サイバー脅威に対する耐障害性を実現する 6 つのステップ

ベリタスで常にサイバーセキュリティに対する脅威の 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。2021 年、ランサムウェア攻撃は 1 秒あたり 19 件発生しており[1]、多数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に対する耐障害性対策にベリタスを導入すべき理由をいくつか紹介します。

ベリタスがサイバー脅威への耐障害性を実現する 6 つの理由

1. 可視化により推測する必要がない。

最先端の技術を活用した継続的な監視とインフラの把握により、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。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、データ回復の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。

2. 企業の脆弱性を放置しない。

ベリタスはネットワークセキュリティ、個人情報およびアクセス管理 (IAM)、データ暗号化により攻撃対象を減らし、大規模な障害を防ぎます。

大規模な信頼性と回復力においては競合他社に比べて多数の実績を誇り、MFA (多要素認証)、ロールベースのアクセス制御、統合型の保護と検知、安全性に優れたコンプライアンスクロック (特許出願中)、リモートアクセスの制限など、標準および先進的な機能による多層的なセキュリティを通じ、あらゆる場所のデータのセキュリティを確保する製品を設計および提供しています。さらに、第三者への依存を最低限にとどめているため、攻撃対象を常に管理下におくことができます。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。

3. 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第三者の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、オブジェクトロックテクノロジー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。

4 ハッカーは常にシステムに潜んでいると考える。

AI を活用した異常検出とマルウェアスキャンにより、環境全体のなかで何らかの異常が発生した場合にアラートを通知し、ユーザーに大きなメリットをもたらします。

第三者のバックアップ製品を含め、あらゆるシステムを継続的にスキャン、監視し、環境内で疑わしい異常を確認した場合にほぼリアルタイムでアラートを発出できるのはベリタスだけです。また、自動化されたオンデマンドのマルウェアスキャン機能により、人工知能や機械学習を活用したマルウェアスキャンを実現します。

5. 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オブジェクトロックテクノロジー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。

6. サイバー攻撃が起きてから復旧を調整していては手遅れである。

ビジネスのすべての階層で DR テストのリハーサルを実施

自動化され、品質が保証されている無停止の DR テストのリハーサルをビジネスのすべての階層で実行しながら、ネットワークフェンシングやサンドボックス環境など本番環境以外のリソースを簡単かつ効率的に活用できるベンダーはベリタスだけです。

今こそベリタスを活用し、プロアクティブで多層的なサイバー耐障害性強化アプローチを実現

ベリタスはデータのプロアクティブな保護、AI を活用した脅威の検出、業界トップクラスの迅速な復旧をこれまでにない規模に実現し、サイバー耐障害性を強化します。リスクの軽減、不確実性の解消、制御の維持を実現するのです。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/resources/white-papers/2022-sonicwall-cyber-threat-report/
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

各国オフィスとお問い合わせ先については、弊社の Web サイトを参照してください。
veritas.com/ja/jp/company/contact

V1550 04/22