概要

分離されたヴォールト、AIベースのML分析ソフトウェアなどを使用して、サイバー レジリエンスを高め、サイバー ランサムウェアの脅威からデータを保護する

Dell Technologies PowerProtect Cyber Recovery with CyberSenseで実現

サイバー脅威はこれまでになく頻発化し、攻撃手法は進化しています。こうした状況において、データ保護計画では、最も表面的な部分から最も深い部分まで、あらゆるITコンポーネントを保護して分析するアプローチが必要です。Dell PowerProtect Cyber Recoveryは、最も重要な機密データを保護しながら、サイバー攻撃やその他の破壊的な事象が発生した際も適切にリカバリーできるよう支援します。

Dell PowerProtect Cyber Recoveryは、ランサムウェア、破壊的なサイバー攻撃、予期せぬ事象からデータとアプリケーションを保護するのに役立つデータ管理、保護、リカバリー ソリューションです。このソリューションはマルチコピー アプローチを採用しています。つまり、バックアップを作成後、保護と分析のために、それらのバックアップを分離されたストレージにコピーします。PowerProtect Cyber Recoveryは、1つまたは複数のストレージ ヴォールトを含む、多くのコンポーネントで構成されます。これらは、オンプレミスのPowerProtect DD（旧称Data Domain）アプライアンスに配置することも、ソフトウェアデファインドのDell APEX Protection Storage for Public Cloud（旧称DD Virtual Edition）経由でクラウドに配置することもできます。いずれのケースでも、ヴォールトは運用上、エアギャップ化されており、本番環境から分離されます。オンプレミス環境では物理的なエアギャップ、APEX環境では論理的なエアギャップを使用することになるでしょう。これにより、悪意のある攻撃者や権限のないユーザーがログ インしてバックアップ コピーを侵害することが極めて難しくなります。

PowerProtect Cyber Recoveryには、完全に自動化された統合型のインテリジェントなセキュリティ分析エンジンであるCyberSenseも搭載されています。ヴォールト内のデータ、ファイル、データベース、イメージを自動的にスキャンして、ランサムウェア攻撃による破損の兆候を検出します。CyberSenseは、ファイルの観測結果を人工知能(AI)ベースの機械学習(ML)モデルの入力に使用して、あらゆるコンテンツを分析します。そして、コア インフラストラクチャ（Active DirectoryやDNSなど）、ユーザー ファイル、重要な本番データベースの大量の削除、暗号化といった不審な変更など、ランサムウェアや破壊的な攻撃の兆候となりうる悪意のあるアクティビティーを検出します。CyberSenseは、破損パターンを検出すると、PowerProtect Cyber Recoveryダッシュボードにアラートを生成し、攻撃の規模と影響に関する追加情報を提供します。[1]

PowerProtect Cyber Recoveryにより、組織はサイバー攻撃を軽減し、離れた場所に存在する複数のデータ バックアップ コピーでデータのレジリエンスを強化し、ダウンタイムを短縮して、ビジネス継続性を維持できます。このレポートでは、公開データを使用して主要なデータ保護機能を明確にし、CyberSenseの競合分析から得られた知見を提示しています。

機密データの保護

バックアップ レプリケーションの実行中に不変データを暗号化し、物理的および論理的に分離されたヴォールトに格納します

SQL Serverページの破損検出

CyberSenseは、競合ソリューションでも検出できなかった感染を特定しました

破損していないバックアップ コピーの特定

CyberSenseは、リカバリーに使用可能な最新の感染していないバックアップ コピーを特定しました

セキュリティ

Dell PowerProtect Cyber Recoveryは、ランサムウェアやその他の高度な脅威から重要なデータを保護し、権限のないユーザーによる機密情報へのアクセスを防止し、迅速なリカバリーで組織が通常の運用を再開できるようにするためのさまざまなセキュリティ機能を備えています。

そして、PowerProtect Cyber Recoveryソリューションが叶えるセキュリティ、整合性、リカバリーには、PowerProtect DDアプライアンスの機能が必要不可欠だと考えられます。そうした機能には、Retention Lock、DDBoost、ロールベースのアクセス制御(RBAC)、二重認証などがあります。

分離

データ分離とは、不正アクセスを防止するために、障壁や境界でデータを分離し、アクセスを制限することです。多くの場合、分離には永続的な接続ではなく、一時的なネットワーク接続を使用します。

感染したネットワークでは、悪意のある攻撃者が構成の変更、データの削除、ポリシーの変更や、ネットワーク トラフィックのスニフィングによるユーザー資格情報の取得を試みる可能性があります。データ分離により、重要なデータを感染したネットワークから隔離したままにできます。また、分離は攻撃対象領域を縮小し、悪意ある攻撃者がアクセスと制御を得る機会を減らすのにも役立ちます。さらに、組織はアクセスを許可された担当者のみに制限できるため、権限のないユーザーによるデータの上書きを防止できます。

PowerProtect Cyber Recoveryは、前述の機能に加えて、エアギャップという物理的および論理的な分離を提供して、データ保護を支援します。物理的に分離されたオンプレミスのPowerProtect DDはヴォールトの役割を担うことができます。本番環境のユーザーやシステムはコンポーネントにアクセスできず、ヴォールトは本番ネットワークから物理的に切断されることになります。[2] 本番ネットワークからリカバリー環境へのアクセスを排除することで、組織は攻撃対象領域を縮小できるでしょう。

不変性*

バックアップを不変にして読み取り専用にすると、組織はそれらのバックアップを信頼してリカバリーに使用できます。運用面では、不変であることがデータの真正性と信頼性を維持するのに役立ちます。DDシステムは、PowerProtect Cyber Recoveryソリューションに含まれるものを含め、MTreesと呼ばれるファイル システムの論理パーティションを使用してデータを保存する方法に不変性を持たせることができます。これらのソリューションでは、MTreeレプリケーションを使用し、DDBoostプロトコル経由で本番DDからヴォールト内の別のDDに不変データ コピーを安全に複製することもできます。[3]

*Dellの製品は、重要なデータを保護するためのお客様の取り組みをサポートするように設計されています。あらゆる電子製品と同様に、データ保護、ストレージ、その他のインフラストラクチャ製品においても、セキュリティの脆弱性が発生する可能性があります。Dellからセキュリティ更新プログラムが提供され次第、速やかにインストールすることが重要になります。

CyberSense

データを適切に保護するには、あらゆるレベルでセキュリティを提供する包括的な戦略が必要です。Dell PowerProtect Cyber Recoveryソリューションの自己修復、セキュリティ、不変性、分離といったあらゆる機能を動員しても、目立たない攻撃が、データ バックアップ レベルなどでエンタープライズ インフラストラクチャに深く入り込み、本番データやユーザー グループ全体が侵害されるまで検出されない可能性があります。Dell PowerProtect Cyber Recoveryソリューションは、サイバー攻撃に対する最後の防御線と、CyberSense経由での迅速なリカバリーを支援する効率的なアプローチを提供します。

CyberSenseと、競合他社（以下、「ベンダーX」）のデータ管理プラットフォームに搭載された同様の機能を持つツールを、同等サイズのアプライアンスを使用してテストしました。このテストにおいて、PowerProtect Cyber RecoveryはSQLデータベース ページで感染を検出しました。ベンダーXのソリューションではこの感染を検出できませんでした。また、PowerProtect Cyber Recoveryは、ベンダーXのソリューションよりも少ない数のバックアップでデータの破損を特定しました。

1. Dell『CyberSense® for PowerProtect Cyber Recovery』、2023年9月8日にアクセス、https://www.delltechnologies.com/asset/en-in/products/data-protection/briefs-summaries/h18214-cybersense-for-dellemc-powerprotect-cyber-recovery-solution-brief.pdf
2. Dell「MTree replication」、2023年9月11日にアクセス、https://infohub.delltechnologies.com/l/dell-powerprotect-cyber-recovery-reference-architecture/mtree-replication-3
3. Principled Technologies『Dell EMC Cyber Recovery protected our test data from a cyber attack』、2023年8月21日にアクセス、http://facts.pt/rkew01n

▶ オリジナルのサマリー（英語）を読む

レポートを読む ▶

Principled Technologies®

Facts matter.®