rubrik

単一の統合プラットフォームによる、Active Directory、Entra ID、Oktaのアイデンティティを保護

エージェント型サイバーレジリエンスプラットフォームで、ツールの断片化による高いTCOを回避し、アイデンティティシステムの安全性、運用性、および復旧可能性を保証

システムへのアクセス権を取得するために、Active Directory（AD）、Entra ID、OktaなどのIdPを侵害する攻撃者が**増加**しています。従来のEDRやマルウェア検知ツールをすり抜け、アイデンティティを侵害してログインすると、正当なユーザーを締め出し、アイデンティティやデータを人質に取り、身代金を要求してきます。企業はシステムへのアクセスができなくなり、ビジネスは混乱し、各チームは対応に奔走することになります。

多くの組織は防御のために単体のソリューションに依存しており、それが危険な死角を生み出しています。ITおよびセキュリティチームは、ドメイン間の関連性が欠如した断片的なアラートを頻繁に受け取り、孤立したデータストリームから一貫した全体像を組み立てる必要に迫られます。複数のツールが存在するため、チームはプレッシャーの高い危機的状況下で複雑なワークフローを調整せざるを得なくなります。

複数のポイントソリューションを使用すると、次のような結果につながります：

- **重要な可視性の欠如と遅延**
- **運用コストの増加**
- **復旧の遅延**
- **TCOの増加**

オーケストレーションによる復旧が必須：依存関係が復旧の成功を左右

1. **ADより前にEntraを復元 → 関連付けが失われ、メタバースの完全同期が必要**

   Active Directoryより前のバックアップからEntraを復元した場合、ハイブリッドオブジェクトが関連付けを解除される可能性があり、関係が再確立された後にEntra Connectの完全同期が必要になる可能性があります。大規模環境では、これには数日かかる場合があり、ダウンタイムが大幅に増加する可能性があります。

2. **Okta Group ID Mappingなしでのポリシーの復元 → アクセス混乱**

   バックアップから復元されたグループには、以前関連付けられていたセキュリティポリシーにマッピングされていない新しいグループIDが割り当てられるため、リソースへのアクセスが妨げられ、意図しないアクセスが可能になる可能性があります。

3. **古いサービス認証情報の復元 → 自動化の停止**

   サービスアカウントを以前の状態に戻すと、アクティブなスクリプトやツールが認識しなくなった古いパスワードが復活し、重要なバックグラウンドワークフローが即座に停止する可能性があります。もしその障害が発生したサービスが他のサービスを監視している場合、そのことに気づくことさえできないでしょう！

4. **分断されたポイントソリューションでの復元 → 攻撃者の永続性**

   個別の復旧ツール間で可視性にギャップがあると、あるプラットフォームから攻撃者を排除できたとしても、別のプラットフォームには、まだ攻撃者が潜んでいる可能性があります。これは、攻撃者が復旧したシステムを再び侵害する可能性があることを意味します。

システム全体のアイデンティティリスク：単一のIdP侵害がもたらす連鎖的影響

Rubrikは、ハイブリッドアイデンティティシステムを保護するための統合されたアイデンティティレジリエンスプラットフォームを提供することで、これらのギャップを解消します。これにより、組織はアイデンティティ関連のインシデントを調査し、運用稼働時間を維持し、信頼を回復することができます。

ハイブリッドアイデンティティシステムを単一プラットフォームで保護することの戦略的メリット

1. **セキュリティポスチャー、保護、コンプライアンスを簡素化：**セキュリティポスチャーに詳細な可視性を取り入れましょう。Rubrikは、信頼性の高い履歴的なアイデンティティ状態とアイデンティティ変更のテレメトリを提供する、不変の記録システムです。また、アクター属性付きの不変アクティビティログを使用することで、コンプライアンス監査やフォレンジック調査を簡素化することもできます。

2. **運用稼働時間を維持：**アイデンティティ変更の追跡、障害の監視、根本原因分析、および構成のロールバックにより、IAMチームはアイデンティティの障害を迅速に検知、診断、解決できます。これにより、ダウンタイムと運用リスクを低減しつつ、数回のクリックでAD、Entra ID、Okta全体におけるインシデント対応と復旧を迅速化できます。

3. **インシデント対応を加速：**連携が取れていないツール間でデータを照合する際の「手間」を軽減します。さまざまなツールからログを手動でつなぎ合わせることなく、脅威がシステム内でどのように移動したかを理解できます。製品内部から変更を元に戻し、正当な変更は維持したまま、攻撃者の永続性を排除します。

4. **TCO削減：**AD、Entra ID、Oktaといった個別のバックアップツールやセキュリティツールを運用する際の、ライセンス料、メンテナンス費用、トレーニング費用を削減します。断片化された個別ソリューションを単一のプラットフォームに置き換えることで、ライセンス料と管理の複雑さを軽減します。

5. **正当な変更を反映：**クリーンなベースラインに復元してから、承認されたアイデンティティ変更を順次適用することで、悪意ある攻撃者の永続メカニズムを削除し、アイデンティティシステムへの数か月分の更新が消去されるのを回避します。

マルチIdPソリューションでAD、Entra ID、Oktaの保護を簡素化

1. **単一プラットフォームによる統合的な保護：**複雑な環境向けに特別に設計された、直感的な単一のコンソールから、オンプレミスのADオブジェクトからクラウドネイティブなOktaの設定に至るまで、アイデンティティ環境全体を保護します。

2. **オーケストレーションによる復旧：**複雑な相互依存関係を容易に処理できます。ADテナント全体を復元する場合でも、OktaやEntraのIDオブジェクトを1つだけ復元する場合でも、Rubrikはシステムが初回から正しくオンラインになることを保証します。

3. **事業継続性：**アイデンティティ環境の復元を簡素化します。複数のIdPが侵害されたかどうかを検知し、障害を特定して隔離し、数クリックで復旧させることで、アプリケーションとユーザーの稼働時間を維持します。

4. **改竄防止アーキテクチャ：**Rubrikの「Bunker in a Box」アーキテクチャは、論理的に隔離された、改竄不可能なバックアップを提供し、重要なアイデンティティとデータを保護します。.

アイデンティティシステムの未来を安全に守りましょう

なりすまし攻撃が高度化し、アイデンティティ環境が複雑化するにつれ、分断化による損失は無視できないほど大きくなっています。Identity Resilienceは、アイデンティティシステムが信頼性、運用性、復旧性を維持することを保証し、組織がハイブリッド環境全体でアクセスを維持し、インシデントを調査し、アイデンティティインフラストラクチャを復旧できるようにします。Rubrikは、攻撃者によるシステムへの潜伏リスクを低減し、正当なアイデンティティ変更を自動的に反映させることで、数ヶ月分の作業データを失うことなく、システムを完全に復旧させることができます。Rubrikを使えば、システムを常にクリーンで最新の状態に保つことができます。

デモをご依頼いただければ、オーケストレーションによるアイデンティティの復旧が実際にどのように機能するかをご覧いただけます。