迅速かつ堅牢なサイバー リカバリー ソリューションでデータ保護計画を強化する

当社の調査によると、Dell Technologies PowerProtect Cyber Recoveryは、バックアップ ヴォールトの物理的な分離と、ランサムウェアの詳細なスキャンを提供できる

物理的なエア ギャップによるバックアップ ヴォールトの分離

データが通過できないように物理的な障壁を作成します

ランサムウェアの詳細なスキャン

CyberSenseは、メタデータだけでなく、ファイルのコンテンツとデータベースを参照します

2倍の異常ワークロードのスキャン

1つのツールで、マルウェアをより多くの場所で探し出すことができます

ランサムウェア攻撃の平均コストは、2年間でほぼ20%上昇し、523万米ドルとなっています。[1]効率的なサイバー リカバリー ソリューションは、インシデントからの迅速なリカバリー、データ ロスの削減、ダウンタイムの最小化、その過程でのブランドの整合性維持を達成できるよう組織をサポートして、これらの潜在的なコストを削減または回避するよう支援できます。攻撃後、既知の良好なデータを特定し、リストアすることで、組織はビジネス リスクとダウンタイムを最小限に抑えながら、重要なデータとシステムを救出することができます。

Dell PowerProtect Cyber Recovery (Cyber Recovery)はそのようなソリューションです。これにより組織は、ランサムウェア、破壊的なサイバー攻撃、予期しないイベントからデータとアプリケーションを保護することができます。このレポートでは、公開されたデータを基に、Cyber Recoveryとその競合ソリューションであるRubrik Security Cloud (RSC)の基本的なデータ保護機能や性能を比較検討しています。具体的には、サイバー リカバリー ソリューションのお客様が重要と考える可能性のある特長と機能（リカバリー ヴォールト、不変性、ワークロードのサポート、スキャン テクノロジー、復元性、分離など）について検討しました。

RSCとは異なり、Cyber Recoveryはマルチコピー アプローチを採用しており、バックアップを作成した後、保護と分析のためにそれらのバックアップ（または通常は選択したサブセット）を分離されたストレージにコピーします。Cyber Recoveryは、オンプレミスのPowerProtect Data Domainアプライアンス内に配置された、またはDell APEX Protection Storage for Public Cloudを介したクラウド上に配置された1つまたは複数のストレージ ヴォールトを含む、複数のコンポーネントからなるシステムです。これに対して、RSCはローカル ヴォールトのオプションを提供していません。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も含まれており、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ソリューションでは、Rubrikソリューションの2倍の異常ワークロードをスキャンできるため、CyberSenseスキャンML（機械学習）では、マルウェアやその他の脅威アクターのアクティビティーの影響をより多くのデータで検出できる可能性があります。PowerProtect Cyber Recoveryの動作の違いと、お客様の組織にとってより有利になる可能性について分析します。

製品概要

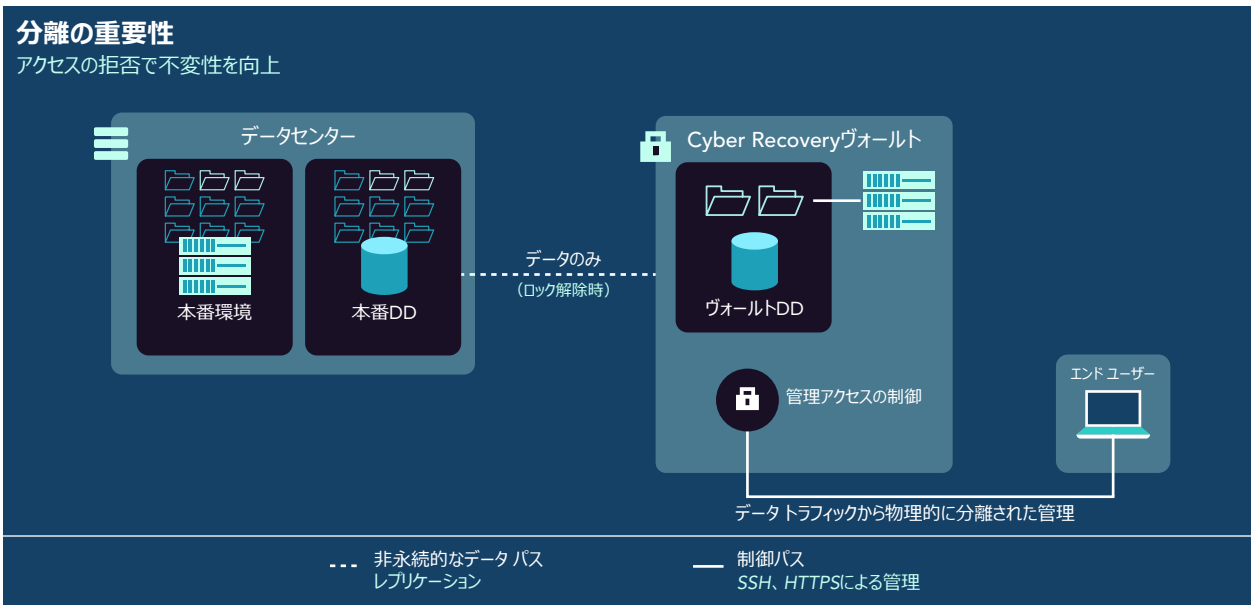
Dell PowerProtect Cyber Recoveryの概要

Dell PowerProtect Cyber Recoveryは、本番データを格納するストレージ アプライアンスと、ヴォールト内のレプリケーション用ターゲット ストレージ アプライアンスで構成されています。また、Cyber Recoveryソフトウェアも含まれています。これは同期の調整、Cyber Recoveryヴォールト内のPowerProtect Data Domain (PPDD)システム上の複数のデータ コピーの管理、リカバリー プロセスの監視、CyberSenseによる分析プロセスの監視を行います。

このソリューションは、MTreeレプリケーションを介して本番PPDD MTreeからヴォールトの対応する部分に一意のデータを転送し、設定された期間、データ不変性*を確保します。ヴォールトには、Cyber Recoveryソフトウェアを含むサーバーと、ソリューションがバックアップ アプリケーションおよびデータを復元するコンポーネントが含まれています。各Cyber Recoveryヴォールトには通常、そのような多くのコンポーネントが格納されています。ヴォールトには、データ分析ソフトウェアを搭載した分析/インデックスホストもあります。これにより、Cyber RecoveryソフトウェアとCyberSenseとの直接統合が可能です。

*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。

図1は、Dell Cyber Recoveryソリューションの概要を示しています。

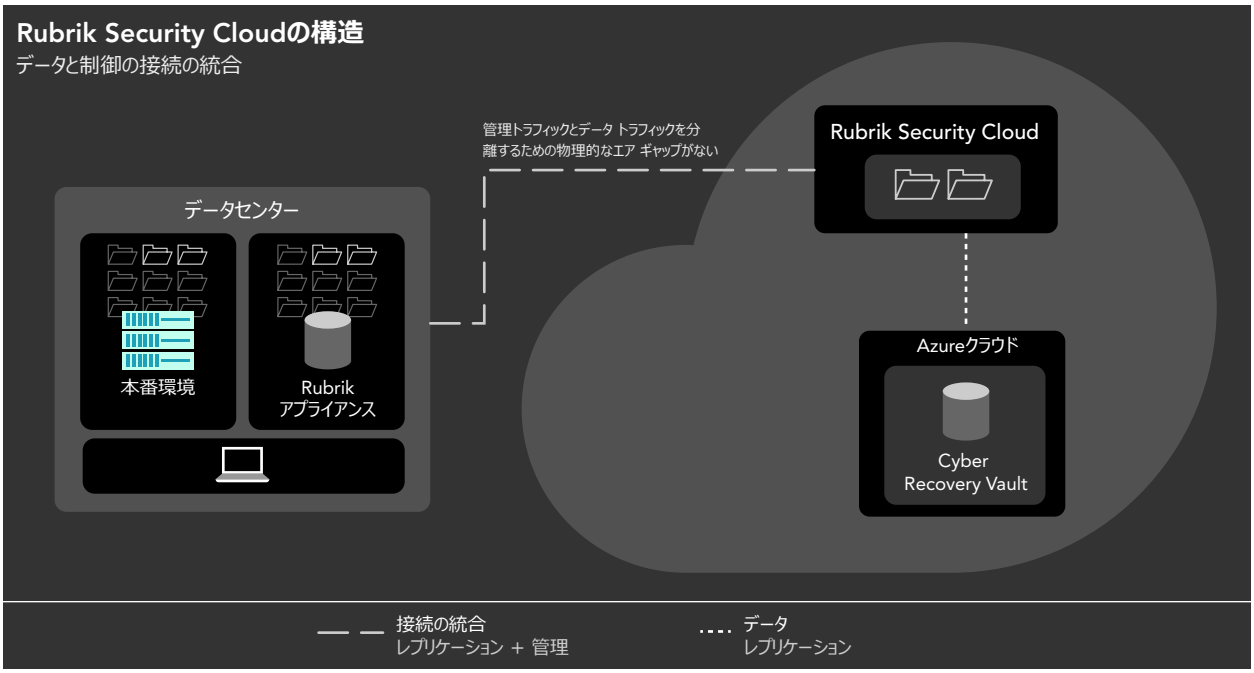


1 Cyber Recoveryヴォールトの概要レベルのデータおよび制御パス アーキテクチャ。出典：Principled Technologies

Dell PowerProtect Cyber Recoveryソリューションの主要コンポーネントの詳細については、『Dell PowerProtect Cyber Recoveryソリューション ガイド』を参照してください。

Rubrik Security Cloudの概要

Rubrikは、Rubrik Security CloudをSaaS（ソフトウェア アズ ア サービス）プラットフォームとして説明しており、これによってお客様は「データの安全性を維持し、データ リスクを監視して、データが企業全体、クラウド、SaaSアプリケーションのどこにあっても、それらのデータを迅速に復旧できる」としています。[4] Rubrikは、「高可用性サービスとGoogle Cloud Platform (GCP)で実行されるインフラストラクチャを使用した安全なマイクロサービス アーキテクチャ」上にソリューションを構築したと述べています。[5]図2はRubrik Security Cloudの一般的な構造を示しています。



2 Rubrik Security Cloudの一般的な構造。出典：Principled Technologies

サポート対象の機能

リカバリー ヴォールト

ヴォールトは、本番環境内でソリューションが取得するバックアップの暗号化コピーを格納する専用ストレージです。ヴォールトは本番バックアップ ソリューションの一部ではなく、それぞれが分離された「バックアップへのバックアップ」の場所として機能し、お客様は検証済みのバックアップをリカバリーできます。

Dellは、オンプレミス、リモート コロケーション サイト、パブリッククラウド内など、複数のヴォールト オプションを提供しています。オンプレミスのヴォールトでは、データセンターに配置されている運用上のエアギャップPPDDを活用します。これは、バックアップ ソリューションと同じラック内に配置することも可能です。エアギャップ ソリューションは通常、本番環境から物理的に分離されています。オフサイトのコロケーション ヴォールトには、オンプレミス バージョンのように、物理ヴォールトへの専用ネットワーク接続が必要ですが、ヴォールトはリモート データセンターに地理的に分離されています。また、Dellはパブリッククラウド内でヴォールトを提供しており、クラウド サービス プロバイダーのAmazon Web Services (AWS)、Microsoft Azure、Google Cloudと提携しています。パブリッククラウド ヴォールトは、お客様のニーズを満たすよう柔軟に構成できます。[6, 7, 8]

Rubrik Cyber Recoveryは、Rubrik Security Cloudのコンポーネントです。ソフトウェア アズ ア サービス モデルを通じて提供されるこのリカバリー ヴォールトは、Microsoft Azure上のストレージのみを使用します。調査で見つかった公開されているドキュメントの多くは、Rubrik Cyber Recoveryヴォールトを、不変性を提供するバックアップ階層であるRubrik Cloud Vaultと結び付けています。[9, 10] このヴォールトは追加のハードウェアを必要とせず、バージョン6.02以降のRubrik Cloud Data Management (CDM)プラットフォームの任意のバージョンで使用できます。

不変性

不変性(Immutability)とは、不変または永続的である状態を指します。変更不可のバックアップやバックアップ コピーを使用することで、管理者は、割り当てられた期間が経過するまでユーザーやシステムがファイルを変更または削除できないようにすることが可能になるため、それらのファイルを長期保存できます。その後、ファイルは「ロール オフ」され、ソリューションによって自動的に削除されます。ソリューションは通常、ポリシーを通じて、またはシステムがファイルを処理する方法を管理する定義を通じて、このプロセスを実行します。[11]

Dell PowerProtect Cyber Recoveryの不変性は、Retention Lock機能を介して使用可能なリテンション ロックに依存しており、バックアップ コピーの削除や変更を（一定期間）防止したり、強制的に早期期限切れにならないようにします。（PPDDは、Retention Lockの有効化状況に関係なく、追記専用のファイル システムとして機能します。[12]）Dellのお客様は、PPDD MTreeを使用してバックアップを管理しています。これはユーザー定義の論理パーティションであり、バックアップ アプリケーションの宛先として割り当てた独立した保存設定を備えています。[13] お客様は、ガバナンスとコンプライアンスの2種類のリテンション ロックから選択できます。この2つのうち、コンプライアンス ロックのほうがより厳格で安全です。お客様はMTree単位でリテンション ロックを有効にします。つまり、特定のMTree内のすべてのファイルは、そのMTreeのリテンション ロック定義に従い、リテンション期間はファイル レベルごとに設定します。お客様がコンプライアンス リテンション ロックを定義すると、ユーザーまたはシステムはそれを削除できなくなります。管理者によってガバナンス リテンション ロックを元に戻すことはできるため、厳格さとしてはこのオプションのほうが低くなります。[14]

Rubrikソリューションの不変性も、バックアップ コピーの削除や強制的な早期期限切れを防ぐためにリテンション ロックを使用します。PowerProtect Cyber Recoveryと同様、Rubrikソリューションは既存のデータを上書きするのではなく、ファイル システムに新しいデータを追加します。このソリューションでは、受信データをフィンガープリントし、データとともに保存します。**Rubrikソリューションではデフォルトでリテンション ロックが有効になっていない**ため、お客様はRubrikサポートへのチケットをオープンするか、リテンション ロックを許可するために2人ルールを有効にする必要があります。（Rubrik Cloud Data Managementバージョン7.0.1より前のバージョンでは、リテンション ロックを有効にするためにお客様はRubrikサポートに連絡する必要がありました。現在も同様にお客様がサポートに連絡する必要があるかどうかについて、Rubrikのドキュメントでは明確に示されていません。）お客様がリテンション ロックを有効にすると、ユーザーまたはシステムは、定義されたパラメーターの範囲外のデータを削除できなくなります。Rubrikリテンション ロックには、時刻同期用の外部Network Time Protocol (NTP)サーバーが必要です。これにより、攻撃者が参照用NTPソースを操作し、リテンション ロックを早期に期限切れにできる可能性があります。[15]

> *Rubrik*のソリューションではデフォルトでリテンション ロックが有効になっていないため、お客様は*Rubrik*サポートへのチケットを作成するか、2人ルールを有効にしてリテンション ロックを許可する必要があります。

ライセンスとサブスクリプション

Dell PowerProtect Cyber Recoveryはライセンスが必要なソリューションです。インストール時に、Dellはデフォルトで90日間の評価版ライセンスをインストールします。90日が経過した後も製品を引き続き使用するには、新しいライセンスを購入する必要があります。Dellは、標準（永続）ライセンスとサブスクリプションベースのライセンスの両方を提供しています。

RubrikはRubrik Cyber RecoveryをRubrik Security Cloud (RSC)に統合しています。Rubrik Cyber Recoveryを使用するには、Rubrik Enterprise Editionのサブスクリプションが必要です。サブスクリプション期間は3年間です。[16] [17] RSC障害が発生した際、SAP HANAおよびDB2ワークロードではサード パーティー製ツールを使用してデータをリカバリーする必要があります。これにより、追加のサブスクリプション費用が発生する可能性があります。[18]

管理アクセス

Dell PowerProtect Cyber Recoveryシステムの管理は、お客様が導入に選択したネットワーク トポロジーに対してローカルで行われます。このソリューションはヴォールトからのリカバリーを開始します。そのため、管理者はヴォールトが存在する場所から管理UIにログインします。オンプレミスのヴォールトにより、管理者はインターネット アクセスを必要とせずにローカルでアクセスできます。これは米国国立標準技術研究所(NIST)によって推奨されています。インターネットへのアクセスが必要な場合、サイバー攻撃者によるサービス

拒否攻撃、またはインターネット接続の切断により、データ保護体制が著しく損なわれることがあります。コロケーション ヴォールトを使用することで、リモート サイトからアプライアンスに物理的なアクセスが可能になり、パブリック インターネット以外の接続を使用できます。クラウドベースのヴォールトでは、リカバリーのためにインターネットにアクセスする必要があり、サイバー攻撃が終了して通常のネットワーク接続が再開されるまで、オンサイトのリカバリーが遅れる可能性があります。

Rubrik Cyber Recoveryの管理にはRubrik Security Cloudへのアクセスが必要であり、これにはインターネット アクセスが必要です。すでに述べたように、このような接続の必要性により、サイバー攻撃後にネットワーク機能が正常に戻るまでオンサイトのリカバリーが遅れる可能性があります。

お客様がRubrik Cyber Recovery機能を使用するにはRSCにアクセスできる必要があるため、RSCは単一障害点となります。そのサービスが使用できなくなった場合、影響を受けたお客様のヴォールトからのリカバリーが妨げられる可能性があります。Rubrikは、RSCサービスの中断の間に10のワークロードをリカバリーできますが、2つのデータベース ワークロードにはサード パーティー製ツールとRubrikのサポート部門の支援が必要になります。[19, 20] さらに、侵害された管理者アカウント、またはRSCプラットフォームへのアクセス権を持つ攻撃者は、単一のヴォールトではなく資産全体にアクセスできるようになる可能性があります。

Managed Detection and Response**に関する追加のサポートを**Dell**から受ける**

組織によっては、サイバーセキュリティに対する「単独での運用」アプローチに不安を感じる可能性があります。そのようなお客様に、DellはManaged Detection and Response (MDR)を提供しています。これは、脅威とリスクを監視および検出し、お客様と協力してリスクを軽減するフル マネージド サービスです。Dellによると、このサービスで提供される内容は次のとおりです。[21]

- 信頼できるサポート（DellがサポートするExtended Detection and Response (XDR)セキュリティ分析プラットフォームの導入と構成に関する専門家のアドバイスを含む）
- 脅威への対応やセキュリティ構成（四半期あたり最大40時間のサービス関連のセキュリティ構成を含む）
- 24時間365日対応の検出および調査（お客様の環境に応じたプロアクティブな脅威ハンティングを含む。これにより、セキュリティ システムを回避する新たな脅威や既知の脅威の亜種を検出）
- サイバー インシデント対応の開始（調査活動を迅速に開始できるようにする、年間40時間のリモート インシデント対応支援を含む）

MDRをAPEX Cyber Recovery Servicesと組み合わせることで、お客様は脅威とリスクを監視、検出、軽減するための多くのオプションから選択できます。オプションが利用可能なため、それらによって対応範囲の拡大や組織のニーズに合ったハイブリッド アプローチが可能になる場合があります。

MDRの詳細については、**https://www.dell.com/en-us/dt/services/managed-services/managed-workplace-services/managed-detection-response.htmを**参照してください。

シームレス性

セットアップ

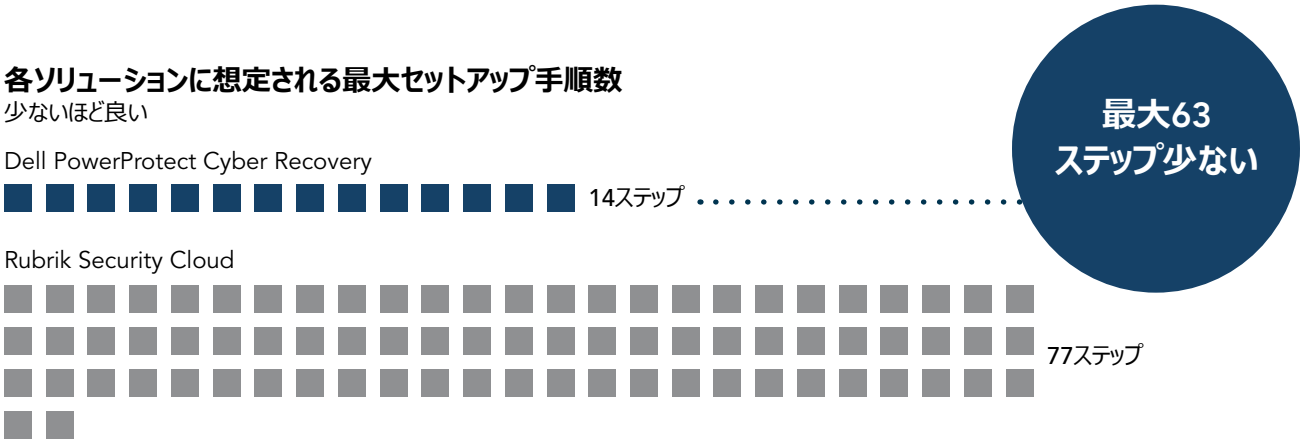
Dell PowerProtect Cyber Recoveryのセットアップには、Linuxシステムへのソフトウェア インストール、またはOpen Virtualization Format (OVF)テンプレートからのVMware® vSphere®アプライアンスの作成が含まれます。ソフトウェアのインストールには14のステップが必要ですが、[22]その代替となるvSphereアプライアンスの導入は8つのステップ、約5分で実施可能です。[23]インストール後、管理者は隔離された環境内からWebブラウザーを介してソリューションにアクセスできます。

お客様は、完全に自動化および統合された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を個別に導入する必要があります。[24] Dell PowerProtect Cyber RecoveryにCyberSenseをインストールする手順は公開されていません。[25]

Dellでは、破壊検出目標(DDO)、破壊評価目標(DAO)、サイバー リカバリー ポイント(CRP)、サイバー リカバリー時間(CRT)、サイバー リカバリー同期間隔、サイバー リカバリー データ コピー数など、多くのパラメーターをユーザーがカスタマイズできます。また、Dellは保護が必要なデータの特徴を明らかにすることも推奨しています。データは、ミッション クリティカル、ビジネス クリティカル、コア インフラストラクチャ サービスやその他のアプリケーションに依存するデータ、または一般的なデータ（アプリケーション バイナリー、ブート イメージ、バックアップ カタログなど）の場合もあります。幅広いオプションにより、お客様はバックアップ環境を完全に制御し、データの分類をカスタマイズすることができます。Dell Consulting Serviceがさらなるサポートや提案を提供することもできます。[26]

Rubrikのセットアップも複数のステップで構成されています。クラスターを作成する前に、Rubrikサポート サービスが Rubrik CDMのインストールと設定を行う必要があります。そして、管理者がCDMの最新バージョンまたは目的のバージョンをダウンロードしてインストールします（15ステップ）。[27] 次に、管理者はUIまたはCLIを使用してRubrikクラスターをセットアップすることができます。クラスターはUIまたはCLIを使用してセットアップできますが、どちらのアプローチでも24のステップが必要です。[28] [29] その後、管理者はオンライン方式（12ステップ）またはオフライン方式（18ステップ）でRubrikクラスターを登録できます。[30] [31] 次に、管理者は多要素認証(MFA)を有効にします。これには13のステップが必要です。[32] 最後に、管理者は初期アカウントを追加（6ステップ）し、その他のアカウントを追加します。[33]図3は、各サイバー リカバリー ソリューションで必要となる可能性がある最大ステップ数を示しています。

Rubrikのお客様は他の指標を調整できないため、ニーズを満たすための柔軟性が低くなる可能性があります。あるレビュアーは、「大半のユーザー インターフェイスはわかりやすいが、一部のオプションについてはその使用方法の説明が不足している場合があり、またオプション自体が見つからないこともある。ユーザー エクスペリエンスを容易にしている一方で、多くの調整可能な機能は存在せず、サポート担当者が顧客環境に変更を加えるためにサポート トンネルを開く必要がある」と指摘しています。[34]



3　Dell PowerProtect Cyber RecoveryおよびRubrik Security Cloudのセットアップのために必要となる可能性がある最大ステップ数。数値が低いほど良い。出典：Principled Technologies

保守

セットアップ後の毎日のメンテナンス操作を実行するためのDell UIとRubrik UIは類似していることが確認されました。設定後、以下のような操作を実行できるようにDell PowerProtect Cyber Recoveryを構成することができます。[35, 36]

- スケジュールに従って、またユーザーの手動要求に応じて、Cyber Recoveryジョブ レポートを自動的に生成する
  - ユーザーまたはスケジュールが、ポリシー、リカバリー操作、システム バックアップ、またはクリーニング操作を開始するときにジョブを作成する
- ヴォールトのステータスやストレージ容量、Cyber Recoveryの進行状況などを自動的に監視し、コピー/同期失敗やCyber Recoveryヴォールトがダウンした場合にはアラートを発信する、またCyber Recoveryジョブも監視する
- 攻撃を自動的かつ継続的にスキャンし、重大度の順にCyberSenseアラートを表示し、ファイルの数、ホスト、影響を受けるポリシー、検出された特定の脅威、攻撃のポイント イン タイムを表示する。これにより、クリーンなバックアップを見つけ、攻撃分析で使用する破損したファイルのリストが得られる

同様に、お客様はRubrikを次のように構成することができます。[37]

- 自動的にRubrik Security Cloudを使用して、接続されているすべてのRubrikクラスターのすべてのイベントを追跡、監視、表示する。次の3つのイベント タイプが用意されている。[38]
  - Critical（クリティカル） - 注意が必要なイベント。バックアップの失敗、アーカイブの失敗、レプリケーションの失敗など。
  - Warning（警告） - バックアップ、アーカイブ、またはリカバリーの終了
  - Informational（情報） - 情報のみ
- Threat Monitorを使用して、スナップショットを自動的かつ継続的にスキャンし、侵害の新規および既存の指標を検出する。これにより、ソリューションが最後にスナップショットを取得した時刻、イベント タイムライン、検出時間、変更されたファイルの数、疑わしいファイルの数、クラスター名、オブジェクトのタイプと名前が表示される

サポート対象の異常ワークロード

Rubrik Security Cloud Data Threat AnalyticsとCyberSenseはどちらも複数のワークロード タイプをスキャンしていますが、ある出典によると、CyberSenseは2倍の異常検出ワークロードをサポートしています。これには、次のタイプのワークロードのスキャンが含まれます。

- VM
- コア インフラストラクチャ
- ドキュメントや契約、知的財産などを含む可能性があるユーザー ファイル
- データベース
- 他のクライアントによって作成されたバックアップ

> 公開されているデータを基に、サポートされているワークロード数を数えると、*CyberSenseは21、Rubrikは7つ*の異常検出ワークロードをサポートしていることがわかります。

公開されているデータを基に、サポートされているワークロード数を数えると、CyberSenseは21、Rubrikは7つの異常検出ワークロードをサポートしていることがわかります。そのため、CyberSenseは、それぞれが公開しているデータによると、Rubrik Security Cloud Data Threat Analyticsの2倍のワークロードをサポートしていることになります。サイバー リカバリー ソリューションがスキャンできるデータ量が多いほど、巧妙なマルウェアや他の侵害を発見する機会が多くなります。

VMワークロードのサポート

VMワークロードとは、物理ホスト サーバーまたはクラウド環境でVMが実行するアプリケーション、サービス、またはタスクを指します。これらのワークロードは機能が異なる可能性があり、その他多くの方法でマルウェアにさらされる可能性が高まるため、VMのスキャンが不可欠です。Rubrik Security Cloud Data Threat Analyticsは、「Anomaly Detection、Threat Monitoring、Threat Hunt、保護対象リソースのデータ リカバリー サービスで構成」され、[39]以下のVMワークロードに対するスキャンをサポートしています。[40]

- VMware
- Nutanix® AHV
- Microsoft Hyper-V
- Microsoft Azure

CyberSenseは、次のVMワークロードのスキャンをサポートしています。[41] [42] [43]

- VMware
- Amazon Web Services（AWS）
- Hyper-Vと、Dell AvamarまたはDell NetWorkerバックアップ

VMwareは、「仮想化されたワークロードの80%がVMwareテクノロジー上で実行されている」と主張しています。[44] 2024年第1四半期には、クラウド インフラストラクチャ サービス市場で最も人気のあるベンダーのAmazon Web Services (AWS)が市場全体の31%を占めていました。Microsoft Azureは市場占有率25%で2位となっています。[45]

コア インフラストラクチャ

コア インフラストラクチャは、テクノロジー環境の運用を可能にする基本的なコンポーネントとサービスです。このレベルでマルウェアを検出すると、コア インフラストラクチャの機能が多くのシステムとユーザーに作用する可能性があるため、攻撃の重大度を軽減することができます。Rubrik Security Cloudのドキュメントでは、コア インフラストラクチャのスキャンのサポートについては言及していません。[46]

対照的に、CyberSenseは以下のコア インフラストラクチャのスキャンをサポートしています。[47]

- Active Directory
- DNS
- LDAP

ドキュメントや契約、知的財産などを含む可能性があるユーザー ファイル

Rubrik Security Cloud Data Threat Analyticsは、以下のユーザー ファイルのスキャンをサポートしています。[48]

- NASファイル セットとデータセット
- Windowsボリューム グループ
- LinuxおよびWindows

CyberSenseは、LinuxおよびWindowsのユーザー ファイルをスキャンできます。[49]

データベースのスキャン

CyberSense = 7 vs.

RSC Data Threat Analytics = 0

データベース

アプリケーションはさまざまな理由のために異なるタイプのデータベースを使用できるため、さまざまなデータベースにマルウェアが存在するかどうかを検出できることが迅速な対応に不可欠となります。Rubrik Security Cloud Data Threat Analyticsはデータベースをバックアップできますが、それらのデータベース バックアップをスキャンできることを示す公開ドキュメントは見つかりませんでした。

CyberSenseは、ページレベル スキャンにより、以下のデータベースのスキャンをサポートしています。[50]

- SQL
- PostgreSQL
- Oracle®
- Epic® Caché
- SAP HANA
- MariaDB/MySQL
- Db2

他のクライアントによって作成されたバックアップ

一部の組織では、冗長性の提供や規制への準拠、その他の重要な理由により、複数のベンダーによるデータ バックアップを採用している場合があります。Rubrik Security Cloudのドキュメントでは、他のバックアップ クライアントによって作成されたバックアップのスキャンのサポートについては言及されていません。[51]

CyberSenseにはこのカテゴリーでの優位性があります。CyberSenseでは、以下のバックアップ クライアントで作成されたバックアップのスキャンをサポートしています。[525354]

- DNAS
- SQL
- NetWorker
- Veritas NetBackup
- Exchange
- Avamar
- Commvault

スキャン テクノロジー

Rubrik Security Cloudには、スキャンや、Data Threat Analyticsでのスキャンに役立つ多くのツールが含まれています。

- Rubrik Anomaly Detectionは、疑わしいファイル、スナップショットの変更[55]、異常の詳細を、異常インシデントとして表示し、お客様がスナップショット調査において精査および使用できるようにします。[56]また、このソフトウェアはリカバリー オプションも提供します。[57]
- Rubrik VM Encryption Detectionは、VMware vSphere仮想ディスク ファイルに対する攻撃を検出します。[58]
- Rubrik Threat Monitoringは、検出された脅威と一致に関する情報を表示します。[59]
- Rubrik Threat Huntは、ユーザーが開始して侵害の兆候をスキャンする機能です。[60]
- Rubrik Quarantineは、Threat Huntに表示されるオブジェクトを隔離します。[61]

Rubrik RSCはまた、各Rubrikクラスター用のRubrikバックアップ サービス コネクターを備えています。

Rubrikのお客様はタスクに適したツールを選択する必要があり、スキャンを手動で開始するか、タスクを実行するために複数のツールを使用する必要があります。一方、DellではCyberSenseスキャニング オプションが1つであり、お客様は容易に管理および運用できる可能性があります。

CyberSenseスキャンは、Rubrik RSC Data Threat Analyticsの「表面のみ」のスキャンと比べて、より深くまで検出します。CyberSenseは、ファイルのフル コンテンツ スキャンとデータベースのページレベル スキャンを実行し、ファイルの部分的な暗号化を検出できます。[62] このツールは、数千ものデータ脅威についてIndex Enginesによってトレーニングされた機械学習(ML)データベースを使用し、200を超える分析ポイントでデータの破損を検出します。[63] Rubrik Threat MonitoringおよびThreat Huntと異なる点として、CyberSenseはマルウェア シグネチャの提供を外部の脅威インテリジェンス機関に頼ることはしていません。それ自体で新たな脅威を発見します。[64]**また、CyberSenseは許容可能なファイル変更の任意のしきい値やスナップショット間のエントロピー レベル（偽陰性につながる可能性がある）に依存せず**、以前の顧客行動のベースラインに合わせてMLをトレーニングすることもありません。[65, 66, 67]

> *CyberSenseは許容可能なファイル変更の任意のしきい値やスナップショット間のエントロピー レベル（偽陰性につながる可能性がある）に依存せず、...*

Rubrik異常検出ソフトウェアは、メタデータのみを使用して、コンテンツ分析を実行する前にスナップショットが破損しているかどうかを判断します。CyberSenseの継続的なMLと比較すると、Rubrikソフトウェアはシグネチャを取得した後に破損を検出します。Rubrikの異常検出では、お客様の通常のベースラインを定義するための行動モデルを構築する必要があります。この設定には複数回のバックアップが必要になる場合があります。Rubrikの行動モデ

ルでは、攻撃のない状況下でファイル システムの典型的な変化のベースラインを作成するために、少なくとも2回のバックアップが必要になります。1つの変更統計セットでは、典型的なものを特定するには不十分な場合があります。ビジネス イベントが、最初と2番目のRubrikスナップショットの間に発生しなかった何らかのアクティビティ（より疑わしいアクティビティ）を引き起こす可能性はあります。Rubrikのソリューションは、より多くのバックアップを分析することにより、ベースラインに基づいて行動モデルをより正確にトレーニングすることができます。[68, 69]

CyberSenseは、すべての分析結果を安全なヴォールト内に保存します。ファイル システムの行動分析パイプラインでは、Rubrikはお客様のファイル システムの変更に関するメタデータをクラウドベースのPolarisプラットフォームに送信して行動分析を行います。この間、攻撃対象領域は開放されることになります。[70]

お客様はRubrik Enterpriseエディションの一部としてのみ、Rubrik Threat MonitoringとThreat Huntを使用できます。[71] お客様はロールベース アクセス制御(RBAC)権限を使用してThreat Huntスキャンを実行する必要があり、どの特定の侵害インジケーター(IOC)をハントするかを指定する必要があります。[72] これは業界のベスト プラクティスではありません。[73] CyberSenseと同様、Threat HuntはVMware、AHV、Hyper-V、NASファイル セット、LinuxおよびWindowsサーバーをサポートしています。[74]

以降のセクションでは、Rubrikソリューションがどのように脅威検出を提供するかについて詳しく説明します。

メタデータとファイル システム統計情報

Rubrik Anomaly Detection ML行動モデルは、追加、削除、移動されたファイルの数など、最後のスナップショット以降のファイル システムへの変更をメタデータとしてログに記録します。[75] 次に、MLモデルはこれらの変更に関してトレーニングされ、ファイル システムの行動モデルの「ベースライン」を構築します。Rubrikは、変更が多すぎることを検出した場合、スナップショットを異常としてフラグ付けします。行動分析によってスナップショットにフラグが設定された後、ソリューションはファイル コンテンツ分析を開始します。[76]メタデータのモニタリングはセキュリティ レイヤーを追加することにはなりますが、イベントによるダウンタイムの予防や軽減に役立つ十分な保護とはならない可能性があります。

> *CyberSense*はベースラインを必要とせず、最初のバックアップ コピー以降におけるファイルおよびデータベース コンテンツの変更を監視、分析します。

逆に、**CyberSenseはベースラインを必要とせず、最初のバックアップ コピー以降におけるファイルおよびデータベース コンテンツの変更を監視、分析します。**CyberSenseのアプローチは、それよりもさらに詳細であり、ファイルの断片やデータベースの個々のページを分析します。Rubrikソリューションと同様、CyberSenseスキャンにはメタデータ プロパティが含まれており、結果がMLエンジンにフィードされます。Rubrikソリューションとは対照的に、CyberSenseはメタデータ スキャンに限定されず、Index Enginesはシグネチャや以前の顧客行動ではなく、Index Enginesによって文書化された攻撃に基づいてMLエンジンをトレーニングします。[77, 78]

しきい値

行動分析中に、Rubrik MLはファイル システムで異常が発生した可能性を判断します。異常の可能性があるとRubrikソリューションが判断した場合は、コンテンツ分析を行います。このしきい値は、行動モデルによって決定された「異常行動」しきい値に基づくと考えられます。たとえば、Rubrikのソリューションは、新規ファイルや変更されたファイルの大量出現や、ランダム性または暗号化の指標が増加した場合に異常動作としてフラグを設定することが可能です。[79] コンテンツ分析中に、Rubrik Anomaly Detectionはファイル コンテンツの変更を表示し、ファイル システムのエントロピーを計算することで暗号化の確率を計算します。ファイル システムのエントロピーは、ランサムウェア攻撃によってファイルが暗号化されている可能性を示すのに役立ちます。エントロピーの異常値を超えた場合、ソリューションはユーザーに対してアラートを発します。[80, 81] データ破損の検出の有効性は、しきい値の厳密さによって異なります。許容量が大きすぎると、偽陰性が発生し、誤った安心感が生じる可能性があります。[82]お客様は適切なしきい値を設定する必要があります。

一方、CyberSenseはファイル コンテンツをスキャンすることでファイルの部分的な暗号化をチェックし、データ破損の検出において99.99%の信頼性（DellとIndex Enginesによる）を提供します。[83]

シグネチャとファイル拡張子

Rubrik Threat MonitoringおよびThreat Huntは、スナップショットをスキャンしてIOCを検出します。Rubrikが監視する複数の脅威インテリジェンス ソースの1つが新たなIOCを検出すると、Threat Monitoringは新しいマルウェア（マルウェア シグネチャ）を識別するためのYARA (Yet Another Ridiculous Acronym)ルールを含む脅威フィードを、すべてのRubrikクラスターにプッシュします。その後、クラスターはスキャンを開始します。[84] 最近のWatchGuardのレポートでは、マルウェアの57.8%がシグネチャによる検出を回避していることが示唆されています。BianLianなどの高度なマルウェアは、シグネチャによる認識を回避する方法を採用しており、新しいマルウェアの亜種は元のものとわずかに異なるシグネチャを持つ可能性があります。そのため、脅威インテリジェンスを最新の状態に保つことは困難になる場合があります。[85]

一方、CyberSenseは200以上の分析機能を活用し、ランサムウェアの多くの亜種に基づく機械学習モデルを提供しています。Index Enginesは、CyberSenseの手法ではシグネチャをダウンロードすることなく、これまで見られなかった巧妙な亜種を検出できることを証明しました。[86]これは、イベント中にインターネットに依存しないことのもう1つの利点となります。

大量暗号化イベント

Rubrikソリューションは、ファイル システム全体のエントロピーを計算することで、大量暗号化イベントを監視します。[87] CyberSenseは、はるかにきめ細かな機能を備えています。ファイル システム全体や個々のファイルをスキャンするのではなく、ファイル内部のコンテンツの断片をスキャンします。Index Enginesによると、ファイル全体を対象にしたエントロピー計算のみで断片のスキャンは行わないと、「ファイル全体の極端な暗号化」、つまり大規模暗号化イベントしか検出できません。[88]

復旧可能性

ドキュメントに照らしてみると、Dell PowerProtect Cyber Recoveryを使用したリカバリーは、Rubrikを使用したリカバリーよりもシンプルで効率的なプロセスと考えられます。本報告書のこのセクションでは、2つのソリューションのリカバリー機能の対比と、それぞれのソリューションでのこれらの機能の実装方法について比較検討しています。

Rubrikのドキュメントには、どのリカバリー機能がどのVMタイプで機能するかが記載されています。これは詳細な情報を有用に提供しているように見えるかもしれませんが、多くの規定とバリエーションにより、リカバリーを複雑化させています。たとえば、Rubrikのお客様がデータ、ファイル、システムをリカバリーする必要がある場合、リカバリー計画に含めるスナップショット オブジェクトを選択する必要があります。Rubrikでは、リカバリー計画を1つ以上作成すると、次のような多くの復元性のオプションが提供されます。[89, 90, 91, 92, 93]

- ファイルをダウンロードまたは上書きして別のフォルダーにリカバリーするか、異なるホストにエクスポートするか、クラスター化されたサービスにエクスポートする
- ダウンロードまたは上書きを介してVMのファイルをリカバリーし、別のフォルダーにリカバリーするか、別の仮想マシンにエクスポートする
- 次の方法で、VMまたはディスク スナップショットの完全なリカバリーを実行する：
  - ライブ マウント（スナップショットから新しい仮想マシン(VM)を生成）
  - 仮想ディスクのマウント（スナップショットから新しい仮想ディスクを作成）
  - 瞬時のリカバリー（現在のVMを、スナップショットによって作成された新しいVMに置き換える）
  - エクスポート（選択したデータストアのスナップショットから新しいVMを作成）
  - VMの一括リカバリー
- ライブ マウントおよびエクスポートによるリカバリー プランの一括サイバー リカバリー
- Rubrik Security Cloud Orchestrated Applicationリカバリーにより、分離されたサンドボックス、リモート サイト、またはイン プレースでVMディザスター リカバリーを実行

Rubrikの一括リカバリー機能を見てみると、リカバリーの複雑さがさらによくわかります。表1は、ハイパーバイザーに応じてRubrikが提供する一括リカバリー機能を示しています。[94]

1 Rubrikでは、異なるハイパーバイザーのための一括リカバリー機能を提供しています。出典：Rubrik。

VM作成オプション				
	ライブ マウント	**ライブ マウント + オプションの移行**	**エクスポート**	**瞬時のリカバリー**
vSphere VM	使用可能、データストアとしてRubrikクラスターを使用	使用不可	使用可能、リカバリーされたハイパーバイザーのデータストアを使用	使用可能、データストアとしてRubrikクラスターを使用
AHV VM	使用可能、データストアとしてRubrikクラスターを使用	使用可能、Rubrikクラスターをデータストアとして使用し、Nutanixコンテナをすべての後続の書き込みに使用	使用可能、Nutanixコンテナをデータストアとして使用	使用不可
Hyper-V仮想マシン	使用可能、データストアとしてRubrikクラスターを使用	使用不可	使用可能、リカバリーされたハイパーバイザーのデータストアを使用	使用可能、現在のVMをスナップショットの新しいVMに置き換える。Rubrikクラスターをデータストアとして使用

Rubrikのソリューションでは、リカバリーされたデータストアは通常、Rubrikクラスターにあり、本番環境にはないため、問題が発生することがあります。これらの問題については、次のセクション「"Rubrik limitations"」で説明します。これに対し、PowerProtectは、リカバリーされたデータをリカバリー環境または本番環境に配置することで、高速でスムーズなリカバリーを実現し、ダウンタイムを最小限に抑えることができます。

表2は、vSphere VMのリカバリーに関するRubrikの追加情報を示しています。[95]この表に示すように、ほとんどのvSphereリカバリーデータストアはRubrikクラスター上にあります。

2 RubrikがvSphere VM向けに提供するリカバリー機能。出典：Rubrik。

RubrikがvSphere向けに提供するリカバリー機能				
動作	**データストア**	**電源状態**	**ネットワーク**	**ソースVM**
ファイルのリカバリー	該当なし	該当なし	該当なし	影響なし
ライブ マウント	ローカルのRubrikクラスター	オンまたはオフ	切断済み	影響なし
仮想ディスクのマウント	ローカルのRubrikクラスター	日付：	切断済み	影響なし
瞬時のリカバリー	ローカルのRubrikクラスター	日付：	接続済み（オプション）	電源をオフにしてから名前を変更
エクスポート	ハイパーバイザーのデータストア	オフ	切断済み	影響なし
インプレース リカバリー	ハイパーバイザーのデータストア	日付：	ソースVMと同じ	インプレース リカバリーでは、VMのプロパティを変更せずに、ソースVMの仮想ディスク ファイルがスナップショットの仮想ディスク データで上書きされる

Rubrikのソリューションは、一括リカバリーを広く実装しておらず、一括リカバリー オプションは限定的で複雑です。このレポートの"Dell PowerProtect Data Manager offers the equivalent of Rubrik "mass restore""セクションで詳しく説明しているように、Dell PowerProtectは合理化され、シンプルになっています。

大規模なリストアの誤りを暴く

Rubrikは、アプリケーション、ファイル、ユーザーを大規模にリカバリーすることで、事業運営を迅速にリストアすることを「マス リカバリー(mass recovery)」と定義しています。[96] Rubrikは多くの一括リカバリー オプションを提供しています。ただし、Rubrikのソリューションは通常、リカバリーされたデータを本番環境ではなく、Rubrikクラスターに保存します。[97]ワークロードは、ソリューションが移行を完了するまで、Rubrikシステムの可用性に依存します。ローカルのRubrikクラスターはティア3のストレージであるため、お客様は計画されたパフォーマンス レベルに戻すために、本番環境への追加の移行を行う必要があります。この単一障害点とシステム移行中のパフォーマンスの低下により、Rubrikソリューションがワークロードを本番環境にリストアするまでリカバリーが完了したとは言えません。

また、Dell PowerProtectは、ユーザーがリカバリーUIで複数のVMを選択してリカバリーできるようにすることで、一括リカバリーも提供しています。

Dell PowerProtect Data Managerは、Rubrikの「マス リカバリー」に相当する機能を提供

Rubrikのソリューションと比較して、DellのソリューションもvSphere VMに関して同等のリカバリー オプションを複数提供しています。Dell PowerProtectは、VMデータをリカバリー環境または本番環境に配置できます。ほとんどのRubrikオプションは、Rubrikクラスターのみにデータを配置します。表3は、Dellのリカバリー オプションを示しています。[98, 99, 100, 101]

3 Dellのリカバリー オプション。出典：Principled Technologies

Dellのリカバリー オプション	
タイプ	**機能の概要**
ファイル レベルのリストア	感染したファイルのみをその位置でリストアするか、ロールバックによってリストアする
ライブのVMセッション	VMをクラスターにリストアし、後で本番環境への移行を行う
新しい場所へのリストア	元の環境または新しい環境（クリーン ルームやリカバリー インフラストラクチャなど）にリストアする。ユーザーは一括リストアまたは大規模リストアのために複数のVMを一度に選択できる
アクセス/ライブVM	本番データの分離されたコピーを作成する
リカバリー オーケストレーション	管理者がリカバリーのスケジュールを設定したり、オンデマンドで使用できるようにする。本番環境またはリカバリー環境へのVMの自動リカバリーを優先

Rubrikの制限事項

Rubrikのソリューションでは、マルウェアに感染したスナップショットを隔離し、将来の分析のために保存します。ただし、Rubrikのソリューションはデフォルトではスナップショットを隔離しません。その後、お客様は隔離されたファイルを手動でダウンロードして実行するか、サード パーティー製ツールを使用してフォレンジック分析を実行します。この間、マルウェアに感染する可能性があります。[102, 103]

> *CyberSenseは、ユーザーが独自のフォレンジックを実行することなく分析を実行し、リストア ポイントの作成を自動化します。*

CyberSenseはデフォルトでファイルとデータベースを分析します。ユーザーがスナップショットを手動で隔離する必要はありません。**CyberSenseは、ユーザーが独自のフォレンジックを実行することなく分析を実行し、リストア ポイントの作成を自動化します。**[104]

Rubrik RSCは、RSCのみの管理モードの場合、多くの機能にとって単一の障害点となります。最も懸念されるのは、攻撃によってRSCサービスが中断され、ユーザーのインターネット接続やユーザー サイトとRSCの間の接続に影響が及ぼされることです。このような攻撃の後、このソリューションではRubrik CDM UIやAPIベースの自動化を介して限定された機能セットを提供します。ただし、これは攻撃前にRSCサービス アカウントを作成しているユーザーに対してのみ提供されます。[105, 106]組織がRSCなしでリカバリーできるワークロードおよびデータは次のとおりです：MongoDB、Microsoft Exchange、ファイル、Hyper-Vスナップショット、管理対象ボリュームからのライブ マウント、NASホスト ファイル、Oracle、SQL Server、VCD、VMware。[107] RSCなしでのSAP HANAのリカバリーには、StudioやCockpit Crossなどのサード パーティー ツールと、Rubrikによるサポート（サポート トンネル経由）が必要です。IBM Db2をRSCなしでリカバリーするには、IBMのサード パーティー ツールとRubrikのサポート（サポート トンネル経由）が必要です。[108]

エア ギャップ/隔離

NISTはエア ギャップを「(a)物理的な接続がなく、(b)自動化された論理的な接続もない2つのシステム間のインターフェイス」と定義しています（このインターフェイスでは、データの転送は人間の制御下で手動でのみ行われます）。[109]

エア ギャップは、ソースからターゲットへのデータの流れを制御するのに役立ち、ランサムウェア対策とサイバー リカバリー戦略の重要な要素となる可能性があります。攻撃やイベントによって本番環境のバックアップ システムが侵害された場合、本番環境のシステムからサイバー リカバリー ヴォールト内の保護されたバックアップにアクセスするトラフィックを遮断することで、フェールセーフを実現できます。

物理的な分離

映画『ミッション・インポッシブル』で物理的に分離されたソリューションの例を見たことがあるかもしれませんが、この場合、主人公は外部ネットワークに接続されていないコンピューター システム上の機密データにアクセスするために、他のすべての施設のセキュリティ機能をバイパスしなければなりませんでした。物理的な分離では、通常、専用の物理ネットワークの切断されたセグメントを使用して、本番システムからヴォールトにバックアップ コピーを転送することもできます。これらの運用上のエア ギャップは、切断されていることで、データが自動的に交わることができない物理的な障壁を生じ、攻撃者がアクセスを取得するのが難しくなります。

組織は、Dell PowerProtect Cyber Recoveryを物理的に分離して、運用上のエア ギャップ戦略を実現することができます。このソリューションは、専用の物理接続を使用し、バックアップ ソリューションからのプッシュ操作ではなく、ヴォールトからのプル操作としてデータ レプリケーションを実行します。コピー/レプリケーション中に、ソリューションは接続をアクティブ化し、データを暗号化して、専用回線を介して移行します。[110]レプリケーションが完了すると、ソリューションはヴォールト側からの接続を再度無効にします。このソリューションでは、ロックされた保存ポリシーを適用してヴォールト コピーを不変に保つため、ユーザーやシステムがアクセス権を取得した場合でも、ヴォールト コピーの変更や削除はできません。管理トラフィックがレプリケーション パスを通過しないため、**悪意のある攻撃者がオンプレミス バックアップ ソリューションを制御した場合でも、ヴォールトはレプリケーション パスを開始および切断し、データソースからの一方向のデータのみのプルを使用するため、ヴォールトへの直接アクセスが制限されます。**[111]

論理的な分離

一方、論理的な分離は、同じ物理ネットワーク上に存在するシステムを使用しますが、システムが相互にデータを送信できないようにネットワークを論理的に分離し、制御します。このソリューションでは、RBACや多要素認証に加え、暗号化やハッシュ化などの追加のセキュリティ実装を使用して、不正なシステムやユーザーが、別のシステム内に存在するデータを読み取ることができないようにします。

Rubrikは、そのサイバー リカバリー機能を、論理的なエア ギャップ戦略を活用したものと説明しています。[112, 113] 公開されているRubrikの主張の多くは、エア ギャップの必要性に疑問を投げかけています。「Rubrik Security – Air Gap and Immutability」と題されたRubrikのプレゼンテーションでは、ソリューションがバックアップを実行すると、Rubrikアプライアンスが物理ネットワーク上に残っているとしても、バックアップにアクセスしたり編集したりする方法がないため、ネイティブ ソリューションはエア ギャップ状態であると主張しています。[114] ただし、認証された不正な攻撃者がアプライアンスのGUIにアクセスできる可能性があり、リカバリーに影響を与える可能性があります。この問題を緩和するために、Rubrikは、バックアップの期限切れを防ぐリテンション ロック機能を備えており、これによりバックアップが不変となります。リテンション ロックを有効にすると、Rubrikクラスターが工場出荷時設定にリセットされて消去されることも防止できます。『Rubrik CDM Security Guide』によると、このソリューションはデフォルトでクラスターのリテンション ロックをグローバルに無効にします。有効にするには、お客様がRubrikサポートに連絡する必要があります。[115]公開されている情報源では、Rubrikサポートもリテンション ロックを無効にできるかどうかが明確化されていません。これにより、許可された攻撃者が依然としてセキュリティ レイヤーを回避できるのではないかという不安が生じます。

> 管理トラフィックがレプリケーション パスを通過しないため、悪意のある攻撃者がオンプレミス バックアップ ソリューションを制御した場合でも、ヴォールトはレプリケーション パスを開始および切断し、データソースからの一方向のデータのみのプルを使用するため、ヴォールトへの直接アクセスが制限されます。

結論

組織は、データセンターに対する多数の攻撃ベクトルを積極的に検討する必要があります。優れたデータ保護計画は、すべてのデータ、特に運用に不可欠な重要なデータを保護することを目的としています。Dell PowerProtect Cyber RecoveryとRubrik Secure Cloudに関する公開情報を調査し、両ソリューションにおける、データ管理、保護、リカバリーに対するアプローチの方法を確認しました。

PowerProtect Cyber Recoveryは、重要なデータのバックアップ コピーをヴォールト内に物理的に分離し、サイバー攻撃が発生した場合の復元性を確保しています。このソリューションは、物理的な分離による運用エア ギャップ戦略を採用しており、これは論理的な分離に依存しているRubrik Secure Cloudとは異なります。

Cyber Recoveryは、CyberSenseのMLベースの分析を使用して、ヴォールト内のデータの整合性を評価し、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。一方、Rubrik Secure Cloudは、ファイルに対して詳細なスキャンを実行するのではなく、異常を検出するMLトレーニング済みの分析ツールを提供しています。

さらに、Cyber Recoveryソリューションは複数のリカバリー 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、効率的でシームレスな運用再開を促進します。多くの場合、PowerProtect Cyber Recoveryは、Rubrik Secure Cloudにない機能と利点を提供できるため、ダウンタイムを最小限に抑えるとともに、リカバリーを高速化するために詳細な分析が可能な、より安全なソリューションを提供できる可能性があります。

---

1. Anastasia DergachevaおよびJesse R. Taylor、『Study Finds Average Cost of Data Breaches Continued to Rise in 2023』（2024年7月25日にアクセス）、https://www.morganlewis.com/blogs/sourcingatmorganlewis/2024/03/study-finds-average-cost-of-data-breaches-continued-to-rise-in-2023。
2. Dell、『Dell PowerProtect Cyber Recovery Solution Guide』（2024年4月18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. Rubrik、『Rubrik Security Cloud Architecture and Security Implementation』（2024年4月18日にアクセス）、https://www.rubrik.com/content/dam/rubrik/en/resources/white-paper/wp-rubrik-security-cloud-architecture-and-security-implementation.pdf。
5. Rubrik、『Rubrik Security Cloud Architecture and Security Implementation』（2024年4月18日にアクセス）、https://www.rubrik.com/content/dam/rubrik/en/resources/white-paper/wp-rubrik-security-cloud-architecture-and-security-implementation.pdf。
6. Rob Emsley、『Public Cloud Vault to Secure, Isolate and Recover Data』（2024年3月20日にアクセス）、https://www.dell.com/en-us/blog/public-cloud-vault-to-secure-isolate-and-recover-data/。

7. Brian White、『Dell's PowerProtect Cyber Recovery Expands to Microsoft Azure』（2024年3月20日にアクセス）、https://www.dell.com/en-us/blog/dells-powerprotect-cyber-recovery-expands-to-microsoft-azure/。
8. Dell、『Cyber Recovery on Google Cloud Platform』（2024年3月20日にアクセス）、https://infohub.delltechnologies.com/en-US/l/dell-powerprotect-cyber-recovery-reference-architecture/cyber-recovery-on-google-cloud-platform/。
9. Chris Mellor、『Up to $5m compensation if Rubrik Cloud Vault recovery busted』（2024年3月20日にアクセス）https://blocksandfiles.com/2022/02/24/up-to-5m-compensation-if-rubrik-cloud-vault-recovery-busted/。
10. Kristina Avrionova、『Frequently Asked Questions about Rubrik Cloud Vault』（2024年3月20日にアクセス）、https://www.rubrik.com/blog/company/22/3/faq-about-rubrik-cloud-vault。
11. Chris Wahl、『Recovering Fast from Ransomware Attacks: The Magic of an Immutable Backup Architecture』（2024年3月22日にアクセス）、https://www.rubrik.com/content/dam/rubrik/en/resources/white-paper/rwp-recovering-fast-from-ransomware-attacks.pdf。
12. Dell、『Data Domain Invulnerability Architecture: Enhancing Data Integrity and Recoverability』（2024年6月7日にアクセス）、https://www.delltechnologies.com/asset/en-us/products/data-protection/industry-market/h7219-data-domain-data-invul-arch-wp.pdf。
13. Dell、『Consolidate Governance and Compliance Archive Data』（2024年4月4日にアクセス）、https://infohub.delltechnologies.com/en-US/l/dell-powerprotect-data-domain-retention-lock/consolidate-governance-and-compliance-archive-data/。
14. Dell、『Dell PowerProtect Cyber Recovery Solution Guide』（2024年3月24日にアクセス）、https://www.delltechnologies.com/asset/en-us/products/data-protection/technical-support/h17670-cyber-recovery-sg.pdf。
15. Rubrik、『Retention-locked SLA Domain attributes』（2024年4月2日にアクセス）、https://docs.rubrik.com/en-us/8.0/ug/cdm/attributes_of_retention_locked_sla_domains.html。
16. Rubrik、『Rubrik Cyber Recovery』（2024年3月20日にアクセス）、https://www.rubrik.com/content/dam/rubrik/en/resources/solutions-brief/brf-rubrik-cyber-recovery.pdf。
17. Rubrik、『Rubrik Licensing: Subscribe to Simplicity』（2024年3月20日にアクセス）、https://www.rubrik.com/content/dam/rubrik/en/resources/data-sheet/rubrik-licensing-data-sheet.pdf。
18. Rubrik、『Workloads require third-party tools for recovery』（2024年5月6日にアクセス）、https://docs.rubrik.com/en-us/saas/saas/workloads_require_third_party_tools_for_recovery.html。
19. Rubrik、『Recoverable workloads during RSC service disruption』（2024年5月6日にアクセス）、https://docs.rubrik.com/en-us/saas/saas/recoverable_workloads_during_rsc_service_disruption.html。
20. Rubrik、『Workloads require third-party tools for recovery』。
21. Dell、『Strengthen your security posture with Managed Detection and Response』（2024年4月2日にアクセス）、https://www.delltechnologies.com/asset/pl-pl/services/managed-services/technical-support/managed-detection-and-response-datasheet.pdf。
22. Dell、『Dell PowerProtect Cyber Recovery 19.13 Installation Guide』（2024年3月20日にアクセス）、https://www.dell.com/support/manuals/en-us/cyber-recovery/irs_p_19.13_installation/installing-the-cyber-recovery-software?guid=guid-8718978d-ddd0-4dc0-bca7-fb04a2f3d1fb&lang=en-us。
23. Dell、『Dell PowerProtect Cyber Recovery 19.13 Installation Guide』。
24. Dell、『Dell PowerProtect Cyber Recovery 19.13 Installation Guide』。
25. Dell、『Installing CyberSense in Dell PowerProtect Cyber Recovery』（2024年3月20日にアクセス）、https://infohub.delltechnologies.com/en-US/l/ransomware-protection-secure-your-data-on-dell-powerflex-with-powerprotect-cyber-recovery-1/installing-cybersense-in-dell-powerprotect-cyber-recovery-1/。
26. Dell、『Dell PowerProtect Cyber Recovery Solution Guide』。
27. Rubrik、『Downloading and installing Rubrik CDM』（2024年3月20日にアクセス）、https://docs.rubrik.com/en-us/saas/install/download_install_cdm_on_appliance_nodes.html。
28. Rubrik、『Setting up a Rubrik cluster using the UI』（2024年3月20日にアクセス）、https://docs.rubrik.com/en-us/saas/install/setting_up_ui.html。
29. Rubrik、『Setting up a Rubrik cluster using the CLI』（2024年3月20日）、https://docs.rubrik.com/en-us/saas/install/setting_up_cli.html。
30. Rubrik、『Registering Rubrik clusters using the online method』（2024年3月20日にアクセス）、https://docs.rubrik.com/en-us/saas/install/registering_clusters_online.html。
31. Rubrik、『Registering Rubrik clusters using the offline method』（2024年4月2日）、https://docs.rubrik.com/en-us/saas/install/registering_clusters_offline.html。
32. Rubrik、『Enabling MFA』（2024年3月21日にアクセス）、https://docs.rubrik.com/en-us/saas/install/rsc_enabling_mfa.html。
33. Rubrik、『Adding the initial account』（2024年3月21日にアクセス）、https://docs.rubrik.com/en-us/saas/saas/adding_the_initial_account.html。

34. TrustRadius、『Learning Rubrik by putting the pieces together Brik by Brik』（2024年3月21日にアクセス）、https://www.trustradius.com/reviews/rubrik-2023-09-20-21-03-04。
35. Dell、『Dell PowerProtect Cyber Recovery Solution Guide』。
36. Index Engines、『CyberSense®: How it Works』（2024年3月21日にアクセス）、https://www.indexengines.com/how-it-works。
37. Rubrik、『Anomaly event details』（2024年3月21日にアクセス）、https://docs.rubrik.com/en-us/saas/saas/anomaly_event_details.html。
38. Rubrik、「Events page』（2024年3月21日にアクセス）、https://docs.rubrik.com/en-us/saas/saas/common/events_page.html。
39. Rubrik、「RSC Data Threat Analytics』（2024年3月21日にアクセス）、https://docs.rubrik.com/en-us/saas/saas/ri_ransomware_monitoring.html。
40. Rubrik、『RSC Data Threat Analytics』。
41. Dell Technologies、『Dell PowerProtect Cyber Recovery: Reference Architecture』（2024年5月6日にアクセス）、https://www.delltechnologies.com/asset/en-us/products/data-protection/industry-market/h18661-dell-powerprotect-cyber-recovery-reference-architecture-wp.pdf。
42. Dell Technologies、『Dell EMC Avamar for Hyper-V』（2024年5月16日にアクセス）、https://www.delltechnologies.com/asset/en-us/products/data-protection/technical-support/docu89876.pdf。
43. Dell Technologies、『Dell EMC NetWorker Module for Microsoft for Hyper-V』（2024年5月16日にアクセス）、https://www.delltechnologies.com/asset/en-us/products/data-protection/technical-support/docu92011.pdf。
44. VMware、『Accelerate IT.Innovate with your cloud』（2024年5月9日）、https://www.vmware.com/files/pdf/VMware-Corporate-Brochure-BR-EN.pdf。
45. Statista、『Cloud infrastructure services vendor market share worldwide from fourth quarter 2017 to first quarter 2024』（2024年7月17日）、https://www.statista.com/statistics/967365/worldwide-cloud-infrastructure-services-market-share-vendor/。
46. Rubrik、『RSC Data Threat Analytics』。
47. Dell Technologies、『CyberSense® for PowerProtect Cyber Recovery』（2024年6月27日にアクセス）、https://www.delltechnologies.com/asset/en-gb/products/data-protection/briefs-summaries/h18214-cybersense-for-dellemc-powerprotect-cyber-recovery-solution-brief.pdf。
48. Rubrik、『RSC Data Threat Analytics」。
49. Index Engines、『CyberSense® Support Matrix』（2024年3月21日にアクセス）、https://www.indexengines.com/csmatrix。
50. Dell Technologies、『CyberSense® for PowerProtect Cyber Recovery』。
51. Rubrik、『Keep Your Databases Running in the Face of Any Threat』。
52. Index Engines、『CyberSense® Support Matrix』。
53. Dell Technologies、『Dell EMC Avamar for Hyper-V』。
54. Dell Technologies、『Dell EMC NetWorker Module for Microsoft for Hyper-V』。
55. Rubrik、『Anomaly incidents』（2024年4月2日にアクセス）、https://docs.rubrik.com/en-us/saas/saas/anomaly_incident.html。
56. Rubrik、『Data Threat Analytics events』（2024年4月2日にアクセス）、https://docs.rubrik.com/en-us/saas/saas/ri_events.html。
57. Rubrik、『Viewing Anomaly Detection』（2024年4月2日にアクセス）、https://docs.rubrik.com/en-us/saas/saas/viewing_ri_investigations.html。
58. Rubrik、『VM Encryption Detection』（2024年4月2日にアクセス）、https://docs.rubrik.com/en-us/saas/saas/vm_encryption_detection.html。
59. Rubrik、『Viewing the Threat Monitoring page』（2024年4月2日）、https://docs.rubrik.com/en-us/saas/saas/viewing_the_threat_monitoring_page.html。
60. Rubrik、『Initiating a threat hunt』（2024年4月2日）、https://docs.rubrik.com/en-us/saas/saas/initiating_a_threat_hunt.html。
61. Rubrik、『Quarantining matched files or objects』（2024年4月2日にアクセス）、https://docs.rubrik.com/en-us/saas/saas/quarantining_matched_objects_or_files.html。
62. Dell、『CyberSense® for PowerProtect Cyber Recovery』。
63. Dell、『CyberSense® for PowerProtect Cyber Recovery』。
64. Index Engines、『The Power of CyberSense's Machine Learning』（2024年4月2日にアクセス）、https://go.indexengines.com/csmachinelearning。
65. Index Engines、『The Power of CyberSense's Machine Learning』。
66. Index Engines、『The Power of CyberSense's Machine Learning』。
67. Dell、『CyberSense® for PowerProtect Cyber Recovery』。
68. Rubrik、『Anomaly Detection behavioral model』（2024年5月20日にアクセス）、https://docs.rubrik.com/en-us/saas/saas/anomaly_detection_behavioral_model.html。
69. Amazon、『Training ML Models』（2024年4月2日にアクセス）、https://docs.aws.amazon.com/machine-learning/latest/dg/training-ml-models.html。
70. Rubrik、『Defense in Depth with Polaris Radar』（2024年3月21日にアクセス）、https://www.rubrik.com/content/dam/rubrik/en/resources/white-paper/Defense-In-Depth-Polaris-Radar-Technical-White-Paper.pdf。
71. Rubrik、『Data Threat Analytics dashboard』（2024年3月21日にアクセス）、https://docs.rubrik.com/en-us/saas/saas/ri_dashboard.html。

72. Rubrik、『Initiating a threat hunt』（2024年3月21日）、https://docs.rubrik.com/en-us/saas/saas/initiating_a_threat_hunt.html。
73. SentinelOne、『What Is A Malware File Signature (And How Does It Work)?』（2024年4月4日にアクセス）、https://www.sentinelone.com/blog/what-is-a-malware-file-signature-and-how-does-it-work/。
74. Rubrik、『Threat hunts』（2024年3月21日にアクセス）、https://docs.rubrik.com/en-us/saas/saas/ri_threat_hunts.html。
75. Rubrik、『Anomaly Detection features』（2024年3月22日にアクセス）、https://docs.rubrik.com/en-us/saas/saas/ri_features.html。
76. Rubrik、『Behavioral model』。
77. Index Engines、『The Power of CyberSense's Machine Learning』。
78. Dell、『CyberSense® for PowerProtect Cyber Recovery』。
79. Rubrik、『Behavioral model』。
80. Rubrik、『Anomaly Detection features』
81. Rubrik、『Behavioral model』。
82. Dell、『CyberSense® for PowerProtect Cyber Recovery』。
83. Morningstar、『Index Engines' CyberSense Announces 99.99% SLA in Detecting Ransomware Corruption, Empowering Smarter Recovery』（2024年7月17日にアクセス）、https://www.morningstar.com/news/pr-newswire/20240618ny41171/index-engines-cybersense-announces-9999-sla-in-detecting-ransomware-corruption-empowering-smarter-recovery。
84. Rubrik、『Threat Monitoring』（2024年3月22日にアクセス）、https://docs.rubrik.com/en-us/saas/saas/threat_monitoring.html。
85. Index Engines、『The Power of CyberSense's Machine Learning』。
86. Index Engines、『The Power of CyberSense's Machine Learning』。
87. Rubrik、『Anomaly Detection features』（2024年3月22日にアクセス）、https://docs.rubrik.com/en-us/saas/saas/ri_features.html。
88. Index Engines、『The Power of CyberSense's Machine Learning』。
89. Rubrik、『Investigating and recovering anomalous files for filesets』（2024年3月22日にアクセス）、https://docs.rubrik.com/en-us/saas/saas/investigating_and_recovering_anomalous_files.html。
90. Rubrik、『Investigating and recovering anomalous files for virtual machines』（2024年3月22日にアクセス）、https://docs.rubrik.com/en-us/saas/saas/investigating_and_recovering_anomalous_files_for_virtual_machines.html。
91. Rubrik、『Full snapshot recovery of a virtual machine』（2024年3月22日にアクセス）、https://docs.rubrik.com/en-us/saas/saas/full_snapshot_recovery_of_a_virtual_machine.html。
92. Rubrik、『Recovery of a batch of virtual machines』（2024年3月22日にアクセス）、https://docs.rubrik.com/en-us/saas/saas/ri_batch_recovery_of_vm.html。
93. Rubrik、『Performing bulk recovery for Recovery Plans』（2024年3月22日にアクセス）、https://docs.rubrik.com/en-us/saas/saas/performing_bulk_recovery_for_recoveryplans.html。
94. Rubrik、『Recovery of a batch of virtual machines』（2024年4月4日にアクセス）、https://docs.rubrik.com/en-us/saas/saas/ri_batch_recovery_of_vm.html。
95. Rubrik、『Recovery of virtual machines』（2024年4月16日にアクセス）、https://docs.rubrik.com/en-us/saas/saas/vs_recovery_vm.html。
96. 通常、リカバリーされたデータストアはRubrikクラスターに配置され、本番環境にはありません。
97. Rubrik、『Recovery of a batch of virtual machines』（2024年4月16日にアクセス）、https://docs.rubrik.com/en-us/saas/saas/ri_batch_recovery_of_vm.html。
98. Dell、『Restore plan』（2024年4月16日にアクセス）、https://infohub.delltechnologies.com/en-US/l/powerprotect-data-manager-protection-for-vmware-cloud-foundation-on-dell-emc-vxrail-1/restore-plan/。
99. Dell、『PowerProtect Data Manager overview』（2024年4月16日にアクセス）、https://infohub.delltechnologies.com/en-US/l/dell-powerprotect-data-manager-deployment-best-practices-1/powerprotect-data-manager-overview-4/。
100. Dell、『PowerProtect Data Manager 19.9 Administration and User Guide』（2024年4月16日にアクセス）、https://www.dell.com/support/manuals/en-us/enterprise-copy-data-management/pp-dm_19.9_ag/file-level-restore-of-a-powerprotect-backup-in-the-vsphere-client。
101. Dell、『Recovery Orchestration with PowerProtect Data Manager Overview』（2024年4月16日にアクセス）、https://www.youtube.com/watch?v=po2oMnAg_x4。
102. Rubrik、『Quarantine files or objects』（2024年3月24日にアクセス）、https://docs.rubrik.com/en-us/saas/saas/quarantine.html。
103. Rubrik、『Downloading quarantined files for forensic analysis』（2024年3月24日にアクセス）、https://docs.rubrik.com/en-us/saas/saas/downloading_quarantined_files_for_forensic_analysis.html。
104. Forrester、『The Total Economic Impact™ Of Dell PowerProtect Cyber Recovery』（2024年4月16日にアクセス）、https://www.delltechnologies.com/asset/en-us/products/data-protection/industry-market/the-total-economic-impact-dell-powerprotect-cyber-recovery.pdf。
105. Rubrik、『Workload recovery during an RSC service disruption』（2024年4月16日にアクセス）、https://docs.rubrik.com/en-us/saas/saas/workload_recovery_during_rsc_outage.html。
106. Rubrik、『Rubrik CDM APIs and service account workflows』（2024年4月16日にアクセス）、https://docs.rubrik.com/en-us/saas/saas/rubrik_apis_sa_workflows.html。

107. Rubrik、『Recoverable workloads during RSC service disruption』（2024年4月16日にアクセス）、https://docs.rubrik.com/en-us/saas/saas/recoverable_workloads_during_rsc_service_disruption.html。

108. Rubrik、『Workloads require third-party tools for recovery』（2024年4月16日にアクセス）、https://docs.rubrik.com/en-us/saas/saas/workloads_require_third_party_tools_for_recovery.html。

109. NIST、『Computer Security Resource Center Glossary: air gap』（2024年7月29日にアクセス）、https://csrc.nist.gov/glossary/term/air_gap。

110. Dell、『Dell PowerProtect Cyber Recovery Solution Guide』。

111. Dell、『Dell PowerProtect Cyber Recovery: Reference Architecture』

112. Adam Eckerle、『Debunking the Myths about Air Gaps』（2024年3月14日にアクセス）、https://www.rubrik.com/blog/technology/2021/11/debunking-the-myths-about-air-gaps。

113. Rubrik、『Air-Gap, Isolated Recovery, and Ransomware - Cost vs. Value』（2024年3月14日にアクセス）、https://www.rubrik.com/content/dam/rubrik/en/resources/solutions-brief/Air-Gap-Isolated-Recovery-and-Ransomware-Cost-vs.-Value.pdf。

114. Brian Williams、『Rubrik Air Gap and Immutability』（2024年3月14日にアクセス）、https://vimeo.com/561870246。

115. Rubrik、『Retention locks in the Rubrik cluster』（2024年3月18日にアクセス）、https://docs.rubrik.com/en-us/9.0/sg/security_guide/retention_locks_in_the_rubrik_cluster.html。

▶ オリジナルの英語版レポートはこちらでご覧いただけます

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。

Principled Technologies®

Facts matter.®