DELL TECHNOLOGIES PARTNER PROGRAM
HEROES

Heroes Forum 2022 April

もはや必須で考慮が必要！
PowerProtect Cyber Recovery

デル・テクノロジーズ株式会社
パートナーセールスエンジニアリング本部
近藤　正樹

DELL Technologies
PARTNER PROGRAM

日本の製粉大手に「前例ない」大規模攻撃　大量データ暗号化　起動不能、バックアップもダメで「復旧困難」

2021年

日経コンピュータ「ITが危ない」　＋ 連載をフォロー

トヨタの工場を止めたサイバー攻撃　サプライチェーン攻撃のリスクが露呈

島津 忠承

デンソー独法人にサイバー攻撃　犯罪グループ「Pandora」がダークウェブで犯行声明

2022年03月14日 14時45分 公開　[ITmedia]

印刷　105　Share　B!　4　0

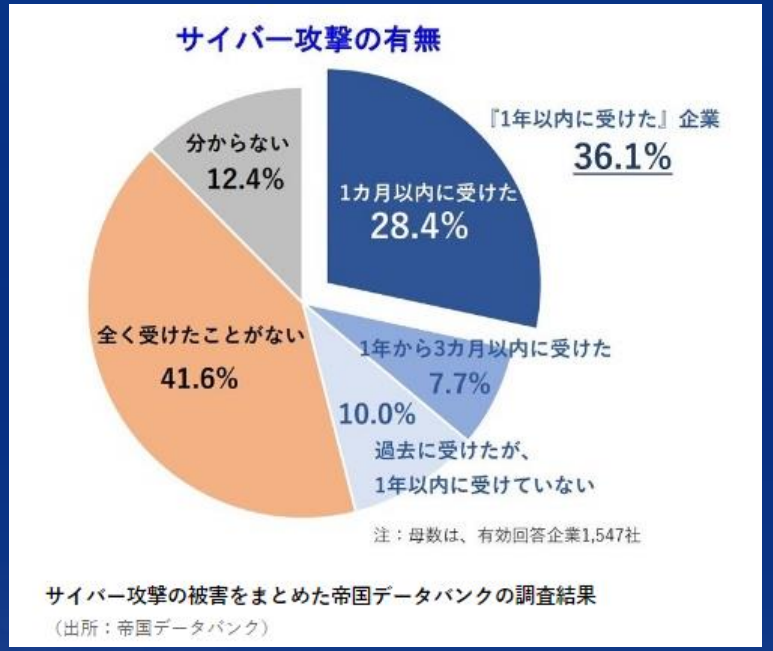
PR 今日からはじめるGitHub。導入や初歩的な使い方を解説

デンソーは3月13日、ドイツ法人「デンソー・オートモーティブ・ドイツ」が3月10日にランサムウェアを使ったサイバー攻撃を受けたと明らかにした。13日にはサイバー犯罪グループ「Pandora」がダークウェブ上で犯行声明を出している。

デンソードイツ法人は自動車部品の開発と販売を手掛ける子会社。デンソーは10日に不正アクセスの痕跡を確認。感染拡大防止のため感染デバイスをネットワークから隔離し、ドイツ当局に被害届を提出した。

Pandoraによると、盗み出したデータは1.4TB、15万7000件超えという。ランサムウェアの感染状況や手口、侵入経路、データが実際に同社から盗まれたものかなどは現地で調査中。身代金の要求の有無については「捜査に影響を与えるため回答を控える」（デンソー）としている。

生産会社ではないため生産や販売に影響はなく、今後も通常通り稼働する。



サイバー攻撃の被害をまとめた帝国データバンクの調査結果
（出所：帝国データバンク）

帝国データバンクが3月15日に公表した調査でもサイバー攻撃の検知が急増しているという
結果が出た。

※同社が3月11～14日に企業1547社へ聞き取りを実施。

© Copyright 2022 Dell Inc.

サイバー攻撃の主な手法

	ばらまき型	標的型
主な攻撃手法	スパムメール ドライブバイダウンロード	環境寄生型 ハッキング（コマンド＆コントロール）
主なターゲット	不特定多数	特定企業

暗号化　**破壊／改ざん**　**情報漏えい**

© © Copyright 2022 Dell Inc.

「ただのバックアップ」はサイバー攻撃には無意味

バックアップサーバー（Windows）

バックアップサーバーが標的にされた場合、**バックアップカタログが暗号化/消去される**等のリスク。
または感染したPC等を介し、間接的な被害を受けるケースも。
バックアップサーバーやメディアサーバーが被害を受けた場合、データをどのように保管していても
基本的に**バックアップデータからの復旧は極めて困難**となる。

バックアップストレージ（バックアップデータ保存先）

・ディスク/NAS（CIFS/NFS）

メディアサーバー上のファイルシステムは、**ターゲットにされ暗号化/消去**されます。

・テープ

被害の前にメディアが排出されオフラインで保管されている場合では回復することが可能だが、運用が煩雑化してしまう。
ただし、**バックアップカタログが隔離・破壊されている場合は、オフライン保管のテープからでも復旧は極めて困難**となる。

© Copyright 2022 Dell Inc.

バックアップ　≠　データ保護

Dell Technologies が提供するのは**「データ保護」**ソリューション

重複排除技術による高効率な多世代データ保持

独自のオペレーティングシステムによる侵入リスクの低減

独自の通信プロトコルによる検出リスクの低減

独自のファイルシステムによるデータ破壊リスクの低減

© Copyright 2022 Dell Inc.


PowerProtect Cyber Recovery

データ保護の多層化によるレジリエンス強化

堅牢

サイバー レジリエンス

最も強固

標準的なデータ保護

- あらゆる場所にあるデータを網羅（エッジ、コア、クラウド）
- データ保全が担保されたディスクベースの格納
  （X オフライン/ テープベース）
- 障害を想定した復旧訓練の実施

ばらまき型

データ保全性の強化

- 製品に実装される標準セキュリティ機能の活用
- 保存・移送時の暗号化や多要素認証の追加
- データへの改竄防止機能実装とアクセス権の分掌

サイバー復旧を意識した強固な

- ネットワーク隔離とヴォルト（Vault）の実施
- 隔離され改変されない復旧用データの確保
- 隔離データを用いた高度なセキュリティ分析

標的型

© Copyright 2022 Dell Inc.

サイバー攻撃被害対応実装に向けた”3 STEP”

Point1: 複数バックアップデータセット
Point2: 独自プロトコル(Boost Protocol)

STEP1：10世代以上の世代バックアップ

ランサムが侵入する前のデータセットの保持と、攻撃対象となりにくい 非標準テクノロジーによるバックアップデータの保管	**PowerProtect DD/DP**重複排除による多世代バックアップデータの保持、CIFS/NFSと異なるファイルシステムによるデータ保管

Point3: ネットワーク環境からの物理的隔離
Point4: 改ざん防止によるデータロック

STEP2：ネットワークから隔離された環境(Vault)の構築

ネットワークから隔離されたVault環境を構築し、ランサムの侵入を物理的に防ぎ、更にVault内データセットへ対し改ざん防止を実施	**CR Vault** ,**DD Replication** , **CRSマネージメントサーバ**によるバックアップデータのオフライン隔離

Point5: Vault内リストアデータ検証
Point6: 定期的なバックアップデータの監視

STEP3：クリーンなデータセットを見つけ出し、確実にリストアする

Vault内の10世代以上あるデータセットから、クリーンなデータセットを見つけ出し、検証、リストア、システムの復旧を行う	**Cyber Sense**, **検証サーバ**, **リストアサーバ**によるバックアップデータの衛生管理と、復旧用データセットの特定

© Copyright 2022 Dell Inc.

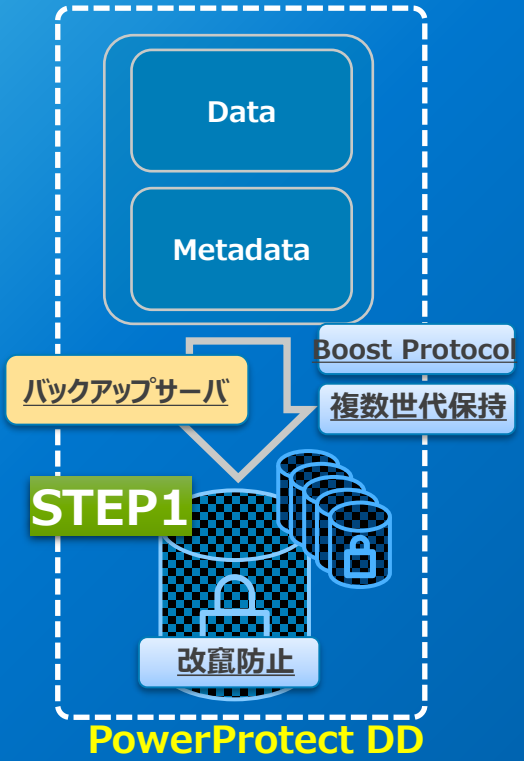
Cyber Recovery Solution 【STEP 1】

- Power Protect DDにデータをバックアップ
- 10世代以上の世代の保持と改ざん防止

Power Protect DDの機能

Cyber Senseの機能（サブスクリプションで提供）

本番環境



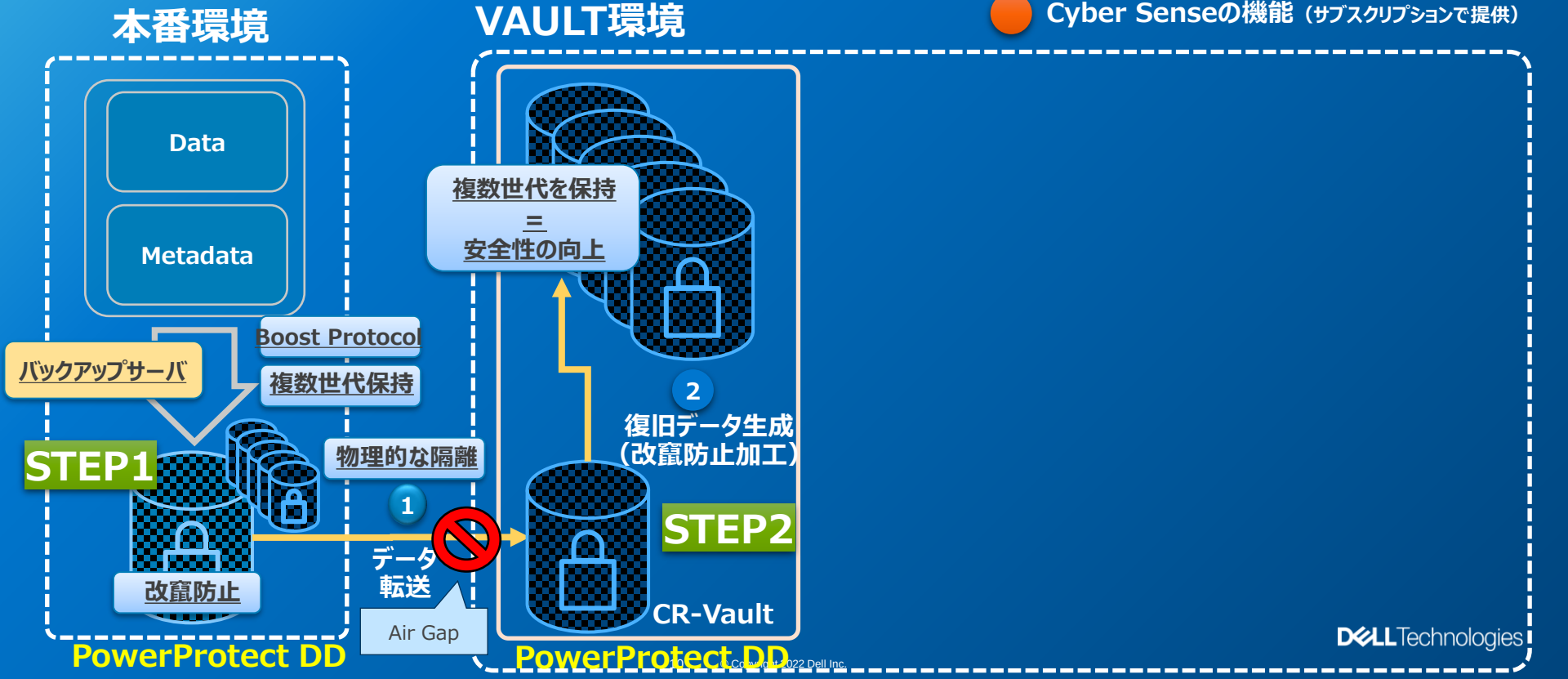
© Copyright 2022 Dell Inc.

Cyber Recovery Solution 【STEP 2】

- Air GAPにより物理的に隔離されたVault環境でデータを転送
- Vault内でも複数世代のバックアップデータセットを保持

Power Protect DDの機能

Cyber Senseの機能（サブスクリプションで提供）



© Copyright 2022 Dell Inc.

Cyber Recovery Solution 【STEP 2】

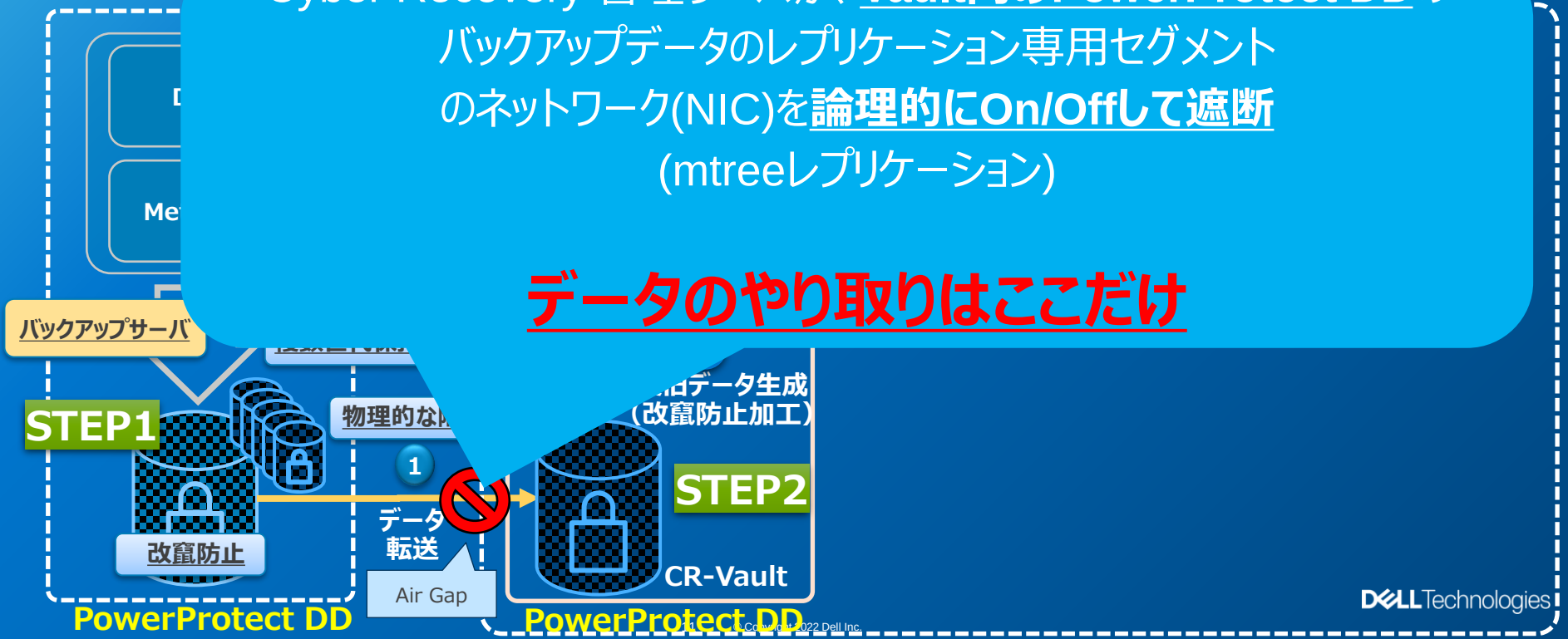
- Air GAPにより物理的に隔離されたVault環境でデータを転送
- Vault内でも複数世代のバックアップデータセットを保持

Power Protect DDの機能

本番

Cyber Recovery 管理サーバが、**Vault内のPowerProtect DD**の
バックアップデータのレプリケーション専用セグメント
のネットワーク(NIC)を**論理的にOn/Offして遮断**
(mtreeレプリケーション)

データのやり取りはここだけ

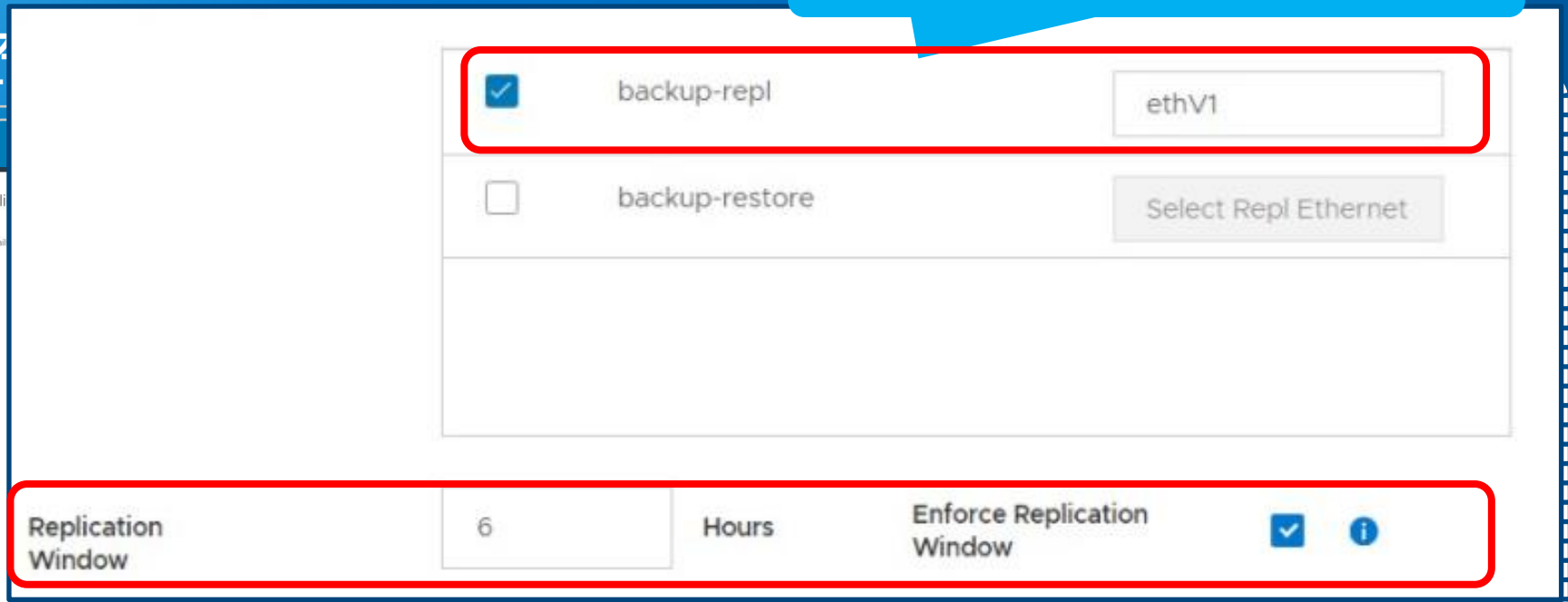


© Copyright 2022 Dell Inc.

Cyber Recovery Solution 【STEP 2】

- Air GAPにより物理的に隔離されたVault環境でデータを
- Vault内でも複数世代のバックアップデータセットを保持

Cyber Recovery GUIからの抜粋



PowerProtect DD

Air Gap

STEP2

CR-Vault

PowerProtect DD

© Copyright 2022 Dell Inc.

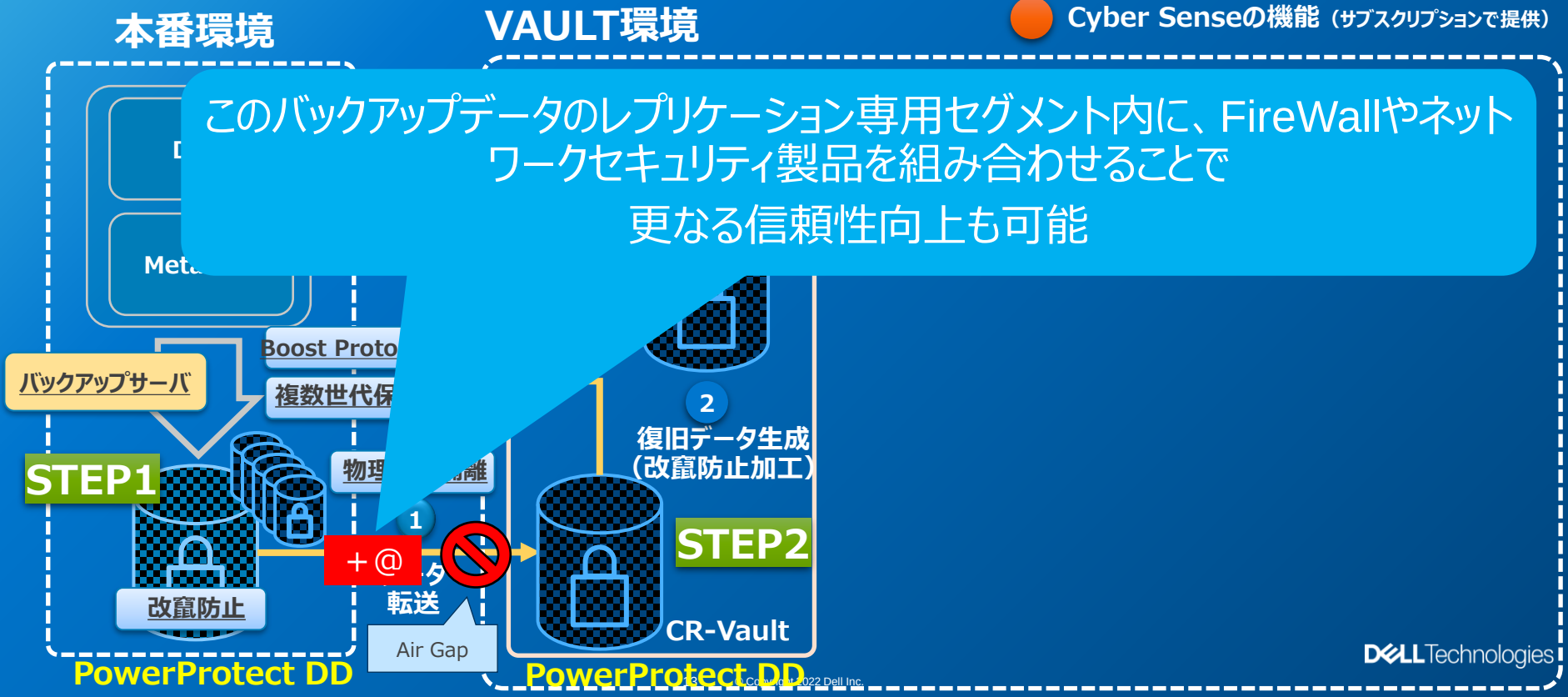
DELL Technologies

Cyber Recovery Solution 【STEP 2】

- Air GAPにより物理的に隔離されたVault環境でデータを転送
- Vault内でも複数世代のバックアップデータセットを保持

Power Protect DDの機能

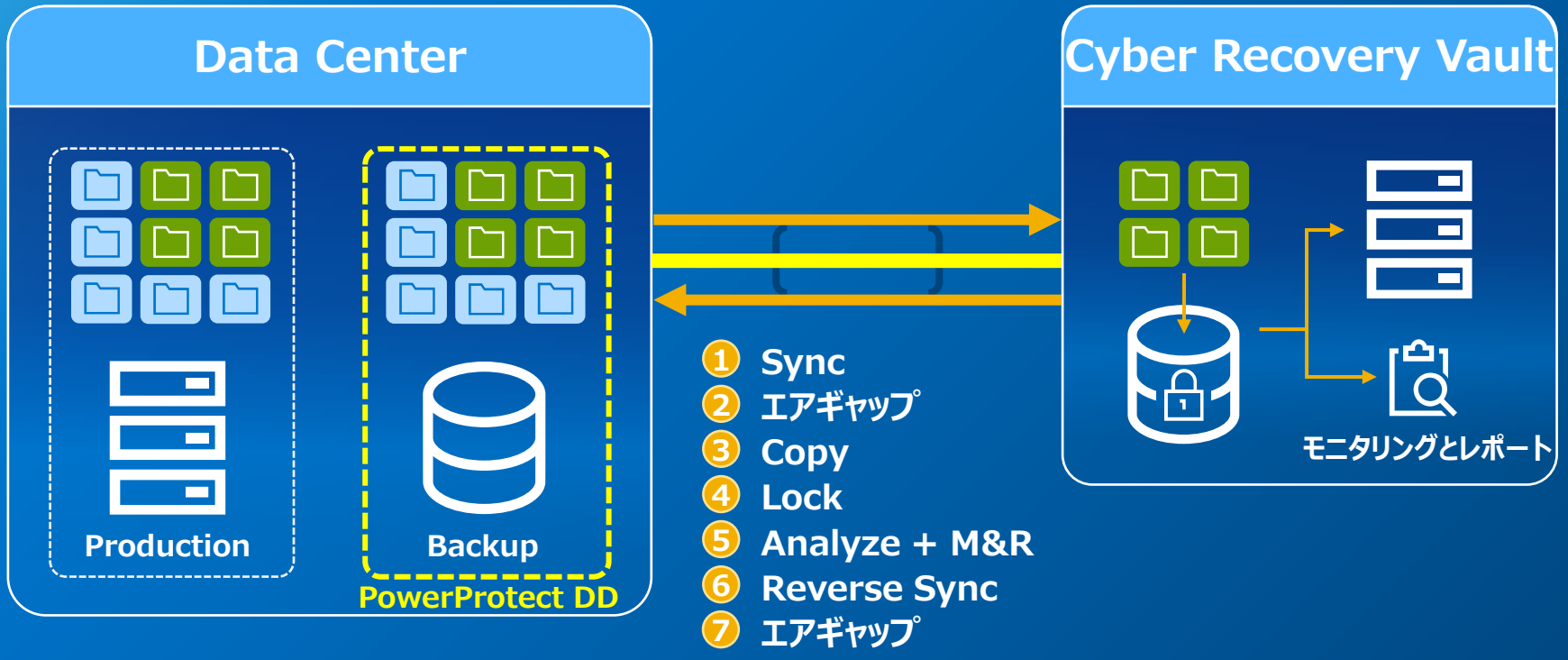
Cyber Senseの機能（サブスクリプションで提供）



© Copyright 2022 Dell Inc.

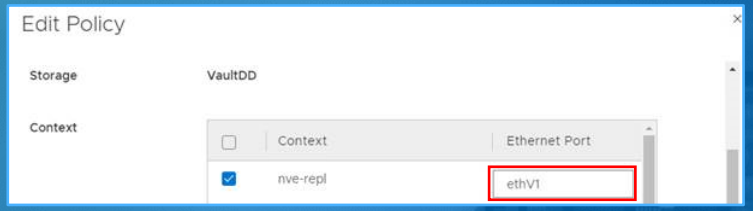
PowerProtect Cyber Recovery (≠ Disaster Recovery)

データヴォルティング（エアギャップ隔離）プロセス



© Copyright 2022 Dell Inc.

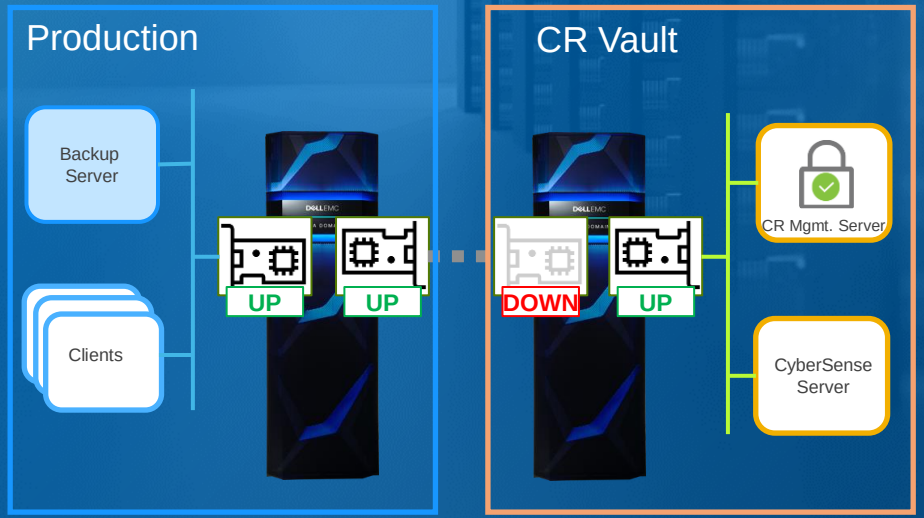
Air Gapの仕組み



CRポリシーでReplicationに使用する
インターフェースを指定。
左の例ではethV1

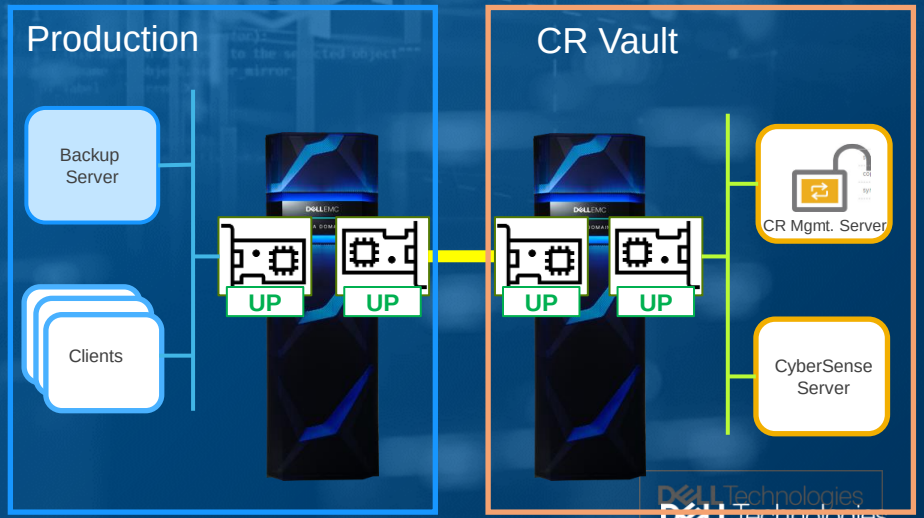
通常時

Sync実行時以外はCR Vault側DDのレプリケーション
インターフェースがDOWNとなりProd-CRV間のリンクはダウン



Replication時

Sync実行時だけCR Vault側DDのレプリケーション
インターフェースがUPとなりProd-CRV間のリンクが疎通



© © Copyright 2022 Dell Inc.

データ「破壊」「改ざん」脅威に対応

サイバー攻撃に対する更なる防御壁の配備

Retention Lock 機能による
バックアップデータの削除や変更を防止

- システム管理者権限を使用しても バックアップデータの変更、破壊、削除は不可
- より高い権限を持ったセキュリティ管理者の監視の元でのシステム管理業務を行う
- ランサムウェア、破損、およびその他の破壊的攻撃に対する付加的な保護を提供

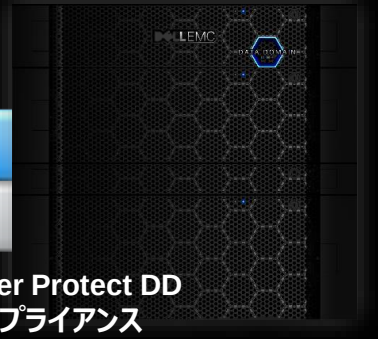
保存期間中はいかなる人もデータを変更できない

データ防御

ソフトウェアのエディション

ガバナンス

コンプライアンス



Power Protect DD
アプライアンス

システム管理者

指定の
「セキュリティ担当者」

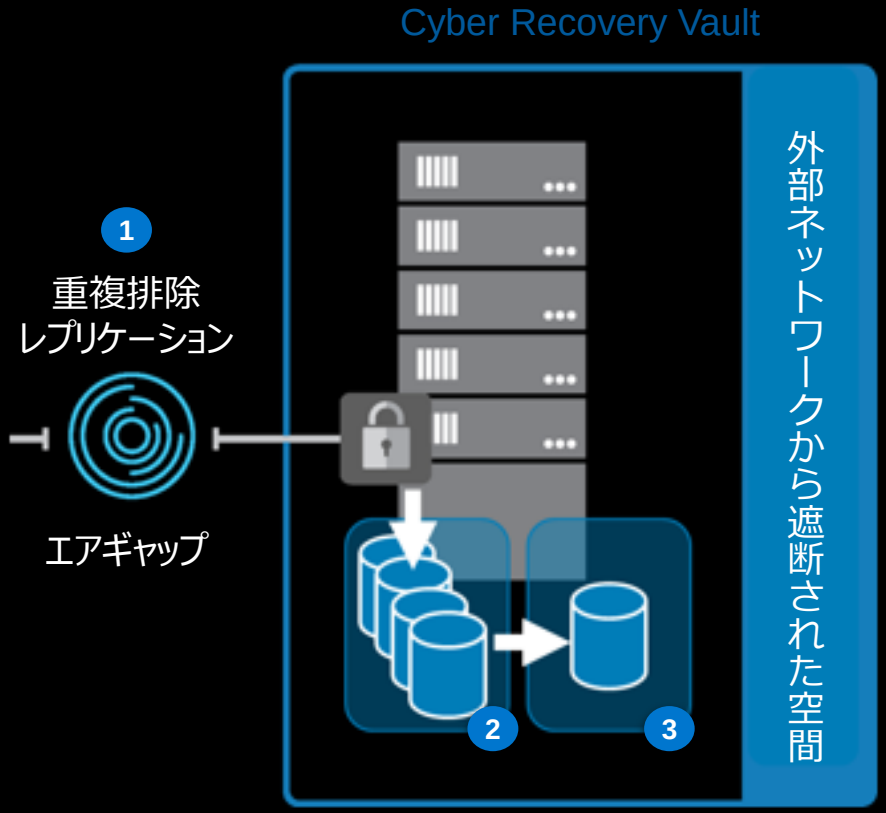
DELL Technologies
PARTNER PROGRAM

© Copyright 2022 Dell Inc.

Cyber Recovery Management Software

ネットワーク隔離(エアギャップ)と復旧データ管理

データ隔離
（隔離）（管理）



1. エアギャップを実現するデータリンク接続・切断の設定とポリシー管理による自動化
2. 「復旧データ」の確保：データの多世代生成・保持と改竄防止ロック適用のポリシー管理による自動化
3. 分析用のサンドボックスデータ生成とエクスポート

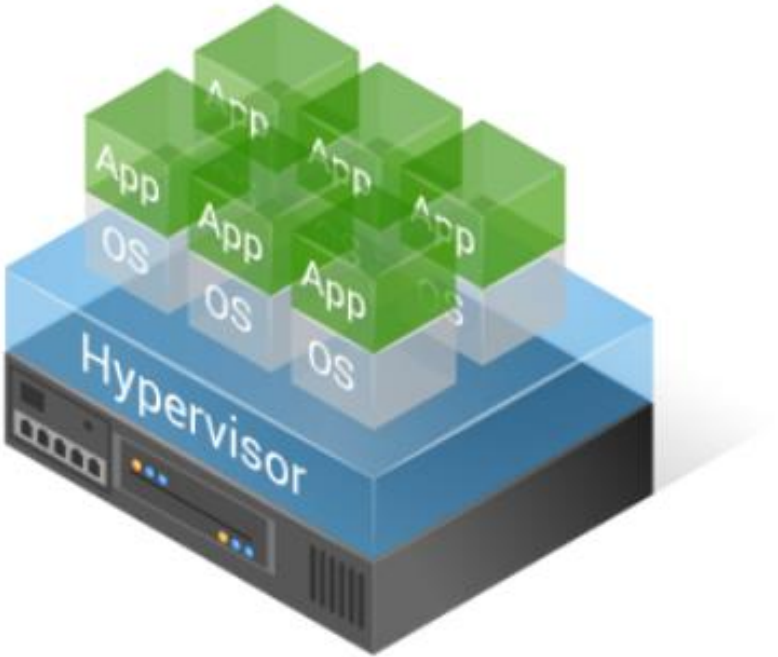
- 専用UI・ダッシュボードによる設定と運用管理の一元化

DELL Technologies
PARTNER PROGRAM

© Copyright 2022 Dell Inc.

Cyber Recovery Virtual Appliance

- Cyber Recovery 仮想アプライアンスは、次の要件を持つVMホストです。
  - VMware vCenter/ESXi、バージョン6.5および6.7。
  - OVA ファイルをデプロイするための約 2 G。
  - 次のようにパーティション分割された 3 台のディスクに約 195 GB。ディスク 1 および 2、48 GB、およびディスク 3、97 GB。シン プロビジョニング環境では、すべての領域が使用されるわけではありません。
  - 4 CPU、ソケットあたりシングルコア。
  - 8 GB のメモリ。



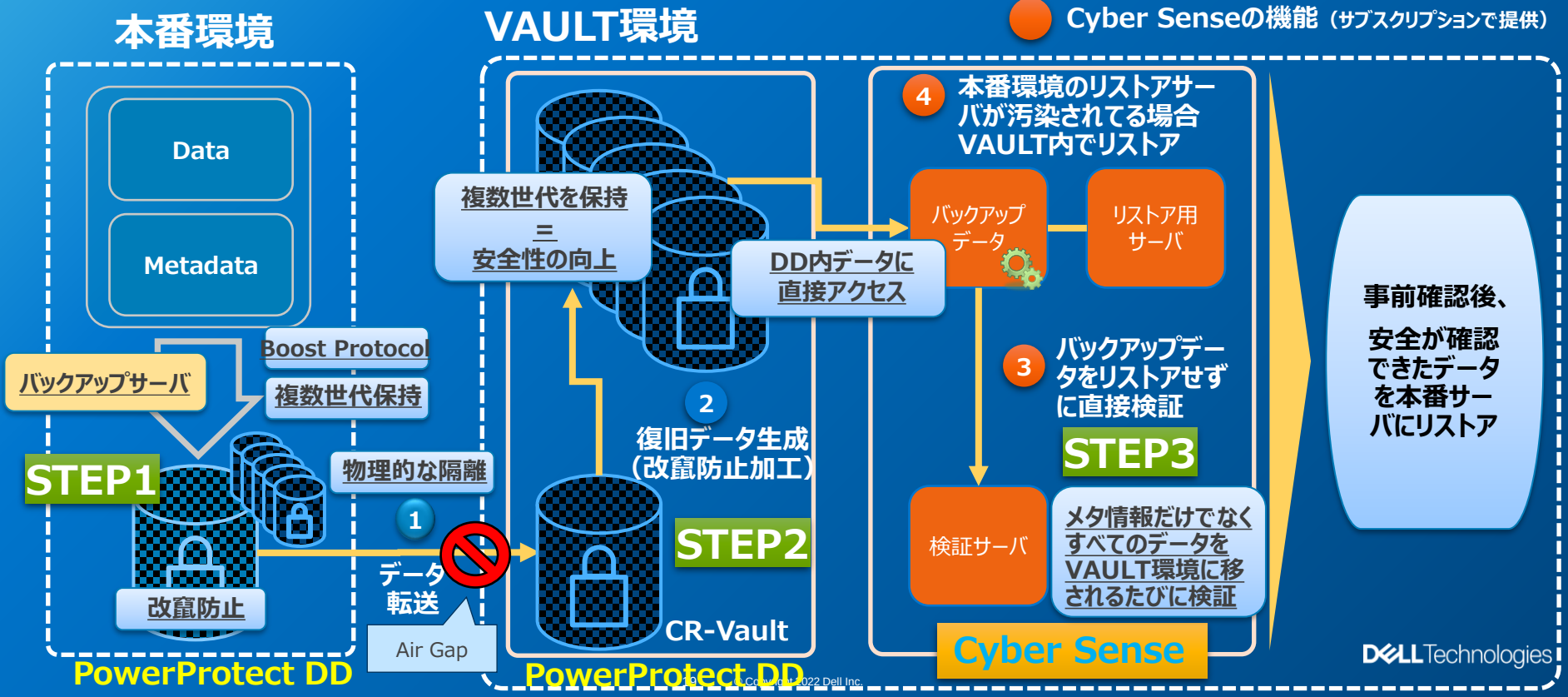
© Copyright 2022 Dell Inc.

Cyber Recovery Solution 【STEP 3】

- 前世代のデータセットとの差分を確認しランサム侵入を検知
- ランサム被害発生時にリストアすべきクリーンデータ私事し迅速にリストア

Power Protect DDの機能

Cyber Senseの機能（サブスクリプションで提供）



© Copyright 2022 Dell Inc.

Dell EMC CyberSence

PowerProtect Cyber Recovery 専用の脅威分析エンジン

データ衛生
（分析）（検証）

- より確実に、最適な復旧用データを準備するための
  サイバー復旧データ専用分析機能
- 「確保」「隔離」「管理」機能と連動した
  「分析」「検証」を提供
- 隔離データから感染兆候
  を発見することで、入口
  対策で検知できなかった
  リスクをフィードバック

© Copyright 2022 Dell Inc.

迅速なレジリエンスを実現する攻撃後の診断

- 迅速なリカバリに必須の情報

WHO?

誰に影響があるのか？

どのくらいのダメージがあるのか？

どのサーバに影響があるのか？

WHAT?

何が攻撃されたのか？

どの部門が攻撃されたのか？

暗号化されたファイルのリストは何なのか？

WHERE?

ソースはどこにあるのか？

ランサムウエアはどこにあるのか？

どのユーザーアカウントが侵害されたのか？

WHEN?

それはいつ起きたのか？

最後の良いデータセットはどこにあるか？

どのバックアップセットがクリーンなのか？

© Copyright 2022 Dell Inc.

CyberSenseのしくみ

機械学習により、サイバー攻撃の早期発見と迅速な回復が可能に

SECURITY ANALYTICS
サイバー攻撃を示す100以上の統計情報

COMPREHENSIVE INDEX
時間の経過に伴うコンテンツの変化

MACHINE LEARNING
数千のトロイの木馬と20以上のアタックベクターのトレーニング

Cyber Recovery with CyberSense

- アタックベクターの通知
- ランサムウェア
- 破損したファイルの詳細
- データの変更/削除
- 侵害されたユーザーアカウント
- 違反した実行可能ファイル
- 最後の健全なコピーによる回復

© Copyright 2022 Dell Inc.

CyberSense と「一般的な」分析の違い

機械学習により、CyberRecoveryボールト内での早期検出と迅速なリカバリが可能

CyberSense:

完全なコンテンツのインデックス作成：

1. ファイル メタデータ
2. ドキュメント メタデータ
3. ドキュメント コンテンツ

99.5%

VS.

Basic Analytics:

オンプレミス分析エンジン

1. ファイルメタデータのみをスキャン

クラウドベース分析エンジン

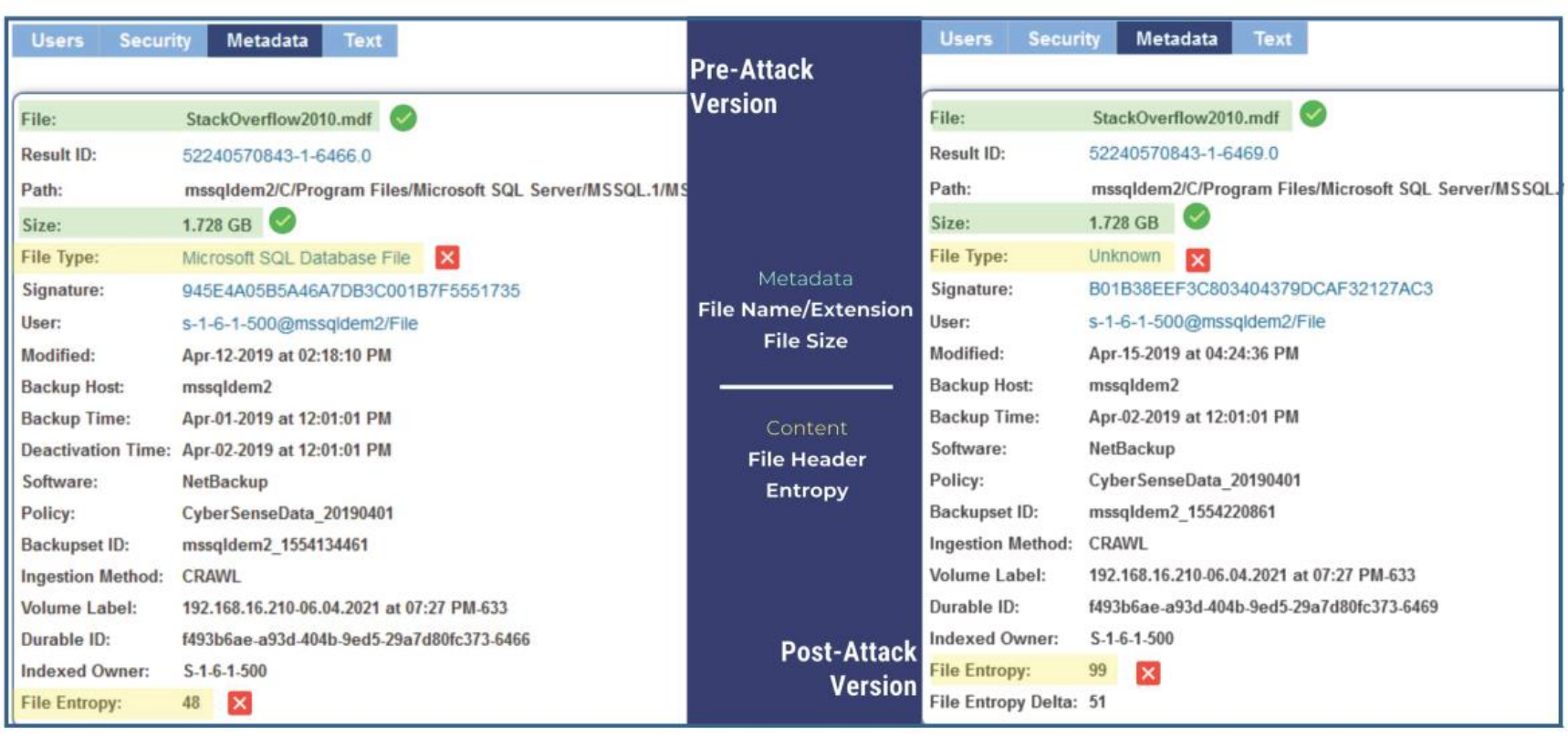
2. 3.

2回目または完全なコンテンツ分析のために疑わしいファイルをクラウドに送信

88%

© Copyright 2022 Dell Inc.

ファイル メタデータでは検知できないケース



Internal Use - Confidential

DELL Technologies

CyberSenseの解析の特徴 - アタックベクターの種類

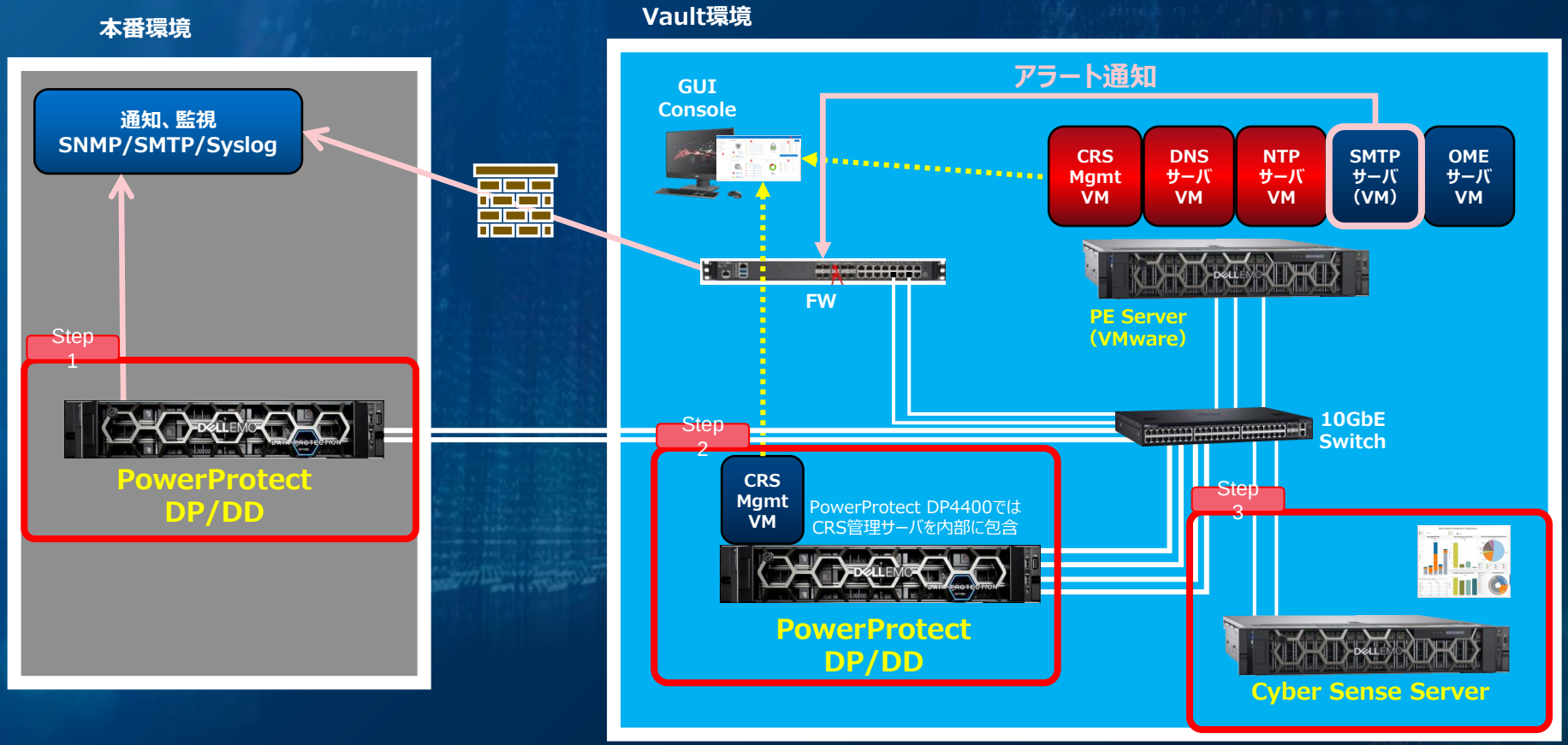
- アタックベクターを特定する分析
- データに特定の影響を与える 28 種類の攻撃がある
  - 暗号化
  - エントロピー変化
  - 削除/作成
  - ファイル拡張子の変更
  - そして、より多くの..
- トップ 6 のアタックベクターが一般的（赤枠）

CyberSenseが着目するポイント

1. 元のファイル名を使用して強力な暗号化を行う	2. 元のファイル名を使用した部分な暗号化	3. RMS/MS_EFS 強力な暗号化	4. 強力な暗号化 新しい既知の拡張機能
5. 部分的な暗号化 新しい既知の拡張子	6. 強力な暗号化 難読化されたファイル名	7. 部分的な強力な暗号化 、難読化されたファイル名	8. 個人アーカイブ
9. おとり交換 (Decoy Replacement)	10. グループアーカイブ	11. Wiper	13. Attack Raw Disk
14.DB Page暗号化	15. Newファイル拡張子	16. ファイル名を難読化	17. 弱い暗号化 新しいファイル拡張子
18. 元のファイル名を使用して脆弱な暗号化を行う	19. ファイル名を難読化する部分暗号化	20. 内部暗号化 元のファイル名	21. 元のファイル名とファイルの種類を使用した部分弱暗号化
22. 脆弱な暗号化 難読化されたファイル名	23. ワイプされた元のファイル名を維持するグループアーカイブ	24. 強力な暗号化 新しい既知の拡張機能 - 重複ファイルをワイプ	25. ゼロフィル 新しい既知の拡張
26. オリジナルファイル名をゼロ塗りつぶす	27. 難読化されたファイル名を含むゼロ塗りつぶし	99. 未知	

© Copyright 2022 Dell Inc.

構成イメージ（弊社推奨構成）



© Copyright 2022 Dell Inc.

THANKS FOR YOUR GREAT PARTNERSHIP

intel

NVIDIA

vmware

BROCADE
A Broadcom Company

Microsoft


DELL Technologies
PARTNER PROGRAM