はじめに
Ransomware Protection

NetApp
June 13, 2022

目次

はじめに

ランサムウェア防御についてご確認ください

ランサムウェア攻撃は、ビジネス時間、リソース、評判を低下させる可能性があります。ランサムウェア防御サービスを使用すると、サイバーセキュリティに関する関連情報を表示し、組織がサイバー攻撃に対する回復力を評価できます。また、データのセキュリティを強化するためのアラートと修正措置のリストも記載されています。

"ランサムウェア対策ソリューションのユースケースをご紹介します"。

ランサムウェア対策サービスは現在ベータ版です。

の機能

ランサムウェア攻撃からの保護では、さまざまな作業環境やインフラレイヤで データ セキュリティ を一元的に管理、調整し、脅威の発生時に適切に対処することができます。現在、サイバーストレージの保護に役立ついくつかの機能が提供されています。今後追加される予定です。現在の機能では、次のような状況

- 作業環境内のボリュームは、定期的な Snapshot コピーを作成して保護されていません。
- を使用してクラウドへのバックアップを作成することで、作業環境内のボリュームを保護することができません "クラウドバックアップ"。
- 作業環境のデータやデータソースは、ではスキャンされません "クラウドデータの意味" コンプライアンスやプライバシーに関する懸念を特定し、最適化の機会を見つける。

  この機能はランサムウェア攻撃からの保護の観点でも重要です。重要な（機密性の高い、ビジネスクリティカルな）データがどこにあるかをより詳しく把握できるため、保護対策に集中しているかを確認できます。

- 最も重要なカテゴリのデータは、ランサムウェア攻撃によってリカバリが必要になった場合にバックアップされません。
- 作業環境またはデータソースで暗号化ファイルの割合が異常に増加しています。

  これは、ランサムウェア攻撃がネットワークで開始されたことを示すインジケータになります。

- 機密データがファイルで検出され、作業環境やデータソースでアクセス権限レベルが高すぎます。
- ユーザーが Active Directory ドメイン管理者グループに追加されました。
- クラスタ上の ONTAP ソフトウェアのバージョンは古く、最高の保護機能とセキュリティ機能を提供するために更新する必要があります。
- ONTAP システムで NAS ファイルシステムの監査が有効になっていません。

  CIFS 監査を有効にすると、システム管理者に対して、フォルダの権限の変更、ファイルの読み取りや書き込みの失敗、ファイルの作成、変更、削除などの情報を追跡する監査イベントが生成されます。

- 組み込みのランサムウェア対策機能が ONTAP システムで有効になっていない。

ONTAP ランサムウェア対策機能は、ランサムウェア攻撃を示す可能性のある異常なアクティビティをプロアクティブに検出して警告します。

"潜在的な問題をランサムウェア対策ダッシュボードで確認する方法をご確認ください。"

Cloud Volumes ONTAP システムを使用している場合、作業環境から直接導入できるランサムウェアの保護機能がいくつか追加されています。 "ランサムウェアに対する保護を強化する方法をご確認ください"。

サポートされている作業環境とデータソース

"クラウドデータの意味" ランサムウェア対策サービスを使用するための前提条件です。データセンスをインストールして有効化すると、ランサムウェア防御を使用して、次のような作業環境やデータソースに対するサイバー攻撃に対するデータの復元力を確認できます。

- 作業環境： *
- Cloud Volumes ONTAP （ AWS 、 Azure 、 GCP に導入）
- オンプレミスの ONTAP クラスタ
- Azure NetApp Files の特長
- ONTAP 対応の Amazon FSX
- Amazon S3
- データソース： *
- ネットアップ以外のファイル共有
- オブジェクトストレージ（ S3 プロトコルを使用）
- データベース（Amazon RDS、MongoDB、MySQL、Oracle、PostgreSQL、 SAP HANA、SQL Serverなど）
- OneDrive アカウント
- SharePoint アカウント
- Googleドライブアカウント

ランサムウェア攻撃からの保護では、グローバルな Active Directory 構成も監視されます "これはクラウドデータセンスで設定されています"。

ランサムウェア防御の仕組み

ランサムウェア対策による防御の概要は次のようになります。

1. Ransomware Protectionは、ストレージシステム、Cloud Data Sense、Cloud Backup、およびその他のCloud Managerリソースから情報を収集し、ランサムウェア防御ダッシュボードにデータを表示します。
2. Ransomware Protection ダッシュボードを使用すると、システムの保護状況の概要を確認できます。
3. 提供されているレポート作成ツールを使用して、サイバーストレージの保護を強化できます。

コスト

ベータ版では、ランサムウェア対策サービスに個別のコストはかかりません。