

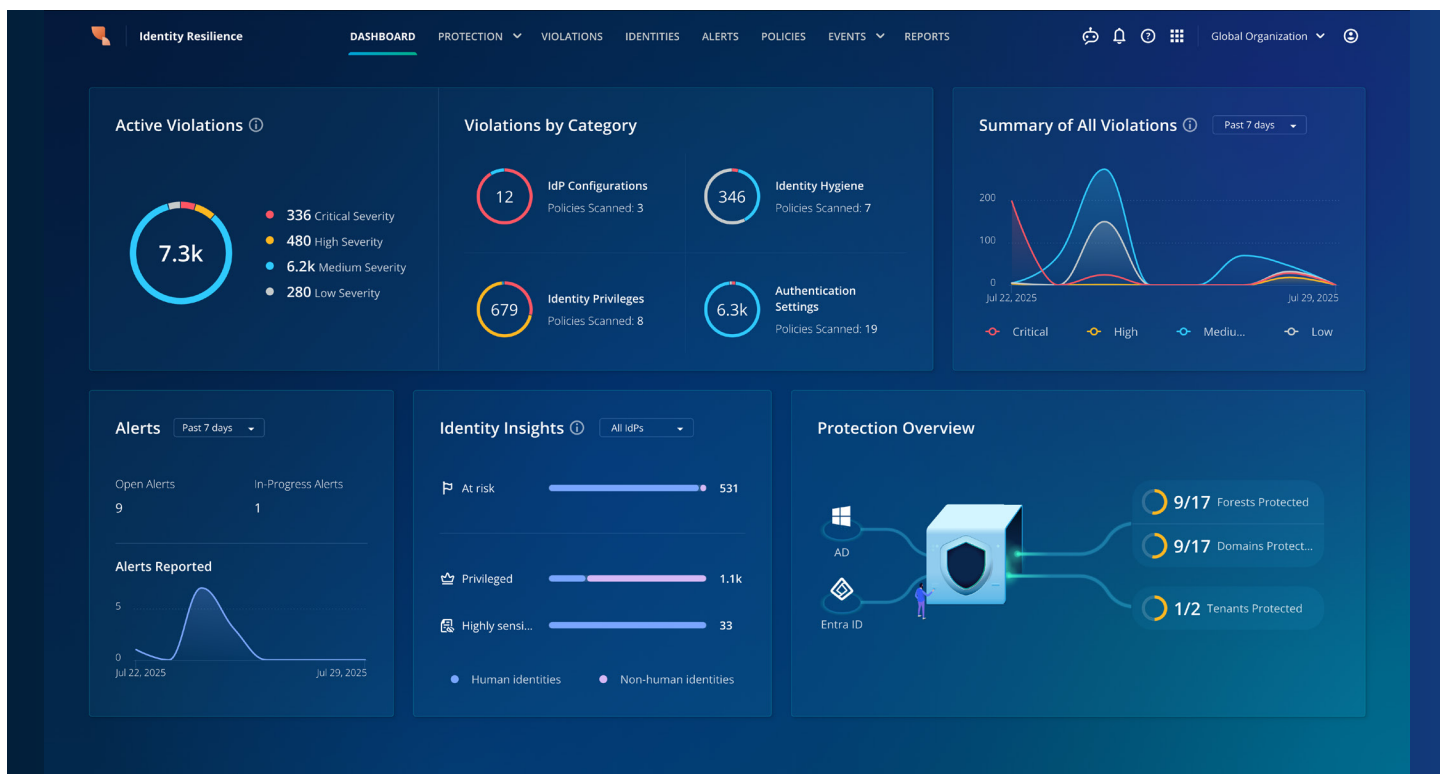
Rubrik Identity Resilience

技術概要

アイデンティティインフラは、攻撃の脅威にさらされています。

Rubrik Identity Resilienceは、攻撃前、攻撃中、攻撃後の各段階において、組織のアイデンティティシステムを保護・復旧できるよう支援します。可視化の確保、リアルタイム検知、オーケストレーションされた復旧を単一の統合プラットフォーム上で実現することで、Rubrikはリスクの修復、重要な変更のロールバック、迅速な復旧を可能にします。これにより、アイデンティティを基点とする攻撃があっても、ビジネスのレジリエンスを維持することが可能になります。

Active Directory (AD) と Entra ID は、企業のアクセス基盤を構成するシステムですが、特にハイブリッド環境やマルチクラウド環境の場合、これらのシステムを保護することはますます複雑になっています。相互に統一性のないツールやスクリプト、ポイントインタイム評価に依存すると、アイデンティティを基点とする脅威に対して脆弱な状態に陥る可能性があります。手作業による脅威調査や、攻撃者が残したバックドアや弱点を特定・ロールバックしようとする作業も、攻撃者が環境内で検出されないまま潜伏し続ける余地を与える恐れがあります。さらに、復旧プロセスを手作業で実行することは、ダウンタイムを長期化させ、ビジネスをより大きなリスクに晒すこととなります。



現在の脅威環境では、アイデンティティを基点とする攻撃経路が主流です。サイバー侵入のうち80%以上が、侵害された認証情報や、権限昇格や、誤設定されたアクセス制御を悪用するという経路でシステムへ侵入し、ネットワーク内をラテラルムーブメントし、業務を妨害しています。Scattered Spiderのような巧妙な脅威グループは、こうした設定上の盲点や検知の隙について、従来型のセキュリティツールを回避しながらネットワーク内を移動します。

既存のITセキュリティスタックには、統合的かつリアルタイムに動作するテレメトリや、アイデンティティの状態や挙動をプラットフォームをまたいで可視化できる機能が欠けていることが多く、そうしたバラバラな性質が大きな問題の源となっています。さらに、ほとんどのソリューションは、不正なアイデンティティ設定変更やアクセス権の濫用があった際にロール

バックや復旧を行うメカニズムを備えていません。その結果、アイデンティティの復旧ワークフローが、手作業のプロセスや、すでに侵害されている可能性のあるシステムバックアップや、不完全で書き換え可能な監査ログに依存しているケースが散見されます。

(継続的なポリシー適用、改ざん防止機能のある監視、オーケストレーションされた復旧機能を組み合わせたという意味で) 統合的かつレジリエンスのあるアイデンティティセキュリティフレームワークを備えていない組織は引き続き、アイデンティティ関連の脅威の深刻化、業務中断、データ侵害の長期化に見舞われることとなります。

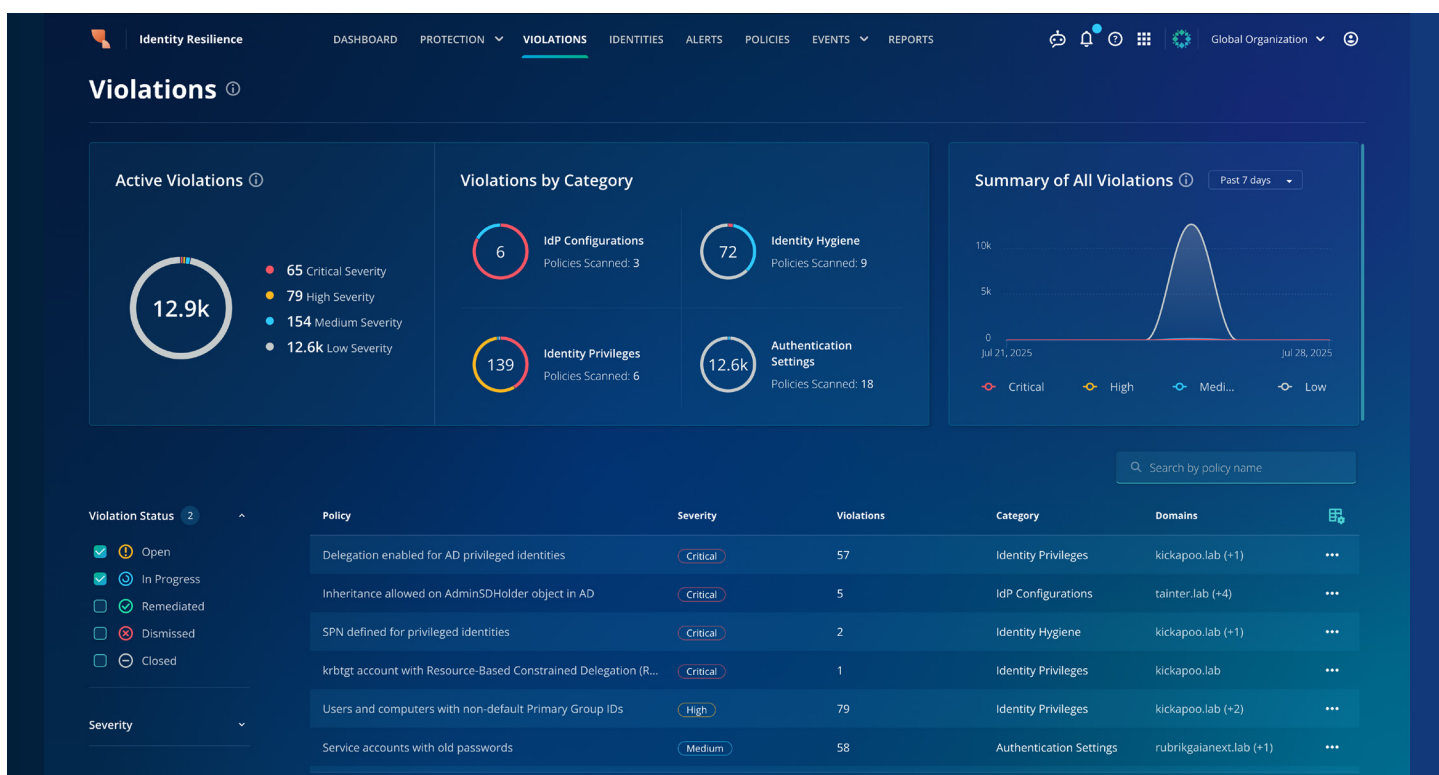
Rubrik Identity Resilienceは、脅威アクターが悪用する最も脆弱なポイントを包括的に可視化することで、こうした不備を解消します。また、ラテラルムーブメントや権限昇格などに利用されてしまう重要な変更をリアルタイムに近い形で継続的に監視・検知することで、迅速にリスク修復を実行し、エクスポージャーギャップを解消し、さらなる被害を及ぼす前に脅威アクターを排除できるよう、組織を支援します。

統合的アイデンティティインベントリ

クラウド内およびクラウド間でのシステム利用が増加する一方、多くの組織はいまだにオンプレミス環境へ多大な投資を続けています。そのため、アイデンティティシステムが複数のプロバイダに分散していることは珍しくありません。Rubrik Identity Resilienceは、統合された単一のアイデンティティインベントリを提供することで、オンボードされたすべてのアイデンティティプロバイダ (IdP) にわたってアイデンティティ (人間と非人間の両方) および関連するリスクやアラートを可視化します。さらに、Rubrik DSPMと連携して使用した場合、各アイデンティティがアクセスできる機密データの詳細も表示します。これにより、アイデンティティを優先順位付けする際に、各アイデンティティが当該IdPの下で備えている権限だけでなく、各アイデンティティがアクセス可能な機密データの重要度も考慮することができるようになります。

ポリシーベースのアイデンティティリスク検知

Rubrik Identity Resilienceは、オンボードされたすべてのIdPにわたってすべてのアイデンティティ (人間のアイデンティティおよび非人間アイデンティティ (NHI) を含む) を表示する、包括的なアイデンティティインベントリを構築します。このインベントリは、一度作成されるとスナップショットが取得されるごとに自動的に更新されます。そして、強力なポリシーエンジンが設定内容を監視し、定義されたポリシーへの準拠状況を継続的にスキャンします。Identity Resilienceは、広く認知されているセキュリティおよびベストプラクティスのフレームワーク (たとえば、MITRE ATT&CK、D3FEND、OWASP、ANSSI) に対応した、多数のポリシーを標準で備えています。該当する場合には、これらのポリシーは、複数のIdP間で統一された内容となっています。これらのポリシーの例としては、「委任権限が有効になっている特権アイデンティティ」、「MFAの適用が弱いまたはMFAが適用されていないユーザー」、「古いパスワードを使用しているサービスアカウント」などが挙げられます。これらは、認証情報が適切にローテーションされていない可能性を示すものです。



ポリシー違反が検出されると、ユーザーインターフェース上で強調表示され、ITSMツール（ServiceNowなど）でチケットを発行するオプションや、可能な場合は当該IdPにおいて違反を直接修正するオプションが提供されます。さらに、セキュリティ違反に関する情報はWebhook経由でSIEMツールやSOARツールへ送信でき、これらのツールから自動的にワークフローをトリガーすることが可能です。

The screenshot shows a security alert titled "Delegation enabled for AD privileged identities" with a "Critical" severity. It was violated by "Black Hat" and detected on "Jul 25, 2025, 5:30 PM". The status is "Open". A "REMIEDIATE" button is visible, with a dropdown menu containing "Create Ticket" and "Disable Delegation". Below the alert, there is explanatory text: "If delegation is enabled, an identity with delegation rights over the privileged identity can take actions on its behalf. Attackers can target those identities and perform administrative actions. Ensure that delegation rights to privileged identities are approved." A table shows the "Framework" as "--" and the "Category" as "Identity Privileges". An "Overview of Black Hat" section includes fields for "Title" ("--"), "Department" ("--"), "Source" ("kickapoo.lab"), and "Native Type" ("AD User"). An "Insights" section shows "Privileged +1" and a "Unique Identifier" of "blackhat@kickapoo.lab". A "Remediation Process" section provides instructions: "Disable delegation for privileged identities. For users, it's recommended to assign them to the 'Protected Users' group. Alternatively, you can enable the setting 'This account is sensitive and can't be delegated'. For computers and service accounts, disable delegation by disabling the setting 'Trust this computer/user for delegation to any service'. If delegation is required, convert to constrained delegation that limits which services an identity can delegate to." A "VIEW IDENTITY SUMMARY" link is at the bottom right.

重要な変更に対する準リアルタイム監視

一部の監視ツールは、不審な活動を検出するために、Windowsイベントログをスキャンしたり、Windowsイベント転送（WEF）を利用します。ただし残念ながら、脅威アクターはこうした仕組みを認識しているうえ、自分たちの都合のよいデータでログファイルを簡単に上書きできることや、痕跡を隠す必要があればログファイルを消去できることも知っています。堅牢なイベント追跡機能がなければ、悪意のある活動を検出することはほぼ不可能になります。

Rubrik Identity Resilienceは、Windowsイベントログに依存せずにActive Directoryを継続的に監視します。この独自のアプローチは改ざん防止機能を備えており、攻撃者が検知されずに潜伏し続けることを著しく困難にします。IdPからRubrikのプラットフォームにイベントデータが書き込まれると、そのデータはバックアップデータと同様に書き換え不可の状態となるため、イベントデータの完全性が保証されます。

不審な活動（権限昇格や、グループポリシーオブジェクト（GPO）の編集など）が検出されると、即座にアラートが出され、トリアージと修復のプロセスが開始されます。

Alert Details

Changes to GPOs can significantly impact system configurations and security postures. Unauthorized or incorrect modifications can compromise security controls and introduce vulnerabilities. It is crucial to investigate such changes promptly to maintain the integrity and security of your environment.

Timestamp	Source	MITRE Tactic
Mar 20 2025, 9:02 PM	design.acme.com	Privilege escalation (+3)

GPO Details

Linked OUs and Domains	GPO Status	Group Owner
Product Design (+1)	Enabled	Mukul Bisht

Recommended Response

To address this alert, revert unauthorized modifications immediately and conduct a thorough examination to identify the root cause. You can use Rubrik's latest snapshot of this GPO to revert the change to a safe state. This ensures your system configuration is restored promptly while the underlying issue is being addressed.

GPO Changes Relative to GPO version on Mar 10, 2025, 8:01 PM

```

< q1:Account>
  <q1:Name>MaxClockSkew</q1:Name>
  <q1:SettingNumber>5</q1:SettingNumber>
  <q1:Type>Kerberos</q1:Type>
</q1:Account>
<q1:Account>
  <q1:Name>MaxRenewAge</q1:Name>
  <q1:SettingNumber>7</q1:SettingNumber>
  <q1:Type>Kerberos</q1:Type>
</q1:Account>
<q1:Account>
  <q1:Name>MaxServiceAge</q1:Name>
  <q1:SettingNumber>600</q1:SettingNumber>
  <q1:Type>Kerberos</q1:Type>
</q1:Account>
<q1:Account>
  <q1:Name>MaxTicketAge</q1:Name>
  <q1:SettingNumber>10</q1:SettingNumber>
+ <q1:SettingNumber>99999</q1:SettingNumber>
  <q1:Type>Kerberos</q1:Type>
</q1:Account>
<q1:Account>
  <q1:Name>TicketValidateClient</q1:Name>
  <q1:SettingBoolean>true</q1:SettingBoolean>
  <q1:Type>Kerberos</q1:Type>
</q1:Account>
<q1:SecurityOptions>
  <q1:KeyName>MACHINE\System\CurrentControlSet\Control\Lsa\NoLmHash</q1:KeyName>
  <q1:SettingNumber>1</q1:SettingNumber>
+ <q1:SettingNumber>0</q1:SettingNumber>

```

アラートと対応



準リアルタイムのアラート生成：不審なイベントが検知されると、詳細なコンテキスト（関係者のアイデンティティ、タイムスタンプ、影響を受けたリソース、推奨される対応アクションなど）を含んだアラートがトリガーされます。



ITSMプラットフォームとの連携：脅威やセキュリティ違反が検知されると、自動的にITSMプラットフォーム上で調査チケットの発行がトリガーされます。Rubrikは、ServiceNow ITSMとのAPIレベルの連携機能を標準で備えています。



Webhook連携：Webhookを使用してSIEMツールやSOARツールにアラートやイベントを送信することができ、これらのツール上で、さらなるトリアージや修復のためのワークフローを自動的にトリガーできます。

アイデンティティプロバイダの復旧

Identity Resilienceは、リスクの低減や不審な活動の検知を通じて脅威アクターによる損害行為を防止することに重点を置いています。これを実現するためには、「侵害の発生を前提とした考え方」に基づく堅牢な戦略が必要であることは明らかです。Identity Resilienceに含まれるRubrik Identity Recoveryは、Active DirectoryとEntra IDの復旧を実現する包括的な機能を備えており、ハイブリッド構成にも対応しています。このような戦略的アプローチを取れば、アイデンティティ攻撃の対象領域をプロアクティブに管理してリスクを最小化しつつ、攻撃者によって重要なインフラコンポーネント（Active DirectoryとEntra ID）が侵害・破壊された場合でも復旧できる能力を確保することができます。

ソリューションのアーキテクチャと導入における考慮事項



セキュリティとコンプライアンス

- さらに、粒度の高いロールベースアクセス制御を活用することで、IAMチームとGRCチームにはIdentity Resilience関連の機能のみにアクセスを許可し、Rubrikの他の機能へのアクセスを不許可とすることが可能です。逆に、バックアップ管理者にはIdentity Resilience関連の機能へのアクセスを不許可とすることもできます。
- 認証済みでコンプライアンスに準拠したプラットフォームとサポートチーム。Rubrik Security Cloudにおけるコンプライアンスの詳細については、<https://www.rubrik.com/compliance-program>をご覧ください。

- 保存期間中と転送時のデータの暗号化が強制的に実行され、加えて管理者に対しては厳格なロールベースアクセス制御（RBAC）が適用されます。
- バックアップデータはプラットフォームに書き込まれた時点で書き換え不可となり、復旧の確実性が保証されます。



ハイブリッド環境のサポート

- Rubrik Backup Serviceは、ドメインコントローラーにデプロイされ、機密性の高いログイン認証情報を開示することも、大規模なネットワーク変更を行う必要もなく、Active Directoryデータを収集します（また、必要に応じてActive Directoryバックアップを取得します）。
- Active Directoryのイベントデータはデータセンター内のクラスタ上で処理され、メタデータのみがRubrik Security Cloudに送信され、追加の処理が行われます。
- Entra IDの場合、1回の管理者ログインでオンボーディングが完了し、必要最小限の権限を持つサービスプリンシパル（エンタープライズアプリケーション）が自動的に作成されます。
- セキュリティポリシーの定義とアラートは、データの保存場所を問わず統一されているため、オンプレミス、ハイブリッド、マルチクラウドの各環境を横断してガバナンスがシンプル化されます。
- Active Directoryの復旧は複数のクラスタ間でオーケストレーションされるため、ローカルでバックアップを取得することと、単一のUIで復旧操作を実行することが両立可能です。



シンプルでグローバルなコントロールプレーン

- 受賞歴もある使いやすいインターフェースにより、アイデンティティとデータのセキュリティ態勢管理や、データとアイデンティティの保護・復旧を簡単に実行可能。
- 攻撃が成功した場合でも、アイデンティティからデータに至るまで重要サービスの全体にわたって、エンドツーエンドかつオーケストレーションされた復旧を実現。
- 世界中で4,000を超える顧客に信頼されている、アイデンティティサービスを保護するエンタープライズグレードのサイバーレジリエンス。

ソリューションのパッケージ構成

Rubrikは、何年にもわたって顧客のアイデンティティ保護に取り組んでおり、すでに4,000社を超える企業からアイデンティティサービスのための支援者として信頼を勝ち得ています。以下の図は、Identity Resilienceを含め、Rubrikのポートフォリオに含まれる各ソリューションが提供する機能の概要を示しています。

	Rubrik Foundation/ Business/ Enterprise Edition	Rubrik Identity Recovery	Rubrik Identity Resilience (Identity Recoveryを含む)
Active Directoryのユーザー、グループ、ドメインコントローラーの保護と復旧	✓	✓	✓
Entra IDのユーザー、グループ、ロールの保護と復旧	✓	✓	✓
Active DirectoryとEntra IDのオブジェクトに対する粒度の高い復旧	✓	✓	✓
Active Directoryフォレストのオーケストレーションされた完全復旧		✓	✓
Active Directoryのオブジェクト属性の比較と復旧		✓	✓
Active DirectoryとEntraのハイブリッド環境におけるハイブリッド型の復旧ワークフロー		✓	✓
すべてのIdPIにわたる人間および非人間のアイデンティティに関するアイデンティティインベントリの一元化			✓
IdPとアイデンティティ設定におけるリスクをポリシーベースで検出			✓
検出されたリスクのアプリ内修復			✓
改ざん防止機能を備えた監視による、重要な変更や不審な活動についての準リアルタイムアラート			✓

要約

Identity Resilienceは、包括的かつポリシーベースのエンジンと、堅牢で改ざん防止機能を備えたイベント監視技術を組み合わせ、Microsoft Active Directory環境およびEntra ID環境におけるエンタープライズアイデンティティを多層的に保護します。

Identity Resilienceは、設定のコンプライアンス状況を継続的に検証し、異常な活動を準リアルタイムで検知し、実用的なインサイトとアプリ内修復機能を提供することで、組織がアイデンティティリスクをプロアクティブに管理し、最も重要な攻撃対象領域を保護し、事業運営のレジリエンスを確保できるよう支援します。



Global HQ

3495 Deer Creek Road
Palo Alto, CA 94304
United States

1-844-4RUBRIK
inquiries@rubrik.com
www.rubrik.com

Rubrik (NYSE : RBRK) は、世界中のデータの安全確保を使命としています。弊社はZero Trust Data Security™を使用して、サイバー攻撃、悪意ある内部関係者、運用上の影響に対するビジネスレジリエンスを組織が実現できるよう支援します。機械学習を活用したRubrik Security Cloudは、オンプレミス、クラウド、SaaSアプリケーションに分散するデータを横断的に保護します。Rubrikは、データ完全性の維持、厳しい状況におけるデータ可用性の確保、データのリスクと脅威の常時監視、インフラが攻撃を受けた場合のデータによるビジネスの復旧など、さまざまな局面で組織をサポートします。

詳しくは、www.rubrik.comをご覧ください。また、X (旧Twitter) で@rubrikIncをフォローいただくか、LinkedInの場合はRubrikをフォローしてください。RubrikはRubrik, Inc.の登録商標です。本文書に記載されているすべての会社名、製品名、およびその他の名称は各社の登録商標または商標です。

brf-rubrik-identity-resilience-Rubrik-ja-JP / 20251211