電子書籍

統合アイデンティティのパワーと可能性の解放

組織にとっての5大成果

okta

アイデンティティの重要な役割

アイデンティティは最新セキュリティのキーポイントです。現在のクラウドベースの世界では、システムとアプリケーションが深く結びついており、アイデンティティによって組織の機密データの安全性または脆弱性が決定します。

攻撃者はすでにアイデンティティが主要なターゲットであることを認識していますが、どの業界でも多くの場合、企業は不意に被害を受けています。アイデンティティ関連の攻撃は前年比で180%増加していますが、1つの組織が侵害を封じ込めるのにかかる平均日数は290日です（ベライゾン2024年度データ漏洩/侵害調査報告書）。

問題の核心は、テクノロジーとセキュリティシステムにわたって、アイデンティティが断片化していることです。アイデンティティセキュリティに対して統合アプローチがなければ、組織のリスク軽減に向けた取り組みは弱体化し、ITチームとセキュリティチームは、現在の複雑な脅威に対処しきれない非効率的なツールしかないため負担が増えてしまいます。

組織は、軌道修正に向けて、アイデンティティに焦点を置いた統合的なセキュリティ戦略を立てなければなりません。この戦略では、ITシステムとセキュリティシステム全体のリスクを検出し、リアルタイムで修復し、一元化されたIdentity Governanceとセキュリティオーケストレーションを通じて将来の攻撃を防ぐ必要があります。

将来に備えたアイデンティティへのガイド

本ガイドでは、組織がセキュリティ戦略に焦点を置いた統合アイデンティティを構築する方法について、以下のトピックで説明します。

- 断片化したアイデンティティによってリスク解消が困難になる仕組み
- 現代の企業がアイデンティティ優先のセキュリティアプローチを必要とする理由
- 統合セキュリティ戦略の5大成果

アイデンティティ優先から始まる適切なセキュリティ対策

今日におけるビジネスの運用方法は、5年前とは劇的に変化しています。ハイブリッドな労働力が意味するのは、現在では生産性が、主要なリソースとネットワークに世界中からアクセスする正社員、契約社員、顧客、社外パートナーの分散されたネットワークへのシームレスな接続にかかっているということです。クラウドサービスやSaaSアプリケーションの導入が加速することで、このような接続が促進され、連携、協働、安全なカスタマーエクスペリエンスの実現がよりフレキシブルな方法で容易になります。

しかし、このような働き方の大幅なシフトは、ビジネスと顧客の安全性を守る方法も根本的に変えてしまいます。レガシーのセキュリティパラダイムは、ネットワーク境界やオンプレミスの導入に伴い展開する傾向がありますが、クラウドネイティブのアプリケーションやリモートコラボレーションの時代に向けた設計ではありません。セキュリティ対策の専門家が何年も主張してきたように、セキュリティ境界という従来のコンセプトはもう通用しないのです。

適切なアイデンティティ対策は、誰が何にどこからどのような条件でアクセスしているかを明確に可視化し、セキュリティとシームレスなエクスペリエンスの両方を確保するうえで非常に重要になります。現代のゼロトラストに対する理解に、信頼済みデバイスや信頼済みネットワークというコンセプトはもはや適用されません。組織は、分散したハイブリッド労働力がどのデバイスからでも、どのネットワークからでも、場所を問わず接続できるようにすると同時に、顧客にはシームレスかつ円滑なインタラクションで安全にサービスにアクセスできる方法を提供しなければなりません。

攻撃者は、アイデンティティがサイバーセキュリティにおける新たな戦場であることを知っています。アイデンティティ関連の攻撃は現在、機密情報への不正アクセスを取得する主要な方法です。2024年には、データ侵害のなんと80%が認証情報の盗難やフィッシング攻撃から始まりました（ベライゾン2024年度データ漏洩/侵害調査報告書）。

アイデンティティは現代のセキュリティの核になっています。組織がゼロトラストレベルの脅威保護を達成し、シームレスなコラボレーション、安全なカスタマーエクスペリエンス、および生産性を実現するには、アイデンティティセキュリティに対して完全で統合的なアプローチに全力で取り組まなければなりません。

アイデンティティを競合優位性に昇華

組織にとってアイデンティティは最大のセキュリティリスクですが、最高の機会でもあります。アイデンティティの中心的な役割を理解し、顧客のIDを含めアイデンティティを活用した機能を最新化することで、リスクを軽減したり、攻撃者を撃退したりして、鍵となる利点を手に入れられます。強力なアイデンティティ戦略はより迅速な接続とさらに素早いコラボレーションを可能にします。また、シームレスなコンプライアンスやセキュリティ上の成果改善も実現します。

断片化したアイデンティティが生み出す危険な盲点

私たちの働き方は大きく変わり、スピードと俊敏性を何よりも優先する、より分散した生産性とコラボレーションへと移行しています。これにより、ほぼすべての業界でセキュリティと技術スタックの構成や構造も根本から変わりました。1社から1つのエンタープライズライセンス契約（ELA）ですべてのスタックを購入する時代は終わったのです。現在、成功している組織は、ターゲットとするビジネス、セキュリティ、カスタマーエクスペリエンスのニーズをサポートするベストオブブリード型ソリューションのエコシステムに依存しています。つまり、このような組織が成長し、自社を保護し、顧客にシームレスで安全なインタラクションを提供する能力は、かかるソリューションに接続し、**その価値を最大限に活かすことにかかっているのです。**

とはいえ、ベストオブブリード型アプローチによって技術スタックは肥大し続けており、ITチームとセキュリティチームは適応と維持に苦労しています。その結果、IT環境が断片化し、核となるリソースやアイデンティティがさまざまなシステムとインフラストラクチャに分散してしまうことが非常によく起こります。

断片化したアイデンティティの弊害

- 組織のリアルタイムのセキュリティ態勢や、各種システムやアプリケーションにおける個々の許可を十分に把握できない
- 対応が遅れることで、攻撃者がアイデンティティ関連の脆弱性を悪用できるようになり、高コストで深刻な侵害へと発展する可能性がある
- ユーザー許可設定の手順は煩雑で時間がかかるため、重要なアクセスの判断で人的なミスが起きやすい

okta

統合アイデンティティセキュリティの事例

手短にまとめると、アイデンティティの断片化は、セキュリティを根本から損ないます。可視性が妨げられるため、組織における最大の脆弱性がどこにあるかを特定できなくなるからです。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。

このような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で統合して、効率と制御を向上させる必要があります。クラウドネイティブの世界では、**アイデンティティこそがセキュリティ**であり、それ相応に扱われるべきです。アイデンティティはセキュリティ戦略の中心であり、断片的な後付けであってはなりません。統合されたアイデンティティレイヤーにより、ITチームとセキュリティチームは脅威を評価し、アクセスポリシーを適用して、疑わしいアクティビティに自動的に対応できます。

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。

アイデンティティ優先の統合セキュリティ戦略の成果

アイデンティティシステムとプロセスを統合する必要性に異論を唱える人はほとんどいないでしょう。ほとんどの組織にとって課題は、概念的な哲学から実行可能な戦略へと内容を落とし込むことです。

アイデンティティ優先の統合セキュリティ戦略は、一連の具体的な成果が組み合わさることで、重要な資産の保護、顧客のインタラクションでの安全性確保、日常業務の効率化、そしてあらゆるビジネス運用におけるパフォーマンス向上といった、測定可能な影響をもたらします。

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。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、巧妙な脅威からエンドツーエンドで保護します。統合型アイデンティティオーケストレーションでは、IT環境、セキュリティ環境、顧客環境の全体でシグナルとポリシーを新たなレベルで可視化し、潜在的なリスクをリアルタイムで阻止するための強力なオプションをチームに提供します。

成果1：アイデンティティ脅威の大幅な可視化とリアルタイムの修復

成果2：包括的で信頼性の高いゼロスタンディング特権と最小権限

成果3：実績のあるゼロトラスト

成果4：人間以外/マシンのアイデンティティに対するコントロールの強化

成果5：テクノロジーとセキュリティに対する投資の価値を最大化

成果1

アイデンティティ脅威の大幅な可視化とリアルタイムの修復

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。

より迅速かつ効果的なリスク修復は、アイデンティティリスクのプロファイルを一元的かつ包括的に把握することから始まります。このプロファイルは、セキュリティツール全体で生成されたすべてのシグナルを統合して優先順位を付け、リアルタイムで実行可能なインサイトの入手を可能にします。顧客のアイデンティティを管理している組織にとっては、アカウント乗っ取りや不正行為、認証情報の侵害をリアルタイムで検出して対処し、顧客からの信頼と機密情報の両方を保護することを意味します。

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。

統合アイデンティティセキュリティにより、これが可能になります。セキュリティスタックを最新のアイデンティティソリューションと統合することで、フィッシング対策をアイデンティティ優先の一元化リスクエンジンと統合し、アイデンティティの脅威が出現し進化するのをリアルタイムで包括的に把握できます。保護対象が従業員か顧客かにかかわらず、このレベルの可視性こそが現在の状況では必要とされており、それを実現するのが統合アイデンティティです。

Oktaでできること

Okta AIを活用した Identity Threat Protection

- システム、デバイス、ユーザータイプ全体を通して脅威をリアルタイムで可視化し、プロアクティブ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、不正アクセスを防止
- ログインセキュリティを改善して、異常なアクティビティをすぐに特定して対応
- 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

成果2

包括的で信頼性の高いゼロスタンディング特権と最小権限

組織全体を通して最小権限のアクセスを確立して適用することは、永遠に続く達成不可能な課題のように感じられます。特に断片化したアイデンティティスタックでは、手動での統合に大きく依存せざるを得ません。

最新のアイデンティティソリューションは、ジャストインタイムのアクセスを強制力のある現実にするためのツールと機能を提供します。Identity GovernanceとPrivileged Access Managementを統合することで、誰が何にアクセスできるかという可視性を一元化し、きわめてきめ細かくアクセスを制御できます。

また、統合アイデンティティセキュリティソリューションは、ガバナンス、特権アクセス管理、およびアイデンティティに関連したその他の機能を単一プラットフォームにまとめることにより、アイデンティティ管理を合理化します。この一元化により、一貫したアクセスポリシーを確保でき、組織の最重要データのセキュリティも強化されます。

Oktaでできること

Okta Identity Governance

- システムとアプリケーション全体のアクセスを一元的に把握し、制御と監視を強化
- ロールベースおよびグループベースのアクセスによりアクセス許可を合理化し、適切なユーザーが適切なアクセスを持つことを実現
- 新入社員が初日から適切なアクセスを持てるようにし、生産性を高めてリスクを削減
- ロール変更とプロビジョニング解除を自動化して、セキュリティを維持

Okta Privileged Access

- 安全なアクセスコントロールによって機密性の高い情報を保護
- 特定のユーザーやユースケースに合わせてアクセスプロトコルをカスタマイズ
- 特権付きアクティビティの可視性を高め、監査とリスク管理を改善
- ユーザーフレンドリーな統合でアクセス要求を簡素化し、セキュリティを損なうことなくワークフローを加速化

Okta Integration Network

Oktaのライブラリには7,000点を超える構築済み統合があり、技術スタックのほぼすべてのコンポーネントに対するアクセスを画面1つで把握できます。

Google Workspace slack salesforce HubSpot zoom

成果3

実績のあるゼロトラスト

以前、ほとんどの組織はゼロトラストの原則に取り組んでいましたが、現在ではゼロトラストのフレームワークで運用している組織はほぼありません。最小権限アクセスの適用のように、断片化したアイデンティティスタックでゼロトラストを実現するには、人間が維持できないペースで手動監視を行うという、ほぼ不可能な格闘が必要だからです。

アイデンティティ優先のセキュリティに対する統合アプローチは、組織がゼロトラスト運用を進めていることを（強い自信をもって）確証するための重要なポイントになります。最新のアイデンティティプラットフォームのもと技術スタックを統一すれば、その全体にわたってゼロトラスト原則に準拠すること、ひいては準拠していることを証明するのも容易になります。各アプリケーションと各システムにわたってすべてのユーザーに許可を手動で確認する必要はもうありません。統合アイデンティティがこの面倒（でエラーの発生しやすい）作業を自動分析に置き換え、リソースを抑えながらより高いレベルの信頼性と脅威保護を提供します。

Oktaでできること

Identity Security Posture Management

- ツールを自動スキャンし、統合されたゼロトラストフレームワークのセットに基づいて設定を評価
- 脆弱性やセキュリティの抜け穴を事前に特定し、悪用される前に対処
- MFA適用の不備やアカウントの無秩序な増加など、重大な構成ミスやセキュリティの抜け穴を継続的に監視
- ゼロトラスト原則に対する信頼と確信を、数日や数週間ではなく、わずか数分で獲得

成果4

人間以外/マシンのアイデンティティに対するコントロールの強化

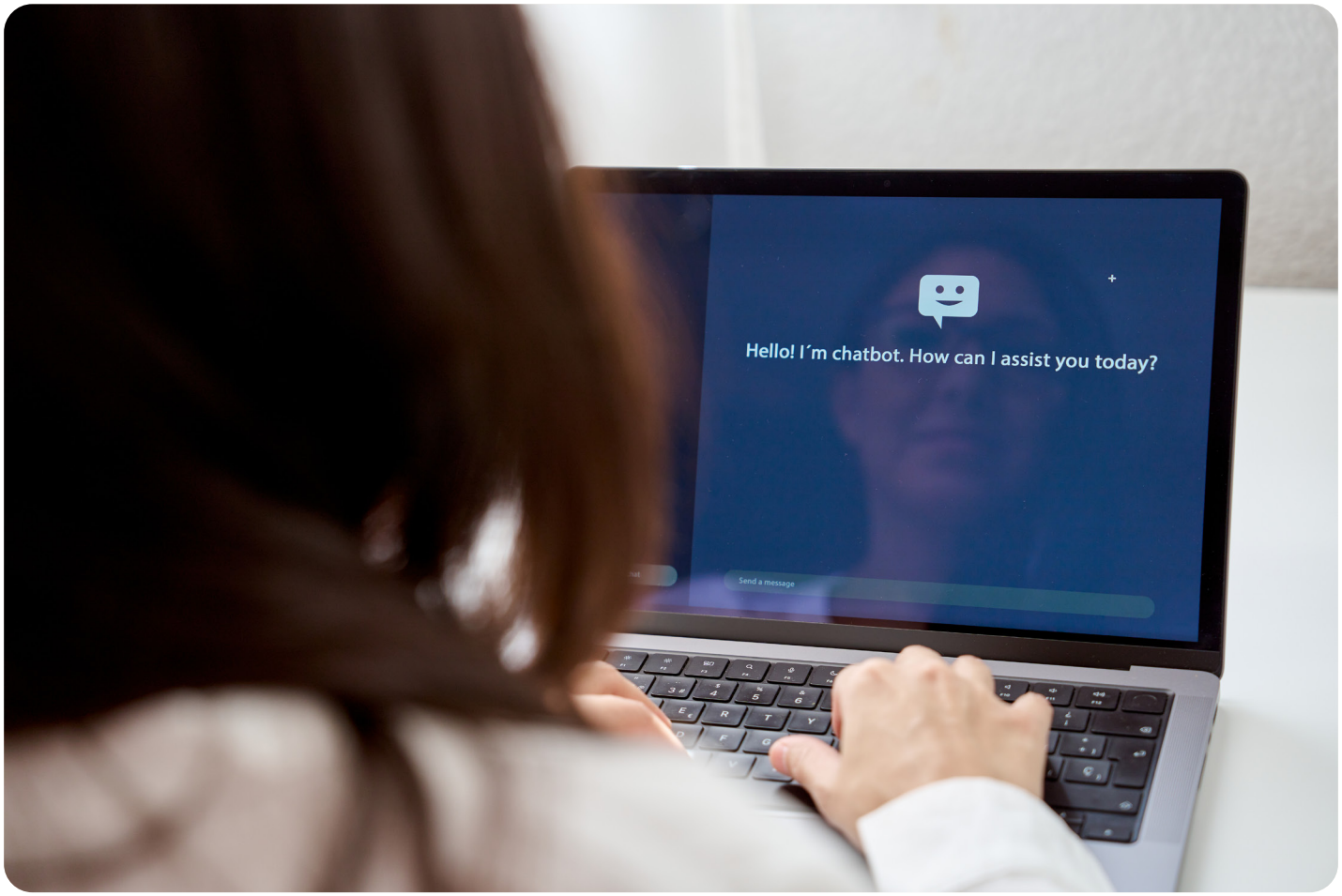
人間以外のアイデンティティ（例：機械、サービス、AIエージェントのアイデンティティ）は、コラボレーションやイノベーション、生産性全般に対してビジネスの中心的な能力を加速化させます。ただし、攻撃者が侵害の手がかりとする、急成長している無監視のベクトルにもなります。

統合アイデンティティは、技術ランドスケープ全体における人間以外のアイデンティティが、どこにいて何にアクセスできるかを表示して包括的な把握を提供することで、この盲点を解決します。この新たな可視性により、人間以外のアイデンティティについて認可を監視し、きめ細かい制御を使用して主要なリソースへのアクセスを管理します。また、最小権限アクセスの原則に基づいて構築された、まさしく包括的なアイデンティティセキュリティ戦略に組み込むこともできます。

Oktaでできること

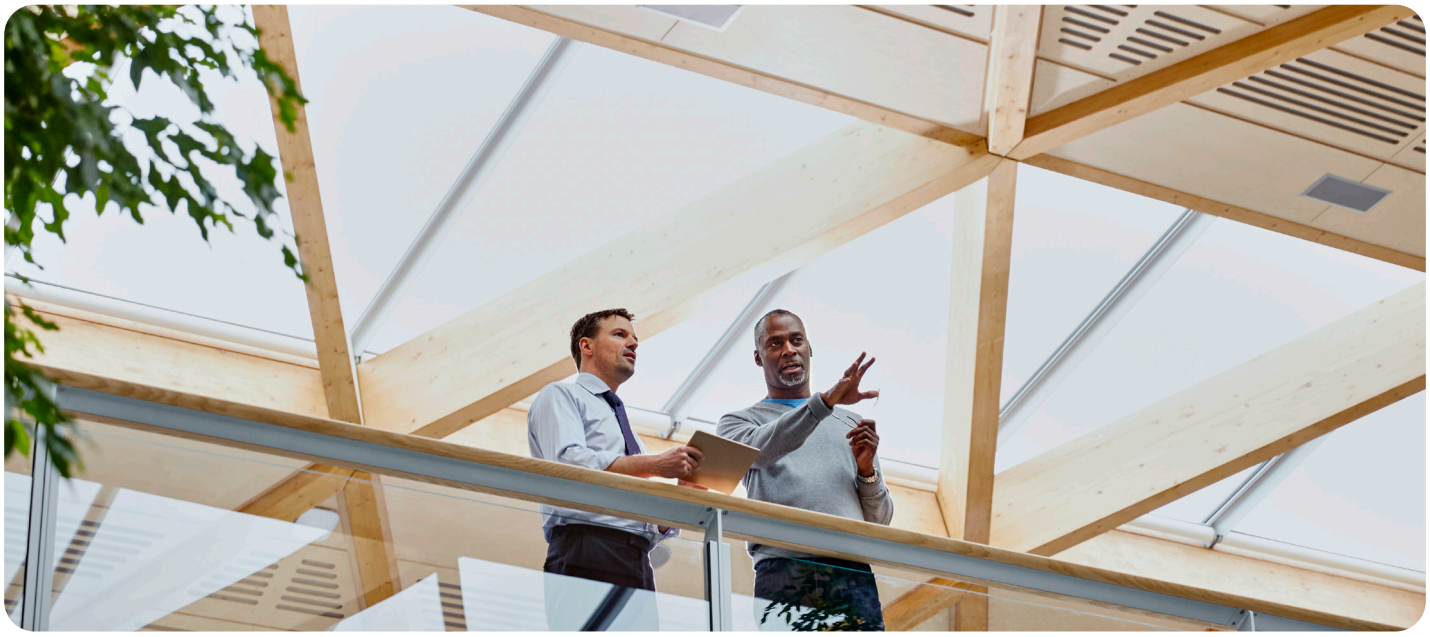
Identity Security Posture Management

- 人間以外のアイデンティティを検出し、いつ何にアクセスできるかを一元的に把握
- 人間以外のアイデンティティによりきめ細かい許可設定をして攻撃対象領域を縮小



成果5

テクノロジーとセキュリティに対する投資の価値を最大化



技術スタックの相互接続性は、テクノロジーへの投資がビジネス価値を生み出す場です。技術スタックのあらゆる部分が幅広くシームレスに統合されていなければ、テクノロジーやセキュリティへの投資から最大限に価値を引き出せません。

これは、特にセキュリティツールに当てはまります。各ソリューションは豊富なデータとシグナルを生成しますが、シグナルがサイロ化されたままでは、機密性の高い内部システムを保護し、安全なカスタマーエクスペリエンスを提供するために今日求められている、堅牢かつ素早い脅威対策や準備を行えません。

アイデンティティ優先の統合セキュリティ戦略は、これらのシグナルを一元化されたプラットフォームに接続することで、拡張されたセキュリティスタックと技術スタックの可能性を最大限に引き出します。このプラットフォームでは、セキュリティ態勢を継続的に評価し、アプリケーションやシステム間のアクセスを管理し、顧客のアイデンティティを保護して、自動修復戦略を決定します。

成功事例

HubSpot
現在ではアクセス要求チケットの80%が自動化によって解決

Delivery Hero
停止を排除することで28,800時間分の生産性を獲得

TakedaID
Oktaを利用することで、社内ソリューションよりも5倍速くアイデンティティを導入

現在のニーズと将来の目標に向けた、アイデンティティを活用したソリューション

ここまで述べてきた5つの成果は、組織のセキュリティハンドブック向けの単に耳当たりが良いフレーズではなく、組織のセキュリティと成功を左右する決定要因です。ますます巧妙化する脅威とAIを活用した新しい攻撃方法によって定義されるリスク状況において、レジリエンスがある安全な組織の未来に向けた最も確実なアプローチは、セキュリティに対してアイデンティティ優先の統合アプローチを採用することです。

その理由は、アイデンティティこそがセキュリティだからです。組織での安全維持に向けたあらゆる最新ストラテジーの核になります。しかし、このセキュリティ向上の約束を果たすには、リスク（およびビジネス価値）が抜け穴をかいくぐる原因となる、アイデンティティの断片化を排除する必要があります。今日の状況において、アイデンティティ優先の統合セキュリティは、加速化する脅威にビジネスが先手を打つ助けになるだけでなく、競争力を維持するために必要なシームレスで摩擦のないIT環境もサポートします。

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。

okta

Okta Inc.
100 First Street
San Francisco, CA 94105
info@okta.com
1-888-722-7871