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

- イミュータブル (変更不可の) スナップショットでバックアップを守る
- 機械学習による異常検知
- 高速な大規模リカバリでダウンタイムの削減

データは、デジタル経済における差別化要因です。そのため、データは最も価値のあるビジネス資産であると同時に、最も狙われる資産にもなっています。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、2021年[1]は11秒ごとに企業がランサムウェア攻撃の犠牲になると予想しています。こうしたデジタル犯罪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の包括的なエンドツーエンドのソリューションは、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削減します。

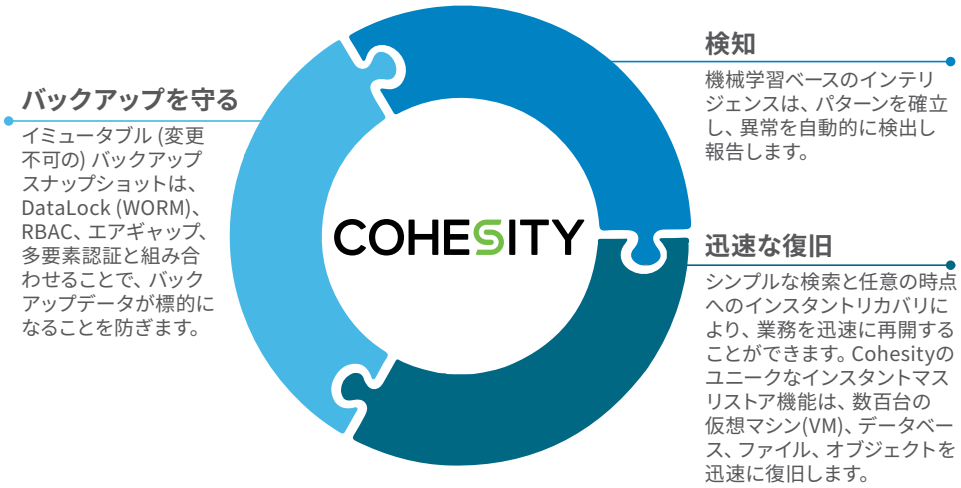

図1: Cohesityは、ランサムウェア攻撃からの保護、検知、復旧のための包括的機能を提供します。

1. Cybersecurity Ventures: Top 5 Cybersecurity Facts, Figures, Predictions, And Statistics For 2021 To 2025 (January 8, 2021)

バックアップデータの保護

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は、全く新しい専用のファイルシステムであるCohesity SpanFS™を備えており、ランサムウェアの攻撃に対して独自の多層防御機能を提供します。中でもCohesityは、読み取り専用モードのスナップショットを持つイミュータブルファイルシステム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。

- イミュータブルファイルシステムは、高い頻度で、無制限に読み取り専用モードのスナップショットを取り、あまり負荷をかけず保存することができます。オリジナルのバックアップジョブは、イミュータブル (変更不可の) 状態で保存され、外部システムからマウントされるといったようなアクセス可能な状態にはなりません。読み書き可能な状態でバックアップをマウントする唯一の方法は、そのオリジナルのバックアップをクローンすることであり、これはシステムによって自動的に行われます。ランサムウェアは、マウントされた (読み書き可能な) バックアップファイルを削除することはできても、イミュータブルスナップショットに影響を与えることはできません。
- CohesityのファイルシステムであるSpanFSは、非常に多くのViewを持ち、これらのViewを瞬時にクローンすることができるので、ストレージ使用量はほとんど増えずコストはほぼゼロです。

機密データへの不正アクセスを防止することは、Cohesityのデータ保護ビジョンの核心です。そのため、ランサムウェア対策に関するCohesityのイノベーションは、イミュータブルファイルシステムだけでなく、以下の機能も提供しています:

- 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。
- エアギャップ – Cohesityは、ミッションクリティカルなデータを隔離するため複数のポリシーベースの方法を提供しています。企業独自の要件に基づいて、データを外部のクラウドストレージや別の物理的な場所へレプリケートまたはアーカイブしたり、Iron Mountainのようなオフサイトストレージへテープアウトしたりすることができます。このポリシーベースのデータレプリケーションまたはアーカイブは、RTOとRPOを低く抑え、別の場所へのデータ転送中はネットワーク接続のみを維持する柔軟性を備えています。
- 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。

マルチクラウドデータ管理プラットフォームであるCohesity Heliosは、DataLock機能を備えたイミュータブルファイルシステムに加え、ポリシーベースのエアギャップとMFAを独自に組み合わせて提供し、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。

侵入者の検知

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。

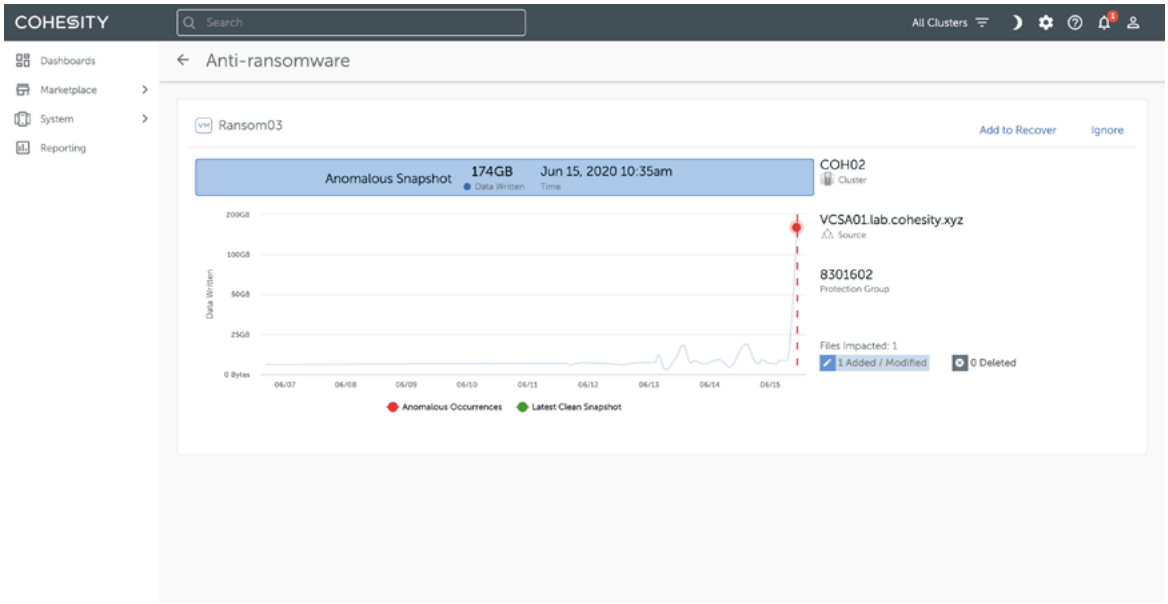

図2: Cohesity Heliosで、企業はランサムウェアの侵入を検知

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アラートが送られ、迅速に修復が行われます。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、Cohesity独自の方法として、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も検知して警告します。これには、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の分析が含まれ、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。

迅速な復旧

攻撃はいつでも起こり、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のデータとアプリケーションを取り戻すプロセスを高速化し、しかも大規模に行います。Cohesity Heliosの機械学習によるサポートは、リストアを実行するためにデータのクリーンコピーのレコメンドを行います。また、Cohesityプラットフォームの Googleライクなグローバル検索機能を利用して、環境間でデータを素早く見つけてアクセスすることもできます。

クリーンリストアを確実に行い、サイバー脅威やソフトウェアの脆弱性を本番環境に再度持ち込まないために、Cohesityの CyberScanは、保護され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、ソフトウェアの脆弱性に対処するため、各スナップショットの脆弱性インデックスと、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、ランサムウェアの攻撃からクリーンかつ予測可能な形で復旧することができます。

Cohesity社が特許を取得したSnapTreeのB+Treeアーキテクチャ、MegaFile、インスタントマウントを用いたフルハイドレイトスナップショットの組み合わせにより、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することで、ダウンタイムを劇的に削減することができます。

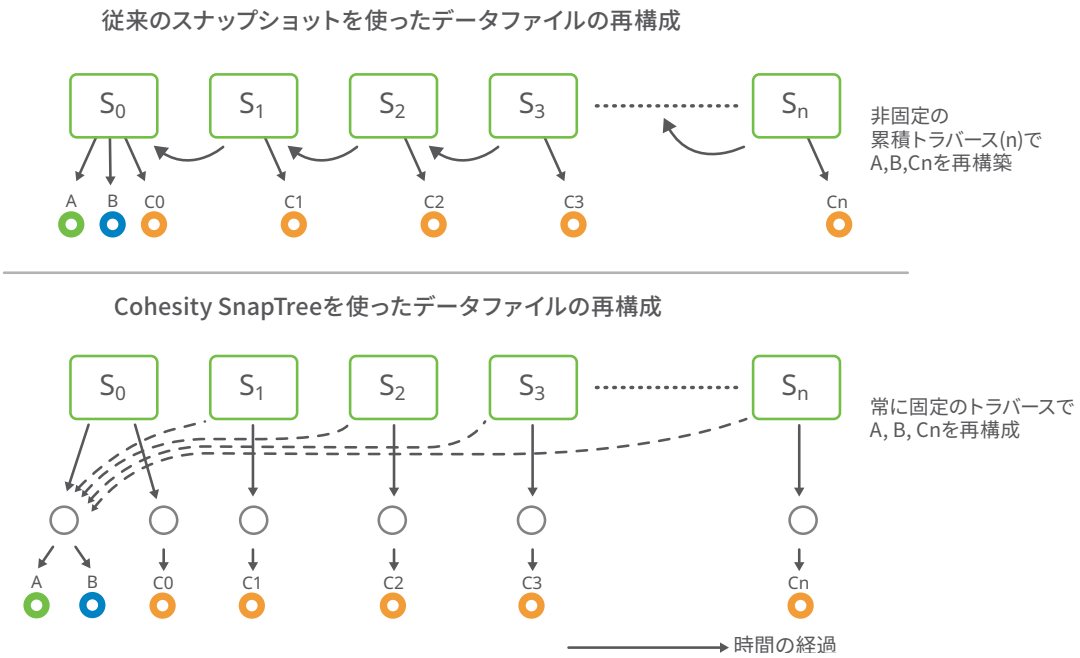

図3: Cohesityの特許技術であるSnapTreeは、オーバーヘッドなしで無制限のスナップを実現し、大規模インスタントリカバリをサポートします。

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、保護、隔離、検出、そして最も重要なのは、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迅速に復旧させることです。

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

COHESITY