COHESITY

ソリューション概要

Cohesityで ランサムウェア攻撃に 対抗する

主なメリット

- 徹底的な防御アーキテクチャでデータとビジネスを守る
- 機械学習ベースの異常検知により、潜在的な攻撃を迅速に特定し、、セキュリティオペレーションと統合
- 信頼性の高い大規模リカバリでダウンタイムを削減

Enterprise Strategy Groupの調べによると、79%の組織がランサムウェアに攻撃され、56%が身代金を支払い、すべてのデータを復旧できたのはわずか14%でした。ランサムウェアは衰える気配がありません。Cybersecurity Ventures社の報告によると、2025年までに世界のサイバー犯罪のコストは年間10.5兆USドルに達し、2031年[1]までには、企業は2秒に1回ランサムウェア攻撃のの被害を受けると予想しています。こうしたデジタル恐喝スキームに対する認識は高まっていますが、バックアップデータやインフラを標的とした、より巧妙で集中的な攻撃は、世界中の企業を脅かし続けています。ランサムウェアの攻撃を受けた企業は、経済的な損失に加えて、顧客の不信感や、医療の場合には人命に関わるリスクを抱えることになります。

Cohesityはランサムウェアの攻撃に効果的に対抗し、企業が身代金の支払いを回避できるようにします。Cohesityの包括的なデータセキュリティとデータ管理ソリューションは、ランサムウェアからバックアップデータを守り、攻撃を検知し、迅速に復旧するための多層的アプローチを特徴としています。Cohesity独自のイミュータブル (変更不可の) アーキテクチャは、バックアップデータの暗号化、変更、削除ができないようにします。また、機械学習を用いて、可視性を提供し、データの異常を継続的に監視します。最悪の事態が発生した場合は、Cohesityはパブリッククラウドを含むお客様が持つすべてのデータからクリーンコピーを探し出し、即座に復旧してダウンタイムを短縮します。

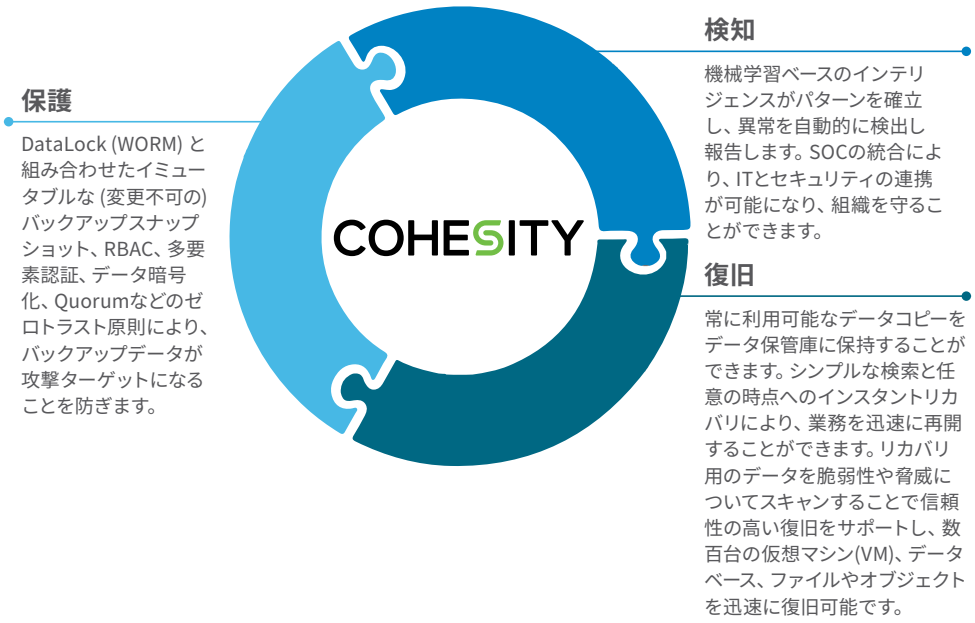

図1: Cohesityは、ランサムウェア攻撃からの保護、検知、復旧のための包括的機能を提供します。

1. Cybersecurity Ventures: Top 6 Cybersecurity Predictions And Statistics For 2021 To 2025 (Dec. 30, 2021)

保護

LockyやCryptoといった巧妙なランサムウェアは、シャドウデータコピーやリストアポイントデータを破壊するために使用されています。そのため、企業のバックアップインフラは、企業の防御の一部として存在するべきなのに、サイバー犯罪者の主要な標的となっています。Cohesityは、バックアップが攻撃対象になるのを防ぐことで、侵入者を阻止します。

Cohesity SpanFS™は、第3世代の分散ファイルシステムで、ランサムウェアの攻撃に対する独自の多層防御機能を提供しています。特に、Cohesityはイミュータビリティ (不変性) を基盤としているため、ランサムウェア攻撃に対して最高レベルの保護を提供することができます。

- **イミュータブルスナップショット** – すべてのバックアップスナップショットは、デフォルトで、Cohesity内にイミュータブル (変更不可) の状態で保存されます。オリジナルのスナップショット (別名ゴールドコピー) が、外部のシステムやアプリケーションにマウントされたり、公開されたりすることは決してありません。新しいデータを書き込んだり、リカバリのためバックアップを読み書き可能な状態でマウントする唯一の方法は、オリジナルのバックアップのゼロコストクローンを作成することで、これはシステムによって自動的に実行されます。
- **DataLock** – バックアップ用のWORM機能により、ロールベースのDatalockポリシーを作成し、選択したバックアップスナップに適用することができます。組織内のセキュリティ担当者は、この機能を使ってスナップを WORM 形式で保存することができます。管理者やセキュリティ担当者のロールであっても、時間的制約をつけた設定を削除することはできず、ランサムウェア攻撃からの保護を強化することができます。
- **ロールベースのアクセス制御 (RBAC)** – データやシステムへの不正アクセスのリスクを軽減するため、Cohesityは、ITスタッフが各人に特定の業務に必要な最小レベルのアクセス権を付与することを可能にします。
- **多要素認証 (MFA)** – 万が一犯罪者が企業のシステムのパスワードにアクセスしても、その個人はMFAまたは多段階認証で追加のセキュリティレイヤーを通過しない限り、Cohesityのバックアップにアクセスすることはできません。Cohesityは、強力なActive Directoryとの統合、MFA、アクセスコントロールリスト、ミックスモードのロールベースアクセス制御 (RBAC)、包括的なシステム/製品レベルの監査など、さまざまな認証および認可機能をサポートしています。
- **データ暗号化** – Cohesityは、転送中および保存中のデータに対して、ソフトウェアベースのFIPS認証のAES-256標準暗号化方式を採用しています。この暗号化モジュールは、米国国立標準技術研究所 (NIST) の連邦情報処理規格 (FIPS) 140-2 Level 1規格で検証され、世界中で信頼されています。
- **Quorum** – 内部の脅威や認証情報の盗難からデータやシステムを保護するため、Cohesityでは、組織内の誰かが行おうとするルートレベルの変更や重要なシステム変更には、複数の人物による承認を必要とすることができます。

次世代データ管理プラットフォームであるCohesity Heliosは、イミュータブルバックアップスナップショット、DataLock機能、RBAC、MFA、さらにQuorum (別名、4つの目のルール) を独自に組み合わせて提供することで、バックアップデータがランサムウェア攻撃の対象になることを防ぎます。

検知

サイバー犯罪者がその手法を強化し、変更し続ける中、Cohesityはグローバルなエンタープライズ SaaSベースの管理ソリューションにより、企業が侵入を検知することを容易にします。Cohesityのお客様は、単一のダッシュボードで、世界中のデータやアプリケーションを監視、管理し、迅速にアクションを取ることができます。ランサムウェアとの戦いにおいて、Cohesity Heliosの機械学習 (ML) は、自動的かつ継続的に監視し、異常が検出されると通知することができるので、人間が見逃してしまうかもしれないインサイトも提供することができます。

最先端のMLアルゴリズムにより、ITニーズをプロアクティブに評価し、定期的にインフラリソースを自動化します。データ取り込みなど組織のデータ変更率が通常の範囲を超えた場合 (データの変更率の評価は、論理データの日々の変更率、グローバル重複排除後の保存データ、または過去のデータ取り込み量をベースに行っています)、Cohesity Heliosの機械学習による異常検知は、IT管理者に通知を送ります。IT部門は、データの変更が通常のパターンと一致していないことを即座に知ることができます。さらに、ユーザーの行動を監視することで、データの使用状況が不正なデータアクセスや利用を示していて、データの流出につながる可能性がある場合、組織はそれを特定することができます。

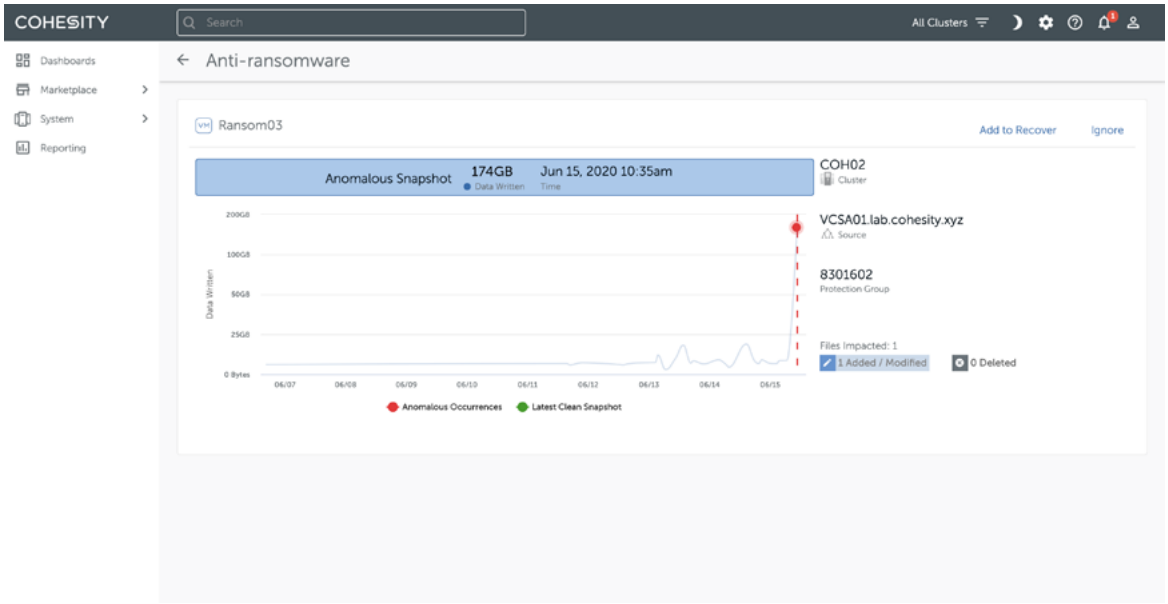

図2: Cohesity Heliosで、企業はランサムウェアの侵入を検知

Heliosは機械学習によってパターンを確立し、データの取り込みや変化率の異常を自動的にスキャンし、ランサムウェアの攻撃の可能性を警告します。異常が検出されると、企業のITチームとCohesityのサポートチームの両方に同時に警告を発し、迅速な対処を可能にします。

Cohesityは、ランサムウェア攻撃の可能性を検知するためにバックアップデータの変更率を監視するだけでなく、非構造化ファイルやオブジェクトデータ内のファイルレベルの異常についてログデータを収集します。組織は、ファイルへのアクセス頻度、特定のユーザーやアプリケーションによって変更、追加、削除されたファイルの数などを確認し、ランサムウェアの攻撃を迅速に検知することができます。

復旧

サイバーセキュリティの脅威は、内部でも外部でも発生し、しかもスピードもあります。だからこそ、復旧は予測可能かつ迅速でなければなりません。Cohesityは、身代金を要求された企業データとアプリケーションの復旧プロセスを、迅速かつ大規模に行います。Cohesityは、イミュータブルバックアップに加え、ミッションクリティカルなデータを隔離し、最新の正常なコピーデータをセキュアに保持するために、複数のポリシーベースの方法を提供しています。お客様独自の復旧要件やセキュリティ要件に対応するため、Cohesityマネージドのクラウドデータ保管庫であるCohesity FortKnoxへのデータの隔離、別のイミュータブルクラスタへのレプリケーション、またはIron Mountainなどのオフサイトストレージへのテープアウトを行うことが可能です。

Cohesity Heliosの機械学習によるサポートは、リストアの実行に使用するデータのクリーンコピーを推奨することで、復旧スピードを加速化します。また、プラットフォームのグローバル検索機能を活用することで、複数の環境にあるデータを素早く見つけて、アクセスすることも可能です。

CohesityのCyberScanは、クリーンなリストアを保証し、本番環境にソフトウェアの脆弱性や暴露ウィルスを再投入しないように、保護したスナップショットの健全性と復元性の状態を深く可視化します。CyberScanは、各スナップショットの脆弱性インデックスと、ソフトウェアの脆弱性に対処するための実行可能なレコメンデーションを表示します。これにより、ランサムウェア攻撃からクリーンかつ予測可能な復旧を行うことができます。機械学習による脅威インテリジェンスを活用し、スナップショットをスキャンすることで、システムへのアクセス、権限の昇格、データの流出や暗号化に脅威者が利用する最新のIOC (侵害指標) を確認できます。プライバシーと業界の規制をサポートするために、組織はデータの露出を理解する必要があります。データ分類を活用することで、企業は、流出した可能性のある個人情報や機密データに迅速にアクセスすることができます。

完全にハイドレートされたスナップショットとCohesity独自のSnapTreeのB+Treeアーキテクチャ、MegaFile、インスタントマウントとを組み合わせることで、数百台の仮想マシン (VM)、ファイル、オブジェクト、大規模データベースを瞬時にリストアし、ダウンタイムの大幅な短縮を実現します。

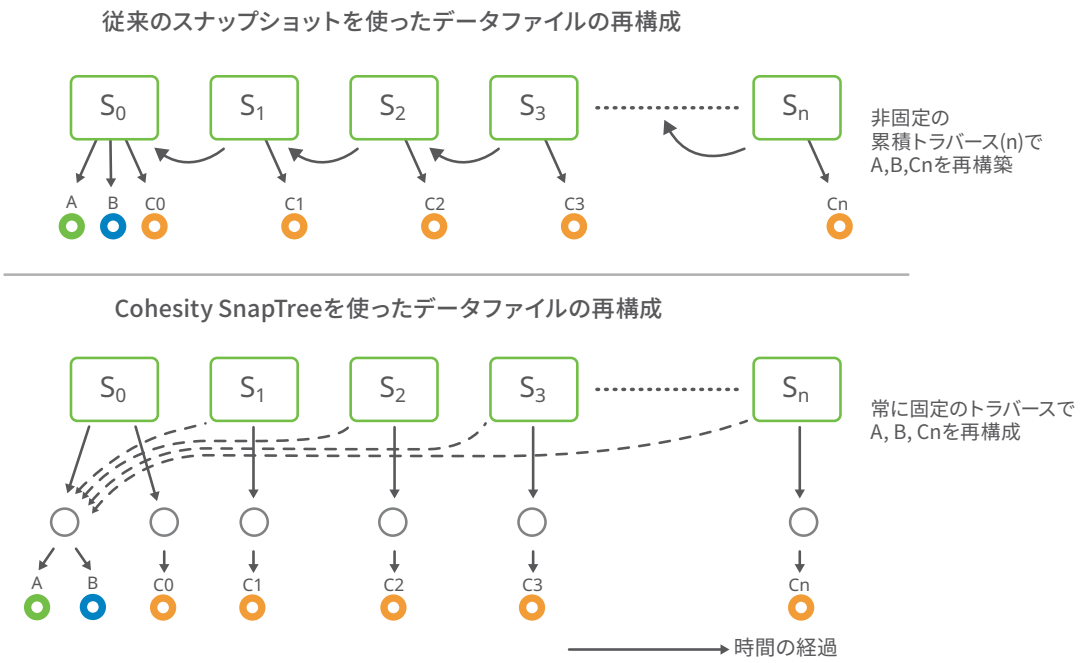

図3: Cohesityの特許技術であるSnapTreeは、オーバーヘッドなしで無制限のスナップを実現し、大規模インスタントリカバリをサポートします。

Cohesityでランサムウェア攻撃に対抗する

バックアップは、巧妙で破壊的なランサムウェア攻撃に対する最初で最後の砦です。Cohesityの包括的なランサムウェア対策ソリューションは、ダウンタイムを縮小し、ビジネスの継続性を確保するために必要なデータを保護、検出し、そして最も重要なこととして、迅速なデータ復旧を可能にします。

詳細はこちら: www.cohesity.com/jp/solutions/ransomware

COHESITY