データ セグメンテーション

データ セグメンテーションは、大規模で複雑な組織に対し、社内のセキュリティ、パートナーのエンタイトルメント、最小権限の適用に対応するレコード レベルのアクセス制御を可能にする SailPoint の機能です。この機能では、SailPoint Identity Security Cloud のコア オブジェクト（アクセス モデル、アイデンティティ、ソースなど）内にあるデータを制限するための手段を提供します。このデータ セグメンテーション機能により、権限が付与されたデータ レコードのみをユーザーに閲覧させることが可能になります。たとえば、サブ管理者には閲覧が許可されている管理用 UI とエンタイトルメント API のエンタイトルメントのみを表示させる、などの制御ができます。エンタイトルメント管理はこのプラットフォームにおける最初のオブジェクトですが、今後はすべてのユーザーを対象とした機能の追加をプラットフォーム全体に進めていく予定です。

機能

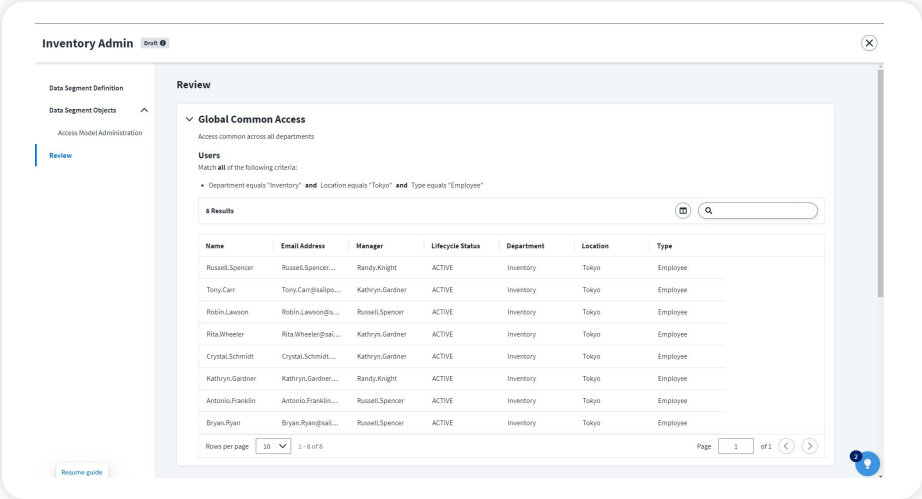
- **最小権限の適用：** ユーザーには、ロール（権限の集合）に合わせて付与されるべきアイデンティティ、ロール、アクセス プロファイル、エンタイトルメント、および申請可能な項目のレコードのみにアクセスできる権限を付与します。
- **管理の委任：** 適切なレコードのみを表示できるようにすることで、SailPoint Identity Security Cloud の実装に向けた構築と維持を、アクセス権限管理に最も適切なチームに委ねることができます。
- **プライバシー：** 個人ユーザーを持つお客様は、社内のプライバシー ポリシーや規制に対応するため、ユーザーや管理者が他のユーザーのアイデンティティ レコードを一切閲覧できないようにすることができます。

利点

- **プラットフォームのセキュリティ向上：** レコードレベルで最小権限を適用することでセキュリティを強化し、適切なユーザーのみが適切なレコードとデータにアクセスできるようにします
- **オーナーシップの拡大/運用コストの分担：** エンタイトルメントの管理と維持（将来的にはさらに多くの機能が追加される予定）を行う際に、それまで集中管理していた1つのチームに頼ることが少なくなります
- **コスト削減：** 極めて複雑な組織で、データ セグメンテーションが要求される組織（子会社が複数あり、各組織間のデータに強力なファイアウォールを必要としている組織など）であっても必要なテナントは1つのみです

一般的なユース ケース

- 管理者は、重要な管理オブジェクト（アクセス モデル、アイデンティティ、アイデンティティ プロファイル、ソース）内にある、特定のレコードに対する特定のユーザーによるアクセスを制限するセキュリティ ポリシーを簡単に作成でき、アイデンティティ アクセス権限管理（IAM）の運用を社内でアウトソースできます。
- IAM チームは、多くの管理業務をローカル部門のエキスパート、ヘルプデスク、IT チームに委任できます。
- たとえば、複数の銀行で構成されているコンソーシアム銀行では、A 銀行の管理者には A 銀行に関連するデータのみを表示するといった運用が可能になります。



SailPoint

SailPointについて

SailPointは、現代の企業がアイデンティティという視点から、アプリケーションやデータへのアクセス権限を迅速かつ大規模でシームレスに管理・保護することを支援します。当社は、この分野を先導する企業として、セキュアな企業の基盤としてのアイデンティティ　セキュリティを今後も改良し続けていきます。SailPointは、今日の動的でアイデンティティを標的にしたサイバー脅威を防御する目的で構築した、インテリジェントで拡張性の高い統合プラットフォームを提供すると同時に、企業の生産性と効率性も向上させます。SailPointは、世界で最も複雑かつ高度な企業の多くが、ビジネスの変革を推進するセキュアなテクノロジー エコシステムを構築できるよう支援します。