ホワイトペーパー

Okta & AI

人工知能はどのようにアイデンティティおよびアクセス管理（IAM）を再構築するのか

目次

サマリー

人工知能（AI）全般が、最適化、データ分析、異常検知、その他の予測ベースのアプリケーションをコモディティ化して、組織の運営のあり方を塗り替え、革新的な製品やサービスを後押ししています。ほとんどの場合、そのような機能は特に新しいものではありません。むしろ、目新しいと言えるのは、コスト削減と性能向上により、こうした能力をほぼ何にでも組み込むことが実用面で可能なったという点です。

新たに注目されているのは、OpenAI の ChatGPT や DALL-E、Google の Bard、Meta の Code Llama といったアプリケーションの中核をなす大規模言語モデル（LLM）の急速な進歩により、あたかも一夜にして実現したように見える生成 AI の登場です。

実際のところ、生成 AI は真の意味で一世代に一度のパラダイムシフトであり、その影響が理解され、感じられるようになり始めたばかりです。

しかも、アイデンティティほど AI の応用にうってつけの領域はほとんどありません。アイデンティティは複雑であるため、AI による改善の余地が大きいと言えます。それだけでなく、アイデンティティのフローとトランザクションが生み出す膨大なデータが、本質的に AI エンジンの駆動力となります。Okta は、アイデンティティの全領域でデータの「ネットワーク効果」の活用を目指していますが、短期的には以下の研究開発への投資に焦点を絞っています。

- セキュリティの強化
- 生産性の向上
- ユーザーエクスペリエンスの向上

ここで強調しておきたいのは、Okta にとって AI は新しいものではなく、すでに以下のような複数の重点領域で AI を活用しているという事実です。

- Okta Workforce Identity Cloud（WIC）は、ThreatInsight、アダプティブ多要素認証（アダプティブ MFA）、電話料金詐欺対策に AI を組み込んでいる
- Okta Customer Identity Cloud（CIC）は、ボット検知機能（および関連するアイデンティティ脅威レベル［ITL］）とアダプティブ MFA で、AI を大いに活用している

Okta はさらに、Oktane 2023 で、AI を活用した数々の新機能を発表しました。WIC には、Okta AI を活用する 4 つの新しい機能が導入されました。

- セキュリティの強化：Identity Threat Protection
- ガバナンスの支援：Governance Analyzer
- 管理の簡素化：Log Investigator、Policy Recommender

CIC には、6 つの新機能が追加されました。

- テナントのセキュリティ強化：セキュリティの推奨事項
- カスタマーエクスペリエンス向上と収益拡大：ファネルコンバージョンの推奨事項、ブランドのカスタマイズ
- 管理の簡素化：コパイロット、アクションの選択と開発、パーソナライズされたテナント構成サマリー

さらに、年に 2 回開催している全社的なハッカソンでは、イノベーションを重視する文化を醸成しています。こうしたハッカソンで検討されたアイデアの多くは、特許や製品の概念実証へと発展し、最終的に何らかの形で市場に投入されます。特に、最近のハッカソンでは、AI の実験に的を絞ったプロジェクトが 25% を占め、その潜在力が注目されています。

AI の重要性の高まり、そして幅広い開発者層にわたって AI が注目されている状況を踏まえ、初の AI 専門ハッカソンも予定しています。

Okta はまた、お客様が LLM で魅力ある優れたエクスペリエンスを生み出すお手伝いもしています。Okta Ventures、Okta Integration Network、Auth0 for Startups、Auth0 Marketplace といった Okta のエコシステムからは、Okta 製品に統合可能な多彩な AI ソリューションが提供されています。

未来に課題がないわけではありません。サイバー犯罪者はすでに AI 全般、特に LLM を活用して新たな攻撃ベクトルを探り、既存の攻撃をより危険なものにしています。しかし Okta は、AI が良い意味で進歩を促進する可能性を信じ、明るい見通しを持っています。

今日、デジタルアイデンティティは、増え続けるアプリケーションやサービスへのアクセスを制御し、現代生活の多くの側面に影響を与えているどころか、ある意味、支配すらしています。今後、こうした影響はさらに大きくなり、認証、認可、そしてアイデンティティは全体として、信頼やセキュリティを確保し、優れたユーザーエクスペリエンスの基盤を提供するものとして欠かせないものになっていきます。

そして Okta は、人、テクノロジー、コミュニティのつながりを強化するために、AI の力を活用することを約束します。

はじめに

ここ数か月、人工知能（AI）の躍進と、それによって可能になる AI の利用（以前から期待されていたものもあれば、予期しないものもあります）について、テクノロジー関連メディアでも主要メディアでも数え切れないほどの記事が掲載されています。

実業家のアンディ・グローブ氏が「偏執狂だけが生き残る」という名言を残したように、さまざまな業界で、規模を問わず多くの企業が、AI を活用して既存のソリューションを改善し、新たなソリューションに力を与え、競合他社に対する優位性を獲得すべく「堀」を固めようと競い合っているのは驚くことではありません。

新たに登場した AI への投資も、Okta にとっては普段と変わらないビジネス活動の一環です。AI はすでに、当社のポートフォリオの中で数多くの重要な製品や機能を支えています。特に、機械学習（ML）は、動的なリスク評価とリスクベースの認証インテリジェンスで中心的な役割を担っています。

現場での長年にわたる経験から、私たちは AI を単一のモジュールや機能、つまりプラットフォームに接続 / 追加しさえすればよいものとは考えていません。むしろ、AI は汎用テクノロジー（より正確には、汎用テクノロジーの集合）であり、アイデンティティインフラストラクチャに組み込まれ、統合されることで最善の利用効果を生み出すものであると認識しています。

このホワイトペーパーでは、Okta と AI の関係について明確化するため、以下の点を解説していきます。

- AI が、あらゆるデジタル領域に破壊的影響を及ぼし、これらの領域を再形成する可能性を持つ理由
- AI のメリットがアイデンティティ分野で特に大きい理由
- AI の活用による直近の主要な価値提案
- Okta Workforce Identity Cloud（WIC）と Okta Customer Identity Cloud（CIC）ですでに AI を活用している機能
- Okta AI を活用した WIC と CIC の新機能

なぜ AI なのか？

基本的なレベルでは、人工知能は、その「賢さ」が人間による意思決定と区別がつかないコンピューターによって行われる意思決定（それをどのように導き出したかに関係なく）として理解できます。

AI の概念を正式に編み出したのは Dartmouth Workshop ですが、最初の前提は 1943 年に、論理学者のウォルター・ピッツと神経生理学者のウォーレン・マカロックが人間の脳の神経細胞の数学的表現を作成しようとしたときに形成されました。当時のこうした発展は、19 世紀のエイダ・ラブレスからアラン・チューリングに至る、計算理論における長い進歩の歴史の上に築かれたものでした。

1960 年代以降の AI は、一般的に機械学習（ML）によって実行され、パターンの検知と認識を含む巨大なアルゴリズムの集合へと進化してきました。ML 分野は、この 15 年間で飛躍的に進歩し、実用的かつ経済的なディープラーニングの出現につながりました。

生成 AI は一世代に一度のパラダイムシフト

AI の発展形態として世界を席巻したのは、驚くべき（衝撃的とも言える）生成 AI の登場です。生成 AI は、主として大規模言語モデル（LLM）の目覚ましい進歩によって急速に進化しています。

LLM を搭載した OpenAI の ChatGPT や DALL-E のようなアプリケーションは、AI をメインストリームに押し上げました。しかし、その理由として、人間を模倣する能力、そしてモデルに取り込まれる（さらに、その振る舞いを形成する）データに関する透明性の欠如が挙げられます。

突如として、散文を書いたり、複雑な（場合によっては、意図的に本物そっくりの）画像を作成したりすることが、もはや人間だけの領域ではなくなりました。さらに、LLM は高い記述能力を持ち（プログラミングも記述の一形態です）、今や多くのものがソフトウェアによって制御されるようになっています。そのため、幅広い領域で LLM が思いがけないブレークスルーや進歩を支えています。

より現代的な AI の時代が始まったのは明らかです。そのため、新旧、そして今後登場する AI の能力をどのように活用すべきかを考えるのは当然のことと言えます。

AI に何ができるのか？

経済学者の Ajay Agrawal 氏、Joshua Gans 氏、Avi Goldfarb 氏は、著書『Prediction Machines』の中で、AI の台頭を予測（利用可能な情報から新しい情報を創出することと定義）のコストを引き下げるものと捉え直しています。

予測は「不確実性の下での意思決定の核心」であり、「私たちのビジネスや個人生活はそのような意思決定に満ちている」ため、予測のコストを下げることは並外れた可能性をもたらします。ほんの一部の例を挙げると、予測は以下に不可欠な要素です。

- 最適化：コンテキストや過去の観測結果を用いて、最適な経路、応答、構成、ユーザーインターフェイス設計などを予測する
- 振る舞い分析：ユーザーの意図を予測するために、過去のアクションのコンテキストを考慮してリアルタイムの振る舞いを観測する
- データマイニング：どのようなデータや洞察がユーザーのクエリやプロンプトを最も満足させるかを予測する（また、予測が LLM や生成 AI の核心でもあることは注目に値する）

従来のコンピューティングと同様、AI は、どのような形態であれ、既存の産業を破壊し、再構築することを約束する汎用テクノロジーです。また、アイデンティティの進化を後押しする可能性について、Okta は特に強気で臨んでいます。

AI と アイデンティティ

デジタルアイデンティティは、特定のアプリケーションによって提供される機能のコンテキストにおいて、特定のユーザーを定義する一連の属性です。今日、デジタルアイデンティティは、増え続けるアプリケーションやサービスへのアクセスを制御し、現代生活の多くの側面に影響を与えているどころか、ある意味、支配すらしています。今後、こうした影響はさらに大きくなり、認証、認可、そしてアイデンティティは全体として、信頼やセキュリティを確保し、優れたユーザーエクスペリエンスの基盤を提供するものとして欠かせないものになっていきます。

その結果、IAM サービスは、従業員、請負業者、パートナー、顧客といった、許可されたユーザーだけが特定のリソースにアクセスできるように確保するという、コネクテッドな世界の要としての役割を担います。概念としての IAM は、アイデンティティを証明したユーザーが、権利を持つリソースへのアクセスを許可されることであり、非常に単純です。しかし実際には、いくつかの要因によって複雑化します。

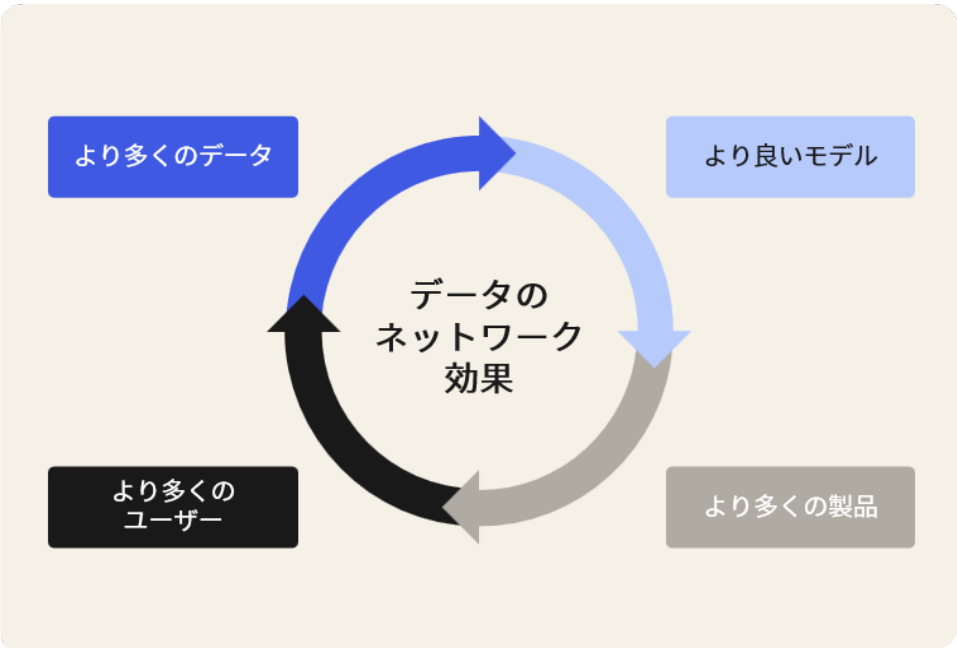
- 今日のデジタル世界には多くのユーザーが存在し、個々のユーザーは多くのデジタルアイデンティティを持つ可能性があり、デジタルアイデンティティを表現する方法は無数にある
- 異なるデジタルアイデンティティは、リソースに関して異なる権利と認可を持ち、これらの権利と認可はますます動的になっている
- セキュリティの境界が消えつつある今、攻撃者はアイデンティティに活動の焦点を当てている

これまで見てきたように、AI は、十分なデータを利用できる範囲においては、複雑さや不確実性への対処に卓越した能力を持ちます。

幸い、アイデンティティの領域には、提供できるデータが豊富にあります。これは、アイデンティティ自体が、静的な一次元の属性から、動的で継続的な相互作用へと進化し、新しいデータポイントごとに自らを再構築しているためです。この進化は、クラウドによって起きた変革なしにはあり得なかったものであり、現在起こっている AI 変革により今後も続くと考えられます。

データのネットワーク効果の活用

この進化がもたらす重要な余波として、データのネットワーク効果の好循環が挙げられます。つまり、AI モデルがアクセスできるデータの量が増え、質が高まるのに伴って、学習速度が速くなり、予測や判断の精度が高まります。これによって、ユーザーにとって製品やサービスの価値が高まり、これがより多くのユーザーを引き付け、さらに多くのデータが生み出され、この好循環の中でモデルにデータがフィードバックされます。



1. **より多くのデータ：**製品やサービスが使われれば使われるほど、ユーザーとのインタラクション、トランザクション、フィードバックなどを通じて、より多くのデータが生成される。
2. **より良いモデル：**このデータが、基盤となる AI モデルを改良するために使用される。データの量が増え、質が高まるのに伴って、モデルの予測や判断がより正確になる。
3. **より良い製品：**AI モデルが向上することで、製品やサービスも向上する。
4. **ユーザー / 用途の増加：**改善された製品やサービスはより多くのユーザーを引き付け、ユーザーがさらに多くのデータを生成し、このサイクルが続く。

こうした自己強化ループは、イノベーションと競争力の差別化を強力に推進します。

こうした脅威環境の変化を受けて、Gartner は次のように警告しています。**「2025 年末まで、セキュリティ意識の高い組織は、生成 AI を使用する攻撃に対処するため、不審な活動を検知するためのしきい値を下げざるを得ず、これによって誤検知が増えるため、人間による対応が減るのではなく、逆に増える状況が続く」**

[1] Gartner, 4 Ways Generative AI Will Impact CISOs and Their Teams, Jeremy D'Hoinne, Avivah Litan, Peter Firstbrook, 29 June 2023)
Gartner は、Gartner, Inc. および / またはその関連会社の米国およびその他の国における登録商標であり、許可を得て使用しています。無断転載を禁じます。

セキュリティの強化

今や、AI が以下の能力を提供することはよく理解されています。

- クレデンシャルスタッフィングやフィッシングなど、既存のアイデンティティ攻撃をより危険なものにする（検知が難しくなる、効果 / 破壊力が高まるなど）
- まったく新しいタイプのアイデンティティ攻撃を可能にし、その多くは実環境で発見されて初めて明らかになる
- 既存のセキュリティ対策を克服する（CAPTCHA を解く、音声認証システムを騙すなど）

加えて、コーディングやスクリプト作成の能力を持つ生成 AI によって、あらゆるスキルレベルの（つまり、コーディング能力に関係なく）犯罪者が簡単に攻撃を実行できるようになり、全体として、サイバー犯罪のエコシステムに引き込まれる参加者が増え、活動が効率化する可能性があります。

しかし、AI は間違いなく攻撃側を助ける一方で、防御側も「パワーアップ」します。

Okta は、あらゆるデバイス（管理対象か非管理かを問わず）、あらゆるプラットフォームで、フィッシング耐性のある FastPass の認証を提供して業界をリードし、ユーザーフレンドリーでフィッシング耐性のある FIDO2 認証を開発者が容易に採用できるよう支援しています。一方で、AI を活用する必要性も認識しています。

- **「セキュアバイデザイン」に基づく Okta の保護強化**：脅威者が AI を使って脆弱性やセキュリティギャップを探索できるのと同様に、Okta のような組織も AI を活用できる。また、私たちには、リリース前のソフトウェアやシステムを AI で堅牢化できるというメリットがある。
- **脅威の自動検知**：コンテキスト分析と行動分析は、インテリジェントなリスク評価と高度なアイデンティティ脅威の検知に役立つ。また、AI の進歩によって、これらの機能を実行する能力が向上し、新たな機能の導入が促進される。
- **お客様に代わってリスクを緩和**：防御策（封じ込めのアクション、悪意ある活動のブロックなど）の自動化、アラートと推奨プレイブックの組み合わせ、GRC（ガバナンス、リスク管理、コンプライアンス）の取り組みのサポートなど、AI はプロアクティブにリスクを軽減し、攻撃に対応する上で非常に大きな価値をもたらす。

幸い Okta は、AI 主導の多くのセキュリティ機能を Workforce Identity Cloud と Customer Identity Cloud の両方に統合してきた実績を持ちます。

生産性の向上

Okta の「開発チームの SaaS 調達状況」レポート（2023 年）では、主な調査結果の 1 つとして、調査対象の開発組織が基本的に 2 タイプに分けられることが明らかになりました。つまり、52% は製品エンジニアリングに AI をすでに導入しており、45% は今後 12 か月以内に導入する予定です。

俊敏性、新しい能力の獲得、コスト削減、時間短縮といった多様なメリットを求めて、組織はデータアナリティクス、品質保証、機械学習、自動化などで AI ツールを統合しています。

Okta は、AI が生産性を向上させる潜在力があるという楽観的な見通しを、社内のエンジニアリング組織で共有しています。

同時に、AI の影響はエンジニアリングの領域をはるかに超え、規模や業種に関係なく、実質的にすべてのお客様組織で働くすべての人々に及ぶはずであるとも認識しています。

現代の成熟したワークフォースアイデンティティのインフラストラクチャは、以下の能力を提供します。

- 従業員、請負業者、ビジネスパートナーが、重要なツールやリソースに、どこからでもシームレスかつ安全にアクセスして、作業できるようにする
- 利便性の高いユーザーエクスペリエンスを提供し、業務効率を高め、管理負担を軽減することで開放された時間や労力を、成長やイノベーションなどの優先事項に集中できるようにする
- あらゆる規模の組織が、俊敏性を拡張・改善できるようにする
- 犯罪者が引き起こす混乱からの保護を支援する

アイデンティティインフラストラクチャ全体に組み込まれた AI は、これらすべてのメリットを促進するだけでなく、新たなメリットも生み出します。

ユーザーエクスペリエンスの向上

次に、摩擦について少し考えてみましょう。

コンシューマー向けのビジネスにとって、摩擦（自社サービスとユーザーのインタラクションを遅らせるすべての要因）は、コンバージョン、ひいては収益の大きな障害となります。Okta の「Customer Identity Trends レポート」によると、調査参加者の 60% 近くが、シンプルで安全、かつ摩擦のないログインエクスペリエンスを得られる場合に、サービスにお金を使う可能性が高くなると回答しています。このデータは、すべてのセクター / 業種で一貫しており、ユーザーがあらゆるインタラクションで利便性を望んでいることを示唆しています。

もちろん、信頼を確立し、セキュリティコントロールを提供するためには、ある程度の摩擦は避けられません。しかし、あらゆるコンシューマーとのインタラクションにおいて、実際に有効なあらゆる部分で摩擦を減らすことで、コンバージョンを高め、それに応じて短期的にも長期的にも収益を伸ばすことができます。

明らかに AI を活用できる領域として、以下の 3 つが挙げられます。

- 継続的なリスク評価を提供し、パスワードレスやログインレスのエクスペリエンスを可能にする
- アイデンティティフローを最適化して、ユーザーの利便性を高める
- ユーザーインターフェイスのデザイン（アイデンティティのトランザクション中）を改善して、ユーザーの利便性を高める

職場での摩擦とは、業務の遂行を妨げたり遅らせたりするあらゆる要因を指します。アイデンティティ自体は、会議を定時に開始させたり、問い合わせに対する同僚の対応を早めたりする能力は持ちません。しかし、成熟したアイデンティティインフラストラクチャは、以下のような面で貢献します。

- ユーザーが適切なリソース（データ、システム、アプリケーションなど）に、適切な権限で、適切なタイミングにアクセスできるように確保する
- セルフサービス能力（リソースへのアクセス要求、プロファイルの変更、セキュリティ要素の登録など）を強化する
- 既存プロセス（アクセスレビュー / 認定、安全なオフボーディングなど）を自動化する

繰り返しになりますが、AI はこうした既存の能力を格段に強化すると同時に、新たな能力を引き出すことができます。たとえば、アイデンティティの展開環境やパフォーマンス指標を大量に分析して、最も効率的で効果的な構成を特定し、このインテリジェンスを使用して、組織 / 部門ごとにパーソナライズされた推奨事項を提供できます。また、管理者が膨大な運用データやログデータの中から必要な情報を素早く見つける上で役立ちます。

加えて、LLM は自然言語に対応することから、コーダー以外の人々がさらに多くのアイデンティティ関連機能を利用できるようになります。Okta Workflows はすでに、ドラッグ&ドロップのインターフェイスを通じて、ノーコードでのアイデンティティの自動化とオーケストレーションを可能にしています。自然言語による指示を受けるソリューションの実現も荒唐無稽な話ではないと言えます。

Workforce Identity Cloud（WIC）における AI

以前はユーザー名とパスワードを管理するユーティリティサービスとしか見なされていなかったアイデンティティは、現代のビジネスにとって必須要素であると同時に、実現要素としての役割を担うようになりました。その結果、アイデンティティインフラストラクチャは、広範な IT 環境の中で相互接続された基盤レイヤーとなり、ユーザーやその他のエンティティと、オンプレミス / クラウドのシステム、データ、リソースを接続しています。

このように、アイデンティティの保護は、強固なセキュリティ態勢の基礎となる要素であり、内部脅威や、窃取された資格情報を悪用する侵入者に対抗する上で役立ちます。

AI は、ワークフォースアイデンティティのインフラストラクチャを脅威から保護するのに役立つだけでなく、ガバナンス活動を支援する高い能力も持ちます。特に、膨大な構成データを調査してリスクを特定し、是正措置を推奨し、多くの一般的で重要なタスクを自動化できます。

同様に、AI は情報を分析して洞察を導き出す能力があることから、膨大なログの解釈に最適です。

これらの能力を自然言語処理や生成 AI と組み合わせることによって、管理者が増え続けるアイデンティティインフラストラクチャを管理する方法がすでに変わりつつあります。

Okta も参加する Identity Defined Security Alliance の「2022 Trends in Securing Digital Identities」レポートによると、IAM やセキュリティの専門家 500 人以上を対象に実施した調査で、以下のような結果が得られました。

- **84%** が、過去 1 年間に自社がアイデンティティ関連の侵害を経験した
- **78%** が、侵害によってビジネスが直接的な影響を受けた
- **64%** が、デジタルアイデンティティの効果的な管理と保護を、セキュリティの最優先事項（16%）またはトップ 3 の優先事項（48%）と考えている

ThreatInsight

AI の役割：Okta の広範な顧客ベースにわたる、攻撃や認証要求の観測と自動化されたフィードバックに基づいて、要求が悪意のあるソースから発信されているかどうかを予測する

ThreatInsight は、Okta エンドポイントに向けられた資格情報を悪用した大量の攻撃（パスワードスプレー、クレデンシャルスタッフィングなどのブルートフォース攻撃）を検知して緩和する基本的なセキュリティ機能です。Okta 管理者コンソールでブロックモードを選択するだけで、攻撃者が認証を試みる前に悪意があると予測された要求を自動的に拒否したり、ログモードを選択して悪意のあるトラフィックを監査したりできます。

ThreatInsight は、1 日に数千の Okta org に対して行われる何百万件もの認証要求のネットワーク効果を利用し、経験則（静的ルール）と機械学習を組み合わせて、資格情報を悪用した攻撃を観測し、インテリジェンスを導き出します。

Okta はさらに、エッジレイヤーでブロックされた悪意のある既知の IP ごとに、100% の確度で悪意が確認できない IP アドレスからの不審なイベントを多数識別します。シナリオによっては、ホテルが大規模な会議を主催する場合など、正当でありながらログインの失敗が複数回起こるユースケースもあり得ます。こうしたシナリオでは、複数の Okta org の複数のアカウントで、発信元がすべて同一のソース（ホテルのネットワークなど）と見られる何十、何百、あるいは何千ものログインの失敗が発生してもおかしくありません。これらの IP アドレスをブロックすることで、正当な認証の試みをブロックしてしまう可能性があります。こうした事態は、DDoS 攻撃の犠牲になるのと同様に回避しなければなりません。

このような誤検知を避けるため、不審な IP アドレスは、Okta の全顧客ベースのアイデンティティ攻撃に関与する IP と定義されます。言い換えると、Okta のお客様すべてにとっての利益となるよう、攻撃に関与していることが判明している IP のみが ThreatInsight データベースに追加されます。

ここで重要となるのは、ThreatInsight はローリングウィンドウを使用しており、次の評価までに疑わしい活動を示さなくなった不審な IP アドレスはデータベースから削除される点です。

アダプティブ MFA

AI の役割：認証イベント（ログインなど）や認証後のアクション（特定のリソースへのアクセスなど）に関連するリスクを予測することで、コンテキストに応じたインテリジェンスを活用した適切な認証方法を提供する

アダプティブ多要素認証（MFA）は、認証要求が発生する、絶えず変化するコンテキストを考慮することで、さらなるインテリジェンスをアイデンティティフローに追加します。アダプティブ MFA は、セキュリティと認証のポリシーを動的に適応させることで、組織のセキュリティ態勢とユーザーエクスペリエンスを同時に向上させます。

たとえば、アダプティブ MFA ポリシーは、ユーザーが SSO 経由でサインインしたり、管理された（既知の）デバイスからサインインしたりする際に MFA を求める頻度を下げることで、ユーザーの摩擦を軽減できます。その一方で、要求に関連するリスクが高いと評価される場合（通常とは異なる時間帯や新しいデバイスからのログイン試行など）や、ログインしたユーザーが特に機密性の高いリソースや情報にアクセスしようとしている場合には、追加の認証要素やより安全な認証要素を要求できます。

アダプティブ MFA ソリューションが提供する柔軟性とコントロールの度合いは、利用可能な MFA 要素と、リスク評価に組み込まれたコンテキストに応じたインテリジェンスの豊富さに大きく依存します。

アダプティブ MFA では、インテリジェントなエージェントが、ユーザー ID、デバイス、ネットワーク、位置、移動、IP、サードパーティやエンドポイントセキュリティインテグレーションからの外部データなど、さまざまなリスクシグナルを調査し、異常を分類して、認証プロセスの各ステップでリスクベースの認証を適用し、ユーザーがログインした後もステップアップ認証などを適用します。

電話料金詐欺対策

AI の役割：さまざまなインプット（IP、電話番号のプレフィックス、国など）に基づき、電話トランザクションに関連する異常を検知し、リスクを分類する

国際レベニューシェア詐欺（IRSF）は、電話料金詐欺とも呼ばれ、詐欺師が大量の高額な国際電話 /SMS を人為的に発生させる詐欺の一種です。長距離国際電話はトランザクションのコストが大きいため、電話料金詐欺は、MFA フローの一環として電話やテキストを使用するビジネスに大きな金銭的被害を及ぼす可能性があります。

電話料金詐欺対策機能は、信頼性の高い電話サービスを提供しながら顧客を保護します。そのために、ヒューリスティックエンジンと複数の ML エンジンという補完的な検知メカニズムを活用します。

大まかに言うと、各トランザクションにはリスクマーカーが割り当てられ、リスクが高いと判断された取引には、より厳しいレート制限が適用されます（これらのコンポーネントの機能や、電話料金詐欺対策機能への組み込みについて、詳細はこちらのブログをご覧ください）。

特筆すべきは、機械学習コンポーネントの導入により、不正トランザクション検知の効果が 20% 向上したことです。

Okta AI を活用した Identity Threat Protection

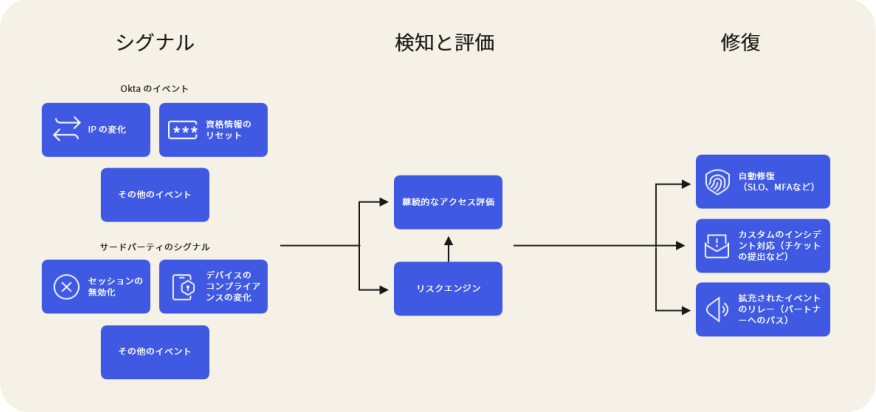
2024 年第 1 四半期に限定早期アクセス

AI の役割：ML モデルが、コンテキストに応じてリスクスコアリングを自動的に適応させ、動的な環境に適した、より正確でニュアンスのある評価を提供する

今日のアイデンティティ脅威に対しては、ユーザーが認証する前に始まり、セッションの有効期間を通じて継続する階層型のアプローチにより防御する必要があります。特に、より強力な認証手法の採用が拡大するのに伴って、攻撃者が MFA を回避してアクティブなセッションをハイジャックするためのリソースを増大させているため、継続的な認証の重要性が増すと予想されます。

Okta AI を活用した Identity Threat Protection は、以下の 3 つの重要な機能により、高度なアイデンティティ脅威から保護します。

1. **継続的なリスク評価：**AI を活用し、ログイン時とアクティブなユーザーセッションの両方でセキュリティポリシーを適用することで、不正アクセスやセッション乗っ取りなどの認証後の脅威の可能性を軽減する。
2. **共有シグナルのパイプライン：**モバイルデバイス管理（MDM）、クラウドアクセスセキュリティブローカー（CASB）、ネットワークセキュリティ、エンドポイント検知 / 応答（EDR）ソリューションなど、さまざまなセキュリティテクノロジー間で新たな脅威を検知して対応できるようセキュリティチームを支援する。
3. **アダプティブなアクション：**機能を有効にしたサポート対象アプリケーションからの Universal Logout、オンデマンドでの多要素認証の要求、新たなリスクに対処するための自動ワークフローの実行など、対象を絞ったアクションを有効にすることで、リアルタイムの脅威に対応する。



Okta AI を活用した Governance Analyzer

2024 年第 2 四半期に限定早期アクセス

AI の役割：幅広いデバイスアクセスシグナル、ユーザーアクセスシグナルなど、コンテキストに応じた重要シグナルを取り込み、実用的なアイデンティティガバナンスの洞察を提供する

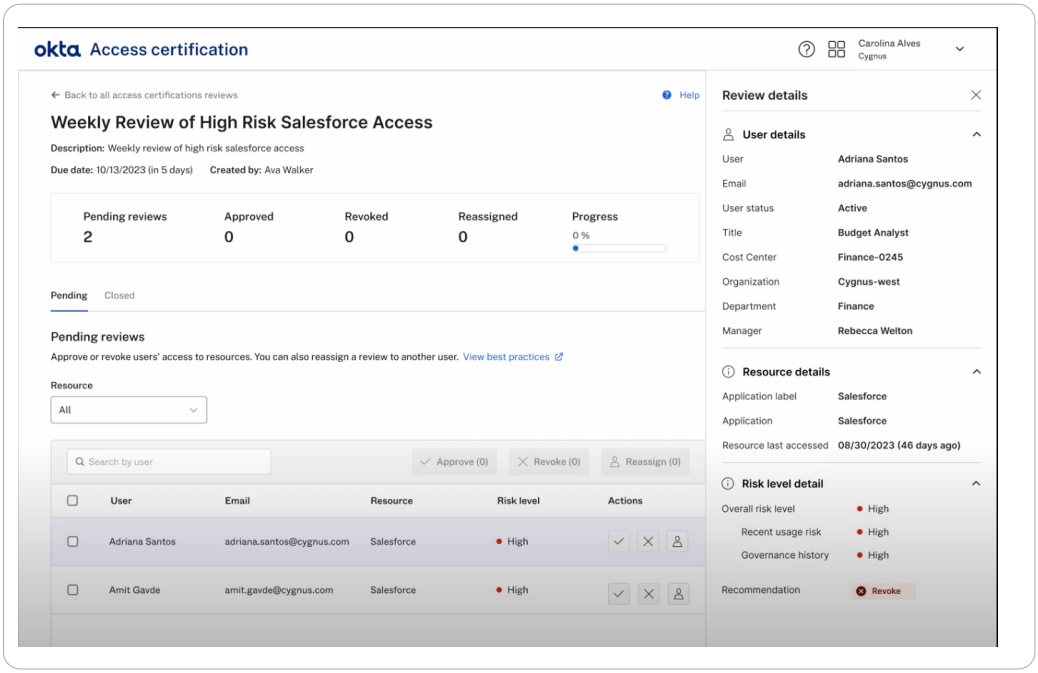
アイデンティティガバナンス / 管理（IGA）は、アイデンティティ管理とアクセス制御のために、以下を組み合わせたポリシーベースのアプローチです。

- アイデンティティガバナンス：職務分掌、ロール管理、ログ管理、アクセスレビュー、アナリティクス、レポーティングを包含するプロセスとポリシー
- アイデンティティ管理：アカウントと資格情報の管理、ユーザーとデバイスのプロビジョニング / プロビジョニング解除、エンタイトルメント管理

IAM、IGA、特権アクセス管理（PAM）の統合プラットフォームとして、他に類を見ない膨大なアイデンティティデータセットを提供する Okta を活用することで、コンプライアンス要件を満たし、監査に必要とされる情報を提供し、プロセスを効率化し、ワークフォースの生産性を向上させるために活用できます。

Okta AI を活用した Governance Analyzer は、こうした目標をサポートするため、機械学習、デバイスアクセスシグナル、ユーザーアクセスシグナルを活用して以下の能力を提供します。

- ガバナンスプロセスにおける意思決定者の認知的な負担を軽減する
- ユーザーとリソースの組み合わせのリスクについて、重要な洞察を提供する
- Okta の幅広いデータを活用して、他のベンダーからは得ることのできない洞察を提供する



Governance Analyzer は、以下のような用途で活用できます。

- ユーザーアクセスの要求や認定で、承認や拡張を判断するための情報を提供する
- 特定のリソースへのアクセスを要求できるユーザーを決定する（特定のリスクしきい値以下のユーザーのみがアクセスを要求できるなど）
- キャンペーンでアクセスをレビューする範囲を設定する（指定したリスクレベルを超えるユーザーを自動的にレビューする、またはより頻繁にレビューするなど）
- 要求または認証キャンペーンで、アクセスを承認 / 拒否する自動アクションを実行する
- 重要リソースがアクセスに必要な承認を受け、アクセスが頻繁にレビューされるよう、適切なガバナンス構成を推奨する

Okta AI を活用した Log Investigator

2024 年第 3 四半期に限定早期アクセス

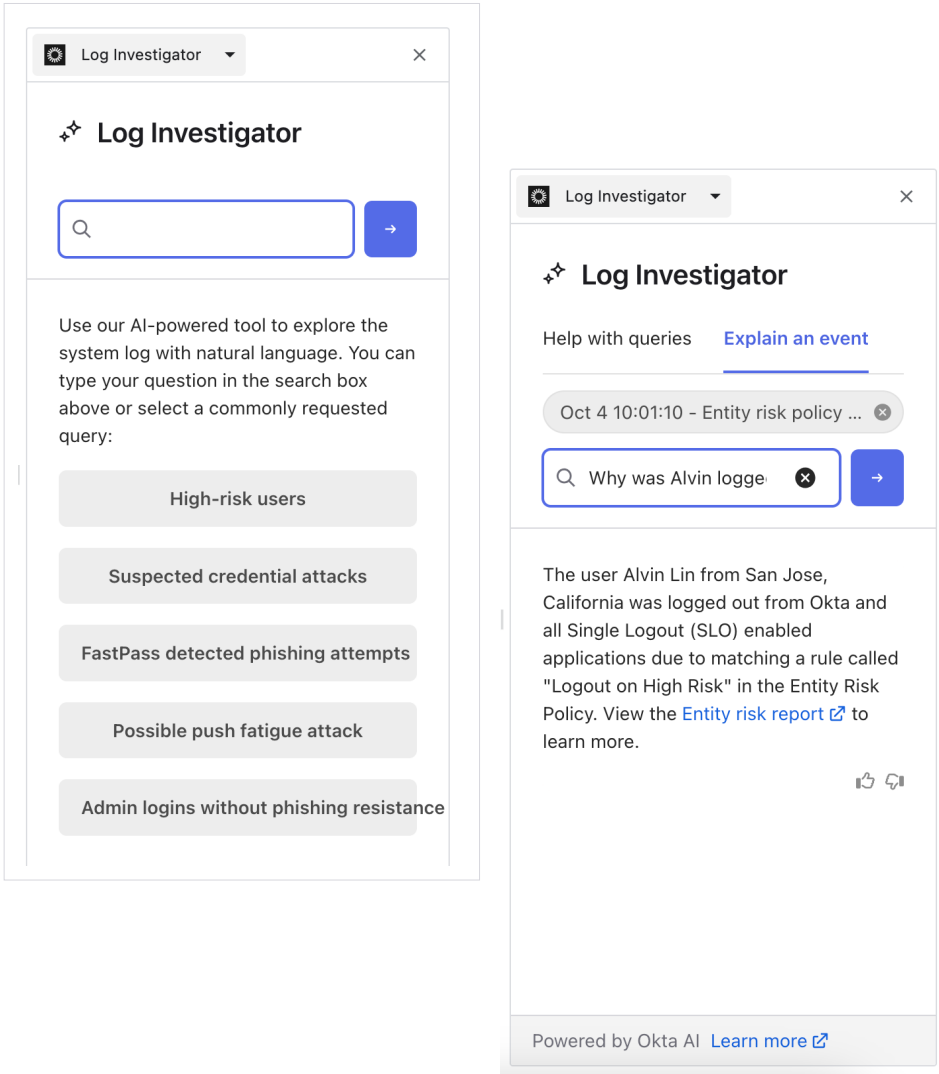
AI の役割：IT の担当者が Okta の膨大なデータセットから情報や洞察を素早く容易に収集できるように、自然言語によるログ /API 検索ツールを提供する

コンピューティングが登場して以来、ログは、何が起きたのか、何が起きているのか、なぜ起きているのかを判断するための貴重な情報リソースとしての役割を果たしてきました。しかし、デジタルテクノロジーのコントロールが事業運営のますます多くの側面を対象とし、コントロールがより細部に及ぶようになるにつれて、ログが急増し、洞察の抽出が難しくなりました。多くの IT システムでは、簡単な質問の答えを見つけるだけであっても、何百もの結果を調べなければならず、慎重に作成されたクエリや多大な手作業が必要になることが少なくありません。

幸いなことに、生成 AI は、有用な情報を抽出するために人々がデータセットと対話する方法を変えつつあります。

Okta AI を活用した Log Investigator は、自然言語によるログおよび API 検索ユーティリティです。IT の担当者は、Okta の膨大なデータセットを簡単かつ迅速に利用して、次のようなアイデンティティ関連の質問に回答できます。

- 最近 1 週間に不審なログインはあったか？
- その中で非管理デバイスからのものはあったか？
- その中で新しい場所のものはあったか？



Okta AI を活用した Policy Recommender

2024 年第 1 四半期に限定早期アクセス

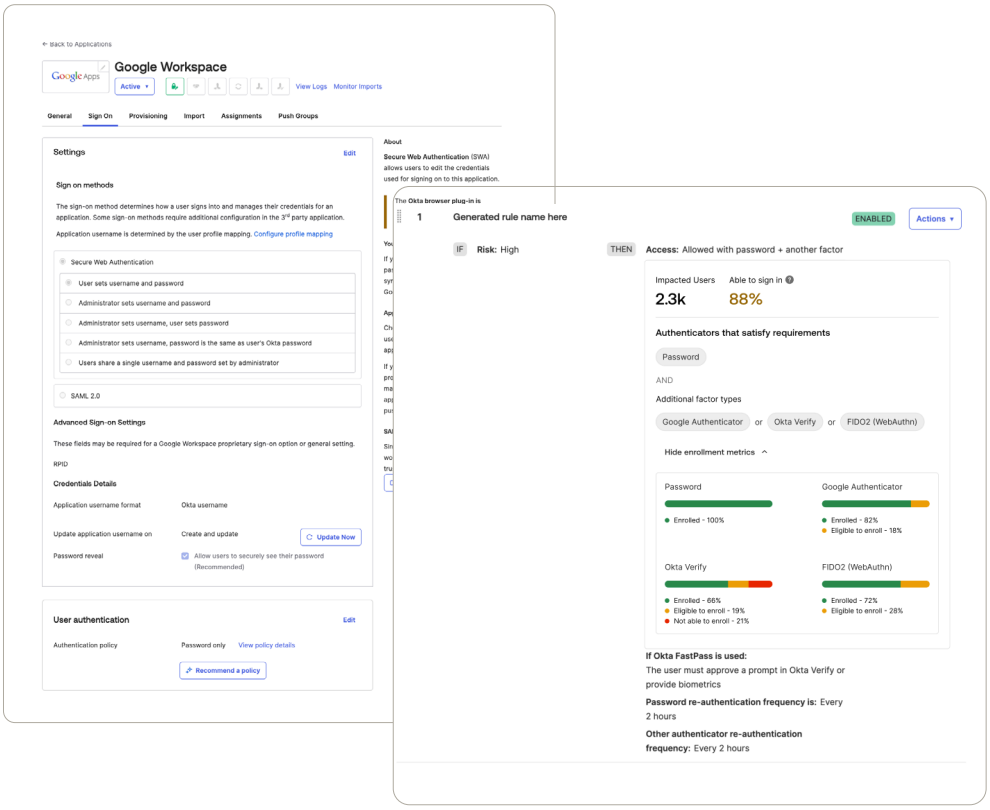
AI の役割：Okta の顧客ベースのポリシー構成データを調査し、ベストプラクティスを抽出し、Okta 環境内で直接適用できる機械可読ポリシーを生成する

アイデンティティインフラストラクチャは、組織の IT 環境全体（さらにはサードパーティのアプリケーションまでも）を広大な網の目のように相互接続しています。そのため、こうした大規模なシステムの構成と管理が複雑化し、時間、エネルギー、専門知識を投入することが必要となります。

同時に、特に Slack、Salesforce、GitHub のように広く利用されているアプリケーションでは、異なる組織が同じ管理シナリオの多くに遭遇し対処しています。このように経験を共有することで、「群衆の英知」を生かす機会が創出されます。

Okta AI を活用した Policy Recommender は、Okta の顧客ベース全体から集約・匿名化された洞察を活用します。これにより、管理者は、Okta Integration Network（OIN）アプリを管理するためのポリシーの推奨と洞察（ポリシーの変更によってどれだけのユーザーが影響を受けるか、ポリシーの適用前に影響をプレビューするなど）を利用して、以下のようなメリットを享受できます。

- 遭遇した問題への理解を深め、簡単に解決する
- 自信を持って、適切な機能に適切な構成と設定を適用する
- 最終的に、セキュリティ、効率、ワークフォースの生産性を向上させる



Customer Identity Cloud（CIC）におけるAI

Accenture は、「Technology Vision 2023」レポートで次のように述べています。**「オンラインで顧客のアイデンティティを認証する能力は、経営幹部の最優先事項となっていると見られ、85%が『戦略的なビジネスの急務になりつつある』と回答している。また、4人に3人は、トランザクションの放棄やユーザーの不満などの顧客認証の課題が、自社の収益に悪影響を及ぼしていると回答している」**

カスタマーアイデンティティおよびアクセス管理（CIAM）は、文字どおりの定義においては変化していません。しかし、特に近年、どのようなユースケースで、どのような機能コンポーネントを使用し、どのようなタイプの組織に対応するのかという点において、真の意味が進化しています。今日、CIAM は以下のために不可欠な存在となっています。

- コンシューマーへのサービス：B2C（コンシューマーとの取引）では、CIAM の効果的な導入によって、企業が高度にパーソナライズされたプロモーションやレコメンデーションを提供できるようになる。これが、さらなる収益の向上と顧客への価値創出を実現すると同時に、複数のデジタルチャネル全体で利便性の高いユーザーエクスペリエンスを確保する。
- 企業顧客の支援：数え切れないほどの組織にとって、B2B（企業間取引）の SaaS アプリケーションはビジネスに不可欠なものとなっている。しかし、組織内のさまざまなユーザーは、さまざまなリソースに異なるレベルでアクセスする必要がある。アイデンティティとアクセス権限を厳格に管理しなければ、利便性と安全性の高いエクスペリエンスを実現できない。CIAM は、B2B で SaaS の顧客が自らアイデンティティを管理できるように支援することで、解決策を提供する。

Okta は、Customer Identity Cloud で AI を採用した当初、顧客向けアプリケーションが広範な脅威に直面しているという単純な理由から、セキュリティに重点を置きました。しかし、ワークフォースアイデンティティの保護に役立つ同じアプローチを、カスタマーアイデンティティにも同じように適用できるとは限りません。企業環境では、セキュリティが利便性よりも優先されることが多いため、管理者はユーザーエクスペリエンスをあまり考慮せずに制御を課すことができます。

対照的に、カスタマーアイデンティティ管理では、摩擦を最小限に抑えながらセキュリティとプライバシーを維持しなければなりません。そのためには、高度な脅威に耐えながらユーザーの目にほとんど触れないような防御を設計する必要があります。

幸い AI は、正当なユーザーを装った攻撃者と、正当なユーザーを見分ける能力が非常に高いことが証明されています。

Okta AI の新しいセキュリティ機能の他にも、機械学習と生成 AI を活用した最新の能力が、カスタマーエクスペリエンスの強化、コンバージョンの向上、管理の簡素化を実現します。

ボット検知

AI の役割：60 以上のシグナルを調査し、どのような場合に認証要求が正当なアカウント所有者ではなくボットからのものであるかを予測する

Customer Identity Cloud の攻撃保護アドオンで重要となるボット検知機能は、ネイティブアプリケーション、パスワードレスのフロー、カスタムログインページに対するスクリプト攻撃（クレデンシャルスタッフィング攻撃、リストバリデーション攻撃など）を軽減します。

ボット検知は、IP アドレスに関連する過去のイベント、最近のログイン履歴、IP レピュテーションデータなど、60 以上の多様なデータソースを分析することで、アイデンティティ要求がボットからのものである可能性を予測します。一定の予測 / 信頼度のしきい値を超えると、認証フローは CAPTCHA などの対抗策を提示します。

ボット検知は、AI が従来の手法を大きく改善できることを示す一例です。

- 2021年2月に導入された最初のバージョンは、ルールベースであり、18% のボットを検知した
- 2021 年 8 月に登場したバージョン 2 は、行動分析に機械学習を採用した。この AI を活用したアプローチにより、ボットの 45% を検知し、効果が 2 倍以上に高まった
- 2022 年 6 月に提供が開始された最新バージョンは、ボットの 79% を検知し、攻撃者が絶えず手法を改良しているにもかかわらず、これまでで最高のパフォーマンスを実現した

重要なことは、このような防御能力が、ユーザーに不必要な摩擦を引き起こさずに達成されたという点です。ボット検知機能の中核を成す AI を慎重に訓練し、継続的に調整することで、人間のユーザーに CAPTCHA がほとんど表示されないようになります。

さらに、ボット検知前後の効果を検証する詳細な内部調査では、以下のような強力な抑止効果が明らかになりました。

- ボット検知を有効にした顧客では、悪意あるトラフィックが平均 40% 以上減少した
- 大規模な顧客で、ボットのトラフィックが 90% 近く減少したケースもあった

ボット検知の構築：アイデンティティ脅威レベル（ITL）

2023 年 4 月、Okta はアイデンティティ脅威レベル（ITL）のイニシアチブを少しだけ紹介しました。Okta は、毎月何十億ものログイントランザクションを保護する CIAM ソリューションでアプリケーションの「正面玄関」として機能することから、独自の有利な見地でアイデンティティ脅威を監視できます。

この強力な視点が ITL の起源であり、トラフィックが CAPTCHA に失敗する確率を示すことで、ボットの活動の推定レベル（0 ～ 10 のスコア）を明らかにします。スコア 0 は、ボットの活動がほとんどないことを意味し、スコア 10 は、ほぼすべてのトラフィックがボットに起因する可能性が高いことを意味します。

顧客ベース全体の観測結果を匿名で集約することで、さまざまな業界や地域の ITL を計算でき、その他の共通属性をさらに細かく分割するオプションも利用できます。たとえば、ITL は以下のような推定を提供できます。

- さまざまな業界や地域で、CIC の顧客に対する悪質なトラフィックがどのように変化してきたと考えられるか
- CIC の顧客に対する悪質と思われるトラフィックのレベルが、業界や地域によってどのように異なるか

過去のトレンドや日々の変化を追跡することで、CIAM のログインやサインアップのフローにリスクが高まっていることを把握できる可能性があります。アプリのプロバイダーはこれを利用して、独自の監視を強化する、しきい値を予防的に強化する、追加の防御策を導入するなど、適切に対処できるようになります。

そのための土台となるのがボット検知です。

アダプティブ MFA

AI の役割：幅広いアイデンティティシグナルを分析することで、認証試行が正当なユーザーによるものか、正当なユーザーを装った攻撃者によるものかを予測して、重要なリスクコンテキストを提供する

アダプティブ MFA は、顧客のログイン行動に適応しながら、ビジネスのニーズに沿ったインテリジェントなアクセスを提供します。

MFA はアカウント乗っ取りに対する実績のある防御策ですが、多くの企業（特に B2C）は、摩擦が増えてユーザーエクスペリエンスが損なわれることを懸念し、利用を敬遠しています。

アダプティブ MFA は、ログインが危険と判断された場合にのみ MFA チャレンジを提示し、それ以外の状況ではシームレスなエクスペリエンスを維持することで、魅力ある代替手段を提供します。

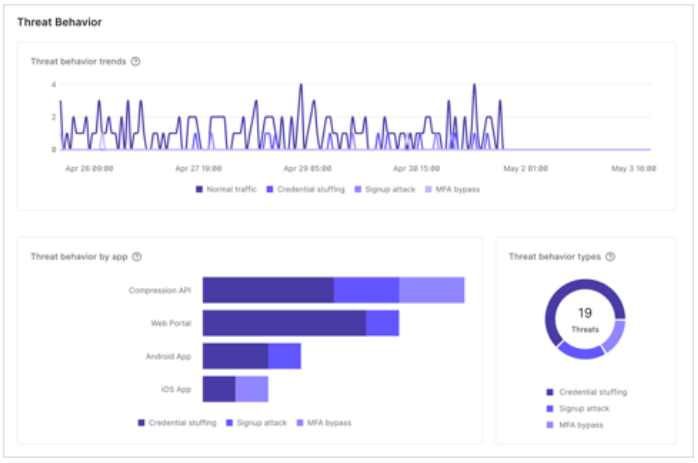
セキュリティの推奨事項

近日提供予定

AI の役割：テナントのセキュリティ態勢を改善するためのインテリジェントな推奨事項を提供する

セキュリティセンターは、IT やセキュリティの担当者が潜在的な攻撃のトレンドを把握して、リアルタイムで迅速に対応できるように、以下の機能を提供します。

- 認証イベント、潜在的インシデント、脅威対応の有効性に関する表示を合理化する
- 異常検知の指標をリアルタイムで通知する
- 潜在的な攻撃トレンド（クレデンシャルスタッフィング、サインアップ攻撃、MFA バイパス試行など）を視覚化する
- 攻撃保護機能（レート制限、CAPTCHA など）がユーザーエクスペリエンスに与える影響について洞察を提供する



これらの能力は、セキュリティのスナップショットアラートやダッシュボード通知を通じて配信される、インテリジェントな ML 駆動によるセキュリティの推奨事項によって拡張されます。

Okta AI を活用した Identity Flow Optimizer

2024 年第 4 四半期に限定早期アクセス

AI の役割：認証データを分析して、カスタマーエクスペリエンスを改善し、コンバージョンを高める方法を提案する

顧客向けビジネスにおいて、「摩擦」は人とサービスのインタラクションを遅らせる、あらゆる手間やストレスを指します。これらのインタラクションには、以下をはじめとするユーザーのアクションが含まれます。

- 自社のサービスに登録する
- ユーザー自身の既存アカウントにログインする
- ユーザー自身の情報や好みを更新する
- アカウントデータを失った場合に復元する
- チェックアウト（購入手続きを完了）する

摩擦が大きければ大きいほど、コンバージョンが低下し、短期的にも長期的にも収益が減少します。しかし、手作業による顧客フローの最適化は、膨大なデータが関与し、多様なユーザーが非常に個人的な嗜好を持つため、非常に困難です。

さらに、アイデンティティフローの保護は、常に優先させる必要があるとは言え、専門家にとって相変わらず難しい取り組みであり、アイデンティティを初めて扱う開発者にとってはなおさら困難です。

こうした課題に対処するため、Identity Flow Optimizer がインラインで提供するアイデンティティの構成とアクションに関する推奨情報を利用することで、開発者はコンバージョンを高め、セキュリティを向上させ、アプリの構築を迅速化できます。

Okta AI を活用した Brand Customizer

2024 年第 4 四半期に限定早期アクセス

AI の役割：組織のブランディングに合わせたデザインテンプレートを自動的に作成 / 表示する

ブランドが厳格なデザインガイドラインを設けているのには理由があります。入念に吟味されたブランドのアイデンティティを積極的に強化する一貫したユーザーエクスペリエンスを提供するためです。

Brand Customizer は、1 ページのテンプレートをデザインし、他のすべての必要なテンプレートにデザインを適応させることができます。開発者がスクリーンショットやロゴを提供すると、AI がテンプレートを作成し、開発者はこれを必要に応じてカスタマイズできます。

このアプローチは、エンドユーザーに一貫したルック&フィールを提供するだけでなく、開発者が優れたカスタマーエクスペリエンスを簡単かつ迅速に構築し、迅速なイノベーションを実現し、ビジネスの拡張に貢献することで、価値実現までの時間を短縮します。

Okta AI を活用した Guide

2024 年第 4 四半期に限定早期アクセス

AI の役割：ユーザーが効果的かつ効率的に Customer Identity Cloud を使用できるよう、平易な言葉で作成したプロンプトを解釈し、コンテキストに応じた支援を提供する

Customer Identity Cloud は強力で、機能が充実し、高度に拡張可能です。しかし、その能力の広さと深さは、新規のユーザーにはとっつきにくく、専門家でも細部まで熟知し、新しい能力を使いこなすことは容易ではありません。

新しいユーザーがすぐに CIC を使い始められるように、またどんなユーザーでも CIC を最大限に活用できるように、Guide は以下の機能を提供します。

- 平易な英語のプロンプトで包括的なオンボーディング支援を提供し、ユーザーが実行すべき最良のステップを直感的に提示することで、最も価値のあるワークフローへとシームレスに誘導する
- プラットフォームの設定や専門用語をわかりやすい言葉で説明し、コンテキストに応じた支援や関連ドキュメントへの適切なリンクを提供して、エクスペリエンスを強化する

Okta AI を活用した Actions Navigator

2024 年第 2 四半期に限定早期アクセス

AI の役割：適切なインテグレーションを簡単に見つけるための平易な言語による検索を可能にし、必要に応じてユーザーが新しいインテグレーションを開発できるように支援する

拡張性は Customer Identity Cloud の中核となる能力であり、Auth0 Marketplace は開発プロセスを簡素化するため、アイデンティティアプリケーションにインテグレーションを追加する簡単な方法を提供します。

しかし、何百ものインテグレーションの中から必要なものを正確に見つけるのは、時として困難です。

Actions Navigator により、開発者は検索プロンプトで質問するだけで、マーケットプレイスのインテグレーションを見つけて実装したり、アクション（CIC の能力をカスタマイズして拡張するための機能）を作成したりできます。コード生成は、生成 AI の最も革新的な用途のひとつであり、この機能は、開発者にとっても、自分でコードを書いた経験のない人にとっても、新しい能力を解き放つものとなります。

Okta AI を活用した Tenant Security Manager

2024 年第 2 四半期に限定早期アクセス

AI の役割：複雑なアイデンティティ構成をわかりやすく要約する

多くの組織には、アイデンティティを含む特定のシステムに関する貴重な組織知を持つ領域専門家がいます。

他の部署への異動や離職などにより、こうした専門家を利用できなくなると、システムの状態や構成の詳細を他の人が理解することが非常に難しくなります。

Tenant Security Manager は、セキュリティのスナップショットアラートとダッシュボード通知によるインテリジェントなセキュリティの推奨事項を付加して Okta の攻撃保護の能力を強化することで、テナントのセキュリティ態勢を改善します。

まとめ

ChatGPT の突然の登場と、それに呼応する同様に印象的なツールの急増は、最先端のテクノロジーが急速に変化していることを示しています。その波及効果は非常に多様であるため、AI とその影響について具体的な予測を立てるのは無意味でしょう。

しかし、はっきりしていることもあります。たとえば、AI、特に生成 AI の影響について言えば、Forrester のプレスリリースの見出しが的を得ています。つまり、「生成 AI を無視することは、企業にとって大きな過ちとなる」のです。

別の見方をすると、AI への投資の効果が正確にはわからないかもしれませんが、確かなのは、投資をしないことで競争が不利になるか、下手をすると存在意義を失いかねないということです。それほど大きなパラダイムシフトが起きています。

Okta は、AI 分野の研究開発に力を入れ、膨大な IAM データセットを活用することで、AI が可能にする革新的な能力を通じて、Workforce Identity Cloud と Customer Identity Cloud の両方でセキュリティ強化、生産性向上、ユーザーエクスペリエンス改善を実現していきます。

この投資がどのような実を結ぶのか、まだ正確にはわかりません。しかし、将来振り返ったときに、現在および進行中の能力が変革の道のりの第一歩であったと理解できると確信しています。

免責事項

本資料および本資料に含まれる推奨事項は、法律、プライバシー、セキュリティ、コンプライアンス、またはビジネスに関する助言ではありません。本資料は、一般的な情報提供のみを目的としており、最新のセキュリティ、プライバシー、法律の動向、また関連する問題をすべて反映していないことがあります。本資料の利用者は、自身の責任において、自身の弁護士またはその他の専門アドバイザーから法律、セキュリティ、プライバシー、コンプライアンス、またはビジネスに関する助言を得るものとし、本書に記載された推奨事項に依存すべきではありません。本資料に記載された推奨事項を実施した結果生じるいかなる損失または損害に対しても、Okta は責任を負いません。Okta は、これらの資料の内容に関して、いかなる表明、保証、またはその他の保証も行いません。お客様に対する Okta の契約上の保証に関する情報は、okta.com/agreements をご覧ください。

本資料で言及される現時点で提供されていない製品、特性または機能は、予定通りに提供されない、またはまったく提供されない可能性があります。製品ロードマップは、製品、特性または機能の提供に対する言質、義務、または約束を表すものではなく、これらに基づいて購入の意思決定を行うべきではありません。

Okta について

Okta は、世界を代表するアイデンティティ企業です。独立系の主要アイデンティティパートナーとして、すべての人が、場所やデバイス / アプリを問わず、どんなテクノロジーでも安全に利用できるように支援しています。世界で最も信頼されるブランドが Okta を信頼し、安全なアクセス、認証、自動化を実現しています。Okta が提供する Workforce Identity Cloud と Customer Identity Cloud は、柔軟性と中立性を中核に据え、カスタマイズ可能なソリューションと 7,000 以上の事前構築済みの統合を提供しています。これにより、ビジネスリーダーや開発者はイノベーションに集中し、デジタルトランスフォーメーションを加速させることができます。Okta は、アイデンティティを積極的に管理できる世界を作っています。詳しくは okta.com/jp/ をご覧ください。