THALES

www.thalesesecurity.com

‹Thales e-security›

Vormetric Data Security Platform

VORMETRIC DATA SECURITY PLATFORM

破壊的なセキュリティ侵害が日々絶え間なく発生し、規格への準拠に対する要求が厳しさを増す中、お客様の組織はさらに多くの環境やシステム、アプリケーション、プロセスおよびユーザーへとデータ保護を拡張する必要性に迫られています。Thales e-Security の Vormetric Data Security Platform を使用すれば、組織全体を通じて保存データのセキュリティを効果的に管理できるようになります。伸展性のあるインフラストラクチャをベースに構築されている Vormetric Data Security Platform は、個別に実装可能ないくつかの製品で構成されており、これらを使用することで鍵とポリシーの効率的な集中管理が可能になります。その結果、お客様のセキュリティチームがデータセキュリティのポリシーや規格への準拠に関する指令やベストプラクティスに対処しつつ、管理の手間と総保有コストを削減することが可能になります。

Vormetric Data Security Platform には、データベースやファイル、コンテナへのアクセスを保護および制御する機能があります。これにより、クラウド環境や仮想環境、ビッグデータ環境、物理的な環境に入っている資産を保護できます。効率的かつ拡張可能なデータセキュリティプラットフォームである Vormetric Data Security Platform なら緊急の要件に対処でき、新たなセキュリティ上の課題や準拠要件が発生した場合の迅速な対応が可能となります。

セキュリティと規格への準拠の強化

セキュリティチームがこれらのフレキシブルかつスケーラブルなソリューションを活用することで、さまざまなユースケースに対応し、組織全体の機密データを保護することが可能になります。このプラットフォームには、ペイメントカード業界データセキュリティ基準（PCI DSS）や一般データ保護規則（GDPR）、医療保険の携行性と責任に関する法律（HIPAA）、連邦情報セキュリティマネジメント法（FISMA）、その他地域のデータ保護およびプライバシー関連の法律を含めた、セキュリティとプライバシーに関するさまざまな指令に総合的に対応するための機能があります。Vormetric Data Security Platform は、データがクラウドや外部プロバイダのインフラストラクチャに保管されている場合にも、APT 攻撃と闘い、インサイダーによる悪用からデータを防御して、一貫した制御を確立するための強力なツールです。

スタッフおよびリソースの効率の最大化

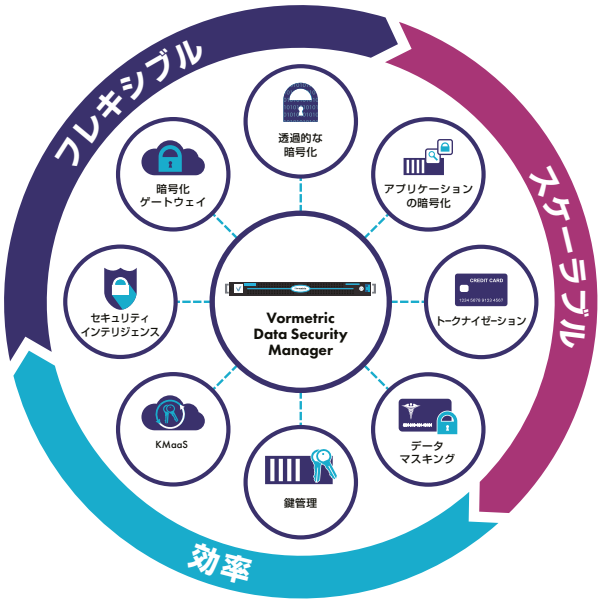
Vormetric Data Security Platform では、Web ベースの分かりやすいインターフェイスや、コマンドラインインターフェイス（CLI）、また REST や SOAP、Java、.Net、C などのアプリケーションプログラミングインターフェイス（API）により、管理作業が簡略化・効率化されます。このソリューションによって、保存データのセキュリティを迅速に一貫して適用できるため、スタッフの効率と生産性を最大化することが可能です。またこのプラットフォームは、Vormetric Orchestrator を使用したオーケストレーションとオートメーションにも対応しています。その上、高性能なソリューションによってサービスデリバリのインフラストラクチャにかかる負荷が軽減され、仮想サーバーリソースと物理サーバーリソースの効率的な利用が可能になります。

機能

- 透過的なファイル暗号化
- アプリケーション層の暗号化
- トークナイゼーション
- スタティックデータマスキング
- ダイナミックデータマスキング
- クラウドストレージの暗号化
- FIPS 140-2、コモンクライテリア認証済の鍵管理
- Key Management as a Service
- 特権ユーザーのアクセス制御
- アクセス監査ログ
- バッチデータの暗号化とトークナイゼーション
- オーケストレーションとオートメーションのサポート

環境と技術のサポート

- IaaS、PaaSおよびSaaS：アマゾン ウェブ サービス、Google Cloud Platform、Microsoft Azure、Salesforce、Amazon S3（および互換性のあるAPIサービス）
- OS：Linux、Windows および Unix
- ビッグデータ：Hadoop、NoSQL、SAP HANAおよびTeradata
- コンテナ：Docker
- データベース：IBM DB2、Microsoft SQL Server、MongoDB、MySQL、NoSQL、Oracle、Sybase その他
- すべてのストレージ環境に対応



プラットフォームの長所

- 保存データのセキュリティポリシーの集中管理
- Vormetric Data Security Platformおよびサードパーティ製の暗号化製品の鍵を管理
- 物理環境、仮想環境、クラウド環境およびビッグデータ環境のすべてにわたって一貫したセキュリティと規格への準拠
- あらかじめ定義されたSIEMダッシュボードにより、きめ細かい実行可能なファイルアクセスのインテリジェンスを実現
- フレキシビリティと拡張性により、ユースケースが増えても迅速に対応可能

準拠対象の規格

- PCI DSS
- GDPR
- HIPAA/HITECH
- NIST 800-53
- FISMA
- PIPA
- データレジデンシーとプライバシーに関する地域的な規則

総所有コストの削減

Vormetric Data Security Platform を使用すれば、保存データの保護が簡略化され、コストも削減されます。このプラットフォームにより、IT 部門とセキュリティ部門が、組織全体のデータを統一された反復可能な方法で迅速に保護することが可能になります。組織中に散在する多くの個別の製品を使用する代わりに、Vormetric Data Security Platform を使用すれば、一貫した統合管理というアプローチをとることができます。

プラットフォーム構成製品

Vormetric Data Security Platform に含まれる製品は以下のとおりです。

- **Vormetric Data Security Manager -** 集中管理により、すべての構造化および非構造化データに対する暗号化やアクセスポリシー、セキュリティインテリジェンスを一貫した反復可能な方法で管理できるようになります。FIPS 140-2 およびコモンクライテリアで認証された仮想アプライアンスや物理アプライアンスとして利用できます。
- **Vormetric Transparent Encryption -** ファイルシステム内で動作するソフトウェアエージェントで、ファイルやディレクトリ、ボリュームに対して、高性能な暗号化と最小権限のアクセス制御を行います。構造化データベースと非構造化ファイルの両方を暗号化することが可能です。次の 2 つの拡張機能があります。
  - **Container Security -** Docker™コンテナ内にコントロールを確立することで、他のコンテナやプロセス、さらにホスト OS も機密データにアクセスできないようにすることができます。暗号化やアクセス制御、データアクセス記録をコンテナごとに適用するために必要な機能です。
  - **Live Data Transformation -** ファイルやデータベースの暗号化と定期的なキーローテーションを（ファイルやデータベースの使用中でも）、ユーザーやアプリケーション、ビジネスのワークフローを乱すことなく実行できます。
- **Vormetric Tokenization with Dynamic Data Masking -** データベース内の機密性の高いフィールドを保護するためのフォーマット保持トークン化と、表示のセキュリティに対するポリシーベースのダイナミックデータマスキングを簡単に実行できます。
- **Vormetric Application Encryption -** NIST 標準の AES 暗号化とフォーマット保持暗号化（FPE）を既存のアプリケーションに追加するプロセスを合理化します。高性能な暗号化処理と鍵管理処理を実行するために使用可能な標準ベースの API です。
- **Vormetric Key Management -** Vormetric Data Security Platform 製品や TDE、KMIP 準拠のクライアントに対する鍵のストレージを集中的に管理・保護したり、証明書を安全に保管したりするための、統合された鍵管理機能です。
- **Vormetric Key Management as a Service -** 暗号化鍵とポリシーに対する強いガバナンスの確立を可能にします。それにより、SaaS 環境をフル活用しつつ、複雑な処理やリスクを最小限に抑えることができます。
- **Vormetric Cloud Encryption Gateway -** Amazon Simple Storage Service（Amazon S3）や、S3 と互換性のあるオブジェクトストレージサービスのようなクラウドストレージ環境にあるファイルを保護できるようになります。暗号化やオンプレミスの鍵管理、詳細なロギングの機能があります。
- **Vormetric Protection for Teradata Database -** お使いの Teradata 環境に、強力な保存データのセキュリティ機能を迅速かつ効率的に実装できます。きめ細かい保護機能により、Teradata データベース内の特定のフィールドやカラムの暗号化が可能になります。
- **Vormetric Security Intelligence -** ルートユーザーのアクセスを含めたファイルアクセス操作の詳細で監査可能な記録を提供する、詳細なログを作成します。セキュリティ情報およびイベント管理（SIEM）システムとの統合が可能になります。ダッシュボードとレポートがあらかじめパッケージされており、規格への準拠に関する報告の合理化とより迅速な脅威の検出が実現されます。
- **Vormetric Orchestrator -** 選択された Vormetric Data Security Platform 製品の実装、構成、管理および監視を自動化します。繰り返し行うタスクを自動化することにより、操作を簡素化してエラーをなくし、実装をスピードアップする機能です。
- **Vormetric Batch Data Transformation -** データベース内にある機密性の高いカラム情報を、より迅速かつかんたんにマスキング、トークン化または暗号化できるようになります。まず、これを使用してから、Vormetric Tokenization や Vormetric Application Encryption によって既存の機密データを保護することができます。スタティックデータマスキングのサービスを行います。

VORMETRIC DATA SECURITY MANAGER

Vormetric Data Security Manager（DSM）は、すべてのVormetric Data Security Platform 製品に対する管理とポリシーを集中管理します。DSM を使用することで、準拠要件や規制要項、業界のベストプラクティスに効率的に対応し、実装や要件の進化に順応していくことが可能になります。このソリューションは LDAP ディレクトリサービスとの統合が可能なため、ユーザーとグループに対する管理を確立して、組織全体でのセキュリティのポリシーの実施を保証することができます。またこのソリューションでは、もっとも厳しい準拠要件への対応に必要なログも作成できます。

FIPS 認証済の、信頼性の高いセキュアなシステム

確実な稼働とセキュリティを最大限に維持するため、DSM のコンポーネントは冗長化されています。アプライアンスをクラスタ構成にしてフォールトトレランスと高可用性を確保することもできます。厳密な職掌分散ポリシーを実施することで、1 人の管理者がデータのセキュリティ作業や暗号化鍵、管理作業を独占しないように規制できます。また、管理者画面へのアクセスに対する二要素認証に対応しています。

フレキシブルな実装オプション

DSM は、さまざまな独自環境やセキュリティ要件に対応可能です。利用可能なフォームファクタには次のようなものがあります。

- FIPS 140-2 Level 1 認証済の仮想アプライアンス
- FIPS 140-2 Level 2 認証済の V6000 ハードウェアアプライアンス
- FIPS 140-2 Level 3 認証済で、nShield のリモートアクセスをサポートする Thales nShield Solo ハードウェアセキュリティモジュール（HSM）が装備された V6100 ハードウェアアプライアンス

このプラットフォームは、AWS（アマゾン ウェブ サービス）Marketplace と Microsoft Azure Marketplace でも利用できます。

主な特長

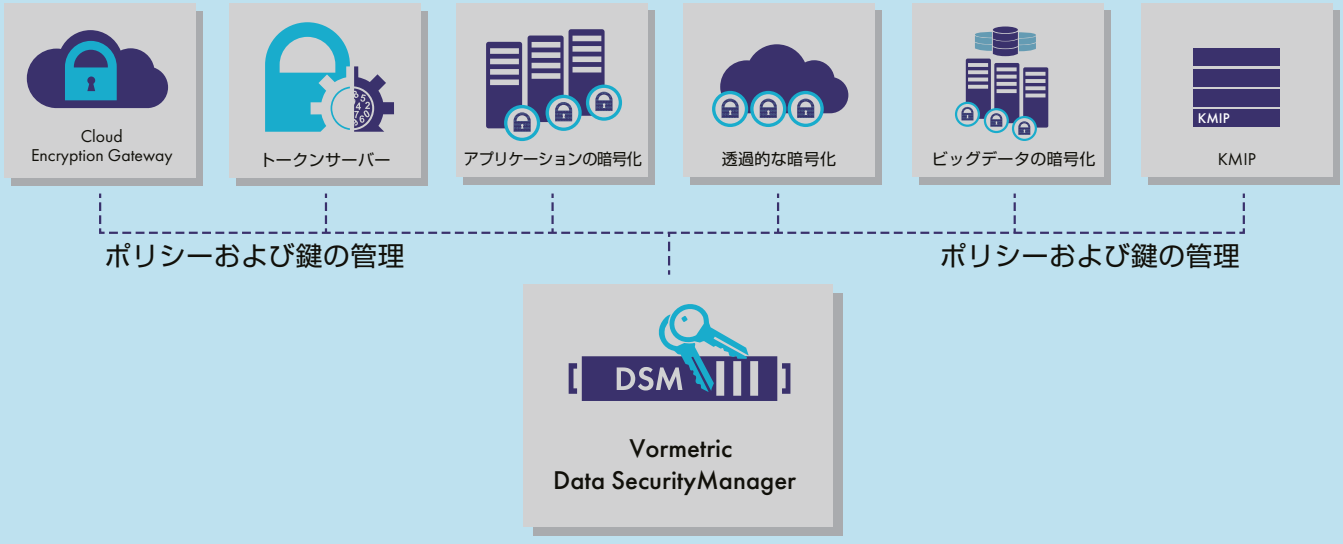
- 1つのコンソールですべてのプラットフォームポリシーと鍵管理に対応
- マルチテナント環境のサポート
- 10,000エージェント規模まで検証された拡張性
- クラスタ化による高可用性運用
- ツールキットおよびプログラミングAPI
- 既存の認証インフラストラクチャとの統合が簡単
- RESTful APIのサポート
- 多要素認証とnShieldのリモート管理
- オーケストレーションとオートメーションのサポート

技術仕様

プラットフォームのオプション

- FIPS 140-2 Level 1仮想アプライアンス
- FIPS 140-2 Level 2ハードウェアアプライアンス
- FIPS 140-2 Level 3ハードウェアアプライアンス
- AWS MarketplaceおよびAzure Marketplace

V6100 DSMでは、スマートカードによる多要素認証を使用したセキュアなnShield HSMのリモート管理が可能です



ハイブリッドエンタープライズ全体で統一された管理運営

DSM を使用すれば、Vormetric Data Security Platform 製品や IBM Security Guardium Data Encryption、Microsoft SQL TDE、Oracle TDE その他の KMIP に準拠する暗号化製品で生成された鍵を含む、ヘテロジーニアスな暗号化鍵の集中管理が可能になるため、コストが最小限に抑えられます。DSM には Web ベースの直感的なコンソールと API が入っており、これを使用してエンタープライズ全体で暗号化鍵やポリシー、監査の管理を行います。ログの収集も集約化されます。

DSM の仕様

ハードウェア仕様

シャーシ	1Uラックマウント、幅17″ × 奥行20.5″ × 高さ1.75″（43.18 cm × 52.07 cm × 4.5 cm）
重量	V6000：21.5 lbs（9.8 kg）、V6100：22 lbs（10 kg）
メモリ	16GB
ハードディスク	デュアルSAS RAID 1（FIPSタンパー証跡シール付き）
シリアルポート	1
イーサネット	2 × 1Gb
IPMI	1 × 10/100Mb
電源	取り外し可能な80 PLUS認証済（100VAC-240VAC/50-60Hz）400W電源2基
シャーシ侵入検知機能	あり。上部カバーにもFIPSタンパー証跡シール付き
最大BTU	最大410BTU
動作温度	10～35°C（50～95°F）
保管温度	-40～70°C（-40～158°F）
動作相対湿度	8～90%（結露のないこと）
保管相対湿度	5～95%（結露のないこと）
安全機関による認証	FCC、UL、BIS認証
FIPS 140-2 Level 3 HSM	nShield Solo HSMが装備されたV6100モデル
HSMのリモート管理	V6100のみ。オプションのnShield Remote Administrationキットが必要

ソフトウェア仕様

管理用インターフェイス	Secure Web、CLI、SOAP、REST
最大管理ドメイン数	1000以上
APIのサポート	PKCS #11、Microsoft Extensible Key Management（EKM）、SOAP、REST
セキュリティ認証	ユーザー名／パスワード、RSA 二要素認証（オプション）
クラスタのサポート	あり
バックアップ	手動バックアップおよび自動スケジュールバックアップ。M of N 鍵リストア
ネットワーク管理	SNMP、NTP、Syslog-TCP
Syslogフォーマット	CEF、LEEF、RFC 5424
認証および検証	FIPS 140-2 Level 1、FIPS 140-2 Level 2、FIPS 140-2 Level 3 コモンクライテリア（ESM PP PM V2.1）

仮想マシンの最低仕様 — 仮想アプライアンスに対して推奨される仕様

CPU数	2
RAM容量	4GB
ハードディスク容量	100GB
シンプロビジョニングのサポート	あり

VORMETRIC TRANSPARENT ENCRYPTION

Vormetric Transparent Encryption には、保存データの暗号化や、特権ユーザーのアクセス制御、セキュリティインテリジェンスのログ収集などの機能があります。このソリューションを使用して、物理環境や仮想環境、ビッグデータ、Docker およびクラウド環境を問わず、構造化データベースと非構造化ファイルを保護することができます。

このソリューションの透過的なアプローチにより、アプリケーションやインフラストラクチャ、業務手順を変更することなく、暗号化を実施することができます。他の暗号化ソリューションと異なり、暗号化鍵を適用しても保護は完結しません。Vormetric Transparent Encryption ではその後も、アクセスのログを記録し、ユーザーやプロセスによる不正アクセスから防御するポリシーを実施し続けます。このような機能によって、データを継続的に防御および制御することができます。

すべての環境でスケーラブルな暗号化が可能

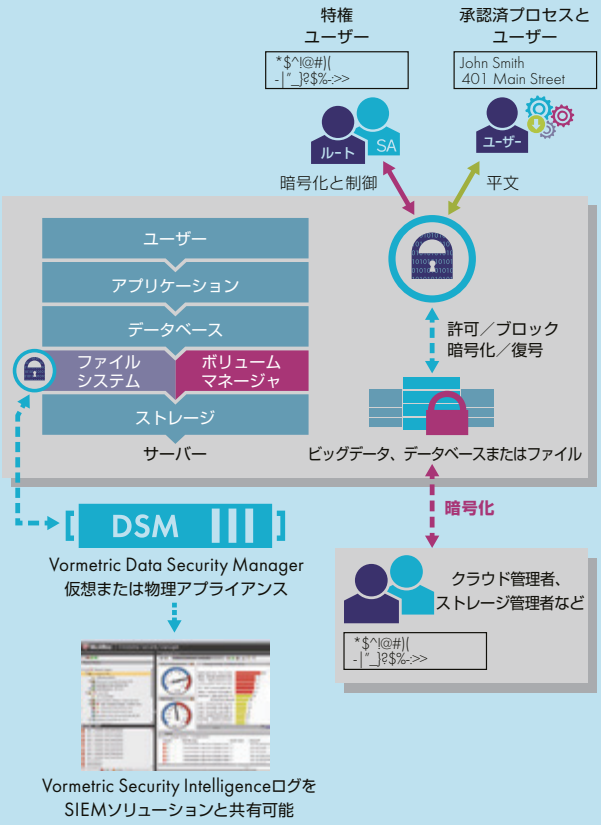
Vormetric Transparent Encryption は、サーバー上のファイルシステムレベルまたはボリュームレベルで動作するエージェントです。このエージェントは、Windows や Linux、Unix など幅広いプラットフォームに利用可能で、基礎となるストレージ技術に関係なく、物理環境、仮想環境、クラウド環境、Docker 環境およびビッグデータ環境で使用できます。管理者は Vormetric Data Security Manager（DSM）を介して、すべてのポリシーと鍵の管理を実行します。

このソリューションはエージェントベースのアーキテクチャになっており、サーバー上で暗号化を実行できます。その結果、従来のプロキシベースのソリューションで問題となる、ネットワーク上の固定ノードを通じてすべての情報がルーティングされるボトルネックが解消されます。最近の CPU（Intel AES-NI や IBM Power8 in-core、Oracle SPARC など）に内蔵されている暗号ハードウェアモジュールを活用することで、性能と拡張性がさらに強化されます。

強力できめ細かいユーザーアクセス制御

このエージェントでは、APT（標的型）攻撃や管理者による不正からデータを保護するために、きめ細かく細分化された特権ユーザーアクセスポリシーを施行します。

ポリシーは、ユーザーやプロセス、ファイルのタイプ、時刻その他のパラメータごとに適用できます。施行オプションは非常に細かく設定可能で、ユーザーが平文のデータにアクセスできるかどうかだけでなく、どのようなファイルシステムコマンドが利用可能かも制御できます。



主な利点

- 複数のプラットフォームや環境にまたがって暗号化を拡張可能
- 実装が簡単：アプリケーションのカスタマイズ不要
- 特権インサイダーによる悪用に対する強力な保護措置を確立

主な特長

- 業界でもっとも幅広いプラットフォームのサポート：Windows、Linux、Unixオペレーティングシステム
- 高い暗号化性能
- 強力な暗号化とSuite Bプロトコルのサポート
- ユーザーやアプリケーション、プロセスからのアクセス試行を、許可されたもの、拒否されたもの、および制限されたものを含めてすべて記録
- 役割ベースのアクセスポリシーにより、アクセスされるデータ、データにアクセス可能な人物、場所、時間および方法を制御
- 特権ユーザーが、平文データにアクセスすることなく自分の作業を実行可能
- 拡張機能により、よりきめ細かいDockerコンテナへのサポートやゼロダウンタイムでのデータ変換などの追加機能が利用可能

技術仕様

拡張機能のライセンス

- Container Security
- Live Data Transformation

プラットフォームのサポート

- Microsoft：Windows Server 2008および2012
  Linux: Red Hat Enterprise Linux（RHEL）、SuSE Linux Enterprise Server、Ubuntu
- UNIX: IBM AIX, HP-UX*、Solaris*

データベースのサポート

- IBM DB2、Microsoft SQL Server、MySQL、NoSQL、Oracle、Sybase その他

アプリケーションのサポート

- Documentum、SAP、SharePoint、カスタムのアプリケーション その他を含めたすべてのアプリケーションに対して透過的

ビッグデータのサポート

- Hadoop：Cloudera、Hortonworks、IBM
- NoSQL：Couchbase、DataStax、MongoDB
- SAP HANA
- Teradata

暗号化ハードウェアの高速化

- AMDおよびIntel AES-NI
- IBM P8暗号化コプロセッサ
- SPARC暗号化

エージェント認証

- FIPS 140-2 Level 1

コンテナのサポート

- Docker

* Vormetric Transparent Encryptionリリース5.xのエージェントではHP-UXとSolarisのみサポート

CONTAINER SECURITY

コンテナという技術は、かつてないほどの利点をもたらしていますが、同時に新しいリスクも伴っています。Vormetric Container Security には、暗号化やアクセス制御、データアクセスのログ取得に関する重要な機能があります。これによって、動的なコンテナ環境にあるデータに対する強力な保護手段を確立することができます。

このソリューションは Vormetric Transparent Encryption に対するソフトウェアライセンスです。セキュリティチームはこのライセンスによって、コンテナ内部の制御を確立することができます。この拡張機能によって、暗号化やアクセス制御、データアクセス監査ログを、コンテナ内部のデータとコンテナからアクセス可能な外部ストレージの両方に対して、コンテナごとに適用できます。

準拠要件への対応

今日、多くのセキュリティチームにとって、コンテナやイメージの中で行われているデータへのアクセスの管理と追跡を行うために許される権限は限られています。その結果、チームに関連する内部セキュリティポリシーや規則要項すべてに準拠することが難しくなっています。Vormetric Transparent Encryption の拡張機能には、準拠要件や規則要項に対応するために必要な暗号化、データアクセス制御および監査機能が入っています。このソリューションを活用すれば、扱う資産がペイメントカードやヘルスケアの記録、その他の機密性の高い資産であっても、機密データを保護することができます。

Docker 環境での総合的で きめ細かいセキュリティの確立

Vormetric Container Security では、Docker のオープンな API とインターフェイスを活用することで、コンテナに格納されている情報やコンテナからアクセスするデータに対するポリシーベースの暗号化、アクセス制御、およびデータアクセスの監査ログの取得が可能になります。このソリューションにより、最も機密性の高い情報を使用する実環境のアプリケーションを安全に実装する際に必要となる、安定した運用と簡単な実装、しっかりした保護が実現します。

効率性に優れた強力な保護機能を採用

Vormetric Container Security には、次のような特長があります。

- **総合的な保護 -** コンテナのボリュームを保護して、データが不正にアクセスされたりエクスポートされたりすることを防ぎます。
- **きめ細かい制御と視認性 -** 特定のユーザーやプロセス、リソースのセットに基づいたきめ細かいアクセスポリシーを確立します。コンテナの間を切り離して、許可されたコンテナのみが機密情報にアクセスできるようにします。
- **フレキシブルで効率的な実装 -** アプリケーションやコンテナ、インフラストラクチャを一切変更することなく、コンテナ環境内で制御を行うことができます。

主な利点

- コンテナ内での、ルートユーザー／特権ユーザー／不正なユーザーによるアクセスから防御する
- 他のコンテナからの権限エスカレーション攻撃からデータを保護する
- コンテナ間のデータアクセスを簡単に切り離せる
- データアクセス制御とコンテナレベルの監査に関する準拠要件を満たす

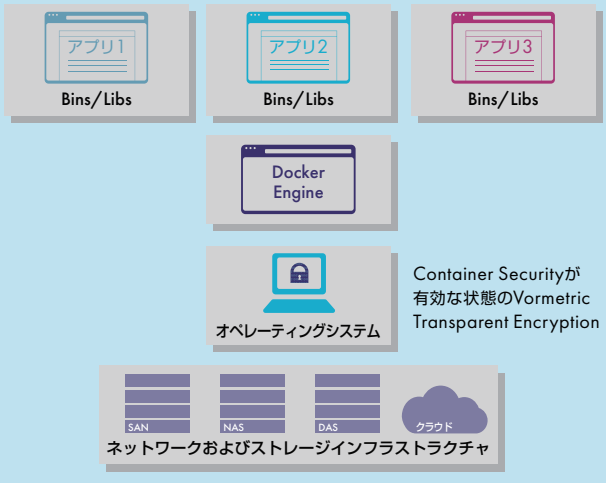
主な特長

- Dockerのホストとイメージの両方に対して、暗号化やアクセス制御、データアクセス監査ログの取得を行う
- コンテナ内に格納されたデータのほか、コンテナからアクセス可能なデータに対応する制御を行う
- 特定のユーザー、プロセスおよびリソースのセットに対するきめ細かい制御を可能にする
- アプリケーションやコンテナ、インフラストラクチャに対する変更が不要
- Vormetric Transparent Encryptionとして設定されたものと同じエージェントとインフラストラクチャを使用する

技術仕様

プラットフォーム／環境のサポート

- Docker
- Red Hat Enterprise Linux 7.x
- 物理システム、VMs およびAWS EC2インスタンス上で動作可能



LIVE DATA TRANSFORMATION

保存データの暗号化の実装と管理では、平文を暗号文に変換するときや、すでに暗号化されているデータの鍵を変更するときに、問題が生じることがあります。従来、このような作業では、ダウンタイムを計画するか、非常に手間のかかるデータのクローン作成と同期作業を行う必要がありました。Vormetric Transparent Encryption の Live Data Transformation Extension 機能を使用すれば、そのような手間が省け、暗号化と鍵の変更が可能になって、これまでにない稼働時間と管理面での効率化が実現します。

ゼロダウンタイムでの暗号化と鍵のローテーション

Live Data Transformation には、次のような鍵に関する機能があります。

- **ゼロダウンタイムでの暗号化の実装 -** このソリューションにより、管理者はユーザーやアプリケーション、ワークフローに対するダウンタイムや混乱を生じさせることなく、データを暗号化することができます。暗号化の実行中、ユーザーとプロセスは通常どおり、データベースやファイルシステムを操作できます。
- **シームレスで混乱が発生しない鍵のローテーション -** セキュリティのベストプラクティスにおいても多くの規則要項においても、定期的な鍵のローテーションが必要となります。Live Data Transformation では、そのような要件に迅速かつ効率的に対処できます。このソリューションにより、データを複製したり、関連のアプリケーションをオフラインにしたりしなくても、鍵のローテーションを実行できます。
- **高度なリソース管理 -** 大きなデータセットを暗号化する場合、長時間にわたってかなりの CPU リソースが必要になる場合があります。Live Data Transformation には高性能な CPU 管理機能があるため、管理者は暗号化と他の業務の間でリソースの需要のバランスを取ることができます。たとえば、暗号化に消費できるシステムの CPU を、業務時間中には 10% のみだが、夜間や週末には 70% と指定するリソース管理ルールを定義することが可能です。
- **バックアップとアーカイブのバージョン管理 -** Live Data Transformation には、鍵のバージョン管理機能とともに、効率的なバックアップとアーカイブ復元機能があります。これにより、より迅速なアクセスが可能になります。データ復元処理では、アーカイブされていた暗号化鍵が Vormetric Data Security Manager から復元され、自動的に古いデータセットに適用されます。復元後のデータは最新の暗号鍵で暗号化されます。

主な利点

- 暗号化の実装を拡大しつつ、ダウンタイムとストレージの要件を最小限に抑えられる
- 暗号化の実装とメンテナンスに関連するコストを節減できる
- ユーザーエクスペリエンスに対する暗号化の影響を最小限に抑えられる
- 混乱が発生しない鍵のローテーションを活用して、セキュリティと規則に対する規格への準拠を強化できる
- 古い鍵で暗号化されたデータの復元を高速化できる

技術仕様

オペレーティングシステムのサポート

- Microsoft：Windows Server 2008および2012
- Linux：Red Hat Enterprise Linux（RHEL）6および7、SuSE Linux Enterprise Server 11および12

クラスタのサポート

- Veritas Cluster Serverアクティブ／パッシブ
- Microsoftクラスタ：ファイルクラスタ、SQL Serverクラスタ

データベースのサポート

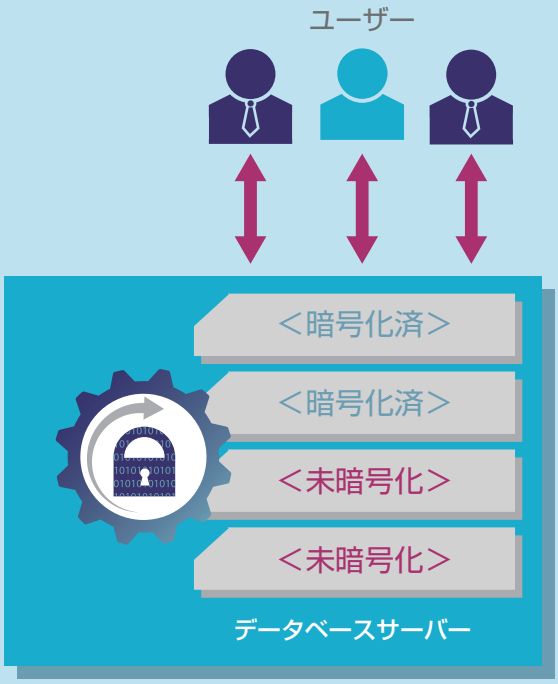
- IBM DB2、IBM Informix、Microsoft SQL Server、Oracle、Sybaseその他

ビッグデータのサポート

- Cassandra、CouchBase、Hadoop、MongoDB、SAP HANA

バックアップ／レプリケーションのサポート

- DB2バックアップ、NetBackup、NetWorker、NTBackup、Oracle Recovery Manager（RMAN）、Windows Server Volume Shadow Copy Service（VSS）



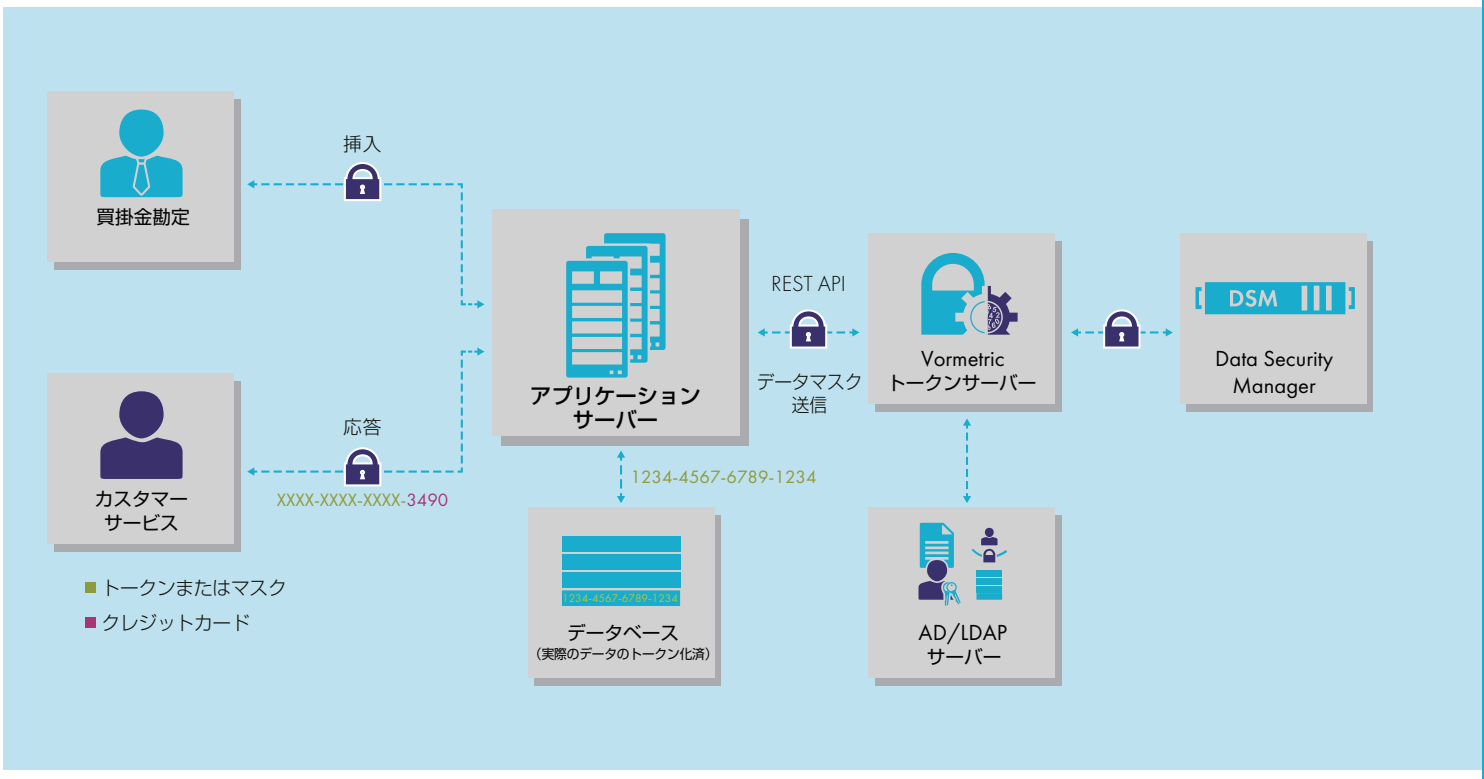
VORMETRIC TOKENIZATION WITH DYNAMIC DATA MASKING

Vormetric Tokenization with Dynamic Data Masking を使用すれば、セキュリティポリシーや、ペイメントカード業界データセキュリティ基準（PCI DSS）などの規則要項に準拠するために必要なコストや手間を劇的に削減できます。このソリューションでは、データベースのトークン化処理とダイナミックディスプレイセキュリティを行います。これにより、機密性の高い資産がデータセンターにあっても、ビッグデータ環境やクラウド上にあっても、そういった資産を保護して匿名化するという目的に効率的に対処できるようになります。

高速なトークナイゼーションとダイナミックデータマスキング

Vormetric Tokenization では、フォーマットを変えないトークン化処理を使用することで、データベース内の機密性の高いフィールドを保護し、ポリシーベースのダイナミックデータマスキングをアプリケーションに追加する作業を簡単に実行できます。このソリューションには、次のような利点があります。

- **ダイナミックデータマスキング -** 管理者は、トークン化されたフィールド全体を元に戻すポリシーか、フィールドの部品を動的にマスキングするポリシーを設定することができます。たとえば、カスタマーサービス担当者の認証情報を持つユーザーは下 4 桁だけが表示されたクレジットカード番号しか受け取れないが、カスタマーサービスのスーパーバイザは完全なクレジットカード番号に平文でアクセスできるようなポリシーを、セキュリティチームが設定することが可能になります。
- **混乱を伴わない実装 -** このソリューションにはフォーマットを変えずにトークン化する機能があります。そのため、既存のデータベースのスキーマを変更することなく、機密性の高い資産へのアクセスを制限することができます。REST API の実装により、アプリケーションデベロッパーが迅速、簡単かつ効率的に、高性能なトークン化機能を設置できるようになります。
- **バッチデータの変換 -** このオプションユーティリティを使用すれば、長時間のメンテナンスやダウンタイムなしで、大量の機密性の高いレコードをトークン化することが可能になります。実際のデータベースやデータベースのコピーの中にある機密性の高いカラムをマスキングしてから、サードパーティのデベロッパーやビッグデータ環境に送信できます。



主な利点

- 最小限のコストと手間で、PCI DSSの対象範囲からカード会員データを削除できる
- リスクを増やすことなく、クラウドやビッグデータ、外部ソースのモデルをフル活用できる
- サイバー攻撃やインサイダーによる悪用から機密性の高い資産を保護するための強力なガードを確立できる

主な特長

- 仮想アプライアンスにより容量の増減が簡単
- AWS環境、仮想環境および物理環境への実装が可能
- オプションのバッチデータ変換ユーティリティにより、大規模なトークン化を合理化
- ポリシーベースのきめ細かいダイナミックデータマスキング

技術仕様

トークン化処理の機能：

- フォーマットを維持
- 暗号化トークン（英字／数字）
- ランダムトークン（数字のみ）
- シングルユースおよびマルチユースのトークン
- 日付のトークン化

ダイナミックデータマスキング機能：

- ポリシーベース
- 英数字に対応
- マスク文字のカスタマイズ

検証のサポート：

- Luhnチェック

仮想アプライアンス：

- オープン仮想化フォーマット（.ovf）
- 国際標準化機構（.iso）
- Amazonマシンイメージ（.ami）

システム要件：

- 最小ハードウェア：4 CPUコア、16～24GB RAM
- 最小ディスク容量：80GB

アプリケーション統合：

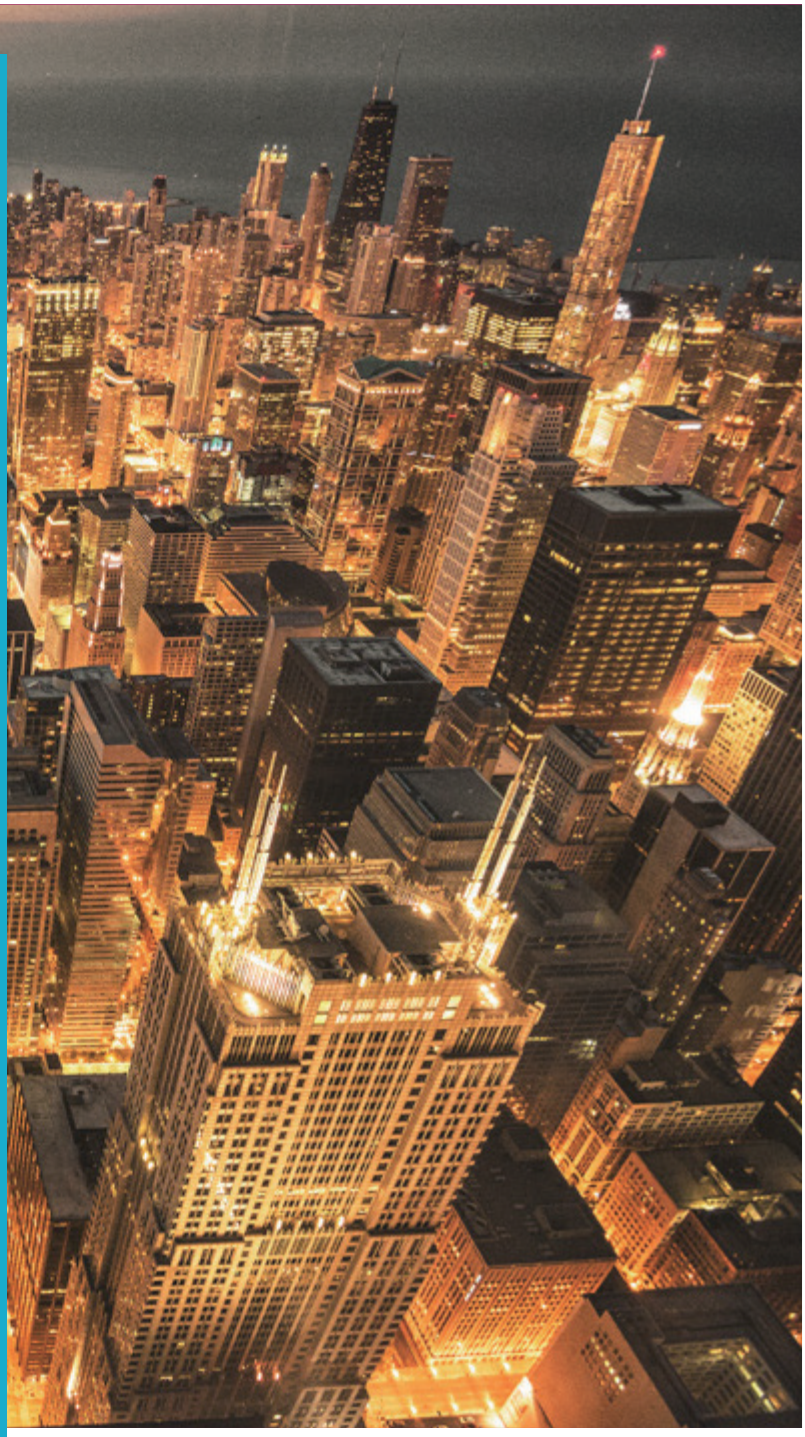
- REST APIs

認証統合：

- Lightweight Directory Access Protocol（LDAP）
- アクティブディレクトリ（AD）

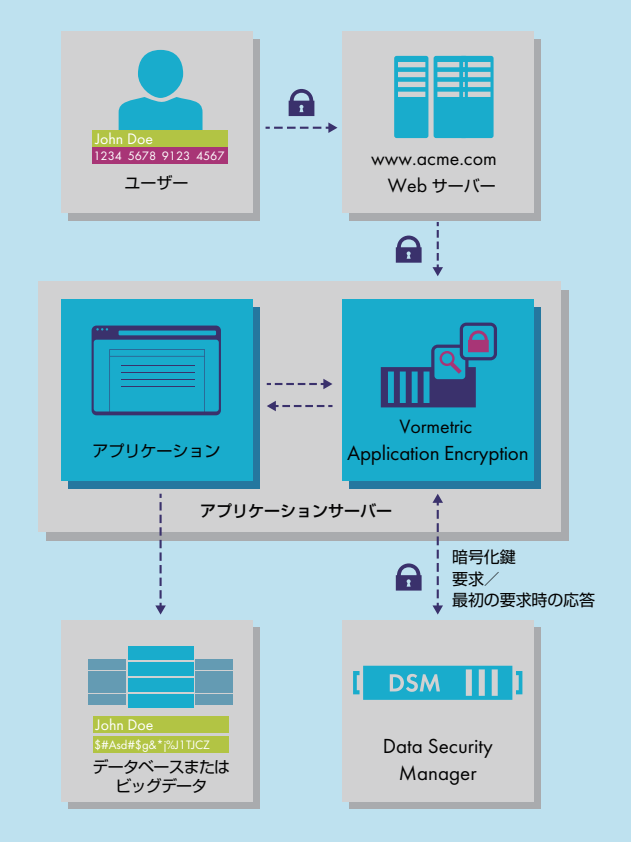
性能：

- 16GB RAMの32コアサーバー（デュアルソケットXeon E5-2630v3）で、トークンサーバー1基あたり（マルチスレッドとバッチ（またはベクトル）モードを使用して）、クレジットカードサイズのトークン化トランザクションが毎秒100万件以上



VORMETRIC APPLICATION ENCRYPTION

Vormetric Application Encryption を使用すれば、データベースやビッグデータノード、Platform-as-a-Service（PaaS）環境内の特定のファイルやカラムを暗号化できます。Vormetric Application Encryption には、既存のコーポレートアプリケーションと暗号化の統合を簡略化するライブラリ機能があります。このライブラリには一連の文書化された標準ベースの API が入っており、これを使用して暗号化や鍵管理の操作を実行できます。Vormetric Application Encryption なら、暗号化および鍵管理ソリューションを社内で開発して実装する時間や複雑な作業、リスクがなくなります。



アプリケーション層の暗号化を簡略化してコストを削減

Vormetric Application Encryption により、既存のアプリケーションに暗号化機能を追加するプロセスが簡略化されます。デベロッパーが Java や .Net、C でライブラリを使用することで、アプリケーションと Vormetric Application Encryption エージェントの間の通信を容易にすることが可能です。Vormetric Application Encryption エージェントは、NIST 標準の AES-CBC またはフォーマット保持暗号化（FPE）を使用してデータを暗号化し、その結果生成された暗号テキストをアプリケーションに返します。ポリシーと鍵の管理はすべて Vormetric Data Security Manager を通じて行われるため、セキュリティの運用が簡略化されます。

クラウド環境およびビッグデータ環境での準拠要件への対応

このソリューションにより、アプリケーション層の特定のフィールドの暗号化を必要とするポリシーや準拠要件に対応できます。機密データがデータベースやビッグデータのリポジトリ、PaaS 環境に格納される前に、データを暗号化することが可能です。

VORMETRIC BATCH DATA TRANSFORMATION ユーティリティの活用

Vormetric Batch Data Transformation を活用することで、長時間のメンテナンスやダウンタイムなしで、大きなデータセットを暗号化できます。アプリケーションやネットワーク構成、ストレージのアーキテクチャを変更する必要もありません。

主な利点

- 社内で暗号化ソリューションを構築する時間や複雑な作業、リスクを排除
- アプリケーション層の暗号化とファイルシステムの暗号化を集中管理
- 幅広いプラットフォームやオンプレミス環境、PaaS環境で機密データを保護
- 悪意のあるDBAやクラウド管理者、ハッカー、提出命令を持つ当局者が重要なデータにアクセスすることを防止
- Vormetric Batch Data Transformationユーティリティによって大規模な暗号化のマイグレーションを合理化

技術仕様

サポート対象の環境
- Microsoft .NET 2.0以上
- Java 7および8
- C

統合標準：
- OASIS PKCS#11 APIs

暗号化：
- AES
- フォーマットを変えない暗号化のFF3

オペレーティングシステム：
- Linux
- Windows 2008および2012

性能：
- 毎秒クレジットカード400,000件分の暗号化トランザクション（シングルスレッド、32コア、16GB、C）

ポリシーと鍵の管理：
- Vormetric Data Security Manager

文字のサポート：
- ASCII
- Unicode

証明書：
- FIPS 140-2 Level 1（審査中）

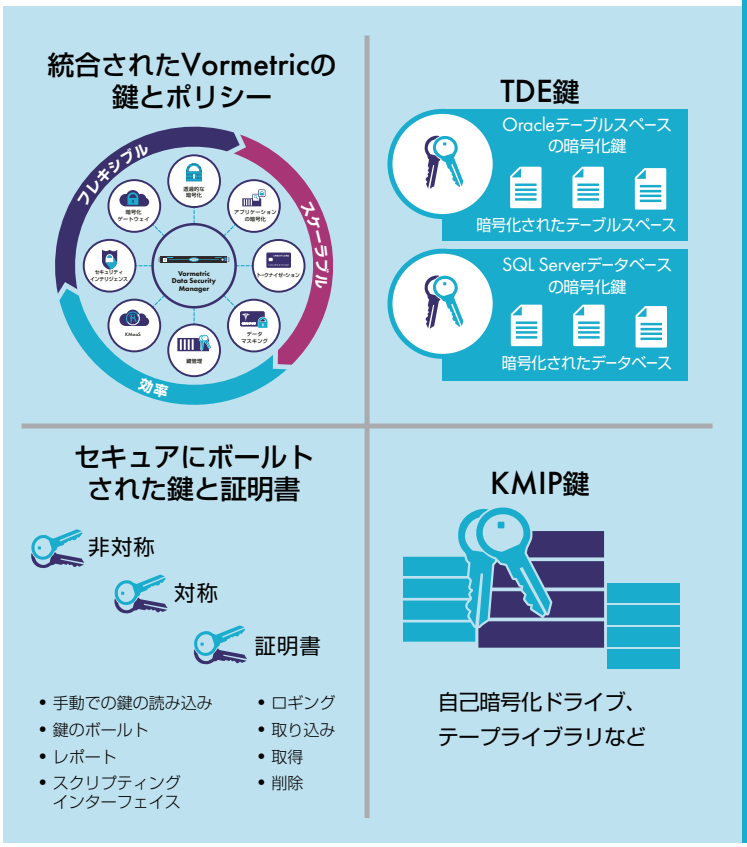
VORMETRIC KEY MANAGEMENT

Vormetric Key Management を使用すれば、すべての Vormetric Data Security Platform 製品の鍵を集中管理したり、サードパーティ製のデバイス（IBM Security Guardium Data Encryption や Microsoft SQL TDE、Oracle TDE、その他 KMIP 準拠の暗号化製品を含む）の鍵や証明書を安全に格納してインベントリを作成したりすることが可能です。鍵の管理を集約することにより、複数のシステムにわたって一貫したポリシーの実装が促進され、研修やメンテナンスのコストが削減されます。

鍵の管理と証明書のボールトへの保管の簡略化

これまで、暗号化を使用するアプリケーションとデバイスの急増に伴い、採用される鍵管理デバイスの数も増加してきました。このように鍵管理システムの数が増加することで、高可用性の暗号化環境の維持はどんどん複雑になり、コストも上昇しました。その上、異なる鍵管理デバイスが存在することにより、重要証明書が保護されないままになって、簡単にハッカーの餌食になることがよくありました。また、このような証明書が管理されないままになった場合、突然証明書が期限切れになって、極めて重要なサービスの予定外のダウンタイムが発生する可能性もありました。

Vormetric Key Management なら、組織の機能を拡張して、Vormetric Data Security Platform ソリューションの鍵のほか、サードパーティ製品の鍵や証明書をより効果的に管理できるようになります。また、クラウド向けの Vormetric Key Management as a Service により、クラウドプロバイダの Bring-your-own-key サービスを活用しつつ、鍵のライフサイクル全体を通じた鍵の完全な制御を確立することが可能です。



強力で監査可能な制御の確立

Vormetric Key Management には、Vormetric Data Security Manager（DSM）の信頼性と可用性に関する機能がすべて入っています。DSM は、V6000 および V6100 という 2 つのハードウェアアプライアンスを通じて、仮想アプライアンスとして提供されます。V6100 は FIPS 140-2 Level 3 認証済のアプライアンスで、Thales nShield Solo ハードウェアセキュリティモジュール（HSM）が装備されています。このプラットフォームは、アマゾン ウェブ サービス Marketplace と Microsoft Azure Marketplace でも利用できます。

主な利点

- 効率的な運用
- 証明書と暗号化鍵のセキュアなストレージとインベントリが継続して利用可能
- 証明書と鍵の期限切れを事前に通知するアラート
- ステータスと特性に関する情報をレポートで提供、監査へのサポート

技術仕様

セキュリティオブジェクトの管理

- X.509証明書
- 対称および非対称の暗号化鍵

管理

- セキュアWeb、CLI、API
- デジタル証明書と暗号化鍵の一括読み込み
- 読み込み時の検証
- アップロードされた証明書と鍵から基本属性をレポート用に抽出
- コマンドラインスクリプト
- 取得と削除

検索、アラート、レポート用の鍵と証明書のフォーマット

- 対称の暗号化鍵アルゴリズム：3DES、AES128、AES256、ARIA128、ARIA256
- 非対称の暗号化鍵アルゴリズム：RSA1024、RSA2048、RSA4096
- デジタル証明書（X.509）：DER、PEM、PKCS#7、PKCS#8、PKCS#12

サードパーティによる暗号化

- Microsoft SQL TDE、Oracle TDE、IBM Security Guardium Data Encryption、KMIPクライアント
- パートナーの例：Nutanix、Linoma、NetApp、Cisco、MongoDB、DataStax、Huawei

APIのサポート

- PKCS#11、Microsoft Extensible Key Management（EKM）、OASIS KMIP

鍵の可用性と冗長性

- 自動バックアップによる、複数のアプライアンスにわたる鍵のセキュアなレプリケーション

クラウド向けのVORMETRIC KEY MANAGEMENT AS A SERVICE

今日の大多数の組織においては、幅広いアプリケーションでクラウド配信モデルが一般的になってきています。多くの企業、特に規制の厳しい業界の企業にとっては、暗号化を使用することも鍵の管理も、ますます一般的になっています。暗号化の普及にともなって、鍵の数も増え続けています。そして、効果的な鍵の日常的な管理を行わなかった場合のリスクも増大しています。クラウド向けの Vormetric Key Management as a Service（KMaaS）を使用することで、暗号化鍵とポリシーに対する強力なガバナンスを確立できます。それにより、クラウドサービスをフル活用しつつ、複雑な処理やリスクを最小限に抑えることができます。

クラウドサービスに対する鍵の管理の合理化

関連する規則要項とセキュリティポリシーへの準拠を保証するためには、暗号化鍵に対する強力かつ独立したガバナンスを維持する必要があります。多くのクラウドプロバイダは、bring-your-own-key（BYOK）サービスを提供することで、このアプローチを支援しています。そういったアプローチを採用することにより、クラウドサービスを活用しつつ、セグリゲーションや準拠のレポート、また会社や監査役の要求を満たすライフサイクル管理を確立することができます。

Vormetric KMaaS は、クラウドプロバイダの BYOK サービスと統合されて使用される、規格に準拠した強力な鍵管理ソリューションです。KMaaS をクラウド上やオンプレミス環境に導入することで要件に対応します。どちらに導入しても、直感的で使いやすいインターフェイスやシンプルな実装、簡単に拡張可能という特長があります。

Vormetric KMaaS はクラウドベンダーから提供される BYOK API を活用して、鍵の作成やアップロード、更新、格納、廃止、レポートを含めた鍵管理のライフサイクルの完全な制御を可能にします。

オンプレミスかクラウドか — それを決めるのはあなたです

フレキシブルな導入モデルであるため、企業が独自の要件に合わせて導入できます。Vormetric KMaaS は、次のようなサービスを提供します。

- **クラウドサービス -** このサービスにより、クラウドでの FIPS 140-2 Level 1 ソリューションの利点を活用しつつ、最適な制御を確保することができます。このソリューションが as-a-Service 配信であるということは、高可用性の鍵管理ソリューションをオンプレミスで構築、導入および維持する必要がないということを意味します。
- **オンプレミスサービス -** 組織の要求により鍵をオンプレミスで規則によって制御する必要がある場合は、こちらが最適なソリューションです。このサービスでは、社内の FIPS 140-2 Level 3 認証済ハードウェアアプライアンスに鍵を格納しつつ、登録制の従量課金モデルを活用することができます。

主な利点

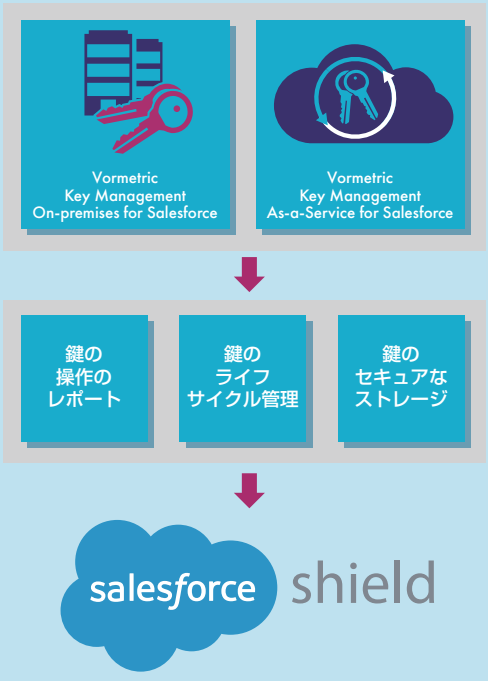
- クラウド環境内のデータを管理するための堅牢で一貫した制御機能と視認性を確立
- 監査役や監督機関の準拠要件に効率的に対処
- 鍵管理の実装と運用に伴うコストと手間を大幅に軽減

主な特長

- データリポジトリから鍵のストレージを分離
- 暗号化鍵と証明書の管理作業の総合的できめ細かい監査ログ
- ボタンを押すだけで鍵とポリシーを作成・変更
- 鍵のライフサイクル管理のための使いやすいポータル

技術仕様

- 対応しているSaaSプロバイダ：Salesforce
- 要件：Salesforceプラットフォームの暗号化
- FIPS 140-2 Level 3オンプレミスサービス
- FIPS 140-2 Level 1 SaaS
- OAuthフェデレーションとSalesforceの統合



VORMETRIC CLOUD ENCRYPTION GATEWAY

Vormetric Cloud Encryption Gateway では、Amazon Simple Storage Service（Amazon S3）や、S3 と互換性のある他のオブジェクトストレージサービスなどのクラウドストレージ環境に、ファイルを安全に保存することができます。Cloud Encryption Gateway は、機密データがクラウドストレージ環境に保存される前に暗号化を行い、暗号化鍵に対する制御権限をユーザーに渡します。機密性の高い資産をさまざまな脅威から防御するために必要な視認性と制御機能を備えたソリューションです。Cloud Encryption Gateway は鍵とポリシーの管理を Vormetric Data Security Manager で行います。

クラウドに格納されたデータに対する強力な制御の確立

Vormetric Cloud Encryption Gateway は、クラウドやデータセンターに仮想アプライアンスとして導入可能です。いずれの場合も常に、セキュリティチームが暗号化鍵を完全に制御することができます。Cloud Encryption Gateway には、次のような利点があります。

- **透過的で簡単な導入 -** トラフィックがユーザーとクラウドの間を移動する過程でそれを傍受し、透過的にファイルを暗号化および復号可能です。
- **強力な鍵管理 -** ポリシーおよび鍵に対する、監査可能できめ細かい制御が常に可能です。
- **詳細な視認性と監査機能 -** ファイルへのアクセスを詳細に見られる監査ログを取得できます。準拠レポートやフォレンジックス作業に対する非常に大きなサポートとなります。
- **高性能なリスク検知 -** Amazon S3 や、S3 API と互換性のある他のクラウドストレージ環境を監視します。セキュリティポリシーに違反している未暗号化ファイルを検出して、自動的にそのファイルを暗号化します。

主な特長

- 透過的な実装
- 堅牢な鍵の管理と暗号化
- ステートレスなアーキテクチャによって費用効率の良い水平拡張性を実現
- 強力なクラウドストレージのセキュリティと準拠制御

技術仕様

仮想アプライアンス

- オープン仮想化フォーマット（.ovf）の配信
- 最小ハードウェア：4 CPUコア、4GB RAM
- 最小ディスク容量：100GB

サポート対象のサービス

- Amazon S3
- Caringo Object Storage
- KMaaS for Salesforce

認証統合

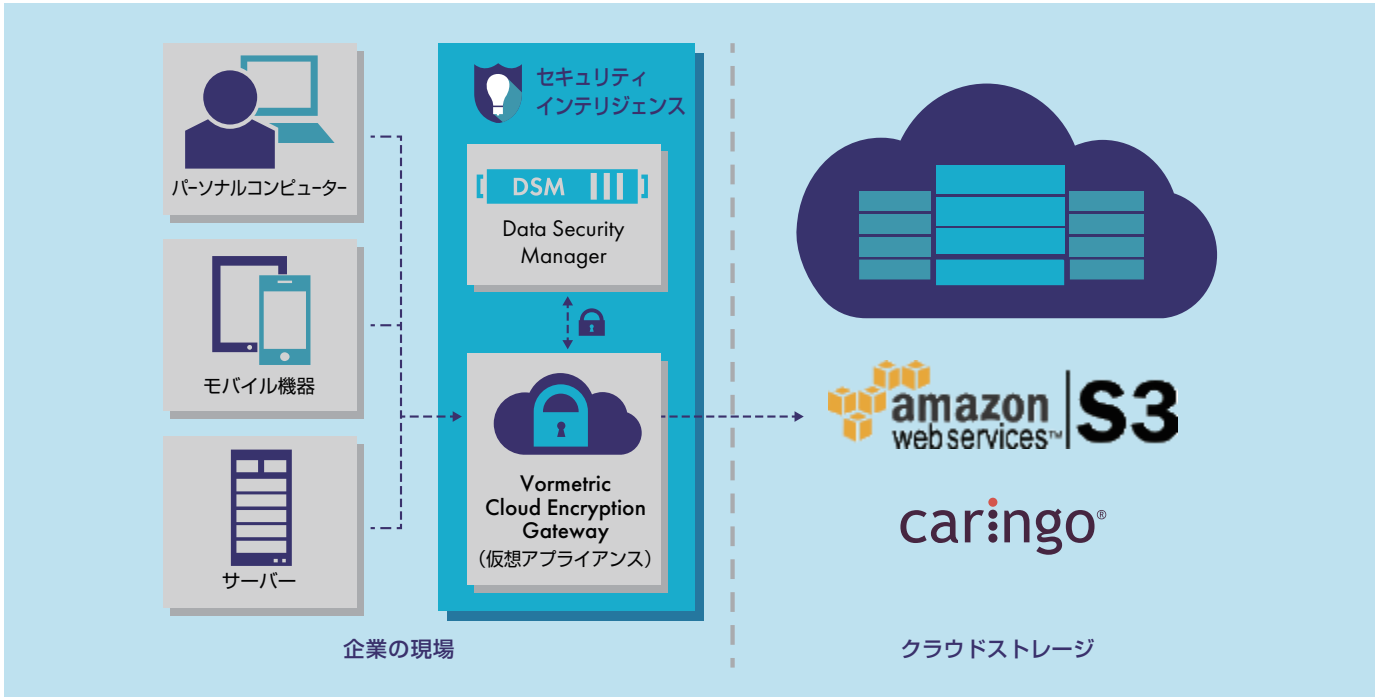
- Lightweight Directory Access Protocol（LDAP）
- アクティブディレクトリ（AD）（Amazon S3のみ）

ポリシー

- ファイルタイプごとに暗号化
- 鍵の自動ローテーション

MongoDBのバージョン

- 2.6.9以上



VORMETRIC PROTECTION FOR TERADATA DATABASE

Teradata 環境に大量の企業データを集めることで、ビジネスに関する思いがけない発見や戦略的な価値を見いだすことができます。しかし残念ながら、膨大なデータを集めることで、予想外のリスクが表れる場合もあります。正しくデータを防御しなければ、これらの環境に組み込まれた機密性の高い資産が、特権管理者による不注意で露出したり、悪意のあるインサイダーや外部攻撃者による盗用の対象になったりするおそれがあります。Vormetric は、このようなリスクから企業のデータを保護します。Vormetric Protection for Teradata Database なら、お使いの Teradata 環境に、保存データを保護する強力な機能を迅速かつ効率的に実装できます。

セキュリティを強化しつつ、混乱やコストを最小限に抑える

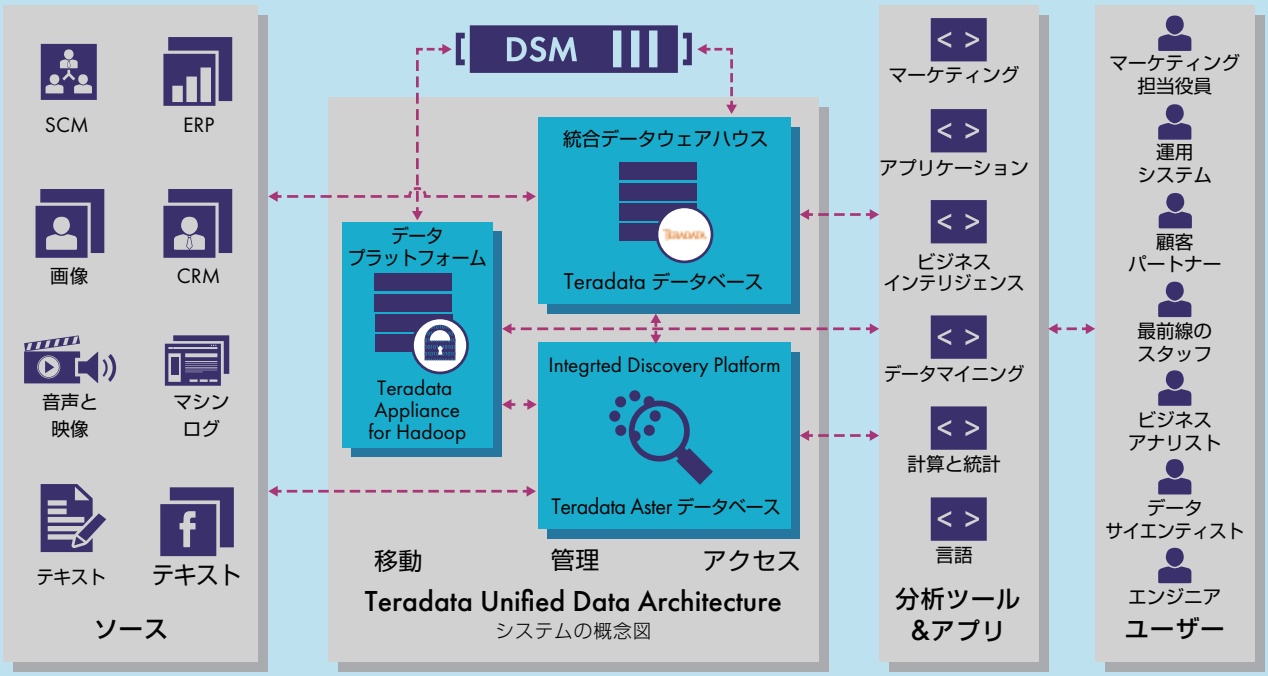
Vormetric Protection for Teradata Database では機密性の高いレコードを保護するプロセスを簡略化します。これにより、Teradata データベース内の特定のフィールドとカラムの暗号化が可能になります。このソリューションには NIST 認証済のフォーマット保持暗号化（FPE）機能もあるため、レコードのフォーマットやフィールドのスキーマを変更することなく、機密性の高いレコードを暗号化することができます。これによって、関連するアプリケーションやワークフローに対する暗号化の潜在的な影響が最小限に抑えられるだけでなく、従来の暗号化の手法を使用した場合に必要となるストレージの増加を回避することが可能になります。

主な利点

- 保存データの暗号化と鍵管理を集約化および合理化できる
- ビッグデータ分析の価値を犠牲にすることなくセキュリティを強化できる
- サイバー攻撃や特権ユーザーによる悪用に対する防御を確立できる
- 迅速な実装が可能

主な特長

- きめ細かい制御を強化するため、管理者が平文の機密データにアクセスしなくても運用タスクを実行できる
- 多数のTeradataノードによる高性能な拡張を実現
- ストレージの増加と暗号化の混乱を最小限に抑えるFPEを活用
- 暗号化と復号のためのユーザー定義関数（UDF）を、既存のSQLコードに簡単に統合
- 顧客が、異なるカラムに対して異なる鍵を使用できる
- ASCIIテキストとUnicodeへの対応により、フレキシブルな言語サポートと技術サポートが可能に
- 認証済みのTeradata暗号化ソリューション



高速暗号化の導入と利用

このソリューションでは、暗号化や鍵管理の操作を実行するために使用可能な文書化された標準ベースのアプリケーションプログラミングインターフェイス（API）とユーザー定義関数（UDF）が提供されているため、デベロッパー側での複雑な作業が削減されます。Teradata ユーザーはこのソリューションを使用して、暗号化と復号の要求（標準の AES 暗号化と FPE からの選択を含む）を送信するための、構成が容易な独自のプロファイルを設定することができます。

鍵とポリシーの管理の集約化を可能にする

Vormetric Protection for Teradata Database は、管理および鍵のストレージのための、FIPS 認証済の強力なアプライアンスである Vormetric Data Security Manager（DSM）とシームレスに連動します。DSM を使用することで、Vormetric Protection for Teradata Database や他の Vormetric Data Security Platform ソリューション、サードパーティ製の暗号化製品の鍵とアクセスポリシーを集中的に管理できます。また、Teradata Appliance for Hadoop の保護に使用可能な Vormetric Transparent Encryption の鍵とポリシーも管理できます。

技術仕様

サポート対象のプラットフォーム：

- Teradataデータベース、バージョン14.0、14.10、15.0 および15.10

オペレーティングシステム：

- SUSE Linux Enterprise Server（SLES）バージョン10 または 11

最大カラム幅：

- ASCII：16KB
- Unicode UDF：8KB

VORMETRIC SECURITY INTELLIGENCE

Vormetric Security Intelligence では、詳細で実行可能なセキュリティイベントログを取得できます。このログによって、これまでにない精度でファイルへのアクセス行為について洞察することができます。このソリューションにより、自動的なエスカレーションと応答を促進する即時アラートを活用することが可能です。これらのログは SIEM システムと簡単に統合できるため、疑わしい行為を効率的に追跡および調査して、規格への準拠とセキュリティに関するレポートを作成できます。

綿密で実行可能なセキュリティインテリジェンスの提供

これまで、SIEM はファイアウォールや IPS、NetFlow のデバイスから取得するログに依存していました。このログはネットワーク層で取り込まれるものであるため、これらのシステムで生成されるデータが大量になり、本当に問題となるイベントを管理者が識別することが困難になっていました。さらに、サーバー上で起こっているデータへのアクセス行為やイベントがまったく見えないという盲点が悪用されたままなのが通例でした。Vormetric Security Intelligence によってこの盲点がなくなり、ターゲットを絞って批判的にファイルへのアクセス行為を見られるようになります。その結果、不正なユーザーアカウントや漏洩したユーザーアカウントが機密データにこっそりアクセスする脅威がなくなります。

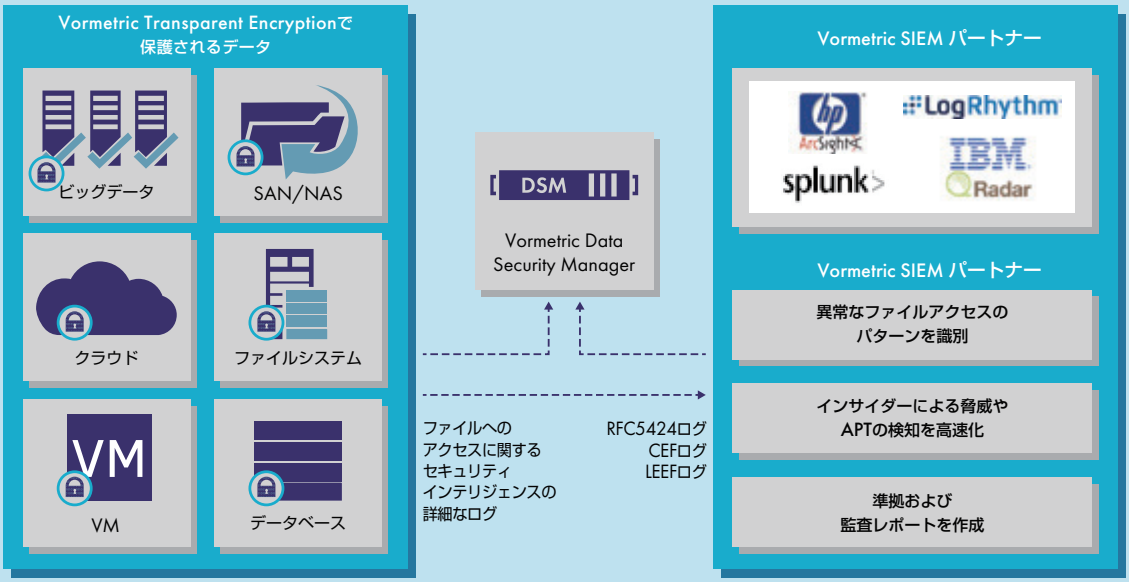
Vormetric Security Intelligence のログでは、ユーザーやプロセスによる、許可されたアクセス試行と拒否されたアクセス試行の監査可能な証跡を作成します。このソリューションの詳細なログを検証することで、ユーザーやプロセスがいつ、どのポリシーでデータにアクセスしたか、またアクセス要求が許可されたか拒否されたかを明示することができます。このログは SIEM プラットフォームと効率的に共有できるため、異常なプロセスやユーザーのアクセスのパターンの解明に役立ち、それによってさらに詳しい調査が促進されます。たとえば、管理者やプロセスが通常よりもはるかに大量のデータに突然アクセスしたり、ファイルの不正ダウンロードを実行しようとしたりする場合があります。このような矛盾する使用パターンは、APT 攻撃や悪意のあるインサイダーによる行為を指している場合があります。

迅速なレスポンスを促進する実行可能なログ

Vormetric Security Intelligence のログによって、データへのアクセスを即座に洞察することができ、その情報を、既存のワークフローや自動スクリプト（実行中であれば）も含めて、セキュリティ運用センターに提供することができます。その結果、もっとも迅速かつ効率的に、リスクを識別および通知し、対処することが可能になります。

監査と規格への準拠の合理化

数多くの準拠要件や規則に従うためには、データ保護が実施され、運用されていることを証明する必要があります。Vormetric Security Intelligence を使用すれば、暗号化や鍵管理、アクセスポリシーが効果的に動いていることを監査役に証明することができます。精密な視認性と統合機能を持つ Vormetric Security Intelligence により、監査や持続的な準拠レポート作成に関連する作業を合理化することが可能になります。



主な特長

- 機密データへのアクセスに対する視認性の強化
- 即時アラートによる迅速かつ自動的な応答の発信
- APTやインサイダーによる脅威の検知の高速化
- Syslog RFC5424、CEF、LEEFなどすべての主要なログ形式でログをエクスポート
- Vormetric SIEMパートナーとの迅速な提携
- 一貫した準拠および監査レポートの強化

技術仕様

SIEMパートナーとの提携

- FireEye Threat Prevention Platform
- HP ArcSight
- IBM Security QRadar SIEM
- Informatica Secure@Source
- McAfee ESM
- LogRhythm Security Intelligence Platform
- SolarWinds
- Splunk

VORMETRIC ORCHESTRATOR

Vormetric Orchestrator は、Vormetric Data Security Platform 製品の実装、構成、管理および監視を自動化します。これらの機能により、企業の大規模なデータセンターおよびハイブリッドクラウド環境全体での実装を拡大すると同時に、管理にかかる手間や総所有コストを劇的に削減することが可能になります。

自動化により、スケーラブルで効率的な運用を促進

大規模な組織やクラウドサービスプロバイダにおいて、唯一確実なものが変化です。オペレーティングシステムが変わり、作業負荷もデータベースもネットワーク構成も変わります。Vormetric Orchestrator では、そのような変化に対応するために必要な自動化を行います。反復的なタスクを自動化することで、運用が簡略化され、ミスが減って実装のスピードが上がります。このソリューションによって、暗号化の実装の維持と拡張に必要なスタッフリソースが削減されるため、チームがより多くの時間をかけて、より差し迫った優先順位の高い戦略的な作業に集中できるようになります。Vormetric Orchestrator には次のような利点があります。

- **自動化による運用効率の改善 -** このソリューションにより、Vormetric Data Security Platform 製品を自動的に導入および維持することが可能になります。たとえば、オペレーティングシステムに重要なパッチが出た場合に、新しいバージョンの Vormetric Transparent Encryption エージェントで自動的に数百台のサーバーを更新するように Orchestrator に指示するジョブを簡単に設定できます。
- **お使いの環境への効率的な統合 -** このソリューションには、独自ツールや Chef などのよく知られたソリューションを含む幅広い構成管理ソリューションとの迅速な統合を可能にするプラグインアーキテクチャが入っています。RESTful API と CLI 両方へのアクセスを可能にすることで、既存の IT オートメーションシステムや自社開発のスクリプトに Vormetric Orchestrator を簡単に統合できます。
- **フレキシブルな導入オプション -** Vormetric Orchestrator は、業界で主流となっている仮想化プラットフォームおよびパブリッククラウドプラットフォームで使用する仮想アプライアンスとして提供されます。このソリューションをデータセンターにインストールすると、リモートデータセンターやプライベートクラウド環境、パブリッククラウドで、Vormetric Data Security Platform 製品を管理できます。

主な利点

- オートメーションを利用して実装を高速化し、運用効率を改善
- 暗号化を拡張しつつ総所有コストを削減
- 幅広い環境のサポートを利用して暗号化の機能を拡張

技術仕様

仮想アプライアンス

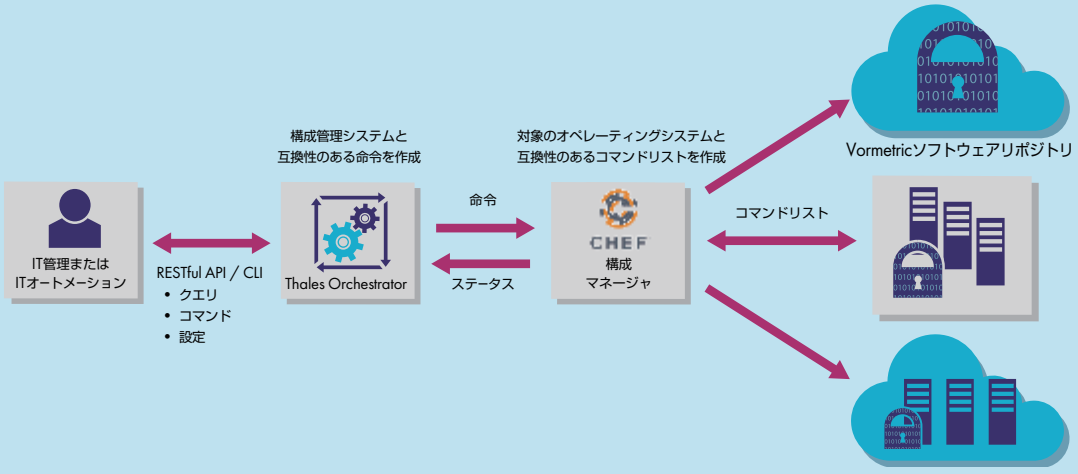
- オープン仮想化フォーマット（.ovf）の配信
  - 最小メモリ要件：4GB
  - CPU要件：仮想CPU 4個
- アマゾン ウェブ サービスの Amazonマシンイメージ（AMI）

構成マネージャのサポート

- Chef（複数のChefサーバーの使用可）

オートメーションのサポート

- Vormetric Transparent Encryptionエージェント
  - エージェントのインストール
  - エージェント登録メカニズム
    - 共有秘密鍵
    - フィンガープリント
  - エージェント更新
- Vormetric Data Security Manager構成



THALES

www.thalesesecurity.com

Thales e-Securityについて

Thales e-Securityは、情報が作成、共有または格納される場所にかかわらず、信頼のおける高性能なデータセキュリティソリューションおよびサービスを提供する業界のリーダーです。当社は、オンプレミスやクラウド、データセンター、ビッグデータ環境といったどのような環境でも、ビジネスの敏捷性を犠牲にすることなく、企業や政府組織に属するデータが安全かつ信頼できる形であることを保証します。セキュリティはリスクを軽減するだけではなく、私たちの日々の生活に浸透しているデジタル構想、すなわちデジタルマネーやe-Identity、ヘルスケア、コネクテッドカーのほか、IoT（モノのインターネット）を使用すれば家事用デバイスまでも実現するものです。

タレスは、暗号化や高度な鍵管理、トークン化処理、特権ユーザーの制御、確実性の高いソリューションを通じて、データやアイデンティティ、知的財産を保護および管理し、規制に準拠するために必要とするものをすべて提供します。世界中のセキュリティ専門家がタレスを信頼し、自信を持って組織のデジタル化を推進しています。Thales e-Securityはタレスグループの一員です。

当社のフォローはこちらで：

南北アメリカ - Thales e-Security Inc. 900 South Pine Island Road, Suite 710, Plantation, FL 33324 USA • Tel: +1 888 744 4976または+1 954 888 6200 • Fax: +1 954 888 6211 • E-mail: sales@thalesesec.com
アジア太平洋地域 - Thales Transport & Security (HK) Lt, Unit 4101-3, 41/F, Sunlight Tower, 248 Queen's Road East, Wanchai, Hong Kong • Tel: +852 2815 8633 • Fax: +852 2815 8141 • E-mail: asia.sales@thales-esecurity.com
ヨーロッパ、中東、アフリカ - Meadow View House, Long Crendon, Aylesbury, Buckinghamshire HP18 9EQ • Tel: +44 (0)1844 201800 • Fax: +44 (0)1844 208550 • E-mail: emea.sales@thales-esecurity.com