COHESITY

ヒントシート

# 保護、検知、復旧でサイバーレジリエンスを高める5つの方法

## 概要

データは攻撃されています。その証拠に、ランサムウェアの脅威が前年比1,070%増となっています[1]。そして、今日の悪質な攻撃者は、単にデータを暗号化するだけではありません。バックアップを破壊し、データを流出させることで利益を得ると同時に、会社の評判も落とします。そのため、ランサムウェアの影響範囲はますます大きくなっています。ランサムウェアの攻撃者に負けてはいけません。保護、検知、復旧で環境を強化し、対応策を改善することができます。

収益や生産性の損失を含む世界のランサムウェアの被害額は、2031年までに2,650億ドルを超えると予測されています。[2]

### 1. バックアップデータとシステムの保護

従来のバックアップソリューションは、ランサムウェアからデータを守るように設計されていません。そのため、企業はいまだに身代金を支払っています。必要なのは、バックアップに組み込まれたデータ保護機能で、顧客の信頼と競争力を維持するために役立ちます。イミュータブル (変更不可の) バックアップスナップショットをネイティブで備えているソリューションを探してください。このようなバックアップスナップショットは、暗号化や、変更、削除ができないため、データの信頼性を守ることができます。また、ソフトウェアベースのWORM (Write Once, Read Many) 機能、FIPS認証の暗号化を備えたバックアップであれば、保護レイヤーを追加することができます。そして、オンサイトおよびパブリッククラウドにおける最新の柔軟なデータ隔離機能は、リカバリ目標と組織のSLAを満たすことを可能にします。最後に、故障したコンポーネントがあっても運用が継続でき、監査やスキャンなどの自動セキュリティ制御を設定して人為エラーを排除できるフォールトトレラントソリューションであることも必要です。

### 2. 不正アクセスリスクの低減

漏洩したユーザーの認証情報は、大金を得ようとする犯罪者の最大の攻撃経路となっています。厳しいアクセス制御機能を備えたデータ管理プラットフォームは、漏洩した認証情報を不正アクセス者が利用することを効果的に阻止することができます。ハッカーや内部脅威に対しては、ゼロトラストの原則で対抗することを検討してください。これには、ロールベースのアクセス制御、多要素認証、一方的な管理者変更を防止するためのQuorum認証、環境の自動セキュリティスコアリングによる監視が含まれます。

## 3. 侵入を阻止し、攻撃を検知

Cybersecurity Venturesの専門家によると、ランサムウェアは現在11秒に1回、企業を攻撃しています。[1] どの組織も、対応できる従業員が十分いないため、新たな攻撃や異常な活動を検知して機密データに光を当てるには、AIと機械学習ベースの検知機能が必要です。機密データを自動で発見/分類し、ほぼリアルタイムで脅威を検知できるインテリジェンスが組み込まれたソリューションを探す必要があります。そのソリューションが持つ基本情報を使用することで、チームは予測分析ベースのアラートを受信し、進行中の暗号化のスタイルやデータ流出攻撃の一部として異常を早期に可視化することができます。

## 4. 既存のセキュリティシステムとのシームレスな統合

ランサムウェアの脅威はなくなることはなく、進化を続けています。そのため、インフラストラクチャーとオペレーション (I & O)、セキュリティオペレーション (SecOps)、ガバナンス/コンプライアンスといった社内のチームが連携して侵害を防止し、迅速に対応することが求められています。データ管理ソリューションは、データのサイロや機能的な障壁を取り除くのに役立ちます。また、脅威の検知、調査、迅速な対応が行える、統合された拡張性の高いソリューションが必要です。そして採用するソリューションは、業界をリードするセキュリティツールを利用でき、脅威と戦いながらも価値を付加し続けられるよう、開発者に豊富なRESTful API を提供できるものである必要があります。

## 5. 大規模データの迅速な復旧

サイバー窃取者は巧妙さに長けているので、最悪のシナリオもあり得ます。だからこそ、身代金の支払いを拒否し、かつ迅速に復旧できるデータ管理ソリューションが必要です。必要なのは、何百台もの仮想マシン、大規模データベース、大容量の非構造化データを、時間や場所を問わず、即時かつ大規模にリストアできるソリューションです。また、利用環境をマルウェアに再感染させないために、スナップショットの健全性を評価する機能を提供し、同じプラットフォーム上で直接、クリーンで予測可能なデータ復旧を実行できるソリューションを見つけることが大切です。これにより、リソースと時間を節約することが可能になります。

## Cohesityでサイバーレジリエンスを強化

ランサムウェアに対抗するソリューションを見つけることは、ビジネス上不可欠なものとなっています。 Cohesityのモダンデータ管理ソリューションは、企業が競争力を維持し、身代金の支払いを自信を持って拒否するために必要なデータセキュリティ、ランサムウェアからの復旧、サイバーレジリエンス機能を提供します。

1. FortiGuard Labs 2021 mid-year Global Threat Landscape Report
2. Cybersecurity Ventures

次世代データ管理の詳細はこちら: Cohesity.com/jp

COHESITY