ソリューション概要

保護、検出、リカバリ：ランサムウェア対策に対するデータ主体のアプローチ

保護：環境をセキュアに保ちます。
検出：脅威を予測します。
リカバリ:すばやく復旧します。

課題

ランサムウェア攻撃は、あらゆる規模の組織にとってますます一般的で高度な脅威となっています。このような悪意のある攻撃は、貴重なデータを暗号化してリリースの支払いを要求し、多くの場合、多大な金銭的損失や業務の中断を引き起こします。

- サイバーインシデントは、世界でナンバーワンのビジネス リスクです。
- ランサムウェアは、2031年までに2秒ごとに攻撃を受けると予想されています。
- 昨年、59%の組織がランサムウェアの影響を受けました。
- ランサムウェア攻撃は、2022年から2023年に73%増加しました。

多くの企業はネットワークとエンドポイントのセキュリティに重点を置いていますが、データが存在するストレージ レイヤを保護することの重要性を見逃さないことが重要です。暗号化、アクセス制御、書き換え不可能なバックアップなど、ストレージレベルで堅牢なセキュリティ対策を実装することで、ランサムウェアに対する防衛線を新たに構築できます。

このアプローチは、ソースのデータを保護するのに役立ち、攻撃者が重要な情報を暗号化または破損するのを難しくします。セキュアなストレージ ソリューションは、迅速なリカバリを支援し、攻撃が成功した場合のデータ損失を最小限に抑えることができます。これは、ストレージ インフラストラクチャの強化を含む包括的なセキュリティ戦略の重要性を強調しています。

NetAppサイバー レジリエンス：ランサムウェア対策に対するデータ主体のアプローチ

サイバー インシデントからの保護には、さまざまな脅威から保護するための複数の防御層が含まれます。強力なサイバー防御は、最も外側のレイヤーである**境界セキュリティ**とともに、最初の防御線として機能する**アイデンティティ セキュリティ**層から始まります。

ネットワーク セキュリティは、この基盤の上に構築されており、転送中のデータを保護し、内部ネットワーク内の異常なアクティビティを検出します。**エンドポイント セキュリティは**、ネットワークに接続されている個々のデバイスの防御層を追加します。**アプリケーション セキュリティ**は、脆弱性や攻撃からソフトウェア アプリケーションを保護することに重点を置いています。

最後に、セキュリティ体制の中核をなすのが**データ セキュリティ**です。データセキュリティは、組織の最も貴重な資産であるデータと最もミッション クリティカルな資産を保護します。このレイヤには、通常、堅牢なバックアップ/リカバリ ソリューションによるデータ保護が含まれます。

これらの相互接続されたセキュリティ レイヤは、企業のデジタル資産を境界からデータセンターまで保護し、ITインフラのあらゆるレベルの脅威に対処するための包括的な防御戦略を作成します。

ミッションクリティカルな資産のデータ レイヤでの保護は、さらに重要であり、固有の要件があります。効果的に機能するには、この層のソリューションが次の4つの重要な属性を提供する必要があります。

- 設計段階からセキュリティを確保し、組織に対する攻撃が成功する可能性を最小限に抑えます。
- リアルタイムの検出と対応により、攻撃が成功した場合の影響を最小限に抑えます。
- エアギャップによるWrite Once Read Many（WORM）保護で重要なデータのバックアップを分離します。
- シンプルなコントロール プレーンで包括的なランサムウェア対策と迅速なリカバリを実現します。

NetAppは、データ レイヤで検出、保護、リカバリを実行できます。

セキュアな設計：ストレージにネイティブなONTAP組み込みのランサムウェア対策

NetApp ONTAPソフトウェアは、セキュアな設計アプローチを通じて、堅牢なランサムウェア対策を提供します。主な機能には、変更や消去が不可能なSnapshotコピーが含まれています。このため、管理者でもデータを変更したり削除したりすることはできません。これにより、信頼性の高いリカバリ用フォールバック ポイントが作成されます。ONTAP FPolicy機能は、悪意のあるファイルをブロックし、システム内の脅威の拡散を防止することでセキュリティを強化します。

主なメリット

- **セキュア バイ デザイン：**ストレージレイヤでのデータ保護機能を標準搭載
- **リアルタイムの検出と対応：**AIを活用したランサムウェア防御：
- **サイバー バックアップ：**変更不可/消去不可のバックアップ：
- **統合コントロール プレーン：**検出からリカバリまでのインテリジェントなオーケストレーション
- **リカバリ保証：**NetApp Snapshotコピーでデータ損失をゼロに

アクセス制御を強化するには、複数の管理者が重要なアクションを承認する必要があります。これにより、内部の脅威やクレデンシャルの侵害のリスクが軽減されます。また、多要素認証によってセキュリティが強化されるため、権限のある担当者のみが機密データやシステムにアクセスできます。

リアルタイムの検出と対応

NetAppは、堅牢なランサムウェア対策に加えて、ONTAPに直接組み込まれたAIを活用した自律型テクノロジを活用して、99%の精度でリアルタイムの検出とほぼ瞬時の応答機能を提供します。この高度な検出機能は、疑わしいアクティビティや異常を継続的に監視し、Amazon FSx for ONTAPのファイル、ブロック、ネイティブ クラウドに対するランサムウェア攻撃の可能性を迅速に特定します。脅威が検出されると、システムは影響を受けるデータを自動的に分離し、それ以上の拡散を防ぎ、潜在的な被害を最小限に抑えることができます。

NetApp Data Infrastructure Insights（DII）は、内部の脅威に対する防御レイヤを追加します。ユーザの潜在的な異常な行動を検出し、ストレージ システムへのユーザ アクセスをブロックしたり、Snapshotを作成したりするなどのアクションを即座に実行します。さらに、DIIはフォレンジック分析と監査のための詳細な分析を提供します。この包括的なアプローチは、プロアクティブな脅威検出、迅速な対応メカニズム、詳細なユーザ アクティビティ監視を組み合わせ、外部のランサムウェア攻撃と内部の脅威の両方に対して多面的な防御を提供します。

図1：NetAppは、エンドツーエンドの暗号化によるデータアクセス、多要素認証、ロールベース アクセスなど、データをインテリジェントかつ効率的に保護する多層防御機能を備え、地球上で最もセキュアなデータストレージを提供します。

分離されたバックアップでサイバー バックアップを実現

SnapLock®コンプライアンス ソフトウェアを基盤とするNetAppサイバー バックアップにより、組織は最も重要なデータ資産を保護するための包括的で柔軟なソリューションを提供します。ONTAPの堅牢なセキュリティ強化手法を使用した論理的エアギャップにより、進化するサイバー脅威に対して耐障害性を備えた、セキュアで分離されたストレージ環境を構築できます。NetAppを使用すると、ストレージ インフラの即応性と効率性を維持しながら、データの機密性、整合性、可用性を確実に確保できます。

セキュリティを強化するために、NetAppではデータ保護レイヤを追加で作成できます。

- セキュアで分離されたストレージ インフラ（エアギャップ型ストレージ システムなど）
- 書き換えや消去が不可能なデータのバックアップ コピー
- 厳密なアクセス制御と多要素認証
- きめ細かなデータ リストア機能
- SnapLockでは、WORMテクノロジを適用することで、データを破棄できない効率的なデータ コピーを使用して、データの暗号化や削除を防止します。

シンプルで堅牢なコントロール プレーン

NetAppは、ワークロード中心のエンドツーエンドのランサムウェア防御テクノロジをインテリジェントに調整して実行するために、NetApp BlueXP™を備えた単一のコントロール プレーンを提供する唯一のストレージ ベンダーです。これらのテクノロジを使用すると、リスクにさらされている重要なワークロード データをワンクリックで**特定して保護し**、正確かつ自動的に**検出して**潜在的な攻撃の影響を制限し、数日や数カ月ではなく数分以内にワークロードを**リカバリして**、貴重なワークロード データを保護し、ビジネスの中断に伴うコストを最小限に抑えることができます。

BlueXPランサムウェア対策オーケストレーション ツールは、NetApp ONTAPの強力な機能とBlueXPデータ サービスを統合し、人工知能や機械学習に基づく推奨事項やガイダンスを自動化されたワークフローに追加して、次のようなメリットをもたらします。

- **特定**：NetAppストレージ内のワークロード（VM、ファイル共有、DB）とそのデータを自動的に特定し、データをワークロードにマッピングして、ワークロードの重要性を判断し、ワークロードのリスクを分析
- **保護**：ワークロード保護ポリシーを推奨してワンクリックで適用

- **検出：**業界最高レベルのMLを基盤とする検出機能により、ワークロード データに対する潜在的な攻撃をほぼリアルタイムで検出
- **対応：**潜在的な攻撃の疑いがある場合に、書き換えや消去のできないSnapshotコピーを作成することで、ほぼリアルタイムで自動的に対応。
- **リカバリ：**バックアップの整合性を検証し、最適なリカバリ ポイントを特定し、シンプルなオーケストレーションによるリカバリを通じて、ワークロードと関連データをすばやくリストアします。

「当社は最近ランサムウェア攻撃を経験したばかりです。Cloud Insightsのランサムウェア検知の機能を目にして、すぐに魅力を感じました」

運輸会社のIT担当ディレクター

BlueXP Ransomware Protection Orchestratorは、ランサムウェアへの備え、攻撃への対応、リカバリのガイドを支援する包括的なソリューションを提供することで、ランサムウェアに関連するダウンタイムやデータ損失からワークロードを保護する際の負担や不安を取り除きます。攻撃が発生したときにすぐに把握でき、貴重なワークロード データが保護され、リカバリが簡単かつ迅速になり、ビジネスの中断が最小限に抑えられるという安心感を提供できるのはNetAppだけです。

NetAppのランサムウェア対策は、データが格納されている場所を特定して保護し、攻撃の可能性を正確かつ自動的に検出して対応し、数日から数カ月ではなく数分以内にデータをリカバリするのに役立ちます。この機能により、貴重なデータを保持し、サイバー レジリエンスのためのコストのかかるシステム停止を最小限に抑えることができます。

ランサムウェアを真剣に受け止めていない企業は、弱体化する可能性があります。データ主体のサイバー レジリエンス アプローチでは、プライマリデータとセカンダリデータに包括的な統合セキュリティと保護を提供し、リカバリを保証するのはNetAppだけです。

NetApp BlueXP ランサムウェア対策の詳細

NetAppについて

NetAppはインテリジェントなデータインフラ企業として、ユニファイド データ ストレージ、統合データ サービス、CloudOpsソリューションを組み合わせることで、混沌とした世界を変革し、あらゆるお客様にビジネス チャンスをもたらしています。NetAppはデータ サイロのないインフラを構築し、オブザーバビリティとAIを活用して業界最高のデータ管理を実現します。業界大手各社のクラウドにネイティブに組み込まれた唯一のエンタープライズクラスのストレージ サービスとして、NetAppのデータ ストレージはシームレスな柔軟性を提供します。さらに、NetAppのデータ サービスは、優れたサイバー レジリエンス、ガバナンス、アプリケーションの即応性を通じてデータの優位性を生み出し、CloudOpsソリューションは、オブザーバビリティとAIを通じてパフォーマンスと効率を継続的に最適化します。データの種類、ワークロード、環境を問わず、NetAppがデータインフラを変革し、ビジネスの可能性を現実のものにします。**www.netapp.com/ja/**

ネットアップ合同会社
Email:ng-sales-inquiry@netapp.com
https://www.netapp.com/ja/forms/sales-contact/