COHESITY
RESILIENCE EVERYWHERE

ランサムウェア時代の サイバーレジリエンス

Cohesityが、NIST Cybersecurity Framework 2.0との整合性を保ちながら、組織がサイバー攻撃に耐え、復旧するのを支援する方法

目次

データレジリエンスから サイバーレジリエンスに

自然災害は、事業運営に深刻な脅威をもたらします。落雷、ハリケーン、竜巻、洪水は深刻な被害をもたらし、ビジネスを停止させる可能性があります。このような状況では、データレジリエンス戦略により、ハードウェア障害、誤削除か、自然災害が発生した場合でも、データの完全性とアクセス性を維持できます。

しかし、これらのイベントは、継続的かつ意図的に貴社を積極的に標的としているわけではありません。

これをサイバー脅威と比較してみます。脅威者は決して手を緩めることなく、新たなツールを駆使してデータを人質に取り、事業を停止に追い込もうとします。攻撃経路は多岐にわたり、巧妙に検知を回避することもよくあります。また、脆弱性、侵害されたアカウント、その他の攻撃の痕跡を自社環境に再び持ち込んでしまうリスクも蔓延しています。従来の事業継続と災害復旧のシナリオでは、通常、根本原因が明らかであるのに対し、サイバー脅威への対応では、これらの原因を発見し、再発を防止するための是正策を推進するために調査が必要です。

さらに、ランサムウェア攻撃では、セキュリティインフラストラクチャと主要な証拠がインシデントの影響を受け、製品とサービスを提供する能力に影響が及ぶ可能性があります。

サイバーレジリエンスの高いビジネスを構築するには、ITとセキュリティのリーダーは、自然災害か技術的障害による通常の機能停止に対応する際に使用するプロセスよりも、より堅牢、ダイナミックで、協調的なプロセスを必要としています。サイバーレジリエンスは、データのレジリエンス慣行に基づいて構築され、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を含みます。

今日のサイバー脅威に対処するには、保護され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間のコラボレーションを効率化する最新のソリューションが必要です。

Cohesityの最新のAIを活用したデータセキュリティソリューションは、組織がサイバー対策の強化、インシデント対応の迅速化、高速でセキュアな復旧を実現するのを可能にします。

COHESITYでは、以下のようなことが可能です。

- あらゆるデータを保護する
- データが常に復旧可能であることを保証する
- バックアップデータの脆弱性と脅威を可視化する
- 攻撃に迅速かつ効果的に対応し、従来の防御をすり抜ける脅威を追跡する
- システムとデータを迅速かつ安全に復旧する

その結果、サイバー攻撃への備え、耐性、対応力、復旧力を高めた、よりレジリエンスの高い事業運営が可能になります。

自信と能力のパラドックス

78%の企業が、自社のサイバーレジリエンス戦略に自信を持っています[1]。この自信が具体的な能力に裏付けられているのであれば、おおむねよい兆候といえます。しかしデータは、戦略上の意図と実際の対応能力との間に乖離があることを示しています。

98%の企業は、攻撃を受けてから1日以内にデータを復旧し、事業プロセスをリストアしたいと考えています[2]。

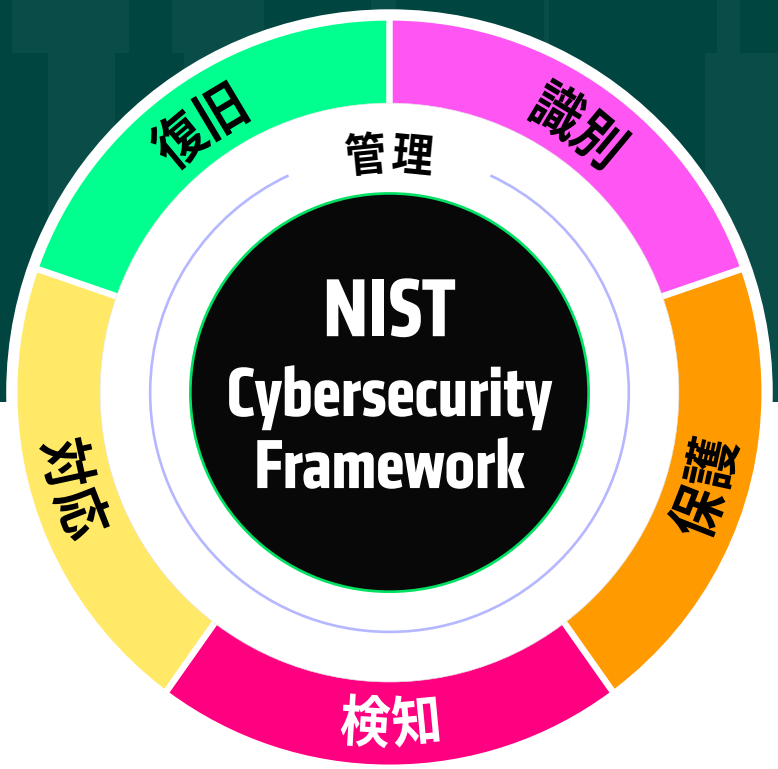
しかし、**2%**の企業しか、これを達成できていません[3]。

幸いなことに、Cohesity は、プロセスとツールを備えた実績のあるプレイブックを提供し、世界中のお客様が迅速に業務を再開し、攻撃の影響を軽減できるように支援しています。

[1-3] 2024年Cohesityグローバルサイバーレジリエンスレポート

サイバーレジリエントなビジネスを構築する 6つの鍵

Cohesityのデータセキュリティソリューションは、組織がリスクをより深く理解し、管理し、低減するとともに、NIST Cybersecurity Frameworkが掲げる「管理、識別、保護、検知、対応、復旧」という主要機能に沿ってサイバーレジリエンスを強化できるように支援します。



管理
- バックアップデータを分類し、規制要件を把握する
- 第三者データに関するサイバー保険の枠組みその他の契約上の義務に対応できるように支援する

識別
- 脆弱なシステムに負荷や影響をかけることなく、脆弱性をスキャンする
- バックアップされていない重要なシステムを識別する
- 将来のインシデント対応とBC/DRの取り組みを改善する
- 組織のサイバーレジリエンスプログラムにおける改善領域を識別する

保護
- エンタープライズ規模でデータを保護する
- バックアップを攻撃から保護する
- バックアップとリストアをテストする

検知
- ランサムウェアによる暗号化、ワイパー攻撃、悪意のある内部者を検知する
- 侵害の痕跡を積極的に探索し、回避技術に対する耐性をつける
- 相関分析のために、セキュリティ検知結果をSOCツールに送信する
- より多くのフォレンジックアーティファクトを取得し、EDR/XDRシグナルに基づいて増分スナップショットをトリガーする
- NASサーバー内のマルウェアを識別する

対応
- 迅速な対応と安全な復旧を実現するために、Cohesity CERT（Cyber Event Response Team）を活用する
- 対応ツールとADを信頼できる状態にリストアし、迅速にアクセスできるようにする
- 対応と復旧のためのクリーンルームを迅速に構築する
- アーティファクトをパッシブに探索し、追加で影響を受けたシステムを識別する
- 過去のファイルシステムをフォレンジック調査する
- 攻撃で悪用された過去の脆弱性を把握する
- 規制当局、パートナーに加え、影響を受けたデータ主体への規制上、コンプライアンス上の通知義務への対応を支援する

復旧
- システムとデータを復旧する際に、脅威を軽減できる状態を確保する

1.

管理規制要件を把握してリスクに対処するためのバックアップデータ

今日のデータ環境は、物であふれ返ったガレージのように無秩序に広がっており、機密データを見つけて適切に保護することがますます困難になっています。こうした可視性の欠如により、データ漏えいと規制違反のリスクが高まります。

このリスクを管理するために、組織は法的要件と規制上の要件（HIPAA、CCPA、GDPRなど）を満たすだけでなく、効果的なサイバーセキュリティガバナンスを通じて、強力な内部統制を示す必要があります。こうした統制は、もはやコンプライアンス対応だけではなく、サイバーセキュリティ保険の加入に不可欠なものになってきています。

サイバー攻撃の発生頻度と被害の深刻さが増す中、サイバー保険は重要なリスク移転戦略となっています。インシデント発生後のデータ復旧費用、訴訟費用、その他の損害などの経済的損失を補償するのに役立ちます。しかし保険会社は、保険の新規契約や更新の前に、強固なデータ保護体制とセキュリティ統制が整っていることの証明を顧客に求めるようになっています。

当社は、これらの要件を先回りして対応できるよう、企業による次の取り組みを支援します。

機密データを見つけて分類します。当社の無制限かつイミュータブルなバックアップスナップショットを使用して、環境全体の機密データを検出して分類します。当社の内蔵データ分類エンジンは、数百種類の分類子とAI駆動型アルゴリズムを用いて、規制対象情報と高リスク情報を識別してラベル付けし、デジタル資産のインベントリと適切なセキュリティポリシーの適用を支援します。

第三者データに関するサイバー保険の要件その他の契約上の義務に対応できるように支援します。当社のプラットフォームは、以下のベストプラクティスの統制を実装することで、保険会社や規制当局の高まる期待に応えるのに役立ちます。

- 本番ネットワークから分離された隔離型バックアップ環境
- 専用のクラウドバックアップサービス
- 送信中のデータも保管中のデータも暗号化
- イミュータブルなバックアップスナップショット
- 分離された認証情報によるロールベースアクセス
- 内部アクセスと外部アクセスの両方に対するMFAの強制適用
- リストアの前にバックアップの完全性を検証し、マルウェアを含まないことを保証

2.

識別サイバーレジリエンスリスク

サイバーセキュリティリスクを効果的に管理するには、バックアップシステムなど、IT環境全体の脆弱性を明確に理解する必要があります。また、データ資産をその分類に応じて優先的に保護し、セキュリティテスト、訓練、過去のインシデント対応と復旧の取り組みから得られた教訓を通じて、継続的に改善していくことも含まれます。

CyberScan
Powered by tenable

脆弱なシステムに負荷や影響をかけることなく、脆弱性をスキャン

Tenableを搭載したCohesity CyberScanを使用して、バックアップスナップショットの脆弱性スキャンを実行し、本番システムへの影響を回避します。

バックアップされていない重要なシステムを識別する

Cohesityを、任意のデータセキュリティ体制管理（DSPM）ベンダーと統合することは、潜在的なサイバーレジリエンスリスクを明らかにするための強力な方法です。DSPMソリューションは、さまざまなクラウド プラットフォームにわたって、既知のデータと忘れ去られたデータの リポジトリの両方を可視化し、データを分類して機密情報を識別し、露出のリスクを判断します。

機密データの多くは、Cohesityデータクラウドと既存のバックアップポリシーによってすでに保護されている可能性がありますが、なお大きなギャップが残っていることが少なくありません。そこで重要になるのが、DSPMとの統合です。

DSPMからのインサイトをCohesityと組み合わせることで、バックアップされていない重要なシステムとデータを特定し、バックアップポリシーを迅速に拡張してカバーすることで、セキュリティを強化し、リスクを軽減できます。

その他の主な運用上のメリットには、次のようなものがあります。

- Cohesityがバックアップするデータストア内のデータの重要度に基づいて、バックアップと保持の頻度を最適化
- データのビジネス上の重要性に基づいた、データの優先的なリストア
- 影響を受けたデータの「ジャストインタイム」分析によるインシデント対応の効率化（これについては、レスポンス機能でさらに詳しく説明します）

DSPMとCohesityのAI搭載データセキュリティプラットフォームを組み合わせることで、マルチクラウド環境全体にわたるセキュリティ体制を改善できます。

2.

識別サイバーレジリエンスリスク

将来のインシデント対応やBC/DRの取り組みを特定する

Destructive Cyberattack Resilience Maturity Model（DCARMM）を用いて、組織の現在の対応力と復旧力を評価し、業界のベストプラクティスに向けた道筋を描きます。

このモデルは、Cohesityが開発し、SANSの6ステップ・インシデント対応プロセス、RE&CT、MITRE D3FEND、NIST SP 800-61など、主要フレームワークに準拠しているので、組織による次の取り組みが可能になります。

- 破壊的なサイバー攻撃に対する準備状況を評価する
- 同業他社か地域基準に対してレジリエンス成熟度をベンチマークする
- ギャップを特定し、継続的な改善のためのロードマップを構築する

このモデルは、サイバーレジリエンス体制を強化し、人、プロセス、テクノロジーへの投資を導くための戦略的ツールとして使用できます。

第三者評価に投資することで、自社のサイバーレジリエンスプログラムの改善が必要な分野を特定する

Cohesity CERT（Cyber Event Response Team）のサイバーレジリエンスコンサルティングサービスは、次のインシデントが発生する前にサイバーレジリエンスを強化するため、専門家主導による積極的な支援を提供しています。DCARMMに基づく徹底したレジリエンス評価から、カスタマイズされたアクションプランまで、CERTはギャップの特定、リスクの低減、持続的な防御体制の構築を支援します。

3.

保護大規模なエンタープライズデータ

データ資産の規模拡大と多様化によってデータ環境がますます複雑になるにつれ、サイバー攻撃やデータ停止による事業に深刻な影響が及ぶリスクも高まっています。

オンプレミス、クラウド、SaaS環境にまたがるすべてのデータソースを、単一の安全なプラットフォームでバックアップすることで、潜在的な攻撃の影響を大幅に抑えながら、データ保護を拡張できます。

攻撃対象領域を削減する

多くの環境は、断片的なポイント製品で構築されています。これとは対照的に、Cohesityは、すべてのバックアップと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。これには、データソース全体にわたるグローバルな可変長重複排除と圧縮が含まれており、これで、攻撃対象領域をさらに縮小できます。

データ資産全体でデータ保護を拡張する

Cohesity Data Cloudは、ハイパースケールアーキテクチャに基づいて設計されているため、IT管理者は、パフォーマンスに影響を与えることなく、Cohesityクラスターを無制限に拡張し、スナップショットとクローンを無制限に保存できます。かつてないレベルのデータ重複排除により、より低コストでより多くのデータを保存できるだけでなく、フォレンジック調査をサポートするために任意の時点のスナップショットを作成することもできます。

3.

保護大規模なエンタープライズデータ

バックアップを攻撃から保護する

Cohesityは、ゼロトラストの原則に基づき、バックアップを標的とするランサムウェアのリスクと、データの不注意か悪意のある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状態のスナップショット – Cohesity Data Cloud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存することでサイバー攻撃を阻止できるように、専用に設計されています。スナップショットは外部アプリケーション向けにマウントされず、イミュータブルなバックアップスナップショットの変更または削除は、承認なしでは行えないようになっています。
- DataLockポリシー – バックアップ向けのwrite-once-read-many（WORM）機能で、特定のロールが選択したジョブに対して変更不可のDataLockポリシーを設定できます。
- 多要素認証（MFA） – Cohesityのバックアップにアクセスするすべての人は、2つの認証要素を用いて認証を受ける必要があります。複数の認証プロバイダーをサポートしているので、プライマリサーバーがサイバーインシデントの影響を受けた場合でも、強力な認証を維持できます。
- データ暗号化 – Cohesityは、転送中と保存中のデータに対して、ソフトウェアベースのFIPS認証済みAES-256標準暗号化を提供します。
- ロールベースのアクセス制御と最小権限 – Cohesityでは、IT担当者が各ユーザーに対して、特定の業務に必要な最小限のデータアクセス権のみを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 Quorumでは、内部脅威と認証情報の窃取からデータを保護するため、rootレベルか重要なシステム変更は、2名以上の承認を得なければなりません。

重要なビジネスデータの分離

オンプレミスかパブリッククラウド上の別のイミュータブルなCohesityクラスターにデータを自動的にレプリケーションすることで、データの改ざん不能コピーを追加で常に利用可能な状態にしておくことができます。

バックアップとリストアをテストする

サイバー復旧オーケストレーションを使用することで、復旧ワークフローを自動化し、非本番環境での厳格なテストを可能にするカスタマイズ可能なブループリントを生成できます。これで、組織はサイバーインシデントへの備えを強化し、復旧を合理化して、ダウンタイムとデータ損失を削減できます。

4.

検知潜在的なサイバー攻撃と侵害

サイバー犯罪者は、データ環境内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。バックアップデータかユーザーの行動における異常な変化を早期に検知することは、攻撃の影響を最小限に抑えるために不可欠です。

そこでAIが重要な役割を果たします。AIは、人間が見逃すかもしれない微細なデータアクティビティパターンを識別します。また、EDR/XDRツールによってランサムウェア攻撃の開始が検知された時に、重要なデータのバックアップスナップショットを自動的に取得することで、データ損失を低減し、復旧を迅速化できます。

ランサムウェアによる暗号化、ワイパー攻撃、悪意のある内部者を検知する

予測分析を使用して運用を積極的に監視、モデル化、最適化し、トレンドを評価します。当社のAIベースのアルゴリズムは、パターンを確立し、時間の経過に沿ってスナップショット全体にわたるデータの異常を継続的にスキャンします。

異常が検知されると、IT管理者とCohesityサポートチームの両方に通知が送られるため、修復対応を迅速に進めることができます。

これで、セキュリティチームは、ランサムウェアかワイパー攻撃、さらには悪意のある内部者の存在を示す可能性のある挙動について、インサイトを得ることができます。

これらのアラートは、イベント相関ツール（SIEMなど）を使用してセキュリティオペレーションセンターと共有することもできます。

バックアップデータ内の脅威を積極的に調査する

ランサムウェアなどの攻撃は、マルウェアを隠すために不正な手口を使います。Cohesity threat huntingは、ランサムウェアやその他のサイバー攻撃の最新の亜種を特定するAI駆動の脅威検知を活用し、潜伏する巧妙な脅威の発見を支援します。

当社の行動パターンの広範なライブラリでは、最新の脅威を反映して頻繁に更新されます。

当社は、CrowdStrike Falcon Adversary Intelligenceなどの商用脅威インテリジェンスフィードもサポートしており、他のサードパーティソースからのYARA形式のIOCも取り込むことができます。

4.

検知潜在的なサイバー攻撃と侵害

相関分析のために、セキュリティ検知結果をSOCツールに送信する

IOC、バックアップデータの変更における異常、機密データアラートなどの重要なセキュリティ検知結果をSOCツール（SIEM、SOARなど）に送信し、脅威の迅速な検知と対応を支援します。

Cohesityは、CrowdStrike、Splunk、Microsoftなどの主要なプラットフォームと統合されており、テレメトリをシームレスに共有するため、SOCはCohesityから得られるインサイトを集約、分析し、インフラストラクチャ全体の大量のログデータと関連付けることができます。

その結果、可視性を高め、潜在的なランサムウェアやその他のサイバー脅威の兆候をより迅速に検知できる、統合的なリアルタイムビューが実現します。

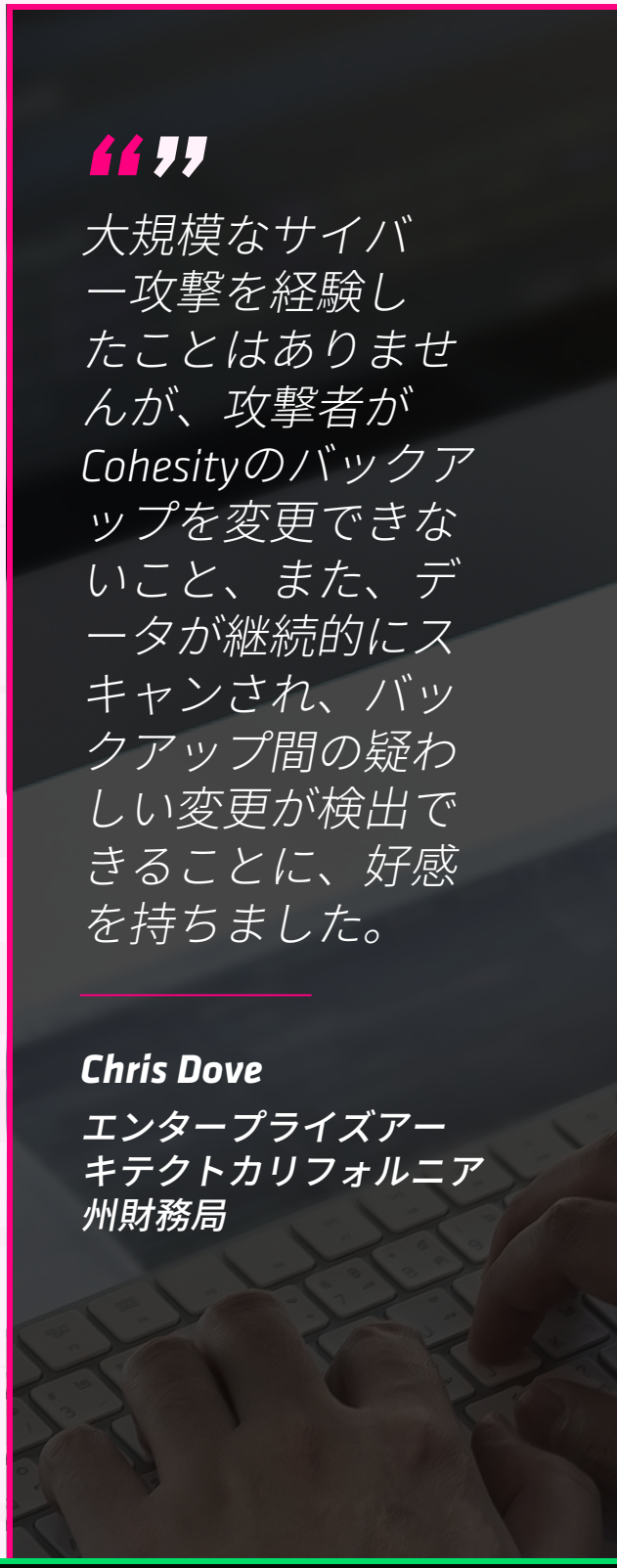
EDR/XDR信号に基づいて、より多くのフォレンジックアーティファクトを取得し、増分スナップショットをトリガーする

Cohesity Data CloudとCisco XDRの連携によりCisco XDRがランサムウェア攻撃を検知した瞬間に重要なデータのバックアップを自動化できるため、目標復旧時点（RPO）を短縮し、事業中断を最小限に抑えられます。

また、これらのバックアップスナップショットにより、インシデント対応担当者はファイルシステムの変更について、より詳細な状況を把握できるため、フォレンジック調査をより迅速かつ効果的に進められます。

NASサーバー内のマルウェアを特定する

Cohesityは、バックアップデータの変更率を監視して潜在的なランサムウェア攻撃を検出するほか、非構造化ファイルとオブジェクトデータ内のファイルレベルの異常を独自の方法で検出してアラートを送信します。



“大規模なサイバー攻撃を経験したことはありませんが、攻撃者がCohesityのバックアップを変更できないこと、また、データが継続的にスキャンされ、バックアップ間の疑わしい変更が検出できることに、好感を持ちました。”

Chris Dove
エンタープライズアーキテクトカリフォルニア州財務局

5.

対応サイバーインシデントに迅速に

サイバーインシデントが検出されたら、組織は迅速に行動し、インシデントを封じ込め、その影響範囲を調査し、安全な復旧を可能にするためのリスク軽減策を講じる必要があります。

ランサムウェアとワイパー攻撃など影響の大きいインシデントは、顧客への製品・サービス提供に必要なシステムだけでなく、それらを管理するために不可欠な社内ITシステムにも支障を来すおそれがあります。こうした状況では、標準的なデータ侵害対応プロトコルを超えた、別種の、より体系的なワークフローが求められます。

脅威の調査と軽減を行わずに復旧を急ぐと、根底にある脆弱性が残る可能性があり、再感染とダウンタイムの長期化を招くおそれがあります。

このような攻撃から安全に復旧するには、インシデントがどのように発生したのかを理解し、その根本原因をどのように是正するかを把握する必要があります。これこそが、すべてのベストプラクティスに基づくサイバーセキュリティインシデント対応フレームワークの本質です。

1. 迅速かつ専門的な支援を受けるために、インシデント対応プロセスの早期段階で **Cohesity CERT をご活用**ください。当社のチームは、脅威の封じ込め、ダウンタイムの最小化、バックアップインフラストラクチャのフォレンジック分析の支援、規制コンプライアンスと侵害通知要件への対応支援、本番環境への安全な復旧の促進を支援します。

2. **対応ツールを信頼できる状態に復元し、迅速なアクセスを提供します。**サイバー攻撃を受けて業務が停止したときには、一刻の猶予もありません。迅速な対応が極めて重要、**digital jump bag**™があれば、直ちに行動に移せます。

Digital Jump Bagは、理想的にはインシデント発生前に準備しておくべきものであり、効果的な対応を開始するために必要なツール、ソフトウェア、構成ファイルに加え、各種文書に迅速にアクセスできる、保護された信頼性の高いリポジトリです。攻撃者の手が及ばない隔離されたイミュータブルな保管場所に保存されることは、Cohesity Clean Roomソリューション全体の基盤となり、インシデント対応の重要な段階をサポートし、セキュアで信頼性の高い復旧が可能になります。

3. **クリーンなActive Directory (AD) インフラストラクチャを復元します。**ADほどビジネスクリティカルで、標的にされやすいシステムはほとんどありません。インシデント対応の開始時には、他の対応ツールをオンラインに戻す前に、かつADを本番環境に復旧する前に、AD 環境を徹底的に調査してクリーンな状態にすることが不可欠です。このステップをスキップすると、攻撃者が再侵入する大きな隙を与えてしまい、復旧作業を損ない、業務の混乱を長引かせます。

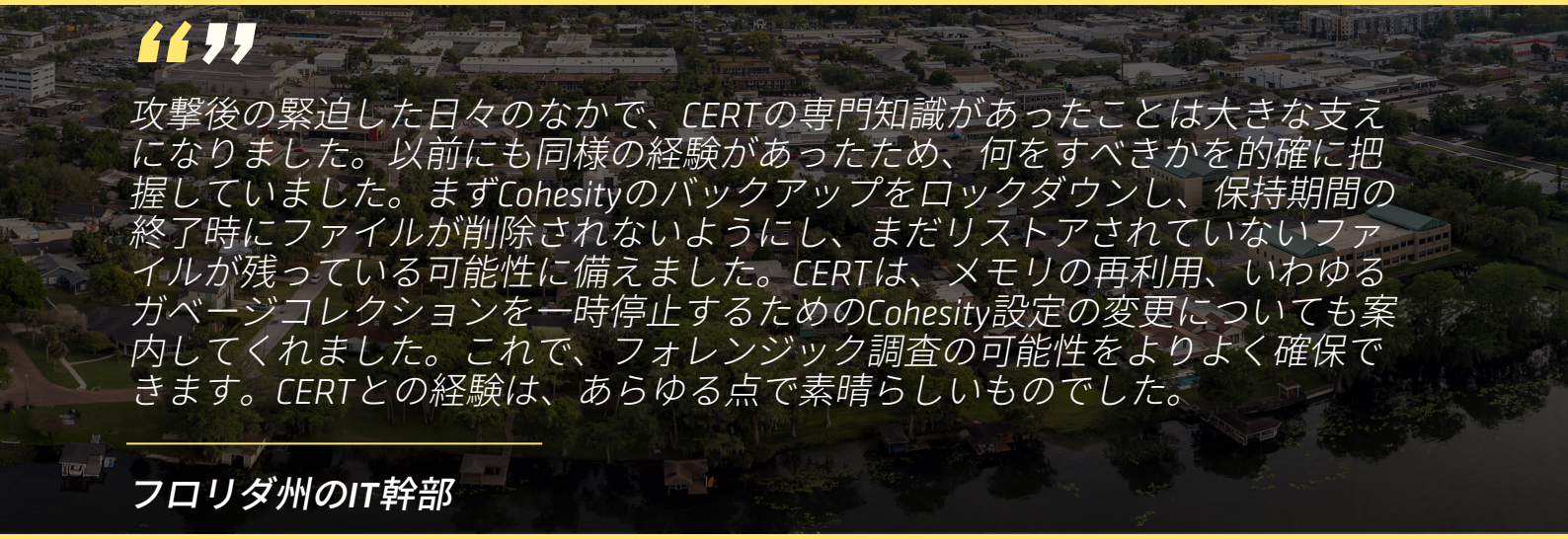
Semperisを搭載したCohesity Identity Resilienceを使用すると、ADを信頼できる状態へ最大90%速くリストアできます。

5.

対応サイバーインシデントに迅速に

4. **対応と復旧のためのクリーンルームを迅速に構築します。**クリーンルームは、アナリストと調査員がフォレンジック調査を実施し、攻撃で悪用された脆弱性を把握し、感染したデータが本番環境に再び持ち込まれないようにするための信頼できる環境として実装する必要があります。

5. **追加で影響を受けたシステムを特定するために、アーティファクトをパッシブに探索します。**当社の脅威ハンティング機能は、封じ込めのためにシステムが隔離されている場合でも、組織のインフラストラクチャ全体でIOCを検出します。この機能は、従来のエンドポイントセキュリティツールによる検知を無効化したり遅らせたりする一般的な防御回避手法に対しても、強い耐性を持っています。



攻撃後の緊迫した日々のなかで、CERTの専門知識があったことは大きな支えになりました。以前にも同様の経験があったため、何をすべきかを的確に把握していました。まずCohesityのバックアップをロックダウンし、保持期間の終了時にファイルが削除されないようにし、まだリストアされていないファイルが残っている可能性に備えました。CERTは、メモリの再利用、いわゆるガベージコレクションを一時停止するためのCohesity設定の変更についても案内してくれました。これで、フォレンジック調査の可能性をよりよく確保できます。CERTとの経験は、あらゆる点で素晴らしいものでした。

フロリダ州のIT幹部

6. **過去のファイルシステムをフォレンジック調査します。**当社のデータ保護により、UIとAPIを通じて改ざん不可能なスナップショットの完全な時系列にアクセスできるため、対応担当者は、保持されたバックアップデータ全体にわたり、ファイルレベルの詳細なフォレンジック調査を実施できます。

7. **攻撃で悪用された過去の脆弱性を把握します。**Cohesity CyberScanソリューションを使用すると、バックアップスナップショットを既知の脆弱性についてスキャンできます。これで、たとえシステムが封じ込めによってアクセス不能になっているか、ワイプされているか、侵入後に攻撃者自身によってパッチが適用されていた場合であっても、セキュリティチームは、攻撃時点で存在していた脆弱性を特定することが可能になります。

8. **規制当局、パートナーに加え、影響を受けたデータ主体への規制上、コンプライアンス上の通知義務への対応を支援します。**当社のAI駆動型データ分類は、バックアップをスキャンして機密データと規制対象データを識別し、重要なデータストアが暗号化されるか消去されるような破壊的なサイバー攻撃でも、組織が規制要件を満たせるように支援します。また、Cohesity Clean Roomソリューションの一環として、インシデント管理に必要な通信機能の復元も支援します。関係者への通知に使うコミュニケーションテンプレートは、すぐにアクセスできるように、デジタルジャンプバッグに保管しておくことができます。

6.

復旧システムとデータを安全に

インシデント対応の復旧フェーズでは、脅威を徹底的に排除し、再感染を防ぎ、将来同様の攻撃が発生する可能性を低減する必要があります。

Cohesity Clean Roomソリューションにより、既存のシステムの復旧とクリーニング、ゼロからの再構築など、組織に適した復旧戦略を柔軟に選択できます。

高速なボリューム復旧をサポートしており、脅威の除去対策を講じる前に、ファイルシステム全体を迅速に復旧できます。また、信頼できるソフトウェアイメージや既知の正常な構成からの再構築も迅速に行うことができます。

私たちの組織は、致命的なランサムウェア攻撃を受け、事実上インフラ全体が機能不全に陥りました。Cohesityのおかげで、マシンとファイル共有を復旧し、クリーンなデータであることを確認してから、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。

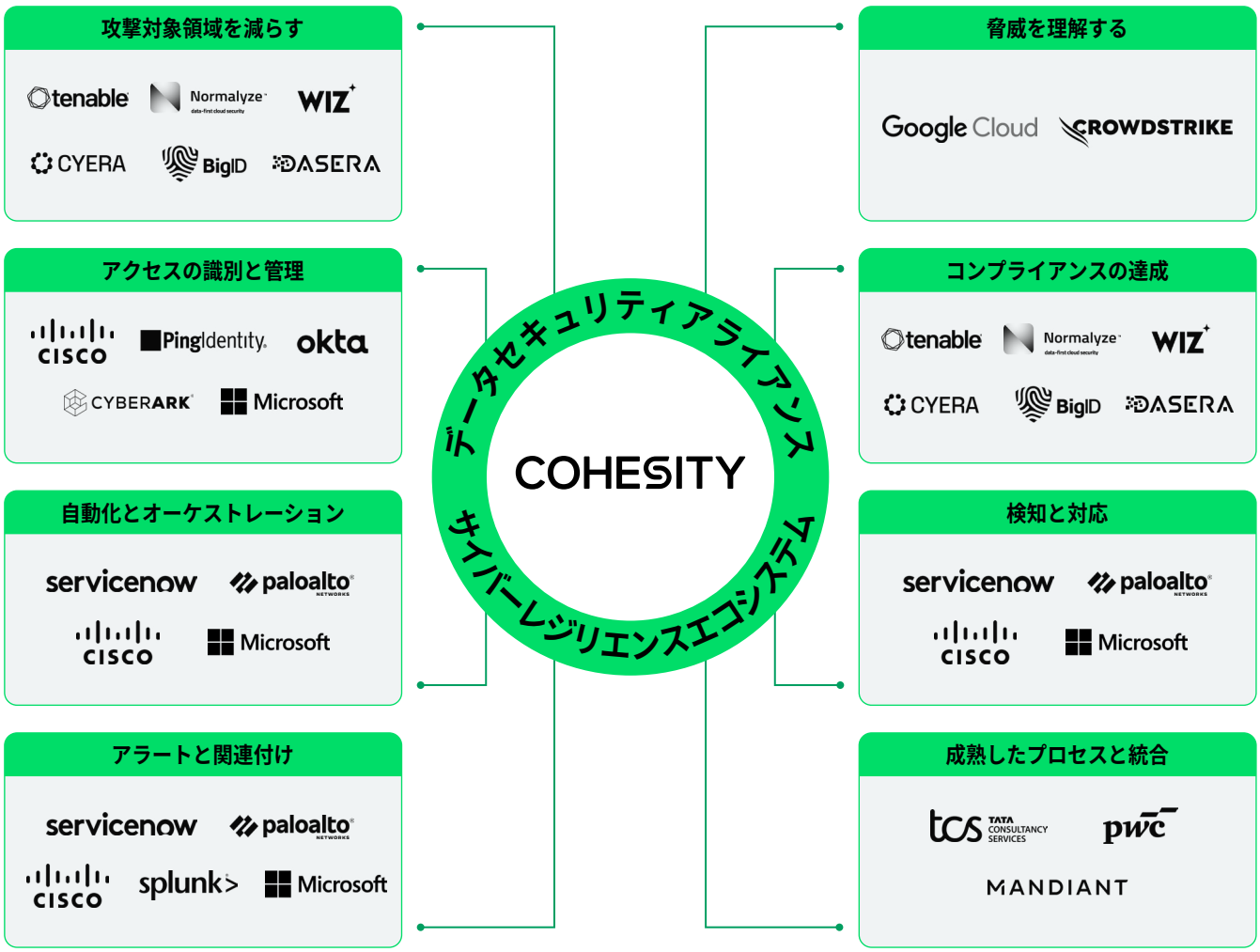
Cohesityのおかげで、文字通り何百時間もの作業時間を節約でき、身代金の支払いを回避することができました。私たちが全員まだ仕事を持ち、コミュニティに機能的な病院があるのは、Cohesityで多くの成功を収めることができたおかげです。

Sam Stewart
Sky Lakes Medical Center
ネットワークシステムアナリスト

パートナーシップを通じたサイバーレジリエンスの強化

サイバーレジリエンスはチームスポーツです。単一のベンダーのソリューションだけでインシデントの調査と是正をすべて完結させることはできません。

そのため、当社はデータセキュリティアライアンスを設立しました。既存のツールを活用しながら、サイバー復旧リスクを低減し、セキュリティオペレーションセンターの効率性を高め、より多くのデータ資産の保護に役立つ、主要なセキュリティ企業とサイバー復旧企業のエコシステムです。

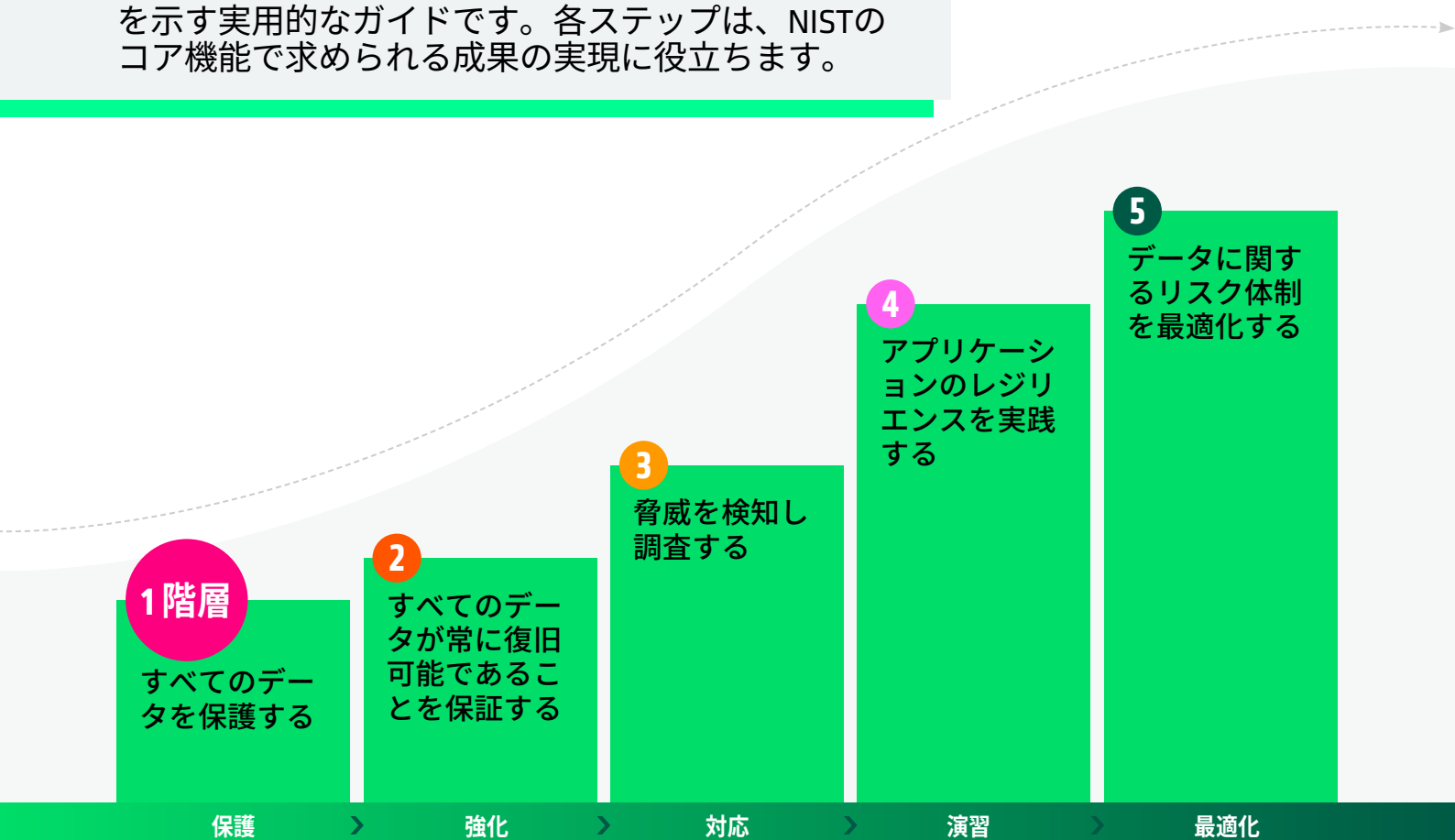


組織の次のステップ...

サイバーレジリエンスの構築に向けたCohesityの5つのステップ

サイバーレジリエンスの高いビジネスを構築するための 6 つの鍵と、NIST サイバーセキュリティフレームワーク（CSF）の各段階をどのようにサポートするかについて学びました。今こそ、これらの洞察を実行に移すときです。

導入を支援するために、**5ステップのサイバーレジリエンスプレイブック**を作成し、サイバー対応と復旧に関する業界のベストプラクティスと調和させました。これは、Cohesity Data Cloudとサービスを使用して、具体的で反復可能なアクションを実装する方法を示す実用的なガイドです。各ステップは、NISTのコア機能で求められる成果の実現に役立ちます。



Cohesityのサイバーレジリエンスへの *5つのステップ*

1. あらゆるデータを保護

NIST CSFとの整合性：*保護*

エンタープライズ規模で、データが存在するあらゆる場所でデータを保護することで、レジリエンスを構築します。Cohesity Data Cloudは、VM、SaaSアプリ、データベース、NAS環境など、**1,000以上のデータソース**をサポートし、グローバルな重複排除と圧縮によってコストとリスクを低減します。

このアプローチは、IT部門のストレージコストを抑えるとともに、セキュリティチームの攻撃対象領域を縮小します。これらは、より強力な保護機能を実現する2つの重要な要素です。

2. データが復旧可能であることを保証

NIST CSFとの整合性：*保護と復旧*

保護の強力さは、復旧できる能力が伴う場合しか意味を持ちません。

- **プラットフォームの強化：**MFA、ロールベースのアクセス制御、Quorumなどの防御機能を有効にして、職務の分離を徹底し、内部者リスクを最小限に抑えます。
- **重要なデータの分離：** Cohesityのサイバーボールトを使用して、セキュアかつ復旧可能なコピーを作成します。これは、Cohesityが管理するクラウドボールトとしても、セルフマネージドソリューションとしても利用できます。

これらの対策により、いざというときに信頼できるコピーをリストアできるようになります。

3. 脅威を検知して調査

NIST CSFとの整合性：*識別と検知*

レジリエンスは、早期検知にかかっています。Cohesityでは、以下のようなことが可能です。

- データ保護のギャップを含む脆弱性を識別します。
- ランサムウェアやマルウェアの兆候がないか、継続的にバックアップをスキャンします。
- バックアップデータ内の特定の脅威を探索することで、回避手法の影響を受けない環境を構築します。
- SIEM/SOARツールに検出結果を送信し、SOCにおける迅速な相関分析と対応を実現します。

成果：脅威はより早く検知され、対応チームはより迅速に行動できます。

4. アプリケーションのレジリエンスを実践

NIST CSFとの整合性：*対応と復旧*

最終ステップをご覧ください >

攻撃を受けてから復旧計画を試すのでは遅すぎます。

- **定期的にリハーサルを実施：** 攻撃を受けている状況を想定して復旧計画を実践し、復旧プロセスと対応準備態勢を検証する。
- **復旧を自動化：**当社プラットフォームの復旧オーケストレーションを使用してワークフローを合理化し、インシデント後のシステム復旧を加速できます。

このステップにより、手作業でストレスの多い復旧プロセスが、繰り返し可能で十分に訓練されたプレイブックに変わります。

Cohesityのサイバーレジリエンスへの *5つのステップ*

5. データに関するリスク体制の最適化

NIST CSFとの整合性：*管理、識別、対応*

- データセキュリティガバナンスを強化：Cohesityのデータと当社のデータ分類機能を使用して、保有しているデータを把握し、そのリスクレベルを評価し、適切なセキュリティコントロールを適用します。
- バックアップされていない重要なシステムを識別：バックアップを含む資産全体の機密データを特定し、それが適切に保護されていることを確実にします。お好みのデータセキュリティ体制管理（DSPM）ツールと当社のプラットフォームの機能を組み合わせることで、このプロセスを合理化できます。
- インシデントによる影響を評価：侵害が発生した場合、特に重要なデータストアが暗号化されるか消去されている場合、バックアップを使用して、どの機密データと規制対象データが漏洩した可能性があるかを迅速に評価できるため、規制当局、パートナー、影響を受けたデータ主体に通知する規制上、コンプライアンス上の義務を果たすことができます。

実際のサイバーレジリエンスを確認

さまざまな業界の7つの組織が、ランサムウェア攻撃から迅速かつセキュアに復旧した方法をご紹介します。

EBOOKを入手する

すべてを統合する

当社の5ステップサイバーレジリエンスプレイブックでは、NIST CSFを運用に組み込むための明確で実行可能な道筋が示されています。

Cohesityの最新のデータセキュリティプラットフォームを使用すると、保護と復旧だけでなく、サイバーレジリエンス体制を継続的に最適化することもできます。

当社のサイバーレジリエンスソリューションについて詳しくは、こちらをご覧ください

COHESITY
RESILIENCE EVERYWHERE

6100008-006-JA 11-2025