DELL Technologies

ソリューション概要

Dell PowerProtect Cyber Recovery for Microsoft Azure

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パブリッククラウド ヴォールト

PowerProtect Cyber Recovery for Azureを導入する理由

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。

データの隔離とガバナンスAzureを使用する隔離されたデータ ヴォールト環境では、内部ネットワークやバックアップ ネットワークから切り離され、アクセスが制限されます。

自動化されたコピーとエア ギャップ本番環境とヴォールト環境の間の運用上のエア ギャップにより保護されている安全なデジタル ヴォールトに保護対象のデータをコピーします。

リカバリーと修復動的なリストア プロセスと手順を用いてインシデントからリカバリーするためのワークフローとツールを活用できます。

ソリューションの計画と設計重要なデータ、アプリケーション、さらに完成度と信頼性の高いソリューションに基づいて構築されたその他の資産を選択するために、デル・テクノロジーズのエキスパートによるガイダンスを得られます。

導入の簡略化
Azure Marketplaceを通じてシンプルに購入、導入できるため、パブリッククラウド ヴォールトを迅速に利用できます。

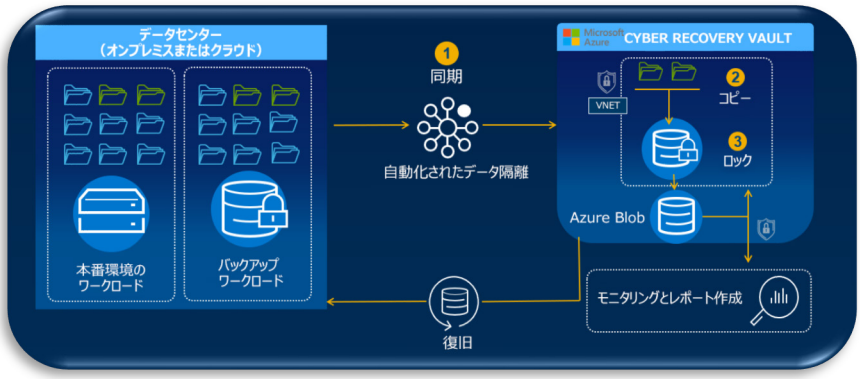
データ主導型組織を脅かすサイバー攻撃

組織の保護はデータの保護から始まります。サイバー脅威の状況は絶えず変化しており、テクノロジーの向上にともない拡大を続けています。攻撃者の新たな戦略はマルウェアやランサムウェアからデジタル恐喝へと移行し、攻撃によって機密性の高い企業の内部データが外部に公開されてしまう状況が続いています。サイバー攻撃の新たな脅威や、データの機密性、可用性、完全性を維持することの重要性などの観点から、特に現在のデータ主導型の企業、学校、組織にとっては、重要なデータとシステムを保護するために最新のソリューションと戦略が必要です。

攻撃が止むことはなく、攻撃あたりの損失額は増加の一途をたどっています。また、特定の規模の企業や業界のみが攻撃の標的になると誤解されがちですが、実際には、あらゆる規模、あらゆる分野の企業が標的になります。

サイバー攻撃による組織的なリスクを低減し、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。

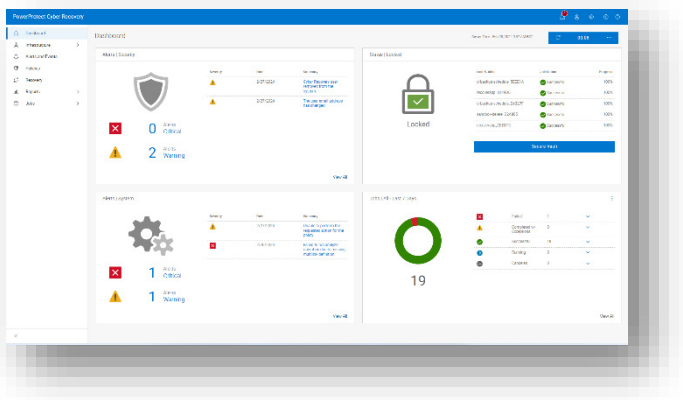
解決策：PowerProtect Cyber Recovery for Azure



Dell PowerProtect Cyber Recovery for Azureは、重要なデータを隔離し、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。

Azure内のCyber Recoveryヴォールト

PowerProtect Cyber Recovery for Azureは複数の保護レイヤーを備えており、サイバー攻撃や組織内部からの脅威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領域から移動し、Azure内で自動化された安全な運用上のエア ギャップを利用して物理的にも論理的にもアクセスから隔離します。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、アクセスには別個のセキュリティ認証情報と多要素認証を必須にすることができます。
PowerProtect Cyber Recoveryは、本番稼働システムとAzure内のサイバー リカバリー 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。



サイバー脅威によるビジネス リスクの軽減

自動化されたワークフローを通じて、ビジネス クリティカルなデータをAzure内の隔離された環境に安全に移動します。保護ポリシーを容易に作成でき、直感的なユーザー ダッシュボードを使用して潜在的な脅威をリアルタイムで監視することが可能です。ヴォールトは常に、運用上のエア ギャップを介して論理的に分離されます。ヴォールトのコンポーネントには本番環境からアクセスできず、エア ギャップのロックが解除された場合でもヴォールト ストレージへのアクセスは厳格に制限され、安全なAzure Virtual Network内で保護されます。
PowerProtect Cyber Recoveryは、本番システムと安全なヴォールト間でのデータ同期を処理し、新たなコピーを保護された形で作成します。サイバー攻撃が発生した場合、許可されたユーザーはすばやくデータにアクセスして重要なシステムのリカバリーを行い、組織的な稼働状況を復旧できます。

リカバリーと修復

PowerProtect Cyber Recovery for Azureは、重要なデータを迅速にオンラインに復帰させるための柔軟なリストアとリカバリーのオプションを備えています。また、テスト済みかつ文書化済みのリカバリー プログラムによってサポートされます。Cyber Recovery for Azureを利用すると、サイバー攻撃を受けた後やリカバリー テストを実施する際に、重要なデータをヴォールトからリカバリーできます。これにより、企業のデータセンターやそれに相当する場所、またはAzure内の新しいVNETやクリーンな環境へのデータ リカバリーが可能になります。

ソリューションの計画と設計

組織のニーズに対応するサイバー リカバリー プログラムの戦略化、実装、適応、拡大に、Dell Technologies Servicesをご活用ください。エキスパート サービスには、保護とリカバリーの調整、サイバー リカバリー技術の導入、サイバー インシデントへの対応、チームへの最新スキルのトレーニングの提供などが含まれます。デルの業界エキスパートがお客様のチームと連携することで、保護対象となる重要なシステムやデータ、およびリカバリーを必要としているインフラストラクチャを特定できます。

導入の簡略化

PowerProtect Cyber Recovery for Azureは、Azure Marketplaceを通じて購入可能なサービスとして提供されます。このため、既存のAzureサブスクリプションを活用いただけます。デル・テクノロジーズは、シンプルな購入方式でDellのAzure向けデータ保護製品ポートフォリオをすばやくご利用いただけるように取り組んでいます。さらに、購入方法が柔軟なため、お客様のご希望の方法に応じて、Cyber Recovery for AzureをDellから直接購入することも、Azure Marketplaceから購入することもできます。

PowerProtect Cyber Recoveryは、サイバー攻撃を受けても、既知の正常なデータを保護、特定、復元し、通常の動作とコンプライアンスを維持できるという安心感をもたらします。

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	Azure Marketplace でオファーを見る	#PowerProtect で会話に参加