DATASHEET

Entrust暗号セキュリティプラットフォーム

鍵とシークレットの管理

概要

従来の中央集約型で単一的な鍵管理ソリューションでは、ますます複雑化するデータセキュリティ、規制、コンプライアンス要件に直面する組織の課題を解決することはもはやできません。きめ細かなポリシー制御を提供し、コンプライアンス要件を確実に満たすためには、可視性と使用パラメータの文書化機能を組み合わせることが不可欠です。オンプレミスまたはas a Serviceで導入可能なEntrust暗号セキュリティプラットフォームは、データ主権とデータ所在に関する規制の厳格さに対応しながら、暗号鍵やシークレットのあらゆる側面を監視できる機能が豊富なダッシュボードを提供します。

このプラットフォームは、鍵ライフサイクル管理と分散型Vaultベースのアーキテクチャを幅広いユースケースに対応する包括的な中央ポリシーおよびコンプライアンス管理機能と組み合わせたものです。

多用途な鍵とシークレットVault：分散型セキュリティモデルは、暗号エコシステム全体における集約リスクの軽減に役立ちます。データは、さまざまな地域のセキュリティポリシーに沿って保護され、規制要件にも準拠することができます。

コンプライアンス・ダッシュボード：コンプライアンスマネージャーは、企業の暗号資産を一元的に可視化する機能と、保管場所にかかわらずすべての暗号鍵や機密情報をきめ細かく制御できるポリシーエンジンを提供します。

ソリューション

Entrust暗号セキュリティプラットフォームは、ますます複雑化するデジタル環境において高まる、包括的な暗号資産管理のニーズに対応します。PKIの運用、証明書ライフサイクル管理、鍵管理、シークレット管理、HSMといった豊富な機能を統合し、これらすべてを単一の統合システムから一元的に管理することで、暗号管理を統一します。

これらの重要なコンポーネントを統合することで、暗号セキュリティプラットフォームは、増え続けるマシンIDのセキュリティ対策に取り組む組織に対し、比類のないセキュリティ、可視性、コンプライアンス対応、および運用効率を提供し、複雑な暗号化要件を満たしつつ、機密データを保護することを支援します。

主な特長

- 幅広いユースケースに対応した、拡張性が高く、コスト効率に優れ、エンタープライズ環境に適した鍵管理システム
- 鍵とシークレットを詳細に把握できる統合ダッシュボード
- コンプライアンスの遵守状況を特定し、禁止されている鍵の使用を警告するための詳細な指標
- 分散型Vaultアーキテクチャ
- 鍵のライフサイクル全体にわたる管理
- レジリエンスに優れたバックアップとリカバリのための完全なHA構成
- Entrust nShieldハードウェアセキュリティモジュール（HSM）とのシームレスな統合により、FIPS 140-3レベル3の信頼の基点のアップグレードが可能（オプション）。

ENTRUST
SECURING A WORLD IN MOTION

鍵とシークレットの管理を再定義

主な機能

Vaultアーキテクチャ
柔軟な暗号セキュリティプラットフォームアーキテクチャは、鍵とシークレットを管理するための以下のVaultオプションをサポートしています。

KMIP用Vault
仮想化プラットフォーム、バックアップとリカバリ、データベース、ストレージワークロードなど、暗号鍵を利用するKMIPワークロード用のVaultを提供します。

データベース用Vault
透過的データベース暗号化（TDE）を使用して、暗号化されたSQLデータベースのライフサイクル管理の主要な機能を提供します。

クラウド鍵管理用Vault
クラウドのメリットを活用しながら、暗号鍵を管理できるようにします。BYOK（Bring Your Own Key）やクラウド管理鍵（ネイティブ鍵）などの顧客管理鍵、およびHYOK（Hold Your Own Key）などの外部保存鍵をサポートします。

暗号API用Vault

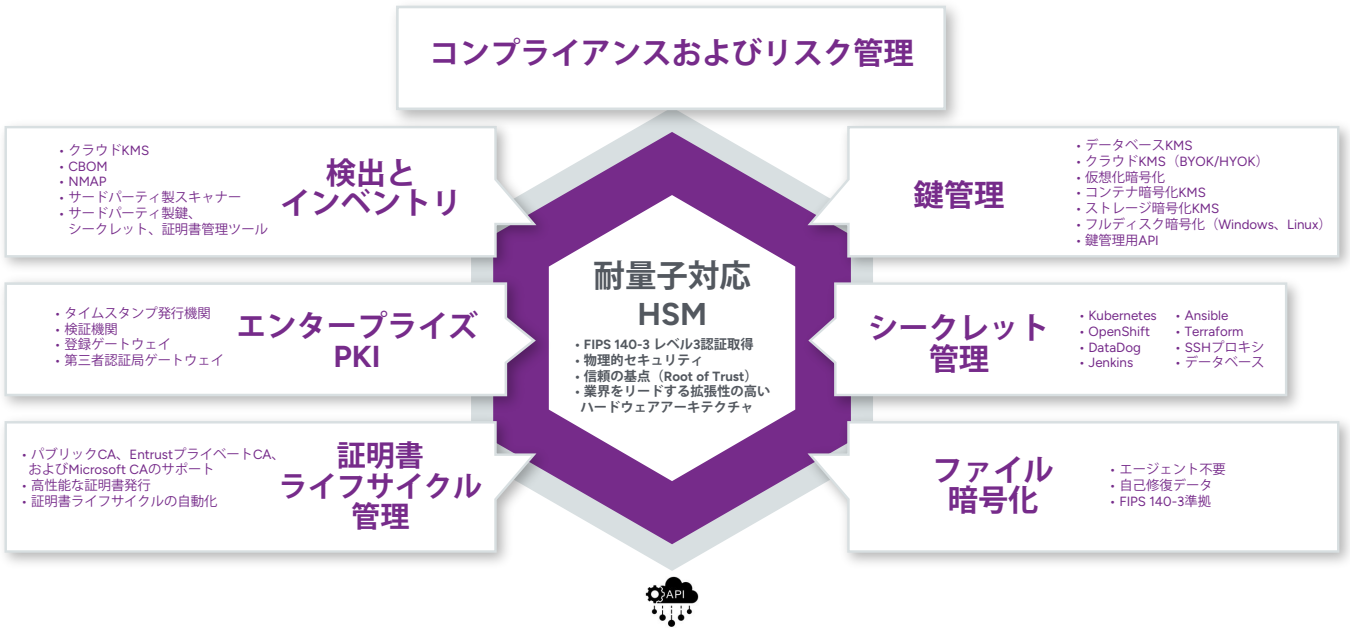
データ暗号化、データトークナイゼーション、フォーマット保持暗号化（FPE）によるデータ署名、データマスキング、鍵管理といった機能を提供することで、幅広いデータ保護のユースケースに対応します。

シークレット管理用Vault
クラウドサービス、データベース、サーバ、コンテナなどのリソースを保護するために、パスワード、トークン、証明書、暗号鍵を安全に保管し、アクセスを厳密に制御できるようにします。

VM暗号化用Vault
エージェントベースの仮想マシン（VM）ワークロード暗号化を提供し、VMごとにダウンタイムゼロの暗号化を実現します。ブート（OS）ディスクやスワップパーティションなど、各パーティションごとに固有の鍵を割り当てて暗号化することができます。

Entrust暗号セキュリティプラットフォームは、PKI、証明書ライフサイクル管理、鍵およびシークレット管理、HSMといった豊富な機能を単一の統合システムから運用することで、暗号管理を一元化する革新的なソリューションです。

このプラットフォームは、ますます複雑化するデジタル環境における、包括的な暗号資産管理に対する高まるニーズに対応します。これらの重要なコンポーネントを統合することで、暗号セキュリティプラットフォームは、増加するマシンIDの保護、機密データの保護、複雑な暗号化要件への対応に取り組む組織に対し、比類のないセキュリティ、コンプライアンス、および運用効率を提供します。



鍵とシークレットの管理を再定義

鍵ライフサイクル管理
暗号鍵のライフサイクル（鍵の保管、バックアップ、配布、ローテーション、失効など）を自動化することで、暗号化されたワークロードの管理を簡素化します。

分散型アーキテクチャ
国および地域のデータ主権に関する規制に対応し、業務ニーズに基づいて保管場所を決定することにより攻撃対象領域を縮小します。

統合ダッシュボード
単一の統合ダッシュボードである暗号セキュリティプラットフォームのコンプライアンスマネージャーにより、1つまたは複数のVaultに保存されている暗号資産を表示および監視することができます。

幅広いVault利用事例に対応
柔軟なVaultアーキテクチャは、KMIP、クラウド鍵管理（BYOKおよびHYOK導入を含む）など、幅広い機能とサービスをサポートします。

企業全体をカバーする暗号セキュリティ
複雑な企業環境において、PKI、HSM、鍵、証明書、シークレットの管理を運用するための豊富な機能を提供します。

ENTRUST
SECURING A WORLD IN MOTION

entrust.com/ja エントラストジャパン株式会社｜東京都港区台場2-3-1 トレードピアお台場22階

HSMinfo@entrust.com

Key&Secret-Management_20260515