opentext™ | Cybersecurity

データシート

Voltage SecureData Enterprise

新しいデータ主導型経済に対応したエンドツーエンドデータセントリックなセキュリティ

データセキュリティの課題

データ量、ユビキタスコンピューティングの高度化、ボーダレスなデータフローは、個人データの使用状況を把握する能力を超えています。このようなデータ主導型の経済では、さまざまな理由から、消費者は個人データの使用に関して企業を信頼できないと感じています。たとえば、データの不正使用に対して消費者が反応することにより企業への支出が約 3 分の 1 減少する可能性があります[1]。また、世界中の企業や政府に対するサイバー攻撃の数値は、頻度と重大度において増加し続けています。

Ponemon Institute の Cyber Crime Study[2] の調査結果は、暗号化技術を使用している企業はサイバー攻撃をより効率的に検出して封じ込めることができることを示唆しています。Ponemon Institute の 2021 Cyber Crime Study[2] によると、1,000 件から 10 万件までのレコードの場合、企業に発生する一般的なデータ侵害のコストは、現在 1 件あたり 424 万ドルとなっています。これは今までの最高記録です。いわゆる「大規模な」データ侵害で 5,000 万件から 6,500 万件のレコードが漏えいした場合、解決するためのコストは現在平均 4 億 100 万ドルに達しています。

しかし、このレポートによれば、人工知能 (AI)、機械学習 (ML)、ゼロトラスト、分析、暗号化をベースにしたセキュリティソリューションを採用している企業はすべて、データ侵害の潜在的なコストを低減しました。高水準の暗号化を使用している組織 (保存中と移動中に 256 以上の AES 暗号化を使用) の場合、データ侵害の総コストは平均 362 万ドルでした。これに対し、低水準の暗号化を使用しているか、暗号化を使用していない組織は、487 万ドルで、両者の差額は 125 万ドル (29.4%) でした。

Voltage SecureData Enterprise は、エンタープライズデータ保護のためのエンドツーエンドのデータ中心アプローチを提供します。ライフサイクル全体、つまりキャプチャされた時点から企業内を移動する間の全体で、

1. Bridging the Trust Gap in Personal Data, BCG, March 2018
2. Cost of a Data Breach Report 2021, Ponemon Institute, July 2021

Voltage SecureData 機能の特長

- あらゆる機密データを保護：さまざまなフォーマット保持データ保護手法を使用してプライバシー、決済に関する規格と法規のコンプライアンスや、データセキュリティのニーズに対処
- FIPS 140-2 と共通基準 (CC) 検証済みソリューション：機密データは、OpenText が先駆けとなった AES 暗号化の NIST 規格 FF1 モードで保護
- 演算負荷の高いニーズや、マルチクラウド、オンプレミス、ハイブリッド IT インフラストラクチャのデータ急増を想定して設計
- REST API、ローカルクライアントライブラリ、プロキシインターセプターとドライバーインターセプターなどの柔軟性の高いさまざまなインターフェイス、および幅広いデータベース、オペレーティングシステム、アプリケーション、プラットフォームとの統合が容易なクラウドネイティブ機能
- オブジェクトストレージ、ストリーミングサービス、データディスカバリ、データウェアハウス、API ゲートウェイ、サーバーレスコンピューティング (FaaS)、マネージド Kubernetes サービス、KMS、シークレットマネージャーなど、主要なクラウドサービスプロバイダーが提供するサービスとの連携が可能
- シームレスなキーローテーション、Bring Your Own Key (BYOK) など、ステートレスなソフトウェアと HSM ベースのキー導出と管理により、高い可用性とスケーラビリティを実現
- Voltage Structured Data Manager by OpenText を使用した統合型データディスカバリ、分析、分類により、データ保護とリスク軽減を自動化

データを保護できる唯一の包括的なデータ保護プラットフォームとなります。ライブ情報を高リスクで脅威の多い環境に露出させることはありません。これが、データ中心セキュリティの本質です。

Voltage SecureData Enterprise は、保存中、移動中、使用中の機密データを保護するプラットフォームです。ユースケースが1つでも数百でも、オンプレミスとマルチクラウドハイブリッド IT のあらゆるデータ保護要件を満たすように拡張できます。データを「匿名化」して攻撃者に役に立たないようにすると同時に、データプロセス、アプリケーション、サービスに対する操作性、有用性、参照整合性を維持します。保護対象のデータが本番システム、分析システム、テスト / 開発システム (トレーニングや品質保証など) のいずれにある場合でも、攻撃者にとってまったく価値のないものにすることによりデータ侵害を無効化します。

独自のアプローチによるエンドツーエンドのデータ保護

Voltage SecureData Enterprise では、実績のある独自のデータセントリックな保護アプローチを取り、アクセスポリシーがデータ自体と共に移動します。データのフォーマットや整合性に変更を加えることなくデータを保護でき、証明書やキーの発行と管理のコストを削減し、複雑さを解消します。その結果、金融サービス、保険、小売、医療、エネルギー、輸送、通信、その他の業界における大手企業が、全社でエンドツーエンドのデータ保護を実現して、わずか 60 日から 90 日で成功を収めています。これは、アプリケーションやデータベーススキーマに及ぼす影響が最低限に抑えられ、ほとんどの場合は影響がないためです。

短時間でデータセキュリティの成功を達成

ほとんどのアプリケーションが、保護対象のデータを変更せずに使用して動作することができます。機密データを最初にキャプチャするアプリケーションやビジネスの管理上の目的でライブデータを必要とするアプリケーションの場合、Voltage SecureData Enterprise は、数十年前のカスタムアプリケーションから最新のエンタープライズプログラムまでほぼすべてのシステムと簡単に連携が可能です。強力で一元管理されたポリシー制御 API により、OpenText™ Vertica™、NonStop、Teradata、IBM メインフレーム、Linux などのオープンシステム、オンプレミス、ハイブリッド、すべての主要なクラウドなど、さまざまなプラットフォームで暗号化とトークン化を実行できます。API により、ETL、データベースとアプリケーション、ネットワークアプライアンス、API ブローカー、Hadoop ディストリビューションなどのポートフォリオに広範にデプロイできます。SIEM システムでは、Voltage SecureData からイベントデータを取得して、データガバナンスレポーティング、アクティビティモニタリング、監査を実行できます。

Voltage SecureData Enterprise は、PCI DSS、HIPAA、GLBA、グローバルなデータプライバシーに関する諸規制 (GDPR、CPA/CPRA、KVKK、POPI など) に準拠して情報を保護します。またVoltage SecureData Enterprise は、ポイントツーポイントの暗号化 (P2PE) の PCI DSS 要件にも対応しているため、コンプライアンスの促進と、PCI 監査の対象範囲、時間、コストの削減が可能になります。

主なメリット

Voltage SecureData Enterprise により、グローバルな組織は、機密データの侵害を受けて露出させることなく、リスクの管理、コンプライアンスの達成、デジタルトランスフォーメーションのメリット享受を実現できます。

業界標準のフォーマット保持テクノロジー

OpenText™ は、NIST (National Institute of Standards and Technology) の AES FF1 Format-Preserving Encryption (FPE) モード規格の特許保有者兼公式ライセンサーとして業界をリードしています。この NIST 規格は、政府機関向けの承認済み、実証済みのデータセントリックな暗号化方式で、グローバルな組織用のデファクトスタンダードとして採用されています。NIST 規格は、組織が法規制や監査のコンプライアンスを維持し、実証済みの方法を使用してデータ漏えいを防止するために基準を設定するうえで重要な役割を担っています。

Voltage SecureData Enterprise は FIPS 140-2 と共通基準 (CC) による検証済みです。当社は、多数の標準化団体および作業グループ間での査読作業により、業界の発展を推進し続けています。

OpenText™ Cybersecurity Voltage の作業を、NIST、ANSI、IEEE、IETF、および独立したセキュリティ評価の専門家と協力して行っていることは、世界最大の金融サービス、銀行および保険機関、小売業者、製造業者、通信業者、決済処理業者に対して、当社がリーダーおよび信頼されるアドバイザーの立場であることを示しています。

NIST National Institute of Standards and Technology U.S. Department of Commerce

IEEE

Common Criteria

ANSI American National Standards Institute

IETF

透過的で動的なステートレスキー管理

アプリケーションとそのユーザーが一元管理されたポリシーに従って適切に認証されて許可された後に、ステートレスキー管理によってアプリケーションに必要なキーを安全に導出します。ステートレスキー管理は、次のようにして IT コストを削減し、管理上の負担を軽減します。

- キーデータベースの必要がないほか、データベースを継続的に保護したり、サイト間でキーを複製またはバックアップしたりするためのハードウェア、ソフトウェア、IT プロセスも不要です。
- シンプルなアプリケーション API により、ネイティブと Web サービスの両方で監督や e ディスカバリの要件を自動化します。
- アイデンティティとアクセス管理のフレームワークと容易に連携してポリシーによってデータフィールドへのデータレベルのアクセス権を動的に適用することにより、アクセスポリシーインフラストラクチャを最大限に再利用します。

GDPR などのプライバシー規制は、データセントリックな保護とポリシーをサービスとしてアプリケーションチームやプラットフォームチームに提供するようにグローバルな組織に新しい圧力を加えています。

Voltage SecureData は、PII、PHI、PCI などの機密データを匿名化してプライバシーを保護し、エンドツーエンドデータセントリックなセキュリティを提供します。Voltage SecureData は、EU 市民の個人データを保護し、新しい GDPR の仮名化ガイダンスに従うための強力で柔軟な暗号化を提供します。

政府機関で価値の高いデータを保護しています。Voltage SecureData は、業界初の Federal Information Processing Standard FIPS 140-2 と共通基準 (CC)、Format-Preserving Encryption (FPE) の検証を達成しました。政府機関や、政府機関を顧客としている民間請負業者は、民間部門のサイバーセキュリティに技術革新を行った強力で実績のあるテクノロジーを活用できるようになりました。

暗号化とトークン化

CBC、GCM、CTR のような AES 256 モードなど、従来の暗号化アプローチは、図 1 に示すように、データ構造、スキーマ、アプリケーションに大きな影響を与えます。Voltage FPE は、AES (Advanced Encryption Standard) アルゴリズムの NIST 規格 FF1 モードを使用するトークン化方式です。暗号化強度を犠牲にすることなく、機密データを暗号化しながら元のフォーマットを維持します。社会保障番号、クレジットカード、口座、生年月日、給与のフィールド、電子メールアドレスなどの構造化データについては、データベースを変更したり、アプリケーションの機能やパフォーマンスに影響を与えたりすることなく保護できます。

従来の暗号化方式ではデータの元のフォーマットが大幅に変更されます。たとえば、16 桁のクレジットカード番号を AES で暗号化すると長い英数字文字列が生成されます。したがって、互換性のないこのフォーマットを利用しやすくするには、データベーススキーマの変更が必要です。Voltage SecureData はデータのフォーマットを維持するため、データベーススキーマの変更やアプリケーションの変更を最小限に抑える必要がありません。バルク暗号化用のツールを使用すると、ファイルやデータベース内の大量の機密データを迅速に匿名化できます。通常、システム全体をわずか数日で迅速に保護し、コストを大幅に削減できます。Voltage SecureData は、暗号化パフォーマンスを高速化してビッグデータ、クラウド分析、IoT の大量のニーズを満たし、事実上無制限のデータタイプをサポートします。

納税者番号
934-72-2356

名：Gunther
姓：Robertson
SSN：934-72-2356
DOB：08-07-1966

FPE AES-FF1 モード	**253-67**-2356	**名：**Uywjlqo **姓：**Muwruwwbp **SSN:** **253-67**-2356 **DOB:** 08-07-1966
通常の AES-CBC モード	8juYE%Uks&dDFa2345^WFLERG	Ija&3k24kQotugDF2390^32 0OWioNu2(*872weW Oiuqwriuweuwr%oIUOw1@

図 1. Format-Preserving Encryption (FPE) と通常の AES 暗号化の比較

トークン化にはさまざまな種類があります。

- **可逆：**これは、トークン解除プロセス (プライバシー用語では仮名化) が存在することを意味します。
  - **暗号：**強力な暗号化を使用してデータ要素から生成されたトークン。クリアテキストのデータ要素は、暗号キーだけでは保存されません。Voltage SecureData には、暗号トークン化用に Format-Preserving Encryption (FPE) が用意されています。
  - **非暗号：**ステートレストークン化。ランダムに生成されたメタデータに、トークンを構築するために安全に組み合わされるデータが格納されています。Voltage SecureData には、非暗号トークン用に Secure Stateless Tokenization (SST) が用意されており、高いパフォーマンス、セキュリティ、拡張性を提供します。

    メモ：Voltage SecureData はデータベースボールトベースのトークン化を提供しないため、他のトークン化ソリューションの中心となっているトークンデータベースやトークンボールトが不要になり、カード所有者などの機密データを保存する必要がありません。SST が使用する事前に生成された静的テーブルのセットには、FIPS 乱数ジェネレーターで作成された乱数が格納されています。これらの静的テーブルを使用して、クリアテキスト PCI または PII の入力ごとに一意のランダムトークンを一貫した方法で生成します。その結果、元のデータと関係がないトークンが生成されます。SST ではトークンデータベースは不要であるため、ボールトベースの方式よりもトークン化プロセスの速度、スケーラビリティ、セキュリティ、管理性が向上します。
- **不可逆：**トークンを元の値に戻すこと (プライバシー用語では匿名化) が実用的ではないことを意味します。
  - 下位の環境での本番データを使用するときなどに、サードパーティ分析のために一方向関数を使用してトークンを作成します。Voltage SecureData には、不可逆トークン化用に Format-Preserving Hash (FPH) が用意されています。

VOLTAGE FORMAT-PRESERVING HASH を使用したデータの匿名化

クリックストリーム分析など、特定のユースケースでは、マスキングされたデータのリカバリが不必要なリスクとなるか、明らかに望ましくない場合があります。Voltage Format-Preserving Hash (FPH) には、FPE と同様にデータのフォーマットと参照整合性を維持するというメリットがありますが、元のデータを復元できないというメリットもあります。これにより、FPH は、従来の一方向変換技術 (SHA-256 など) とは異なり、非破壊式で柔軟なアプローチで、高パフォーマンスのデータ操作性を提供できます。

機密データのタイプ	保護対象データの例	クレジットカード番号
クレジットカード番号	1111-2222-3333-4444	1111-2287-9581-4444
納税者番号	111-22-3333	740-36-3333
住所	1234 Maple Street	7321 Uqhap Fbzir
電話番号	415-555-1234	819-913-0471
電子メールアドレス	surfer1@mycompany.com	d8wLa2k @ cPAzlu3la .8fq
運転免許証番号	A1234567	P9162047
誕生日	20-12-1970	10-01-1956
名前	王秀英	樂魚快的
IP ドレス	130.57.66.19	910.48.17.26
ジオロケーション	37.3974044, -121.9770816	81.7380129, -391.0193528
VIN	2W87Z7N139933	UV19PA07CBL13
治療コード	81082	81XXX

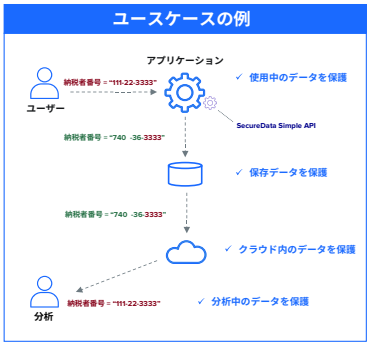

図 2. SecureData は世界で最も機密性の高いデータを保護

テストデータの安全な管理とコンプライアンス

Voltage SecureData は、テストデータ管理のユースケースについては、本番データを匿名化し、有効な構造のテストデータを作成します。これにより、開発者やユーザーは、機密データを露出させることなく QA やデータ分析を実行できます。Voltage SecureData Enterprise 管理コンソールにより、ポリシーを簡単に制御して監査機能を提供できます。Voltage Structured Data Manager (SDM) は、ライフサイクル全体にわたる構造化データの完全な管理を可能にします。SDM では、オンプレミス、クラウド、ハイブリッドシステム内の機密データを検出し、社内ポリシーに基づいてアーカイブ、保護、削除、その他の廃棄を定義して廃棄の対象データを分類できます。Voltage SecureData Enterprise と Voltage SDM の連携により、テストデータ管理を自動化してプライバシーのコンプライアンスをサポートし、テストおよび分析のユースケースで機密データを保護します。

メモ：OpenText Voltage のパートナーとプロフェッショナルサービスは、プロジェクトの範囲を決定し、高度な脅威に対処し、コンプライアンスの負担を軽減し、困難なデータプライバシーの課題を迅速に解決するのに役立ちます。

VOLTAGE SECUREDATA のアーキテクチャ

Voltage SecureData プラットフォームには、柔軟なデプロイメントオプションが用意されており、マルチクラウドハイブリッド IT インフラストラクチャ全体で高可用性とパフォーマンスを確保します。仮想アプライアンスをデプロイする場合でも、Kubernetes クラスター内で実行されるクラウドネイティブのコンテナ化マイクロサービスをデプロイする場合でも、SecureData を拡張して、最も要求の厳しいエンタープライズ要件を満たすことができます。

したがって、Voltage SecureData Enterprise のお客様は、さまざまな環境のユースケースに対処するために適切な手法を組み合わせて選択できます。同時に、複数の製品をデプロイして管理する際のコストと複雑さも回避できます。

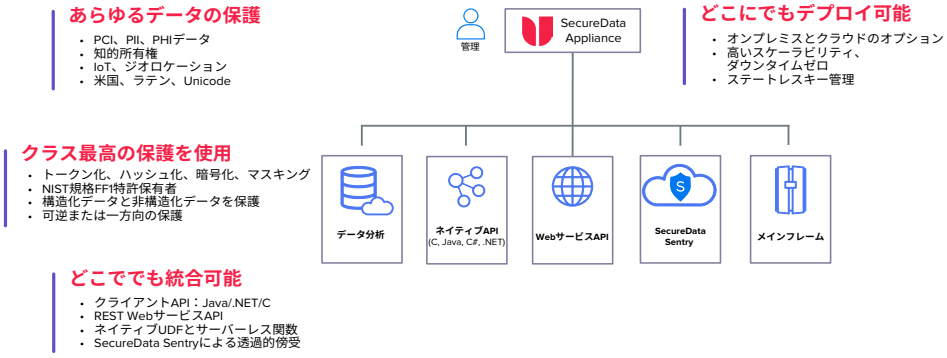

図 3. Voltage SecureData のアーキテクチャ

お問い合わせ
www.opentext.com

「当社は最新の金融サービスの規制を完全に順守しています。Voltage SecureData [Enterprise] のおかげで、既存のインフラストラクチャを変更することなく、業務への影響を最小限に抑えながらこれを実現できました。当社は、複雑な分散環境において、きわめてコスト効率の高い方法で機密データを保護しています」

Christian Stork 氏
戦略プロジェクト責任者
SIX

VOLTAGE SECUREDATA SENTRY：透過的なデプロイメントにより価値実現までの時間を短縮

ハイブリッド IT に移行して SaaS アプリケーションへの依存度が増すなか、組織は API レベルの統合に対応できない場合や、その開発リソースを持っていない場合があります。Voltage SecureData Sentry by OpenText は、ネットワークを流れる機密データを捕捉することにより透過的なデータ保護を実現します。Voltage SecureData Sentry は、ハイブリッド IT の移行を簡素化してセキュリティコンプライアンスを迅速に実現することにより、価値実現までの時間を短縮します。また、オープンなアプリケーションを壊したり、IT アーキテクチャの資格を再度大規模に付与したりすることなく一貫した方法でエンドツーエンドのデータ保護を実行します。

詳細はこちら：
www.microfocus.com/ja-jp/cyberres/data-privacy-protection/securedata-enterprise

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。

760-JA0020-005 | O | 12/23 |