

Cohesity FortKnox

サービスとしてのデータの隔離と復旧

企業活動を支えるデータは、かつてないほど貴重になっています。またデータは、サイバーセキュリティの脅威、停電、自然災害に対して、これまで以上に脆弱になっています。このような現実から、企業はデータのバックアップに関する3-2-1戦略（3つのデータのコピーを、2種類のメディアに保存し、そのうち1つをオフサイト環境に置く）へのアプローチを見直す必要に迫られています。データを磁気テープに保存し、オフサイトに移動してデータを隔離するという従来のエアギャップ手法は、増加するランサムウェア攻撃に対してデータのセキュリティを確保する一方で、迅速な復旧を妨げ、厳しいサービスレベル契約（SLA）を達成する妨げになっています。データを保護しながら競争力を維持するために、企業は物理的およびネットワーク的に隔離された仮想エアギャップを取り入れ、データの安全性と高可用性の両方を提供する最新の3-2-1戦略を採用しています。

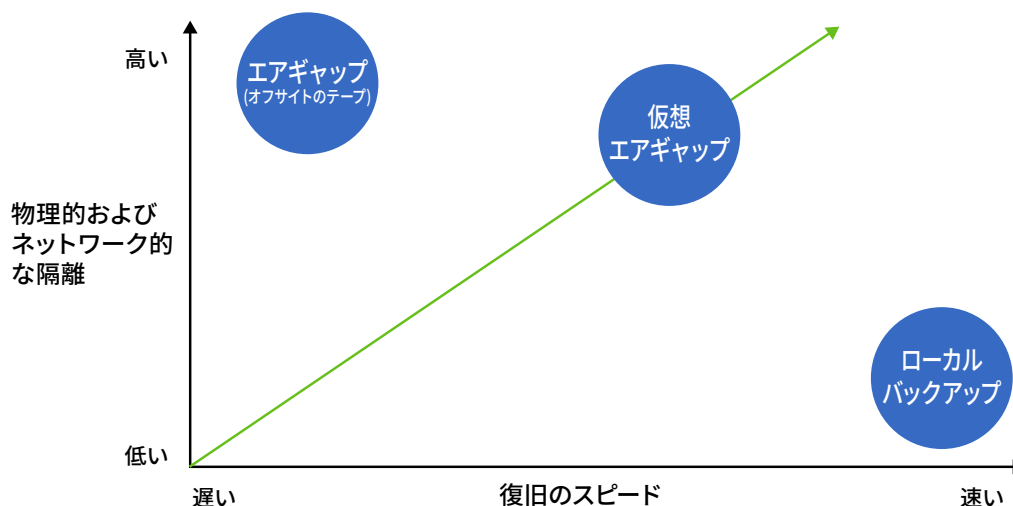
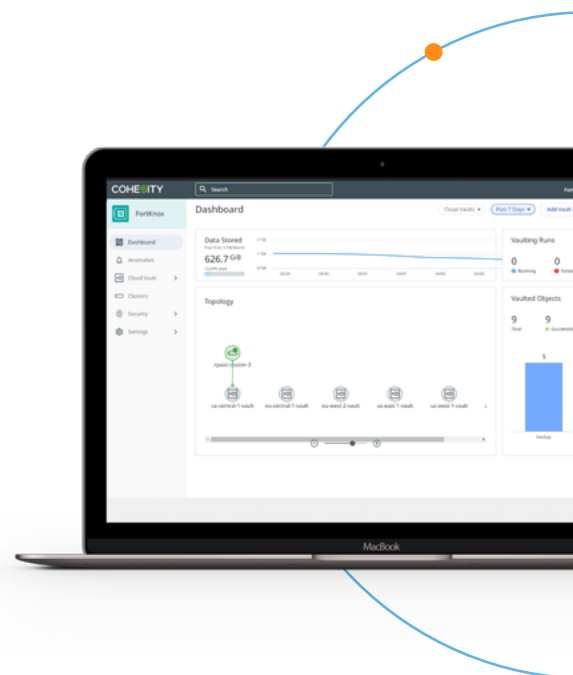


図1: 仮想エアギャップによる最新のデータ隔離で、セキュリティとアジリティのバランスをとる

クラウド時代の最新のエアギャップ

Cohesity FortKnoxは、企業のセキュリティとアジリティの優先順位を効果的にバランスし、クラウド時代の最新の3-2-1戦略を推進します。FortKnoxは、SaaS型のデータ隔離と復旧ソリューションで、仮想エアギャップを介してCohesityが管理するクラウド保管庫にイミュータブルな（変更不可の）データコピーを置くことで、サイバーレジリエンスを向上させることができます。FortKnoxを利用する組織は、物理的、ネットワーク的、運用的なデータ隔離により、ランサムウェアやその他のサイバーセキュリティの脅

威に対し追加のセキュリティレイヤーを得ることができます。FortKnoxは、運用を劇的にシンプルにし、コストを削減できるため、社内で管理する際の隔離ソリューションの複雑さとリソース要件を不要にします。FortKnoxは、パブリッククラウドを含む、元の場所や代替場所へのきめ細かい復旧をサポートすることで、攻撃への備えと迅速かつ確実な復旧を可能にするクラウドサービスです。

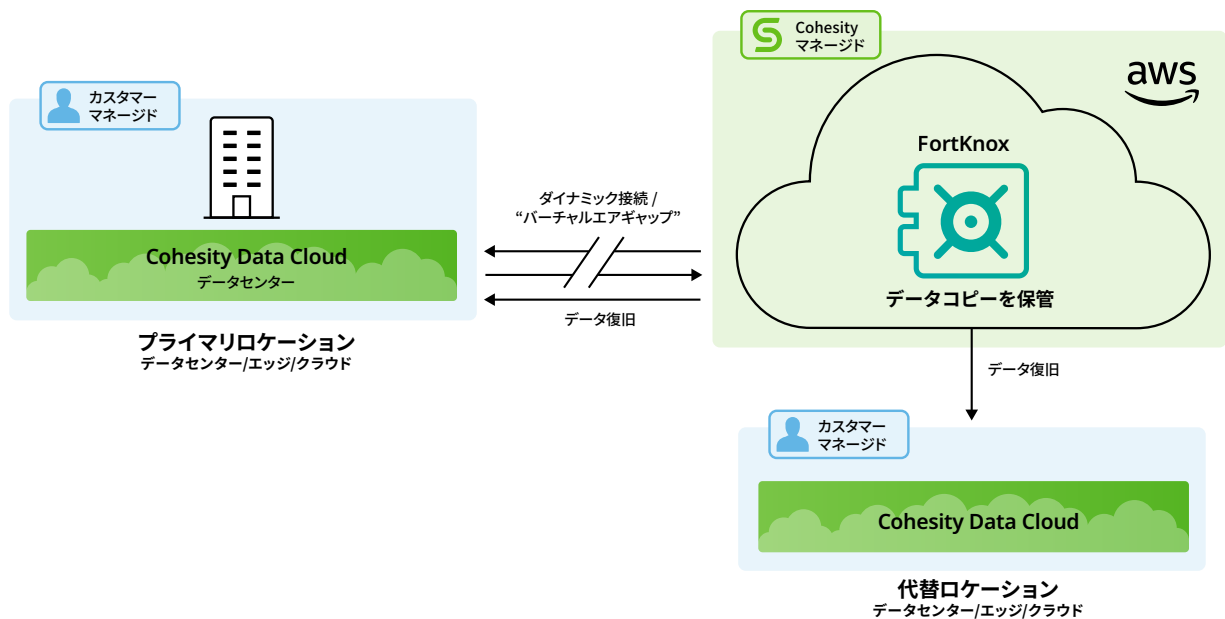


図2: Cohesity FortKnox は、元の場所または代替場所へのデータ復旧により、サイバーレジリエンスを向上

主なメリット

オンプレミスまたはクラウド内のデータ保管庫を管理することは、社内チームにとって複雑でコストがかかる場合があります。特に、バックアップを削除してデータを盗むといった破壊的なランサムウェアとスキルのギャップに直面した場合です。FortKnoxは、新しいデータ隔離技術によってこれらの障害を克服し、ランサムウェア攻撃が増加する中、データの回復力を向上させます。

追加の保護レイヤーでデータと評判を守る

FortKnoxは、最小特権と職務分離という概念に基づき、詳細なレベルのゼロトラストセキュリティの原則で構築された多層構造のCohesity脅威防御アーキテクチャの不可欠な要素です。高度なアクセス制御と脅威の早期検知機能により、犯罪者を寄せ付けないようにします。FortKnoxは、設定可能なデータ転送時間すなわち仮想エアギャップを介してCohesityが管理するクラウド保管庫にイミュータブルな(変更不可の)データコピーを保存し、そのデータコピーはさらに安全に保護されます。例えば、ロールベースアクセス(RBAC)、暗号化、多要素認証(MFA)、WORMロックポリシー、重要なアクションを承認するために少なくとも2人の従業員を必要とするクォーラムルールなど、不正なアクセスや改ざんからデータを保護するための保護対策が講じられています。FortKnoxは、単一のUIでグローバルのデータ保管庫を管理できるほか、異常なスナップショットを監視してサイバー犯罪を自動的にスキャンする機能も備えています。

As a Serviceの利用により、オペレーションの劇的なシンプル化とコストの削減を実現

FortKnoxは、システム規模に応じて支払いをするサービスでコストを抑え、企業が接続、データ保管、データ復旧をシンプルに行えるようにします。「DIY」のデータ保管庫を導入/維持するように、関連するクラウドストレージ

やエグレスコストについて心配する必要はありません。FortKnoxのサブスクリプションでカバーされるからです。データをクラウド保管庫に安全に預けたり、迅速に復旧したりする必要がある場合、Cohesityは非常に安全な一時的なネットワーク接続を確立し、サイバー犯罪者や権限のない内部関係者が隔離したデータへアクセスすることを制限しながらも、ビジネスSLAを満たします。チームは、カスタマイズ可能な保護ポリシーで、FortKnoxのデータ保管と復旧を活用することができます。FortKnoxは、企業の攻撃対象領域を最小限に抑えるだけでなく、データ侵害の可能性も低減します。

また、Cohesityは、FortKnoxに2つのストレージ階層オプション(ランサムウェア対策のユースケースに適した即時データ復旧用のウォームストレージ層と、コンプライアンスのユースケースに適した最大12時間のRTOのコスト効率の良いコールドストレージ層)を提供することで、様々なRTOと予算要件に対応する柔軟性をお客様に提供しています。

高速復旧で時間短縮と事業継続性の向上を実現

FortKnoxは、データを元の場所または代替場所へ高速かつき細かい単位で復旧し、企業の俊敏性を向上させます。推奨する復旧サイトは、オンサイト、パブリッククラウド(Amazon Web Services、Microsoft Azure、Google Cloud Platformなど)、またはエッジロケーションです。FortKnoxはデータ保管庫のデータが変更されるのを防止しているため、本番データが感染または紛失した場合でも、感染していないデータコピーを用意に判別して復旧することができ、組織は安心することができます。従来のバックアップやエアギャップソリューションとは対照的に、FortKnoxは、データボリューム全体をリストアする必要がなく、特定のファイルやオブジェクトを迅速に復旧させることができます。

仕様	
バーチャルエアギャップ	- 転送ウィンドウを設定可能で、それ以外の時間はデータ保管庫への書き込みや読み取りをロック - データ保管庫のデータコピーを、物理的、ネットワーク的、管理的にカスタマー環境から隔離 (バーチャルエアギャップともいいます)
イミュータビリティ (変更不可)	- AWSのオブジェクトロック機能を利用した変更不可のデータロック (WORM) - 読み取り専用のスナップショットにより、意図的または非意図的なデータ保管庫のデータの変更/削除を防止
データセキュリティ	- 保存中のデータと転送中のデータの暗号化 - Cohesity管理またはお客様管理による柔軟なKMS - クォーラム制御による復旧で、データ流出経路を最小化
アクセス制御	- 多要素認証 (MFA) - きめ細かいロールベースのアクセス制御 - 復旧などの重要なアクションに対するクォーラム - トークンによる短時間の認証でデータ保管庫へのアクセスを制限 - HTTPS経由の認証済みAPIコールベースのアクセス - 認証済みCohesityクラスタのみにアクセスを制限
ランサムウェアの検知	機械学習による異常検知とレポートニング
高速復旧	- マシン主導のクリーンなスナップショットの推奨で、インシデントに対する迅速なレスポンスが可能 - 厳しいSLAを満たすため、元の場所または代替場所への迅速できめ細かい復旧
As a Serviceでの消費	- 接続、保管、復旧のシンプルなSaaSソリューション - カスタマイズ可能な保護ポリシーによるセルフサービスのデータ保管と復旧 - バックエンドTB (BETB) の使用量に応じた従量課金モデル
ひとつの管理コンソール	- グローバルのデータ保管庫をダッシュボードで一元的に表示/管理 - SLAベースのポリシーでシンプルに管理

Cohesity FortKnoxでデータの隔離と復旧をシンプルかつモダナイズ。
FortKnoxは[無料トライアル](#)でお試しいただけます。

COHESITY



© 2023 Cohesity, Inc. All rights reserved.

Cohesity、Cohesityのロゴ、SnapTree、SpanFS、DataPlatform、DataProtect、Helios、およびその他のCohesityのマークは、米国および/または海外におけるCohesity, Inc.の商標または登録商標です。その他の会社名および製品名は、関連する各企業の商標である可能性があります。本資料は、(a) Cohesityと弊社の事業および製品に関する情報を提供することを目的としています。(b) 本資料が作成された時点では、真実かつ正確であると考えられていますが、予告なく変更されることがあります。(c) 本資料は、“現状有姿”で提供されます。Cohesityは、いかなる種類の明示的または黙示的な条件、表明、保証も放棄します。