COHESITY

ソリューション概要

データの隔離でランサムウェア攻撃と内部脅威を防御

主なメリット

- データセキュリティ戦略の強化
- サイバー攻撃と内部脅威の両方からデータを守る
- SLAを満たし、ビジネスリスクを低減
- 大規模なインスタントリカバリでダウンタイムを削減

Cybersecurity Ventures社の最近の調査によると、2031年までに企業は2秒に1回ランサムウェアの攻撃を受け、その被害額は2,650億ドル以上になるとされています。また、全世界の企業の34%以上が内部からの攻撃に直面し、過去2年間と比べ47%増加する、と Tech Jury社は報告しています。サイバー攻撃や内部攻撃の件数と深刻さが増していることから、企業はITシステムとデータの強化に取り組み、その多くは NISTのCybersecurity Framework の指針に従って、多層防御戦略を取り入れています。

Cohesityの次世代データ管理に投資する企業は、先手を打つことができます。Cohesityは、以下のような徹底的な防御機能を持つことを目的として構築されているからです:

- **イミュータブル (変更不可の) スナップショット** - バックアップデータのゴールドコピーとし、外部に公開したりマウントしたりすることはありません
- **DataLock** - バックアップスナップショットを変更できないよう、時間を区切ってWORMロックします
- **暗号化** - 保存時も転送時もデータを暗号化します
- **ロールベースのアクセス制御 (RBAC)** - 最小権限 (least privilege) と知る必要 (need to know) の原則に基づき、きめ細かい管理者アクセスとユーザーアクセスを実装可能です
- **バックドアなし** - 正規の顧客ユーザーのみによるアカウント有効化をサポートしています
- **安全なSSHアクセス** - 安全ではないネットワーク上で安全なアクセスパスを提供します
- **データの隔離** - サイバー脅威や内部の脅威からデータを安全に保つためのデータ隔離が可能です

データの隔離は、既存のバックアップやリカバリ、ディザスタリカバリ (DR) ソリューションに取って代わるものではなく、むしろ追加の保護レイヤーを提供する方法です。その目的は: データセキュリティ戦略全体を強化することにあります。

Cohesityによる最新のデータ隔離

NISTの定義によると、エアギャップは、セキュリティ強化のために、少なくとも1つのデータコピーを物理的および電子的に分離して保存することを求めています。安全性は高いものの、この方法は現代の企業が必要とするRTO/RPO目標には対応できません。そのため、RTO/RPO要件をより良くサポートする代替案として、データ隔離という方法が登場しました。この方法では、一時的に非常に安全な接続を行うことで、バックアップデータを、クラウドや他の場所に保存することができます。これにより、ランサムウェアや内部脅威からデータを保護し、かつ、組織のSLAをサポートする改ざん耐性が高い環境を提供することができます。

Cohesityを使用することで、企業はSLAやリスク許容度に妥協することなく、最大限の選択肢と柔軟性を持って、組織のデータを犯罪者から隔離し保護することができます。Cohesityは、柔軟な実装で下記へのデータ隔離をサポートします:

- **遠隔地のCohesityクラスタ** – お客様は、あるイミュータブルなCohesityクラスタから、オンプレミスで稼働している、またはパブリッククラウド上の仮想クラスタとして稼働している別のリモートクラスタへデータをレプリケートすることができます。テープをオフサイトに輸送する必要がある従来のデータ隔離手法と異なり、このデータ隔離手法ではリモートクラスタ上のデータをすぐに利用できるため、RTOとRPOを短縮することができます。
- **NASターゲット** – Cohesityは、WORMをサポートするNAS外部ストレージターゲットにデータをアーカイブすることで、より低いRTOとRPOでデータを隔離することができます。
- **クラウド** – パブリッククラウドの拡張性と弾力性を活用するため、企業はデータ隔離を実現する最新の方法の1つとしてクラウドを利用しています。Cohesityは、クラウドや、オブジェクトロックとオブジェクトバージョニングをサポートするS3互換のストレージへのアーカイブをサポートし、データの隔離、RTOとRPOの短縮、TCOの削減を実現します。
- **テープ (エアギャップ)** – Cohesityは、バックアップからテープへのデータアーカイブを可能にし、IT部門がテープをオフサイトストレージに送ることで、物理的な関与によってのみのアクセスを保証します。

Cohesityクラスタへのデータ隔離による最適なリスクとSLAのバランス

Cohesityのお客様は、バックアップデータを遠隔地のCohesityクラスタにレプリケートすることで、データの回復力を得るだけでなく、リスクを低減しながら厳しいビジネスSLAを達成することができます。NISTのCybersecurity Frameworkの多層防衛モデルに従って、Cohesity は、隔離サイトにある別のイミュータブルCohesityクラスタにデータをレプリケートします。これにより、最新のデータ保管庫を提供し、分離したネットワークに保存し、WORM をサポートすることを可能にします。

図1は、Cohesity が DataLock有効化ポリシーを使って、外部やアプリケーションへの直接アクセスがない、ファイアウォール内側の分離したネットワーク上にあるCohesityクラスタに、イミュータブルバックアップデータのコピーをレプリケートする方法を示しています。企業の管理者だけが、データ転送の間だけ必要なポートを開いたり閉じたりすることで、データの安全性を確保します。また、このプロセスさえも、イミュータブルスナップショットや、プライマリのCohesityと隔離環境との間で異なるネットワークポートを使用することで守られています。

隔離したCohesityクラスタに複製することで、企業はデータセンターをモダナイズし、より強力なサイバー防御、大規模インスタントリカバリ機能を備えた高速リカバリ、ネットワーク帯域幅要件を下げながらもより短いRTO/RPOを達成することができます。Cohesityのエアギャップ保護でITシステムを強化し、増加するランサムウェアや内部脅威からビジネスを守ることができます。

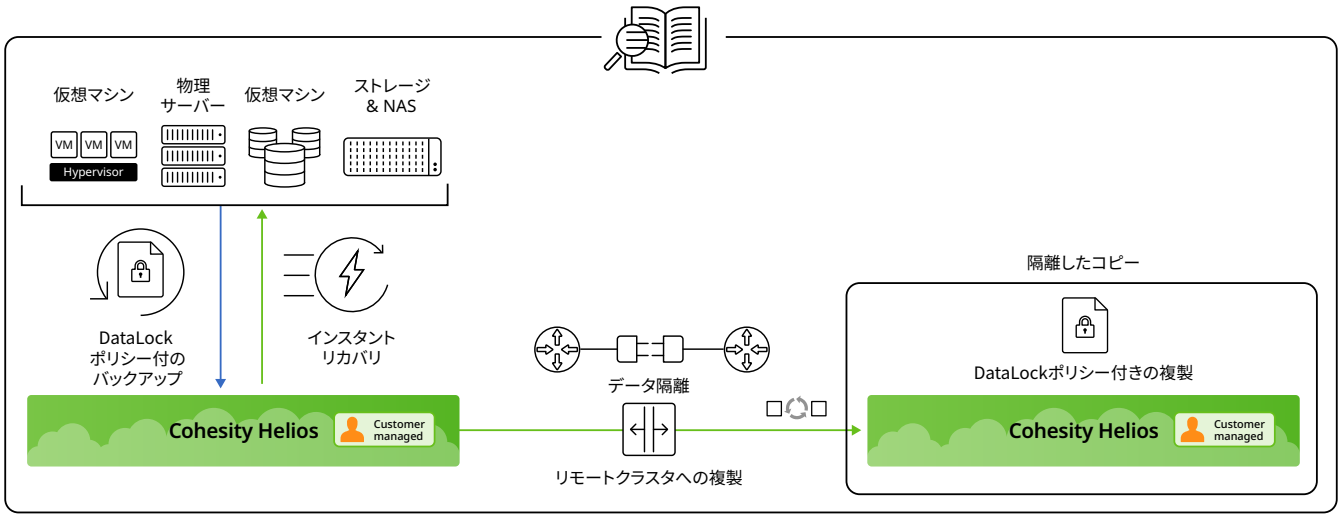

図1: 遠隔地のCohesityクラスタへのデータ隔離

詳しくはこちらをご覧ください: www.cohesity.com/jp

COHESITY