Dell PowerProtect Backup Serviceでランサムウェアリカバリーを迅速化

1日がかりではなく、数時間でランサムウェアから復旧

主な機能

ランサムウェア攻撃はさらに高頻度 高レベル 高コストに

- 感染していないバックアップまたはファイルの迅速な特定とリストアができない
- リカバリー データからの汚染の拡散と再感染
- データ ロス、完全なデータ セットをリカバリーできない
- インシデント対応オーケストレーションの調整が困難
- RPO/RTO時間の短縮に対する要求
- 収益の喪失やブランド評価の低下を招く、コストのかかるビジネス ダウンタイム
- 不十分なデータ保護による法規制上の罰金

課題

ランサムウェアはあらゆる企業にとって深刻な脅威です。サイバー攻撃は頻繁に発生しており、壊滅的な損害を引き起こす可能性があります。79%のセキュリティ実務担当者が、今後12か月以内に破壊的な出来事が発生することを懸念しています1。災害後、データを失った企業は、破産申請のリスクにさらされます。ランサムウェア攻撃は発生頻度が高いだけでなく、技術的にも高度化し、その対策コストも増加しています。

解決策

迅速で確実なリカバリーを行うことができれば、身代金の支払いを考える必要もなくなります。しかし、セキュリティ インシデントやサイバー攻撃が発生した場合、組織はリカバリーに先立ち、被害範囲と根本原因を把握しなければなりません。ワークロードと仮想マシンの24時間365日利用可能なエアギャップされた汚染されていないスナップショット、ユーザーとデータの異常に対する継続的な監視、セキュリティ ツールとの統合、クリーン データの自動リカバリーによってセキュリティ体制を改善し、壊滅的な試練を存続可能なインシデントに変えることができます。

機能

すべてのワークロードに提供：

• エアギャップされた不変のバックアップを24時間365日利用可能

• 数日または数週間ではなく、数時間のRPO/RTOで、オンプレミスまたはクラウド内のクリーンデータをリカバリー

• Managed Data Detection and Response (MDDR)サービスで、バックアップ環境を24時間365日リアルタイムで監視

• 本番組織のデータを使用して任意のAWSリージョンやアカウント間でワークロードやVMをリストアし、そのコピーを数多く作成して複数の場所に保存すると、組織を大きなリスクにさらすことになります。

主要ワークロードでのランサムウェア リカバリー迅速化：

• MLベースのアルゴリズムを使用して異常を監視し、プロアクティブに検出

• SIEMとSOARの統合により、対応とリカバリーのアクティビティーをオーケストレーション

• リカバリー前にスナップショットのマルウェアをスキャンし、感染したスナップショットとファイルをバックアップから削除

• 指定期間内のすべてのファイルの最新のクリーン バージョンをゴールデン スナップショットから自動的にリカバリー

保護

ランサムウェアによる被害を防ぐには、まずエアギャップされた不変のデータ コピーを確保する必要があります。Dell PowerProtect Backup Serviceは、レジリエンスに優れたクラウド インフラストラクチャ上に構築されており、ランサムウェアはバックアップ データを暗号化できません。多要素認証、エンベロープ暗号化、個別のアカウント アクセスなどのゼロトラスト アーキテクチャにより、ランサムウェアは侵害したプライマリー環境の認証情報を使用してバックアップ環境やデータを改ざんできません。最後に、過剰な削除防止とソフト削除（ごみ箱）の機能により、削除からバックアップを保護するためのセキュリティ レイヤーが追加されます。

検知

ランサムウェア攻撃をできるだけ早く検出すれば、インシデント対応チームを助け、汚染の拡大を防ぐことができます。Dell PowerProtect Backup Serviceのランサムウェア リカバリー迅速化モジュールは、バックアップ環境の状態を監視するためのセキュリティ コマンド センターを提供します。アクセス インサイトと異常検出により、環境とデータ全体の異常なアクティビティーを迅速に特定できます。ユーザーとAPIによるすべてのアクセス試行について、場所、ID、アクティビティー情報を確認できます。独自のMLアルゴリズムで異常を検出し、異常なデータ アクティビティー（削除、暗号化など）に関するアラートを発行します。このアルゴリズムは、お客様固有のバックアップ環境のパターンを学習するため、ルールの設定やチューニングは必要ありません。また、エントロピーに基づくインサイトを使用して、誤検出も減らします。

回答

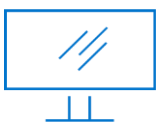
セキュリティ アナリストやITアナリストが不審なイベントを検出した場合、あるいはさらに深刻なランサムウェア インシデントが発生したことを確認した場合、対応のスピードが重要になります。検出と対応のオーケストレーションに使用できる有用なプライマリー環境セキュリティ ツールは数多くありますが、セカンダリー データ（バックアップ システム）からの分析と変更ログ データは、調査、対応、フォレンジック アクティビティーを強化します。Dell PowerProtect Backup Serviceのランサムウェア リカバリー迅速化モジュールは、すぐに利用できる堅牢なAPI統合機能を備えているため、セキュリティ エコシステム全体にソリューションを簡単に組み込むことができます。SIEMとSOARソリューションを使用して対応アクティビティーをオーケストレーションすると、感染したシステムやスナップショットの隔離、事前に定義されたランサムウェア プレイブックに基づくIOCのバックアップのスキャンといったアクションが自動的に実行され、平均対応時間(MTTR)を大幅に短縮できます。

リカバリー

初期対応の後には、大変なリカバリー作業が待っています。多くの企業にとって、これは手間や時間のかかる作業です。悪意のある攻撃者やランサムウェアの滞留時間は数週間から数か月に及ぶため、クリーン データを見つけるためにどこまで遡るべきかを把握するのは困難です。 最適なスナップショットが特定された後でも、隠れたマルウェアが再感染を引き起こす可能性があります。とはいえ、2週間前のリカバリー ポイントは、ほとんどのビジネス ユーザーにとって受け入れられるものではありません。しかし、ランサムウェア インシデント後に最新のデータを見つけて検証するのは、人手による面倒な作業であり、多くの場合、やり遂げることができません。

Dell PowerProtect Backup Serviceは、効果的なバックアップ アーキテクチャと自動化されたツールで、この負担を軽減し、リカバリーを迅速化します。Dell PowerProtect Backup Serviceクラウド プラットフォームでは、ワークロードをクラウドに直接バックアップするため、ランサムウェア攻撃が発生した場合にもすぐにリカバリーを行えます。

ランサムウェア リカバリー迅速化モジュールを使用すると、リカバリー データの衛生状態を確保し、自信を持ってリカバリーを行うことができます。組み込みのウイルス検出機能を使用するか、独自のフォレンジック調査や脅威情報フィードからの脅威インテリジェンスを使用して、スナップショットのマルウェアとIOCをスキャンできます。リカバリー前にスナップショットをスキャンすることで、再感染を阻止できます。



もっと詳しく知る
PowerProtect Backup Serviceについて

お問い合わせ：デル・テクノロジーズ エキスパート