Entrust KeyControl

暗号化されたワークロードのためのマルチクラウド鍵管理

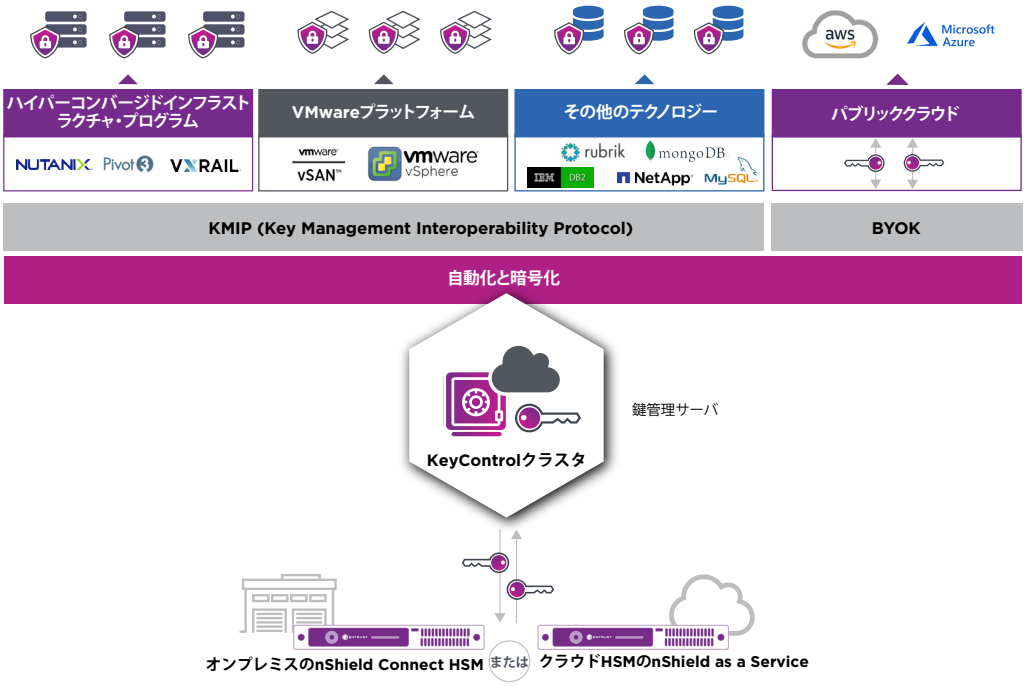
仮想化環境におけるワークロードのセキュリティ管理は、管理者にとって複雑な課題

ワークロードを暗号化することで、データ侵害のリスクを大幅に軽減できます。しかし、何万もの暗号化されたワークロードの鍵管理は容易ではありません。強力なデータセキュリティを確保するには、鍵を頻繁に変更し、安全に移動および保管しなければなりません。堅牢なデータセキュリティへの需要の高まりに伴い、仮想環境においてもPCI DSS（ペイメントカード業界標準）、HIPAA（医療保険の携行性と責任に関する法律）、NIST（アメリカ国立標準技術研究所）800-53、およびGDPRなどの規制要件への準拠がますます求められるようになっています。

Entrust KeyControl（旧HyTrust製品）を使うことで、企業は大量の暗号鍵を簡単に管理することができます。アメリカ連邦情報処理標準（FIPS）140-2に準拠した暗号化方式を採用したKeyControlは、鍵の保管、配布、交換、廃棄といった暗号鍵のライフサイクルを自動化・簡略化することで、暗号化されたワークロードの管理を容易にします。

ハイライト

- KMIP（Key Management Interoperability Protocol）対応の暗号化エージェントをサポートし、エンタープライズレベルの拡張性と可用性を実現
- 包括的で、マルチクラウドのワークロードを暗号化できるEntrust DataControlにアップグレード可能
- FIPS 140-2 レベル3準拠のEntrust nShield®ハードウェア・セキュリティ・モジュール（HSM）とシームレスに統合可能
- vSphere®およびvSAN®の仮想化プラットフォームに対応するソフトウェアとして、VMware®より認定取得済み
- Microsoft AzureおよびAWSのクラウド環境におけるBring Your Own Key（BYOK）に対応



KeyControlの詳細は、entrust.com/ja/cloud-securityをご覧ください。

Entrust KeyControl

主な機能および特長

KMIPクライアントのための鍵管理

KeyControlはVMware認定済で、スケーラブルで機能豊富なKMIPサーバとして、暗号化されたワークロードの鍵のライフサイクル管理を簡素化します。VMware vSphereやvSANの暗号化されたクライアントや、NetApp、Nutanix、Pivot3、DB2、MySQL、MongoDBなどのKMIP対応製品のKMSとして機能します。

KMIPマルチテナント対応

セキュリティと規制遵守のために、管理者は異なるテナント環境を分離できます。

エンタープライズレベルの拡張性と性能

KeyControlは、すべての仮想マシンおよび暗号化されたデータストレージの暗号鍵を管理でき、数千の暗号化されたワークロードもサポートできるよう、拡張することができます。1つのクラスタに最大8つの鍵マネージャーを追加可能です。

AzureおよびAWSでのBring Your Own Key (BYOK)

KeyControlでは、Microsoft AzureおよびAWSのユーザマスター鍵と、AWSおよびAzureのネイティブ鍵に対して、単一の管理コンソールで鍵を一元管理することができます。これはMicrosoft AzureおよびAWSで生成したネイティブ鍵のライフサイクル管理を可能にするだけでなく、独自の暗号鍵を生成したい場合は制御、自動化および管理を最大限に行うことができ、自社環境で作成した鍵のMicrosoft AzureおよびAWSへの持ち込みも可能となります。これには、以下のような多数のメリットがあります。

- Bring Your Own Key（BYOK）の生成とMicrosoft AzureおよびAWSへのエクスポートの工程を簡素化
- nShield HSMを活用し、豊富な情報量から暗号鍵要素を作成
- Microsoft AzureおよびAWS上でのマスター鍵の完全な管理
- 鍵はKeyControlにバックアップ（復元可能）され、ユーザによる制御を維持
- 詳細な鍵のライフサイクル管理：期限切れへの対応（無効化、鍵要素の削除）と鍵の交換

マルチクラウドのワークロード暗号化へのアップグレード

KeyControlは、マルチクラウドのワークロード暗号化とポリシーベースの鍵管理を可能にする、Entrust DataControlに簡単にアップグレードすることができます。これにより、複数のクラウドプラットフォーム間を移動しても、インストールから起動、各ワークロードの安全な停止まで、ポリシーを確実に適用することができます。

対応するプラットフォーム

- プライベートクラウドプラットフォーム：vSphere、vCloud Air (OVH)、VCE、VxRail、Pivot3、NetApp、Nutanix
- パブリッククラウドプラットフォーム：AWS、IBM Cloud、Microsoft Azure、VMware Cloud (VMC) on AWS、Google Cloud Platform (GCP)
- 対応するハイパーバイザー：ESXi、Hyper-V、Xen、AWS、Azure

対応するオペレーティングシステム

CentOS、Red Hat Enterprise Linux、Ubuntu、SUSE Linux Enterprise Server、Oracle Linux、AWS Linux、Windows Server Core 2012/2016、Windows Server 2012/2016、Windows 7/8/8.1/10

デプロイメントメディア

ISO、OVA (Open Virtual Appliance)、AMI (Amazon Web Services marketplace)、VHD (Microsoft Azure marketplace)

技術仕様

- VMware認定取得済みKMS（vSphere 6.5/6.7/7.0、vSAN 6.6/6.7/7.0、vSphere Trust Authority 7.0に対応）
- KMIP 1.1～1.4をサポート
- アクティブーアクティブのクラスタ構成による高可用性（HA）対応（1クラスタあたりKMSサーバ8台まで）
- Entrust nShield HSMを連携させることにより、オンプレミスまたはクラウドサービス(as a service)において、FIPS 140-2 レベル3に準拠
- 仮想マシンでVirtual Trusted Platform Module(vTPM)の暗号プロセッサを使用可能
- すべての登録クライアント間でTLS 1.2の使用をサポート

Entrust KeyControlは、Entrust DataControl、CloudControlとともに、データ暗号化およびマルチクラウド鍵管理を行う製品群のひとつです。

詳細は下記URLをご覧ください。
entrust.com/ja/cloud-security

ENTRUST

エントラストジャパン株式会社
DPS事業本部
東京都港区台場二丁目3番1号
トレードピアお台場
HSMinfo@entrust.com