データのバックアップと復元にゼロトラストを拡大

ITおよびセキュリティの
プロフェッショナルのための
実践的ガイド

コンテンツ

エグゼクティブサマリ

「ゼロトラスト」は、ランサムウェアやその他の脅威からエンタープライズITインフラストラクチャをより強力に保護するための、最新の非常に効果的な戦略です。データのバックアップと復元のシステムはエンタープライズにとって重要であり、あらゆるゼロトラストイニシアチブに組み込む必要があります。

しかし、ゼロトラストは設計と実装が複雑になる場合があり、これまで、データのバックアップと復元のシステムにゼロトラストをどのように適用するのが最適かについてのコンセンサスが得られていませんでした。

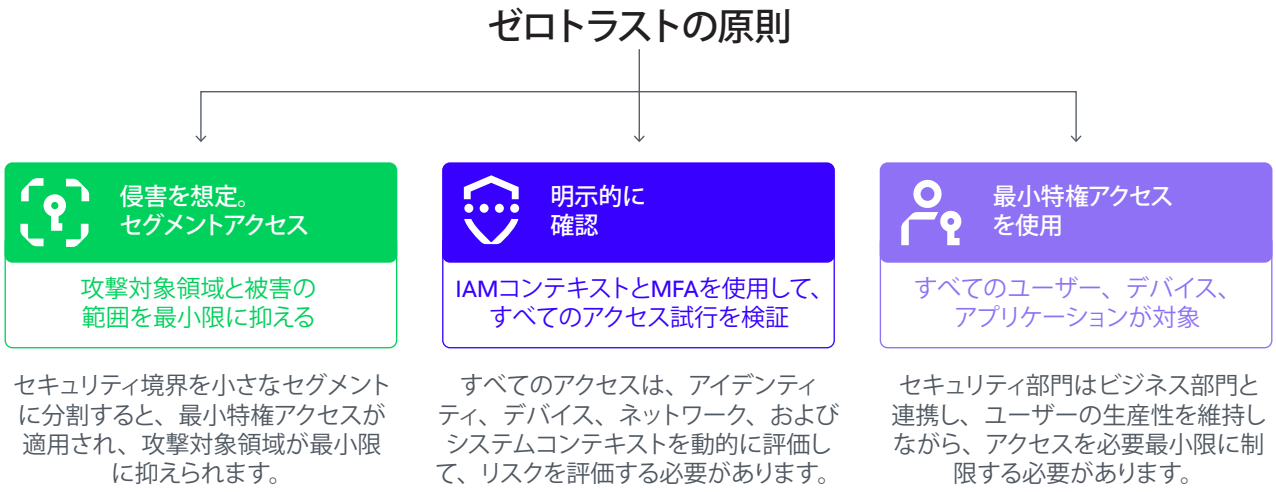
ゼロトラストのデータレジリエンス（ZTDR）は、VeeamとNumberline Securityが導入した新モデルで、Cybersecurity and Infrastructure Security Agency（CISA）のゼロトラスト成熟度モデルに基づいて構築されています。ZTDRは、ゼロトラストの原則をバックアップと復元に拡張し、エンタープライズがリスクを軽減し、セキュリティと回復力の目標を達成できるようにします。

このガイドで説明するゼロトラストのデータレジリエンスのアプローチに従うことで、データのバックアップと復元のプラットフォームとアーキテクチャで何を探すべきかを学び、環境で迅速かつ効果的に開始できるようになります。

ゼロトラスト：概要のご説明

ゼロトラストは、ユーザー、デバイス、またはネットワークパケットを暗黙的に信頼してはならないという考えに基づく最新のセキュリティ戦略です。データセキュリティを確保するには、重要なデータ資産へのアクセスをセグメント化し、アクセスを許可する前に、すべての通信を認証、評価、承認する必要があります。これは、各セグメントとそのデータ、アプリケーション、資産、またはサービスに適用する必要があります。

これは、静的なネットワークベースの境界をベースとしていてランサムウェアや悪意のある攻撃者からのエンタープライズの保護に明らかに失敗していた従来の情報セキュリティアーキテクチャからの大きな転換です。



ゼロトラストのデータレジリエンス（ZTDR）の導入

データのバックアップと復元のシステムはエンタープライズITにとって重要な要素であると同時に、頻繁に攻撃の標的となります。それらは適切かつ総合的に保護されていなければなりません。

ZTDRの原則に従い、ZTDRガイダンスに基づいてバックアップおよびストレージのベンダーを選択することで、エンタープライズはより強力な防御、より効率的な運用、より高速で信頼性の高い復元を得ることができます。

ZTDRがゼロトラストのコア原則を強化

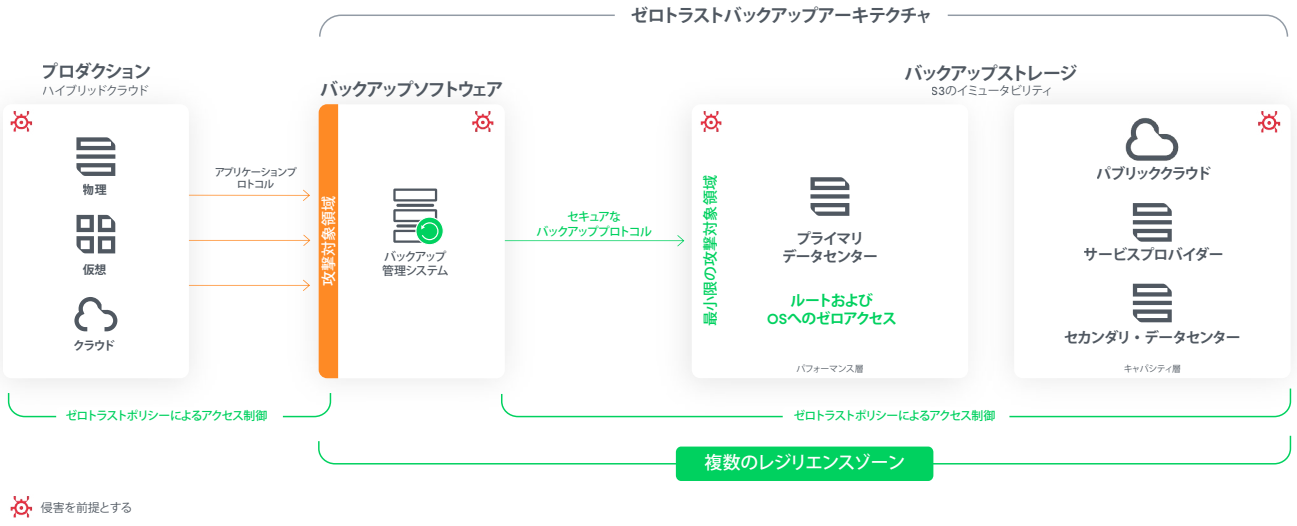
	バックアップソフトウェアとバックアップストレージの分離	複数のレジリエンスゾーン	イミュータブルなバックアップストレージ
	攻撃対象領域と被害の範囲を最小限に抑える	3-2-1バックアップルール	バックアップデータを変更や削除から保護
ソリューションの要件	バックアップソフトウェアとストレージを分離し、理想的にはバックアップストレージへのルートまたはOSアクセスを防止するように設計された、データのバックアップと復元ソリューションを探します。 これらの機能により、ゼロトラストポリシーを介してアクセス制御を厳密に実施できるようになります。	複数のレジリエンスゾーンをサポートする、データのバックアップと復元ソリューションを探します。これにより、単一のバックアップシステムやストレージ環境が消失または侵害されても組織は耐えることができます。 これにより、バックアップの3-2-1ガイドラインを容易に満たすことができます。	堅牢で信頼性の高い、イミュータブルバックアップストレージを簡単かつ効率的にサポートする、データのバックアップと復元ソリューションを探します。 これにより、たとえ悪意のある攻撃者がいたとしても、バックアップされたデータが削除や変更から保護されているという安心感が得られます。

バックアップのベストプラクティスのための3-2-1ルール：

3	2	1
本番データを含む、データのコピーを3つ作成する。	別々のレジリエンスゾーンにあるイミュータブルストレージ上にバックアップデータのコピー2つを保存する。	コピーの1つはオフサイトに保管する。

ZTDRリファレンスアーキテクチャ

このZTDRリファレンスアーキテクチャでは、ゼロトラストプラットフォームをバックアップ管理とストレージシステムと組み合わせて導入する方法を示します。



ZTDRの使用開始

ゼロトラストは1つの取り組みですが、データのバックアップと復元のインフラストラクチャのセキュリティの回復力を向上させるために、すぐに実行できるインパクトのあるステップがあります。

今週：

貴社のバックアップと復元のシステムがZTDR要件をどの程度満たしているかを確認します。

タスク	質問集
ネットワークのセグメンテーションについて、ネットワークおよびITインフラストラクチャチームと話し合ってください	• ネットワークはどのようにセグメント化されていますか？ • バックアップソフトウェアとバックアップストレージは別々のセキュリティゾーンに区分されていますか？ • バックアップインフラストラクチャの各セグメントへの、そして各セグメントからのアクセスはどのように制御されますか？
バックアップデータストレージが複数のレジリエンスゾーンに編成されているかを評価する	• 業界のガイダンス（3-2-1ルール）に沿っていますか？ • バックアップゾーンの1つが利用できない場合、バックアップと復元のプロセスはどうなるでしょうか？ • バックアップゾーンのうち2つが利用可能ではない場合、バックアップと復元のプロセスはどうなるでしょうか？
バックアップストレージシステムが適切にイミュータブルであるかどうかを判断する	• ストレージベンダーはどのようにしてイミュータビリティを文書化し、保証していますか？ • 悪意のある管理者が、ルートまたはOSによるストレージへのアクセスを使用して、イミュータビリティや保持の設定を変更できますか？ • システム時刻が悪意を持って進められた場合はどうなりますか？
復元プロセスを検証する	• 当社のDR対応計画はどのようなものですか？最後にテストしたのはいつですか？ • 文書化された手順に従ってシステムを正常に復元できるITチームまたはストレージチームのメンバーは何人いますか？ • インシデント時に（重要人物X）が不在の場合はどうなりますか？

来週：

貴社のプロセスとツールを検証し、バックアップと復元のインフラストラクチャとプロセスに対する短期的および中期的な変更について計画し、合意を形成します。

タスク	質問集
定期的（週次または月次）のテストを実施することにより、復元プロセスの信頼性と再現性を評価する	• 復元テストはどのくらいの頻度で実行していますか？ • ドキュメントやプロセスのギャップについて何を学びましたか？ • これらはいつ是正できますか？

タスク	質問集
ネットワーク構成、セグメンテーション、またはファイアウォールルールの変更の計画を開始する	• ITチームまたはセキュリティチームの誰と一緒に、潜在的な変更を詳しく調べることができますか？ • セキュリティチームでゼロトラストの取り組みを主導しているのは誰で、どのようにサポートすればよいですか？ • どのようなネットワークセグメンテーションまたはインフラストラクチャの変更が進行中ですか？
イミュータビリティのギャップを埋めるために、ストレージ構成の変更や新規ベンダーの評価を計画する	• 追加のバックアップストレージを評価および調達するためのプロセスはどうなっていますか？ • どのような財務的、効率、またはリスクの正当化を行う必要がありますか？ • ベンダー評価プロセスを開始するための承認を得るには、どのようにすればよいですか？
プロセスとドキュメントの改善に責任を持つ所有者を割り当てる	• （プロセスX）の変更の承認と実装には、誰が関与しますか？ • 相互に合意できる導入期限を設定するにはどうすればよいでしょうか？

来月：

短期的な変更の実施と必要な長期的な変更の特定を開始します。

タスク	質問集
改善したディザスタリカバリプロセスを導入して再度テストする	• DRプロセスはどの程度改善されましたか？ • プロセスとドキュメントのすべてのギャップに対処できましたか？
ネットワークセグメンテーションを検証し、反復する	• ネットワークのどの領域で、バックアップシステムとの間での広範なネットワークアクセスが許可されていますか？ • セキュリティを強化するには、ランサムウェアに対する回復力をどのように向上させるべきでしょうか？
ストレージ容量、場所、イミュータビリティの改善を実行する	• バックアップストレージの容量にどの程度自信がありますか？ • バックアップストレージシステムがイミュータブルであるとどの程度確信できますか？ • 3-2-1のベストプラクティスガイダンスにどの程度適切に従っていますか？ • 複数のレジリエンスゾーンをどのように活用していますか？

他に何を探すべきですか？

プロアクティブなディザスタリカバリ検証

バックアップされたデータの復元を必要とするインシデントは、予期しないタイミングで、ストレスのかかる状況で発生する可能性が高くなります。組織は、よく理解され、十分に文書化され、繰り返し練習されたディザスタリカバリの計画とプロセスを持つことが重要です。また、バックアップされたデータの整合性と有効性に対する高い信頼度を確保します。

運用のシンプルさ

組織が簡単かつ自信を持って運用できるほどシンプルでありながら、企業のニーズを完全に満たすのに十分な機能、スケーラビリティ、および洗練さを備えたシステムを選択するようにしてください。スタッフの能力とスキルを明確に理解し、業務が特定の個人や「スーパーヒーロー」に依存しないようにします。

よくある質問

ゼロトラストはベンダーから購入できるものですか？

いいえ。ゼロトラストは貴社が**実践する**ものであり、IT、セキュリティ、ビジネスの成果を変化させ改善するセキュリティ戦略です。

ゼロトラストは、アクセスを制限し、ユーザーの生産性を低下させるだけなのでしょうか？

いいえ — ゼロトラストとは、ユーザーの生産性を維持しながら**不要な**アクセスをすべて排除することです。多くのエンタープライズは、ゼロトラストによってユーザーの生産性とユーザーエクスペリエンスを実際に**向上**させています。

なぜゼロトラストが重要なのですか？

ゼロトラストは、ランサムウェアや悪意のある攻撃者、その他のリスクからエンタープライズを守るための最も効果的な方法です。現在の脅威の状況を考えると、私たちにはそれを利用する責任があります。

現在のセキュリティインフラストラクチャをゼロトラストに使用できますか？

ほとんどの場合、はい！最新のファイアウォール、ID、インフラストラクチャシステムを適切に使用すれば、ゼロトラストの取り組みを開始する際にサポートできます。最適なレベルのゼロトラスト成熟度を達成するには、追加の投資が必要になる場合がありますが、これはZTDRリファレンスアーキテクチャなどのツールによって導かれます。

関連情報

ゼロトラストとZTDRについてもっと知りたいですか？

- ZTDRの調査の全文と、データセキュリティおよびサイバー回復力に対するVeeamのアプローチについては、VeeamのWebサイトをご覧ください。
- ZTDRの調査ホワイトペーパー全文と、これに関するNumberline Securityの見解については、NumberlineのWebサイトをご覧ください。

Veeam Softwareについて

データレジリエンスにおけるNo. 1のグローバルマーケットリーダーであるVeeamでは、企業は必要なタイミングと必要な場所で、あらゆるデータを管理する必要があると考えています。Veeamは、データのバックアップ、データの復元、データの自由、データセキュリティ、データインテリジェンスを通じて、データの回復性を提供します。米国ワシントン州シアトルを拠点とするVeeamは、世界中で55万社以上のお客様に保護を提供しており、お客様からはビジネス継続性について多大な信頼をお寄せいただいています。詳細については、www.veeam.com/jpをご覧になるか、LinkedIn（@veeam-software）とX（@veeam）でVeeamをフォローしてください。

詳細はこちらveeam.com