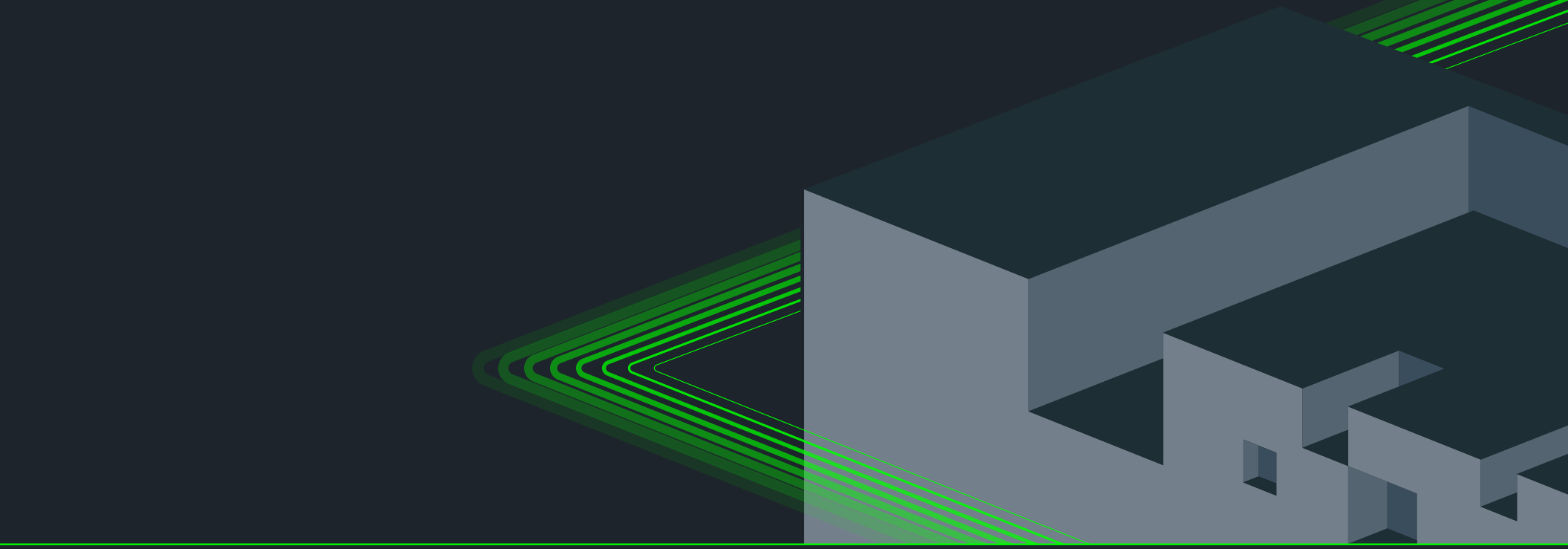


ランサムウェア時代のサイバーレジリエンス

サイバー攻撃に耐え
そこから復旧するための5つの鍵

COHESITY

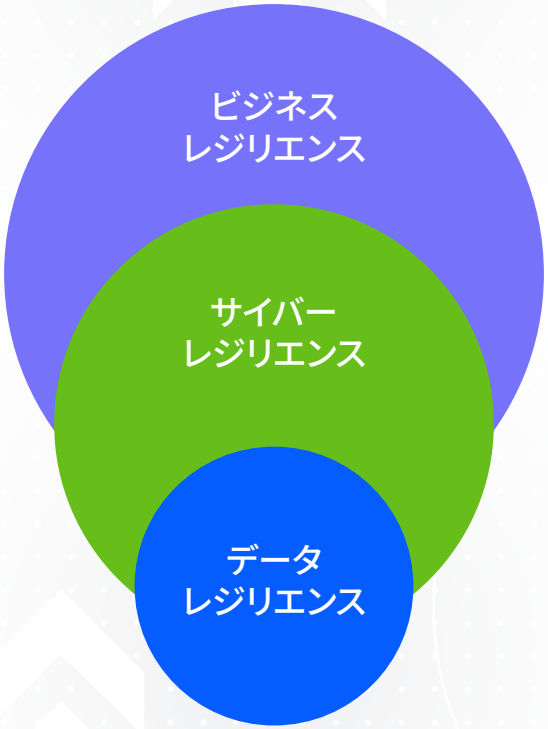
データレジリエンスからサイバーレジリエンスへ

自然災害は事業運営にとって大きな脅威です。落雷、ハリケーン、竜巻、洪水は大きな被害をもたらし、ビジネスを停止させる可能性があります。とはいえ、こうした災害は、継続的な攻撃で能動的にビジネスを脅かそうとするものではありません。このような場合は、ハードウェアの故障、不慮の削除、または自然災害が発生しても、データレジリエンス戦略によって、データを無傷のまま、アクセス可能な状態に維持することを保証できます。

これをサイバー脅威と比較してみます。脅威の行為者は、決して活動を止めることはなく、あなたのデータを人質に取り、ビジネスを停止させるために、新しいツールを採用し続けます。攻撃ベクトルは多くの場合、多面的で狡猾です。そして、脆弱性、侵害されたアカウント、その他の攻撃成果物が再び本番環境に注入されるリスクは、蔓延する脅威となっています。根本的な原因が明らかな従来の事業継続や災害復旧のシナリオに比べ、サイバー攻撃者に立ち向かうには、原因を突き止め、再発防止のための対策を講じるための調査が必要となります。

さらに、ランサムウェア攻撃では、セキュリティインフラや重要な証拠がインシデントの影響を受け、製品やサービスを提供する能力に影響を及ぼす可能性があります。

サイバーレジリエントなビジネスを展開する場合、ITとセキュリティのリーダーは、自然災害や技術的な障害による標準的なシステム停止に対応する場合と比較して、より堅牢で、動的かつ、協調的なプロセスが必要になります。サイバーレジリエンスは、データレジリエンスの実践の上に構築され、サイバーセキュリティへの備え、インシデント対応計画、従業員トレーニング、脅威インテリジェンスなどの要素が含まれます。



データレジリエンスからサイバーレジリエンスへ

今日のサイバー脅威には、保護したデータ資産のグローバルな可視化を促進し、IT担当者とセキュリティ担当者のコラボレーションを効率化するモダンソリューションが必要です。CohesityのAIを活用したモダンなデータセキュリティとデータ管理ソリューションは、サイバーレジリエンスを強化し、ビジネス全体を保護する能力を提供します。

その結果は、サイバー攻撃の脅威に耐えることができる、よりレジリエントなビジネスの実現です。

Cohesity でできることは:

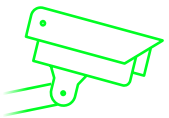
- データとリスクの把握
- データの安全性と可用性の確保
- セキュリティ運用の自動化
- 攻撃に対する効率的かつ効果的な対応
- クリーンデータの大規模復旧

もし、ではなく、いつ...

ランサムウェア攻撃は近年、複雑さと頻度を増しています。実際、組織の90%は、ランサムウェア攻撃の脅威が2023年に増加したと考えています[1]。それにもかかわらず、80%の組織は自社のサイバーレジリエンス戦略が十分でないと危惧しています[2]。このリスクの増大は、セキュリティおよびITリーダー、CEO、取締役会メンバーにとって最重要課題であり、彼らは、もし攻撃が発生したら、ではなく、攻撃が発生した時に、迅速かつ安全に対応できることに対する確実性を求めています。

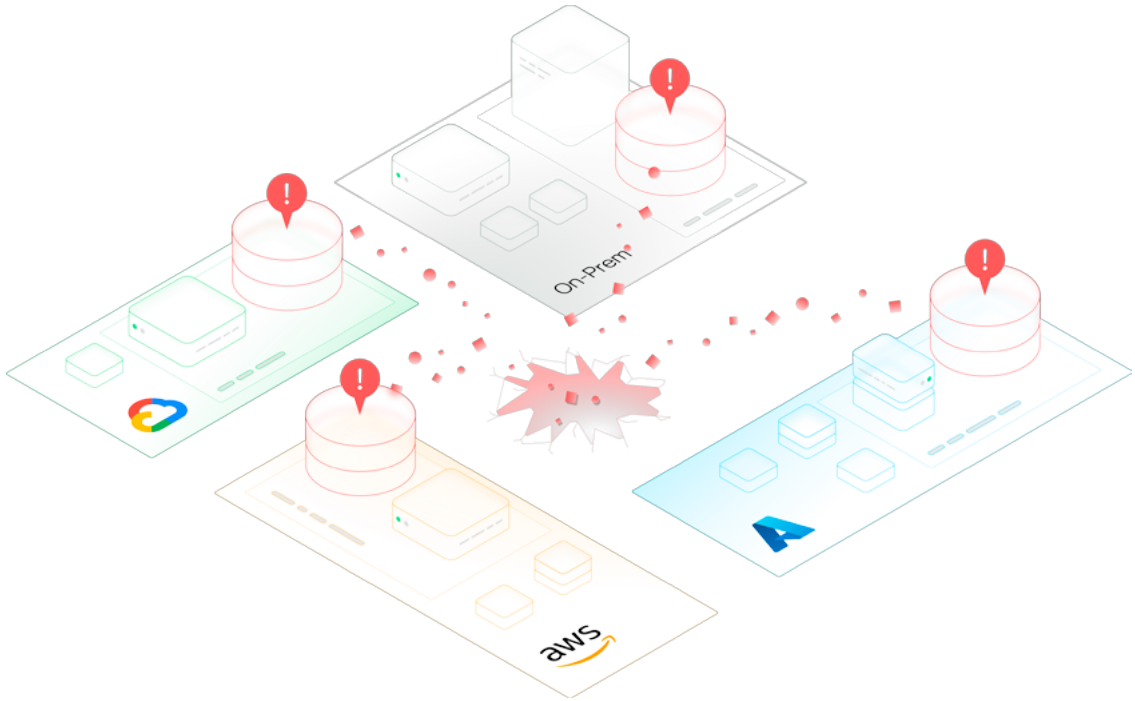
攻撃が発生した場合、脅威を最小化するために検知をスムーズに行うことが第一の課題です。組織は、汚染されたデータを本番稼動に戻す前にリスクを評価できるよう、異常やサイバー脅威を自動検知し、すべてのデータ資産を一元的に可視化する必要があります。

レガシーシステムと新しい既存のデータセキュリティ技術 (脆弱性管理など) 間の相互運用性の欠如や、システム拡張のための緊急のニーズ (クラウドホスティングなど) が、このリスクをさらに悪化させています。



80%

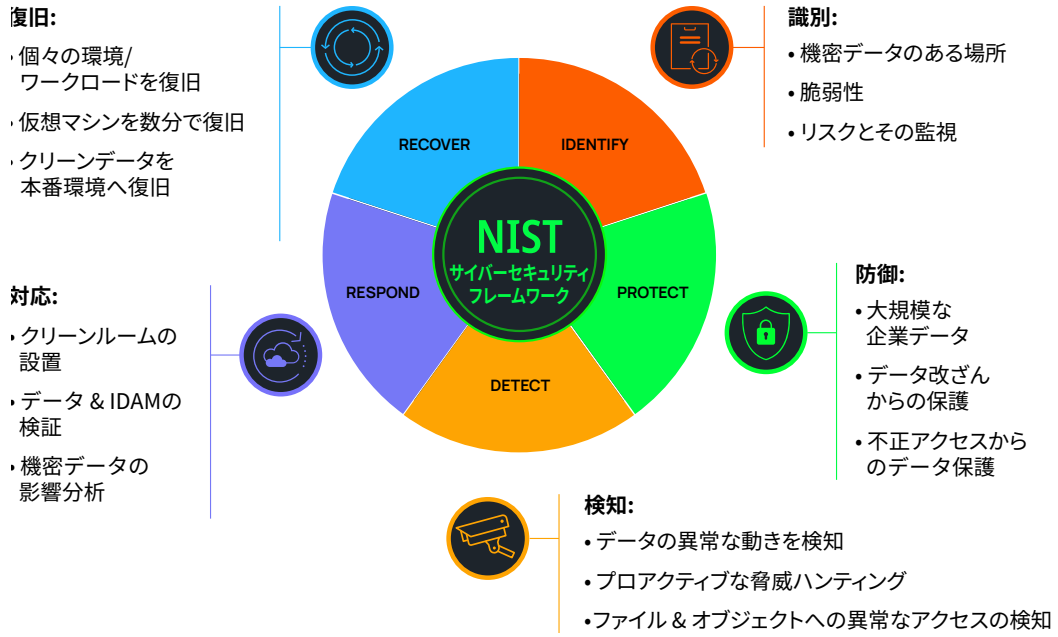
80%の組織が、自社のサイバーレジリエンス戦略が十分でないことを危惧しています。



[1-2] The State of Data Security and Management Report. 2023

5つの鍵でサイバーレジリエントなビジネスを構築

Cohesityのデータセキュリティとデータ管理ソリューションは、NISTサイバーセキュリティフレームワークの主要機能 (識別、防御、検知、対応、復旧) に適合しています。



攻撃を受ける前 — 攻撃を受けている間 — 攻撃を受けた後

識別 (Identify)	防御 (Protect)	検知 (Detect)	対応 (Respond)	復旧 (Recover)
AIを活用したデータ分類で重要なデータや機密データを識別し、継続的に異常をスキャンします。	イミュータブルなスナップショットと多層的なセキュリティ制御により、オンプレミス、クラウドネイティブ、SaaSのデータを保護、隔離します。	AIを活用した脅威インテリジェンスにより攻撃を検知し、最新のランサムウェアやその他のサイバー攻撃を特定し、影響を最小限に抑えます。	サイバークリーンルームを迅速に設け、トリアージ、調査、修復作業をサポートし、次なる攻撃を防止します。	あらゆる規模、あらゆる時点のデータを対象としたリストアで、サイバー攻撃から迅速かつ安全に復旧します。

今日の脅威の要因に対してサイバーレジリエンス戦略を向上させる各機能の主要な能力をご覧ください。

1: 識別する

重要なビジネスデータや異常値を識別

サイバーレジリエントは、最新のバックアップとリカバリから始まります。無制限のイミュータブルスナップショットにより、Cohesity内のバックアップデータを使用して、リスクエクスポージャーを把握し、攻撃の影響を最小限に抑えることができます。まず、組織の最も機密性の高いデータの場所を特定することから始めます。次に、AIによるデータ分類を使用して、機密データにタグを付け、リスク管理を効率化し、リソース割り当てを最適化し、サイバー脅威に対する全体的なレジリエンスを強化します。

- **機密データの発見と特定** – データ分類により、企業は機密データやデジタル資産をその重要性と機密度に基づいて発見し、分類することができます。お客様は、標準搭載の200以上データ分類とAI駆動型アルゴリズムにより、データセットの分析、タグ付け、カテゴリー分け、ラベル付け、分類を行うことで、誤検出を追跡する時間を節約し、解決までの時間を短縮することができます。データ分類は、トリアージと対応の優先順位付けを行い、規制当局への通知ワークフローのガイダンスを行い、規制リスクを最小限に抑えるために、侵害の程度を特定することにも役立ちます。また分類機能は、ガバナンス、リスク、コンプライアンスツールと統合することもでき、対応時間をさらに短縮することができます。
- **バックアップデータの異常を自動監視** – ランサムウェア攻撃、悪意のある内部者、さらにはワイパー攻撃のシグナルとなる異常を監視し、検出します。これらのアラートを業界をリードするSIEM/SOARソリューションと共有し、運用チームと連携します。ランサムウェアとの戦いにおいて、CohesityのAI駆動型学習は、プライマリソースから取り込まれたデータを自動かつ継続的に監視することで、人が見逃している可能性のあるインサイトを提供し、お客様に強みをもたらします。
- **データとセキュリティ体制を総合的に可視化** – Cohesityセキュリティセンターは、データと組織の評判にリスクをもたらすランサムウェアやその他の脅威に対する管理と対応を一元化します。強力なダッシュボードとドリルダウンの機能で、セキュリティ体制の監視、異常と脅威の検知、データの分類、ユーザーアクティビティの追跡、サイバーデータ保管庫を活用することができ、組織のデータを保護し、攻撃を検知し、身代金を支払うことなく迅速に復旧することを可能にします。

1: 識別する

重要なビジネスデータや異常値を識別

“私たちは次世代のデータ管理プラットフォームを必要としていました。Cohesityは使いやすく、大規模でも迅速に復旧でき、サイバー対策も強固で、群を抜いていました”

Nationwide社

2: 防御する

企業データを大規模に保護

データ資産の多様化と大規模化によりデータエステートが複雑化するにつれ、サイバー攻撃やデータ停止が発生した場合、ビジネスに深刻な影響が及ぶ可能性も高くなります。ワークロード (オンプレミス、クラウド、SaaS) を横断する単一の管理プレーンでデータ保護を拡張することで、攻撃の影響を大幅に低減することができます。

- **重要なビジネスデータの隔離** – オンプレミスまたはパブリッククラウド上の別のCohesityクラスターにデータを自動的にレプリケートし、追加のイミュータブルなデータコピーが常に利用できるようにします。
- **攻撃対象領域の削減** – 多くの環境は、断片化されたポイント製品で構成されています。対照的に、Cohesityはすべてのバックアップと災害復旧のコンポーネントを単一のグローバルプラットフォームに統合します。また、データソース全体に対し可変長グローバル重複排除と圧縮を行うことで、攻撃対象領域をさらに削減します。Cohesity CyberScanを使用することで、Tenableのライセンスを持つお客様は、バックアップスナップショットに対して脆弱性スキャンを実行することもでき、本番環境への影響を回避することができます。
- **データエステート全体にデータ保護を拡大** – Cohesityはハイパースケールアーキテクチャで設計されているため、IT管理者はCohesityクラスターを無制限に拡張し、パフォーマンスに影響を与えることなくスナップショットやクローンを無制限に保存することができます。前例のないデータ重複排除により、より多くのデータをより低コストで保存できるだけでなく、スナップショットを任意の時点でインスタンス化し、フォレンジック調査を向上させることができます。

2: 防御する

企業データを大規模に保護

- **多層的なセキュリティアーキテクチャにより、バックアップデータを大規模に保護** – ゼロトラストの原則に基づき、Cohesityはバックアップがランサムウェアの標的となるリスクや、不注意または悪意によるデータ削除のリスクを最小限に抑える多層的なセキュリティアプローチを採用しています。

  - イミュータブルな読み取り専用スナップショット – Cohesityのプラットフォームは、バックアップスナップショットをイミュータブルな状態で保護し、保存することで、サイバー攻撃を阻止することを目的として構築されています。スナップショットは外部アプリケーションからマウントできず、また、承認なしにイミュータブルバックアップスナップショットを変更したり削除したりすることはできません。

  - DataLockポリシー – CohesityのバックアップWORM (Write-once-read-many) 機能は、特定のロールが選択したジョブに対して変更不可能なDataLockポリシーを設定することができます。

  - 多要素認証 (MFA) – Cohesityのバックアップにアクセスする人は、2つの認証方法を用いて認証する必要があります。Cohesityは複数の認証プロバイダーをサポートしており、プライマリサーバがサイバーインシデントの影響を受けた場合でも、強固な認証を維持することができます。

  - データの暗号化 – Cohesityは、転送中および保存中のデータに対し、ソフトウェアベースのFIPS認証を受けた AES-256標準の暗号化機能を備えています。

  - ロールベースのアクセス制御と最小特権 – Cohesityは、ITスタッフが特定の業務に必要なデータへの最小限のアクセス権を各担当者に付与できるようにすることで、不正アクセスのリスクを低減します。

  - 職務の分離 – Cohesityのクォーラム認証を使用すると、ルートレベルまたは重要なシステム変更を行う際に、内部脅威や盗まれた認証情報の利用からデータを保護するために、複数の担当者によって承認することを求めます。

3: 検知する

脅威の検知

サイバー犯罪者は、データ環境の脆弱性を見つけて悪用するためなら手段を選びません。攻撃の影響を最小限に抑えるには、プロアクティブな脅威ハンティング、データの変化やユーザーの行動の継続的な監視、異常の検出が重要です。AIは、人間には不可能なデータの動きを検知することができ、サイバー犯罪者の先手を打つという重要な役割を果たすことができます。

- **脅威のプロアクティブなスキャン** – 組織のデジタルインフラ内の脆弱性と潜在的なセキュリティリスクを系統立てて識別し、評価します。Cohesityは、AI学習ベースのランサムウェア検知エンジンを搭載しており、ランサムウェア攻撃の異常、潜在的な脅威、その他の指標を迅速にスキャンすることで、インテリジェントな脅威対策を提供します。このソリューションには、毎日更新される高度にキュレーションされ管理されたIOC (侵害の痕跡) 脅威フィードのセットが統合されています。10万を超える組み込みの脅威ルール、または独自のYaraルールを活用して、見つけにくいマルウェアを確実に特定します。ネットワーク、システム、アプリケーションを定期的にスキャンすることで、マルウェアの痕跡があるバックアップと、痕跡がないバックアップを容易に絞り込むことができます。

- **パターン、データ変化、ユーザー行動の異常の認識** – 傾向を評価する予測分析を使用して、業務をプロアクティブに監視、モデル化、最適化します。CohesityのAIベースのアルゴリズムは、パターンを確立し、Cohesity内のデータ変化を継続的にスキャンします。Cohesityの異常検知は、お客様のIT管理者とセキュリティ管理者、およびCohesityのサポートチームに通知を送信することで、修復を迅速化します。インシデント対応担当者は、監査ログを容易に検索し、誰がファイルを作成、変更、アクセス、または削除しているかを特定することができます。これにより、セキュリティチームは、ランサムウェアやワイパー攻撃、あるいは悪意のある内部者の可能性を示す行動についてインサイトを得ることができます。

- **迅速な対応** – いったん通知を受け取ったら、お客様のIT管理者とセキュリティ管理者、Cohesityのサポートチームが連携して次のステップを決定します。Cohesityは、バックアップデータの変更率を監視してランサムウェア攻撃の可能性を検知するだけでなく、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を独自に検知し、警告を出します。

3: 検知する

脅威の検知

“大規模なサイバー攻撃は経験したことはありませんが、Cohesityのバックアップは攻撃者によって改ざんされることがなく、バックアップから次のバックアップでなにか疑わしい変更があれば検出できるようデータが継続的にスキャンされていることを知り、大変満足しています。”

カリフォルニア州財務局、エンタープライズアーキテクト、**Chris Dove氏**

4: 対応する

脅威に迅速に対応

ランサムウェア攻撃で脅威者が防御を回避してデータを暗号化した場合、復旧を検討する前に、再攻撃の可能性を低くするため、対応の時間に投資することが重要です。ランサムウェア攻撃を受けたら、1秒たりともコンシューマーに製品やサービスを提供できないということを意味します。幸いなことに、前もって対応策を準備しておくことで、復旧作業を効率化することが可能です。

- **アクション可能なグローバル検索** – すべてのワークロードのデータとメタデータをグローバル検索し、インシデント発生時やランサムウェア攻撃からの復旧時に、単一のUIからシステムの迅速なインスタンス化などの適切なアクションを実行することができます。

- **サイバークリーンルームを設け、影響を評価** – データを隔離し、悪質な行為者からデータを守る必要があります。そうすることで、復旧時にバックアップコピーを利用可能でクリーンに状態にしておくことができ、データ、アプリ、システムを安全にリストアできます。仮想エアギャップを介してデータを隔離することで、フォレンジックを実行し、攻撃で悪用された脆弱性を理解し、感染したデータが本番環境に再導入されないようにするためのクリーンルームを設けることができます。

4: 対応する

脅威に迅速に対応

“Cohesityのビューがなければ、私たちは迅速に調査し、必要なフォレンジック作業を行うことはできませんでした”

SiteOne Landscape Supply社、テクノロジーサービス担当副社長、
David Bannister氏

- **機密データの暴露と規制遵守のためのスキャン** – ML/NLP (機械学習/自然言語処理) を使用して、機密データの漏洩の有無を判断し、適切な修復とコンプライアンスプロセスを確保します。Cohesityは、パッケージ化されたカスタマイズ可能な200を超えるパターンをサポートしており、規制上の義務 (GDPR、HIPAAなど) を理解し、情報漏えいが発生した場合に個人情報、医療情報、財務データを自動的またはプロアクティブに検出、分類し、攻撃中に機密データが暴露されたかどうかを判断します。Cohesityによって検出されたデータの異常は、SOARやITSMシステムにルーティングされ、インシデントの処理と管理を自動化し、規制当局とのやり取りを効率化します。

- **インシデントタイムラインの作成** – Cohesityは、クリーンルーム内で任意の時点にインスタンス化できる無制限のイミュータブルスナップショットを提供します。そこから、データやシステム (Active Directoryなど) に対し差分を簡単に比較して、インシデントのタイムラインを作成し、インシデント対応者が攻撃に至るまでの詳細なフォレンジックを実行できるようにします。

- **脆弱性を修正し、持続的なメカニズムを削除** – クリーンルームでのフォレンジック調査で得られた知識を使用して、脆弱性にパッチを適用し、制御を強化し、不足している予防と検出ルールを策定および展開し、攻撃の成果物を削除します。

5: 復旧する

データを安全に復旧する

最悪の事態が発生し、攻撃者が身代金を要求してきた場合、一番の目標はデータを復旧し、損失を最小限に抑えることです。データ損失はコンプライアンス違反につながるだけでなく、重要な商取引を失うリスクもあるからです。データ保護の常識はリカバリポイントに表れており、ビジネスデータのバックアップスナップショットを頻繁に取得することの重要性が指摘されています。

- **信頼できるクリーンリカバリのための深い可視性** – データのリストア中にサイバー脆弱性を本番環境に再投入しないようにすることで、リスクを軽減します。脆弱性スキャンと詳細なダッシュボードにより、バックアップスナップショットの健全性ステータスとサイバー脆弱性インデックスをチームに表示し、クリーンな時点にリカバリしてビジネスSLAを満たします。
- **対象ワークロードの復旧** – Cohesityは、数百のVMを任意の時点に瞬時にリカバリする機能をサポートしていますが、この機能は、通常、サイバー攻撃の復旧よりも災害復旧のシナリオに適しています。Cohesityは、クリーンなデータとシステムを容易に選択して復旧する柔軟性を提供します。

5: 復旧する

データを安全に復旧する

“私たちの組織は、深刻なランサムウェア攻撃を受け、インフラ全体が機能不全に陥りました。Cohesityを使って、マシンとファイル共有を復旧し、それらがクリーンであることを確認し、アプリケーションをオンラインに戻すことができました。Cohesityのおかげで、文字通り、何百時間もの作業時間を節約し、実際に身代金を支払わなくて済みました。私たちにまだ仕事があり、この地域に機能的な病院があるのは、Cohesityで多くの成功を収めることができたおかげです”

スカイレイクスネットワークシステムアナリスト、**Sam Stewart氏**

スカイレイクスメディカル

サイバーレジリエンス向上のためのパートナーシップ

ネットワークセキュリティから、データ保護、暗号化、脅威検知、インシデント対応、コンプライアンスまで、個人やひとつのベンダーですべてを行うことはできません。サイバー脅威に対抗するには、多様な才能と企業が協力し合うチームが不可欠であり、それがCohesityがデータセキュリティアライアンスを設立した理由です。

Cisco、BigID、Palo Alto Networks、Tenable、Microsoft、CrowdStrike、Qualysなど、業界をリードするパートナーとともに、世界中の大きな組織のサイバーレジリエンスを向上させるために、重要なテクノロジーの連携、ベストプラクティス、ソートリーダーシップを一丸となって提供します。

脆弱性スキャン	ランサムウェアへの自動対応	脅威スキャン	機密データ損失防止	インテリジェントなデータ保護
バックアップデータを使用してリスクエクスポージャーを把握し、攻撃を防ぎ、リスクを通知します。 Tenable社が提供するCohesity CyberScanは、バックアップとスナップショットに対して脆弱性スキャンの実行を可能にします。 - 本番システムに影響を与えることなく潜在的な脆弱性を発見 - アクション可能な修正レコメンデーション機能で攻撃を防止 - バックアップスナップショットの健全性確認により、リカバリ時の脆弱性の再投入を回避	ランサムウェア攻撃への対応と復旧を行います。 Cohesityは、インシデントアラートと関連メタデータをSOCと共有し、復旧と対応のワークフローを開始します。 - Cohesityのインサイトにより、アクティブなランサムウェアの脅威に対するSOCの可視性を強化 - ランサムウェアのインシデントへの関連付け、トリアージ、調査、対応を一元管理	バックアップをスキャンすることで、マルウェアの再感染を防止します。 Cohesityは、既知のマルウェアのマーカーを特定し、リスクのあるファイルやデータを修復するために脅威フィードを取得します。 - マルウェアの痕跡があるバックアップと痕跡がないバックアップを特定 - システム環境を自信をもって迅速にリストア	機密データの意図しない暴露や意図的なデータ流出を防止します。 Cohesityは、機密データを分類し、その情報をパートナーと共有することで、インターネットトラフィックのフィンガープリントと監視を行い、データ損失を防止します。 - Cohesityによる保存データの保護とパートナーによる転送データの保護の連携 - バックアップデータの分類をはるかにシンプルにし、本番システムへの影響を防ぎ、追加のインフラを不要に	保護すべきデータを可視化します。 どのデータが保護されているか、または保護されていないかに関するCohesityからの増強されたインサイトにより、パートナー間でのデータ発見、データ分類、データポスチャーがクラウドをまたがって行えます。 - データの種類を深く理解したバックアップ管理 - データリスクの統合ビュー - 悪意のある攻撃からデータをプロアクティブに保護
tenable	Microsoft, splunk>, CROWDSTRIKE, servicenow, cisco, paloalto	paloalto, CROWDSTRIKE, zscaler, netskope	zscaler, netskope	BigID, sentra, Normalyze, securiti, CYERA

サイバーレジリエンスを向上させるデータセキュリティアライアンスのパートナーシップに関する詳細は、[こちらのホワイトペーパーをお読みください](#)。

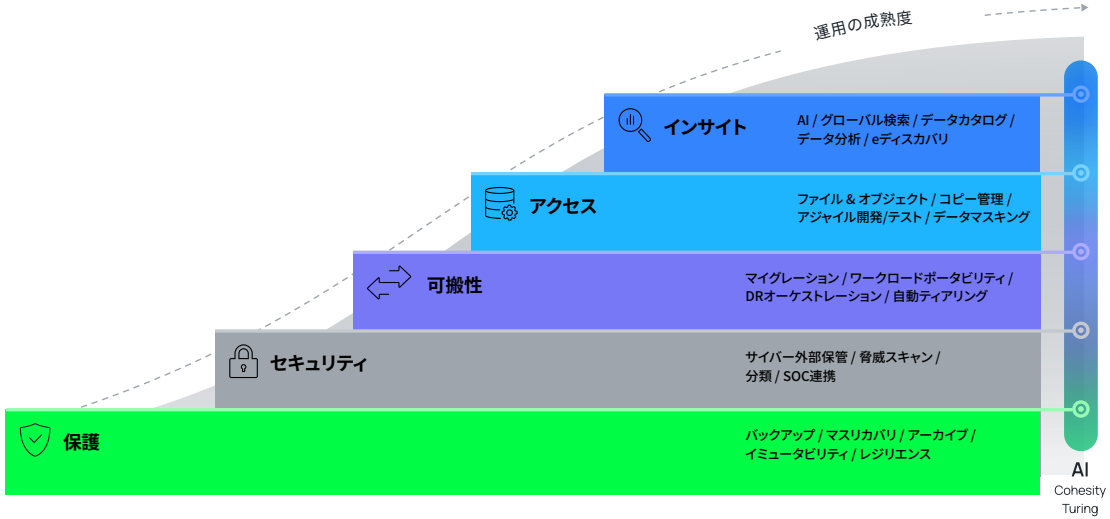
モダンサイバーレジリエンスの始め方

マルチクラウド、ハイブリッド環境、ランサムウェア攻撃の脅威が高まる中、今日の企業は、保護したデータ資産全体の可視化を促進し、ITチームとセキュリティチーム間のコラボレーションを効率化するモダンソリューションを必要としています。

サイバーレジリエンスの基礎となるレイヤーはデータ保護です。堅牢なバックアップとリカバリの機能は、予期せぬ障害から組織をスムーズに回復させる能力に対する自信を与えてくれます。

そこから、組織はデータセキュリティへと進むべきです。この段階では、組織はデータレジリエンスシステムを、追加のサイバーレジリエンス機能やその他の既存のセキュリティ投資と統合し、サイバー攻撃やその他の脅威からのリスクをさらに低減します。

最新のデータセキュリティとデータ管理を大規模に導入するための詳細な計画を立てている組織の方は、Cohesityのリソースやホワイトペーパーをご覧ください:



モダンデータセキュリティとデータ管理のためのエグゼクティブガイド

ホワイトペーパーを入手する

サイバーサイバーレジリエンス戦略を成熟させる準備はできていますか？

データセキュリティソリューションを見つける

COHESITY

www.cohesity.com/jp

6100008-005-JP 11-2023