COHESITY

ホワイトペーパー

復旧のその先へ:バックアップデータを使用してサイバーレジリエンスを強化するためのCISOガイド

目次

エグゼクティブサマリー

サイバー攻撃がますます頻繁かつ深刻になる中で、最高情報セキュリティ責任者 (CISO) は、防止だけに頼る考え方から、より広範なサイバーレジリエンスへの視点転換が求められています。つまり、攻撃を受けても組織が耐えられるように、迅速に対応し、安全に復旧し、将来的に同様の攻撃が再発しないよう対策を講じることが求められます。

このホワイトペーパーでは、高度なバックアップシステムの従来の認識に異議を唱え、サイバーセキュリティリスク管理戦略の重要な要素として位置付けています。最新のセキュアなバックアップは単なる復旧ツール以上の役割を果たし、脅威ハンティング、早期の攻撃者の阻止、インシデント対応の加速などを行います。特に、主要なセキュリティ防御を回避または隔離するシナリオでは、バックアップは、運用の整合性を維持するために必要な重要な可視性と制御を提供することができます。バックアップシステムに含まれる豊富な履歴情報を活用することで、組織は潜在的な脅威に関するより深いインサイトを得て、インシデント対応とセキュアな復旧を加速化し、より回復力の高いサイバーセキュリティプラクティスを構築できます。

1. 強化された脅威ハンティング

脅威ハンティングは、攻撃シーケンスのできるだけ早い段階で攻撃者を阻止するために、組織のネットワーク内の隠れた脅威の証拠を積極的に検索する積極的なサイバーセキュリティ慣行です。従来の脅威ハンティングでよくある手法は、エンドポイントエージェントとシステムログに依存するものです。

ほぼすべてのランサムウェア・アズ・ア・サービス (RaaS) プラットフォームに、一般的な回避技術が組み込まれています。Bring Your Own Vulnerable Device Driver (BYOVD) この手法では、攻撃者は、オペレーティングシステムレベルを下回る署名付きデバイスドライバを展開し、エンドポイントセキュリティソリューションを効果的にレンダリングし、攻撃に対してログを隠します。ここで、バックアップデータが脅威ハンティングにとって貴重な資産になります。

脅威ハンティングにバックアップデータを使用する際の主な利点は以下の通りです:

- **受動的な脅威ハンティング**: バックアップ・コピーはプライマリ環境から隔離されているため、攻撃者、特にランサムウェア・アズ・ア・サービス (RaaS) プラットフォームに回避技術を埋め込んで、エンドポイント検知と応答 (EDR) や拡張検知と応答 (XDR) などの一般的なセキュリティ・コントロールをバイパスするランサムウェアギャングが改ざんしたりかいくぐったりすることはできません。この隔離により、効果的でステルスな脅威ハンティングが可能になります。
- **過去の状況**: バックアップデータを使うことで、アナリストはシステムの状態や経時的なデータの変化を確認することができ、悪意のある活動の長期にわたる微妙なパターンを識別するのに役立ちます。
- **包括的な対応範囲**: バックアップには組織全体のデータが含まれることが多いため、一見関連性のない事象同士の結びつきを明らかにする全体的な視点が得られます。
- **オフラインでの分析**: 脅威ハンティングではバックアップデータをオフラインで分析できるため、実行中の攻撃者に検知活動が知られるリスクが低減します。
- **削除済みや変更済みのデータの復旧**: バックアップによって、稼働中のシステムで削除または変更された可能性のある証拠を明らかにすることができます。これは、巧妙な攻撃を発見する上で非常に重要です。

2. リアルなデータコンプライアンス

人工知能 (AI) 支援のセキュリティが急増する中、データセキュリティ体制管理 (DSPM) のためのツールは、強力なワンツーパンチのためのバックアップシステムと連携し始めています。DSPMツールは、医療データや財務データなどの機密情報をITシステムやネットワーク、データストアでスキャンするだけでなく、また、データの場所、アクセス頻度、ユーザーも表示します。高度なバックアップシステムと組み合わせることで、コンプライアンスリーダーは機密データの漏洩リスクを劇的に削減できます。

DSPMソリューションを高度なバックアップシステムと統合する利点は次のとおりです。

- **バックアップされていないシステムを迅速に特定する。**DSPMソリューションは、シャドウデータや忘れられたデータベースなど、多様な環境のデータ資産を自動的に検出して分類します。このデータの一部は、既存のバックアップポリシーですでにカバーされている可能性があります。しかし、大量の機密データがカバーされていないこともあり得ます。API統合を通じて高度なバックアップシステムとペアリングすると、セキュリティチームはバックアップカバレッジのギャップを簡単に調査し、これらのデータソースを組織のバックアップポリシーに追加するための措置を講じることができます。最終的に、セキュリティレジリエンスの向上とリスクの低減という結果につながります。
- **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します。**
- **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。**
- **データインシデントの証拠をリアルタイムで分析することで、インシデント対応のプロセスを簡素化し、より迅速な対応が可能になります。**バックアップされたデータのコピーは、DSPMアクティビティが以前の「ダーク」データを照らし、保護するための豊富な環境です。
- **規制当局または影響を受けるデータ主体へのタイムリーな通知を義務付けるGDPRやSEC 8-Kなどの規制要件へのコンプライアンスを向上します。**

3. 包括的なインシデント対応と復旧

堅牢なインシデント対応と復旧戦略は、組織に対するセキュリティインシデントの影響を最小限に抑える上で非常に重要です。では、バックアップデータを使ってインシデント対応を強化しセキュアな復旧を確実にする方法について詳しくご説明します。

ランサムウェア、ワイパー攻撃、悪意のある内部者検知

バックアップと復旧オペレーションにおける異常なデータパターンとユーザーアクティビティは、潜在的な攻撃の早期の警告サインを提供する可能性があります。これらの異常は、トリアージと調査の作業を加速するアラートをトリガーし、チームがより迅速に対応できるようにします。

ランサムウェアへの対応

インシデント対応者は、強力なチェーン・オブ・カストディを持つリソースとしてイミュータブルなバックアップデータを使用できます。そのため、インシデント・レスポンダーは、ファイルシステムのフォレンジックを実行し、アーティファクトを発見し、ランサムウェアやワイパー攻撃によって引き起こされる構成やその他のファイルに対する悪意のある変更を特定できます。高度なバックアップシステムを使用して、この分析を長期間保持される一連のスナップショットにわたって実行し、攻撃のタイムラインについてより深い洞察を得ることができます。

対応者は、ネットワーク内でまだアクティブである可能性のある攻撃者からの干渉や情報漏えいなしに、安全で隔離された環境でバックアップコピー内のIOCを受動的にハンティングすることもできます。さらに、バックアップデータによって攻撃中に悪用された過去の脆弱性が明らかになり、攻撃対象領域を縮小して攻撃を未然に防ぐための貴重なコンテキストが得られます。脆弱性の悪用は現在、ランサムウェアのオペレーターが初期アクセスに使用する主要な方法であり、数日以内にランサムウェア・アズ・ア・サービス (RaaS) プラットフォームにエクスプロイトがベイクされ、システムを復元する前に脆弱性にパッチを適用できないため、元の攻撃者による攻撃だけでなく、RaaSプラットフォームを使用する何千もの他のアフィリエイトへの攻撃にもさらされてしまいます。

イミュータブルバックアップとは、変更や削除ができないデータのコピーのことです。このイミュータビリティ (変更不可) により、プライマリデータがランサムウェアに侵害された場合でも、バックアップデータが変更されず、復旧可能であることが保証されます。

ランサムウェア緩和策

ランサムウェア攻撃は、あらゆる規模の組織でますます脅威となっています。このような攻撃が発生した場合、セキュアで信頼性の高いバックアップがあるかどうかが、軽微な混乱で済むか大惨事になるかの分かれ道となります。当たり前のことのように思えるかもしれませんが、基本的なセキュリティ対策を活用していない組織が非常に多いため、再度検討することが重要です。これらのセキュリティ施策には以下のことが含まれます。

- **イミュータブルバックアップとシステムの堅牢化** Write Once、Read-Many (WORM)、最小権限アクセス、多要素認証、データ暗号化、職務分離などのゼロトラストベースの原則と組み合わせたイミュータブルなバックアップスナップショットにより、バックアップデータがターゲットになるのを防ぎます。
- **エアギャップバックアップ**: エアギャップバックアップはネットワークから物理的に隔離されているため、セキュリティが強化されます。そのため、ネットワークが侵害されても、バックアップがランサムウェア攻撃を受ける心配はありません。
- **定期的なバックアップスケジュール**: 定期的なバックアップスケジュールを設定することで、データが常に更新され、保護されていることが保証されます。バックアップの頻度が高いほど、攻撃の際に組織がデータを失う可能性が低くなります。
- 本番環境にリスクを与えることなく全面的なペネトレーションテストを行うために**システムをクローンします。**
- **本番同様のエンドツーエンド訓練**: デスクトップ演習を超えて、エンドツーエンドのテストと、人、プロセス、テクノロジーの継続的な改善を可能にする本格的な訓練に移行します。本番システムのクローンを作成し、暗号化や破壊を含むシナリオをチーム全体で実行することで、応答と復旧のあらゆる側面をテストできます。実際の破壊的サイバー攻撃に初めて直面しても、初めてのサイバー攻撃対処ではなくなるのです。

テストと訓練

定期的なテストと訓練は、バックアップと復旧プロセスが効果的であり、全関係者がインシデント中の自分の役割をよく把握していることを保証する上で欠かせません。

- **災害復旧訓練**: 定期的に災害復旧訓練を行って実際のシナリオをシミュレーションすることで、チームが対応手順を練習し、改善することに繋がります。こうした訓練は、潜在的な弱点や改善の余地を特定するのに役立ちます。
- **テストの自動化**: バックアップデータのテストを自動化することで、人手を介さずにバックアップの完全性と回復性を検証できます。このような自動化によって、バックアップの信頼性が高いことを保証し、必要に応じて迅速かつ確実にリストアすることができます。
- **文書化とプレイブック**: 詳細な文書と復旧プレイブックがあれば、全員が自分の責任とインシデント中に取るべき手順を把握できるようになります。こうしたプレイブックは、テストと訓練の結果に応じて定期的に更新する必要があります。

詳細なモニタリングとレポート

効果的なインシデント対応と復旧には、バックアップ運用がスムーズに実行され、問題が迅速に対処されていることを確認するための詳細なモニタリングとレポートが必要です。

- **リアルタイムモニタリング**: バックアッププロセスをリアルタイムに監視することで、どんな障害や問題も即座に検知して解決することを保証し、潜在的なデータ損失を防ぎます。
- **アラートの自動化**: 自動アラートでバックアッププロセスのあらゆる異常や障害をITチームに知らせ、迅速に介入して是正できるようにします。
- **包括的なレポート**: バックアップの状況、成功率、復旧時間に関する詳細なレポートで、バックアップ戦略の効果に関するインサイトを提供し、改善が必要な領域を明らかにします。CISOはこうした高度なバックアップ戦略を導入することで、組織が確実にインシデントの迅速かつ効果的な対応と復旧に対する万全の備えを整えられるようにします。このような包括的なアプローチはダウンタイムやデータの損失を最小化するだけでなく、今後の脅威に対する全体的な組織のレジリエンスも強化します。

4. データの完全性とコンプライアンス

データの完全性と規制要件への遵守を維持することは、特にサイバーセキュリティにおいてはどの組織にとっても重要な懸念事項です。バックアップデータは、データの完全性の監査、検証、リストアに使用できる信頼性が高く検証可能な情報源を提供することで、このような懸念に対処する上での重要な役割を果たします。ここでは、バックアップデータがどのようにデータの完全性とコンプライアンスの向上に繋がるのか、詳しくご紹介します。

規制コンプライアンス

組織は、厳格なデータ保護と完全性要件を義務付ける多数の規制フレームワークの下で運営されています。バックアップデータは監査証跡を提供してデータの保持を奨励することで、こうした規制への遵守を達成し、明示するのに役立ちます。

- **監査証跡**: バックアップソリューションでは、すべてのバックアップとリストア活動に関する包括的なログを維持することができます。これらのログはコンプライアンスの監査中に欠かせないもので、データにアクセスした人、アクセスした日時、どんな行動を行ったかに関する詳細な記録を提供します。
- **データ保持ポリシー**: GDPR、HIPAA、SOXといった規制に遵守するには、多くの場合厳格なデータ保持ポリシーへの遵守が求められます。自動化されたバックアップソリューションでは、求められる期間中のデータの保持と不要になった場合のセキュアな削除を保証することで、こうしたポリシーを実行することができます。

セキュアなデータストレージとアクセス制御

バックアップデータを不正アクセスから守ってセキュアに保管することは、データの完全性とコンプライアンスの基本的な側面です。

- **暗号化**: 保存中と転送中の両方のバックアップデータを暗号化することで、不正アクセスからセキュアに保ちます。強力な暗号化プロトコルで機密情報を保護し、適切な復号キーなしには誰も解読できないようにします。
- **ロールベースのアクセス制御 (RBAC)**: RBACを実装すると、権限のある担当者のみがバックアップデータにアクセスできるようになります。この制御によって露出を制限し、データの漏洩や悪用のリスクを低減します。
- **多要素認証 (MFA)**: バックアップシステムへのアクセスでMFAを実施することで、セキュリティレイヤーが追加されます。資格情報が漏洩しても、不正アクセスは防がれます。

災害復旧と事業継続計画

効果的な災害復旧と事業継続計画は、包括的なコンプライアンス戦略に欠かせない要素です。バックアップデータがあれば、組織は混乱から迅速に復旧し、最小限の影響で事業を継続することができます。

- **ビジネスインパクト分析 (BIA)**: ビジネスインパクト分析 (BIA): BIAの実施は、データの損失や破損が事業に与える潜在的な影響を、組織が把握するのに役立ちます。バックアップデータは、重要なシステムとデータの信頼できるリストア手段を提供することで、この分析において重要な役割を果たします。
- **目標復旧時間 (RTO) と目標復旧時点 (RPO) を達成したことをどうやって知ることができるのでしょうか?** 明白なRTO目標やRPO目標があれば、組織は許容される時間枠内に最小限のデータ損失でデータを復旧することができます。バックアップソリューションは、こうした目標を満たすよう設計されていなければなりません。
- **継続計画**: バックアップデータは継続計画に欠かせないもので、災害の発生中や発生後も運営を維持できるようにします。バックアップデータを使って災害復旧計画を定期的にテストすることで、より効果的で信頼性の高い復旧プロセスになります。

データの完全性とコンプライアンスは、今日の複雑な規制環境において、信頼性と運用に対する信用を維持する上で重要です。バックアップデータを効果的に活用することで、組織は規制要件を満たし、データの完全性を守り、堅牢なセキュリティ対策を維持することができます。包括的な監査証跡、データ保持ポリシーの実施、セキュアなストレージとアクセス制御の提供を実現する高度なバックアップソリューションを導入すれば、こうした目標を達成し、安心感を得ながら継続的な成長とレジリエンスを支える強固な基盤を築くことができます。

5. 可視性と制御の強化

最高情報責任者 (CISO) にとって、組織のデータとバックアッププロセス全体の可視性と制御を強化することは、堅牢なセキュリティと効率的なデータ管理を維持する上で欠かせないことです。高度なバックアップソリューションを利用することで、CISOはデータ環境に対する包括的なインサイトを獲得し、管理プロセスを効率化して、重要な情報の保護を強化することができます。ここでは、バックアップデータの効果的な活用によってどのように可視性と制御の両方が強化されるのか、詳しくご紹介します。

一元管理

一元管理のアプローチでは、バックアップ運用を統合し、組織のすべてのバックアップ活動を一か所で監督できるようにします。この一元化によって管理プロセスがシンプルになり、データ保護慣行における一貫性が確保されます。

- **統合ダッシュボード**: 統合ダッシュボードは、バックアップジョブの状態、ストレージの使用状況、潜在的な問題など、バックアップ環境の全体像を提供します。このようにリアルタイムで可視化することで、CISOはバックアップの健全性とパフォーマンスを効果的に監視することができます。
- **管理のシンプル化**: 一元管理ツールを使うと、複数のバックアップシステムやロケーションを管理する際の複雑性が低減されます。管理がシンプルになることでより効率的な運用ができ、設定ミスやエラーのリスクが低減します。
- **ポリシーの実施**: 一元制御をすることで、組織全体で一貫したデータ保護ポリシーを実施することができます。データの保持、暗号化、アクセス制御に関するポリシーを均一に適用できるため、コンプライアンスとセキュリティが向上します。

包括的なレポートと分析

詳細なレポートと分析ではバックアップ運用に対する貴重なインサイトが提供され、CISOによる情報に基づく意思決定とデータ保護戦略の最適化に役立ちます。

- **監査ログに対応**: 詳細な監査ログでは、バックアップデータに関するすべてのアクセスとアクティビティを追跡します。このようなログには、データにアクセスした人、行った行動、発生日時が明確に記載されており、セキュリティモニタリングとコンプライアンス監査の両方に役立ちます。
- **カスタマイズ可能なレポート**: カスタマイズ可能なレポートツールを使えば、CISOは、コンプライアンス要件、運用パフォーマンス、セキュリティ監査といった特定のニーズに合わせてレポートを生成することができます。こうしたレポートでは、バックアップ活動を明確かつ包括的に確認できます。
- **傾向分析**: データの成長パターン、ストレージの使用状況、復旧時間といったバックアップデータの傾向分析は、長期の傾向や潜在的な問題領域を特定するのに役立ちます。この分析は、戦略的な計画やリソースの割り当てを支援します。
- **データインサイト**: 高度な分析ツールは、最も多くのデータを生成しているシステムや部門、最も重要なデータ、潜在的な脆弱性の特定など、バックアップデータに関するより詳細なインサイトを提供します。こうしたインサイトを得ることで、より対象を絞った効果的なデータ保護対策が実現します。

一元管理、高度なアクセス制御、リアルタイムモニタリング、包括的なレポート、自動化を提供する高度なバックアップソリューションを採用することで、CISOは組織のデータが保護され、規制に遵守し、復旧に使用できる状態にあることを保証することができます。こうした機能は全体的なセキュリティ体制を強化するだけでなく、データ保護戦略の最適化と組織の長期にわたる成功を支援するために必要なインサイトと制御も提供します。

6. 戦略的なインサイトと意思決定

サイバーセキュリティ領域では、効果的なリソースの管理、将来の課題の予測、堅牢なセキュリティ体制の維持をする上で、戦略的な意思決定が欠かせません。バックアップデータは活用されていないこともおおくありますが、情報に基づく意思決定を促し、組織全体のセキュリティ戦略を強化する貴重なインサイトを提供します。前項では、過去の状況を考慮することで、脅威を発見したり、データ利用に関する基本的な行動に関するインサイトを獲得したりすることができる傾向分析が実現する点についてお話ししました。本項では、バックアップデータがビジネスの健全性に関する戦略的なインサイトの獲得にどのように役立つか、というテーマを扱います。

リソース配分の最適化

セキュリティへの投資効果を最大化するには、効果的なリソースの割り当てが重要です。バックアップデータはどのシステムやデータが最も重要なのかに関する詳しいインサイトを提供するため、組織はセキュリティ対策の優先順位を付け、最も必要な領域にリソースを割り当てることができます。

- **重要なデータの特定**: バックアップデータは、事業運営に欠かせないデータやシステムはどれかを特定するのに役立ちます。異なるデータセットの重要性を把握することで、組織は保護と復旧の優先順位を付けることができます。
- **コスト管理**: バックアップデータの保存と使用に関するパターンを分析することで、コスト削減の機会を明らかにすることができます。組織はストレージソリューションを最適化し、冗長なデータを排除して、データを保護しながら全体のストレージコストを下げることができます。
- **リソースの優先順位付け**: バックアップデータのインサイトを活用すると、最も価値のある領域にリソースを集中させることができます。このような対象を絞ったアプローチでは、最も重要な資産が最も高度に保護されます。

戦略的なビジネスインサイト

バックアップデータは、セキュリティやコンプライアンスにとどまらず、組織のより広範な目標を支援する戦略的なビジネスインサイトを提供することができます。

- **運用効率の向上**: バックアップデータを分析することで、データ管理や運用プロセスにおける非効率を明らかにすることができます。組織はこうしたインサイトを、運用の効率化、冗長性の低減、全体的な効率の向上に利用することができます。
- **データの活用**: 組織全体でのデータの使われ方を理解することは、データの活用と管理を強化する機会を特定するのに有益です。バックアップデータから得られるインサイトは、データのアーカイブ、ライフサイクル管理、アクセスポリシーに関する意思決定に役立ちます。
- **イノベーションの成長**: バックアップデータを使って、イノベーションとビジネスの成長を支援する傾向やパターンを見つけ出すことができます。データの経時的な進化を分析することで、組織は新たな機会を特定し、プロセスを最適化して、戦略的な取り組みを促すことができます。

戦略的なインサイトと意思決定にバックアップデータを活用することで、効果的なリソース管理、脅威の予測と対応、規制コンプライアンスの維持を実現する組織の力が高まります。バックアップデータをより広範な組織戦略に統合することで、CISOは継続的な改善を促し、リソース配分を最適化し、組織の長期的な成功を支援することができます。堅牢な分析、レポート、自動化機能を提供する高度なバックアップソリューションは、組織がデータの持つ力を最大限に活用し、戦略的な計画と意思決定のための貴重な資産に変えるのに役立ちます。

まとめ

どのCISOも、厳格な規制を遵守しながら、巧妙化した脅威から組織のデータを守るという非常に困難な課題に直面しています。クラス最高のバックアップソリューションは、災害復旧をサポートするだけでなく、コンプライアンスとセキュリティのリスクを低減します。今や、サイバー保険の品質を語る際に必須です。

高度なバックアップシステムは、“多層防御”の不可欠な要素であり、サイバーインシデントの最後となる防御線です。クラウドでもオンプレミスでも、大量の機密データをコスト効率の高いストレージに効率的かつ安全に移行し、目標復旧時間 (RTO) を証明することで、データ損失、運用上のダウンタイム、およびビジネスの評判のリスクを低減します。このテクノロジーを最適化して活用することで、CISOはますます複雑化するデジタル世界で、回復力をもち、俊敏かつ長期的なビジネス価値を強化することができます。

詳細はCohesity.comをご確認ください。

COHESITY
cohesity.com
1-855-926-4374
2625 Augustine Drive, Santa Clara, CA 95054

2000053-002-EN 4-2025