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、お客様の貴重なデータを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 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。

データの不変性
変更不可能なデータ コピーを作成することで、何層ものセキュリティと制御により、データの整合性と機密性を保持します。

自動化されたデータ隔離
変更不可能なデータコピーを本番環境のバックアップから、アクセス制限が強化された安全なデジタル ヴォールトに自動的に隔離します。

インテリジェント分析
AIベースの機械学習とフルコンテンツ インデックス作成を使用した自動整合性チェックに、安全なヴォールト内で行われる徹底した分析を組み合わせることで、データがマルウェアによる影響を受けているかどうかを判断します。

リカバリーと修復
動的なリストア プロセスと既存のディザスター リカバリー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、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です。

課題：データ主導型ビジネスを脅かすサイバー攻撃。

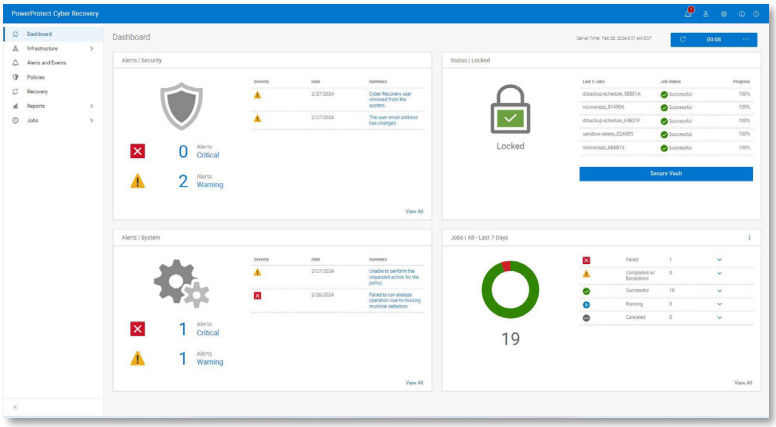
デジタル経済において、データは通貨であり、重要な資産となるため、保護、機密性の保守が必要なだけでなく、アクセスのしやすさも必要になります。現代のグローバル市場は、相互接続されたネットワーク間を流れ続けるデータに依存しています。デジタル トランスフォーメーションの取り組みや生成AIの使用の増加により、機密情報の露出リスクが高まっています。

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]。

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。



PowerProtect Cyber Recoveryは、重要なデータを隔離して不審なアクティビティーを特定することで迅速なデータ復旧を実現する実績のあるレジリエンスに優れた最新でインテリジェントな保護機能を提供します。重要なデータをスマートに復旧し、素早く通常業務に戻れることができます。Forrester Consultingの調査によると、サイバー攻撃が発生した場合、Dell PowerProtect Cyber Recoveryはダウンタイムを75%削減し、リカバリーに費やす時間を80%短縮すると報告されています。[2]

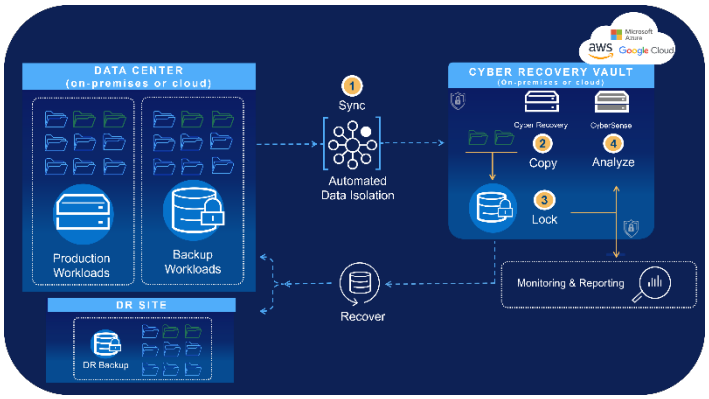
PowerProtect Cyber Recovery：不変性、隔離、インテリジェンス

不変性 - PowerProtect Data Domain

PowerProtect Data DomainはDell PowerProtect Cyber Recoveryの基盤となります。何層にもわたるゼロトラスト セキュリティで、データの整合性と機密性を確保するための不変バックアップ コピーを提供します。ハードウェア ルート オブ トラストやセキュア ブート、暗号化、Retention Lock、ロール ベースのアクセス、多要素認証などの機能により、データの復旧可能性を確保します。

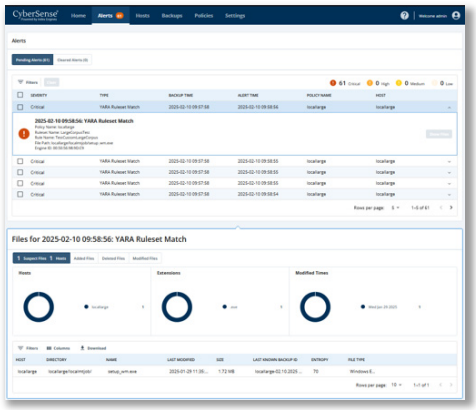
隔離 - Cyber Recoveryヴォールト

PowerProtect Cyber Recoveryヴォールトは、複数の保護レイヤーを備える隔離環境で、内部からのサイバー攻撃にも耐えることができます。その自動化されたデータ隔離機能により、重要なバックアップ データ（オープン システムやメインフレームを含む）は本番環境の攻撃対象領域から離れた、物理的に隔離されたヴォールトに安全にコピー（同期）されるため、管理パスが脅威アクターに公開されることはありません。次に、不変コピーが自動的に作成され、データの変更が防止されます。専用の管理、ネットワーク、サービスは本番環境から独立しており、リカバリー作業やテスト作業のためにデータにアクセスするには、個別のセキュリティ認証と多要素認証が必要です。



インテリジェンス - 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。すべてがCyber Recoveryヴォールトのセキュリティ内で行われるよりスマートな復旧です。CyberSenseは、メタデータのみのソリューションにとどまらず、フルコンテンツ分析により、攻撃後のデータ破損を99.99%の精度で検出し[3]、インテリジェントかつ迅速なリストアを容易にします。CyberSenseは、不変のデータ バックアップを活用してデータの経時的な変化を観察し、AIベースの機械学習を利用してランサムウェア攻撃による破損を示唆する兆候を検出します。CyberSenseは、巧妙な攻撃によって発生するコア インフラストラクチャ（Active Directory、DNSなど）やユーザー ファイル、データベース内の大量の削除、全体または一部の暗号化、その他不審な変更を検出します。カスタムの警告しきい値を作成することができ、破損の兆候が検出されるとアラート ダッシュボードと攻撃後のフォレンジック レポートにより、データのクリーン コピーの特定など、攻撃の規模と影響を迅速に診断して、重要なシステムを復旧します。カスタムYARAルールとマルウェア シグネチャー検索により、組織がサイバー脅威からプロアクティブに防御できるようにカスタマイズし、強化することができます。



PowerProtect Cyber Recovery – 導入オプション

ハイブリッドおよびマルチクラウド環境におけるCyber Recovery

重要なデータは、オンプレミスに存在することもあれば、異なるデータセンターに併置されていることも、複数のクラウドやリージョンにグローバルに存在することもあり、ビジネス全体のさまざまな場所に存在し得ます。そのため、場所に関係なく、サイバー攻撃からのリカバリーが必要な場合は、データの安全と不正アクセスや侵入が行えない状態を確保する必要があります。

PowerProtect Cyber Recoveryは、*AWS*、*Microsoft Azure*、*Google Cloud*向けのパブリッククラウド マーケットプレイスから利用および取引が可能で、迅速にアクセスしてクラウド内のサイバー リカバリー ヴォールト内のデータを保護します。PowerProtect Cyber Recoveryは、本番稼働システムとパブリッククラウド内のサイバー リカバリー ヴォールト間の重要なデータの同期を自動化します。標準的なクラウドベースのバックアップ ソリューションとは異なり、管理インターフェイスへのアクセスはネットワーキングの制御によってロックダウンされ、アクセスには別のセキュリティ認証情報と多要素認証が必要になります。複数のクラウドにデータを分散させたり重複させたりすると、セキュリティ リスクやコンプライアンス リスクの他、同期に関する問題やリソース コストの増加を招く可能性があります。このアプローチによって、さまざまな環境での可視性が低下し、日々進化するサイバー脅威からの保護が不十分になる可能性もあります。

Dell PowerProtect Data DomainオールフラッシュReady Node

重要なデータが増加し続ける中、ビジネス継続性とサイバー レジリエンスを確保するためには、サイバー イベントから迅速かつ効率的に復旧できることが最重要事項になります。重要なデータの管理が拡大している組織は、Cyber Recoveryヴォールトなど、隔離されたリカバリー環境からのデータ取得に優れている必要があります。Dell PowerProtect Data DomainオールフラッシュReady Nodeは、エネルギー効率とコスト効率が高く、合理化されたサイバー リカバリー ソリューションを提供します。強化されたCyberSense分析や高速リストアの機能を備え、組織のSLAに準拠します。使用するハードウェア、スペース、エネルギーが削減されることで、組織はデータ アクセス速度と運用効率を向上させて、データの整合性を確保できるようになり、最終的にはダウンタイムと全体的なメンテナンス コストの低減につながります。

PowerProtect Cyber Recovery – 業務の再開

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を作成します。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。

ソリューションの計画と設計

Dell Professional Services for Cyber Recovery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を作成できる他、復旧に必要なインフラストラクチャを構築できます。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。

まとめ

Sheltered Harborなどの業界による取り組みでは、バックアップを含む基幹システムに障害を引き起こすサイバー攻撃の際に、お客様や金融機関、米国の金融システムに対する国民の信頼を守るために、PowerProtect Cyber Recoveryを活用しています。CyberSenseを備えるCyber Recoveryは、何千社もの企業で利用され、多くのビジネス リーダーに自信を持って利用していただいています。サイバー脅威の発生時には、迅速なデータの復旧が立証されています。

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。

いつもの仕事に戻りましょう。

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

他のリソースを表示

#PowerProtectで会話に参加

[1]デル・テクノロジーズの委託によりVanson Bourneが実施した調査『Global Data Protection Index 2024スナップショット』に基づきます。（2023年10月）に基づきます。
[2]デル・テクノロジーズの委託によりForrester Consultingが実施した調査『Dell PowerProtect Cyber RecoveryのTotal Economic Impact』（2023年8月）
3 Index Enginesの委託によるESGのレポート、『Index EnginesのCyberSenseはランサムウェアによる破損の検出で99.99%の有効性を立証』に基づきます。2024年6月