Modèle de maturité de l’identité Okta

Votre feuille de route pour renforcer la sécurité et la conformité par le biais du Zero Trust, améliorer l’expérience utilisateur et optimiser l’agilité opérationnelle grâce à l’identité

Liens

Renforcer la sécurité — et bien plus encore

La gestion des identités et des accès (IAM, Identity and Access Management) se limitait autrefois à la gestion des noms d'utilisateur et des mots de passe. Aujourd'hui, ce terme englobe une réalité bien plus vaste : l'IAM permet à votre entreprise d'interagir en toute sécurité avec ses collaborateurs, clients et partenaires et ce, à tout moment, où qu'ils se trouvent et sur tous les terminaux.

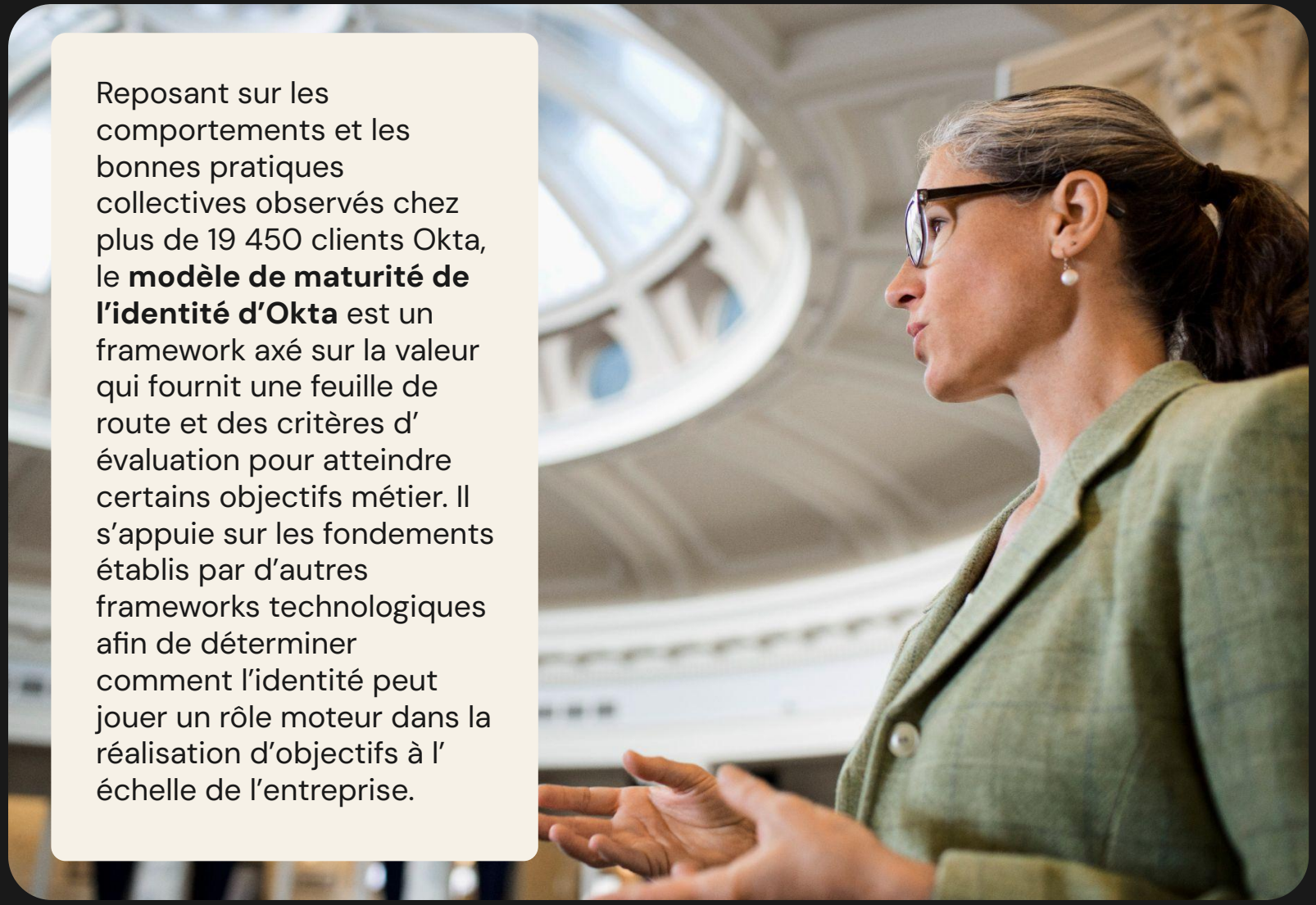
Lorsque l'identité est robuste :

- La sécurité est renforcée et la gouvernance, les risques et la conformité (GRC) sont simplifiés.
- Les opérations sont plus rapides, avec une automatisation poussée et moins d'erreurs.
- Les utilisateurs peuvent accéder plus facilement aux ressources dont ils ont besoin quand ils en ont besoin.

Toutefois, au vu de la portée, de l'impact et de la complexité de l'identité, il peut être difficile de savoir par où commencer, d'évaluer votre situation actuelle et de créer une feuille de route pour aider votre entreprise à atteindre ses objectifs.

okta

Le modèle de maturité de l’identité d’Okta



Reposant sur les comportements et les bonnes pratiques collectives observés chez plus de 19 450 clients Okta, le **modèle de maturité de l’identité d’Okta** est un framework axé sur la valeur qui fournit une feuille de route et des critères d’ évaluation pour atteindre certains objectifs métier. Il s’appuie sur les fondements établis par d’autres frameworks technologiques afin de déterminer comment l’identité peut jouer un rôle moteur dans la réalisation d’objectifs à l’ échelle de l’entreprise.

Dans le modèle de maturité de l’identité, quatre stades progressifs permettent d’évaluer les fonctionnalités d’identité tout au long du parcours de maturité :

Fondamental

Répondre aux besoins essentiels en matière d’identité tout en posant des bases solides pour progresser dans le parcours de maturité

Évolutif

Étendre l’environnement d’identités consolidé à de nouvelles applications, de nouveaux services, de nouveaux cas d’usage et de nouveaux utilisateurs

Avancé

Étendre l’automatisation et l’intégration pour optimiser l’expérience, améliorer l’agilité et renforcer la sécurité

Stratégique

Obtenir un avantage stratégique grâce à des initiatives qui facilitent le travail des collaborateurs, optimisent l’efficacité et tirent parti de l’identité pour détecter et neutraliser les menaces en temps réel

Le tableau ci-dessous montre comment le passage par ces stades permet d’obtenir des résultats significatifs et mesurables au niveau des piliers de valeur critiques que sont la sécurité et la conformité, l’agilité opérationnelle et l’expérience utilisateur.

okta

Pilier de valeur	Exemples de résultats	Stade 1 : Fondamental	Stade 2 : Évolutif	Stade 3 : Avancé	Stade 4 : Stratégique
		Les entreprises ont souvent du mal à gérer les applications et les utilisateurs tout en prévenant les attaques d'identité. Pour gagner en maturité, elles doivent consolider et simplifier leur infrastructure d'identités.	Une fois les fonctions d'identité fondamentales mises en place, l'accent est mis sur les améliorations qui permettent aux opérations sous-jacentes d'évoluer. Il faut pour cela multiplier les contrôles de sécurité et développer l'automatisation.	Les entreprises ont mis en place un large éventail de systèmes d'identité, en se concentrant sur l'application de contrôles à fort impact et facilement réalisables par le biais de l'automatisation ou de politiques de sécurité renforcées.	Ce dernier stade de maturité, qui se poursuit sur la durée, consiste essentiellement à étendre les contrôles et l'automatisation autant que possible au sein de l'entreprise et à atteindre un état stable, caractérisé par des ajustements et des optimisations.
Sécurité et conformité	• Atténuation et neutralisation proactives des menaces d'identité • Obtention et conservation de certifications de conformité critiques • Rationalisation et sécurisation de l'accès des utilisateurs finaux selon le principe du moindre privilège	Renforcez la protection contre les attaques d'identité en implémentant l'authentification unique (SSO) et l'authentification multifacteur (MFA) de base avec des politiques de contrôle d'accès basé sur les rôles (RBAC, Role-Based Access Control).	Mettez en place les premiers stades d'une architecture Zero Trust avec des politiques d'accès dynamiques.	Implémentez une authentification et une autorisation sensibles aux risques et résistantes au phishing.	Appliquez une authentification et une autorisation intelligentes, contextuelles et continues capables de tenir la cadence des intrusions modernes.
Agilité opérationnelle	• Augmentation de l'efficacité opérationnelle et réduction des coûts d'exploitation • Amélioration de l'efficacité des collaborateurs • Rationalisation des intégrations liées aux fusions et acquisitions	Arrêtez de gérer manuellement les utilisateurs et les applications.	Automatisez le cycle de vie des utilisateurs et le provisioning.	Tirez parti d'une gestion avancée du cycle de vie, en automatisant les tâches courantes telles que les demandes d'accès, les approbations et le provisioning des applications.	Automatisez entièrement les workflows IT et sécurité relatifs aux politiques, à la gestion du cycle de vie et à l'identité pour l'ensemble des applications et des services cloud.
Expérience utilisateur	• Amélioration de l'expérience numérique des utilisateurs • Augmentation des conversions d'inscription et de connexion	Dressez un inventaire de toutes les applications et sécurisez les flux de connexion à l'aide de protections de base telles que le MFA, la détection des bots et des politiques de mots de passe forts.	Étendez le SSO et le MFA à tous les types d'utilisateurs, déployez rapidement des options sans mot de passe telles que FastPass et les passkeys, et standardisez l'accès en libre-service pour les besoins courants.	Étendez l'accès sans mot de passe à tous les terminaux et canaux, prenez en charge un libre-service fluide et utilisez les signaux d'identité pour personnaliser l'accès en temps réel.	Offrez un accès personnalisé et sans mot de passe sur tous les points de contact grâce à des fonctionnalités avancées telles que des identifiants vérifiables, des politiques adaptatives et un contrôle de session en temps réel.

Remarque : ce tableau a pour but d'illustrer la portée de l'identité. Il ne constitue pas une représentation exhaustive des caractéristiques et des comportements qui définissent chaque stade du parcours ou les résultats métier.

okta

À propos de ce document

Nous avons créé le modèle de maturité de l'identité d'Okta afin de fournir aux entreprises des conseils pratiques, basés sur la valeur et orientés résultats pour élaborer et améliorer leur stratégie d'identité.

Cette approche distingue ce modèle des frameworks technologiques et des checklists de maturité, qui ont tendance à décrire des fonctions ou à prescrire des technologies, mais qui omettent d'examiner en détail la valeur ou les résultats attendus.

De même, le fait que le modèle de maturité de l'identité dépasse le cadre strict de la sécurité (et de la conformité) le démarque de ces autres ressources.

Néanmoins, prenant acte du fait que la sécurité est souvent la raison principale qui motive les projets d'identité, ce guide examine la maturité de l'identité à travers le prisme familier des quatre fonctions de l'identité et des trois capacités transversales du célèbre modèle de maturité Zero Trust de la CISA :

Authentification	Référentiels d'identités	Évaluations des risques	Gestion des accès
Visibilité et analyses	Automatisation et orchestration	Gouvernance	

Dans ce document, nous allons :

- Fournir des informations et des exemples concrets
- Effectuer des comparaisons avec le modèle de maturité Zero Trust
- Suggérer des solutions Okta qui pourraient aider votre entreprise à atteindre ses objectifs en matière de maturité de l'identité

Maturité de l'identité et Zero Trust

L'identité est le premier des cinq piliers du modèle de maturité Zero Trust (ZTMM) mis au point par la Cybersecurity and Infrastructure Security Agency (CISA).

La sous-section « Identité » de ce modèle recommande aux organismes publics étasuniens de prendre les mesures suivantes :

- Veiller à ce que les utilisateurs et les entités aient accès aux ressources adéquates au bon moment et pour des raisons valables, sans octroyer un accès excessif.
- Intégrer des solutions de gestion des identités, des accès et des identifiants chaque fois que possible dans toute l'entreprise pour appliquer une authentification forte, octroyer des autorisations adaptées au contexte et évaluer les risques liés à l'identité pour les entités et utilisateurs.
- Intégrer des systèmes de gestion et des référentiels d'identités dans les cas requis, pour améliorer la sensibilisation aux identités d'entreprise ainsi qu'à leurs droits et responsabilités.

Bien qu'il ait été mis au point au départ pour les organismes publics américains, le modèle ZTMM est utilisé par de nombreuses entreprises du secteur privé. Il complète les directives de l'architecture Zero Trust du NIST (SP 800-207), qui décrit des principes tels que la vérification continue et le moindre privilège. Cependant, le guide de la CISA est plus descriptif que prescriptif, ce qui a conduit de nombreux clients Okta à nous demander comment faire évoluer leurs pratiques d'identité conformément au modèle ZTMM de la CISA.

C'est la raison pour laquelle ce guide fait spécifiquement référence à des aspects particuliers du modèle ZTMM de la CISA, afin de mettre en évidence les points communs avec le modèle de maturité de l'identité d'Okta.

Découvrez en particulier comment le modèle de maturité de l'identité d'Okta prend en charge le Zero Trust pour les secteurs réglementés.

okta

Authentification

L'authentification vérifie l'identité d'un utilisateur ou d'une entité demandant l'accès à une application, à un service ou à une autre ressource.

Les cybercriminels ciblent généralement l'authentification, notamment au moyen des méthodes suivantes :

- La force brute pour essayer de nombreuses combinaisons d'identifiants
- Le social engineering pour inciter les utilisateurs à divulguer leurs identifiants
- Des infostealers pour voler des identifiants, des cookies et des tokens
- L'échange de carte SIM et des attaques Adversary-in-the-Middle pour contourner les formes vulnérables de MFA

Il est évident que l'authentification constitue un élément important de la sécurité, mais elle influence également l'expérience utilisateur et la productivité du personnel, ce qui peut avoir des répercussions importantes.

Par exemple, d'après le rapport Customer Identity Trends Report 2025 d'Auth0, près d'un quart des utilisateurs abandonnent toujours (6 %) ou souvent (17 %) un panier d'achat en ligne en raison de problèmes liés à l'inscription ou à la connexion, et 40 % le font parfois. De même, un collaborateur qui ne parvient pas à accéder à une application ou à des informations ne peut pas faire son travail.

Une fonction d'authentification mature combine une sécurité forte et résistante au phishing (y compris l'intégration de signaux de risque) avec une grande facilité d'utilisation. Elle rend l'accès extrêmement difficile et coûteux pour les cybercriminels, tout en offrant un accès fluide aux utilisateurs légitimes.

Par ailleurs, une fonction d'authentification mature ne se contente pas d'évaluer les risques une seule fois (c'est-à-dire lorsque l'utilisateur se connecte), mais le fait en permanence pour se prémunir contre le détournement de session et d'autres menaces similaires après la connexion.

Autorisation

L'authentification vérifie l'identité d'une entité, tandis que l'autorisation détermine les informations ou les privilèges auxquels l'entité peut accéder, en vertu de la configuration du système.

Le modèle ZTMM de la CISA aborde la question de l'autorisation dans le contexte d'autres fonctions (dans la section « Authentification », l'autorisation est évoquée sous la forme de « droits d'accès »), alors que nous en avons fait un aspect à part entière dans ce document.

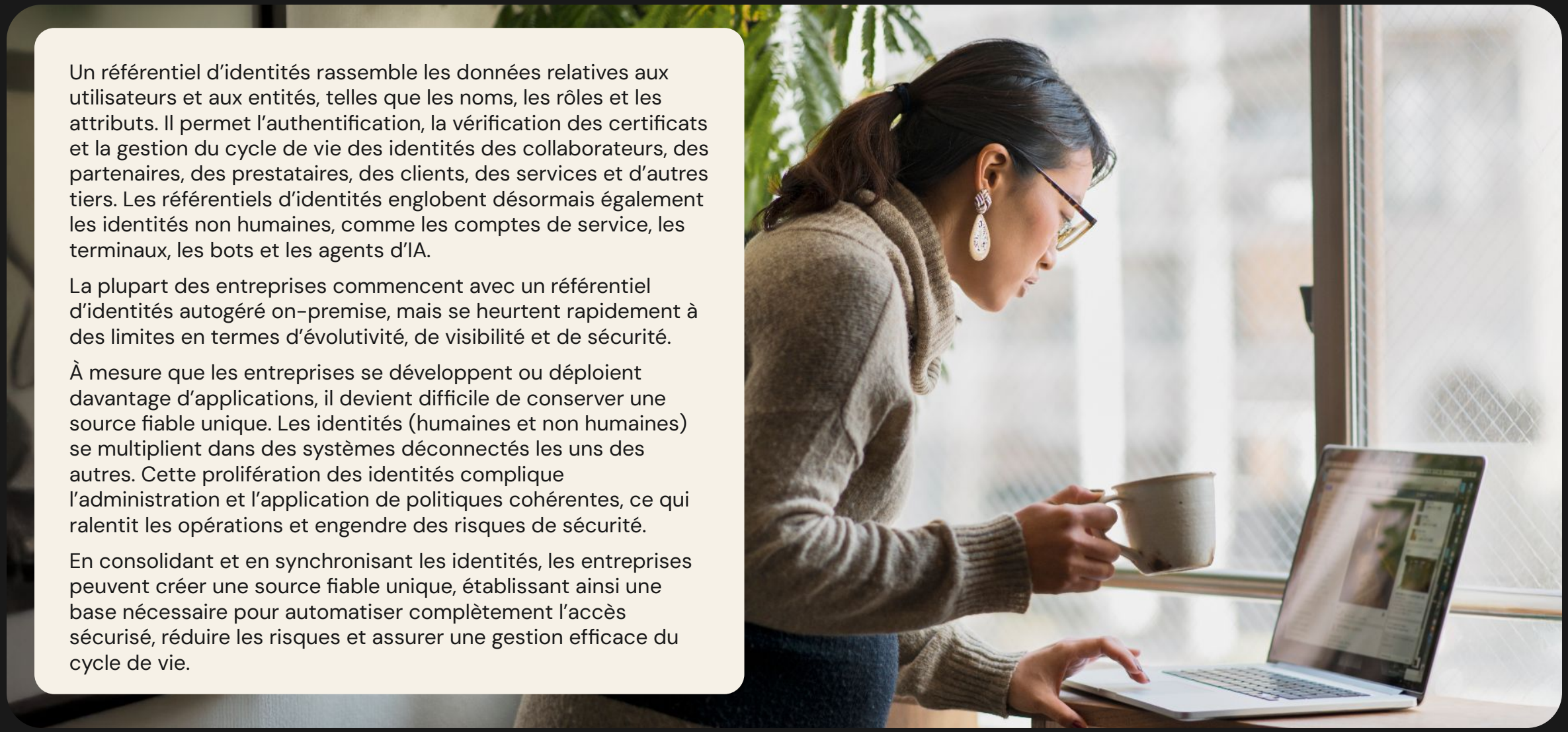
En cas d'implémentation immature de l'identité, ces droits sont assez grossiers et déterminés par des facteurs statiques au moment de la connexion.

En revanche, une implémentation mature de l'identité :

- utilise des attributs dynamiques ;
- a recours à une évaluation contextuelle (localisation, posture du terminal, etc.) ; et
- attribue des droits de manière granulaire.

Stade	Description	Solutions Okta associées
 **Fondamental**	Lors de ce stade à haut risque, l'authentification repose principalement sur des paires de noms d'utilisateur et de mots de passe. Le MFA est parfois utilisé, mais n'est pas obligatoire pour l'ensemble du personnel et peut avoir recours à des techniques vulnérables au phishing (SMS, e-mails, etc.). En outre, l'autorisation est prédéfinie et fixe, et ne tient pas compte des conditions contextuelles ou en temps réel.	• Multi-Factor Authentication • Adaptive Multi-Factor Authentication • Single Sign-On • Universal Directory
 **Évolutif**	L'entreprise applique le MFA à toutes les entités, la sécurité étant renforcée par l'introduction de facteurs de possession et d'inhérence qui peuvent être résistants au phishing. Associée au SSO, l'authentification est désormais plus forte et plus pratique. Les référentiels d'utilisateurs simplifiés et centralisés favorisent une gestion plus efficace de l'autorisation. Des contrôles d'accès basés sur les rôles (RBAC) ou basés sur les attributs (ABAC) sont en place et intègrent des facteurs dynamiques qui peuvent servir à évaluer les risques, tels que la localisation de l'entité, l'heure locale et le type de terminal.	• Adaptive Multi-Factor Authentication • Single Sign-On • Universal Directory • Fine-Grained Authorization
 **Avancé**	L'entreprise commence à supprimer progressivement les mots de passe, les codes d'accès/mots de passe à usage unique, les questions de sécurité et les notifications push. Le MFA résistant au phishing est étendu à l'ensemble de l'entreprise et comprend des implémentations de MFA sans mot de passe via FIDO2 ou, le cas échéant, un justificatif gouvernemental sécurisé tel que la vérification de l'identité personnelle (PIV, Personal Identity Verification). Le contrôle d'accès basé sur les relations (ReBAC) permet une autorisation précise et dynamique. La gestion des accès et le MFA sont étendus à la manière dont les utilisateurs se connectent via des ordinateurs. Les flux d'authentification sont dissociés pour une initiation sécurisée et sans mot de passe par des systèmes de confiance, tels que les centres d'appels, les bornes de service ou les agents d'IA, éliminant ainsi le besoin de questions de sécurité, de mots de passe à usage unique ou de codes PIN.	• Adaptive Multi-Factor Authentication • Single Sign-On • Universal Directory • Identity Threat Protection • Okta FastPass • Fine-Grained Authorization • Okta Device Access • CIBA (Client-Initiated Backchannel Authentication)
 **Stratégique**	Toutes les identités sont validées par le biais d'une authentification résistante au phishing et sans mot de passe. Les contrôles d'accès s'étendent de la connexion aux terminaux à la connexion aux applications pour une sécurité intégrée qui simplifie également l'expérience utilisateur. Les droits d'accès sont désormais évalués en continu à l'aide de variables dynamiques, afin de permettre la détection des menaces post-authentification. Les actions sensibles des clients (comme les transactions à haut risque ou les changements de profil) sont authentifiées et protégées par des mécanismes de confirmation en temps réel qui renforcent la sécurité sans perturber l'expérience utilisateur. En coulisses, les canaux de communication avec les clients et les échanges de données sont renforcés pour répondre à des standards conformes aux exigences du secteur financier, ce qui empêche toute altération ou interception tout au long du parcours du client.	• Adaptive Multi-Factor Authentication • Single Sign-On • Universal Directory • Identity Threat Protection • Okta FastPass • Fine-Grained Authorization • Okta Device Access • Strong Customer Authentication • FAPI (Financial Grade API)

Référentiels d’identités



Un référentiel d’identités rassemble les données relatives aux utilisateurs et aux entités, telles que les noms, les rôles et les attributs. Il permet l’authentification, la vérification des certificats et la gestion du cycle de vie des identités des collaborateurs, des partenaires, des prestataires, des clients, des services et d’autres tiers. Les référentiels d’identités englobent désormais également les identités non humaines, comme les comptes de service, les terminaux, les bots et les agents d’IA.

La plupart des entreprises commencent avec un référentiel d’identités autogéré on-premise, mais se heurtent rapidement à des limites en termes d’évolutivité, de visibilité et de sécurité.

À mesure que les entreprises se développent ou déploient davantage d’applications, il devient difficile de conserver une source fiable unique. Les identités (humaines et non humaines) se multiplient dans des systèmes déconnectés les uns des autres. Cette prolifération des identités complique l’administration et l’application de politiques cohérentes, ce qui ralentit les opérations et engendre des risques de sécurité.

En consolidant et en synchronisant les identités, les entreprises peuvent créer une source fiable unique, établissant ainsi une base nécessaire pour automatiser complètement l’accès sécurisé, réduire les risques et assurer une gestion efficace du cycle de vie.

Stade	Description	Solutions Okta associées
 **Fondamental**	L'entreprise n'utilise que des référentiels d'identités autogérés (c'est-à-dire planifiés, déployés et gérés) comme Active Directory ou LDAP. Ces référentiels se concentrent généralement sur les utilisateurs humains, les identités non humaines telles que les comptes de service n'étant souvent pas gérées ou étant suivies de manière informelle.	• Single Sign-On • Universal Directory
 **Évolutif**	Les entreprises commencent à unifier les référentiels d'identités (qu'ils soient autogérés ou hébergés dans le cloud) afin de limiter la prolifération des identités et les risques associés, tout en appliquant une gouvernance cohérente aux identités humaines et non humaines créées via l'automatisation et l'IaC (Infrastructure-as-Code). Qui plus est, les entreprises synchronisent les référentiels, standardisent les pratiques de gestion du cycle de vie et commencent à suivre formellement les identités non humaines. Ces mesures jettent les bases d'une réduction des doublons, améliorant ainsi la visibilité et mettant en place des workflows automatisés et évolutifs.	• Single Sign-On • Universal Directory • Lifecycle Management • Workflows
 **Avancé**	Les référentiels d'identités sont consolidés et les politiques de gouvernance sont appliquées aux identités humaines et non humaines, ce qui limite la prolifération des identités et accroît la sécurité et l'efficacité des opérations d'identité (telles que le SSO) et de l'administration (comme le provisioning et la gestion du cycle de vie). Les comptes de service, les API et les bots sont intégrés et suivis de manière plus formelle. La visibilité s'améliore et les événements du cycle de vie des identités sont centralisés.	• Universal Directory • Single Sign-On • Lifecycle Management • Workflows • Okta Identity Governance • Okta Privileged Access
 **Stratégique**	Les référentiels d'identités sont unifiés dans tous les environnements, ce qui réduit le nombre de référentiels utilisés et permet une gestion automatisée du cycle de vie. Les identités non humaines (qui comprennent désormais des agents d'IA émergents) sont gérées parallèlement aux utilisateurs humains. L'entreprise met en place des politiques adaptatives, une gestion automatisée du cycle de vie et une gestion de la posture par le biais d'un écosystème d'identité partagé.	• Universal Directory • Single Sign-On • Lifecycle Management • Workflows • Okta Identity Governance • Okta Privileged Access • Identity Security Posture Management

Évaluations des risques

Okta adopte une vision élargie des risques liés à l'identité, qu'il définit comme *« toute vulnérabilité dans les processus de gestion des identités et des accès d'une entreprise »*.

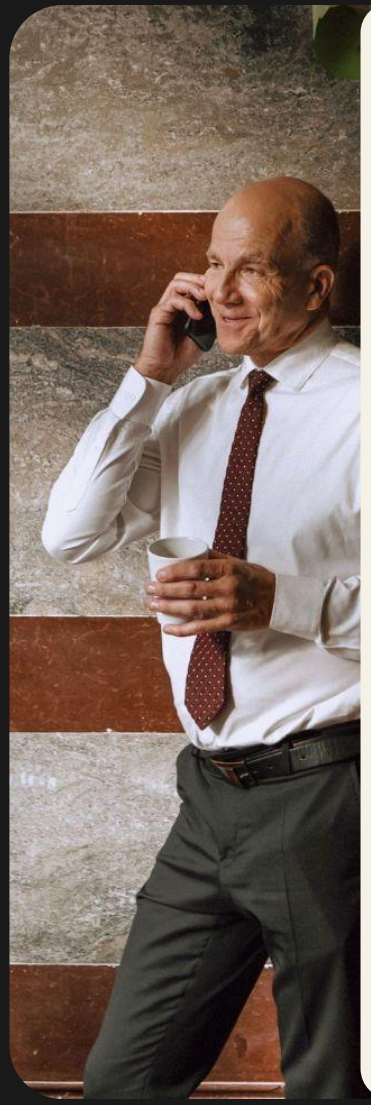
Cette définition large englobe à la fois les risques liés aux identités individuelles et ceux associés aux éléments suivants :

- Mauvaises pratiques d'IAM (comptes orphelins, provisioning excessif, etc.)
- Erreurs de configuration entraînant des failles dans la sécurité
- Utilisation de technologies obsolètes

À mesure que les entreprises évoluent vers le stade Stratégique, elles doivent donner la priorité aux fonctionnalités qui renforcent leur posture de sécurité et réduisent dynamiquement les risques liés à l'identité. Ainsi, elles doivent ingérer et analyser les signaux de sécurité issus de l'ensemble de l'environnement, y compris l'identité, les terminaux, le réseau et la posture des terminaux.

Ces signaux en temps réel contribuent à l'élaboration de politiques adaptatives et permettent aux entreprises de réduire de manière proactive la surface d'attaque des identités et de renforcer la sécurité grâce aux processus suivants :

- **Détection :** identification des menaces cachées et des erreurs de configuration chez les fournisseurs d'identité, dans les applications SaaS et dans l'infrastructure cloud (IaaS)
- **Hiérarchisation :** identification et priorisation des vulnérabilités telles que le contournement du MFA, le provisioning excessif des accès utilisateurs et un offboarding inapproprié
- **Correction :** obtention d'informations de sécurité exploitables pour favoriser une correction rapide
- **Surveillance continue :** analyse permanente et continue de l'exposition aux risques liés à l'identité au sein de l'entreprise et surveillance basée sur les risques en vertu des standards de sécurité, de conformité et IAM (p. ex. NIST, CIS, ISO, SOX et PCI DSS)



Risques liés à l'identité

Dans le modèle ZTMM de la CISA, *la définition des risques liés à l'identité se limite à la probabilité* qu'une identité soit compromise, ce qui est bien plus restrictif que la définition d'Okta[1].

Par conséquent, le modèle vise à aider les entreprises à détecter rapidement et avec précision les identités compromises. Par exemple, la détection d'un comportement anormal (tel qu'un compte de service accédant à des ressources sensibles avec lesquelles il n'a jamais interagi auparavant) entraîne un signalement pour qu'il donne lieu à un examen plus approfondi.

Bien que le modèle de maturité Zero Trust de la CISA n'établisse pas explicitement de lien entre l'évaluation des risques et la fonction d'authentification, elles sont pourtant étroitement liées et Okta aide à combler ce fossé. Par exemple :

- Si un processus évalue avec une forte probabilité qu'une identité a été compromise, cette entité peut se voir refuser l'authentification.
- Si le comportement d'une entité lors de l'authentification est suspect, l'observation de ce comportement pourrait être prise en compte dans les évaluations des risques.

Okta développe cette relation en évaluant les risques tout au long du cycle de vie des identités, et pas seulement au moment de la connexion, et en surveillant en temps réel les signaux comportementaux et contextuels provenant d'autres surfaces d'attaque. Cette approche permet des réponses rapides, telles que la clôture/déconnexion de session basée sur des politiques ou l'authentification renforcée adaptative, afin de contenir les menaces à mesure qu'elles émergent.

[1] CISA. Zero Trust Maturity Model, version 2.0. Avril 2023, p. 14. Consulté le 9 juin 2025 à l'adresse https://www.cisa.gov/sites/default/files/2023-04/zero_trust_maturity_model_v2_508.pdf.

okta

Ces fonctionnalités se recoupent avec la fonction Gestion des accès et les trois capacités transversales (Visibilité et analyses, Automatisation et orchestration, Gouvernance) du modèle ZTMM de la CISA.

Stade	Description	Solutions Okta associées
 **Fondamental**	À ce stade de maturité, les entreprises ont une capacité très limitée à évaluer les risques liés à l'identité et à les intégrer aux politiques d'accès. Toute évaluation existante est probablement basée sur des attributs statiques et les politiques associées sont simplistes (p. ex. binaires).	• Multi-Factor Authentication • Adaptive Multi-Factor Authentication
 **Évolutif**	Les politiques sont légèrement plus riches, avec des évaluations qui peuvent intégrer des données télémétriques d'authentification au moment de la connexion. Néanmoins, les évaluations restent relativement basiques et vulnérables aux attaques d'identité, notamment en raison de l'utilisation de méthodes manuelles et de règles statiques.	• Adaptive Multi-Factor Authentication
 **Avancé**	Les évaluations s'appuient sur l'automatisation et des règles dynamiques, en utilisant une multitude de signaux d'authentification (dont ceux provenant de solutions d'assurance et de gestion des terminaux, par exemple) pour prendre des décisions en matière d'accès. Cependant, les évaluations sont encore principalement effectuées au moment de la connexion et ne sont pas revues au cours de la session de l'utilisateur.	• Adaptive Multi-Factor Authentication • Identity Threat Protection • Identity Security Posture Management
 **Stratégique**	Les évaluations des risques sont effectuées en continu, en temps réel, et tirent parti d'un contexte dynamique et d'un large éventail de signaux provenant de l'infrastructure d'identités et des systèmes IT et sécurité auxiliaires. Par ailleurs, l'automatisation et l'intégration permettent des réponses appropriées et l'application de politiques, y compris une déconnexion sécurisée immédiate et l'activation de workflows IT ou sécurité pour protéger l'entreprise et les utilisateurs compromis.	• Adaptive Multi-Factor Authentication • Identity Threat Protection • Identity Security Posture Management • Workflows

okta

Gestion des accès

Selon le modèle ZTMM de la CISA, le concept de gestion des accès est axé sur la gouvernance et l'administration des identités (IGA, Identity Governance and Administration). Dès lors, les quatre stades décrivent la maturité de l'implémentation et des processus, plutôt que d'aborder des solutions techniques. Néanmoins, la capacité d'une entreprise à implémenter des politiques IGA requiert la mise en place de certaines fonctionnalités.

En général, une entreprise immature dispose de processus manuels de contrôle des accès, de privilèges d'accès à très longue durée et d'autorisations très larges et peu précises. Cette combinaison entraîne généralement un provisioning excessif des accès et des combinaisons toxiques (p. ex. un seul utilisateur peut à la fois demander et approuver une élévation des privilèges), ce qui offre de nombreuses possibilités d'abus. De plus, l'évolutivité n'est tout simplement pas au rendez-vous.

En revanche, une entreprise mature tire pleinement parti de l'automatisation, n'accorde un accès qu'en cas de nécessité, sans aucun privilège permanent, et octroie des accès de manière extrêmement précise, conformément au principe du moindre privilège.

Gouvernance et administration des identités

La fonction Gestion des accès du modèle ZTMM de la CISA se rapporte au concept d'IGA, une approche de la gestion des identités et du contrôle des accès basée sur des politiques qui combine :

- **Gouvernance des identités :** processus et politiques s'appliquant à la séparation des tâches, à la gestion des rôles, à la journalisation, aux vérifications des accès, aux analyses et au reporting
- **Administration des identités :** gestion des comptes et des identifiants, provisioning et déprovisioning des utilisateurs et des terminaux, et gestion des droits

Stade	Description	Solutions Okta associées
 **Fondamental**	À ce stade, probablement plus courant dans les petites entreprises, l'accès aux comptes à privilèges et aux comptes standard est généralement autorisé de manière permanente, avec des vérifications périodiques uniquement. L'accès n'est pas contextuel, l'application est limitée et l'accès est probablement suivi manuellement (p. ex. dans une feuille de calcul).	• Okta Identity Governance • Identity Security Posture Management
 **Évolutif**	L'accès aux comptes à privilèges et aux comptes standard est suivi via des vérifications automatisées. La principale différence au stade Évolutif est que l'accès expire avec les vérifications automatisées, sauf prolongation. Les informations utilisées pour prendre des décisions en matière d'accès restent limitées et peuvent être fondées sur le rôle plutôt que sur les besoins ou les logs d'accès antérieurs, ce qui peut entraîner un accès de longue durée. Les entités peuvent également obtenir des privilèges excessifs en raison de la granularité limitée du contrôle des accès.	• Okta Identity Governance • Identity Security Posture Management • Okta Privileged Access • Fine-Grained Authorization
 **Avancé**	L'accès est géré en fonction des besoins et des sessions, adapté aux actions et aux ressources, et résilié automatiquement ; le principe du moindre privilège est appliqué avec un accès sans mot de passe limité dans le temps et en flux tendu, en particulier pour les infrastructures critiques telles que les serveurs. Cette stratégie s'étend également à la manière dont l'accès est géré pour la connexion aux terminaux, qui est fondée sur les risques et les politiques définies. L'implémentation intègre des conditions granulaires basées sur la posture du terminal, le réseau et les signaux de risque comportementaux.	• Okta Identity Governance • Identity Security Posture Management • Okta Privileged Access • Fine-Grained Authorization • Workflows • Okta Device Access
 **Stratégique**	Le principe du moindre privilège et les politiques d'autorisation d'accès en flux tendu sont désormais automatisées, adaptant l'accès aux actions individuelles et aux besoins en ressources, ce qui permet d'éliminer les privilèges permanents. L'application des politiques d'accès est totalement adaptative et réagit aux signaux en temps réel de l'ensemble de la pile technologique. Les décisions relatives à l'authentification et à la session sont basées sur une évaluation continue. L'authentification renforcée basée sur les risques et d'autres actions sont automatisées et exécutées en temps réel, ce qui améliore l'expérience utilisateur tout en préservant la posture de sécurité.	• Okta Identity Governance • Identity Security Posture Management • Okta Privileged Access • Fine-Grained Authorization • Workflows • Okta Device Access

okta

Visibilité et analyses

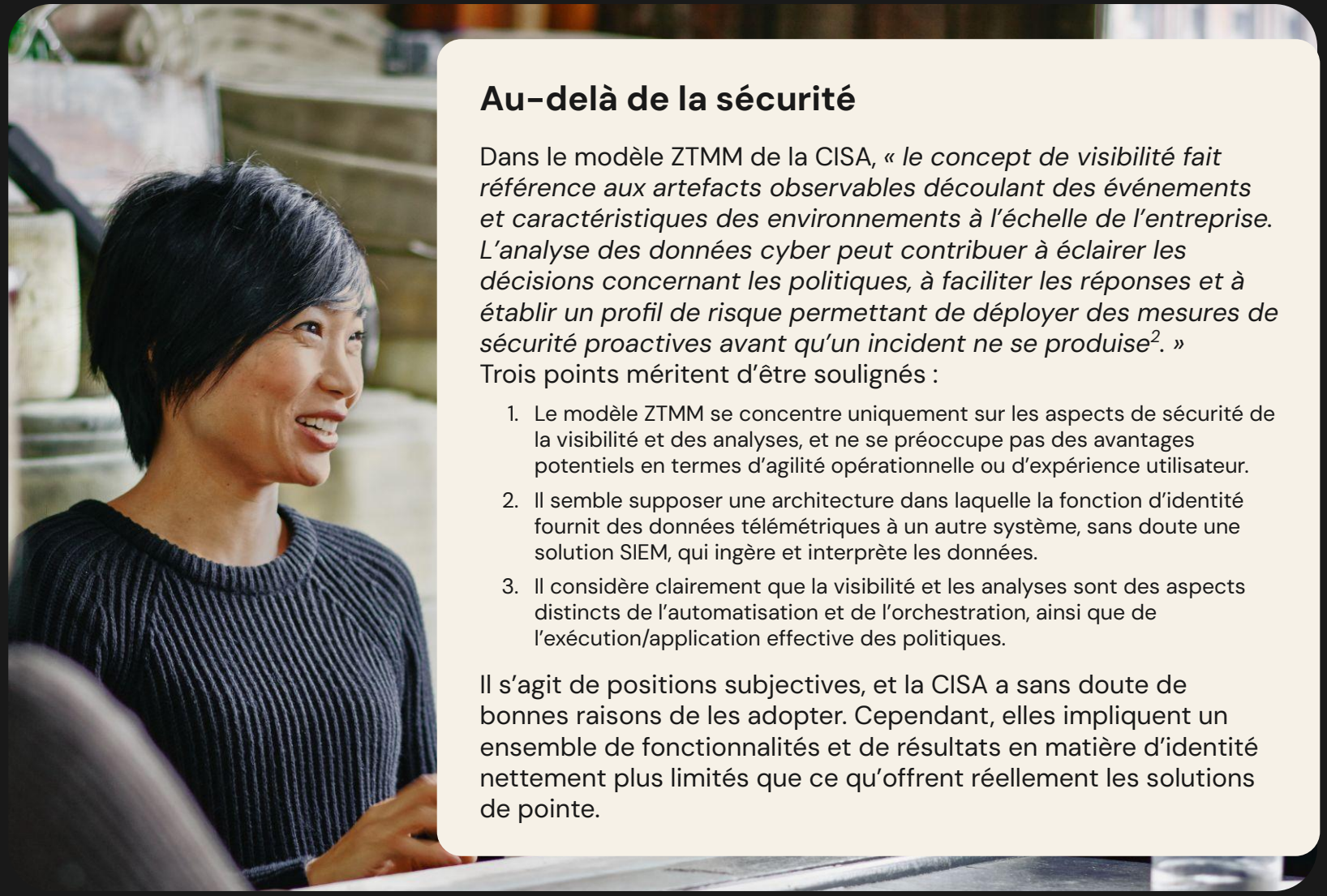
Mieux une entreprise appréhende la façon dont ces entités utilisent les systèmes d'identité, mieux elle peut :

- Améliorer l'agilité opérationnelle
  (p. ex. en automatisant les workflows)
- Optimiser l'expérience utilisateur
  (p. ex. en affinant les politiques de gestion des accès)
- Renforcer la sécurité
  (p. ex. en implémentant des mesures de prévention, de détection et de réponse)

Certaines solutions d'identité peuvent détecter les risques en temps réel, souvent plus rapidement et avec plus de précision que les outils de sécurité généraux, sans qu'il soit nécessaire d'envoyer des données à un SIEM. Autre aspect important : les analyses locales peuvent compléter les systèmes externes.

Certaines solutions d'identité appliquent aussi directement des politiques en réponse aux menaces, par exemple en empêchant l'authentification ou en déconnectant les utilisateurs compromis. Grâce à la détection en temps réel offerte par la même solution, cette combinaison efficace permet d'atténuer rapidement les menaces, renforçant ainsi la posture de sécurité de l'entreprise.

Les résultats obtenus varient toutefois en fonction de la plateforme d'identité et de ses fonctionnalités de télémétrie.



Au-delà de la sécurité

Dans le modèle ZTMM de la CISA, « *le concept de visibilité fait référence aux artefacts observables découlant des événements et caractéristiques des environnements à l'échelle de l'entreprise. L'analyse des données cyber peut contribuer à éclairer les décisions concernant les politiques, à faciliter les réponses et à établir un profil de risque permettant de déployer des mesures de sécurité proactives avant qu'un incident ne se produise*[2]. »
Trois points méritent d'être soulignés :

1. Le modèle ZTMM se concentre uniquement sur les aspects de sécurité de la visibilité et des analyses, et ne se préoccupe pas des avantages potentiels en termes d'agilité opérationnelle ou d'expérience utilisateur.
2. Il semble supposer une architecture dans laquelle la fonction d'identité fournit des données télémétriques à un autre système, sans doute une solution SIEM, qui ingère et interprète les données.
3. Il considère clairement que la visibilité et les analyses sont des aspects distincts de l'automatisation et de l'orchestration, ainsi que de l'exécution/application effective des politiques.

Il s'agit de positions subjectives, et la CISA a sans doute de bonnes raisons de les adopter. Cependant, elles impliquent un ensemble de fonctionnalités et de résultats en matière d'identité nettement plus limités que ce qu'offrent réellement les solutions de pointe.

[2] CISA. Zero Trust Maturity Model, version 2.0. Avril 2023, p. 11. Consulté le 9 juin 2025 à l'adresse https://www.cisa.gov/sites/default/files/2023-04/zero_trust_maturity_model_v2_508.pdf.

okta

Stade	Description	Solutions Okta associées
 **Fondamental**	À ce stade, l'entreprise collecte les logs d'activité liés à l'identité, en accordant une attention particulière aux identifiants à privilèges. Bien que l'analyse des logs puisse être effectuée de manière routinière, elle est réalisée manuellement. Ces analyses sont donc comparativement incapables d'identifier les risques en temps utile ou les menaces avancées.	• Universal Directory
 **Évolutif**	En plus de l'analyse manuelle des logs, l'entreprise profite désormais d'analyses automatisées. Toutefois, si les analyses automatisées améliorent la rapidité de la détection, la corrélation limitée entre les types de logs entrave toujours la détection des menaces avancées.	• Universal Directory • Workflows
 **Avancé**	Les analyses sont désormais entièrement automatisées (ou presque), avec une corrélation entre les types de logs, mais sans inclure tous les types de logs sur les utilisateurs et les entités. Les logs sur les identités sont également reliés à d'autres sources, ce qui permet d'éliminer les lacunes en matière de visibilité et d'offrir des fonctionnalités de détection des menaces plus complètes.	• Universal Directory • Workflows • Identity Threat Protection
 **Stratégique**	L'entreprise obtient et conserve une visibilité complète grâce à l'analyse automatisée de tous les types de logs d'utilisateurs et d'entités, reliés à d'autres sources.	• Universal Directory • Workflows • Identity Threat Protection

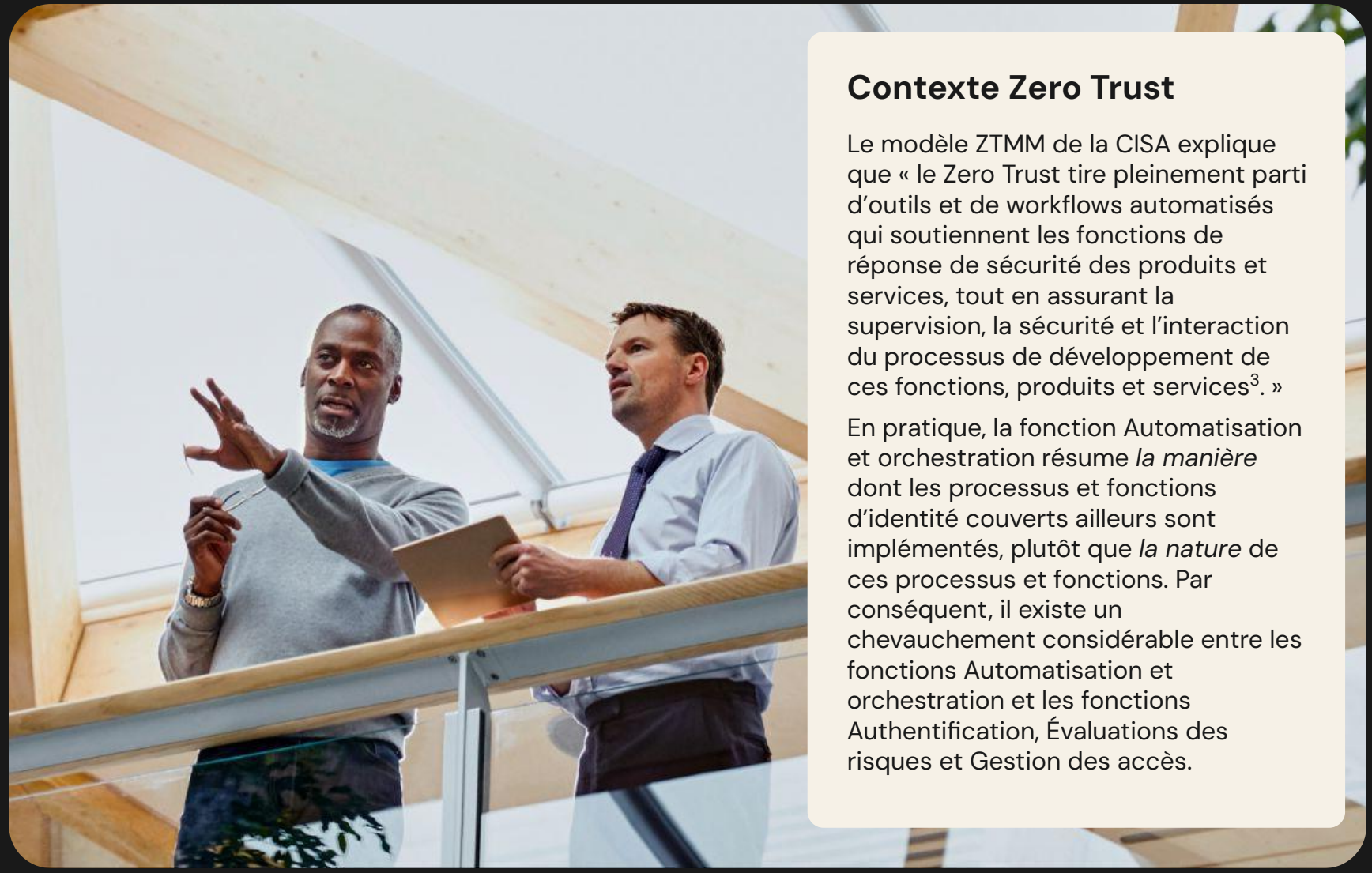
okta

Automatisation et orchestration

La mesure dans laquelle une entreprise peut faire évoluer ses fonctionnalités d'automatisation et d'orchestration des identités dépend fortement des plateformes et des produits d'identité qu'elle déploie.

Les solutions d'identité les plus puissantes ne prendront pas seulement en charge l'automatisation et l'orchestration en s'intégrant à la pile technologique au sens large, mais offriront elles-mêmes de telles fonctionnalités.

Ces fonctionnalités intégrées permettent de créer des workflows pour gérer le cycle de vie des identités (dont les processus de recrutement, mutation et départ), favoriser une gouvernance solide, contrôler les accès à privilèges, renforcer la posture de sécurité, etc. sans avoir besoin d'un outil d'automatisation et d'orchestration généraliste.



Contexte Zero Trust

Le modèle ZTMM de la CISA explique que « le Zero Trust tire pleinement parti d'outils et de workflows automatisés qui soutiennent les fonctions de réponse de sécurité des produits et services, tout en assurant la supervision, la sécurité et l'interaction du processus de développement de ces fonctions, produits et services[3]. »

En pratique, la fonction Automatisation et orchestration résume *la manière* dont les processus et fonctions d'identité couverts ailleurs sont implémentés, plutôt que *la nature* de ces processus et fonctions. Par conséquent, il existe un chevauchement considérable entre les fonctions Automatisation et orchestration et les fonctions Authentification, Évaluations des risques et Gestion des accès.

[3] CISA. Zero Trust Maturity Model, version 2.0. Avril 2023, p. 11. Consulté le 9 juin 2025 à l'adresse https://www.cisa.gov/sites/default/files/2023-04/zero_trust_maturity_model_v2_508.pdf.

Stade	Description	Solutions Okta associées
 **Fondamental**	À ce stade, l'entreprise travaille presque exclusivement avec des identités autogérées et exécute manuellement les processus de gestion du cycle de vie, y compris l'onboarding/offboarding, principalement par le biais de l'e-mail, d'applications de collaboration, de demandes d'assistance et d'outils similaires. Il y a peu d'intégration entre les différents systèmes, et les vérifications (p. ex. pour les privilèges d'accès) sont effectuées manuellement à une fréquence prédéterminée.	• Lifecycle Management • Workflows
 **Évolutif**	À ce stade, l'entreprise commence à implémenter un certain degré d'automatisation pour orchestrer les processus liés aux utilisateurs sans privilèges et aux identités autogérées. Le provisioning et le déprovisioning des utilisateurs sont de plus en plus souvent automatisés. L'entreprise continue d'orchestrer manuellement les identités à privilèges, mais gère désormais également les identités externes.	• Lifecycle Management • Workflows • Okta Identity Governance • Okta Privileged Access
 **Avancé**	À ce stade, l'entreprise bénéficie d'une intégration suffisante dans tous les environnements pour permettre l'automatisation et l'orchestration des identités internes et externes. Les identités à privilèges demeurent orchestrées manuellement. La détection et la correction des risques liés à l'identité sont automatisées, avec des fonctionnalités permettant d'identifier et de neutraliser les menaces potentielles de façon proactive.	• Lifecycle Management • Workflows • Okta Identity Governance • Okta Privileged Access
 **Stratégique**	Au stade Stratégique, tous les processus d'orchestration des identités sont automatisés, couvrent l'ensemble des identités et des environnements, et sont basés sur les comportements, les inscriptions et les besoins en matière de déploiement. L'entreprise a la possibilité d'automatiser les mesures correctives en déclenchant des processus en aval, adaptés à ses besoins spécifiques, une fois les risques détectés.	• Lifecycle Management • Workflows • Okta Identity Governance • Okta Privileged Access

okta

Gouvernance

La gouvernance des identités fait référence à la définition et à l'application par une entreprise de politiques, procédures et processus pour soutenir ses objectifs métier (p. ex. en implémentant les principes Zero Trust, en améliorant l'efficacité et en augmentant la productivité) et la conformité aux réglementations, frameworks, standards et obligations contractuelles.

Dans le contexte de la gouvernance, la maturité consiste à remplacer les approches cloisonnées et manuelles par des approches globales et automatisées. Cela comprend l'unification des politiques relatives aux identités humaines et non humaines, l'application de contrôles d'accès basés sur les rôles et les risques, ainsi que la mise à l'échelle de la gestion du cycle de vie et des processus de certification.

À mesure que les entreprises gagnent en maturité, la gouvernance passe de contrôles ponctuels à une automatisation continue et intelligente qui s'applique de manière égale aux API, aux comptes de service et aux processus robotiques. Les identités non humaines sont devenues une préoccupation centrale en ce qui concerne la gouvernance. Elles sont soumises au principe du moindre privilège, aux vérifications des accès et à une surveillance de la conformité à toutes les étapes du cycle de vie des identités.

Stade	Description	Solutions Okta associées
 **Fondamental**	La gouvernance des identités est très peu développée et les programmes existants ont tendance à être cloisonnés (plutôt qu'alignés sur des objectifs métier et de gouvernance partagés) ou autonomes, et axés uniquement sur les identités humaines. Il n'existe aucune supervision centralisée des identités non humaines, qui prolifèrent souvent sans contrôle, ce qui accroît les risques.	• Lifecycle Management • Workflows
 **Évolutif**	L'entreprise a simplifié certains aspects de la gouvernance et de la conformité grâce à l'automatisation des vérifications des accès et des flux de demande d'accès. La gouvernance devient plus structurée grâce à des modèles basés sur les rôles. Le provisioning et le déprovisioning sont automatisés en fonction des événements du cycle de vie, et les certifications d'accès sont programmées périodiquement. Des contrôles des identités non humaines en amont peuvent être implémentés et consistent généralement en une automatisation de base du cycle de vie des comptes de service et des bots.	• Lifecycle Management • Workflows • Okta Identity Governance • Okta Privileged Access
 **Avancé**	L'entreprise a mis en place des pratiques opérationnelles et de gouvernance matures pour que l'identité puisse continuellement s'adapter aux besoins métier et apporter une valeur ajoutée. L'accès est régi par des contrôles dynamiques basés sur des politiques qui tiennent compte des attributs des utilisateurs, des niveaux de risque et des règles métier. Un accès en flux tendu et limité dans le temps est implémenté. Les demandes à haut risque déclenchent des approbations « humain dans la boucle » (human-in-the-loop), et la séparation des tâches est appliquée pour prévenir tout accès contradictoire. La gouvernance des identités non humaines est mise en place de manière systématique, en appliquant le principe du moindre privilège, des vérifications et des contrôles du cycle de vie semblables à ceux appliqués aux utilisateurs humains.	• Lifecycle Management • Workflows • Okta Identity Governance • Okta Privileged Access
 **Stratégique**	L'entreprise tire parti de l'IA pour renforcer la sécurité et la gouvernance des identités, optimiser l'expérience utilisateur et simplifier la configuration et le développement. La gouvernance est continue et proactive. Les décisions d'octroi d'accès sont autonomes et tiennent compte des risques. Elles sont guidées par des analyses prédictives et des politiques unifiées dans les environnements cloud, hybrides et on-premise. Les certifications auparavant périodiques sont orientées événements, les identités non humaines étant pleinement intégrées aux processus de gouvernance adaptative. La supervision « humain dans la boucle » (human-in-the-loop) n'est appliquée qu'aux scénarios à haut risque, garantissant une gouvernance adaptative qui concilie automatisation et intervention intelligente. La gouvernance autonome des identités non humaines, avec analyse des risques, automatisation de l'accès et correction intelligente, devient une fonctionnalité essentielle.	• Lifecycle Management • Workflows • Okta Identity Governance • Okta Privileged Access

okta

Conclusion

Bien que le parcours d'identité de chaque entreprise soit unique, il existe néanmoins des points communs et des schémas récurrents.

En accordant la priorité à la maturité de l'identité, une entreprise peut bénéficier d'une posture de sécurité renforcée, d'effectifs plus productifs, d'une efficacité opérationnelle améliorée et d'une croissance continue de ses activités.