あらゆるアイデンティティ脅威を把握し、リアルタイムで対応する方法

最新のアイデンティティファーストのセキュリティ戦略を採用

ビジネスが成長し、変化するとき、リスクプロファイルも増加します。

俊敏な対応力とリモートでのコラボレーションを実現するために、貴社のような競争力のある企業は、優れたソリューション群を連携させたエコシステムを活用しています。こうして綿密に構築された技術スタックは、組織全体でより良い成果をもたらします。ただし、それらは貴社にリスクをもたらす可能性もあります。

ビジネスが変化し成長する中で、ITチームやセキュリティチームはしばしば調整に苦しみ、対応しきれない状況に陥ります。これにより、**断片化されたIT環境**が生まれ、重要なリソースやアイデンティティが複数のシステムやインフラに散在するようになります。

その結果、組織のセキュリティ態勢が見えにくくなり、コストのかかる侵害のリスクが高まります。

攻撃者にとって第1の攻撃手段となったアイデンティティ

データ侵害の**80%**は、認証情報の盗難やフィッシング攻撃から始まっています

アイデンティティ関連の攻撃は、**前年比180%**の割合で増加しています

Verizon 2024年版データ侵害レポート

統合アイデンティティセキュリティによる可視性の向上

断片化したテクノロジーとセキュリティスタックは、リスクと潜在的な脅威にさらされた膨大なデータを生成します。チームはログをふるいにかけ、本当に注意すべき点についての共通認識を見付ける必要があるため、リアルタイムの修復はほぼ不可能になります。

つまり、アイデンティティの断片化により、貴社の最大の脆弱性がどこにあるかを特定できなくなるのです。脅威検知と対応が遅くなり、盗んだ認証情報を使用して大規模な損害をもたらす機会を攻撃者に与えてしまいます。また、日々巧妙化する脅威情勢において、組織と顧客に制御不能なリスクを負わせます。

このリスクを効果的に管理するには、アイデンティティシステムとプロセスを単一のプラットフォームに統合して、効率と制御を向上させる必要があります。最新のアイデンティティプラットフォームがセキュリティに対する統合アプローチを可能にします。

Oktaで重要な成果を実現

Okta Platformは、アイデンティティ優先のセキュリティに対して、堅固で大幅に簡略化されたアプローチを可能にします。Oktaは、さまざまな製品と機能を通じて、ワークフローやカスタマーエクスペリエンスに過度の負担をかけることなく、巧妙な脅威からの保護をエンドツーエンドかつリアルタイムで提供します。

あらゆるアイデンティティ脅威への完全な可視性を実現する（およびリアルタイムの修復を可能にする）方法

効果的なリスクの修復は、リスクプロファイルを一元的に表示して、セキュリティシグナルをリアルタイムで実行可能なインサイトに統合することから始まります。顧客アイデンティティ管理においては、アカウント乗っ取り、不正行為、および認証情報の漏洩を迅速に検出および対応できるようにすることで、機密データの保護を実現します。

また、リスクの修復を緩慢な手作業に任せることはできません。アイデンティティソリューションは、リアルタイムで得たインサイトを、特定のビジネスニーズに応えて調整できる、自動化された修復ワークフローへと結びつける必要があります。

これは、アイデンティティセキュリティの統一により可能になります。フィッシング対策を最新のアイデンティティファースト型のリスクエンジンと統合することで、新たな脅威をリアルタイムで可視化できます。従業員であれ顧客であれ、誰を守るにしても、今日の脅威情勢ではこのレベルの保護が欠かせません—そして、それを実現できるのは、アイデンティティを統合したアプローチだけです。

Oktaでできること

Oktaはアイデンティティオーケストレーションを一元化することで、IT、セキュリティ、そして顧客環境全体にわたるシグナルやポリシーの可視性を新たなレベルで実現し、強力なリアルタイムの脅威検知と対応能力をチームに提供します。

Okta AIを活用した Identity Threat Protection

- すべてのシステム、デバイス、ユーザータイプにわたる脅威をリアルタイムで可視化し、積極的なセキュリティ態勢を確保
- Oktaからのファーストパーティデータと共にサードパーティのシグナルも活用し、より深い洞察を得て、素早く脅威を検知
- MFAのトリガーや侵害されたユーザーのログアウトといった、カスタマイズ可能な自動アクションで、脅威のダメージを迅速に緩和

Okta FastPass

- パスワードレスでフィッシング耐性のある認証を有効にして、シームレスかつ安全なユーザーエクスペリエンスを提供
- 認証時にデバイスのセキュリティ態勢を検証し、コンプライアンスを強制
- ユーザーと管理者にフィッシング試行を警告し、攻撃をログに記録して可視化を促進
- 認証プロセスが悪用される前に、信頼できないアプリをブロック

アプリの安全な導入

- （従業員や顧客を問わず）新しいユーザーが、初日から重要なアプリやリソースに適切な権限でアクセスできるようにする
- 一元化された単一プラットフォームから、エンドユーザーアクセスに変更を追加
- 人事ソフトウェアやディレクトリと統合して従業員情報と許可を一元管理し、顧客アイデンティティシステムと連携させて顧客アカウントを大規模に管理および保護
- 従業員が退職した際にアクセス権を自動的に削除することで、セキュリティを強化し、コストを削減
- 顧客アカウントをシームレスに管理し、顧客のアクティビティや趣向に基づいて安全かつ最新のアクセスを確保

Identity Security Posture Management

- 継続的な監視とAIを活用した分析を通じてアイデンティティプロバイダー、SaaS、およびクラウドインフラストラクチャ全体で隠れたアイデンティティリスクを検出し、優先順位を付ける
- MFAバイパス、管理者権限の過剰付与、退職したがまだアクセス権が残っているユーザー、非人間アイデンティティ（NHI）リスクなど、重大な脆弱性を悪用される前に特定することで、攻撃対象領域を積極的に縮小
- NIST、CIS、ISO、PCI-DSSなどのフレームワークを活用し、継続的かつ自動化された制御策の監視と報告を行うことで、コンプライアンス検証を簡素化
- システム間で統合されたアイデンティティコンテキストを提供し、複雑なアイデンティティ関係をグラフを用いて可視化することで、セキュリティチームの生産性を向上させ、チームが最小限の時間投資でセキュリティ態勢を理解し、管理できるようにする

可視性の力を手に入れましょう

脅威がますます巧妙化するリスク環境において、安全でレジリエントな組織を実現するための最も確実なアプローチは、一元化されたアイデンティティファーストセキュリティです。

ただし、より強固なセキュリティを実現するためには、セキュリティエコシステムを弱体化させ、リスクが隙間から漏れ出す原因となるアイデンティティの断片化を排除する必要があります。

セキュリティ戦略を最新のアイデンティティソリューションに統合する方法の詳細は、当社チームにお問い合わせいただき、Okta Platformの動作をご覧ください。