DELL Technologies

ソリューション概要

Dell PowerProtect Cyber Recovery

ランサムウェアと破壊的なサイバー攻撃から重要なデータを保護する、モダンでレジリエンスに優れた保護ソリューション。

Cyber Recoveryの特長

サイバー攻撃は、バックアップを含めたお客様の貴重なデータを破壊、盗難、または侵害することを目的としています。重要なデータを保護し、データの整合性を確保しながらリカバリーを行うことは、攻撃を受けた後に通常業務を再開するための鍵となります。サイバー攻撃が巧妙さを増している状況で、ビジネスが生き残るためにはどうしたらよいでしょうか。サイバー レジリエンスに優れたこのソリューションは以下の要素で構成されます。

データの隔離とガバナンス
企業内ネットワークとバックアップ ネットワークから切り離されており、適切な許可を得たユーザー以外は使用できない、隔離されたデータセンター環境です。

自動データ コピーとエア ギャップ
セキュリティ保護されたデジタル ヴォールトに変更不可能なデータ コピーを作成し、本番稼働/バックアップ環境とヴォールトの間に運用上のエア ギャップを設けるプロセスです。

インテリジェントな分析とツール
機械学習およびフルコンテンツのインデックス作成機能により、安全なヴォールト内で高性能な分析を行います。自動整合性チェックにより、データがマルウェアによって影響を受けているかどうかを判断し、必要に応じて修復を支援するツールを利用できます。

リカバリーと修復
動的なリストア プロセスと既存のDR手順を用いて、インシデント後のリカバリーを実行するためのワークフローとツールです。

ソリューションの計画と設計
重要なデータ セット、アプリケーション、およびその他の重要な資産を選択して、RTOやRPOを決定し、リカバリーを効率化するための専門家によるガイダンス。

課題：データ主導型ビジネスを脅かすサイバー攻撃

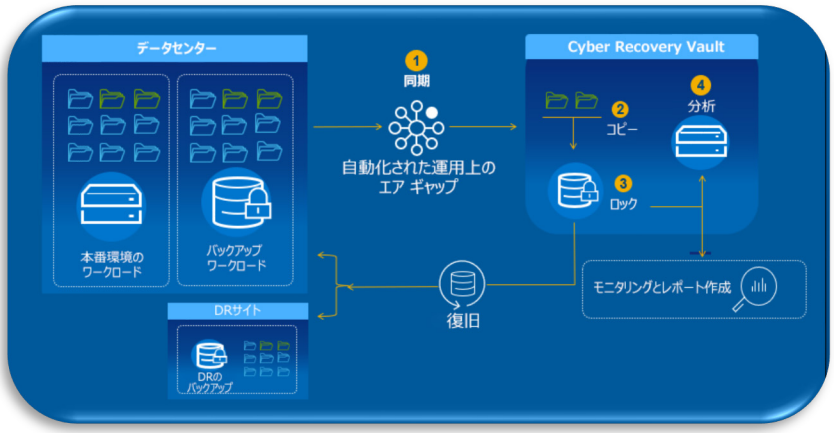
インターネット経済において、データは通貨であり、保護され、機密性が保たれ、瞬時に利用可能でなければならない重要な資産です。今日のグローバル市場は相互に接続されたネットワーク間を常に流れるデータに依存しており、デジタル トランスフォーメーションに向けた取り組みによってリスクにさらされる機密データも増加しています。

そのため、組織のデータはサイバー犯罪者にとって魅力的でうまみのある標的となります。業界や組織の規模にかかわらず、企業や政府機関は絶えずサイバー攻撃によるリスクにさらされています。そのリスクは、データ侵害、ダウンタイムによる売上の損失、評判の低下、規制違反による多額の罰金などです。

サイバー レジリエンス戦略を備えていることは企業や政府機関のリーダーにとって必須事項となっていますが、多くの組織は自社のデータ保護ソリューションに関して自信を持てずにいます。Global Data Protection Indexによると、IT導入決定者の79%が今後12か月以内に破壊的な事象が発生することを懸念しており、75%が組織の既存のデータ保護手段ではマルウェアやランサムウェアの脅威に対抗するのに十分でない可能性があると懸念しています[1]。

それでは、組織や顧客、従業員、そして貴重なデータを保護するためにはどうすればよいのでしょうか。

解決策：Dell PowerProtect Cyber Recovery



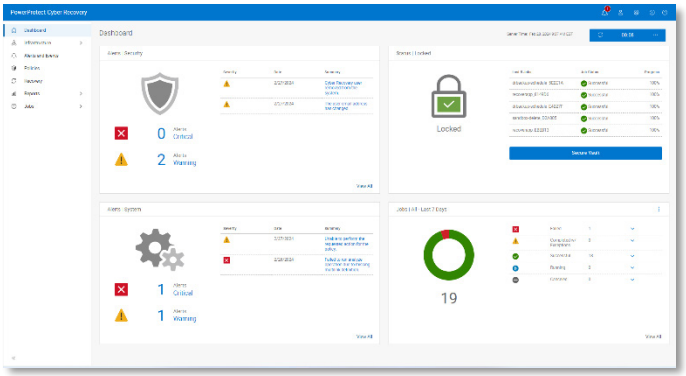
サイバー攻撃によるビジネス リスクを低減し、従来よりもサイバー レジリエンスに優れたデータ保護アプローチを構築するためには、リカバリーとビジネス継続性に関する戦略のモダナイズと自動化を行い、最新のインテリジェント ツールを利用してサイバー脅威の検出と防御を行うという方法をとることができます。

Dell PowerProtect Cyber Recoveryは、重要なデータを隔離し、不審なアクティビティを特定し、データ リカバリーを加速するための実証済みかつモダンでレジリエンスに優れたインテリジェントな保護機能を提供することで、通常業務をすばやく再開できるようにします。

PowerProtect Cyber Recovery：不変性、隔離、インテリジェンス

Cyber Recoveryヴォールト

PowerProtect Cyber Recoveryヴォールトは複数の保護レイヤーを備えており、内部関係者の脅威も含めたサイバー攻撃に対するレジリエンスをもたらします。重要なデータを攻撃対象から遠ざけ、データセンター内の保護された場所に物理的に隔離し、アクセスに際しては別のセキュリティ認証と多要素認証を求めます。さらなる安全対策として、自動化された運用上のエア ギャップによりネットワークを隔離し、侵害される可能性のある管理インターフェイスを排除できます。PowerProtect Cyber Recoveryは、オープン システムやメインフレームを含む本番稼働システムとヴォールトの間におけるデータの同期を自動化し、保持ロック ポリシーを使用して不変コピーを作成します。サイバー攻撃が発生した場合、迅速にクリーンなデータ コピーを特定し、重要なシステムを復旧し、通常業務を再開させることができます。



CyberSense

PowerProtect Cyber Recoveryは、CyberSenseを完全に統合した初めてのソリューションです。CyberSenseは、攻撃がデータセンターに侵入した際に、データの破損を発見するためのインテリジェントな保護レイヤーを追加します。この革新的なアプローチは、フルコンテンツ インデックス作成機能を提供し、AIベースの機械学習(ML)を使用して200以上に及ぶコンテンツベースの統計情報を分析し、ランサムウェアによる破損の兆候を検出します。CyberSenseは、最大99.5%の信頼度で破損を検出することにより、ヴォールトのセキュリティ内のビジネスクリティカルなコンテンツを保護しながら、脅威の特定と攻撃ベクトルの診断を支援します。

リカバリーと修復

PowerProtect Cyber Recoveryは、ビジネスクリティカルなシステムを迅速かつ確実に再開させるための、自動化されたリストアとリカバリーの手順を提供します。リカバリー機能は、お使いのインシデント対応プロセスと統合できます。イベントが発生すると、インシデント対応チームは本番環境を分析して、イベントの根本原因を特定します。CyberSenseは、攻撃の深度と範囲を把握するための攻撃後のフォレンジック レポートや、破損前の最後の正常なバックアップ セットを示すリストも作成します。その後、本番環境のリカバリーを行う準備が整ったら、Cyber Recoveryの管理ツールとテクノロジーを利用して実際のデータ リカバリーを実行できます。このようにして、リカバリーやセキュリティ分析に使用される復元ポイントの作成を自動化します。

ソリューションの計画と設計

オプションのDell Advisory Servicesでは、お客様が保護すべきビジネスクリティカルなシステムを決定し、関連するアプリケーションとサービスの依存関係マップの作成、それらを復旧するために必要なインフラストラクチャの構築を行えるよう支援します。また、このサービスでは、リカバリー要件と設計の代替案を作成して、データの分析、ホスティング、保護を行うためのテクノロジーを特定し、ビジネス ケースと導入スケジュールを提示します。

重要なデータをサイバー攻撃から保護するには、実証済みかつモダンでレジリエンスに優れたソリューションが必要です。PowerProtect Cyber Recoveryを利用すると、サイバー攻撃を受けた後に、既知の正常なデータを迅速に特定してリストアし、通常業務を再開できるという安心感を得ることができます。

[1]デル・テクノロジーズの委託によりVanson Bourneが2023年10月に実施した調査『Global Data Protection Index 2023スナップショット』に基づきます。

Dell PowerProtect Cyber Recovery の詳細はこちら	デル・テクノロジーズのエキスパートに問い合わせる	他のリソースを見る	#PowerProtect で会話に参加