opentext™ | Cybersecurity

データシート

Voltage SecureData Sentry

Voltage SecureData Sentry は、クラウドベースのサービスとオンプレミスアプリケーションにおける強力でデータセントリックなセキュリティの導入を簡素化し、加速します。Voltage SecureData Sentry は、アプリケーションのコード変更を回避すると同時に、新たな価値の創造とプライバシーポリシーのコンプライアンスを迅速に実現します。

製品の概要

ハイブリッド IT の導入における機会と変更

今日のデータ主導型企業では、組織の境界がなくなりつつあります。クラウドアプリケーションを採用することで、オンプレミスシステムやクラウドサービスとの間でデータが常に流れていることが保証されます。これには、SaaS アプリケーション、市販製品 (COTS) アプリケーション、社内独自のアプリケーションが含まれます。しかし、一般データ保護規則 (GDPR)、CCPA、PCI DSS、HIPAA などの厳格なプライバシー規制に加え、ホスト環境への信用性の限界もあり、個人データの保護は、そうしたデータが存在する場所を問わず、必須となっています。

データセキュリティの容易な導入

Voltage SecureData Sentry by OpenText™ は、オンプレミスとクラウドでのデータセキュリティの導入を容易にします。Voltage SecureData by OpenText™ ポートフォリオに追加されたこの製品は、既存のインフラストラクチャに簡単に導入できるデータ保護およびプライバシーの仲介を担います。Voltage SecureData Sentry はクラウド間だけでなく、アプリケーションやデータベースとの間で転

Voltage SecureData Sentry の主な利点

- さまざまなアプリケーションを変更することなくデータ保護を簡素化
- ハイブリッド IT 全体へのデータセキュリティの柔軟な導入により、価値実現までの時間を短縮
- クラウドサービス内の暗号化キーとデータを一元管理
- プライバシーのコンプライアンスとデータの安全な使用に対する業務中断を伴わないアプローチを推進
- Voltage のフォーマット保持型暗号 (FPE)、セキュア・ステートレス・トークナイゼーション (SST)、フォーマット保持型ハッシュ (FPH) の保護方法からフィールドレベルで選択できる柔軟性を提供
- 企業の規模や地域に関係なく、複数の SaaS アプリケーション間で暗号化されたデータの相互運用性を実現

送されるデータフィールドやファイルを保護します。このソリューションは、複数の保護メカニズムを組み合わせることにより、さまざまなコンテンツ形式とプロトコルをサポートしています。

Sentry は、プロキシ遮断と API を使用して、Salesforce、ServiceNow、ALM Octane、Microsoft Dynamics 365 など、幅広い種類の SaaS アプリケーションをサポートしています。このソリューションは、ネットワークを流れる機密データにアクセスして保護し、クラウドアプリケーションで使用されるデータの管理を維持できるようにします。また、同じ技術を使用して、プログラミングによる API 連携をせずに、市販製品 (COTS) アプリケーションと社内アプリケーションを保護することができます。Voltage SecureData Sentry のインスペクションモードでは、対象アプリケーションのデータフィールドを特定し、フィールドレベルの保護を容易に設定できます。

データ保護の価値実現までの時間を短縮
組織はクラウドコンピューティング戦略を採用して市場での優位性を獲得し、運用コストの削減などの経済的な節約を実現しています。しかし、機密性の高い企業の知的財産や個人データ (財務記録や医療記録など) については、新たなクラウドサービスの導入により、ビジネスとコンプライアンス上のリスクが生じます。こうした個人を特定できるデータをフィールドレベルで保護することにより、機密情報の漏えいの可能性を最小限に抑え、監査範囲を縮小し、コンプライアンスコストを削減できます。 さらに、Voltage SecureData Sentry の部分検索やワイルドカード検索をサポートするセキュアなローカルインデックス、SMTP リレー用のセキュアなメールアドレスフォーマットなどの追加機能により、競合ソリューションでは影響を受けるクラウド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。価値の高いデータを永続的に保護することにより、組織は柔軟な計算モデルや第三者の分析オプションをより安全に活用し、ビジネスにより貢献する新たなメリットを手に入れることができます。

多くの SaaS やクラウド CASB セキュリティモデルとは異なり、Sentry では独自の暗号キーやトークンテーブルに対する権限を保持し、さまざまなユースケースやアプリケーションへのセキュリティ導入を簡素化できるため、企業はライフサイクル全体を通じてビジネスデータをエンドツーエンドで管理できます。一貫した保護と参照整合性により、複数のサービスと環境間で保護されたデータのポータビリティが確保されます。Voltage SecureData Sentry は、アプリケーション内のデータ保護に必要な労力を削減し、データ漏洩のリスクを軽減することにより、データセントリックなセキュリティに対する企業の価値実現までの時間を短縮し、投資収益率を向上させるのに加え、導入の妨げとなる障害を排除してハイブリッド IT を実現します。

Sentry は、CASB ソリューションを置き換えるのではなく、シャドー IT の可視性、DLP、マルウェアの検出などの補完的なテクノロジーの提供を専門とするブローカーと共存し、暗号化処理を行うことでデータセキュリティを強化し、SaaS やクラウドサービスに加え、社内ネットワークの市販アプリケーションや自社開発アプリケーションに適用できる強力でデータセントリックな保護メカニズムを追加します。

データ漏えいリスクを低減
Voltage SecureData Sentry は、フォーマット保持型暗号 (FPE)、セキュア・ステートレス・トークナイゼーション (SST)、ステートレスな鍵管理、フォーマット保持型ハッシュ (FPH) など、Voltage by OpenText の市場をリードするデータ保護テクノロジーの導入を簡素化し、その範囲を拡大します。また、データを匿名化して攻撃者にとって無意味なものにするとともに、ビジネスプロセス、アプリケーション、サービスに対する価値を維持します。Voltage SecureData Enterprise は、保護されたデータが本番、分析、テスト / 開発のいずれの環境にあるかにかかわらず、攻撃者にとっての価値をなくすことで、データ侵害の影響を最小限にします。

Voltage ポートフォリオの NIST FF1 AES 暗号化規格のデータセキュリティ開発により、Voltage SecureData Enteprise は Common Criteria 認定を取得した唯一の FPE 製品となり、さらに FIPS 140-2 認定も取得しています。OpenText のデータセキュリティは、NIST、ANSI、IEEE、IETF 規格をサポートしているほか、独立したセキュリティ評価スペシャリストによるパブリックピアレビューを受けることで、製品の最高レベルのセキュリティ保証レベル認定を可能にしています。OpenText のデータセキュリティへの信頼は、第三者機関による世界最高水準の分析によって裏付けられています。

データプライバシーのコンプライアンスを容易に実現
多くの国や地域では、個人情報保護に関する規制強化が進められており、コンプライアンス要件への迅速な対応が求められています。たとえば、EU は GDPR を導入し、すべての住民のデータ保護を強化しました。GDPR では、個人データを保護する方法として、匿名化と仮名化を推奨しています。Voltage SecureData Sentry を使用すれば、Voltage の暗号化とトークン化を使用して、業務を中断することなくプライバシーコンプライアンスに対処できます。この 2 つのデータの非識別化の手法により、保護された情報をビジネスプロセスで引き続き使用でき、安全に再識別できます。

Voltage のデータ保護方法の最新技術であるフォーマット保持型暗号 (FPH) は、不可逆的な匿名化を実行して、匿名化を求めるデータ消去の権利である GDPR 第 17 条 (通称「忘れられる権利」) をサポートし、不可逆的な匿名化を実現します。Voltage の FPH は、FPE の強みとユースケースの汎用性を備えた一方向変換を実行し、既存のデータベーススキーマやアプリケーションを変更せずに使用したり、データ分析の使用を妨げることなく作業できます。

機密データの検出と相互運用性
Voltage SecureData Sentry は、オンプレミスで集中管理し、ユーザーに対して透明性を確保しながら、ポリシーに従って機密データの保護とアクセスを行います。また、JSON、XML、HTML、docx、xlsx、csv など、さまざまなコンテンツ形式をサポートしています。Voltage SecureData Sentry は、HTTPS や SMTP などの主要な通信プロトコルに加え、REST、SOAP、JDBC、ODBC などの一般的な API を介してストリーミングされたデータにアクセスします。

一貫した保護機能を備えた JDBC および ODBC プロトコルのサポート機能と、オンプレミスとクラウドへの高い拡張性を実現するステートレスな鍵管理機能は、今日の市場では

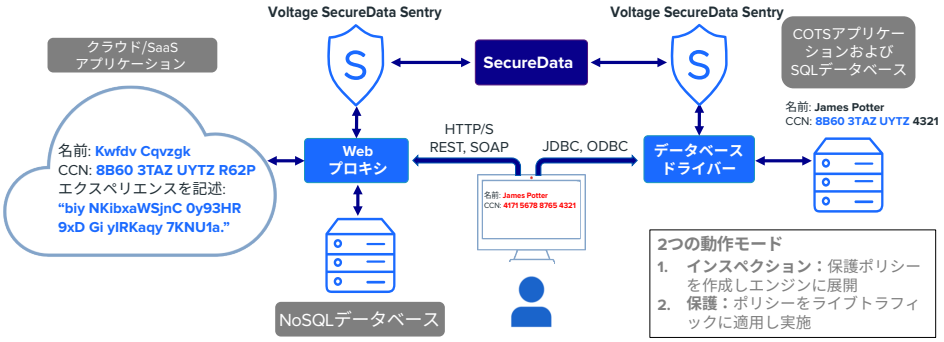

図 1. Voltage SecureData Sentry は、オンプレミスとクラウドで一貫性のある透過的なデータ保護を実現します。

独自の機能で、エンタープライズクラスのパフォーマンスを実現します。Voltage SecureData Sentry は、企業の規模や地域に関係なく、複数の SaaS アプリケーション、セキュアなアウトソーシングおよび同様のユースケース間で暗号化データの相互運用を可能にします。

Voltage SecureData Sentry のコンポーネント	説明
Voltage SecureData Sentry 管理コンソール	Sentry を管理するロールベースの管理インターフェイスで、完全な監査が可能。ポリシーは、アプリケーションタイプとドキュメントタイプ、規制要件に基づいて作成。
Voltage SecureData Sentry エンジン	コンテンツ検出、データ保護、アクセスを実行し、HA、およびロードバランシングオプションを使用して拡張可能。高パフォーマンスで、フォワードプロキシとリバースプロキシ、データベースドライバーをサポート。
Voltage SecureData Sentry データベースプライバシーサービス	データベースのデータを保護するサービスで、NoSQL データベースの ODBC、JDBC、REST をサポート。
Voltage SecureData Sentry 保護メカニズム	Voltage の FPE、SST、FPH、およびステートレスキー管理をサポートするメソッドで、すべてのコンテンツ形式に対応。

Voltage SecureData Sentry のアーキテクチャ
Voltage SecureData Sentry はオンプレミスにもクラウドにも導入できます。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 コールを遮断して、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ボルトを他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できます。また、Voltage SecureData Sentry のインスペクションモードにより、機密情報を含む特定のデータフィールドや添付ファイルにセキュリティポリシーを適用できます。

Voltage SecureData Sentry は、Voltage SecureData Enterprise プラットフォームの共通インフラストラクチャを使用します。そのため、複数の製品を導入および管理するコストと複雑さを回避しながら、さまざまな環境におけるユースケースに対応する適切なデータの匿名化のための暗号化技術の組み合わせを選択することができます。

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

お問い合わせ
www.opentext.com

主な機能

SaaS アプリケーション
- Salesforce、Microsoft Dynamics、OpenText™ ALM Octane などの外部ホスト型クラウドアプリケーションで透過的なデータ保護を実現するデータプライバシーブローカー機能。

市販および社内アプリケーション
- 市販製品 (COTS) アプリケーションおよび社内のエンタープライズアプリケーションで透過的なデータ保護を実現するデータプライバシーブローカー機能。

データ傍受
- ICAP/S、HTTP/S、SMTP などの主要な通信プロトコル、および REST、SOAP、JDBC、ODBC などの一般的な API を介してデータを傍受。

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-JA0002-004 | O | 12/23 |