ランサムウェア攻撃からの回復力を確保するための 4 つの方法

ベリタスで常にランサムウェアによる脅威の 1 歩先を行く。

ランサムウェア攻撃とマルウェア攻撃が増加し、すべての企業と業種にとって差し迫った脅威となっています。ランサムウェア攻撃はこの 1 年で 185% 増加し[1]、多くのレポートで今年はそのコストが 200 億ドルを超えると予想されています。[2] 攻撃者は新しい巧妙な手段を取り入れて企業のインフラに侵入し、その機能を停止させようとしています。いつ攻撃されてもおかしくない状況の中、最良の防御は攻撃に備えることです。

ベリタスでは、包括的な多層型の回復力フレームワークにおける信頼性の高い要素として、バックアップとリカバリを優先的に対応することをお勧めします。具体的には、企業の全体的なサイバーセキュリティ戦略の保護、検出、および回復の各コンポーネントをサポートします。ベリタスのソリューションは、お客様がすべての重要かつ貴重なデータを強化し、ランサムウェアによる潜在的な脅威を検出し、リカバリのオーケストレーションと自動化を行い、迅速に稼働できるよう支援します。ランサムウェア攻撃からの回復力に関する戦略にベリタスを導入すべき理由をいくつか紹介します。

ベリタスがランサムウェア攻撃からの回復力を確保できる主な 4 つの理由

1. データをリスクにさらさない。ベリタスを導入すると、コスト効率の高い優れた改ざん防止機能によってすべての貴重な情報を保護できます。

ベリタスは、改ざん防止に対して「1 つの製品ですべてに対応する」というアプローチを採用していません。改ざん防止機能を備えたサードパーティハードウェアとの接続を必要とする場合でも、ベリタスのネーティブの改ざん不可能なストレージを使用する場合でも対応できるよう、さまざまなオプションと柔軟性を提供します。また、AWS S3 オブジェクトロックをサポートしており、改ざん防止機能を拡張することもできます。

2. 攻撃発生時に貴重な時間を無駄にしない。ベリタスなら、リカバリのオーケストレーションによって、どのレベルでも制限なく、ワンクリックで迅速にリカバリできます。

ボタンを 1 つクリックするだけで、クロスサイトまたはクラウドのリストア全体の自動化とオーケストレーションを効率的かつ大規模に実現できます。さらに、データにアクセスできるだけでなく、すべての必要な依存関係とともにアプリケーションをオンラインの状態に戻せます。また、重複排除済みのデータを AWS S3 オブジェクトロックに送信して保存でき、この効率的に保存された重複排除済みのデータからデータセンター全体を必要に応じて起動できるベンダーはベリタスだけです。ベリタスを使用すれば、テクノロジのコアに組み込まれた信頼性と実績の高い回復力ソリューションにより、完全なリカバリの自動化とオーケストレーションをすべてのレベル (データからアプリケーション、データセンター全体) で制限なしで実現できます。

3. 可視化により推測する必要がない。継続的な監視とインフラの把握によるベリタスの最先端の異常検出により、すべてのストレージ、バックアップ、およびクラウドベンダーを 1 カ所で包括的に把握できます。

本番環境とバックアップベンダー (競合ソリューションを含む) についてのレポートを作成し、これらすべてのデータポイントを相互参照してシステムが 1 つも見過ごされないようにすることができるベンダーはベリタスだけです。ベリタスでは、この優れた可視性をパノラマビューと呼び、環境全体を完全に保護するために不可欠な要素だと考えています。企業はベリタスのソリューションを導入することで、プライマリデータだけでなく、データ保護 (バックアップ) 環境、インフラ全体、個々のファイルの異常を総合的に明らかにすることができます。広範なデータソースにわたってこうした脆弱性を

監視およびレポートする機能は、脅威ベクトルを効果的に管理するにあたって極めて重要です。また、仮想マシンの自動検出および保護、追加のバックアップ監視、リカバリへの対応準備はすべて、回復するための準備が整っているという高い安心感をもたらします。

4. データを脆弱なままにしない。ベリタスのデータ暗号化機能により、高い安心感を得られます。身代金を支払う必要はありません。

ベリタスの製品は、ネットワークセキュリティ認定や業界認定を競合他社よりも多く取得しており、送信中と保存中のデータを暗号化することで、場所に関係なくデータを保護し、その整合性を維持するよう設計されています。ベリタス製品を導入すれば、バックアップ環境へのランサムウェア攻撃によってデータを盗み出すという副次的な目的の実行を防ぎ、身代金を支払うこともなければ企業の評判を損なうこともありません。

プロアクティブな統合アプローチを取るべきとき

ベリタスのランサムウェア攻撃からの回復力ソリューションは業界トップクラスの包括性、安全性を備え、コンプライアンスにも対応しており、避けられない攻撃に対する安心と自信をお客様にもたらします。米国標準技術局 (NIST) フレームワークに準拠するベリタス製品なら、エッジからコア、クラウドまで、どこに保存されているデータでも保護、検出、回復できます。

保護

システム強化と改ざんおよび消去不可能なイメージ管理およびストレージ、データ暗号化 (送信中と保存中の両方)、ID およびアクセス管理 (IAM)、ロールベースのアクセス制御 (RBAC) と多要素認証 (MFA) を備えた IAM によってデータの整合性を確保。

回復

大規模で非常に要求の厳しいマルチクラウド環境やデータセンター環境で、システム間のリストア全体の自動化とオーケストレーションを実現。柔軟なリカバリ方法、回復力オーケストレーションツール、数秒で一括リカバリできる VMWare 向けのインスタントロールバックを提供。

検出

機械学習に基づく AI および予測分析を利用して自社環境を包括的に把握し、インサイトの獲得、バックアップ検出機能、データ内の異常検出を促進。システムアクティビティに関する継続的な監視とレポート機能を備えた包括的な統合ビューで脅威と脆弱性を軽減。

リスクを軽減し、不確実性を解消して、制御を維持するための詳細については、https://www.veritas.com/ja/jp/ransomware をご覧ください。

1. https://www.sonicwall.com/news/sonicwall-record-304-7-million-ransomware-attacks-eclipse-2020-global-total-in-just-6-months/
2. https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-250-billion-usd-by-2031/

ベリタスについて

Veritas Technologies はデータの可用性および保護のグローバルリーダーです。複雑化したIT環境においてデータ管理の簡素化を実現するために、Fortune Global 500 の 87% を含む、先進企業 50,000 社以上が、ベリタスのソリューションを導入しています。ベリタスのエンタープライズ・データサービス・プラットフォームは、お客様のデータ活用を推進するため、データ保護とデータリカバリのオーケストレーションを実現して、ビジネスに不可欠なアプリケーションの可用性を常に確保し、複雑化するデータ規制対応に必要なインサイトを提供します。ベリタスのソリューションは信頼性とスケーラビリティに優れ、500 以上のデータソースと 60 のクラウドを含む 150 以上のストレージ環境に対応しています。ベリタステクノロジーズ合同会社は、Veritas Technologies の日本法人です。

VERITAS

〒107-0052 東京都港区
赤坂 1-11-44
赤坂インターシティ 4 階
www.veritas.com/ja/jp

世界各地の連絡先については、以下をご覧ください。
veritas.com/ja/jp/company/contact

V1384 08/21