政策方針書

OpenText の企業向けバックアップ / リカバリソリューション Data Protector のセキュリティ

opentext™

目次

ページ

マルウェアがバックソリューションに忍び込む可能性がないようにし、すべてのデータの移動や保存を暗号化して行うことが必要です。

セキュリティ戦略の一環としての Data Protector

データ保護 (バックアップとリカバリ) がセキュリティ戦略の一環であるとされるのを不思議に思うかもしれません。

第一に、バックアップデータを安全で攻撃を受けないようにしたいはずです。マルウェアがバックソリューションに忍び込む可能性がないようにし、すべてのデータの移動や保存を暗号化して行うことが必要です。使用する戦略 (3-2-1 など) に応じて、バックアップコピーをさまざまな場所や多様な種類のメディアに保存する必要があります。これはすべて中央コンソールから実施し、レポート作成、監査、モニタリングが簡単に自動実行されるようにしなければなりません。

次に、情報が失われたり破損したりした場合には、DP は最後の防御線となります。ボタンひとつで重要なデータを取り戻すことができ、感染したデータを置き換え、失われたデータを復元します。その対象は、ファイアウォールサーバー、ネットワークプロキシ、またはデジタル著作権管理ソリューションのようなセキュリティシステムであったかもしれません。

この政策方針書では、Data Protector がより大きなセキュリティ戦略の一環として使用する概念や機能のそれぞれについて紹介します。

セキュリティモデル

セキュリティはすべてのベースラインです。

バックアップデータの処理方法は、出発点からセキュアであることが必須です。もし攻撃者がコマンドやバックエンドに保存されているデータや移動中のデータに忍び込むことが可能であれば、コンセプト全体が疑わしいものになります。そのため、手順全体をサポートするさまざまなセキュリティ機能を導入しています。

セキュリティ向上のために最初に取る非常にシンプルなステップは、主要な DP コンポーネントを備えたセキュリティ強化版 Linux プラットフォームを使用することです。Linux はマルウェア攻撃に対しての脆弱性が低いと考えられるからです。DP が内部データベースを使用するため、侵入がさらに困難になります。

こうしたセキュリティ機能は、コモンクライテリア (CC) の認定を取得するための重要なポイントです。これ以降の主なトピックは、暗号化、ネットワーク、アーキテクチャ、ストレージです。

コモンクライテリア (CC) 認定
情報技術セキュリティ評価のためのコモンクライテリア (**Common Criteria** あるいは **CC**) は、情報技術セキュリティ認証の国際標準 (ISO IEC 15408) です。最新版はバージョン 3.1 リビジョン 5 です。

コモンクライテリアは、コンピュータシステムのユーザーがセキュリティターゲット (ST) におけるセキュリティの**機能要件**と**保証要件** (それぞれ SFR と SARS) を**規定**できるフレームワークで、保護プロファイル (PP) から取得できます。ベンダーは、製品のセキュリティ属性を**実装**または主張することができ、テストラボは製品を**評価**して、実際に主張を満たしているかどうかを判断できます。つまりコモンクライテリアによって、使用する対象の環境にふさわしいレベルの、厳格で標準化された反復可能な方法で、コンピュータセキュリティ製品の仕様作成、実装、評価が実施されていることが保証されます。

Data Protector は、実績があり認定を受けたマルウェア・ランサムウェア対策ソリューションを利用しています。

本文テキストは、サイズ 11 の Calibri フォントで、フォント色は黒でスタイル設定されています。適切なコミュニケーションは、メッセージが意図したとおりに受信され、理解されたときに発生します。事前に書かれた承認済みの資料については、Brand Central をご確認ください。

エンタープライズクラスのスケーラビリティとセキュリティ

DATA PROTECTOR のセキュリティモデル

- 集中管理された指揮と統制
- TLS を介したセキュアなクライアント通信
- 自由に構成可能なデータ暗号化
- クライアントごとの AES/TLS データ暗号化
- ユーザー認証と LDAP 統合
- ネットワークポートの統合：DP 動作用の主要ポートは 1 つだけ

ランサムウェアからのリカバリ戦略

ランサムウェアからのリカバリ戦略を成功させるためには、次のような複数のステップをサポートする必要があります。

- ランサムウェアが想定している期間を超える保持期間 (少なくとも 6 か月)。スナップショットでは長期保存が提供されません。ストレージシステムが急速にいっぱいになったり、全体的なストレージパフォーマンスが低下したりすることがあり、ソースボリュームから独立していないためです。**スナップショットは、データの独立した 1 対 1 のコピーではありません。**
- 別の (感染していない) システムに復元できること
- 検証プロセスを使用してバックアップセットをテストし、リストア手順をテストする
- プラットフォームや、複数のコピーで使用されるバックアップデバイスから独立している
- 3-2-1、3-2-1-1-0、4-3-2 のバックアップ戦略をサポート
- 明確な RTO/RPO が設定されており、レポートで定期的に検証される
- 主要なエントリポイントであるワークステーションとサーバーでスキャン / 検出が実行される

Data Protector は、各バックアップセッションの終了時に、内部データベース (IDB) からのバックアップオブジェクト情報を各メディアに保存します。これにより、メディアを「送出」することで、ある CM から別の CM にバックアップデータを移行できます。

マルウェア対策の構成要素

このセクションでは、リカバリ戦略と OpenText が提供している複合ソリューションを示します。

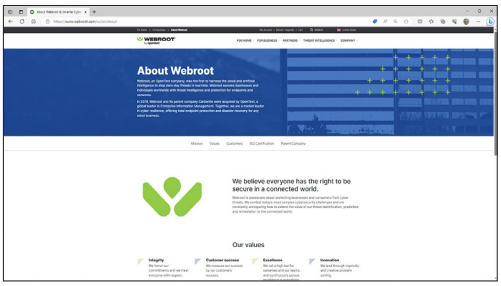
Type of Activity	Data Protector
Offline Backup	✓
True Air Gap Backup	✓
Immutable Backup	✓
WORM Media	✓
Backup Verification	✓
Enhanced Automatic DR	✓

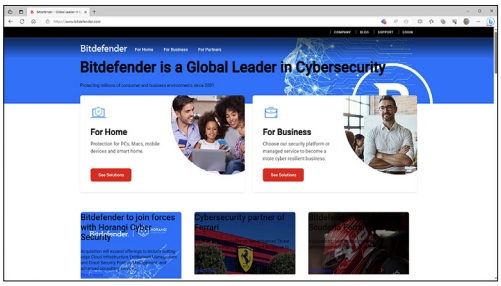
Backup Method	Data Protector
Backup to Cloud	Data Protector supports private and public cloud as backup target.
Backup to Tape	Data Protector supports an exhausting list of Tape Drives and Tape Libraries
Backup to Disk	Data Protector makes use of deduplication Appliance Features. Data-at-Rest Encryption, Data Immutability, Data Replication, Cloud Upload
Backup Replication	Data Protector provides the option to configure a second cell in remote (DR) location.
Secure Backup Transport	Data Protector provides encrypted command and data communication

ソリューションとしてのマルウェア保護

Data Protector は、実績があり認定を受けたマルウェア・ランサムウェア対策ソリューションを利用しています。これらは継続的に更新され、多くの機会で有効性が証明され、業界のリーダーに受け入れられています。バックアップセットに感染する前に感染を検出することが重要です。したがって、バックアップおよびリストアのパフォーマンスが著しく低下しないように、データのスキャンはバックアップクライアントで実行する必要があります。これにより RPO/RTO の再設計が必要になります。

DP は、OpenText Webroot または BitDefender とのセットでも提供可能ですが、これらの 2 つに限定されません。





ランサムウェア / マルウェアからのリカバリオプション：EADR

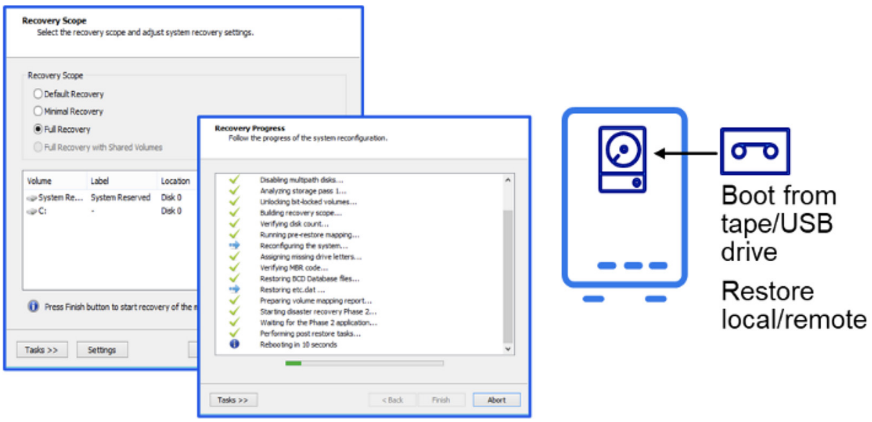
感染したシステムの一部または全部をオンラインのまま上書きするのは危険すぎることがあります。その場合は、DP の拡張自動障害復旧 (EADR) の手順を使用してシステムを消去し、回復できます。このプロセスは部分的にオフラインで、パーティションとファイルシステムのセットアップから開始して、以前あったマルウェアの残骸を消去します。このプロセスは、物理サーバーでも仮想サーバーでも機能します。

ベアメタル障害復旧：

- 拡張自動障害復旧 (EADR)
- 手動 DR
- 別システムへの DR
- 仮想マシンへの DR (P2V)

注：中規模から大規模の移行の場合は、推奨ソリューションとして PleateSpin が提供されています。

不変性により、定義された時間枠がなくなるまでは、バックアップデータのバックアップターゲットからの変更や削除はできません。



Cell Manager が失われた場合の対応

Cell Manager (CM) がマルウェア攻撃で失われ、CM のリストアが何らかの理由で機能していないと想定します。

Data Protector は、各バックアップセッションの終了時に、内部データベース (IDB) からのバックアップオブジェクト情報を各メディアに保存します。これにより、メディアを「送出」することで、ある CM から別の CM にバックアップデータを移行できます。一方、必要なメディアをすべてインポートすることによって CM IDB を再作成することもできます。

メディアは常時 CM から切断された状態です。CM に何が起ころうと、それがバックアップメディアに到達することはありません。また、DP には、通常のデータベースのような外部への公開がない内部データベースが付属しています。

- DP によってバックアップされたシステム上で感染が特定されている (マルウェアスキャナで実行され、ツールで感染を駆除できなかった)
- DP Cell Manager に送信される情報とスケジュールは、このクライアントで一時停止 / 無効化される (この部分は、現在は手動で統合する必要がある)
- DP は感染前の時間枠からのリストアを表示する (最終の正常確認版)
- クライアントデータのリストア / 上書きを提供するか、さらに確認するためにまず安全な場所にリストアする
- マルウェアスキャナが、クライアントがクリーンであり本番環境に戻すことができると確認

Data Protector は、バックアップデバイス管理について普遍的なアプローチを取っており、このアプローチをサポートしています。データ管理は DP オブジェクトコピー機能を使用して実行されます。この機能を使用すると、バックアップデータをいつでも他のデバイスにコピー / 移行できます。

マルウェアからのリカバリのワークフロー

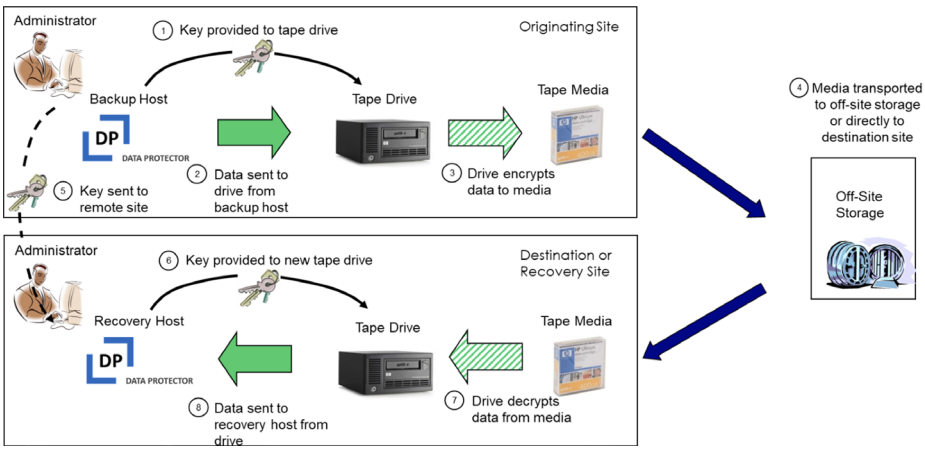
- DP によってバックアップされたシステム上で感染が特定されている (マルウェアスキャナで実行され、ツールで感染を駆除できなかった)
- DP Cell Manager に送信される情報とスケジュールは、このクライアントで一時停止 / 無効化される (この部分は、現在は手動で統合する必要がある)
- DP は感染前の時間枠からのリストアを表示する (最終の正常確認版)
- クライアントデータのリストア / 上書きを提供するか、さらに確認するためにまず安全な場所にリストアする
- マルウェアスキャナが、クライアントがクリーンであり本番環境に戻すことができると確認

テープドライブの暗号化

テープドライブとメディアは、ランサムウェアやウイルスなどのマルウェアからの保護に対処するセキュリティソリューションにおける究極のエアギャップアプローチです。

- まず、テープメディアではファイルシステムのようなアクセスが提供されないため、マルウェアから直接アクセスされることが一切ありません。データは通常、インターリーブのうえ暗号化され、デバイスを使用するバックアップアプリケーションによってのみ読み取り可能です。
- 次に、ドライブまたはライブラリからテープメディアを取り出して、セキュアな場所に保存することができます。これもまた、火災、洪水、地震などの災害への対処となります。
- テープメディアは、セキュアでない可能性のある WAN 接続を介してデータを移動させることなく、別の場所に移動させることができます。また、非常に大量のデータを一度に移動することもできます。
- DP は、場所情報を設定することにより、メディアのヴォールティングをサポートします。メディアを失いたくはないはずです。
- 最後に、テープメディア上のデータを暗号化して WORM (Write-Once, Read Many) 形式で使用することで、物理層で変更が発生するのを防ぐことができます

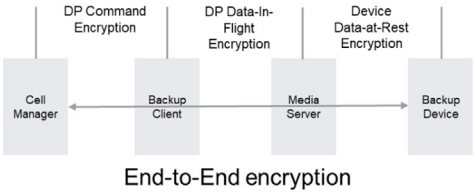
テープドライブ暗号化のワークフロー



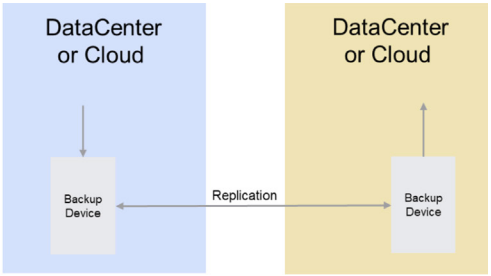
重複排除用のソフトウェアとアプライアンスの暗号化

重複排除アプライアンスを使用する場合、次の機能が最も重要です。

- 暗号化
- レプリケーション
- 不変性



End-to-End encryption



不変性

Data Protector は、以下の機能でバックアップターゲットの不変性をサポートしています。

- DP 重複排除 (ソフトウェアベースの重複排除ターゲット)
- HPE StoreOnce (アプライアンスベースの重複排除ターゲット)
- Dell/EMC DataDomain (アプライアンスベースの重複排除ターゲット)

不変性により、定義された時間枠がなくなるまでは、バックアップデータのバックアップターゲットからの変更や削除はできません。これにより、バックアップマネージャシステムの感染や使用不能からも、管理者によるメディア管理のミスからも保護されます。バックアップデータは、不変期間中はいつでもバックアップマネージャシステムに再インポートできます。

バックアップ戦略

Data Protector は、次のように多くのバックアップ戦略をサポートしています。

- 3-2-1 バックアップ戦略
- 3-2-1-1-0 バックアップ戦略
- 4-3-2 バックアップ戦略

また、戦略を組み合わせて使用することも、カスタマイズした独自の戦略を作成することもできます。最も重要なのは戦略が存在することであり、定期的なテストは必須要素であり、ビジネス継続性計画の一部です。

3-2-1 戦略

3-2-1 ルールでは、データの 3 つのコピー (例：プライマリコピー 1 つとバックアップ 2 つ) を 2 つの異なるメディア (例：内部ハードディスク上にプライマリコピー、テープにバックアップコピーを 1 つ、さらに外部ハードディスクもしくはテープにもう 1 つのバックアップコピー) に保存し、1 つのコピー (通常はテープバックアップ) をオフサイトに保存することが推奨されています。

Data Protector は、バックアップデバイス管理について普遍的なアプローチを取っており、このアプローチをサポートしています。データ管理は DP オブジェクトコピー機能を使用して実行されます。この機能を使用すると、バックアップデータをいつでも他のデバイスにコピー / 移行できます。プライマリバックアップが何らかの理由で使用できない場合は、コピーが自動的に使用されます

バックアップ完了直後にデータを移行するアプローチが好まれることも、データの大部分については専用の時間枠内で移動する統合アプローチが好まれることもあります。

3-2-1-1-0 戦略

3-2-1-1-0 戦略では、次のことを推奨しています。

- ビジネスデータのコピーを少なくとも 3 つ保持する。
- 少なくとも 2 種類のストレージメディアにデータを保存する。
- バックアップのコピーを 1 つオフサイトに保管する。
- そのメディアのコピー 1 つをオフラインにするか、エアギャップを確保する。
- すべての復元性ソリューションにエラーがないことを確認する。

このアプローチでは、3-2-1 と同じ機能セットを使用しますが、さらに DP オブジェクト検証を使用して、表示されているメディアレベルではないエラーをチェックします。これにより、バックアップの品質が保証され、適切に報告されます。

4-3-2 戦略
バックアップ戦略に、4-3-2 ルールが採用される場合もあります。

- データのコピーは 4 つ。
- 3 つの場所にデータを保存 (自分のオンプレミス、MSP のオンプレミス、クラウドプロバイダー)
- オフサイトの 2 か所にデータを保管。

OpenText 商標情報

会社情報

会社名：OpenText
登記場所：イングランドおよびウェールズ
登記番号：5134647
登記住所：The Lawn, 22-30 Old Bath Road, Berkshire, RG14 1QN

詳細はこちら：
www.microfocus.com/ja-jp/products/data-protector-backup-recovery-software/overview

お問い合わせ

262-JA0094-001 | O | 03/24 | © 2024 Open Text

opentext™