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です。これには次のものが含まれます。

1. **不変性**
   不変データは、変更や削除はできず、書き込みのみ可能です。DDシステムは、本番システムとサイバー ヴォールトの両方に不変バックアップを書き込めます。つまり、攻撃者がバックアップ システムへのアクセス権を何らかの手段で獲得したとしても、既存の保護されたコピーを変更、削除、侵害することはできません。[2] DDシステムが本番環境で作成するバックアップは即座に変更できなくなり、ヴォールトにコピーすることでセキュリティを強化できます。不変性については、このレポートの次のセクションで詳しく見ていきます。

2. **Retention Lock**
   DD Retention Lock機能を使用すると、事前に設定された期間、データは不変になります。ソリューションがデータをリテンション ロック状態にすると、ロック期間が終了するまで、いかなるユーザーやシステムもデータを削除または変更できません。[3]

   Retention Lockには、ガバナンス モードとコンプライアンス モードがあります。コンプライアンス モードでは、多くの規制基準を満たすことができます。DD Retention LockがSEC規則17a-4(f)(2)および240.18a-6(e)(2)、ならびにFINRA規則4511(c)で指定されたストレージ要件を満たしていることは、独立した第三者によって証明済みです。[4]この機能は、FDA 21 CFR Part11、サーベンス オクスリー法、IRS 98025および97-22、ISO規格15489-1、ならびにMoREQ2010を遵守する取り組みの支援にも役立つ可能性があります。[5]

   攻撃者は、Retention Lockを回避しようと、システムのクロックを変更する可能性があり、それが成功すれば、ソリューションがファイルを本来よりも早く削除してしまいます。そのため、DDにはセキュリティ クロックが内蔵されています。システムは、セキュリティ クロックとシステム クロックの時刻を定期的に比較します。この2つの間に1暦年で時間のずれが累積して2週間になると、システムはDDファイル システム(DDFS)を自動的に無効にして、データへのアクセスを阻止します。[6]

3. **DDBoostによる実行データの暗号化**
   実行データは、重大なセキュリティ リスクをもたらす可能性があります。DDBoostは、バックアップ サーバーやアプリケーション クライアントが、すべてのデータではなく一意のデータ セグメントのみをネットワーク経由でDDアプライアンスに送信できるようにすることで、実行データの量を制限します。さらに、データの認証と暗号化に、証明書の有無にかかわらず、DDBoostプロトコルを使用できます。証明書があると、データ転送機能のセキュリティが高まります。実行暗号化を使用すると、アプリケーションは、システムからLANを介してバックアップまたはリストアする実行データを暗号化できます。クライアントは、TLS (Transport Layer Security)を使用して、クライアントとシステム間のセッションを暗号化できます。[7]

4. **DDオペレーティング システム(DD OS)セキュリティ**
   DDのセキュリティ機能の対象にはオペレーティング システムも含まれます。DD OSは、セキュリティを目的として、Bashシェルにカスタムのアクセス制御および制限を実装します。制限付きBashシェル モードでは、各自の役割やタスクに必要な事前定義されたコマンド一式のみ実行できます。DD OSは、不正な変更や意図しない変更をシステムに加える未定義コマンドをブロックして、データの整合性を強化します。[8]

5. ロール ベースのアクセス制御(RBAC)とDDファイル システム(DDFS)のセキュリティ

DDシステムでは、いくつかの手段を使用して、ファイル システム内のファイルやデータを保護します。まず、DDシステムはRBACを提供しており、管理者は特定の権限を持つロールを定義し、ユーザーを割り当てることができます。アプライアンスやそのデータには、適切な権限を持つ許可されたユーザーのみアクセスできます。これにより、ユーザーがアクセスできるのはタスクの実行に必要な機能とデータに限られ、不正なアクセスや偶発的なデータ露出のリスクが軽減されます。

また、DDFSでは、データの整合性検証にハッシュを使用します。ハッシュは、指定されたキーまたは文字列を別の値に変換します。アプライアンスが一意のデータ チャンクを論理ストレージ コンテナに保存し、ファイル システムがデータ チャンクとコンテナの両方をハッシュ化します。システムは、データを取得するとハッシュ値を再計算し、DDFSに保存されているハッシュ値と照合するため、データの改ざんや破損がないことの確認に役立ちます。[9]

6. 二重のロール承認

DD Retention Lockのコンプライアンス モードを有効にすると、DDシステムはデュアル サインオンの形で管理セキュリティを強化します。具体的には、システム管理者と、別の許可されたユーザー（セキュリティ担当者など）が、一緒にサイン オンする必要があります。DD Retention Lockのコンプライアンス モードにおけるデュアル サインオン メカニズムは、ロックされたファイルの整合性をリテンション期間の終了前に損なうおそれのあるアクションへの保護手段として機能します。[10]

7. Data Invulnerability Architecture

DD OSは、エンドツーエンドの検証、障害の回避と抑制、継続的な障害の検出と修復、およびファイル システムのリカバリーを提供して、ハードウェアやソフトウェアの誤動作によるデータ整合性の問題から保護します。DDシステムがバックアップ ソフトウェアから書き込み要求を受け取ると、まず、データ セグメントのフィンガープリントを計算し、システムに保存されている既存のフィンガープリントと比較して、データ セグメントの冗長性を分析します。ディスクには、一意のデータ セグメントとそのフィンガープリントのみ保存します。続いて、ディスクからデータを連続的にリード バックし、そのフィンガープリントを再計算し、ディスク上のフィンガープリントと一致することを確認します。処理中に破損を検出した（すなわち、リード バックした内容が書き込んだ内容と一致しなかった）場合、DDシステムは自己修復プロセスを実行して、破損したデータを再構築し、データを正しい状態にリストアします。加えて、自己修復プロセスは、プラットフォームの整合性に影響を与えかねないその他の変更からシステムを保護するのに役立ちます。

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、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。

*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。

仕組み

DDシステムでは、データの保存方法に不変性を提供するのに、MTreeを使用します。MTreeは、ファイル システムの論理パーティションです。アプリケーションがMTreeにデータを書き込むと、DDシステムは高速コピーと呼ばれる機能を使用して、元のMTreeのポイントインタイム コピーを新しいMTreeに作成します。DDは、新しいMTree内でRetention Lockを適用して、保存期間によって定義されている期間中、ユーザーまたはプロセスが新しいMTreeを削除できないようにします。新しいMTreeはデータの不変コピーであり、元のMTreeからは独立しています。[11]

PowerProtect Cyber Recoveryソリューションでは、MTreeレプリケーションを使用して、不変データ コピーを本番DDからヴォールト内の別のDDに、DDBoostプロトコル経由で安全に複製することもできます。[12] 2つのDDS間の初期同期において、このソリューションはすべてのデータをヴォールトDDにコピーします。以降の同期では毎回、新規または変更データ部分のみがコピーされます。このレポートで後述するCyberSenseは、ヴォールト内のすべての不変コピーをスキャンして、破損の可能性がないかを確認します。

不変性へのアプローチ

不変バックアップを削除する必要性が生じることは、まれですが実際にあります。削除できない不変バックアップが蓄積されると、組織は容量の問題とそれに伴うコストの問題に直面する可能性があります。バックアップの保存には膨大な容量が必要になる場合があり、ハードウェアへの初期投資に加えて、継続的な運用、管理、監視のコストが必要になります。こうした問題の解決には、不変バックアップの定期的な削除が役立つ可能性があります。

前述のとおり、Dell PowerProtect Cyber Recoveryは、Retention Lockなどのツールを活用して不変性を提供しています。Retention Lockにはある程度の柔軟性があり、コンプライアンスとガバナンスという2つのモードによって、不変性の実装方法をわずかに調整できます。不変性とは、ユーザーや攻撃者がバックアップを削除できないことを意味しますが、ストレージ容量の問題などがある場合、PowerProtect Cyber RecoveryではRetention Lockのガバナンス モードを使用するとバックアップの削除が可能です。

PowerProtect Cyber Recoveryと比べて、他社の類似製品はどの程度の機能を備えているでしょうか？Cohesity Cyber Recovery、Veeam、Rubrik、Veritas NetBackupの公開情報を調査しました。Cohesity Cyber Recoveryを除き、ソリューションはオンプレミスまたはクラウドに配置できます（CohesityはAWSを基盤とするクラウドベースのソリューション）。4社のソリューションとも、ドキュメントには不変性を提供していると記載されていますが、RubrikおよびNetBackupにはPowerProtect Cyber Recoveryと明らかに異なる点があります。

Rubrikの場合、管理者はバックアップを削除できますが、クライアント側からは削除できないほか、特定の制御が設定されている場合に限られます。さらに、すべての書き込みは「アウトオブプレース」であり、新しい書き込みは以前書き込まれたデータに一切触れません。[13]

NetBackupも不変性を提供していますが、管理者や攻撃者は、NetBackup WORM対応ストレージ内のバックアップのロックを削除できます。そのうえで、bpexpdateコマンドを使用してイメージを削除できます。[14]

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。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。PowerProtect Cyber Recoveryでは、バックアップ データが本番ネットワークから物理的に切断され、分離された場所に保存される物理エア ギャップと、ネットワーク アクセス制御を使用して、論理的に切断されたバックアップ コピーを本番環境から分離する論理エア ギャップの両方を使用できます。両タイプのエア ギャップに対応していることに価値があります。論理エア ギャップだけでは、ヴォールトにネットワーク経由でアクセスできる内部ユーザーによるデータ アクセスやデータ侵害を阻止できないからです。

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。[15] 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ます。また、出典16にあるとおり、分離されたデータへのアクセスには、個別のセキュリティ認証情報と多要素認証(MFA)が必要です。[16]

分離へのアプローチ

Gartnerは、「分離されたリカバリー環境(IRE)に不変データヴォールト(IDV)を備えることで、インサイダー脅威やランサムウェアなどのハッキング形態に対し、最高レベルのセキュリティとリカバリーが実現される」と述べています。[17] 同社はまた、「IDVを備えたIREは、影響を受けたシステムをリカバリーするためのすべてのツール、プロセス、リソースを備えており、第3の不変バックアップ コピーを提供することで、従来のバックアップおよびディザスター リカバリー(DR)システムの代替ではなく、むしろ補完となっている」と指摘しています。[18]

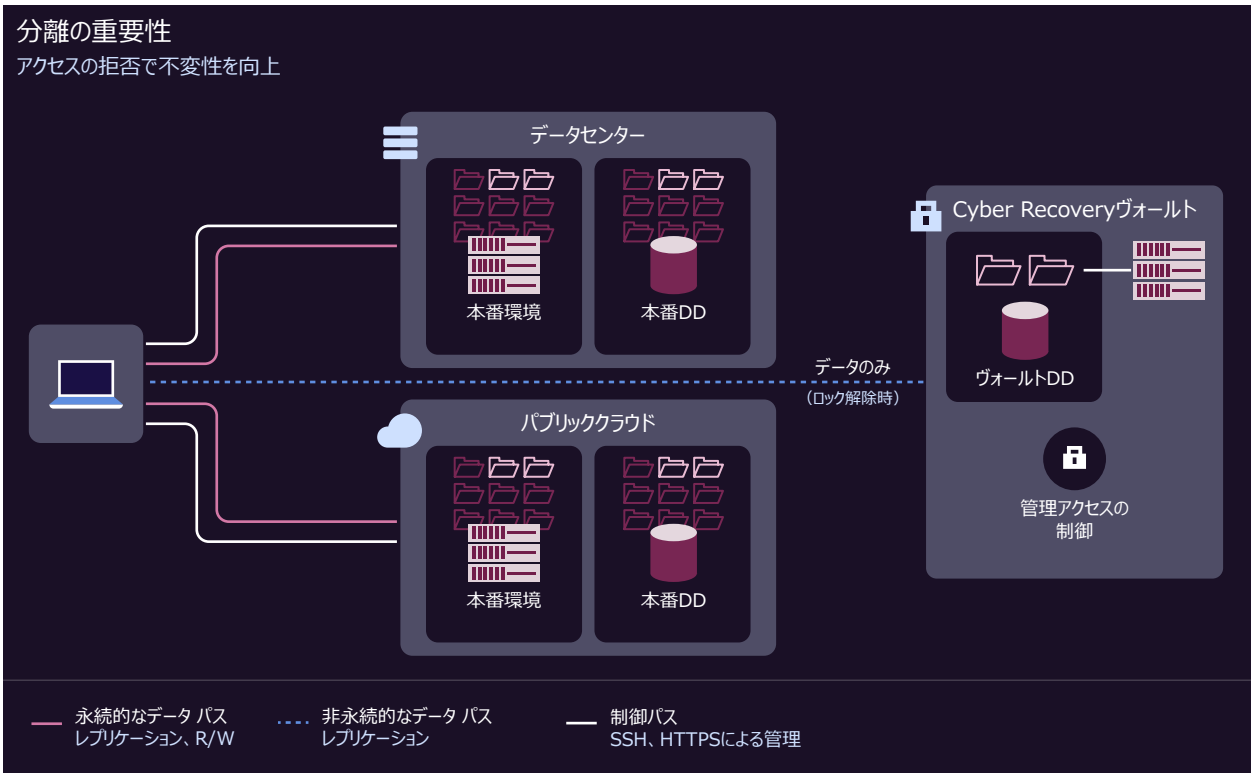
Cohesity、Veeam、Rubrik、Veritasの各ソリューションに関する公開情報を確認したところ、IREへのアプローチがPowerProtect Cyber Recoveryとは少なくとも若干異なっていることがわかりました。Dellのソリューションでは、DDヴォールトを本番環境から物理的または論理的に分離し、本番環境の制御プレーンやデータ プレーンをヴォールトとは別にできます。また、PowerProtect Cyber Recoveryではエア ギャップが自動化されており、これは一部の他社製品にはない機能です。

ドキュメントによると、

- Cohesity Cyber Recoveryは、AWSベースのFortKnoxヴォールトに対して、動的かつ自動化された論理エア ギャップのみ提供します。[19]
- Veeamは、Veeam Cloud Connectでパブリッククラウドやプライベートクラウドのプロバイダー向けに論理エア ギャップをサポートしていますが、自動化はされていません。また、Veeam Hardened Repositoryを提供しており、これはソリューションのオンプレミス ヴォールトとして機能し、物理エア ギャップを持つように構成できます。[20]
- Rubrikは、Rubrik Cloud Vaultに自動エア ギャップを提供していませんが、Microsoftとのサードパーティー パートナーシップを通じて論理エア ギャップを追加できます。[21]
- NetBackupでは、論理エア ギャップを手動で有効にする必要があります。また、オンプレミスやオフプレミスのソリューションで物理エア ギャップを作成できます。[22]

仕組み

図1に、分離されたCyber Recoveryヴォールトのネットワーク パスを示します。ご覧のように、ヴォールトには本番環境への管理パスも制御パスもなく、攻撃対象領域が縮小されています。



1 Cyber Recoveryヴォールトの概要レベルのデータおよび制御パス アーキテクチャ。出典 : Principled Technologies

Cyber Recoveryヴォールトに必要な接続は、定期的なデータ同期のためのデータ パスのみです。ここでの同期とは、Cyber Recoveryソリューションがレプリケーションのために、ポリシー主導の短い間隔でデータを取得することです。[23] 『PowerProtect Cyber Recovery Solution Guide』では、次のように記述されています。「Cyber Recoveryソリューションの基本的なアーキテクチャは、PowerProtect DDシステムのペアと、Cyber Recovery管理ホストという構成です。この基本構成では、管理ホスト上で実行されているCyber Recoveryソフトウェアが、Cyber Recoveryヴォールト内のPowerProtect DDシステムにおいて、レプリケーション用Ethernetインターフェイスとレプリケーション コンテキストの有効と無効を切り替えることで、本番環境からヴォールト環境へのデータ フローを制御します」[24] Dellは、データ パスを保護および分離するための方法をほかにも提案しています。テストでは、レプリケーション中およびレプリケーション後に、Cyber Recoveryがヴォールトをアンロックおよびロックすることが確認されました。

ヴォールトの物理的な実装について、Dellは次のように述べています。「Cyber Recoveryヴォールト機器は、物理的なアクセス制御を備えた専用の部屋またはケージに設置することをお勧めします。この安全な部屋には、鍵の貸し出し管理や鍵の使用は2人以上でのみ行うなど、制限付きアクセス リストを備える必要があります。ケージまたは部屋の入り口や機器のビデオ監視を導入する必要もあります。セキュリティを最大限確保するには、Cyber Recoveryソフトウェアへのアクセスを、Cyber Recovery管理サーバーとそれに関連付けられたキーボードとマウスによる物理アクセスに限定する必要があります」[25]

Cyber Recoveryの物理および論理エア ギャップによる分離オプションは、管理パスと制御パスの分離によって他のソリューションと一線を画しています。ソリューションのなかには、本番環境のインターフェイスからヴォールト データにアクセスできるものがあります。その場合、ヴォールト データが本番データと同じ攻撃対象領域に置かれ、侵害された認証情報を使用して攻撃者がバックアップ コピーにアクセスするおそれが生じます。

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は分析エンジンであり、ヴォールト内のバックアップやバックアップ内のファイルのユーザー コンテンツをスキャンし、AIベースのML分析アルゴリズムを使用してその整合性を検証します。

CyberSenseはヴォールト内で実行されており、本番環境とは分離されています。ヴォールト内のファイル、VMイメージ、データベースを監視し、データの整合性を分析することで、攻撃が発生したかどうかを判断します。Cyber Recoveryソリューションがバックアップ コピーをヴォールトに複製し、Retention Lock機能を適用すると、CyberSenseはそのコピーを自動スキャンし、ファイル、データベース、コア インフラストラクチャのポイントインタイムの観察記録を作成します。この分析エンジンは、メタデータだけではなく、ファイルや各データベース ページのコンテンツ全体をスキャンします。他のソリューションがデータしきい値やメタデータの変更を探すのに対し、CyberSenseはファイルの内容を調べてデータの整合性を検証します。こうした観察記録をもとに、CyberSenseはファイルやデータベースの経時変化を追跡し、多くの高度な隠れた攻撃を明らかにします。さらに、ファイルの暗号化、削除、作成、難読化など、不正行為を示している可能性のある破損パターンを検出したことを示す分析結果を生成します。[26] 他のソリューションは分析をクラウドで行うため、攻撃対象領域が拡大するおそれがありますが、CyberSenseでは、オンプレミスまたはCyber Recoveryがサポートする多くのクラウド オプションのどちらで実行するかを選択できます。

CyberSenseでは、200を超える分析にデータ観測記録を組み合わせており、観測記録は蓄積されるにつれてその有用性が高まります。MLアルゴリズムが、マルウェア感染に関する数千件の情報を基に、異常な行動パターンを見つけてユーザー活動とランサムウェアを区別し、偽陽性や偽陰性を最小限に抑えます。このアルゴリズムは、継続的な調査を通じて、攻撃の亜種などに関して新たな訓練を受けます。また、既存のCyberSenseの顧客から得られた実際のデータに基づく最新情報を受け取ります。[27]

さらに、CyberSenseは、Dell、IBM、CommVault、Veritasの一般的なディスク バックアップ形式でのデータのインデックス作成をサポートしています。[28] 他ベンダーのバックアップ形式をサポートすることで、Dellはデータ バックアップに関してお客様の現状に対応する姿勢を示しています。

Dell PowerStore™ 7000Tに搭載されたCyberSense for Dell PowerProtect Cyber Recovery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等の機能を持つツールという、2つのターンキー エンタープライズ データ保護およびサイバー リカバリー ソリューションのインテリジェントなML主導分析ソフトウェアについて、同等規模のアプライアンスを使用してテストしました。

テスト方法

すべてのテストをリモートで実行し、テストベッドへのアクセスや制御は制限なく自在に行うことができました。Dellのソリューション（CyberSense、PowerProtect Data Managerバックアップ アプリケーション、APEX Protection Storage（旧DD Virtual Edition）、PowerProtect Cyber Recoveryソリューションなど）とベンダーXのソリューションは、どちらもオフサイトのデータセンター ラボに配置しました。

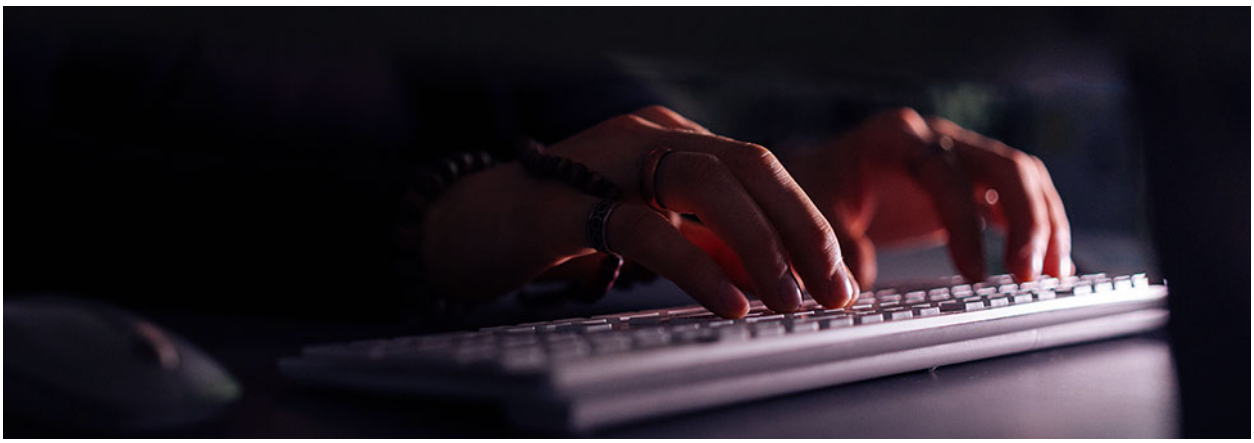
どちらのソリューションでも、バックアップを対象とした、スクリプトベースの悪意のあるイベント シナリオを3種類実行しました。

図2： 使用したテスト シナリオ。出典：Principled Technologies

どちらのソリューションでも、最初の2つのシナリオでは同じ一般的な手順に従いました。まず、Dell PowerProtect Data ManagerとベンダーXのストレージ アプライアンス上で、完全にクリーンなVMのフル バックアップを作成してから、スキャン対象となる増分バックアップを作成し、ターゲット ソリューションが脅威を検出しなかったことを確認しました。これにより、攻撃スクリプトの実行対象にできるバックアップのベースライン セットが得られました。

次に、オペレーティング システムとアプリケーション タイプが異なる4つのVMに対し、ランサムウェア シミュレーション スクリプトを実行し、ターゲット アプライアンスから新しい増分バックアップを取得し、ターゲット分析ソフトウェアが暗号化の脅威を検出したかどうかを確認しました。

3つ目のシナリオ（SQL Serverページに感染）では、他の2つのシナリオと同様の手順に従いましたが、ここではSQL VMに焦点を当て、暗号化スクリプトではなくページ破損スクリプトを使用しました。スクリプトは単一のVM上で実行しました。



テスト結果

シナリオ1：難読化されたファイル名を持つ暗号化ファイルの検出

このシナリオでは、悪意のあるイベントとしてファイルの暗号化と名前の難読化をシミュレートし、ファイルのメタデータと内容を変更しました。このタイプの攻撃は一般にランサムウェアと呼ばれており、システムの所有者またはユーザーが所定の金額を支払うまで、悪意のあるソフトウェアがコンピューター システムへのアクセスをブロックするセキュリティ イベントです。米国のサイバーセキュリティ・インフラストラクチャ セキュリティ庁(CISA)は、「ランサムウェアやデータ恐喝による経済面および評判面への影響により、初期のシステム停止期間中、そして場合によっては長期にわたる復旧期間を通じて、あらゆる規模の組織が困難とコストを強いられました」と述べています。[29] バックアップの暗号化を検出できるインテリジェントな分析ソフトウェアを使用すると、データ保護戦略を強化でき、貴重な機密情報が保護される、サイバー攻撃によって手痛いダウンタイムが発生する可能性を抑えられます。

テストでは、両方のインテリジェント分析アプリケーションが、ファイル名の変更された暗号化ファイルを検出しました。ベンダーXのソリューションでは、感染を検出するまでバックアップ15個からなるベースライン（フル バックアップ1個と増分バックアップ14個）が必要でしたが、CyberSenseは1回のフル バックアップで感染を検出しました。つまり、ベンダーXのソリューションではCyberSenseと比べてバックアップが14個多く必要でした。

ベンダーXのソリューションによる不審なアクティビティの警告で示されたのは、何かが多くのファイルを削除し、同数のファイルを追加したことだけで、これはバックアップのエントロピー評価に基づく不審なアクティビティでした。[30] ベンダーXのソリューションでは、ファイルが暗号化されていたことや、ファイル名が変更されていたことは示されませんでした。これに対し、CyberSenseを使用したCyber Recoveryでは、何かが暗号化を行い、ファイル名を難読化したことを警告しました。

ベンダーXの結果は偽陽性の可能性を示しています。言い換えれば、ベンダーXのソリューションを使用して日次バックアップを実行していた場合、異常が検出されるまでに感染ファイルを14日間取得していた可能性があります。対照的に、CyberSenseはわずか1個のベースラインとなるバックアップから、感染とその詳細に関する情報を警告しました。この例のこの段階において、ベンダーXのソリューションでは本番ネットワークが14個の感染バックアップにさらされている可能性がありますが、Cyber Recoveryを使用するリカバリーは分離されたヴォールトから実行されるため、その心配はないことが保証されます。

図3： 各ソリューションで破損検出のベースライン作成に必要とされたバックアップの数。
出典：Principled Technologies

シナリオ2：ファイル名は元のままの暗号化ファイルの検出

このシナリオは最初のシナリオに似ていますが、暗号化されるファイルの元ファイル名が維持されたケースです。今回、変更の影響を受けたのはファイルの内容に限られ、ファイルのメタデータに影響はありませんでした。これは時限式ランサムウェアの可能性を示しており、その場合、一定の休止期間ののちに活動が開始されます。時限式ランサムウェアは、検出を回避してバックアップを標的にでき、組織が必要とするときにバックアップが感染済みで使用できなくなっているおそれがあります。[31] ファイルは、メタデータの変更がない場合、表面上は感染していないように見え、潜伏攻撃の隠蔽に寄与します。

テストでは、両方のインテリジェント分析アプリケーションが暗号化ファイルを検出しました。今回も、ベンダーXのソリューションでは、異常を検出するまで、14個の増分バックアップを含む15個のバックアップからなるベースラインが必要でした。CyberSenseは、わずか1個のフル バックアップからなるベースラインで異常を検出しました。

最初のシナリオと同様、ベンダーXのソリューションは、何かが多くのファイルを変更したことのみ警告しましたが、これはバックアップのエントロピー評価に基づき不審とされたものでした。何かがファイルを暗号化したことは示しませんでしたが、CyberSenseを使用したCyber Recoveryはそれを指摘しました。このような形の破損を検出しているということは、CyberSenseが表面的なメタデータだけではなく、ファイルの内容に目を向けていることを意味しています。このタイプのスキャンにより、バックアップのセキュリティ、ひいてはデジタル インフラストラクチャや資産全体のセキュリティがいっそう強化されます。CyberSenseは「本当の意味で」インテリジェント分析アプリケーションと言えるかもしれません。さらに、ソリューションでベースラインの作成に要したバックアップの個数が大幅に少なかったことから、CyberSenseでは破損を早期に検出できる可能性があります。組織のバックアップスケジュールによっては、何日も早まる可能性があります。

図4： 各ソリューションで破損検出に必要とされたバックアップの数。出典：Principled Technologies

シナリオ3：SQL Serverページの破損の検出

このシナリオでは、SQL Serverページを破損させる悪意のあるイベントをシミュレートしました。SQL Serverにおいて、データストレージの基本単位はページで、データベースはデータ ページ全体を読み書きします。[32] 今回も、変更の影響を受けたのはファイルの内容に限られ、ファイルのメタデータに影響はありませんでした。このタイプの攻撃は一般にSQLインジェクションと呼ばれており、攻撃者は、SQLデータに基づくアプリケーションを標的とし、Webページ入力を介してSQLステートメントに悪意のあるコードを注入します。[33] 感染した場合でも、データベースは実行を継続する可能性があります。データの盗難に加えて、SQL Serverページが破損すると、データの整合性の問題、データ ロス、データベース機能の中断が生じるおそれがあります。こうした事態になれば、組織の評判に傷がつき、業務の流れが混乱し、経済的損失を被りかねないほか、法的責任を問われるおそれもあります。

最初の2つのシナリオで、CyberSenseとベンダーXのソリューションはどちらも暗号化を検出しましたが、シナリオ3で、SQL Serverページの破損を検出できるほどの深部までスキャンできたのはCyberSenseだけでした。このことは、2つのソリューションがあるレベルでは同様の検出機能を提供しているのに対し、CyberSenseは、ビジネス クリティカルでありうるSQL Serverベースのアプリケーションのバックアップをより深いレベルまでスキャンできることを示しています。このように、CyberSenseは、より深いスキャンとより包括的な保護で、セキュリティ レジリエンスを強化しています。

SQL Serverは、金融、小売、医療などの業界で、多くのアプリケーションの原動力となっています。SQL Serverは開発アーキテクチャのバックエンドとして機能するため、SQL Server攻撃はダウンタイムを引き起こし、運用を中断させ、アプリケーションが生み出す収益を脅かすおそれがあります。

Dell PowerProtect Cyber Recoveryを使用したリストアとリカバリー

Dellのサイバー レジリエンス戦略では、幅広いリカバリー機能を提供しています。リカバリー オプションには、インスタント アクセスや、本番環境に保持されている不変バックアップを使用した従来型のリカバリーなど、業界標準の機能が含まれています。加えて、DellはPowerProtect Cyber Recoveryソリューションを通じて、独自のリカバリー機能を提供しています。PowerProtect Cyber Recoveryはコピーを分離して維持し、CyberSenseを使用して整合性をスキャンするため、攻撃を受けたらすぐコピーにアクセスしてリカバリー手順を開始したり、クリーン ルームなどの代替リカバリー プラットフォームへの即時リストアを実行したりできます。

この即時対応のユース ケースと比べて、本番環境かパブリッククラウドでしかデータにアクセスできない場合はどうでしょうか。根本原因を特定して修復し、攻撃者の永続的な侵入を排除し、保険会社や法務部門向けにフォレンジック イメージを取得し、データを再スキャンし、バックアップ インフラストラクチャへのアクセスに十分利用できるインフラストラクチャ（AD、DNS）を用意するまでは、侵害された領域に保存されているデータには安全にアクセスできません。このプロセスには、攻撃の範囲と巧妙さに応じて数日から数週間かかる場合があります。

仕組み

通常の本番運用において、PowerProtect Cyber Recoveryは、リカバリーおよびセキュリティ分析用のリカバリー ポイントを自動作成します。サイバー攻撃が発生した場合、Cyber Recoveryは、自動化されたリストアおよびリカバリー手続きと作成済みのリカバリー ポイントを使用して、ビジネス クリティカルなシステムをオンライン状態に戻します。CyberSenseとフォレンジック レポートは、サイバーセキュリティやリカバリーの担当チームが攻撃の影響を診断するのに役立ちます。本番環境がクリーンになり、リカバリーの準備が整うと、Cyber Recoveryは実際のデータ リカバリーを実行するためのツールとテクノロジーを提供します。

サイバー攻撃が発生すると、いくつかのデータ保護メトリックをもとに、リカバリーのスピード（サイバー リカバリー時間(CRT)）と、破壊的な攻撃後にユーザーが戻れる時点（サイバー リカバリー ポイント(CRP)）が決定されます。Cyber Recoveryソリューションでは、以下のメトリックも使用されます。

- **破壊検出目標(DDO)：**攻撃からその検出までの時間に基づくローリング ウィンドウ。分析などのCyber Recoveryメカニズムは、この期間内に稼動する必要があります。
- **破壊評価目標(DAO)：**侵入後、被害の範囲と可能な対応を判断するために、サイバーセキュリティ チームに割り当てられる時間。
- **Cyber Recovery同期間隔：**Cyber Recoveryソリューションが本番環境からヴォールトにデータをコピーする頻度。頻度は、ソリューション向けに以前確立された目標リカバリー ポイント(RPO)に基づくものです。コピーのリテンション期間はソリューションによって異なり、通常は1週間から1か月です。
- **Cyber Recoveryデータ コピー数：**Cyber Recoveryヴォールトに保持されているデータ コピーの数。このメトリックを同期間隔と組み合わせることで、データをどこまでさかのぼってリカバリーできるかの大まかな目安ができ、たとえばコピーが7個、間隔が24時間であれば、1週間前までのデータをリカバリーできます。

データの同期間隔とリテンション期間の決定には、リカバリー要件に加えて、ソリューションが保護するデータのタイプが役立つことがあります。『Cyber Recovery Solution Guide』によると、リカバリーの柔軟性を最大限に高めるため、ソリューションが保護するデータを次のバックアップ ストリームのいずれかに分類できます。[34]

- バイナリーおよび実行可能ファイルのバックアップ（オペレーティング システムのベースレベルのディストリビューションやアプリケーションのビルドを含む）
- アプリケーションやファイル システムのフル バックアップ（イメージやアプリケーション固有のデータを含む）

この別個のバックアップ ストリームに対して、2つの異なるリカバリー戦略が導かれます。

1. **Cyber Recoveryヴォールト内のデータやアプリケーション バイナリーのリストア：**
   このソリューションでは、使用可能なリストア ポイント、およびマルウェアとその存在箇所を特定し、マルウェアをバックアップ イメージからクレンジングするか、それともCyber Recoveryヴォールトのコピーを使用して再構築を行うかを判断します。セキュリティ パッチの適用後、アプリケーションのディザスター リカバリー ランブックを使用してデータをリカバリー ホストにリストアし、リカバリー処理によってマルウェアの影響が排除されたかどうかを判断します。次に、ヴォールト コンピューティングを使用してアプリケーションでテスト実行を実施し、本番環境のクレンジングまたは再イメージ化を実行します。最後に、リカバリー ホストを本番環境に接続し、アプリケーションやデータを本番環境にコピーします。このプロセスを図5に示します。

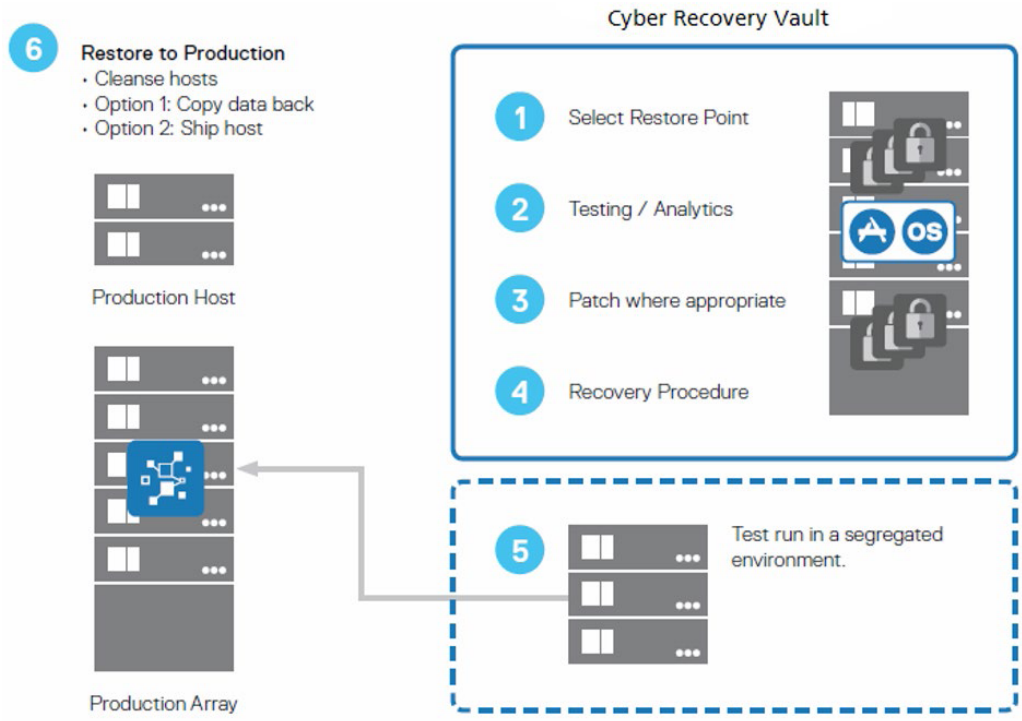
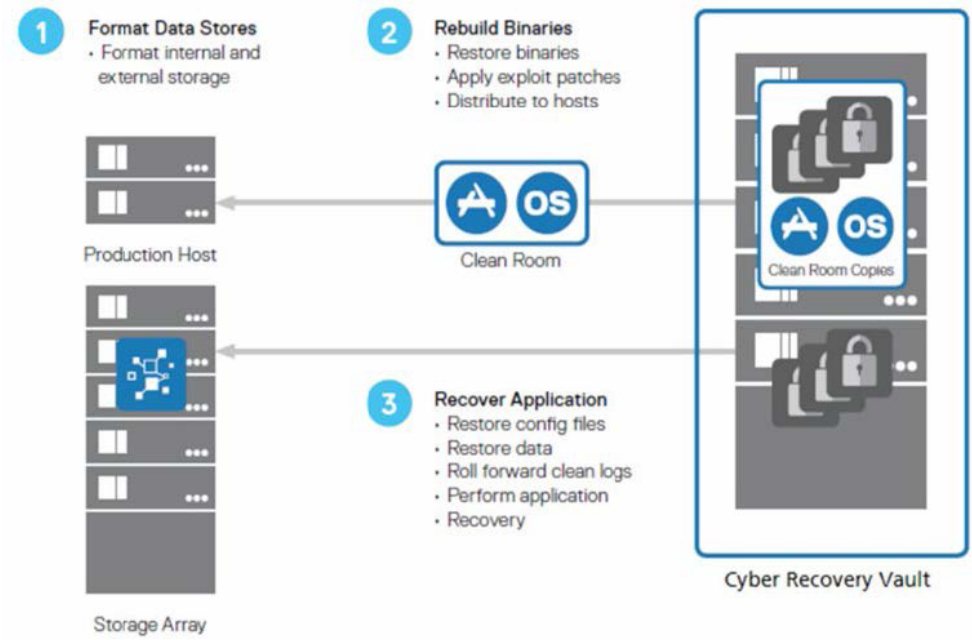


図5： データとアプリケーション バイナリーをリストアするプロセス。出典：デル・テクノロジーズ。[35]

2. **Cyber Recoveryヴォールトからの完全な再構築：**
このアプローチの場合、Cyber Recoveryソリューションは、インシデント対応中になされたフォレンジック評価で決定された損害レベルに基づき、本番システムを再構成します。その後、Cyber Recoveryヴォールトのコピーをもとにバイナリーを再構築し、使用可能なセキュリティ パッチを適用します。最後に、アプリケーションの関連ディザスター リカバリー ランブックに基づき、アプリケーション、データ、構成ファイルの正しいコピーを本番環境にリストアします。このプロセスを図6に示します。



6 Cyber Recoveryヴォールトから完全に再構築するプロセス。出典：デル・テクノロジーズ。[36]

Cyber Recoveryソリューションには、Cyber Recoveryソフトウェアがリカバリーに使用できる物理または仮想リカバリー ホスト（またはその両方）が含まれています。これらのホストには、バックアップ アプリケーション リカバリー サーバー（バックアップ アプリケーションとバックアップ アプリケーション カタログのリカバリー先となるサーバー）とアプリケーション リカバリー サーバーの両方が含まれています。組織は、ソリューションのリカバリー要件に応じて、複数のサーバーを導入できます。Cyber Recoveryソフトウェアは、サンドボックス（新規または未テスト ソフトウェアを安全に実行するためのテスト環境）データ コピーを任意のホストに公開して、ファイル システム データ、IBM/CommVault/Veritasのバックアップ データ、またはDell NetWorker、Dell Avamar、Dell PowerProtect DPシリーズ アプライアンス、Dell PowerProtect Data Managerソフトウェアによって保護されているデータなど、ヴォールト内のデータのリカバリーを実行できます。ヴォールト内でバックアップ アプリケーションをリカバリーした後、ソリューションはそのデータをヴォールト内の追加リカバリー ホストにリストアできます。

組織は事前に、バックアップ アプリケーション リカバリー サーバーの規模を、Cyber Recoveryソリューションが保護するすべてのバックアップ アプリケーションを復旧できるように設定しておきます。同様に、アプリケーション リカバリー サーバーは、ソリューションによるアプリケーションのリカバリー先となるサーバーです。アプリケーションによっては、先に他の依存アプリケーションをリカバリーしておく必要が生じる場合があります。ヴォールト内のインフラストラクチャは、ソリューションが保護する最大の本番アプリケーションのリカバリーをサポートできます。

結論

組織は、データ保護計画を策定する際、多くの攻撃ベクトルを考慮する必要があります。これには、すべてのデータの保護が含まれますが、何より大事なのは、運用に欠かせない重要なデータです。PowerProtect Cyber Recoveryは重要なデータを分離し、サイバー攻撃が発生した場合にデータを適切にリカバリーするのに役立ちます。Cyber Recoveryは、CyberSenseのMLベース分析を使用して、ヴォールト内のデータの整合性を判断し、リカバリーのためのクリーンなバックアップデータを特定します。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。競合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、競合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。これらすべてに加え、Cyber Recoveryソリューションは多くのリカバリー オプションを提供し、ヴォールトからの侵害されていないデータを活用して、運用を効率的かつシームレスに再開します。

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『Dell PowerProtect Cyber Recovery Solution Guide』（2023年8月23日にアクセス）https://www.delltechnologies.com/asset/en-us/products/data-protection/technical-support/h17670-cyber-recovery-sg.pdf
3. Dell、『Dell PowerProtect Cyber Recovery Solution Guide』
4. Cohasset Associates, Inc『Dell Technologies PowerProtect DD and DDVE – Compliance Assessment: SEC 17a-4(f), SEC 18a-6(e) and FINRA 4511(c)』（2023年10月27日にアクセス）https://infohub.delltechnologies.com/section-assets/cohasset-dell-powerprotect-dd-compliance-assessment
5. Dell「Data Domain：Retention Lockに関するよくある質問/FAQ」（23年9月12日にアクセス）https://www.dell.com/support/kbdoc/en-us/000079803/data-domain-retention-lock-frequently-asked-questions-faq
6. Dell「Data Domain：Retention Lockに関するよくある質問/FAQ」
7. Dell「Encryption types offered by DD series encryption appliance」（2023年9月8日にアクセス）https://infohub.delltechnologies.com/l/powerprotect-dd-series-appliances-encryption-software-1/encryption-types-offered-by-dd-series-encryption-appliance
8. Dell『Dell EMC Data Domain – Security Configuration Guide』（2023年9月11日にアクセス）https://www.delltechnologies.com/asset/en-us/products/data-protection/technical-support/docu91808.pdf
9. Dell「Role based access control (RBAC) in Data Domain」（2023年9月11日にアクセス）https://www.dell.com/community/en/conversations/data-domain/role-based-access-control-rbac-in-data-domain/647f70a9f4ccf8a8dee30f99
10. Dell『Dell EMC Data Domain – Security Configuration Guide』
11. 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

12. Veeam『Dell EMC Data Domain - DataDomain MTree overview and limits』（2023年9月11日にアクセス）https://bp.veeam.com/vbr/2_Design_Structures/D_Veeam_Components/D_backup_repositories/datadomain.html
13. Chris Wahl、『Recovering Fast from Ransomware Attacks: The Magic of an Immutable Backup Architecture』（2023年12月13日にアクセス）、https://www.rubrik.com/content/dam/rubrik/en/resources/white-paper/rwp-recovering-fast-from-ransomware-attacks.pdf。
14. Veritas『NetBackup™ Security and Encryption Guide』（2023年12月13日にアクセス）https://www.veritas.com/support/en_US/doc/21733320-149123528-0/v143394540-149123528
15. 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
16. Dell『Dell PowerProtect Cyber Recovery』（2023年9月12日にアクセス）https://www.delltechnologies.com/asset/en-us/products/data-protection/briefs-summaries/isolated-recovery-solution-overview.pdf
17. Jerry RozemanおよびMichael Hoeck『Innovation Insight for Leveraging Isolated Recovery Environments and Immutable Data Vaults to Protect and Recover From Ransomware』（2023年12月14日にアクセス）https://www.gartner.com/doc/reprints?id=1-27MOHCBD&ct=211011&st=sb
18. Jerry RozemanおよびMichael Hoeck『Innovation Insight for Leveraging Isolated Recovery Environments and Immutable Data Vaults to Protect and Recover From Ransomware』
19. Nikitha Okmar『Going Beyond the Air Gap - Data Isolation and Recovery for the Modern Era』（2023年12月13日にアクセス）https://www.cohesity.com/blogs/going-beyond-the-air-gap-data-isolation-and-recovery-for-the-modern-era/
20. Marco Horstmann『How to protect your data from ransomware and encryption Trojans』（2023年12月13日にアクセス）https://www.veeam.com/blog/how-to-protect-against-ransomware-data-loss-and-encryption-trojans.html
21. Rubrik『Rest easy with immutable, off-site data storage』（2023年12月13日にアクセス）https://www.rubrik.com/products/rubrik-cloud-vault
22. Veritas『NetBackup Isolated Recovery Environment』（2023年12月13日にアクセス）https://www.veritas.com/content/dam/www/en_us/documents/solution-overview/SO_flex_appliance_netbackup_ire_solution_V1543.pdf
23. CSI Group『Dell Cyber Recovery Vault (overview by CSI)』（2023年8月23日にアクセス）https://youtu.be/ej5nZzWNRM0
24. Dell、『Dell PowerProtect Cyber Recovery Solution Guide』。
25. Dell、『Dell PowerProtect Cyber Recovery Solution Guide』。
26. Dell、『CyberSense® for PowerProtect Cyber Recovery』。
27. Dell『CyberSense® for Dell PowerProtect Cyber Recovery – Powered by Index Engines』（2023年9月13日にアクセス）https://www.delltechnologies.com/asset/en-us/products/data-protection/industry-market/cybersense-for-dell-powerprotect-cyber-recovery-whitepaper.pdf
28. Index Engines『CyberSense for Dell Cyber Recovery』（2023年9月25日にアクセス）https://indexengines.com/csmatrix
29. CISA「#StopRansomware Guide」（2023年8月1日にアクセス）https://www.cisa.gov/stopransomware/ransomware-guide
30. 「セキュリティの分野ではたいてい、シャノンのエントロピーに基づく、0～8の値を返す特定のアルゴリズムが使用されています。値が大きいほどデータのランダム性が高く、多くの場合、値が大きいということは、データが圧縮または暗号化されていることを意味します」Mueller、Clint「How to Use Entropy Analysis in Penetration Testing」（2023年8月28日）https://www.schellman.com/blog/cybersecurity/penetration-testing-methods-entropy
31. Cooper、Steven「How to Protect your Backups from Ransomware in 2023」（2023年8月1日）https://www.comparitech.com/net-admin/protect-backups-from-ransomware/
32. Microsoft「Pages and extents architecture guide」（2023年8月3日にアクセス）https://learn.microsoft.com/en-us/sql/relational-databases/pages-and-extents-architecture-guide?view=sql-server-ver16
33. W3 Schools「SQL Injection」（2023年8月3日にアクセス）https://www.w3schools.com/sql/sql_injection.asp
34. Dell、『Dell PowerProtect Cyber Recovery Solution Guide』。
35. Dell、『Dell PowerProtect Cyber Recovery Solution Guide』。
36. Dell、『Dell PowerProtect Cyber Recovery Solution Guide』。

このレポートの背景情報を読む ▶

▶ オリジナルの英語版のレポートは https://facts.pt/64FU3b2でご覧いただけます

Principled Technologies®

Facts matter.®

このプロジェクトは、[デル・テクノロジーズ]の委託を受けて作成されています。