックス、SMTP リレーのためのセキュアな電子メールアドレスフォーマットなどの他にはない機能が追加されるため、競合ソリューションでは影響を受けるアプリケーション機能もそのまま使用することができます。Sentry はデータフロー傍受の手法を使用してネットワークを流れる機密データを保護します。そのため、Voltage SecureData Enterprise と直接連携できない SaaS アプリケーションや COTS アプリケーションで使用されるデータのセキュリティも保護できます。

Sentry 搭載の Voltage SecureData

ハイブリッド IT への移行が進み SaaS アプリケーションへの依存度が高まっていますが、自社開発のアプリケーションを API レベルで連携することができない、またはそのような連携を実現するだけの開発リソースがない組織もあるでしょう。Sentry のテクノロジーにより、プログラミングにより API を連携することなく、このような社内アプリケーションの保護を推進することができます。Voltage SecureData Sentry により、ハイブリッド IT へのシンプルな移行が可能になるほか、プライバシーのコンプライアンスを維持する機能があらかじめ備えられているため価値実現までの時間を短縮し、エンドツーエンドで一貫した形でデータを保護できます。

Voltage SecureData Sentry はオンプレミスにもクラウドにも導入できます。Voltage SecureData Sentry は、HTTP プロキシやロードバランサーなどの Internet Content Adaptation Protocol (ICAP) 対応ネットワークインフラストラクチャと通信してクラウドとの間で送受信されるデータにセキュリティポリシーを適用し、Java Database Connectivity (JDBC) および Open Database Connectivity (ODBC) の API コールを取得して、データベース間で送受信されるデータにセキュリティポリシーを適用します。導入する場所にかかわらず、暗号化キーやトークン保管庫を第三者と共有することなくインフラストラクチャを完全に管理することができます。また、Voltage SecureData Sentry の検査モードにより、特定のデータフィールドや機密情報を含む添付ファイルを対象にセキュリティポリシーを適用することができます。

Voltage SecureData Sentry はデータフロー傍受の手法を使用してネットワークを流れる機密データを保護します。そのため、Voltage SecureData と直接連携できない SaaS アプリケーションや COTS アプリケーションで使用されるデータのセキュリティも保護できます。

主なメリット

エンタープライズデータ保護およびプライバシーによる高いスケーラビリティと機敏性

SecureData Cloud & Analytics および Voltage SecureData Sentry は、データ中心のセキュリティを適用することにより、データ自体を保護するとともに、クラウドで生じるセキュリティに関する主な課題に対応します。企業が運営するさまざまなクラウドサービスにおけるクラウド導入のリスクを軽減し、ハイブリッド IT に対して一貫性のあるデータセキュリティを提供します。

Voltage SecureData Cloud & Analytics および Voltage SecureData Sentry により、以下のことが可能です。

- 実績あるデータ中心のセキュリティによりアプリケーション、データ、ワークロードを安全に導入し、クラウド移行を促進

- クラウドベースの分析、アプリケーション、ビジネスプロセスにおけるデータプライバシーに関するコンプライアンスを実現
- クラウドデータウェアハウスシステムで大規模な分析およびデータサイエンスを安全に実施
- プラットフォームを問わないソリューションであるため、ハイブリッド IT、IaaS、SaaS、PaaS クラウドサービスにまたがるデータの保護を一貫性のある形で管理し、マルチクラウドエコシステムで柔軟なスケーラビリティを実現
- クラウドのデータに対する侵害や共有環境における内部からの攻撃のリスクを低減
- 攻撃者がデータを利用できない状態にしてデータ侵害の影響を無効化
- 個人データが確実に保護されるため、GDPR などの規制により求められている侵害の影響を受けた消費者への通知が不要
- データのライフサイクル全体を通してどこで保存または処理されるかにかかわらず一貫してデータを保護

クラウド移行のための一貫性のあるデータ中心のセキュリティ

企業におけるクラウドへの移行を安全に実現する鍵は、ハイブリッド IT 全体で一貫性を保ちながら永続的かつシームレスにデータのセキュリティを組み込むことにより、あらゆる環境を流れるデータのセキュリティを確保することです。Voltage SecureData Cloud & Analytics および Voltage SecureData Sentry を利用することにより、データ、アプリケーション、ワークフローをオンプレミスとクラウドで実行できる、信頼性の高い IT アーキテクチャを容易に導入できます。これにより、新規ビジネスモデルの導入を促進してコスト効率や競争力を高めると同時に、最も重要なデータを確実に保護することができます。

Voltage SecureData Cloud & Analytics および Voltage SecureData Sentry を利用することにより、データ、アプリケーション、ワークフローをオンプレミスとクラウドで実行できる、信頼性の高い IT アーキテクチャを容易に導入できます。これにより、新規ビジネスモデルの導入を促進してコスト効率や競争力を高めると同時に、最も重要なデータを確実に保護することができます。

お問い合わせ

www.opentext.com

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。

762-JA0030-005 | O | 02/24 |