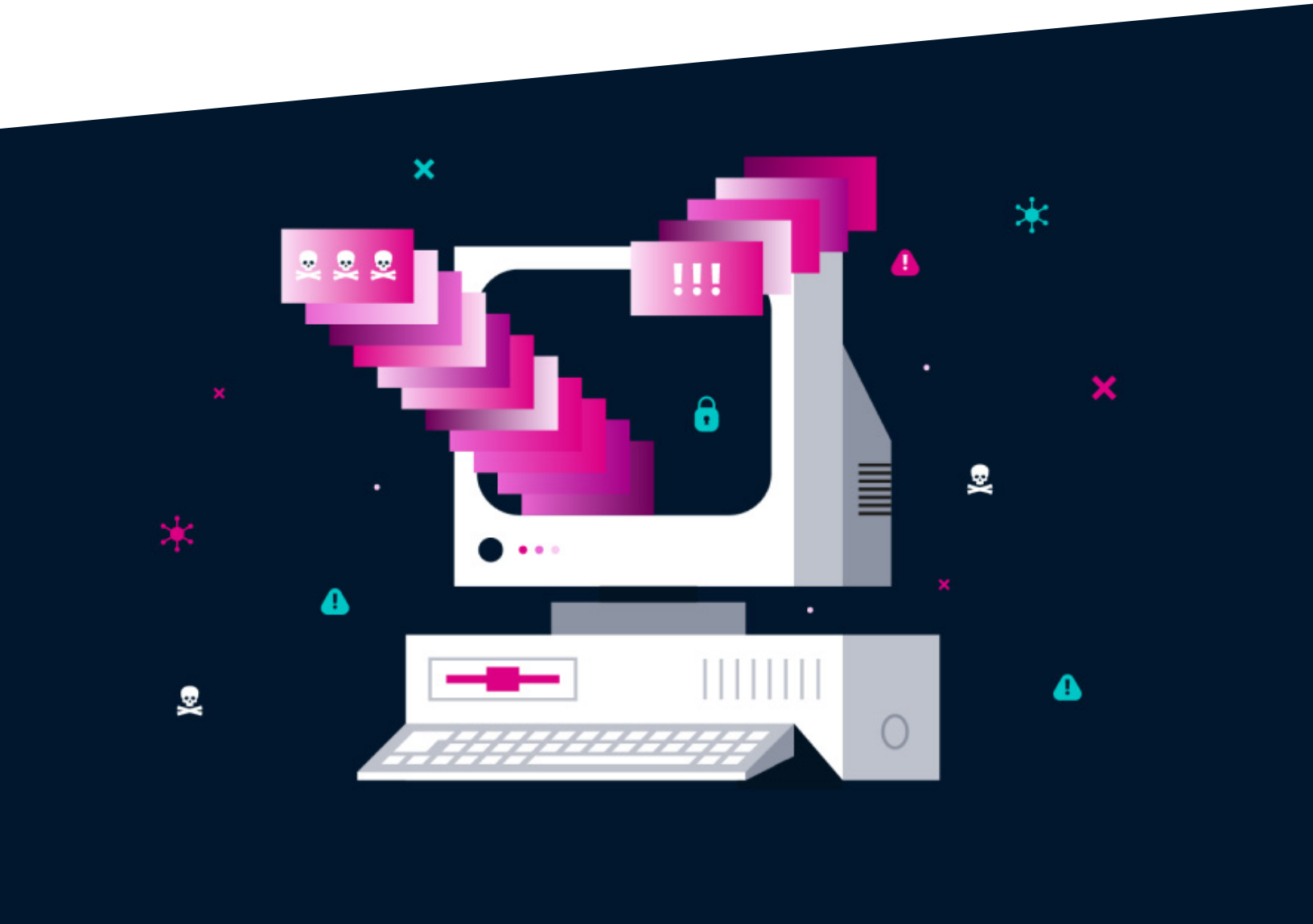
rubrik

Eブック

レガシーバックアップベンダーが教えてくれない5つのこと

レガシーバックアップではサイバー攻撃から守れない理由ー代わりに何をすべきか。



目次

サイバー攻撃は増加しています

サイバー攻撃は今や、インフラが標的にされるかどうかではなく、**いつ**標的にされるかが問題になるほど広まっています。

そして、サイバー攻撃が成功してしまうと、ビジネスに甚大な被害をもたらす可能性があります。

- **ビジネスへの影響：**サイバー攻撃を受けた組織の93%は、その結果として、ビジネスに対する一定のマイナスの影響（業務の中断から評判の損害まで）を被っています。
- **収益の損失：**サイバー攻撃は、業務の中断、身代金の要求、財務上の機密情報の窃取などにより、財務上の損失につながる可能性があります。
- **ITおよびセキュリティチームへの影響：**サイバー攻撃は、リーダーシップの交代、信頼の喪失、不安の増大など、組織とそのITおよびセキュリティのチームに広範な影響をもたらす可能性があります。
- **罰金およびその他の罰則：**サイバー攻撃が成功してしまうと、機密データの漏洩につながる可能性があります。その結果、法的罰則、規制当局による罰金、評判の損害が発生してしまうかもしれません。

サイバー攻撃が発生する確率は非常に高く、ビジネスに深刻な影響を与える可能性があります。そのため、被害を最小限に抑え、迅速な復旧を支援するための戦略的な計画が必要です。

あなたのデータはサイバー攻撃に耐えられますか?

ほとんどの組織にとって、従来のバックアップは最後の砦です。それは落雷、地震、高波といった自然災害の後に環境をゼロから再構築するのには適していますが、サイバー攻撃から復旧するには十分ではありません。

しかし、レガシーバックアップベンダーはそのことを教えてはくれません。

レガシーバックアップソリューションでデータを守るのは、ハタキで有毒廃棄物を取り除こうとするようなものです。最近のサイバー犯罪は高度に組織化されていて、手口も非常に巧妙です。そのため、サイバー復旧用に考案されたデータセキュリティソリューション以外は頼りになりません。

サイバー攻撃からのデータ保護に関して、レガシーバックアップベンダーが教えてくれない5つのことを見てみましょう。

用語集

サイバーリカバリ：サイバー攻撃から数時間または数日以内に（数週間や数か月ではなく）通常通りのビジネスに迅速に復帰する能力です。

サイバーポスチャー：機密データを可視化し、アクセス活動を分析し、最小特権コントロールをプロアクティブに有効化することによって、サイバーリスクを低減するための取り組みです。

サイバーレジリエンス：サイバー攻撃に耐え、そこから迅速に復旧する能力です。完全なサイバーレジリエンスには、サイバーポスチャーとサイバーリカバリの両方が必要です。

1 標的はバックアップです

多くの組織が、レガシーバックアップソリューションをサイバーセキュリティの頼みの綱としています。しかし、これらのバックアップは安全な避難先とは程遠いものです。最近のサイバー犯罪者は、特にレガシーバックアップを標的としており、攻撃に対する安全装置としてのそれらを無効化しています。

考えたくもない真実がここにあります：**「悪意のある侵入者がサイバー攻撃の際にデータのバックアップを改ざんしようとした、と90%の外部組織が報告しています。」**

レガシーバックアップはなぜこれほどまでに標的にされやすいのでしょうか。

- **時代遅れのセキュリティ：**レガシーバックアップソリューションは、さまざまなサイロ化されたソースからデータを収集および管理するために必要な連携ツール（クラウドインスタンスを含む）を備えていない可能性があります。また、データの健全性とパフォーマンスを監視し、データ異常の根本原因を明らかにする監査証跡を作成するデータ観測機能を欠いている可能性があります。

  実際、レガシーバックアップが構築されているプラットフォームは、多要素認証、ロールベースのアクセス制御などの基本的なセキュリティ機能を欠いている可能性があります。

- **オープンテクノロジー：**レガシーバックアップシステムは、ハッカーがデータに不正アクセスしたり、操作したりできる状態になっている恐れのあるオープンストレージプロトコルを使用している可能性があります。これは、多要素認証がないなど、他のセキュリティ上の弱点と組み合わさった場合に、特に問題となります。

- **洞察力の欠如：**レガシーバックアップシステムは、危険にさらされているデータに対する分析やリアルタイムの視認性を欠いていることが多く、侵害の範囲や詳細が不明瞭です。

今日、多くのベンダーが「最新」のバックアップソリューションを提供していると主張していますが、それらは多くの場合、安全でない従来のアーキテクチャに依存しています。バックアップを標的とすることで、攻撃者はこれらのシステムの脆弱性を悪用して機密データに不正アクセスし、組織の存続を脅かす恐れがあります。

急速に進化する今日の脅威の状況を鑑みると、レガシーバックアップを防御として頼ることは、明らかに勝ち目のない戦略です。**実際、それは重大な結果をもたらす恐れがあります。**

>>> PRO TIP

重要なビジネスデータを保護する唯一の方法は、データを頑丈にし、脅威を特定でき、迅速な復旧を促進するサイバーレジリエンスソリューションです。

2 バックアップにはセキュリティ上のフェールポイントが複数あります

レガシーバックアップは、利便性という名の下に、堅牢なセキュリティ機能を犠牲にすることがよくあります。また、バックアップの「災害復旧」が、サイバー攻撃ではなく自然災害後の業務復旧のみを意味していた時代に設計されたものもあります。その結果として、レガシーバックアップは、脆弱性を悪用しようとする攻撃者にとって格好の標的となってしまうのです。

言い換えると、バックアップがあるからデータは安全だと思うことで、夜もぐっすり眠れるかもしれません。しかし、そのバックアップデータ自体が、ランサムウェアやマルウェア、データ侵害に対して脆弱なのです。

多くの場合、レガシーバックアップソリューションは、メンテナンスが必要なオペレーティングシステム上で実行され、パッチ適用が必要なソフトウェアを使用し、配慮が必要なデータベースを含んでいます。これは通常、技術スタッフがバックアップのセキュリティを強化するために、特定の行動を取らなければならないことを意味します。この作業の多くは手作業で行われます。さらに、サーバーのオペレーティングシステムを保守するチームとセキュリティを担当するチームが異なることがよくあります。その結果、レガシーバックアップに定期的な更新やメンテナンスが行われない可能性があり、既知の脆弱性を悪用しようとするサイバー犯罪にさらされることになります。

Brent

“

ランサムウェアによる攻撃ー特にハックニー評議会（実質的に私たちの隣人）やレッドカー&クリーブランド評議会に対する攻撃ーによる被害が増えてきました。このことが、優先順位を上げて早急に環境を一新するきっかけとなったのです。

Kevin Ginn
ブレント評議会運営責任者

- レガシーソリューションでは心の平穏を保証できなかった
- Rubrikの新ソリューションにはランサムウェアからの復旧機能が組み込まれている
- **100%**のセキュリティとコンプライアンス
- **50%**の時間を節約

また、レガシーバックアップソリューションは自動化や直感的なユーザー制御に欠けることも多く、そのためこれらのシステムはヒューマンエラーに対する脆弱性をもつことになります。たとえば、スタッフが誤って重要なデータを削除または上書きしてしまったり、バックアップを適切に保護できず、不正アクセスにさらされたりする可能性があります。

さらに、レガシーバックアップシステムは、機密データを保護するための高度な暗号化や認証のメカニズムがないオープンストレージプロトコルを使用していることがよくあります。

実際、多要素認証のような基本的なものは、レガシーバックアップのセキュリティ慣行から完全に欠如しているかもしれません。そして、多くのレガシーバックアップシステムは暗号化されていないデータベースにデータを保存するため、攻撃が成功してしまうと、重要なシステムに対する保護されていないパスワードが公開されてしまう可能性があります。つまり、「王国の鍵」が引き渡されてしまい、悪意のある者がインフラ全体を自由に支配できるようになります。

この悪夢のようなシナリオでは、バックアップそのものが攻撃の足掛かりとして利用される可能性があります。つまり、攻撃から守るために頼っているシステムそのものが、自らに対する武器へと変わってしまうのです。

>>> PRO TIP

バックアップソリューションは、サイバーレジリエンスのために構築されなければなりません。それは、ゼロトラスト設計、エアギャップ設計、および安全なプロトコル使用を実現していなければなりません。また、ネイティブな不変性、データ暗号化、ロールベースのアクセス制御、および多要素認証のサポートが必要です。

WABASH™

“

私たちが使用していたバックアップソフトウェアソリューションは時代遅れでした。複数のパッチを適用し、ファームウェアを頻繁に更新する必要があり、日々のバックアップ作業を実践的に管理する必要がありました。

- ライセンスの廃止とストレージの統合により、**TCOを60%節約**
- パフォーマンスを損なうことなく、**RTOを45分から数秒に短縮**
- 高頻度のバックアップで**RPOを改善**し、SQLとExchangeのダウンタイムを削減

3 バックアップでは攻撃を見抜くことはできません

ほとんどのレガシーバックアップシステムは、個人を特定できる情報を含む顧客記録や取引記録内の財務データなど、ネットワーク上の機密データに対する重要な洞察や視認性を提供することができません。

また、レガシーバックアップには、攻撃中にどのデータが影響を受けたかを迅速に判断する機能もありません。つまり、進行中のインシデントに対応しながら、最も機密性の高いデータに何が起こったかを正確に把握するために貴重な時間を費やさなければならないかもしれません。その間、サイバー犯罪者はシステム内で大混乱を起こし続ける可能性があります。

ここでは、攻撃を受けている際、レガシーバックアップに不足している上位3つの領域を紹介します。

- **データの不完全な表示：**レガシーバックアップシステムでは、保存データの可視性が限られていることがよくあります。そのため、脅威が発生した時に、セキュリティチームは最も機密性の高いデータを見つけるのに労力を要するかもしれません。また、最も重要で機密性の高いデータを事前に特定しようとさえしていない場合、攻撃がビジネスに与える影響を完全に理解できない可能性があります。さらに、自動保護ポリシーのないレガシーバックアップでは、システムを完全にリストアするために必要なすべてのデータを取得できない可能性があります。攻撃者は、復旧を実行するために重要なファイルを削除することで、これを悪用することができます。
- **脅威の特定機能の欠如：**サイバー攻撃を発見するのに最適な場所はバックアップシステム内であり、ここであればセキュリティチームはプロダクションシステムに影響を与えることなく、脅威を迅速に特定することができます。効果的な脅威特定ツールがなければ攻撃元を見つけることができず、どのデータが改ざんまたは削除されたかを確認することもできません。
- **復旧に時間がかかる：**レガシーバックアップに保存するデータが多ければ多いほど、すべての企業データを完全にリストアするのに時間がかかります。攻撃の範囲を決定する（そして、どのデータが影響を受けたかを理解する）ツールがなければ、的を絞った精密な方法で重要なデータを復元することはできません。企業の完全な復旧を待っていては、影響を受けていないシステムをオンラインに迅速に戻すことができません。

自社のデータを効果的に監視できないため非常に脆弱な立場に置かれ、迅速かつ正確にリスクを評価して脅威を是正する能力が著しく損なわれます。

そして、無知のために失う一秒一秒は、攻撃者が貴重なデータを盗み、あなたのビジネスを崩壊させる可能性がある一秒一秒よりも長いのです。

>>> PRO TIP

最新のバックアップソリューションは、サイバーレジリエンスのために設計されなければなりません。セキュリティチームがバックアップインスタンスにある機密性の高い企業データへの脅威を容易に特定できるように、サイバーポスチャー機能が組み込まれていなければなりません。そうすることで、ミッションクリティカルなプロダクションシステムへの影響を最小限に抑えられます。サイバーリカバリ機能は、標的となったシステムを迅速にリストアし、サイバー攻撃による事業運営への影響を抑えることができなければなりません。

4 バックアップも感染しているかもしれません

最近のサイバー犯罪者は、レガシーバックアップを標的にすることが増えていると言ったのを覚えているでしょうか。つまり、バックアップは、データの完全なコピーとは程遠く、**「最初の標的」**になる可能性があるということです。

システムが最初に感染した場合、ITチームやセキュリティチームが侵入に気づくまでには、「滞留時間」と呼ばれる期間があります。

この間、バックアップは通常通り実行されており、マルウェアは自社の他のデータと一緒にバックアップされています。感染したバックアップからリストアすると、マルウェアをプロダクション環境にそのままコピーしてしまうことになります。

バックアップが感染していることに気づかないまま、マルウェアの痕跡をすべて取り除くために、プロダクションシステムのクリーニングに何時間も（場合によっては何日も）費やすことを想像してみてください。もし最初の感染がいつ起こったかわからなければ、感染したバックアップでリストアし、また同じことを繰り返す危険性があります。その結果、さらに過去に遡ることを余儀なくされ、感染していないバックアップを見つけようとして失敗するたびに、貴重な時間を浪費することになるのです。

攻撃者はまた、発見されるまでの滞留時間を利用してバックアップ自体を標的にし、データを暗号化することでリストアしたくてもできないようにすることもできます。ではどうすれば良いのでしょうか。

ゲームオーバーです。

>>> PRO TIP

サイバーリカバリソリューションは、データの履歴を分析してセキュリティ侵害の兆候をとらえ、初期ポイント、範囲、感染時刻を明確にすることで、マルウェアの再感染を阻止し、電子情報の科学捜査をサポートするものでなければなりません。

AMERICAN FAMILY INSURANCE®

“

脅威の特定はAmFamにとっての革命でした。これにより、当社のセキュリティチームは、エコシステム全体にわたって特定のマルウェアやゼロデイ脆弱性を探すことができます。

Nate Brooks
AmFam、
テクノロジーサービスマネージャー

- 13のバックアップベンダーを1つの安全なソリューションに**統合**
- レジリエンス状況とセキュリティフットプリントの**単一表示**
- **1,300万人**の顧客を保護
- レジリエンス時間を数日から数時間**に短縮**

carhartt

“

私たちは侵入者を防ぐために
懸命に働きます。しかし、侵入者が
侵入経路を見つけ出すことを
前提に行動しなければなりません。

Michael Karasienski
Carhartt、
クラウドプラットフォームマネージャー

- レガシーバックアップツールに**マルウェアを発見**
- クラウドとオンプレミスの**単一ソリューションに移行**
- **600以上**のワークロードを移行
- 毎月のコストを**50%以上**削減

5 バックアップに時間がかかると、復旧も遅くなる可能性があります

従来のソリューションを使用してデータをバックアップすると、時間も手間もかかります。これは、常に変化する大量のデータをバックアップしている場合に特に当てはまります。たとえば、オンライン決済を利用するビジネスの場合、取引情報は多くの場合、指数関数的に増大する可能性のあるデータベースに保存されます。そのようなデータをすべてバックアップすると、重要なシステムの動作が遅くなったり、最悪の場合、完全にクラッシュしたりする可能性があります。

問題を引き起こすもう一つの要因は、自動化および連携の欠如です。レガシーシステムでは、バックアップやリストアを開始するために、手作業の介入が必要になることがよくあります。手作業であるため、これらの介入には時間がかかり、エラーが発生しやすくなります。また、復旧のシミュレーションやテストができないため、復旧が必要な場合にどれくらいの時間がかかるのか、あるいは復旧できるかどうかさえもわからないまま放置されることがよくあります。

さらに、最悪の事態が発生して攻撃後に復旧が必要になった場合、レガシーシステムでは、必要なデータだけをリストアするのではなく、システム全体（場合によってはペタバイト相当のデータ）をリストアしなければならないことがよくあります。復旧する必要のない大量のデータを復旧することは、**一分一秒を争う**プロセスにおいて、膨大な時間を浪費する可能性があります。

繰り返しますが、レガシーシステムはリストアされたデータにマルウェアがないことを確認する簡単な方法さえ提供しません。そのため、たとえ素早くシステムを再稼働させることができたとしても、その環境には時限爆弾が仕掛けられている可能性があり、数か月にわたってその影響に対処しなければならないこともあります。

サイバー攻撃からの復旧に取り組んでいる場合、そのような時間はありません。

>>> PRO TIP

手動プロセスを制限する自動化、復旧プランのテストと検証を可能にするサイバーリカバリシミュレーション、必要なデータのみのリストア機能により、サイバーリカバリが攻撃から可能な限り迅速に立ち直るのに役立つことを確認してください。

SLCC
SOUTH LOUISIANA COMMUNITY COLLEGE

“

Rubrikのバックアップがなければ、復旧には何週間もかかったでしょう。Rubrikの書き換え不可のバックアップのおかげで、**今回の侵害は**バックアップを再起動する間の2時間の**不便のみにとどまりました。**

Nick Pitre
南ルイジアナコミュニティカレッジ（SLCC）のIT責任者

- **2時間**以内に100%復旧
- 失ったデータは**ゼロ**
- ランサムウェアによる身代金の支払は**ゼロ**

“

私たちの顧客は、信頼できる安全な会社と提携していることを知りたがっています。Rubrikは私たちのデータに対する保険証券です。**その安心感を、いかにして数値化できるでしょうか。まさにプライスレスです。**

PAYETTE

“

ニュースは決して止まることはありません。サイバー脅威が私たちのスピードを緩めることは許されないのです。**Rubrikのおかげで、データが保護され、利用可能であるという安心感が得られます。**これにより、読者に情報を提供し、地域社会が繁栄するための力を与える最高のニュースソースになるというコミットメントに集中することができます。

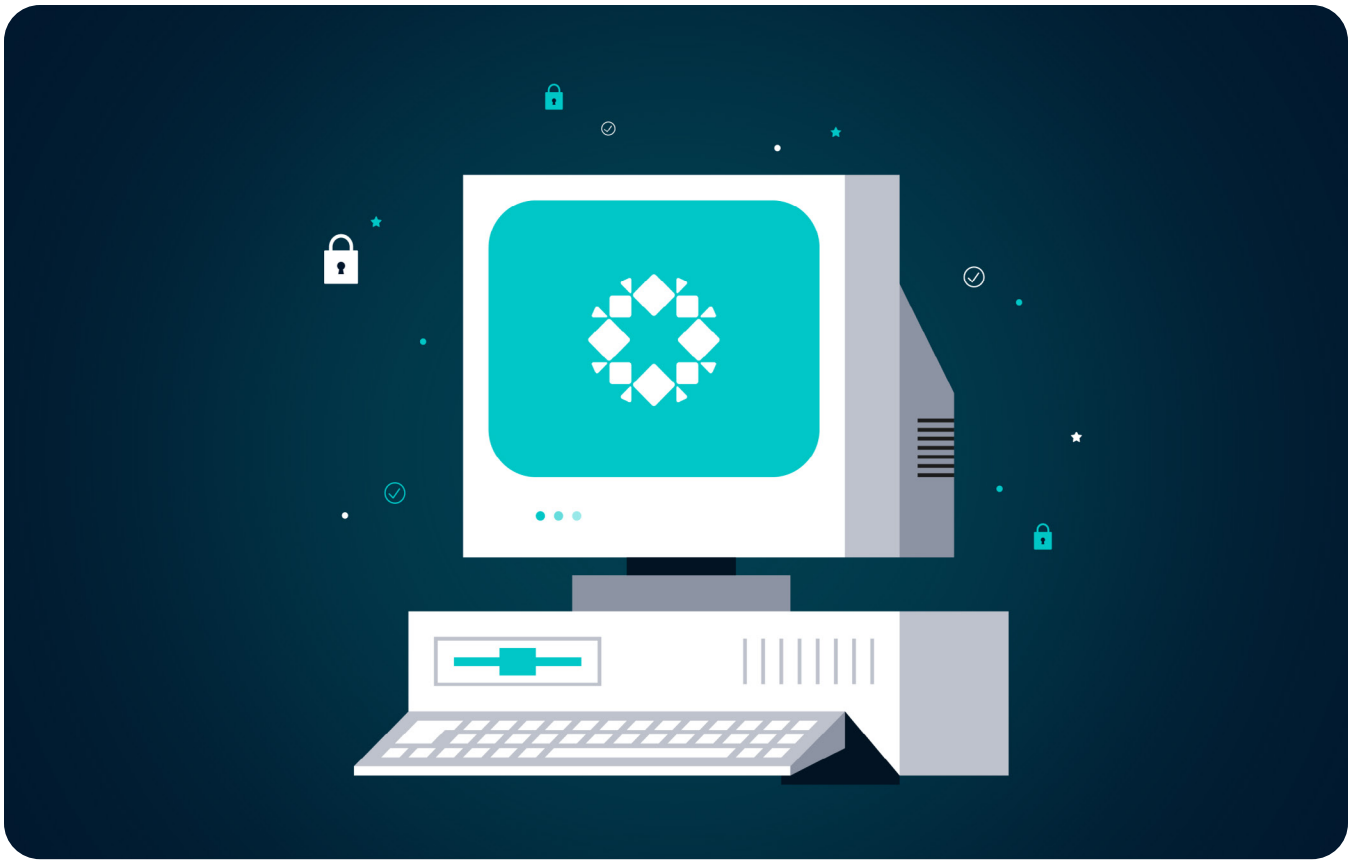
GANNETT

データをRUBRIK SECURITY CLOUD以外に託さないようにしましょう

レガシーバックアップベンダーはこれらのことを教えてくれません。では、現代のセキュリティ専門家はどうすればいいのでしょうか。

今こそレガシーバックアップを捨てて、サイバーレジリエンスソリューションを手に入れる時です。そうすることでデータの安全性と可用性を維持し、データリスクと脅威を早期に発見でき、より速く、より安全で、さらに信頼性の高いデータ復旧を可能にします。

Rubrik Security Cloudsのゼロトラストアプローチは、悪質業者を排除し、脅威を監視することで、データを可能な限り迅速に復旧させます。さらに、システムパフォーマンスへの影響を最小限に抑える自動化と永久増分バックアップにより、お客様のデータ保護をより簡単にします。そのため、無限に続くと思われる手作業に時間を費やすことなく、何があっても稼働し続ける能力に確信を持つことができます。



Rubrikは、レガシーバックアップソリューションにはない4つのユニークな利点をあなたの組織に提供します。

- **データ保護：**自動化およびエアギャップ化され、また、変更不可能でアクセス制御されたバックアップは、サイバー攻撃、悪意のある内部者、運用の中断に耐えられるように設計されており、データの完全性と可用性を確保します。
- **データ脅威分析：**ランサムウェア、データ破壊、侵害の兆候など、データへの脅威を継続的に監視します。
- **データセキュリティ態勢：**機密データの漏洩（ユーザーアクセス分析を含む）をプロアクティブに特定および監視し、インテリジェントな洞察力を活用してデータへのリスクを軽減します。
- **サイバーリカバリ：**数週間から数か月ではなく、数時間から数日以内に通常通りの業務に迅速に復帰します。自動化された復旧連携とシステム検疫により、マルウェアの再感染を回避しながら脅威を封じ込め、アプリケーション、ファイル、またはオブジェクトを迅速に復元できます。

レガシーバックアップが失敗だったと気づくのは、サイバー攻撃によってビジネスが停止してからでは遅すぎます。サイバーリカバリのために設計されたデータセキュリティソリューションに切り替えましょう。Rubrikならデータを安全に保ち、脅威を特定し、迅速な復旧を促進します。

レガシーバックアップにビジネスを任せないでください。手遅れになる前に、真のサイバーレジリエンスソリューションを手に入れましょう。

こちらから詳細をご覧ください。