ソリューション概要

InfiniGuard® Infinisafe®で ランサムウェアをその場で阻止

課題

ランサムウェアはデータを暗号化して人質にとり、身代金を要求する不正ソフトウェアです。

従来は、運用システムがランサムウェアによる攻撃を受けても、バックアッププロセスが機能していれば感染前のデータをリストアできました。しかし、ランサムウェアのコードは着実に進化を遂げており、現在はバックアップデータ自体を攻撃することが一般的になっています。企業に対するランサムウェア攻撃が平均して11秒に1件発生している[1]状況では、以前のように「攻撃されても、バックアップをリストアすればよい」と悠長に構えていることはできません。

ランサムウェアに侵害された場合、何らかの損失は免れません。身代金を支払って、運良く暗号化キーを入手できる場合もありますが、身代金だけ取られて何も戻ってこないことも少なくありません。高額な暗号化データ復旧サービスの利用が必要になる場合もあれば、オフラインで保管していたテープカートリッジを物理的に輸送し、手間のかかるリカバリを行わなければならない場合もあります。

IDCによると、ランサムウェアの被害額は、大規模企業だけでも年間200億ドルに上ると推定されています。中小規模の会社も含めると、その額はさらに増加します。

ランサムウェアの現状

サイバーセキュリティプロバイダーのBlackFog[2]は、2021年の前半に起こった大規模なサイバー攻撃について報告しています。米国ニューヨーク州のビクターセントラル学区に対する攻撃では、データとシステムが暗号化され、ユーザーがアクセスできなくなりました。その結果、学区内のすべての学校が休校を余儀なくされました。3月にはコンピューターメーカーのAcerが、抜き出された機密データの公開を免れるために、5,000万ドルの身代金を支払うことになりました。

さらに最近では、米国東海岸の燃料供給の45%を担うColonial Pipelineへのランサムウェア攻撃が大きな話題になりました。この攻撃はロシアのハッカー集団によるものでした。Colonial Pipelineは攻撃の拡大を封じるため、速やかにシステムをシャットダウンしましたが、米国の広い地域で、ガソリンスタンドへのガソリン供給に支障が出ました。

中小企業も例外ではありません。セキュリティ企業のInfrascaleによると、中小企業の46%がランサムウェア攻撃を経験していると推定され、そのうちの73%が実際に身代金を支払っています[3]。これらの企業が支払った身代金は、5,000万ドルには及ばずともその損失は大きく、攻撃者が約束を守るという保証もありません。

バックアップがあっても万全とは限らない

バックアップデータが無事であれば、有利であることは間違いありません。しかし、攻撃者も経験を重ねて巧妙化し、最近ではまずバックアップシステムを標的にする攻撃が増えています。バックアップデータをリストアできなければ、攻撃者はより優位に立つことになります。従来のバックアップや

[1] Cybersecurity Ventures https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021
[2] BlackFog https://www.blackfog.com/the-state-of-ransomware-in-2021
[3] Infrascaleによる2020年の調査 https://www.infrascale.com/press-release/infrascale-survey-reveals-close-to-half-of-smbs-have-been-ransomware-attack-targets/

InfiniGuard InfiniSafeの主な機能：

- ペタバイト規模での高速リストアでエンタープライズのニーズに対応
- 削除、暗号化、変更ができない改竄防止機能を備えたスナップショットで、サイバー攻撃からバックアップを保護
- 統合バックアップと改竄防止機能を備えたスナップショットで、規制要件に確実に準拠
- パフォーマンスに影響することなく複数のバックアップとリカバリ操作の同時実行をサポート
- リカバリ環境を検証
- アクティブ/アクティブ/パッシブ構成における冗長化された重複排除エンジンによりデータを保護しバックアップとリカバリ操作をフェイルオーバー
- 最大50ペタバイト*のアプライアンス1台にバックアップを統合することで、電力コストと管理経費を削減
- 拡張性がきわめて高く、複数のプロトコルVTL、NFS、CIFS、OST、RMAN、DB/2）をサポート
- 瞬時にかつ安全にデータをリストアすることで、収益の損失や評判へのダメージを最小限に抑制
- サイバー攻撃、技術的な誤動作、自然災害、人為的なエラーなどの原因にかかわらず、データの完全性を損なうことなくデータを回復

INFINIDAT

ディザスタリカバリの手法がサイバーリカバリとして機能しなくなっている現状では、サイバーリカバリのニーズを考慮してサイバーセキュリティ計画を立てる必要があります。

ITチームは従来、合成フルバックアップと重複排除機能のあるバックアップストレージを採用して、バックアップスピードを高めていました。サイバー攻撃に伴う大規模なリカバリでは、何世代ものバックアップからデータを統合することになるため、バックエンドのストレージで非常にランダムな読み取りIOパターンが発生します。したがって、リカバリに時間がかかり、ビジネスに重大な影響が出る可能性があります。

ソリューション：InfiniSafe搭載のInfiniGuard

Infinidatのデータ保護/リカバリソリューションであるInfiniGuardには、InfiniSafeが搭載されています。InfiniGuardのデータ保護アーキテクチャにInfiniSafeを組み合わせることで、他の競合バックアップアプライアンス（PBBA）よりも格段に低いコストでの高速リカバリを実現しています。InfiniGuardはマルチペタバイトクラスのInfiniBox®をバックエンドに採用し、革新的なソフトウェアレイヤーを追加しています。これにより、バックアップ速度を犠牲にせずに高速リカバリを実現できるようデータレイアウトを最適化しています。

InfiniGuardの革新的なテクノロジーは、厚いDRAM（Dynamic Random-Access Memory）の層をプライマリキャッシュとして利用し、より厚いSSD（ソリッドステートドライブ）の層をセカンダリキャッシュとして利用します。独自のTRIEアルゴリズム（バイナリツリーやハッシュアルゴリズムではなく、ノードツリー）によってIOパターンを予測し、データを事前にキャッシュすることで、バックアップとリカバリを高速化します。

InfiniGuardは、複数のバックアップアプライアンス、各種記憶媒体、ストレージサイトからデータをリカバリするのではなく、最大で物理容量2ペタバイト、実効容量50ペタバイト*に拡張できる管理が容易なアプライアンス1台に複数のバックアップを統合します。

InfiniSafeの詳細

InfiniGuardのネイティブ機能であるInfiniSafeの各種機能は、保護能力とリカバリ能力を高めます。InfiniSafeはランサムウェア攻撃に対する防御策の基盤として、サイバーリカバリソリューションの核となる以下の4つのテクノロジーを備えています。

1. 改竄防止機能を備えたスナップショット

改竄防止機能を備えたスナップショットは削除も変更もできません。Infinidatのエキスパートがお客様と協業して、リテンション設定、スケジュール設定、関連するポリシーの作成など、お客様のサイバーセキュリティのニーズに合わせてスナップショットの構成を行います。攻撃者による悪意あるアクションや経験の浅いITスタッフのミスによって、改竄防止機能を備えたスナップショットの設定が変更または削除されることはありません。

2. 論理エアギャップによる保護

保護対象のデータをシステムの他の領域から確実に分離しておくことは非常に重要です。一部のソリューションでは、コピーやレプリケーションによっ

InfiniSafe搭載のInfiniGuardなら、Infinidatの改竄防止機能を備えたスナップショットにより、バックアップストレージ全体を保護できます。各重複排除エンジン（DDE）は個別に、任意の時点の状態にリストアできます。InfiniSafeまたは検知テストも、スタンバイ環境で有効化できます。

INFINIDAT

て保護対象のデータを別個のシステムに移動するためコストと複雑性が増大します。InfiniSafeテクノロジーではこのプロセスをローカルシステムで実行することで、コスト増と複雑化を抑制できます。

3. 隔離されたフォレンジックネットワーク

データの検証とリカバリに使用される、完全にプライベートのネットワークです。

4. ほぼリアルタイムのリカバリ

攻撃を受けた際のリカバリでは、データの可用性を可能な限り迅速に 回復することが重要です。InfiniSafeを利用すると、問題がないことがわかっている検証済みのデータを、バックアップリポジトリのサイズにかかわらず、数分のうちに利用可能な状態にリストアできます。ペタバイト規模のリポジトリであっても、リストアの所要時間に影響は生じません。

リカバリでは、体系的かつ高速な処理を実行できること、検証が可能なこと、過去の任意の時点の状態までほぼリアルタイムで復旧できることが求められます。
隔離された使いやすいテスト環境が備わっていることで、実際の業務環境にデータをリストアする前にデータを当該のデータを検証できます。またこのテスト環境を利用して、セカンダリシステムの利用やデータの移動を必要とせず、日々のバックアップ作業に影響を与えずに、バックアップが安全に行われていることを定期的に確認することもできます。

まとめ

サイバー攻撃の脅威は企業にとって、ますます深刻さの度合を強めている現実的なリスクであり、そこからもたらされ得る損害を甘く見ることはできません。最近のサイバー攻撃では、バックアップ環境をまず標的にすることで防御策の有効性を低下させ、攻撃側の優位性を確保するという傾向が明らかになっています。こうした攻撃者の戦略に先んじるために、サイバー攻撃、技術的な故障、自然災害、人為的なエラーといったさまざまな脅威から組織を保護する、InfiniSafeを搭載したInfiniGuardの導入をご検討ください。InfiniSafeを搭載したInfiniGuardを活用することで、安心して速やかにデータを回復し、通常の業務運営へと復帰できる体制を確立できます。

* 実効容量。実際の数値は環境によって異なります。

jp_sales@INFINIDAT.com | 03-4243-6343