Livre blanc

Okta et l'IA

Comment l'intelligence artificielle redéfinit la gestion des identités et des accès (IAM)

Sommaire

Résumé

L'intelligence artificielle (IA) redéfinit le mode de fonctionnement des entreprises et stimule la création de produits et services innovants en simplifiant l'optimisation, l'analyse des données, la détection des anomalies et d'autres opérations basées sur la prédiction. La plupart de ces fonctionnalités ne datent pas d'hier, mais la réduction des coûts et l'amélioration des performances offertes par l'IA permettent désormais de les intégrer à n'importe quel environnement ou presque.

L'élément neuf, par contre, a été l'essor extraordinaire et soudain de l'IA générative, qui s'explique par les progrès rapides des grands modèles de langage (LLM) au sein d'applications telles que ChatGPT et DALL-E d'OpenAI, Bard de Google et Code Llama de Meta.

Nous sommes convaincus que l'IA générative représente un changement de paradigme majeur, dont nous commençons à peine à ressentir les effets, sans pouvoir encore les appréhender pleinement.

En outre, l'identité est un domaine particulièrement propice à l'utilisation de l'IA. Non seulement l'identité est complexe (ce qui ouvre de nombreuses perspectives d'optimisation par l'IA), mais les flux et transactions d'identité produisent d'énormes quantités de données, qui constituent fondamentalement le carburant des moteurs d'IA. Et si nous aspirions à tirer parti des effets de réseau des données sur l'ensemble du domaine de l'identité, à court terme, nous concentrons nos investissements en recherche et développement sur trois axes :

- Renforcement de la sécurité
- Amélioration de la productivité
- Optimisation des expériences utilisateurs

Bien évidemment, l'intelligence artificielle est loin de constituer une nouveauté pour l'équipe Okta, et nous l'avons d'ores et déjà adoptée dans plusieurs domaines clés. Par exemple :

- Okta Workforce Identity Cloud (WIC) intègre l'IA dans les fonctionnalités ThreatInsight, Adaptive Multi-Factor Authentication (Adaptive MFA) et Anti-Toll Fraud.
- Okta Customer Identity Cloud (CIC) utilise l'IA dans les fonctionnalités Bot Detection, le score Identity Threat Level (ITL) qui y est associé et Adaptive MFA.

Lors de l'événement Oktane 2023, nous avons annoncé un certain nombre de nouvelles fonctionnalités basées sur l'IA. Okta AI dote WIC de quatre nouvelles fonctionnalités pour :

- Renforcer la sécurité : Identity Threat Protection
- Faciliter la gouvernance : Governance Analyzer
- Simplifier l'administration : Log Investigator, Policy Recommender

CIC bénéficie de six nouvelles fonctionnalités pour :

- Renforcer la sécurité des tenants : Security Recommendations
- Améliorer l'expérience client et augmenter les revenus : Funnel Conversion Recommendations, Brand Customization
- Simplifier l'administration : Co-Pilot, Action Selection and Development, Personalized Tenant Configuration Summary

Nous favorisons également une culture de l'innovation, notamment en organisant deux hackathons par an au sein de l'entreprise. Bon nombre des idées explorées lors de ces hackathons aboutissent au dépôt d'un brevet et à la réalisation de POC, avant de se concrétiser sur le marché sous l'une ou l'autre forme. Soulignons que lors d'un récent hackathon, 25 % des projets étaient axés sur l'expérimentation de l'IA, et nous sommes séduits par leur potentiel.

Reconnaissant l'importance de l'IA et l'enthousiasme qu'elle génère parmi les rangs des développeurs, nous avons également organisé notre tout premier hackathon entièrement dédié à l'IA.

Nous aidons nos clients à créer des expériences agréables et élégantes à l'aide des LLM, et l'écosystème Okta étendu – Okta Ventures, Okta Integration Network, Auth0 for Startups et Auth0 Marketplace – offre un vaste réseau de solutions d'IA qui peuvent être intégrées à nos offres.

L'avenir ne manquera pas de défis : les cybercriminels tirent déjà parti de l'IA en général, et des LLM en particulier, pour explorer de nouveaux vecteurs d'attaque et rendre les attaques existantes encore plus dangereuses. Quoi qu'il en soit, nous restons persuadés que l'IA peut être et sera une force au service du bien commun.

Aujourd'hui, les identités numériques contrôlent l'accès à un nombre croissant d'applications et de services. À ce titre, elles ont un impact considérable sur de nombreux aspects de la vie moderne. Cet impact ne fera que grandir à l'avenir : l'authentification, l'autorisation et l'identité en général deviendront des éléments essentiels au maintien de la confiance et de la sécurité, et le socle d'expériences utilisateurs optimales.

Nous avons à cœur d'exploiter la puissance de l'IA pour renforcer les liens entre les personnes, les technologies et les communautés.

Introduction

Ces derniers mois, les médias généralistes et spécialisés en technologies ont publié d'innombrables articles sur les percées de l'intelligence artificielle (IA) et les applications – certaines attendues, d'autres imprévues – rendues possibles par ces avancées.

Comme le disait Andy Grove, « seuls les paranoïaques survivent ». Il n'est dès lors pas surprenant que les entreprises, de toutes tailles et tous secteurs, s'empressent de tirer parti de l'IA afin d'améliorer les solutions existantes, d'en créer de nouvelles et de gagner un avantage en creusant l'écart avec la concurrence.

Dans une large mesure, notre investissement dans l'IA émergente ne nous change pas de nos activités habituelles. L'IA optimise déjà bon nombre de produits et fonctionnalités phares de notre portefeuille. Plus particulièrement, le machine learning (ML) est au cœur de nos évaluations dynamiques des risques et de nos informations d'authentification basées sur les risques.

Riches de notre longue expérience de terrain, nous ne considérons pas l'IA comme une fonction ou un module distinct, une technologie que l'on viendrait simplement greffer à notre plateforme. Au contraire, nous savons que l'IA est une technologie généraliste (ou, plus précisément, un ensemble de technologies généralistes) au mieux de ses performances lorsqu'elle est étroitement intégrée à une infrastructure d'identités.

Dans ce livre blanc, nous levons le voile sur la relation d'Okta avec l'IA, en nous penchant sur les points suivants :

- Pourquoi l'IA promet de bouleverser et de redéfinir pratiquement tous les domaines de l'univers numérique
- Pourquoi l'identité est particulièrement bien positionnée pour tirer parti de l'IA
- Les principales propositions de valeur que nous entrevoyons pour l'IA dans un avenir proche
- Comment nous appliquons déjà l'IA dans Okta Workforce Identity Cloud (WIC) et Okta Customer Identity Cloud (CIC)
- Comment nous utilisons Okta AI dans le cadre des nouvelles fonctionnalités de WIC et de CIC

Pourquoi l'intelligence artificielle ?

À un niveau élémentaire, l'intelligence artificielle (IA) peut être considérée comme une décision prise par un ordinateur et dont « l'intelligence » la rend impossible à distinguer d'une décision humaine, indépendamment de la manière dont la décision est prise.

Si le concept de l'IA a été officiellement défini lors du Dartmouth Workshop, l'idée de départ remonte à 1943, lorsque le logicien Walter Pitts et le neuroscientifique Warren McCulloch tentèrent de créer une représentation mathématique des neurones d'un cerveau humain. Ces avancées contemporaines sont fondées sur l'ensemble des progrès de la théorie du calcul, d'Ada Lovelace au XIXe siècle à Alan Turing.

Depuis les années 1960, l'IA a évolué pour englober de très nombreux algorithmes, y compris la détection et la reconnaissance de modèles, généralement assurées par le machine learning (ML). Le domaine du machine learning a progressé de manière spectaculaire au cours des 15 dernières années, ce qui a permis l'émergence du deep learning, ou apprentissage profond, pratique et économique.

L'IA générative représente un changement de paradigme majeur

L'évolution de l'IA qui a le plus marqué les esprits, certains diront même secoué le grand public, est l'apparition et les progrès rapides de l'IA générative, principalement grâce à des avancées remarquables dans les grands modèles de langage (LLM).

Optimisées par les LLM, des applications telles que ChatGPT et DALL-E d'OpenAI ont porté l'IA à l'attention du grand public, notamment en raison de ses capacités à imiter l'être humain et de l'absence de transparence concernant les données ingérées par le modèle (qui influencent son comportement).

Soudain, la rédaction en prose et la création d'images complexes (et réalistes, si tel est le but recherché) ne sont plus l'apanage des seuls humains. De plus, comme les LLM maîtrisent bien l'écriture, y compris la programmation, et que beaucoup de choses sont aujourd'hui contrôlées par logiciel, ils sont à l'origine de percées et d'avancées inattendues dans un grand nombre de domaines.

Il ne fait aucun doute que nous sommes entrés dans une nouvelle ère de l'intelligence artificielle. Il est naturel de se demander comment mettre à profit ses fonctionnalités – anciennes, récentes et émergentes.

Que peut faire l'intelligence artificielle ?

Dans leur ouvrage *Prediction Machines*, les économistes Ajay Agrawal, Joshua Gans et Avi Goldfarb recadrent l'essor de l'IA en le présentant comme une baisse du coût de prédiction, qu'ils définissent comme l'utilisation d'informations disponibles pour en générer de nouvelles.

Étant donné que la prédiction « est au cœur de la prise de décisions dans l'incertitude » et que « nos vies professionnelles et personnelles sont truffées de telles décisions », la diminution du coût de prédiction s'accompagne d'un potentiel incroyable. Pour donner quelques exemples, la notion de prédiction est un composant essentiel des domaines suivants :

- Optimisation – Utilisation du contexte et des observations antérieures pour prédire une voie à suivre, une réponse, une configuration, une conception d'interface utilisateur, etc.
- Analyse comportementale – Observation du comportement en temps réel dans le contexte d'actions historiques pour prédire les intentions d'un utilisateur.
- Data mining – Prédiction des données et informations qui répondent le mieux à la requête ou à l'invite d'un utilisateur. (Il convient de noter que la prédiction est également au cœur des LLM et de l'IA générative.)

Comme l'informatique classique, l'IA (sous toutes ses formes) est une technologie généraliste qui promet de bouleverser et de révolutionner un certain nombre de secteurs d'activité. Nous sommes particulièrement optimistes en ce qui concerne son potentiel à stimuler l'évolution de l'identité.

Intelligence artificielle et identité

Une identité numérique est une série d'attributs définissant un utilisateur donné dans le contexte d'une fonction fournie par une application spécifique. Aujourd'hui, les identités numériques contrôlent l'accès à un nombre croissant d'applications et de services. À ce titre, elles ont des répercussions considérables sur de nombreux aspects de la vie moderne. Cet impact ne fera que grandir à l'avenir : l'authentification, l'autorisation et l'identité en général deviendront des éléments essentiels au maintien de la confiance et de la sécurité, et le socle d'expériences utilisateurs optimales.

Par conséquent, les services IAM sont les pierres angulaires de notre monde connecté. Ils permettent que seuls les utilisateurs autorisés (collaborateurs, prestataires, partenaires, clients) peuvent accéder à des ressources particulières. Conceptuellement, l'IAM est très simple : un utilisateur prouve son identité et est autorisé à accéder à une ressource pour laquelle il dispose des droits requis. Mais en pratique, plusieurs facteurs compliquent les choses :

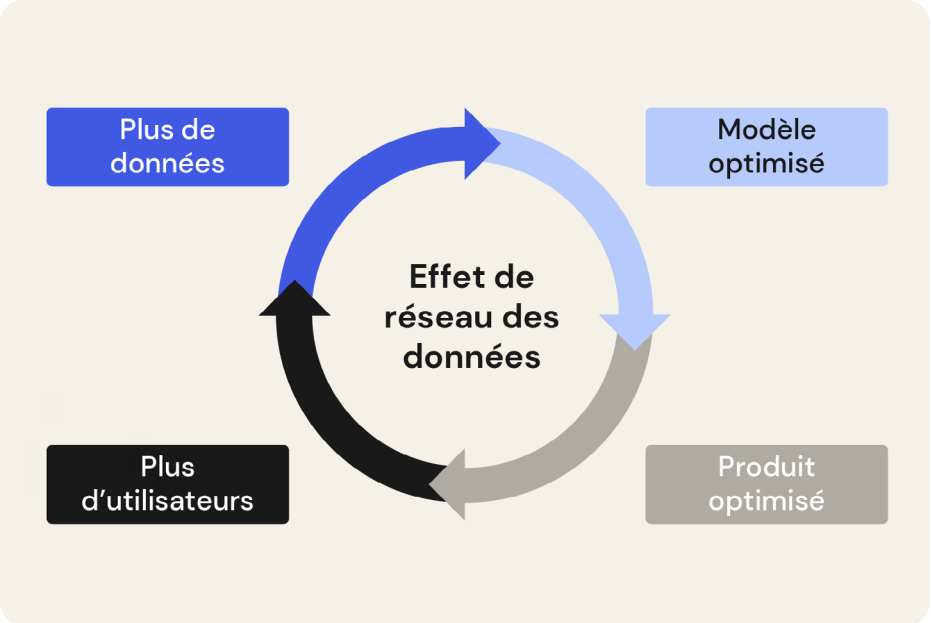
- Le monde numérique actuel inclut de nombreux utilisateurs, chaque utilisateur peut posséder de nombreuses identités numériques, et il existe d'innombrables manières d'exprimer une identité numérique.
- Chaque identité numérique dispose de droits et d'autorisations différents sur les ressources, et ces droits et autorisations sont de plus en plus dynamiques.
- Alors que les périmètres de sécurité tendent à s'estomper, les cybercriminels concentrent leurs efforts sur l'identité.

Comme nous l'avons constaté, l'IA est parfaitement capable de gérer la complexité et l'incertitude, à condition de disposer de suffisamment de données.

Heureusement, le domaine de l'identité ne manque pas de données, car l'identité elle-même a évolué : d'attribut unidimensionnel statique, elle est devenue une interaction continue et dynamique, redessinée par chaque nouveau point de données. Cette évolution n'aurait pas été possible sans la transformation cloud que nous avons traversée, et se poursuivra grâce à la transformation de l'IA actuellement en cours.

Tirer parti de l'effet de réseau des données

Une conséquence importante de cette évolution est qu'elle permet un cycle vertueux d'effets de réseau des données : plus le volume et la qualité des données auxquelles un modèle d'IA a accès sont élevés, plus le modèle peut apprendre rapidement et plus ses prédictions ou décisions deviennent précises. La valeur ajoutée du produit ou service pour ses utilisateurs est ainsi accrue, ce qui attire davantage d'utilisateurs, qui génèrent alors plus de données, qui peuvent venir alimenter le modèle selon un cycle vertueux :



1. **Plus de données –** Plus un produit ou service est utilisé, plus le volume de données générées par les interactions des utilisateurs, les transactions, les feedbacks, etc. est élevé.
2. **Modèle optimisé –** Ces données permettent d'affiner le modèle d'IA sous-jacent. Plus le volume et la qualité de données sont élevés, plus les prédictions ou les décisions du modèle deviennent précises.
3. **Produit optimisé –** À mesure que le modèle d'IA s'améliore, le produit ou service se perfectionne également.
4. **Plus d'utilisateurs –** Le produit ou service optimisé attire plus d'utilisateurs, qui génèrent encore plus de données, ce qui permet au cycle de continuer.

Cette boucle autoalimentée peut être un puissant levier d'innovation et de différenciation concurrentielle.

L'évolution du paysage des menaces a poussé Gartner à tirer la sonnette d'alarme : **« D'ici 2025, les attaques basées sur l'IA générative contraindront les entreprises soucieuses de leur sécurité à abaisser les seuils de détection des activités suspectes, générant ainsi plus de fausses alertes, ce qui nécessitera une intervention humaine plus importante. »**

[1] Gartner, 4 Ways Generative AI Will Impact CISOs and Their Teams, Jeremy D'Hoinne, Avivah Litan, Peter Firstbrook, 29 juin 2023. GARTNER est une marque déposée et une marque de service de Gartner, Inc. et/ou de ses sociétés affiliées aux États-Unis et dans le monde. Cette marque est utilisée ici avec autorisation. Tous droits réservés.

Renforcer la sécurité

Aujourd'hui, il est largement admis que l'IA peut :

- rendre les attaques existantes ciblant l'identité, comme le credential stuffing et le phishing, plus dangereuses (plus difficiles à détecter, plus efficaces, plus dévastatrices, etc.) ;
- favoriser l'apparition de tout nouveaux types d'attaques ciblant l'identité, dont beaucoup ne deviendront apparentes que lorsqu'elles seront identifiées sur le terrain ;
- contourner certaines des mesures de sécurité existantes (p. ex. résoudre les CAPTCHA ou piéger les systèmes biométriques vocaux).

Par ailleurs, les capacités de codage et de création de scripts de l'IA générative permettent aux cybercriminels de lancer plus facilement des attaques, quel que soit leur niveau de compétence (notamment en programmation), ce qui pourrait attirer davantage de prétendants dans l'écosystème de la cybercriminalité et améliorer leur efficacité opérationnelle.

Si l'IA aidera sans aucun doute les cybercriminels, elle permettra aussi de doper les capacités des équipes de sécurité.

Okta est déjà un leader du secteur avec l'authentification résistante au phishing de FastPass, compatible avec n'importe quelle plateforme pour les terminaux gérés et non gérés, et permet aux développeurs d'adopter facilement l'authentification FIDO2 conviviale et résistante au phishing. Nous reconnaissons cependant la nécessité d'utiliser l'IA pour :

- **Renforcer la sécurité d'Okta dès la conception –** Tout comme les cybercriminels, les entreprises telles qu'Okta peuvent utiliser l'IA pour détecter les vulnérabilités et les failles de sécurité. Nous avons l'avantage de pouvoir tirer parti de l'IA pour renforcer la sécurité des logiciels et des systèmes avant même leur sortie.
- **Automatiser la détection des menaces –** L'analyse contextuelle et comportementale est déjà capable d'éclairer les évaluations des risques intelligentes et de détecter les menaces avancées ciblant l'identité. Les progrès de l'IA ne feront qu'améliorer notre capacité à exécuter ces fonctions et à en introduire de nouvelles.
- **Réduire les risques pour nos clients –** Qu'il s'agisse d'automatiser les mesures de défense (telles que les actions de confinement ou le blocage des activités malveillantes), d'associer une série d'actions recommandées à une alerte ou de soutenir des initiatives de gouvernance, gestion des risques et conformité (GRC), l'IA offrira une aide précieuse pour la réduction des risques et la réponse proactive aux attaques.

Heureusement, nous possédons déjà une grande expérience en la matière, au travers notamment de l'intégration de fonctionnalités de sécurité pilotées par l'IA à Workforce Identity Cloud et à Customer Identity Cloud.

Améliorer la productivité

L'une des principales conclusions du rapport *Le point sur l'adoption des services SaaS par les équipes de développement* publié par Okta en 2023 est qu'il existe fondamentalement deux types d'entreprises de développement : celles qui utilisent déjà l'IA dans l'ingénierie produits (52 %) et celles qui prévoient de le faire dans les 12 prochains mois (45 %).

Dans leur quête de nouveaux avantages, ou facteurs de différenciation (agilité, nouvelles fonctionnalités, réduction des coûts ou encore gain de temps), les entreprises intègrent des outils d'IA pour l'analyse des données, le contrôle qualité, le machine learning, l'automatisation et bien plus encore.

Nous partageons cette vision optimiste du potentiel de l'IA à améliorer la productivité dans notre propre service d'ingénierie.

Parallèlement, nous reconnaissons que l'impact de l'IA devrait s'étendre à tous les membres du personnel de presque toutes les entreprises clientes, quels que soient leur taille et leur secteur d'activité.

Une infrastructure de gestion des identités collaborateurs moderne et mature :

- permet aux collaborateurs, prestataires et partenaires de travailler où ils le souhaitent en bénéficiant d'un accès fluide et sécurisé aux outils et ressources critiques ;
- offre une expérience utilisateur pratique, augmente l'efficacité opérationnelle et réduit la charge d'administration, ce qui libère du temps et de l'énergie à consacrer à la croissance, à l'innovation et à d'autres priorités ;
- permet à l'entreprise d'évoluer et d'améliorer son agilité, quelle que soit sa taille ;
- contribue à préserver l'entreprise contre les perturbations causées par les cybercriminels.

Intégrée à une infrastructure d'identités, l'IA peut renforcer tous ces avantages, et sans doute en offrir de nouveaux.

Optimiser les expériences utilisateurs

Concentrons-nous quelques instants sur la notion de friction.

Dans le cas des entreprises commerciales, les points de friction (c'est-à-dire tout ce qui ralentit les interactions d'une personne avec un service) constituent un obstacle important aux conversions et, par extension, à l'augmentation de leurs recettes. Le rapport Customer Identity Trends Report d'Okta a révélé que près de 60 % des personnes interrogées seraient plus susceptibles de faire appel à une marque dont les services offrent un processus de connexion simple, fluide et sécurisé. Cette constatation s'applique à tous les secteurs d'activité, ce qui suggère que les utilisateurs recherchent la praticité dans toutes leurs interactions.

Bien entendu, un certain degré de friction est nécessaire pour établir la confiance et mettre en œuvre des contrôles de sécurité, mais la réduction des points de friction chaque fois que possible, dans toutes les interactions des consommateurs, peut accroître les taux de conversion et, par conséquent, augmenter les revenus à court et long terme.

Quel est le rôle de l'IA ? Voici trois usages parmi les plus évidents :

- Effectuer une évaluation continue des risques afin de favoriser des expériences sans mot de passe (passwordless) et sans connexion (loginlesss)
- Optimiser les flux d'identité pour le confort des utilisateurs
- Améliorer la conception de l'interface utilisateur (notamment pendant les transactions d'identité) pour le confort des utilisateurs

Sur le lieu de travail, tout élément empêchant ou ralentissant l'accomplissement de tâches peut être considéré comme un point de friction. Si l'identité ne peut pas (à elle seule) démarrer une réunion à l'heure ou encourager un collègue à répondre plus rapidement à une demande, une infrastructure d'identités mature contribue d'autres manières, par exemple :

- en veillant à ce que les utilisateurs puissent accéder aux ressources appropriées (données, systèmes, applications, etc.) avec les privilèges adéquats au bon moment ;
- en fournissant des fonctionnalités en libre-service (p. ex. pour demander l'accès à des ressources, modifier des profils ou activer des facteurs de sécurité) ;
- en automatisant les processus existants (vérifications des accès et certifications, offboarding sécurisé, etc.).

Là encore, l'IA peut doper l'efficacité de ces fonctionnalités existantes, mais aussi offrir de nouvelles perspectives. Par exemple, l'IA peut analyser de nombreux déploiements d'identité et indicateurs de performance pour déterminer les configurations les plus efficaces, et utiliser ces informations pour formuler des recommandations personnalisées à l'intention de chaque entreprise ou service. L'IA peut également aider les administrateurs à trouver rapidement les informations dont ils ont besoin au sein d'un volume astronomique de données opérationnelles et de logs.

En outre, grâce aux fonctionnalités en langage naturel des LLM, même les fonctions davantage axées sur l'identité peuvent devenir accessibles aux personnes sans compétences en codage. Okta Workflows offre déjà une automatisation et une orchestration no-code des identités via une interface par glisser-déposer. Il n'est donc pas irréaliste d'imaginer une solution qui comprendrait les instructions en langage naturel.

L'IA dans Workforce Identity Cloud (WIC)

Auparavant considérée comme un simple service utilitaire gérant les noms d'utilisateur et les mots de passe, l'identité est devenue une nécessité et un facilitateur pour toutes les entreprises modernes. Une infrastructure d'identités est donc une couche interconnectée et fondamentale au sein de l'environnement IT au sens large, qui connecte des utilisateurs et d'autres entités à des systèmes, données et ressources on-premise et dans le cloud.

Par conséquent, la sécurisation de l'identité est un élément essentiel d'une posture de sécurité forte, permettant de lutter contre les utilisations abusives découlant de menaces internes et contre les intrus qui exploitent des identifiants volés.

En plus de contribuer à protéger l'infrastructure de gestion des identités collaborateurs contre les menaces, l'IA est tout à fait capable d'optimiser les activités de gouvernance, notamment en examinant d'énormes volumes de données de configuration pour identifier les risques, recommander des actions correctives et même automatiser de nombreuses tâches courantes et importantes.

De même, la capacité de l'IA à analyser des informations lui permet d'interpréter d'importantes quantités de logs.

L'association de ces fonctionnalités au traitement en langage naturel (NLP) et à l'IA générative transforme d'ores et déjà la façon dont les administrateurs gèrent leur infrastructure d'identités en constante évolution.

Dans son rapport *2022 Trends in Securing Digital Identities*, basé sur une enquête menée auprès de 500 professionnels de l'IAM ou de la sécurité, l'Identity Defined Security Alliance (dont Okta fait partie) a révélé que :

- **84 %** des personnes interrogées ont déclaré que leur entreprise a été victime d'une brèche liée à l'identité au cours de l'année précédente.
- **78 %** ont affirmé qu'une brèche avait eu des conséquences directes sur l'activité.
- **64 %** ont indiqué que la gestion et sécurisation efficaces des identités numériques constitue leur principale priorité (16 %) ou fait partie de leurs trois principales priorités (48 %).

ThreatInsight

Le rôle de l'IA – Prédit si les demandes émanent d'une source malveillante, en fonction des observations et des retours automatisés sur les attaques et les demandes d'authentification de la clientèle d'Okta dans son ensemble.

ThreatInsight est une fonctionnalité de sécurité de base qui détecte et neutralise les attaques de grande envergure basées sur les identifiants (password spraying, credential stuffing et attaques par force brute similaires) qui ciblent les endpoints Okta. Dans la console d'administration Okta, le client peut sélectionner le mode de blocage pour refuser automatiquement les demandes prédites comme malveillantes avant que les cybercriminels ne tentent de s'authentifier, ou le mode de logging pour auditer le trafic malveillant.

Tirant parti de l'effet de réseau des millions de demandes d'authentification effectuées chaque jour dans les milliers d'organisations Okta, ThreatInsight utilise une combinaison d'heuristique (règles statiques) et de machine learning pour observer et extraire des informations des attaques basées sur les identifiants.

Pour chaque adresse IP malveillante connue bloquée en périphérie, Okta observe de nombreux autres événements suspects provenant d'adresses IP dont la malveillance ne peut pas être confirmée avec certitude. L'échec répété de plusieurs tentatives de connexion n'est pas forcément synonyme d'activité malveillante. Cette situation peut notamment se produire lorsqu'un hôtel organise une grande conférence. Dans ce scénario, il est normal que se produisent des dizaines, des centaines, voire des milliers d'échecs de connexion pour plusieurs comptes associés à plusieurs organisations Okta, qui semblent tous provenir de la même source (le réseau de l'hôtel). Bloquer ces adresses IP pourrait bloquer des tentatives d'authentification légitimes, ce qui serait finalement aussi désastreux qu'être victime d'une attaque DDoS.

Pour éviter de tels faux positifs, les adresses IP suspectes sont définies comme des adresses IP impliquées dans des attaques lancées contre les clients Okta. En d'autres termes, seules les adresses IP participant effectivement à des attaques sont ajoutées à la base de données ThreatInsight, dans l'intérêt de tous nos clients.

Il est important de souligner que ThreatInsight utilise une période glissante et que les adresses IP suspectes cessant de présenter des activités douteuses lors de l'évaluation suivante sont éliminées de la base de données.

Adaptive MFA

Le rôle de l'IA – Fournit des informations contextuelles à combiner avec une méthode d'authentification appropriée par la prédiction des risques associés aux événements d'authentification (p. ex. la connexion) et aux actions post-authentification (p. ex. l'accès à une ressource spécifique).

Adaptive Multi-Factor Authentication (AMFA) fournit des renseignements supplémentaires sur les flux d'identité en tenant compte du contexte en constante évolution dans lequel une demande d'authentification est effectuée. En adaptant dynamiquement les politiques de sécurité et d'authentification, la fonction Adaptive MFA peut améliorer simultanément la posture de sécurité et l'expérience utilisateur d'une entreprise.

Par exemple, une politique MFA adaptative peut réduire les points de friction en demandant moins souvent aux utilisateurs d'effectuer une authentification multifacteur lorsqu'ils se connectent via l'authentification unique (SSO) ou un terminal géré ou connu. Toutefois, la même solution MFA adaptative peut demander un facteur d'authentification supplémentaire ou plus sécurisé lorsque le risque associé à une demande est évalué comme étant plus élevé, par exemple une tentative de connexion effectuée à une heure inhabituelle de la journée ou à partir d'un nouveau terminal, ou si un utilisateur connecté tente d'accéder à des ressources ou informations particulièrement sensibles.

Le degré de flexibilité et de contrôle offert par une solution MFA adaptative dépend en grande partie des facteurs MFA disponibles et de la richesse des informations contextuelles intégrées à l'évaluation des risques.

Avec la fonction Adaptive MFA, un agent intelligent examine divers signaux de risque tels que l'ID utilisateur, le terminal, le réseau, l'emplacement, le déplacement, l'adresse IP et les données externes provenant des intégrations de sécurité d'endpoints et de tiers. Au départ de cette analyse, il catégorise les anomalies et applique une authentification basée sur les risques à chaque étape du processus d'authentification, même après la connexion de l'utilisateur (p. ex. pour l'authentification renforcée).

Anti-Toll Fraud

Le rôle de l'IA – Détecte les anomalies et catégorise les risques associés aux tentatives de transactions téléphoniques en fonction de diverses données (adresse IP, préfixe, pays, etc.).

La fraude au partage des recettes internationales (IRSF, International Revenue Share Fraud), également appelée fraude au numéro surtaxé, est un type de fraude où des escrocs génèrent artificiellement un important volume d'appels/SMS internationaux sur des lignes coûteuses. Au vu des coûts élevés associés aux transactions téléphoniques internationales longue distance, la fraude au numéro surtaxé peut avoir un impact financier considérable sur les entreprises qui utilisent les appels téléphoniques et/ou les SMS dans le cadre du flux MFA.

La fonction Anti-Toll Fraud protège les clients tout en fournissant un service téléphonique fiable. Pour cela, elle tire parti de mécanismes de détection complémentaires : un moteur heuristique et plusieurs moteurs de machine learning.

En résumé, chaque transaction se voit attribuer un indice de risque, et les transactions présentant un risque plus élevé sont soumises à des limitations plus strictes du débit. (Pour découvrir comment fonctionnent ces composants et comment ils sont intégrés à la fonction Anti-Toll Fraud, consultez cet article de blog.)

L'introduction des composants de machine learning a permis une amélioration de 20 % de l'efficacité de la détection des transactions frauduleuses.

Identity Threat Protection avec Okta AI

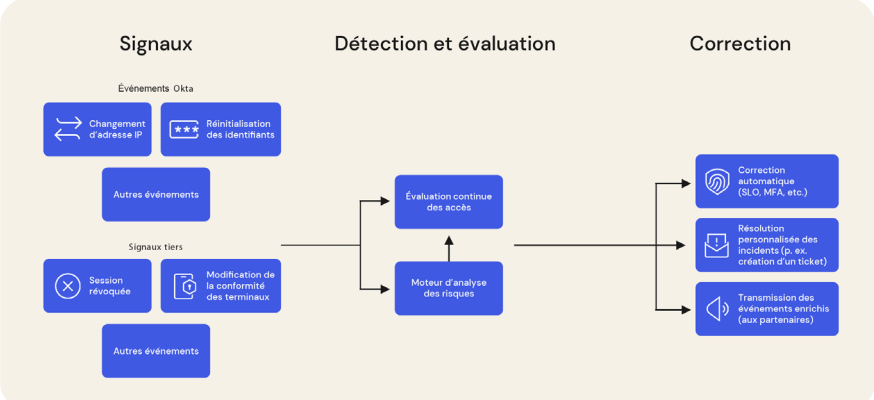
Disponible en Early Access au T1 2024

Le rôle de l'IA – Le modèle de machine learning adapte automatiquement l'analyse des risques à différents contextes, pour des évaluations plus précises et nuancées adaptées aux environnements dynamiques.

Pour se protéger contre les menaces actuelles ciblant l'identité, les entreprises ont besoin d'une approche multiniveau qui commence avant qu'un utilisateur ne s'authentifie et qui se poursuit pendant toute la session. L'authentification continue, en particulier, devrait prendre de l'importance avec la généralisation de l'adoption de techniques d'authentification plus fortes, auxquelles les cybercriminels s'adaptent en allouant plus de ressources au contournement du MFA et au détournement de sessions actives.

Identity Threat Protection avec Okta AI permet de lutter contre les menaces avancées ciblant l'identité grâce à trois fonctionnalités essentielles :

1. **L'évaluation continue des risques** utilise l'IA pour appliquer des politiques de sécurité au moment de la connexion et au cours d'une session utilisateur active, ce qui réduit le risque d'accès non autorisés et de menaces post-authentification telles que le détournement de session.
2. **Le vivier des signaux partagés** renforce la visibilité sur les menaces dans tout l'écosystème technologique, ce qui permet aux équipes de sécurité de détecter et de neutraliser les menaces émergentes avec diverses technologies de sécurité, telles que le MDM (Mobile Device Management), les solutions CASB (Cloud Access Security Broker), la sécurité réseau et les outils EDR (Endpoint Detection and Response).
3. **Les actions adaptatives** répondent aux menaces en temps réel par le biais d'actions ciblées telles qu'Universal Logout, mises en œuvre par des applications prises en charge dans lesquelles la fonctionnalité est activée. Elles invitent les utilisateurs à procéder à une authentification MFA à la demande et exécutent des workflows automatisés pour gérer les risques émergents.



Governance Analyzer avec Okta AI

Disponible en Early Access au T2 2024

Le rôle de l'IA – Ingère un large éventail de signaux d'accès au niveau des terminaux et des utilisateurs, ainsi que d'autres signaux contextuels essentiels pour fournir des informations exploitables sur la gouvernance des identités.

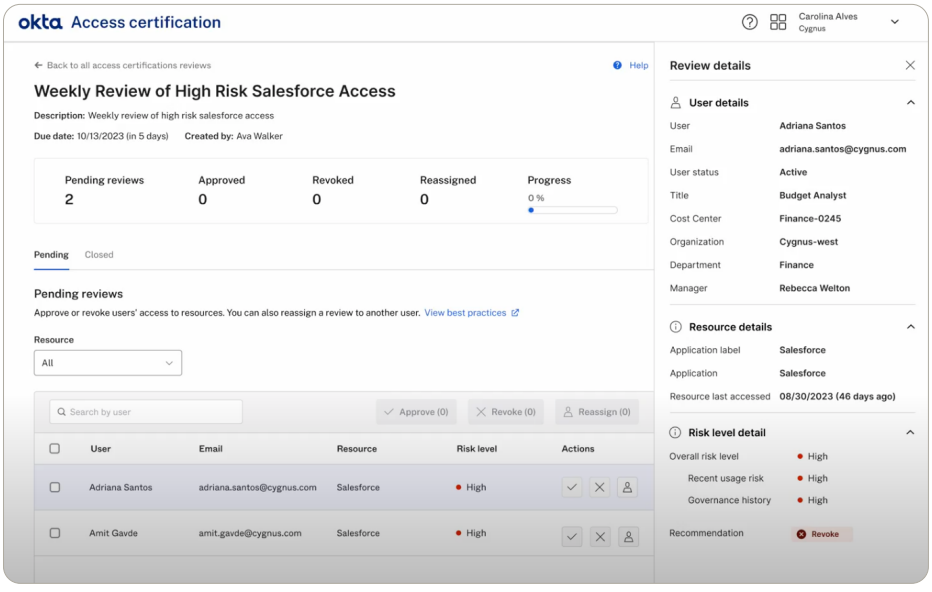
La gouvernance et l'administration des identités (IGA, Identity Governance and Administration) repose sur une approche de la gestion des identités et du contrôle des accès qui est basée sur des politiques et combine les éléments suivants :

- Gouvernance des identités – Processus et politiques couvrant la séparation des fonctions, la gestion des rôles, le logging, les vérifications des accès, les analyses et le reporting.
- Administration des identités – Administration des comptes et des identifiants, provisioning et déprovisioning des utilisateurs et des terminaux, et gestion des droits.

La position d'Okta en tant que plateforme unifiée pour l'IAM, l'IGA et le PAM (Privileged Access Management) offre un vaste ensemble de données d'identité qui peut aider les entreprises à satisfaire les exigences de conformité, à répondre aux besoins en informations des audits, à améliorer l'efficacité des processus et à renforcer la productivité des collaborateurs.

Governance Analyzer avec Okta AI soutient ces objectifs en s'appuyant sur le machine learning, les signaux d'accès des terminaux et les signaux d'accès des utilisateurs pour :

- réduire la charge cognitive des décideurs impliqués dans les processus de gouvernance ;
- fournir des informations non triviales sur les risques de combinaisons utilisateur-ressource ;
- tirer parti des nombreuses données d'Okta pour fournir des renseignements que les autres éditeurs ne sont pas en mesure de fournir.



Quelques exemples de cas d'usage de Governance Analyzer :

- Étayer la prise de décision déterminant si l'accès d'un utilisateur doit être approuvé (p. ex. lors d'une demande) ou étendu (p. ex. lors d'une certification)
- Déterminer qui peut demander un accès à une ressource donnée (p. ex. seuls les utilisateurs en dessous d'un certain seuil de risque ont la possibilité de demander un accès)
- Déterminer quels accès sont vérifiés dans une campagne (p. ex. tout utilisateur au-dessus d'un certain seuil de risque est automatiquement vérifié ou vérifié plus régulièrement)
- Automatiser l'approbation ou le refus des accès, dans une campagne de demande ou de certification
- Recommander des configurations de gouvernance appropriées afin que les ressources critiques disposent des approbations requises pour obtenir un accès et que cet accès est vérifié régulièrement

Log Investigator avec Okta AI

Disponible en Early Access au T3 2024

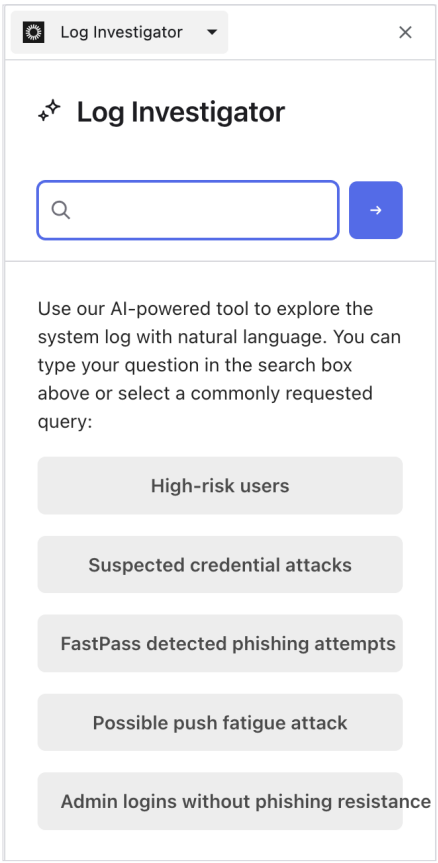
Le rôle de l'IA – Offre un log en langage naturel et un outil de recherche API permettant au personnel IT de trouver rapidement des informations dans le vaste ensemble de données d'Okta.

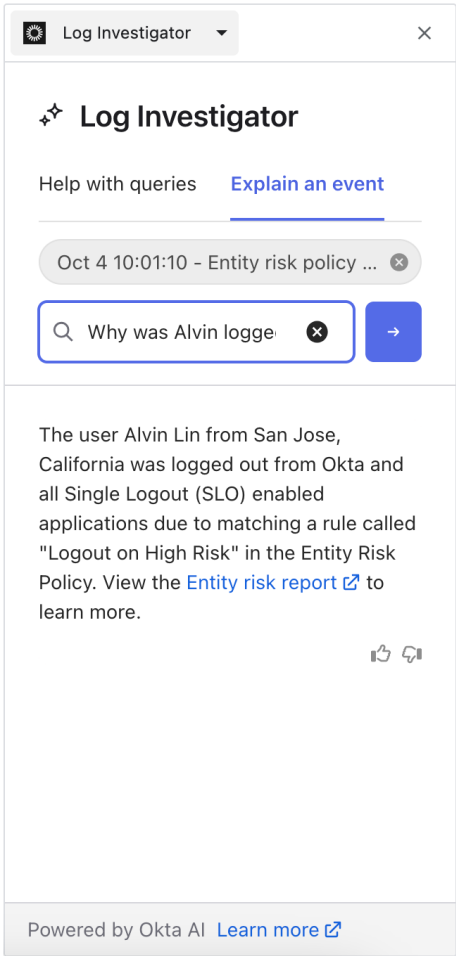
Les logs ont toujours constitué une précieuse source d'informations permettant de déterminer ce qui s'est passé et ce qui se passe dans un environnement, et pourquoi. À mesure que les technologies numériques ont pris la main sur le contrôle de nombreux aspects des opérations métier et que la granularité de ce contrôle a augmenté, le volume de logs a explosé et les informations pertinentes qu'ils contiennent sont devenues plus difficiles à extraire. Dans de nombreux systèmes IT, trouver les réponses aux questions les plus simples nécessite souvent des requêtes soigneusement élaborées et/ou des efforts manuels conséquents pour passer au crible des centaines de résultats, monopolisant du temps et des ressources déjà limités.

Heureusement, l'IA générative transforme la façon dont les individus interagissent avec les ensembles de données pour extraire des informations utiles.

Log Investigator avec Okta AI est un log en langage naturel et un outil de recherche API aidant le personnel IT à parcourir facilement et rapidement le vaste ensemble de données d'Okta, l'aidant à répondre à des questions liées à l'identité telles que les suivantes :

- « Avons-nous observé des connexions suspectes cette semaine ? »
- « Lesquelles émanaient de terminaux non gérés ? »
- « Certaines d'entre elles provenaient-elles d'un nouvel emplacement ? »





Policy Recommender avec Okta AI

Disponible en Early Access au T1 2024

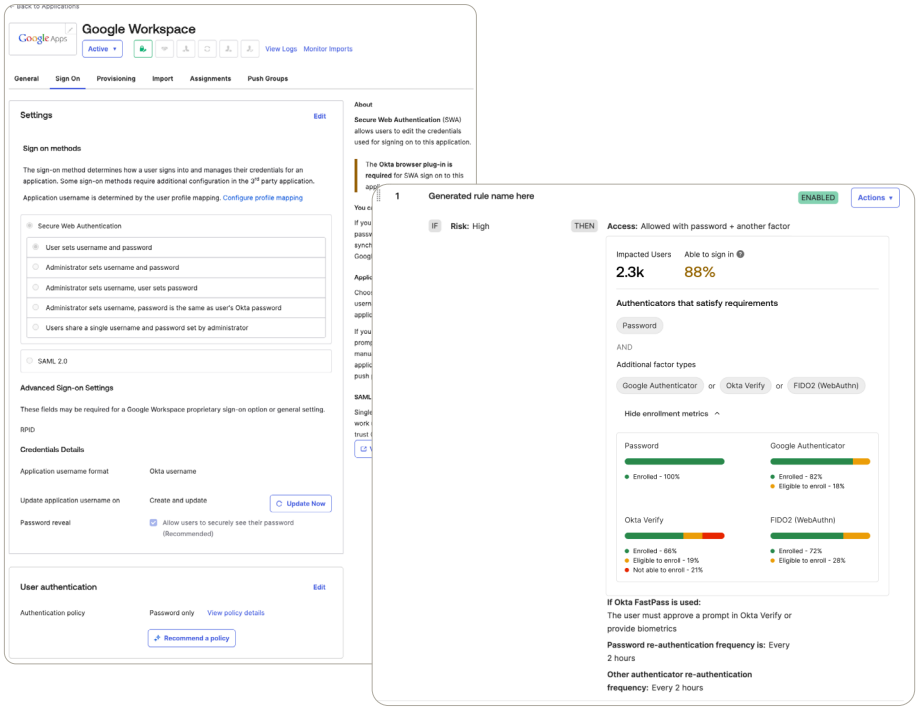
Le rôle de l'IA – Examine les données de configuration des politiques de la clientèle d'Okta pour extraire des bonnes pratiques et générer des politiques lisibles par une machine, qui peuvent être directement appliquées au sein d'environnements Okta.

L'infrastructure d'identités forme un vaste réseau interconnecté couvrant l'ensemble de l'environnement IT d'une entreprise, et même au-delà puisqu'il englobe les applications tierces. Par conséquent, la configuration et la gestion d'un tel système étendu constituent une tâche complexe qui peut exiger beaucoup de temps, d'énergie et d'expertise.

De nombreuses entreprises sont confrontées à des scénarios d'administration similaires, en particulier dans les applications courantes comme Slack, Salesforce et GitHub. Ces expériences partagées représentent une opportunité d'exploiter leurs connaissances collectives.

Policy Recommender avec Okta AI s'appuie sur les informations agrégées et anonymisées de la clientèle d'Okta pour fournir aux administrateurs des recommandations de politiques et des renseignements exploitables (p. ex. nombre d'utilisateurs concernés par un changement de politique, aperçu de l'impact d'une politique avant son application) pour la gestion des applications Okta Integration Network (OIN), ce qui permet aux administrateurs de :

- mieux comprendre et résoudre plus facilement les défis qu'ils rencontrent ;
- appliquer la configuration et les paramètres adéquats aux fonctionnalités appropriées en toute confiance ;
- améliorer la sécurité, l'efficacité et la productivité des collaborateurs.



L'IA dans Customer Identity Cloud (CIC)

D'après le rapport Technology Vision 2023 d'Accenture, **« la capacité à authentifier les identités des clients en ligne semble être une priorité absolue pour les dirigeants : 85 % d'entre eux affirment que cela devient un impératif stratégique et trois personnes interrogées sur quatre ont déclaré que des problèmes d'authentification des clients ont eu un impact négatif sur les résultats de leur entreprise, sous la forme de transactions abandonnées, de frustration ressentie par les utilisateurs, etc. ».**

Bien que la définition de base du CIAM reste la même au sens propre, ce à quoi ce terme renvoie (cas d'usage spécifiques, composants fonctionnels mis en jeu, organisations concernées, etc.) a évolué, en particulier au cours des dernières années. Aujourd'hui, le CIAM répond à de nombreux besoins :

- Clients particuliers – Dans le contexte B2C, l'implémentation réussie d'un CIAM permet aux entreprises de proposer des promotions et recommandations hautement personnalisées, et capables de générer des recettes supplémentaires, mais aussi d'apporter une valeur ajoutée aux clients, accompagnée d'une expérience utilisateur pratique sur plusieurs canaux numériques.
- Clients professionnels – Un très grand nombre d'entreprises s'appuient principalement sur des applications SaaS B2B (business-to-business) pour soutenir leurs activités. Toutefois, au sein de chaque entreprise, chaque type d'utilisateur a besoin d'un niveau d'accès spécifique aux différentes ressources. Leur proposer une expérience simple et sécurisée implique donc de gérer de façon précise les identités et les droits d'accès. Le CIAM offre néanmoins une solution idéale à ces difficultés en permettant aux clients d'applications SaaS B2B de gérer eux-mêmes leurs identités.

L'adoption initiale de l'IA dans Customer Identity Cloud avait pour but de renforcer la sécurité, dans la mesure où les applications orientées clients sont ciblées par un large éventail de menaces. Toutefois, les approches qui peuvent contribuer à sécuriser les identités collaborateurs ne sont pas toujours applicables aux identités clients. Dans un environnement d'entreprise, la sécurité est souvent préférable à la praticité. Les administrateurs peuvent donc imposer des contrôles avec (comparativement) moins d'égards pour l'expérience utilisateur.

En revanche, la gestion des identités clients doit assurer sécurité et confidentialité tout en réduisant les points de friction, ce qui nécessite d'ériger des défenses capables de déjouer les menaces sophistiquées tout en restant presque invisibles pour les utilisateurs.

Heureusement, l'IA a démontré qu'elle était en mesure de faire la distinction entre les utilisateurs légitimes et les cybercriminels usurpant leur identité.

En plus des nouvelles fonctionnalités de sécurité Okta AI, d'autres fonctions récentes tirent parti du machine learning et de l'IA générative pour améliorer l'expérience client, augmenter les conversions et simplifier l'administration.

Bot Detection

Le rôle de l'IA – Examine plus de 60 signaux pour prédire lorsqu'une demande d'authentification provient d'un bot plutôt que du titulaire légitime du compte.

Composant essentiel de l'extension Attack Protection pour Customer Identity Cloud, la fonctionnalité Bot Detection neutralise les attaques de script (p. ex. le credential stuffing ou la validation de listes) contre les applications natives, les flux sans mot de passe et les pages de connexion personnalisées.

En analysant plus de 60 sources de données (tels que des événements passés associés à une adresse IP, l'historique des connexions récentes, les données de réputation des adresses IP et une série d'autres facteurs), Bot Detection prédit quand une demande d'identité est susceptible de provenir d'un bot. Au-delà d'un certain seuil de prédiction/confiance, le flux d'authentification présente une contre-mesure, telle qu'un CAPTCHA.

Bot Detection est un exemple de la façon dont l'IA peut améliorer les techniques antérieures :

- La première version, introduite en février 2021, était basée sur des règles et permettait de détecter 18 % des bots.
- La deuxième version, lancée en août 2021, utilisait le machine learning pour l'analyse comportementale. Cette approche optimisée par l'IA a plus que doublé l'efficacité, enregistrant un taux de détection de 45 % des bots.
- La version la plus récente, lancée en juin 2022, détecte 79 % des bots, soit la meilleure performance à ce jour, en dépit du fait que les cybercriminels ne cessent d'affiner leurs propres techniques.

Il est important de souligner que ces fonctionnalités défensives optimisées ont été implémentées sans créer de points de friction inutiles pour les utilisateurs. En entraînant et en adaptant continuellement l'IA au cœur de la fonction Bot Detection, il est possible d'éviter dans la plupart des cas l'affichage d'un CAPTCHA aux utilisateurs.

De plus, une étude interne détaillée examinant les effets avant/après de Bot Detection a révélé un fort effet dissuasif :

- En moyenne, les clients de l'étude qui ont activé Bot Detection ont constaté une réduction du trafic malveillant de plus de 40 %.
- Certains clients de grande taille ont constaté une baisse de plus de 90 % du trafic de bots.

Complément de Bot Detection : Identity Threat Level (ITL)

En avril 2023, nous avons dévoilé un aperçu de notre initiative Identity Threat Level (ITL). Notre solution CIAM sécurise des milliards de transactions de connexion par mois et sert de porte d'entrée aux applications. À ce titre, nous bénéficions d'une position privilégiée à partir de laquelle nous pouvons surveiller les menaces ciblant l'identité.

C'est de ce constat qu'est né le score ITL : compris entre 0 et 10, il indique le niveau estimé d'activité de bots en représentant la probabilité que le trafic ne parvienne pas à résoudre un CAPTCHA. Un score de 0 signifie qu'il n'y a pratiquement pas d'activité de bots, tandis qu'un score de 10 indique que presque tout le trafic est vraisemblablement imputable à des bots.

En agrégeant anonymement les observations recueillies chez nos clients, nous pouvons calculer un score ITL pour différents secteurs d'activité et régions géographiques, avec la possibilité d'analyser plus précisément d'autres attributs courants. Par exemple, le score ITL peut indiquer :

- comment le trafic probablement malveillant à destination des clients CIC de différents secteurs et régions a évolué au fil du temps ;
- quels sont les niveaux de trafic probablement malveillant à destination des clients CIC de différents secteurs et régions.

Le suivi des tendances historiques et des évolutions quotidiennes peut permettre d'identifier des risques élevés pour les flux d'inscription et de connexion CIAM, afin que les fournisseurs d'applications puissent renforcer leur propre surveillance, réajuster les seuils de façon proactive, implémenter des défenses supplémentaires ou prendre d'autres mesures le cas échéant.

Toutes ces analyses et informations sont rendues possibles par Bot Detection.

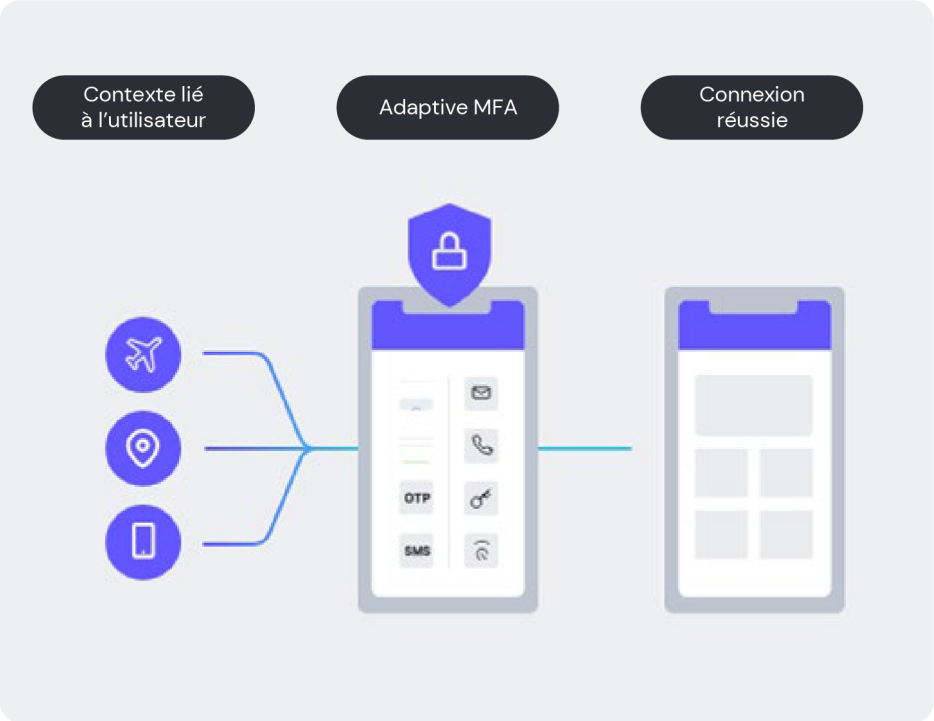
Adaptive MFA

Le rôle de l'IA – Permet de contextualiser les risques en analysant un vaste ensemble de signaux d'identité pour prédire si une tentative d'authentification provient de l'utilisateur légitime ou d'un cybercriminel qui en usurpe l'identité.

La fonction Adaptive MFA propose un accès intelligent qui répond aux besoins des entreprises tout en s'adaptant aux comportements de connexion des clients.

Bien que le MFA constitue une défense éprouvée contre les usurpations de compte, de nombreuses entreprises, en particulier dans les environnements B2C, rechignent à l'utiliser par peur que les frictions introduites ne nuisent à l'expérience utilisateur.

La fonction Adaptive MFA offre une alternative attrayante, en ne présentant une demande MFA que lorsqu'une connexion est considérée comme risquée et en préservant une expérience fluide à tout autre moment.



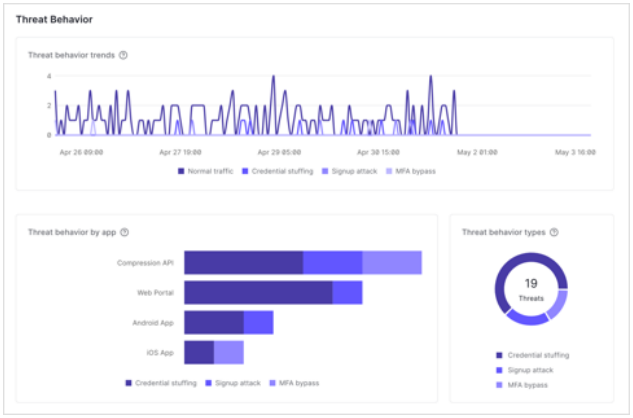
Security Recommendations

Bientôt disponible

Le rôle de l'IA – Fournit des recommandations intelligentes permettant aux entreprises d'améliorer la posture de sécurité de leur tenant.

Security Center permet aux équipes IT et sécurité de visualiser les tendances d'attaques potentielles et d'y répondre rapidement en temps réel, en offrant :

- une vue simplifiée des événements d'authentification, des incidents potentiels et de l'efficacité de la réponse aux menaces ;
- des notifications en temps réel sur les indicateurs de détection des anomalies ;
- des visualisations des tendances d'attaques potentielles (credential stuffing, fraudes à l'inscription, tentatives de contournement du MFA, etc.) ;
- des informations concernant l'impact des fonctionnalités Attack Protection sur l'expérience utilisateur (limitation du débit, CAPTCHA, etc.).



Ces fonctionnalités seront désormais complétées par des recommandations intelligentes basées sur le machine learning sous la forme d'alertes et de notifications affichées sur le tableau de bord.

Identity Flow Optimizer avec Okta AI

Disponible en Early Access au T4 2024

Le rôle de l'IA – Analyse les données d'authentification pour suggérer des pistes destinées à optimiser l'expérience client et à augmenter les conversions.

Dans une entreprise orientée clients, le terme « friction » ou « point de friction » désigne tout ce qui ralentit les interactions d'un client avec un service. Pour un utilisateur, ces interactions peuvent inclure (sans s'y limiter) :

- L'inscription à un service
- La connexion à un compte existant
- La mise à jour d'informations ou de préférences
- La récupération de données de compte
- La finalisation d'un achat

Plus les frictions sont nombreuses, moins le taux de conversion et les recettes seront élevés à court terme comme à long terme. Toutefois, l'optimisation manuelle des flux clients peut s'avérer complexe en raison des importantes quantités de données impliquées et des préférences hautement personnelles des différents utilisateurs.

En outre, la sécurisation des flux d'identité doit toujours être une priorité, mais reste une tâche difficile pour les experts, sans parler des développeurs qui manquent d'expérience dans le domaine de l'identité.

Pour relever ces défis, Identity Flow Optimizer fournit aux développeurs des recommandations en ligne concernant les configurations d'identité et les actions qu'ils peuvent ajouter pour stimuler les conversions, renforcer la sécurité et accélérer la création d'applications.

Brand Customizer avec Okta AI

Disponible en Early Access au T4 2024

Le rôle de l'IA – Crée ou complète automatiquement des modèles de design avec les éléments de branding d'une entreprise.

Si les marques sont soumises à des règles strictes en matière de design, c'est pour une bonne raison : offrir une expérience utilisateur cohérente qui renforce une identité de marque soigneusement réfléchie.

La fonction Brand Customizer peut créer un modèle d'une page et adapter le design à tous les autres modèles requis. Un développeur peut également fournir une capture d'écran ou un logo. L'IA crée alors les modèles et le développeur les personnalise si nécessaire.

Non seulement cette approche crée une identité visuelle cohérente pour les utilisateurs finaux, mais elle accélère également le délai de rentabilisation en permettant aux développeurs de créer des expériences clients de qualité, d'innover et de contribuer au développement de l'entreprise – plus facilement et plus rapidement.

Guide avec Okta AI

Disponible en Early Access au T4 2024

Le rôle de l'IA – Interprète les invites en langage simple et offre une assistance contextuelle pour aider les utilisateurs à travailler efficacement avec Customer Identity Cloud.

Customer Identity Cloud est performant, riche en fonctionnalités et hautement extensible, mais l'étendue de ses capacités peut être intimidante pour les nouveaux utilisateurs, et même les experts pourraient ne pas maîtriser tous les détails ou être au fait des nouvelles fonctionnalités.

Pour favoriser un onboarding rapide des nouveaux utilisateurs et aider chaque individu à tirer le meilleur parti de CIC, la fonction Guide :

- offre une assistance complète à l'onboarding, qui identifie intuitivement les étapes à suivre par les utilisateurs et les oriente vers les workflows les plus pertinents grâce à des invites simples (en anglais) ;
- peut traduire n'importe quel paramètre ou jargon de la plateforme en un langage facilement compréhensible, ainsi qu'enrichir l'expérience avec une assistance contextuelle et des liens vers une documentation pertinente.

Actions Navigator avec Okta AI

Disponible en Early Access au T2 2024

Le rôle de l'IA – Permet d'effectuer des recherches en langage simple pour trouver plus facilement des intégrations appropriées, et aide les utilisateurs à développer de nouvelles intégrations si nécessaire.

L'extensibilité est une caractéristique fondamentale de Customer Identity Cloud, et Auth0 Marketplace vise à simplifier les processus de développement en offrant un moyen simple d'ajouter une intégration aux applications d'identité.

Cela étant, avec des centaines d'intégrations, il n'est pas toujours facile de trouver exactement celle qui répond à vos besoins.

La fonction Actions Navigator permet aux développeurs de découvrir et d'implémenter des intégrations de marketplace ou d'écrire une action (c'est-à-dire une fonction utilisée pour personnaliser et étendre les fonctionnalités de CIC) en exprimant simplement une requête dans une invite de recherche. La génération de code fait partie des usages les plus novateurs de l'IA générative. Elle offre de nouvelles possibilités non seulement aux développeurs, mais aussi à ceux qui n'ont aucune expérience en codage.

Tenant Security Manager avec Okta AI

Disponible en Early Access au T2 2024

Le rôle de l'IA – Permet de générer des descriptions synthétiques, exprimées en langage simple, de configurations d'identité complexes.

De nombreuses entreprises disposent d'experts qui possèdent de précieuses connaissances sur des systèmes particuliers, y compris l'identité.

Quand ces experts ne sont pas disponibles, par exemple lorsqu'ils changent de service ou qu'ils quittent l'entreprise, il peut être très difficile pour les autres acteurs de comprendre l'état du système et les détails de sa configuration.

Tenant Security Manager enrichit les fonctionnalités Attack Protection d'Okta avec des recommandations de sécurité intelligentes sous la forme d'alertes et de notifications affichées sur le tableau de bord, dans le but d'améliorer le niveau de sécurité du tenant du client.

Conclusion

La popularité soudaine de ChatGPT et l'émergence consécutive d'une longue liste d'outils tout aussi impressionnants montrent que la technologie évolue si rapidement et que les retombées sont si variées qu'élaborer des prédictions spécifiques sur l'IA et ses répercussions est mission impossible.

Toutefois, certaines choses sont claires. Par exemple, en ce qui concerne les conséquences de l'IA, en particulier de l'IA générative, le titre d'un communiqué de presse de Forrester en dit long : « Ignorer l'IA générative pourrait coûter cher aux entreprises ».

Autrement dit, même si vous ne savez pas exactement où vos investissements dans l'IA vous mèneront, soyez assuré que l'absence d'investissement dans l'IA vous placera au mieux dans une position de désavantage concurrentiel, au pire entraînera votre obsolescence. Le changement de paradigme est à ce point historique.

En consacrant une part considérable de notre budget de recherche et développement à l'IA, et en tirant parti de notre vaste ensemble de données IAM, nous continuerons à proposer des fonctionnalités novatrices pilotées par l'IA pour renforcer la sécurité, améliorer la productivité et optimiser les expériences utilisateurs, que ce soit dans Workforce Identity Cloud ou dans Customer Identity Cloud.

Si nous ne savons pas exactement quels seront les fruits de nos propres investissements, nous sommes convaincus que les fonctionnalités déployées actuellement et celles encore dans notre vivier constitueront les premières étapes d'un parcours transformateur.

Clause de non-responsabilité

Le présent document et toute recommandation qu'il propose ne constituent pas des conseils juridiques, commerciaux ou en matière de confidentialité, sécurité ou conformité. Le contenu de ce document revêt un caractère purement informatif et pourrait ne pas refléter les normes de sécurité, de confidentialité et les réglementations les plus récentes, ou tous les problèmes pertinents. Pour obtenir de tels conseils, il vous revient de vous adresser à votre conseiller juridique ou à tout autre conseiller professionnel en matière de sécurité, confidentialité ou conformité, et de ne pas vous en remettre aux recommandations formulées dans le présent document. Okta décline toute responsabilité quant aux pertes ou dommages pouvant résulter de la mise en œuvre des recommandations fournies dans le présent document. Okta ne formule aucune déclaration, garantie ou autre assurance concernant le contenu de ce document. Pour en savoir plus sur les assurances contractuelles d'Okta à ses clients, rendez-vous à l'adresse okta.com/agreements.

Tous les produits, fonctions et fonctionnalités référencés dans ce document qui ne sont pas encore disponibles pourraient être distribués à une date ultérieure à la date annoncée, ou annulés. Les roadmaps produits ne représentent en rien un engagement, une obligation ou une promesse d'offre de produit ou fonctionnalité, et les clients ne doivent pas se baser sur ces plans pour prendre leur décision d'achat.

À propos d'Okta

Partenaire leader indépendant en matière d'identité, Okta permet à chacun d'utiliser en toute sécurité n'importe quelle technologie, partout, sur n'importe quel terminal ou application. Les plus grandes marques font confiance à Okta en matière d'accès sécurisé, d'authentification et d'automatisation. De par leur flexibilité et neutralité, les solutions Okta Workforce Identity Cloud et Customer Identity Cloud offrent aux dirigeants d'entreprises et aux développeurs la possibilité de se concentrer sur l'innovation et d'accélérer leur transformation digitale, grâce à des solutions personnalisables et plus de 7 000 préintégrations. Nous construisons un monde où l'identité vous appartient. Pour en savoir plus, consultez notre site à l'adresse okta.com/fr.