データシート

Identity Manager

企業のIDおよびアクセス管理のリスクを軽減

メリット

- リクエストからユーザおよびデータ用の作業完遂まで、オンプレミス、クラウド、ハイブリッドリソースのアクセスを管理
- ユーザに必要なアクセスのみを確実に与えることでリスクを低減
- アテステーションおよび再認証ポリシーにより、監査とコンプライアンスで先手を打つことが可能
- ビジネス内部で帰属するアクセス権の決定が可能
- 既存の資産やインフラストラクチャを活かした拡張が可能

概要

従来のIDおよびアクセス管理（IAM）フレームワークは、構築のコストがかかり、導入やメンテナンスに時間がかかっていました。こうした管理はほとんどのIT部門で大きな負荷となっています。これは、すべてのユーザIDのライフサイクル管理をIT部門で取り扱っていることが多いためです。さまざまなビジネスユニットでの多様なIAMニーズに応えるために、IT部門では対象範囲の限られたツールやセキュリティポリシーを個別に適用して作業し、ポリシーの強制を手動のプロセスに頼ることが珍しくありません。こうした状況はビジネス環境を脆弱にし、リスクを増大させるばかりか、SLA（サービス・レベル・アグリーメント）の順守も困難にします。

ユーザのアクセス権を、業務に必要なデータやアプリケーションのみに限定することで、生産性を高められます。

必要なデータやアプリケーションへのアクセス権のみをユーザに与えることで、リスクの軽減、データの保護、アップタイム要件への適合、コンプライアンスの準拠を実現できます。これにより、IDおよびアクセス管理（IAM）を、IT部門の能力ではなく、ビジネスニーズに基づいて行うことが可能になります。Identity Managerにより、現在、そして今後長きにわたってセキュリティポリシーを統一し、ガバナンスのニーズを満たすことができます。

それと同時に、モジュラー式でスケーラブルなIAMソリューションにより、現在および将来にわたり、ビジネスの俊敏性を改善できます。

リスクの軽減、アクセスの管理、IDの管理、データの保護。

IDおよびアクセス管理（IAM）がついに、ビジネスニーズに基づくものになります。

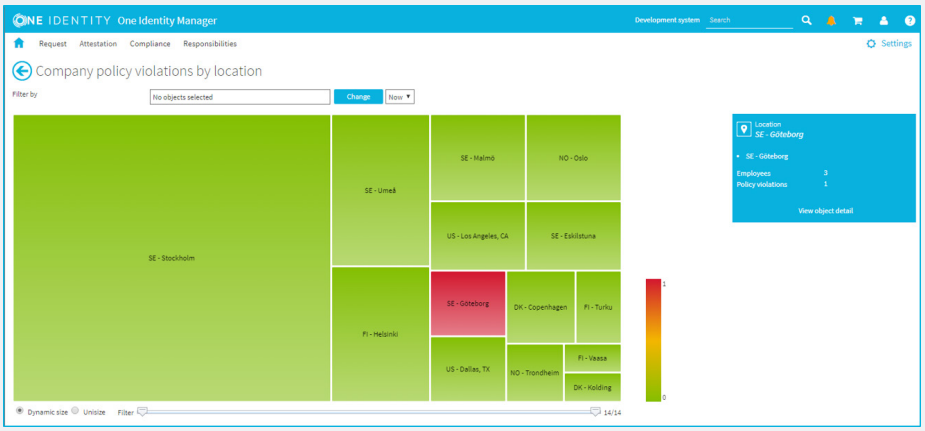

図1. *Governance Heatmapにより、ポリシー違反の素早いドリルダウンが可能になります。*

特長

SAP認定

高精度の機能を持つ、認定済の高度なSAP統合を提供し、既存のSAPセキュリティモデルを拡張します。さらに改善することも可能です。

リスクの軽減

複数のソースから得たセキュリティに関する情報とポリシーを集約して、より的確にセキュリティ上の判断を下すことで、リスクを減らし、情報のサイロ化を防ぎます。

クラウド

クラウドベースのアドオンやマネージドサービス製品により、オンプレミスのアプリケーションからハイブリッドおよびSaaSアプリケーションに至るまで、IDガバナンス資産を拡張します。

360度のガバナンス

監査役にリアルタイムで提供される詳細なガバナンスレポートには、環境内にどのようなリソースがあり、それにアクセスできるのは誰か、いつ、どのような理由でそのアクセス権が付与/剥奪されたのか、などが詳しく記載されます。

適切なプロビジョニング

あらゆるシステム、プラットフォーム、オンプレミスまたはクラウドのアプリケーションのプロビジョニングを自動化して、手動によるミスを排除します。プロビジョニングを、Exchange Online、SharePoint、Oracle E-Business Suiteなどのエンタープライズアプリケーションに拡張します。

適切なアクセス

セキュリティ強化のため、従業員、請負業者、パートナー、顧客、学生、卒業生、関係者、患者などに対して、本当に必要なアクセス権のみを付与します。

コンプライアンスの重要性

外部の規制が心配ですか? 心配はご無用です。社内ポリシーが問題ですか? 心配はご無用です。さまざまなグループの要望を満たしつつ、求められる可視化を完全な形で実現できます。

データのガバナンス

データを管理し、可視化を行いましょう。

セルフサービス型のアクセスポータル

ビジネスの時間を節約し、自分で対応することが可能です。カスタマイズ可能なオンラインの「ショッピングカート」ポータルは、直感的に使用することができるため、IT部門の労力を削減できます。これにより、ユーザは定義済みの承認プロセスおよびワークフローで、物理資産、グループ、配布リストなどのセキュリティ資産へのアクセスを申請し、IDのライフサイクル全体にわたってアクセス権や権限を制御できます。

特権アクセス管理

ガバナンスが統一され、ユーザは、同じコンソール内で、特権ユーザと一般ユーザのアクセス権に対するリクエスト、プロビジョニング、アテステーションを行えます。

Attestation Reviewダッシュボード

アテステーションのスケジュールを設定し（オンデマンドまたは定期的）、グループおよび配布リストのステータスを簡潔で分かりやすいダッシュボードビューに表示します。また、検出に関する詳細なレポートの作成や、コンプライアンスの準拠も可能です。

パスワードの再設定

ユーザアカウントのパスワードをリセットし、組織のパスワード規定や要件を反映したユーザポリシー設定を行います。ユーザロールに合わせ、複数のパスワードポリシーを設定できます。

複数段階認証

Identity Managerにより、エンタープライズアプリケーション全体の統合展開を行い、One Identity Starling Two-Factor Authentication（2FA）と統合することで、二要素認証を有効化します。

スケールアップおよびスケールアウト

既存の資産やインフラストラクチャを活かして、拡張することができます。

システム要件

システム要件の完全なリストについては、こちらを参照してください。https://support.oneidentity.com/identity-manager/8.1

One Identityについて

One Identityは、組織のIDおよびアクセス管理（IAM）の権利取得を支援します。IDガバナンス、アクセス管理、特権管理、サービスとしてのアイデンティティソリューションのポートフォリオなど、当社製品の独自のコンビネーションにより、組織はセキュリティ問題に悩まされることなく脅威から身を守り、そのポテンシャルを最大限に発揮することができます。OneIdentity.comで詳細をご確認ください。