ホワイトペーパー

CIAMは、セキュリティと顧客体験(CX)のバランス改善を支援

セキュリティの目標は変化し続けています。強力なCIAMソリューションがあれば、貴社のニーズと顧客ニーズの最適なバランスを実現します。

玄関の鍵をかけ忘れていませんか？

私たちの生活では日々、色々なことが起こっています。コーヒーを飲みながら、子供の世話をして、外出用のバッグを準備する一方で、後についてくる猫の相手をしなければならない場合もあるでしょう。このような忙しさの中で、例えば玄関の鍵をかけるといった基本的な動作を忘れてしまう場合もよくあります。このように、生活は速いスピードで進みます。

仕事においても同様に、速いスピードで進みます。仕事に集中している最中に、最新の顧客フォーカスグループの結果が出て、プロジェクトマネージャーがランチミーティングを予約しようとしたので、自身の定例会議に出るのを忘れそうになるといったことが起こります。各業界でデジタル化のスピードが加速し続ける一方で、コロナ禍による影響も長引いていますが、ビジネスの世界も目まぐるしい速さで変化しています。

実際、Twilioの調査によると、既存の取り組みとコロナ禍によってもたらされた加速が組み合わさった結果、多くの企業で変革が平均で6年、一部の業界では10年近くもスピードアップしたとのことです。同じ調査において、企業の意思決定者の97%は、パンデミックがこのスピードアップの原因であると答えています。急速に進む顧客接点のオムニチャネル化を管理するため、今後のリリースでは、単一の統一されたユーザー管理システムを実現する必要があります。

顧客アイデンティティおよびアクセス管理（CIAM）は、ユーザーアカウントやデータを1つの中央拠点から取得し、整理し、管理することができるソリューションです。

ログインページは、顧客から見れば玄関だと言えます。顧客が最初に目にするものなので、ログインの流れには優れたユーザー体験（UX）が求められます。それと同時に、多くのハッカーたちがデータを盗み出そうと試みるときに、悪用できる脆弱性がないかを探す最初の場所でもあります。そのため、高度なセキュリティが必要で、その効果も貴社の姿勢次第で決まります。中途半端なセキュリティのまま、顧客を迎えたいと思いますか？それとも、安全錠やチェーンを付けて、ユーザーがドアをノックした後に待たなければ入れないほどのセキュリティにしますか？セキュリティが弱すぎれば誰でも侵入が可能になる一方で、厳しすぎると誰も入りたがらなくなるでしょう。セキュリティと顧客体験（CX）のバランスを取ることが重要です。

顧客アイデンティティおよびアクセス管理（CIAM）は、ユーザーアカウントやデータを1つの中央拠点から取得し、整理し、管理することができるソリューションです。強力なCIAMツールは、適切なセキュリティ対策を設定し、顧客データを安全かつ正常に保つ一方で、ユーザー向けにシームレスな体験を提供します。

端的に言えば、煩雑なログインはコンバージョン率を低下させます。CAPCHAを3回行うように求められてアクセスを断念した新規ユーザーや、面倒なパスワードリセットに嫌気のさした重要顧客もいるでしょう。このようにログインプロセスの煩雑さは、ユーザーがそのプロセス、ひいてはその企業自体を見放すことにもつながります。そうした口コミは友人にも広がり、長期的に見ると企業ブランドに計り知れないダメージをもたらします。

CIAMは、デジタルの玄関口において、セキュリティ、プライバシー、利便性を兼ね備えた独自のポジションを占めています。これら3つの基本要素を自社製品や顧客にとって最適な形でバランスをとることは、さらに難しい作業と言えるでしょう。というのも、独自ソリューションの開発のために開発リソースを割くことになってしまい、製品の中核機能の開発から引き離すことになってしまうためです。開発チームは、担当の業務で最も力を発揮するはずです。そして、彼らはその高い能力を、可能な限り最高の中核商品を開発するために利用したいでしょう。顧客のログイン体験とデータセキュリティについては、アイデンティティ管理のエキスパートに委託することで、同一の対応を取っても良いのではないでしょうか？

アイデンティティ管理専用のSaaSサービスを導入すれば、開発者はその能力を中核製品の開発業務に集中させることが可能になります。さらに、顧客情報を守るための考えられるあらゆる対策が講じられ、長期的にはブランドの信頼醸成にも大いに役立ちます。2020エデルマン・トラストバロメーター・レポートによれば、信頼とブランドの評判は、購買の意思決定を左右する要因として、価格の次（同率2位）にランクインしています。

CIAMがセキュリティプライバシー利便性のバランスを実現

あらゆる業界でデジタル化が加速し続ける中、外部と接している境界領域を攻撃するサイバー攻撃も、同時並行で急増しています。ブランドの信頼性と評判を守ることは、多くの経営者にとって喫緊の課題となっています。これはつまり、顧客と接している境界領域を保護することが、ビジネスの最優先事項であるということです。データ侵害は、ブランドの評判を損なうだけでなく、実際の事件の発生から数年に渡って収益に影響を与え続けるリスクがあります。起こりうる攻撃を阻止するために、できる限りの取り組みを行うことは、ビジネスの観点からも有意義です。

大抵の企業の業績は、コンバージョン率で左右されます。そして、煩雑なログインはコンバージョン率の低下につながるため、ログインページで煩雑さを減らす対策を取れば、コンバージョン率を向上させることが可能になります。CIAMを通じて、顧客のログイン体験の流れや、それをニーズの変化に合わせて長期的に発展させ続けるために必要なデータ管理の能力を入手することができます。セキュリティ、プライバシー、顧客体験の適切なパラメーターを設定し、自社および顧客のビジネスの適切な組み合わせを実現することで、必要なセキュリティレベルを確保しながら、顧客が求めるシームレスな体験を提供することが可能になります。

しかし、CIAMは、単にシームレスなログオンを実現するだけではありません。強力なCIAMソリューションでは、サイバー攻撃からの保護、ユーザーデータのプライバシー、直感的なユーザーアカウント管理などの機能が統合されています。

CIAMは、境界領域の防御を固めることで、一般的な攻撃ベクトルを防ぐために役立つ

ではここで、理論上のユースケースのシナリオを見ていきましょう。貴社はWeb上でのプレゼンスを高めようとしています。最近eコマースのスタートアップ企業を買収し、日替わりの取引を行う会員限定のポータルサイトを開発することで、現行のWebアプリやストアを補完しようとしています。開発チームには、新しいWebアプリを介して、これらすべての機能を単一のインターフェースに集約する任務が課せられています。これは、拡張可能でスケーラブルなCIAMソリューションを統合し、単一の認証情報ですべてにアクセスできるようにしつつ、攻撃される領域を減少させる絶好の機会です。

加えて、ボット検出や修復サポート、多要素認証（MFA）の統合、ログストリーミングなどの機能を備えたCIAMソリューションを導入できれば、防御をさらに固めるために役立ちます。現在の分散型アーキテクチャの世界においては、アイデンティティが境界領域となっています。拡張性、スケーラビリティ、およびパートナーの統合は、CIAMソリューションがビジネスを成長させると同時に境界領域とデータを安全に守れるかどうかを評価する上で、重要なカギとなります。

CIAMは、パスワードの文字制限（再利用ポリシーも含む）やスムーズなパスワードリセットの手順の確立、そしてMFAの導入などによってアイデンティティの境界を確実なものにします。

多くの攻撃ベクトルに共通するテーマは、同じパスワードが再利用されがちであるという事実です。実際、パスワード管理ツール「LastPass」のメーカーであるLogMeInの最近の調査によると、一般人の91%は、パスワードの再利用がセキュリティリスクを生むことを知りながら、66%はパスワードを再利用しているとのことです。CIAMは、この分野で確立されているベストプラクティスを導入できるようにサポートします。CIAMは、最小限のパスワード要件（再利用ポリシーを含む）を課してパスワードリセットの流れを合理化するとともに、MFAを導入することで、アイデンティティの境界領域を守ります。

統合されたユーザーデータは保護しやすい

データ管理フレームワークの1つである、信頼できる唯一の情報源（SSoT）は、「ビジネスにとって理想的な状況は、データを複数のサイロ化された場所に保存するのではなく、関連する全データを1か所に集中して保存できることである」としています。CIAMはこのコンセプトを採用しています。すべてのアカウント情報を1か所に集約することで、ユーザーデータにもこのコンセプトを適用しています。アプリがどれだけ多くのプラットフォームにまたがって実行されていても、CIAMがユーザーアカウントをまとめて管理し、すべての入力データを同じアイデンティティSSoTに送ります。

これにより、保護するべき対象が1か所になるため、データをまとめて守りやすくなります。ユーザーアカウントの一元管理は、主要なデータプライバシー規制に準拠する上でも重要です。例えば、GDPRとCCPAの下では、企業は求めに応じてユーザーデータのコピーとそのデータの使用方法の情報を提出する必要があります。これはパートナーのシステムやデータも対象です。そのため、CIAMでコンプライアンスを確保するために必要となる容易なアクセスを実現できれば、顧客の期待値に応えることができます。

アイデンティティSSoTは、ユーザー体験も充実させます。シングルサインオンではSSoTから記録を引き出すため、覚えるべき認証情報は1組だけになります。これにより満足度が向上して、アプリの使用が断念されにくくなるほか、長期的には、攻撃の糸口となりやすい孤立アカウントが減ることも期待されます。すべてのステークホルダーを満足させるのは簡単ではないものの、モジュール化されたCIAM SaaSツールを使用すれば、その理想に一歩近づくことができます。

プロセスの合理化でユーザーを満足させる

顧客が新規アカウントを追加したり、既存アカウントにログインするとき、顧客はその企業を信頼しているのです。それは、ログインのプロセスにおいて、顧客を苛立たせるようなことがないだろうという信頼です。顧客は、アカウントを登録する際に、ほんのわずかな直感的なプロセスだけで認証され、アカウントを利用できたという体験を通じて、そうした信頼が間違っていなかったと実感するのです。

CIAMソリューションは、以上のすべてを行います。アカウント作成プロセスを合理化して、新規ユーザーが歓迎されていると感じられるようにする一方で、データ取り扱い手順の安全性も確保します。PwCの調査によると、たった1度、不快な体験をしただけでも、驚くべきことに顧客の32%がその企業を見放すとのことです。実に、調査対象の3分の1が、たった1度の不都合な体験によって、企業との関係を完全に絶ってしまうと回答しているのです。その人たちの不都合な体験が、文字通り企業との初めての付き合いだったときに、彼らが友人に口コミで何と伝えるかを想像してみてください。次のセクションで説明するように、CIAMは、すべてのユーザーアカウントのプロセスとフローに対して同一の処理を実行することができます。

シンプルなユーザーライフサイクルは守りやすい

新しいアカウントを作成する理由は他にもあるかもしれません。例えば、パスワードを忘れてしまい、「パスワードのリセット」フローも使いづらいときなどです。もちろん、この結果、企業が気づかないうちに管理すべきアカウントが重複して増えていくことになります。完全に統合されたCIAMソリューションを導入すれば、ユーザーのライフサイクル全体にわたってセキュリティ上のメリットがあります。

アカウント作成

アカウントの放棄をなくすためには、アカウント作成プロセスをできる限りシームレスにする一方で、ユーザーのアイデンティティを検証しやすくすることが重要です。シングルサインオンが可能なCIAMソリューションは、まさにそれを実現します。ユーザーが既存のソーシャルネットワークアカウントを使用して適切にログインできるようにすることにより、検証済みアイデンティティをうまく利用すると同時に、新規アカウントを瞬時に作成することができます。この直感的なプロセスによって、パスワードの再利用が減ると見込まれ、結果としてアカウントがハッキングされづらくなり、データを適切に保護しやすくなります。

アカウント管理

ユーザーアカウントを全体的に良い状態で維持するためには、自動化が心強い味方となります。一般的なパスワードリセットプロセスを煩雑でないものに保つため、CIAMでは、パスワードリセットの流れを自動化します。ログインしている人物が本人であるかの懸念を減らすことができるMFAオプションは、完全なアカウント管理プラットフォームの実現に向けての次のステップとなります。また、フェデレーションIDとは、ユーザーが間違って重複アカウントを作成してしまった場合に、アイデンティティSSoTでその人物の別のアカウントを見つけて統合することを言います。このMFAが提供する追加的なセキュリティと、アカウントの重複や放棄をなくすことにより、セキュリティ侵害のリスクを抑制します。

アカウント終了

ユーザーがアカウントを忘れてしまった場合や、他の製品に移行してアカウントを完全に放棄してしまった場合、その後には何が起きるでしょうか。多くのケースで、何も起きないというのが怖いことです。アカウントが適切に管理されていない場合、アイデンティティSSoTは時が経つとともに、放棄され使用されなくなったアカウントや、重複するアカウントであふれてしまいます。これは単に保守の問題だけでなく、セキュリティの問題にもなり得ます。というのも、これらの認証情報が何らかのデータ侵害事件に巻き込まれ、システムの攻撃に使用される可能性があるからです。あらかじめ定められた時間以上休眠しているアカウントにメールを送信するなどの自動アカウント管理機能や、自動アカウント無効化機能、そして最終的な削除機能などは、上記のような一般的な攻撃ベクトルを阻止します。

アカウント認証情報が漏れると、さまざまな攻撃ベクトルが開かれます

データ侵害でユーザー認証情報が盗まれると、パスワードを繰り返し使用され、多くのサイトへの侵入を許してしまう可能性があります。サイバー犯罪者は、データベース自体に侵入する技術を持っていない場合でも、こうしたユーザー名とパスワードなら簡単に入手できます。

これらのいわゆる「スクリプトキディ」は、ダークウェブで認証情報の「コンボリスト」を購入した後、同じくダークウェブで入手可能な既存のスクリプト、または本格的なアプリケーションを使用して、クレデンシャルスタッフィングやその他のブルートフォース攻撃でセキュリティ侵害を引き起こします。自社のユースケースに可能な限り最適な方法でCIAMを統合したい場合には、これらの攻撃ベクトルとその使われ方を理解する必要があります。

クレデンシャルスタッフィング

ここで紹介する最も一般的なベクトルの1つは、「クレデンシャルスタッフィング」と呼ばれるブルートフォース攻撃です。これは、攻撃者がユーザー名とパスワードのリストを入手し、さまざまなサイトのログインフローでその情報を使用することを意味します。パスワードの使い回しが広く行われているために、この攻撃ベクトルは、悪意あるアクターにとって魅力的な手段となっています。彼らが試しに入力する認証情報は、少なくともその努力に見合う以上の働きをしてくれます。これらの攻撃は、面倒くさがりで、簡単に見破られる基本的なパスワードを使い回している人々を一番の対象にしています（現在最もよく使われているパスワードは、「123456」や「password」など）。

ビジネスメール詐欺（BEC）

漏洩したパスワードデータは、他の攻撃の温床となる場合もあります。例えば、ハッカーは、標的として狙っている特定の企業に関するコンボリストを購入することがあります。特定の高い地位にある役員のネットワーク認証情報を抜き出して、なりすましに使用すれば、この役員から標的を定めたフィッシングメールを送信することができるようになります（「スピアフィッシング」と呼ばれます）。これらの攻撃は、ボットの使用によって頻度が増えていますが、主としてソーシャルエンジニアリングを利用した攻撃ベクトルであり、人手によるセキュリティ（またはその欠如）が成否に関係します。

ボット攻撃

一部のハッカーは、単に標的の企業に属するシステムに混乱を引き起こすことを目的としています。彼らは何かを盗み出すのではなく、単に標的企業の業務を中断させて、その組織が侵入を阻止してダウンタイムから復旧しようと慌てて混乱するのを見届けることで目的を達成します。分散型サービス不能（DDoS）攻撃は、その最も一般的な例です。ハッカーがボットを使用して、サイトに大量のトラフィックを送信することで、正当な訪問者が一定時間サイトにアクセスできなくなるようにします。こうした攻撃により、標的となった企業は風評被害を受けるほか、ダウンタイムが発生したことによる経済的な損失も発生します。

他の一般的なボットを使用した攻撃の例としては、eコマースのログインフローへのアクセスを繰り返し、需要の高い商品を買い占めるやり方が挙げられます。このような「ボットスウォーム」の手法は、世界中のゲーマーたちが熱心に待ち望んでいるNvidiaのグラフィックスカードの新製品で最近よく見られます。同様に、MicrosoftがX-Box Xを発売し、Sonyが待望のPlayStation 5を発売したときも、数十万件のボットが作成したアカウントがすべての購入可能な在庫を買い占めてその後の値段を吊り上げようとしたため、WalmartやAmazonで処理能力に多大な負荷がかかりました。これらのスウォーム攻撃シナリオは、主要な商品の在庫不足を招くだけでなく、攻撃が是正されるまで正当なユーザーがサイトを使用できなくなることから、企業に対して金銭と評判の面で大きな負担を強いることになります。

Okta のセキュアな CIAM

「セキュリティについて考えるときは、常にリスクを考える必要があります。汎用的なセキュリティソリューションというものはなく、自分のビジネスや顧客、ユーザーに特化したリスクに基づいて、セキュリティに関する適切な意思決定を行う必要があります。そうすれば、それに基づきセキュリティ制御を強化したり抑制したりすることができます。これは、過剰なセキュリティ設計により利便性に悪影響を与えないようにするためにも役立ちます。」

Duncan Godfrey
副社長、セキュリティエンジニアリング担当、Okta

Okta の Duncan Godfrey は、セキュリティの目標は変化し続けているという事実を述べています。本書で議論してきたセキュリティ上の脅威やハッカーの脅威に未然に対処するには、セキュリティ、プライバシーおよび顧客体験を適切に融合できるスケーラブルで堅牢な CIAM ソリューションを含めた複合的な取り組みが必要です。

CIAM は、企業のデジタル玄関口という特殊な位置を占めているため、境界防御の最前線にあります。これは、悪意ある攻撃者が重点的に狙っている場所であるとともに、顧客が最初にやり取りや購入を行うときに利用する場所でもあります。また、顧客のデータを管理し、分析し、安全に保管するための場所でもあります。

モジュール性は、すでにアプリのアセンブリで急速に標準化されつつあり、決済、メッセージ送信、および認証システムでも、SaaSツールの統合が率先して進められています。Auth0の調査によると、昨今開発されている最新アプリの83%が認証を必要としますが、調査対象となったアプリのうちサードパーティのSaaSツールを使用しているのは58%にとどまることが分かりました。企業の開発チームが可能な限り優れた中核製品を提供するために努力を重ねている中、弊社の開発チームが最適かつ最も安全なCIAMソリューションを提供したいと考えるのには、さまざまな理由があります。

セキュリティチームが最新情報を確実に得られるようにすることで、攻撃を早期段階で特定し、対応時間を短縮し、セキュリティ侵害後の大きな副次的影響を防ぐことが可能になります。

オープン標準

他のサイバーセキュリティツールと同様に、CIAMソリューションはオープン標準に従うことが可能です。これをいわゆる「ブラックボックス」ソリューションにすることも可能です。後者では、ベンダーしかシステムのバックエンドにアクセスできないことから、そのベンダーに縛られることを意味します。これは「ベンダーロック」と呼ばれますが、これを避けられれば俊敏なセキュリティ展開が可能になるとともに、容易な拡張性を確保できます（下記参照）。

OAuth2、OpenIDConnect、SAMLといったオープン標準は、顧客体験を最優先する一方で、開発者が自身の作業に集中できるようにするために重要な役割を果たします。訪問者がすでに持っている認証情報を使用して瞬時に新しいアカウントを作成できれば、ユーザー体験は劇的に向上します。これにより、少数の強力なパスワードのみを使うことが可能になるため、データが複数のシステムに分散する代わりに、アイデンティティプロバイダーによってまとめて安全に守られていると皆が安心することができます。

拡張性

顧客のビジネスニーズに柔軟に対応できるソリューションを提供する上でカギとなるのは、機能を迅速かつシームレスに追加またはカスタマイズできるようにすることです。Oktaがこれに取り組みつつユーザーに必要なバランスを提供する方法の1つは、「ルール」の使用です。例えば、ルールにより、「あり得ない移動（impossible travel）」シナリオのトリガーを作成することができます。シカゴのユーザーがブラジルでログインを試みると、ブラジルのログインを試みるユーザーにはMFAのプロンプトが表示されますが、すでにアイデンティティが検証済みのシカゴのユーザーには表示されません。こうしたルールは、イベント監視や顧客サービスの目的で、他のシステムにログインイベントを通知する際に使用することもできます。

Oktaのパートナーエコシステムは、開発者が拡張性を確保するためのカギとなっています。弊社の中核サービスに含まれていない機能をお探しの場合も、高い確率でそれを見つけることができます。なぜなら、弊社のマーケットプレイスには、業界リーダーの機能も統合されているからです。例えば、新しい規制に継続的に準拠するための同意を管理しなければならない場合なども、専用の統合機能が用意されています。

ログストリーミング

強力なセキュリティ態勢の機能の1つとして、サイバーセキュリティツールで生成されたデータを使用できる能力が挙げられます。データインフラのある組織では、ログストリーミングによって、CIAMから既存のSIEM (Security information and event management) ソリューションや、SOAR (security orchestration, automation, and response) ソリューションに、リアルタイムのデータが直接、送信されます。これは、上述のデータセキュリティ規制の報告および削除要件に対応するための重要な要素でもあります。

Oktaのマーケットプレイスには、Splunk、Sumo Logic、Datadog、その他の統合機能が含まれています。もしくは、広範なAPIおよびSDKライブラリを使用し、カスタム統合機能を構築することもできます。セキュリティチームが最新情報を確実に得られるようにすることで、攻撃を早期段階で特定し、対応時間を短縮し、セキュリティ侵害後の大きな副次的影響を防ぐことが可能になります。

ブルートフォースへの防御

単純に説明すると、ブルートフォース攻撃とは、攻撃者がいくつかの共通パスワードを入力し、単一のユーザーアカウントへのアクセスを試みることです。この一見、洗練されていない攻撃は有効な場合もあり、非効率と言えるものの、ずっと使われ続けています。同じIPアドレスから特定のアカウントに10回以上のログイン試行があった場合には、Oktaが検出します。ブルートフォースに対する防御機能が、該当のユーザーアカウントに対するそのIPからのアクセスをブロック（同じ場所の他のアカウントにはまだアクセス可能）すると同時に、ユーザー宛てに警告メールを送信します。攻撃を受けたユーザーは、そのメールに記載されているIPのブロックを解除するか、パスワード変更時にブロックを自動的に解除することもできます。

ボット検出

より複雑なクレデンシャルスタッフィング攻撃を止めたい場合は、ボット検出が有効なケースもあります。Oktaボット検出は、月に45億件のログインデータをリスク信号分析と組み合わせることにより、ボットネットやスクリプトからのログインの疑いを特定し、フローにCAPTCHAステップを導入することができます。Auth0の調査によると、これによりクレデンシャルスタッフィング攻撃の効果を85%減らせることが分かりました。例えば、既知の適切なIPアドレスからログインする正当なユーザーに対しては、この追加のセキュリティステップは不要です。こうして、本物の顧客に対してはフローの複雑さを少なくすることができます。本物のユーザーに対してリスクを軽減すると同時に煩雑さを減らすことができれば、貴社および貴社の顧客のセキュリティと顧客体験との間で適切なバランスを取りやすくなります。

アダプティブMFA

National Institute of Standards and Technology（NIST：アメリカ国立標準技術研究所）は、MFAがベストプラクティスであると認識しており、常時MFAを使用することを推奨しています。また業界団体のThe Open Web Application Security Project（OWASP）も、MFAは「パスワード関連の攻撃の大半に対する極めて優れた防御策である」と述べています。Okta アダプティブMFAは、ユーザー体験とデータセキュリティを次のレベルへ引き上げます。アダプティブMFAは、場所、固有のデバイス識別子、前回ログインからの時間といった情報から得られる手がかりを利用することで、各ユーザーログオンイベントのリスク分析を実行し、前述の「あり得ない移動」のケースのように、必要と考えられるときのみ追加要素での認証を要請します。

パスワードレス認証

パスワード管理がいかに問題になっているかを踏まえると、そろそろログインフローから顧客のパスワード自体をなくすべき時期かもしれません。Okta Passwordlessでは、メールまたはSMSでユーザーに送るワンタイムコードをパスワードの代用とすることにより、それを実現できます。パスワードをなくすことで、クレデンシャルスタッフィング攻撃やその他のアカウント侵害にさらされるリスクが軽減されます。そして、使用制限のある公開APIを使用することで、ユーザーのデータを自動攻撃やボット攻撃から守れます。

CIAMはログインのフリクションを低減しながらセキュリティを向上

貴社とチームは、次のスプリントまでセキュリティに忙殺されることはありません。モジュール化のトレンドに従い、可能な限りサードパーティのSaaSソリューションを統合していけば、CIAMを迅速かつ安全に導入していくことができます。優れたセキュリティを提供しながら顧客の満足度を維持する上でカギとなるのは、正当なユーザーが増加すれば、同時に貴社のデータを入手しようとする悪意ある攻撃者も増加していくという事実を把握することです。この仕組みを踏まえたCIAMソリューションなら、ユーザー数の増加と防御の拡張に同時に対応することもできます。

デジタルアイデンティティへの取り組みに注目する企業は増えています。ログインページから顧客体験を管理することは、信頼性の高い関係性を創出していく上でカギとなるでしょう。

Okta顧客アイデンティティを弊社のROI計算機とあわせて使用することで実現できるビジネス上のメリットについては、こちらをご覧ください。