Insight

Sécurité des identités :
Guide Stratégique Pour Acheteurs

Sommaire

Sécurité des Identités : Guide Stratégique Pour Acheteurs

Dans les entreprises modernes, chaque connexion utilisateur, chaque compte de service et chaque connexion tierce est un risque potentiel. Avec le travail hybride, les applications Cloud et l'IA qui redessinent l'entreprise, les attaquants ciblent désormais les identités – et non les pare-feux. Pourquoi s'introduire par effraction quand on peut voler une identité et se connecter ? protéger les identités numériques est l'un des moyens les plus efficaces pour prévenir les failles, maîtriser l'accès et maintenir la confiance.

L'identité est devenu le principal vecteur d'attaque :

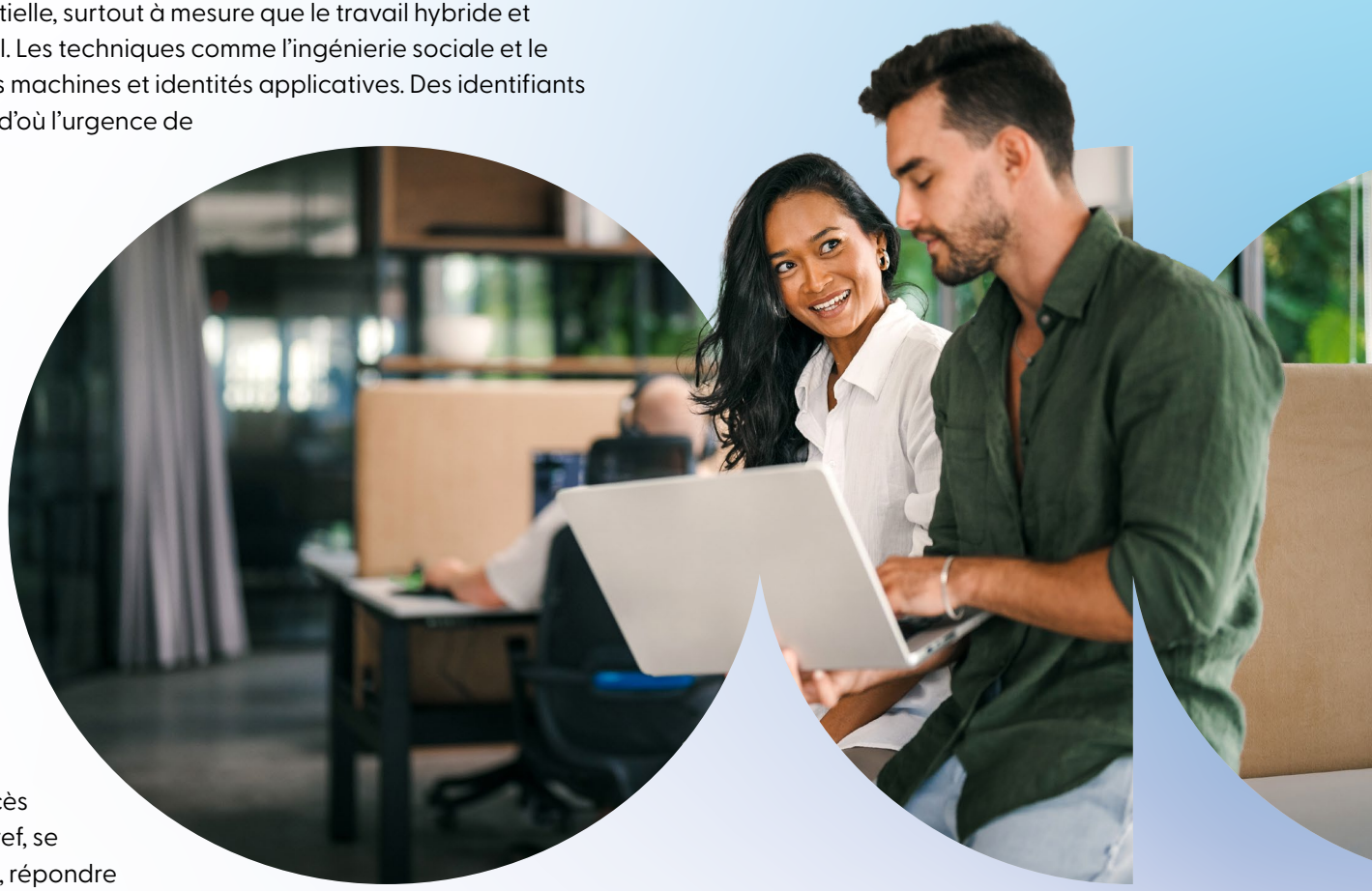
93 % des organisations ont connu au moins **deux attaques liées à l'identité** l'an dernier.*

Pour les leaders sécurité, protéger les identités est désormais critique. Ce guide clarifie IAM, IGA, PAM, ITDR, MFA, etc., et explique l'importance de chacun pour votre organisation. Il souligne aussi comment Insight, avec un partenariat Microsoft de premier plan, peut vous aider à bâtir un programme complet de sécurité des identités.

*https://investors.cyberark.com/news/news-details/2024/Report-93-Of-Organizations-Had-Two-or-More-Identity-Related-Breaches-in-the-Past-Year/)

Pourquoi la Sécurité des Identités Compte

Les entreprises modernes font face à une explosion d'identités – des employés et clients aux bots logiciels et services Cloud. Chacune représente une porte d'entrée potentielle, surtout à mesure que le travail hybride et l'adoption du Cloud dissolvent le périmètre réseau traditionnel. Les techniques comme l'ingénierie sociale et le vol d'identifiants ciblent autant les utilisateurs que les comptes machines et identités applicatives. Des identifiants faibles ou volés sont en cause dans la majorité des violations, d'où l'urgence de protections d'identité solides.



On estime que **86** % des violations impliquent le vol d'identifiants**

Au-delà du risque immédiat, de mauvaises pratiques d'identité entraînent : accès non autorisés aux données sensibles, non-conformité réglementaire, arrêts opérationnels et perte de confiance. À l'inverse, un programme robuste active les principes de Zero Trust (« ne jamais faire confiance par défaut, toujours vérifier ») afin que seules les bonnes personnes (ou systèmes) obtiennent le bon accès, dans les bonnes conditions. Cela améliore aussi l'expérience utilisateur en remplaçant le chaos (multiplication des connexions, processus manuels) par un accès fluide et sécurisé – productivité sans sacrifier la sécurité. En bref, se concentrer sur la sécurité des identités aide à réduire le risque, répondre aux obligations et donner confiance dans l'accès aux ressources.

**https://keepnetlabs.com/blog/top-phishing-statistics-and-trends-you-must-know

Piliers Clés de la Sécurité des Identités

Pour protéger l'organisation, la sécurité des identités doit couvrir plusieurs domaines. Ce n'est pas un produit unique mais un ensemble de capacités interconnectées qui répondent à : qui (ou quoi) peut accéder à quoi, quand et comment ? le schéma ci-dessous illustre l'ensemble des capacités – de la gestion des identités et des privilèges à la surveillance des menaces.

Cadre de stratégie d'identité Insight

Identités & accès
Qui accède à quoi ?

Fondations d'identité

- Services d'annuaire
- Fédération/ B2B
- Approvisionnement et désaprovisionnement
- Identité client / B2C

Authentification

Incluant MFA, résistante au phishing et sans mot de passe

Autorisation

Authentification unique

Libre-service utilisateur

Gouvernance et administration des identités (IGA)
Doivent-ils toujours avoir accès ?

Gouvernance d'identité

- Revues/certifications d'accès ;
- Gestion de la conformité ;
- Audit

Administration de l'identité

- Gestion des workflows

Accès privilégiés

- Découverte de comptes
- Gestion des identifiants
- Enregistrement de session
- Élévation et délégation des privilèges

Détection et Résonance des Menaces d'Identité (IDTR)
Sommes-nous attaqués ?

Détection des menaces

- Détection d'anomalies et analyse comportementale utilisateurs/entités (UEBA)

Réponses aux menaces

- Suspension de comptes, réinitialisation forcée des mots de passe,
- Ré-autorisation ou authentification renforcée

Gestion de L'identité et des Accès (IAM)

La gestion des identités et des accès (IAM) est le fondement d'une stratégie de sécurité des identités. Elle consiste à établir et à gérer les identités numériques (des employés, des partenaires, des clients et même des comptes logiciels) et à contrôler leur accès aux ressources. L'IAM couvre. La création d'identités utilisateur dans les systèmes d'annuaire, l'attribution de comptes aux applications et les services d'authentification tels que l'authentification unique. Elle « établit la base de référence pour déterminer qui ou quoi doit avoir accès à quoi » dans l'organisation. Dans la pratique, les solutions IAM (telles que Microsoft Entra ID, anciennement Azure AD) permettent aux utilisateurs de. Se connecter de manière sécurisée et pratique, d'appliquer des politiques de mot de passe ou de se connecter sans mot de passe.

Pourquoi est-ce important ? : Une base IAM solide garantit que seuls les utilisateurs authentifiés et autorisés peuvent accéder aux ressources sensibles, réduisant ainsi le risque d'accès non autorisé. L'IAM centralisé améliore la sécurité et l'expérience utilisateur en éliminant la prolifération des mots de passe et en permettant aux utilisateurs professionnels d'accéder aux ressources dont ils ont besoin (par exemple, grâce à l'authentification unique pour les applications cloud). Il jette également les bases nécessaires à la mise en œuvre de politiques de sécurité telles que l'authentification multifactorielle et l'accès conditionnel dans toute l'entreprise. Sans une gestion des identités et des accès (IAM) efficace, les organisations sont souvent confrontées à des contrôles d'accès incohérents

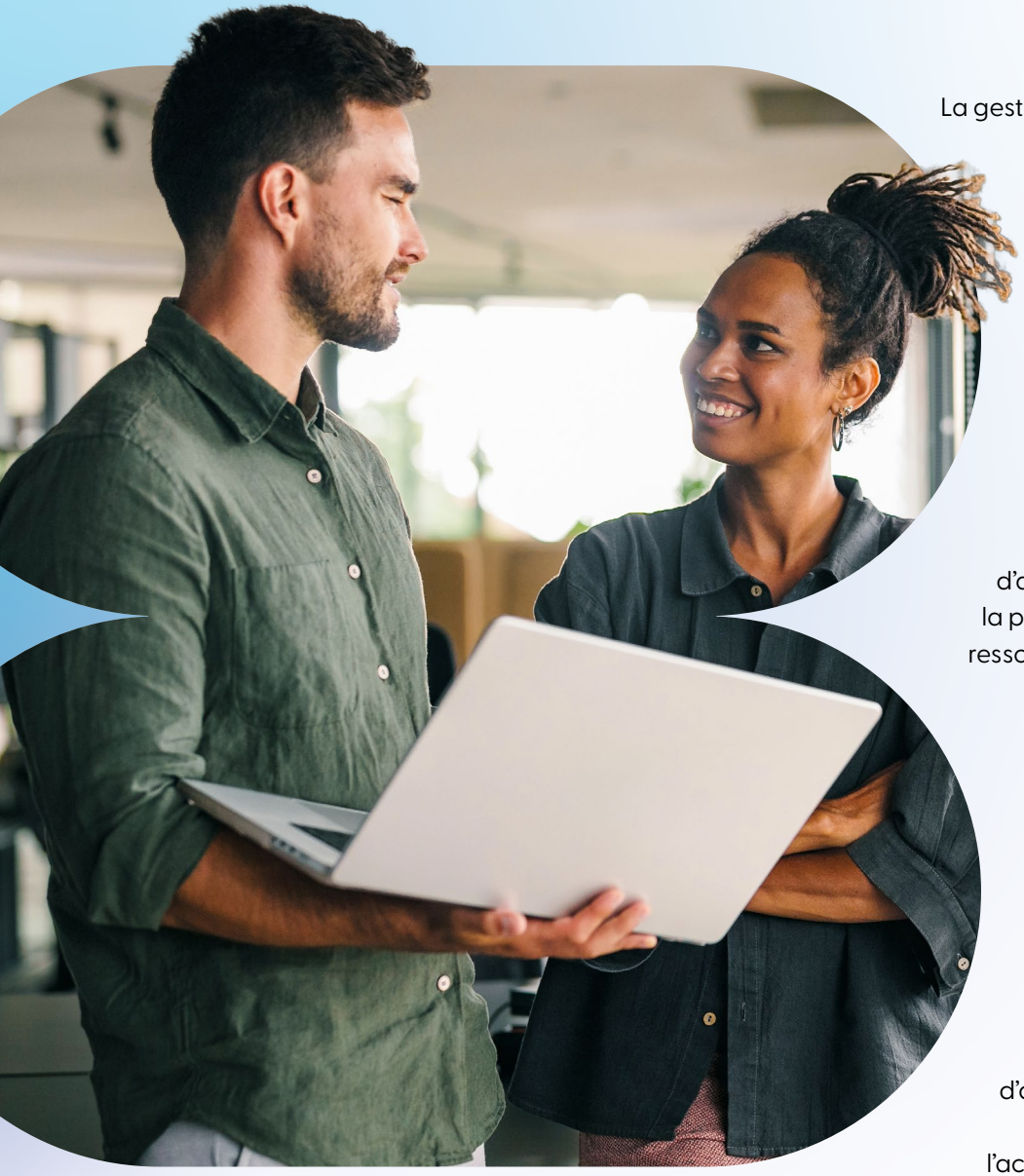
Et à des « silos » d'identités, ce qui entraîne des failles de sécurité, des utilisateurs frustrés et des conclusions d'audit. En résumé, la gestion des identités et des accès (IAM) est cruciale tant pour la productivité que pour la sécurité, car elle constitue la première ligne de défense contre l'utilisation abusive des identités. Les principales fonctionnalités de l'IAM comprennent généralement : des services d'annuaire pour stocker et vérifier. Les identités des utilisateurs, des mécanismes d'authentification (des mots de passe à la biométrie et à l'authentification multifactorielle), la fédération pour les connexions des partenaires ou des clients (B2B/B2C) et des processus d'attribution/retrait des droits d'accès pour accorder et révoquer l'accès lorsque des personnes rejoignent, changent de poste ou quittent l'entreprise. Les systèmes IAM modernes mettent l'accent sur une authentification forte et un accès contextuel (abordés plus en détail ci-dessous), car les pirates informatiques ciblent de plus en plus les identifiants de connexion.

Identity Governance and Administration (IGA)

L'iga prolonge l'IAM en gouvernant la pertinence des accès dans le temps. Si l'IAM crée identités et accès, l'IGA s'assure que ces droits restent appropriés et conformes à mesure que l'organisation et les rôles évoluent. En pratique, cela recouvre des certifications périodiques d'accès par les managers, des workflows d'approbation des demandes, des politiques de séparation des tâches pour éviter les combinaisons toxiques, et l'audit des données d'identité.

Pourquoi c'est important : L'IGA est essentielle pour la conformité, la sécurité et l'efficacité. Sans gouvernance, les utilisateurs accumulent des privilèges excessifs ou conservent l'accès à des systèmes dont ils n'ont plus besoin (changement de poste, départ). Ce « privilege creep » crée des vulnérabilités et des échecs d'audit. L'IGA permet d'appliquer le moindre privilège et fournit des preuves pour les réglementations (GDPR, NIS2) que l'accès aux données sensibles est correctement contrôlé et revu. En automatisant revues et approbations, l'IGA réduit la charge manuelle et rend la gestion des accès plus évolutive.

Gestion des Accès Privilégiés (PAM)



La gestion des identités et des accès (IAM) est le fondement d'une stratégie de sécurité des identités. Elle consiste à établir et à gérer les identités numériques (des employés, des partenaires, des clients et même des comptes logiciels) et à contrôler leur accès aux ressources. L'IAM couvre. La création d'identités utilisateur dans les systèmes d'annuaire, l'attribution de comptes aux applications et les services d'authentification tels que l'authentification unique. Elle « établit la base de référence pour déterminer qui ou quoi doit avoir accès à quoi » dans l'organisation. Dans la pratique, les solutions IAM (telles que Microsoft . Entra ID, anciennement Azure AD) permettent aux utilisateurs de
Se connecter de manière sécurisée et pratique, d'appliquer des politiques de mot de passe ou de se connecter sans mot de passe.

Pourquoi est-ce important ? : Une base IAM solide garantit que seuls les utilisateurs authentifiés et autorisés peuvent accéder aux ressources sensibles, réduisant ainsi le risque d'accès non autorisé. L'IAM centralisé améliore la sécurité et l'expérience utilisateur en éliminant la prolifération des mots de passe et en permettant aux utilisateurs professionnels d'accéder aux ressources dont ils ont besoin (par exemple, grâce à l'authentification unique pour les applications cloud). Il jette également les bases nécessaires à la mise en œuvre de politiques de sécurité telles que l'authentification multifactorielle et l'accès conditionnel dans toute l'entreprise. Sans une gestion des identités et des accès (IAM) efficace, les organisations sont souvent confrontées à des contrôles d'accès incohérents. Et à des « silos » d'identités, ce qui entraîne des failles de sécurité, des utilisateurs frustrés et des conclusions d'audit. En résumé, la gestion des identités et des accès (IAM) est cruciale tant pour la productivité que pour la sécurité, car elle constitue la première ligne de défense contre l'utilisation abusive des identités. Les principales fonctionnalités de l'IAM comprennent généralement : des services d'annuaire pour stocker et vérifier. Les identités des utilisateurs, des mécanismes d'authentification (des mots de passe à la biométrie et à l'authentification multifactorielle), la fédération pour les connexions des partenaires ou des clients (B2B/B2C) et des processus d'attribution/retrait des droits d'accès pour accorder et révoquer l'accès lorsque des personnes rejoignent, changent de poste ou quittent l'entreprise. Les systèmes IAM modernes mettent l'accent sur une authentification forte et un accès contextuel (abordés plus en détail ci-dessous), car les pirates informatiques ciblent de plus en plus les identifiants de connexion.

Authentification Forte et Contrôle d'accès

Une authentification efficace sous-tend tous les domaines d'identité susmentionnés. L'authentification est le processus qui consiste à vérifier qu'un utilisateur ou un système est bien celui qu'il prétend être. Une authentification faible (comme le recours exclusif à des mots de passe) est un maillon faible connu : les mots de passe peuvent être devinés, volés ou piratés. L'authentification forte exige plusieurs facteurs (MFA) ou des méthodes modernes difficiles à contourner.
Pour les utilisateurs : codes à usage unique, applications d'authentification, clés physiques de sécurité, biométrie – en complément ou à la place du mot de passe.
Pour les identités systèmes (APIs, comptes de service), l'authentification forte implique d'éliminer les mots de passe statiques au profit de certificats ou de tokens, avec une gestion de clés sécurisée.

Pourquoi c'est important : Selon Microsoft, la MFA empêche 99,9 % des compromissions de comptes utilisateurs. En imposant la MFA à l'échelle, le risque chute fortement – même si un mot de passe est volé, l'attaquant ne peut fournir le second facteur. Les politiques d'accès conditionnel (adaptées au contexte/risque) renforcent encore l'authentification : si une tentative provient d'un lieu inhabituel ou d'un appareil non sain, exiger des vérifications supplémentaires ou bloquer l'accès. Cela assure la sécurité sans gêner indûment les légitimes.

Détection et réponse aux menaces d'identité (ITDR)

Même avec des mesures préventives, il faut supposer que certaines compromissions surviendront (phishing, comptes hérités compromis). L'ITDR se concentre sur la détection et l'atténuation des attaques centrées sur l'identité en temps réel ; il surveille l'usage abusif ou la compromission d'identités et observe des schémas anormaux révélateurs d'usurpation ou d'utilisation non autorisée des identifiants.
Cela inclut des outils qui analysent les comportements de connexion (voyage impossible, heures inhabituelles, changements d'appareil ou d'IP), détectent des attaques sur l'infrastructure d'annuaire (élévation de privilèges dans Active Directory, abus de tokens SSO) et s'intègrent aux opérations de sécurité pour répondre aux menaces sur les identités.

Pourquoi c'est clé : La surveillance traditionnelle se concentre sur les Endpoints et les réseaux, mais des attaquants modernes les contournent via des faiblesses d'identité – en utilisant des identifiants valides pour se connecter puis élever silencieusement leurs privilèges. L'ITDR comble cette lacune en apportant une détection dédiée aux attaques identitaires, qui peuvent passer inaperçues ailleurs. Microsoft met l'accent sur l'union de la protection d'identité et des opérations de sécurité – partage des signaux entre systèmes d'identité et Centre des opérations de sécurité (SOC) pour stopper rapidement les attaques.
En termes métier, l'ITDR réduit la probabilité qu'une compromission d'identité se transforme en incident majeur et limite le rayon d'action en détectant et en réagissant tôt.

Élaborer un programme complet de sécurité des identités

Comprendre les différents éléments est un bon début, mais comment les assembler de manière stratégique ? Une sécurité des identités efficace repose autant sur les personnes et les processus que sur la technologie. Voici les étapes clés et les meilleures pratiques pour mettre en œuvre un programme holistique :Bâtir un programme complet de sécurité des identités

Evaluer et inventorier toutes les identités et leurs accès : Identités humaines et non humaines (comptes de service, rôles Cloud…), accès associés ; identifier les identités à risque (domaines admins, comptes fournisseur tiers) et les comptes orphelins. Ceci révèle les écarts (privilèges excessifs, apps sans MFA) et alimente les priorités.

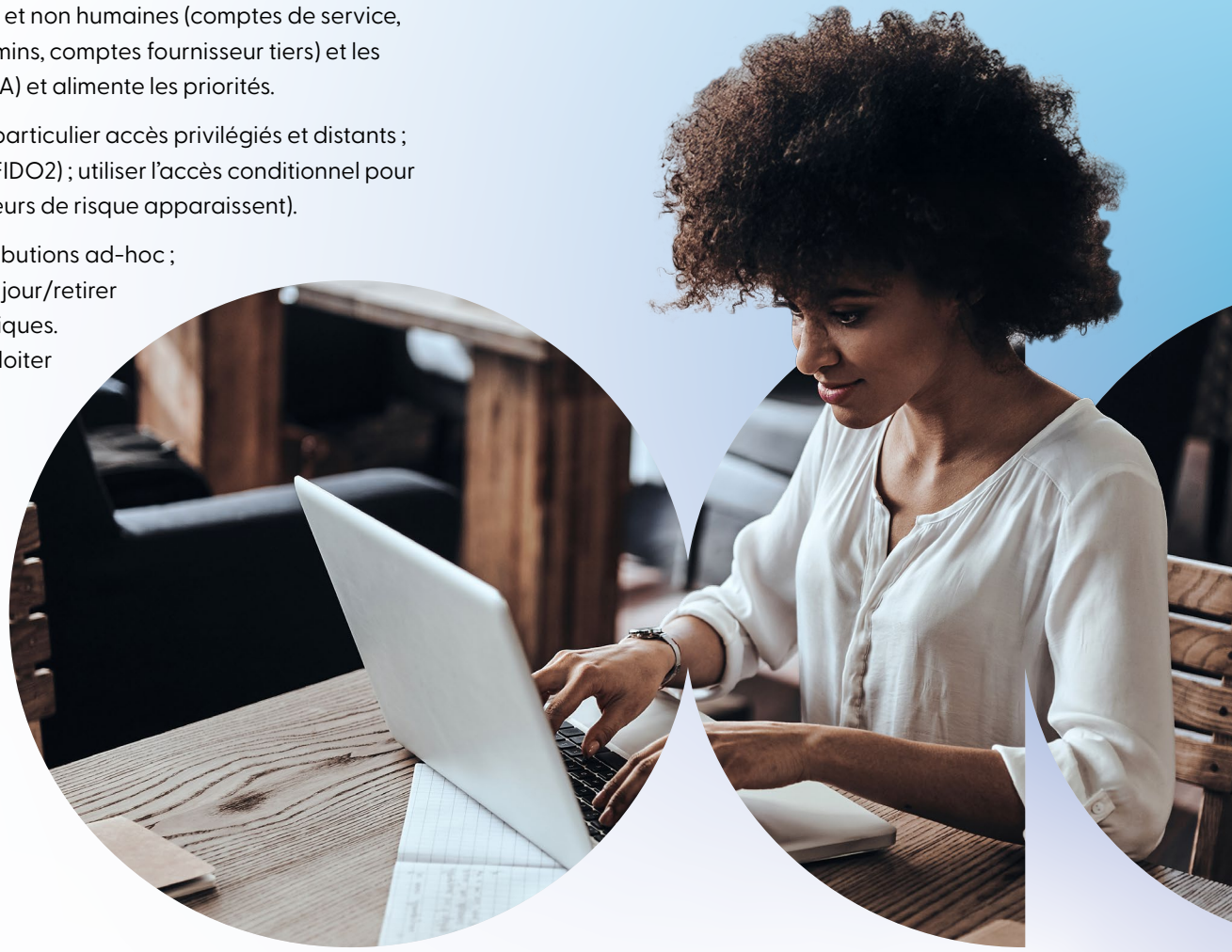
Imposer une authentification forte partout : MFA obligatoire pour tous, en particulier accès privilégiés et distants ; déployer des méthodes avancées comme le passwordless (biométrie, clés FIDO2) ; utiliser l'accès conditionnel pour adapter selon le risque (exiger la MFA pour apps sensibles ou si des indicateurs de risque apparaissent).

Adopter le moindre privilège via IAM & IGA : Rôles RBAC pour éviter les attributions ad-hoc ; processus de cycle de vie : à l'arrivée, lors des mobilités, au départ, mettre à jour/retirer les accès ; réaliser des revues régulières (attestations) pour les systèmes critiques.

Sécuriser et surveiller l'accès privilégié : Envisager une solution PAM ou exploiter les fonctions Cloud (ex. Entra Privileged Identity Management) ; mettre en coffre les mots de passe admin ; check-out avec approbations ; élévation JIT ; enregistrer les sessions ; alertes sur activités privilégiées inhabituelles ; durcir l'infrastructure d'annuaire (Active Directory/Entra ID) en tant qu'actif « tier 0 ».

Intégrer les signaux d'identité dans la détection : Envoyer logs d'IAM/annuaire/SSO vers le SIEM/SOC ; déployer Entra ID Protection et Microsoft Defender for Identity ; playbooks de réponse (désactiver compte, reset mot de passe, exiger ré-auth) ; simulations régulières (ex. exercice phishing).

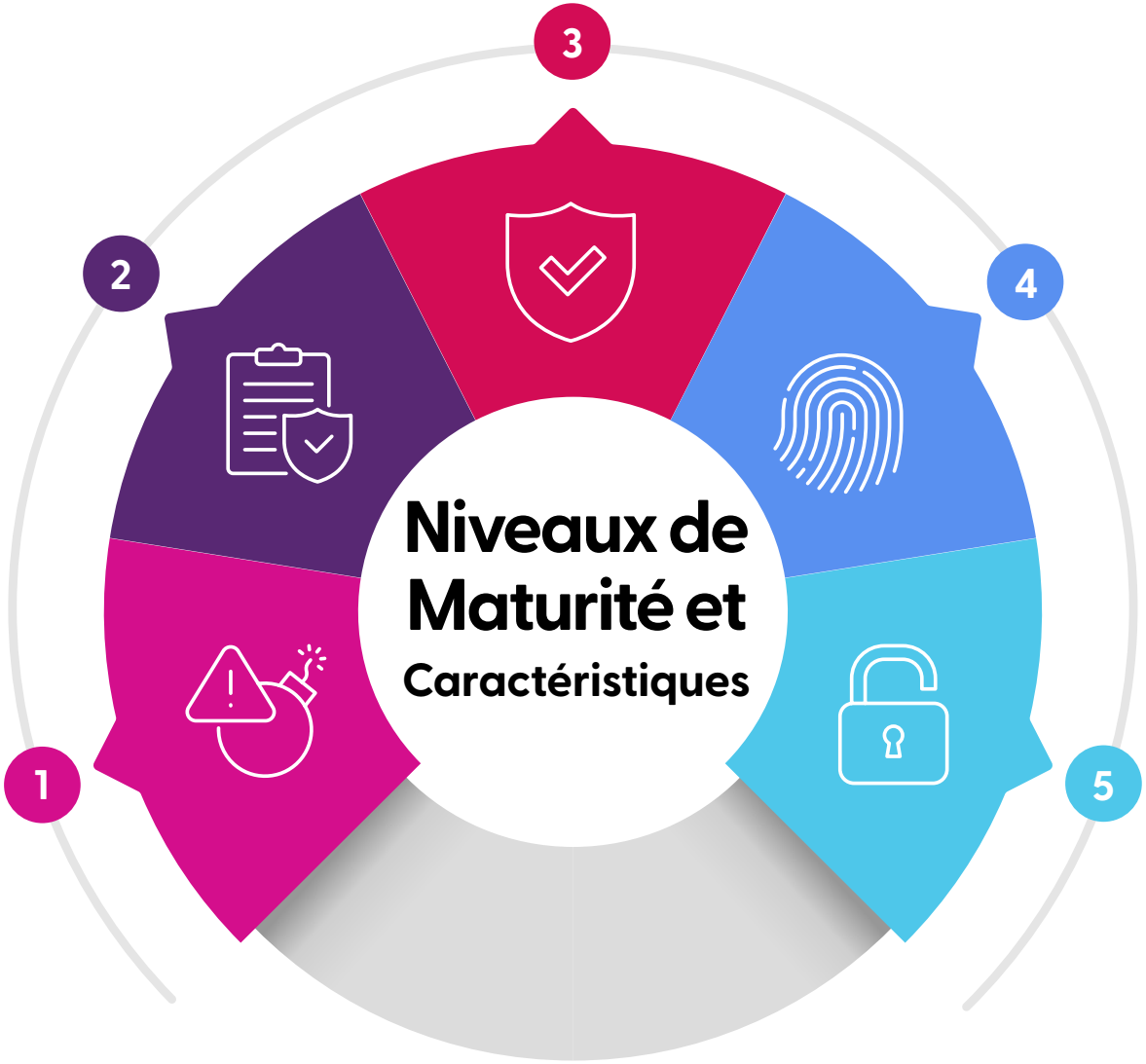
Instaurer une culture sécurité : Sensibiliser aux bonnes pratiques (reconnaître phishing, gestion de mots de passe/secrets, ne jamais partager des identifiants) ; politiques et formations ; partenariat étroit entre administrateurs d'identité et équipe sécurité.



Maturité Identité

Géré
Provisioning automatisé, SSO sur les applications majeures, contrôles d'accès privilégiés, revues d'accès routinières.

Référence
Annuaires centralisés, MFA pour certains utilisateurs, RBAC basique, audits occasionnels.



Optimisé
Politiques d'accès conditionnel, détection de menaces fondée sur l'identité, gouvernance solide.

Adhoc
Systèmes déconnectés, hygiène de mots de passe faible, approvisionnement manuel, peu ou pas de MFA.

Adaptatif
Accès piloté par le risque, sans mots de passe, détection portée par l'IA, aligné sur Zero Trust et les résultats business.

Détection et Réponse aux Menaces

la sécurité des identités ne se limite plus au contrôle d'accès. Elle devient une base dynamique, pilotée par l'intelligence, qui permet une collaboration sécurisée, un accès décentralisé et l'automatisation à l'échelle. Avec l'adoption du Cloud, le travail hybride et l'IA, l'identité évolue d'un garde-barrière réactive vers une défense proactive et un moteur pour le business.

Voici les tendances qui façonnent l'avenir – et leurs impacts.

Avenir de la Sécurité des Identités

Identité décentralisée et justificatifs vérifiables.

L'identité décentralisée (DID) permet aux utilisateurs de gérer/contrôler leurs données d'identité sans autorité centrale. Les identités s'appuient sur des justificatifs vérifiables, stockés hors-chaîne dans des portefeuilles numériques sécurisés et validés par cryptographie ou registres distribués. Microsoft investit via Entra Verified ID pour soutenir ce basculement.

Pourquoi c'est important :
Ce modèle réduit la dépendance aux fournisseurs d'identité et permet de valider des attributs (statut employé, certifications, état de santé) sans stocker les données personnelles. Dans l'éducation, les pouvoirs publics et la santé, il renforce la confidentialité, prévient la fraude et simplifie la conformité (ex. GDPR). À mesure que l'adoption progresse, il faut des stratégies pour émettre, vérifier et consommer des justificatifs décentralisés de façon sécurisée et à grande échelle.

Identité en Tant que code ,
et Accès basé sur des Politiques

Inspiré par l'infrastructure en tant que code, l'identité en tant que code traite les configurations d'identité (rôles, politiques, autorisations) comme du code contrôlé par version, intégré dans des pipelines CI/CD. Des outils tels que Microsoft Entra Permissions Management et les cadres de gouvernance basés sur Terraform introduisent ce concept dans les environnements d'entreprise traditionnels.

Pourquoi c'est important :
Définir les politiques d'identité comme du code permet des déploiements plus rapides et cohérents, et une meilleure audibilité. Cela favorise la collaboration des équipes sécurité et plateforme via des workflows DevSecOps, réduisant les erreurs humaines. Dans des environnements multi-Cloud/hybrides, l'identity-as-code garantit que les contrôles d'accès évoluent au même rythme que l'infrastructure.

Explosion des Identités Machines

Les identités non humaines – APIs, containers, IoT, microservices – dépassent désormais les utilisateurs dans la plupart des entreprises. Chacune exige des identifiants (tokens, secrets, certificats) et des contrôles d'accès. or beaucoup les traitent encore comme une arrière-pensée (secrets en dur, rotation insuffisante, absence de gestion de cycle de vie).

Pourquoi c'est important :
Dans les programmes d'identité prêts pour l'avenir, les identités humaines et machines sont régies avec la même rigueur. Les identités machines sont des cibles majeures pour obtenir un accès persistant et discret. Pour les gérer efficacement, il faut mettre en place des contrôles dédiés, notamment la rotation automatisée des secrets, la visibilité sur les comptes de service inutilisés ou surprivilégiés et l'intégration avec des outils de gestion des secrets (par exemple Azure Key Vault, HashiCorp Vault).

Protection Augmentée par l'IA

L'IA et le machine learning deviennent essentiels pour défendre les identités. Microsoft Entra ID Protection et Defender for Identity utilisent déjà l'IA pour détecter des anomalies de connexion (voyage impossible, re-jeu de jetons, attaques de fatigue MFA). Ces capacités évoluent vers des décisions plus contextuelles et autonomes.

Pourquoi c'est important :
Des règles statiques ne suffisent plus face au rythme et à la créativité des attaquants. La protection pilotée par l'IA permet un scoring de risque en temps réel, des politiques adaptatives et une remédiation automatisée – ce qui réduit les temps de réponse et limite l'impact. À mesure que les modèles progressent, attendez-vous à ce que les plateformes d'identité gèrent davantage la boucle détecter-décider-agir, en n'escaladant que les cas sérieux ou ambigus.

Insight et Microsoft : Vos Partenaires Pour L'excellence en Matière de Sécurité des Identités

Mettre en œuvre tout le spectre de la sécurité des identités peut être complexe. Le bon partenaire fait la différence. Insight se positionne comme un leader des services de sécurité des identités, soutenu par un partenariat exceptionnel avec Microsoft. L'équipe Insight possède une expérience approfondie et concrète des technologies identité/sécurité Microsoft – d'Azure Active Directory (désormais Microsoft Entra ID) aux outils les plus récents de gouvernance et de protection contre les menaces.

Insight fait partie des partenaires Microsoft de tout premier plan en sécurité : nous détenons les quatre spécialisations avancées de sécurité Microsoft, dont Identity & Access Management, ainsi que Cloud Security, Information Protection et Threat Protection. Insight appartient à la Microsoft Intelligent Security Association (MISA), en collaboration étroite avec les équipes produit sécurité de Microsoft.

Pour les clients, cela signifie qu'Insight apporte une expertise avérée pour concevoir et déployer une stratégie adaptée, en s'appuyant sur le meilleur des technologies Microsoft. Que vous renforciez des identités on-premises ou adoptiez l'ensemble Entra pour l'identité Cloud, Insight compte plus de 1 500 architectes et ingénieurs certifiés pour vous assister. Nous avons aidé des entreprises dans le monde à déployer la MFA, activer le SSO pour des milliers d'apps, automatiser le cycle de vie avec Entra ID Governance, et intégrer les signaux d'identité dans les plateformes de détection. Nous alignons ces solutions sur vos objectifs métier pour concilier sécurité et expérience utilisateur.

Le partenariat étroit d'Insight avec Microsoft nous place à l'avant-poste des avancées. Par exemple, avec l'arrivée des capacités ITDR et d'insights pilotés par l'IA, Insight les a intégrées tôt dans ses services managés (Insight figure parmi les premiers avec le statut Managed XDR vérifié). Nous suivons la Microsoft Security Reference Architecture pour assurer l'intégration harmonieuse des pièces d'identité dans votre environnement. Résultat : une solution cohésive plutôt que des outils en silo.

Surtout, Insight considère la sécurité des identités comme un **levier stratégique**. Au-delà des technologies, nous co-construisons politiques, modèles de gouvernance et stratégies d'adoption pour rendre les solutions efficaces. Selon l'équipe sécurité UK d'Insight, « l'identité numérique est la clé d'accès au cœur de toute organisation et doit être protégée avec la même priorité que la donnée ou l'infrastructure… Microsoft offre une architecture complète, mais l'impact réel se produit quand on combine culture, processus et engagement organisationnel ». Nous aidons à rassembler ce tableau d'ensemble.

Nous proposons des services allant des évaluations et ateliers initiaux aux déploiements opérationnels, jusqu'aux opérations managées de sécurité des identités. Quel que soit votre niveau de maturité, Insight possède l'expertise pour vous faire progresser. En choisissant Insight, vous gagnez une équipe techniquement pointue et véritablement investie dans votre succès : nous mesurons notre réussite à votre capacité à prévenir les brèches, atteindre la conformité et adopter sereinement les nouvelles technologies – sous l'égide d'un cadre de sécurité des identités robuste.

Microsoft

Conclusion

La sécurité des identités dépasse la checklist : c'est un impératif stratégique. En comprenant et en intégrant les piliers (IAM, IGA, ITDR), les organisations protègent leurs actifs critiques et donnent aux équipes les moyens de travailler efficacement et en sécurité. Le chemin peut sembler complexe, mais vous n'êtes pas seul : avec un partenaire de confiance comme Insight – armé des solutions Microsoft et d'une expertise inégalée – vous pouvez bâtir un programme qui protège aujourd'hui et se prépare au futur.

Glossaire

Terme	Définition
Contrôle D'accès	Politiques et technologies déterminant qui peut accéder à des systèmes, données ou services, et dans quelles conditions.
Athentification	Vérification de l'identité d'un utilisateur, appareil ou système, via mot de passe, biométrie ou clés de sécurité.
Autorisation	Détermination de ce qu'une identité authentifiée est autorisée à faire ou à consulter.
Accès Conditionnel	Politiques dynamiques qui évaluent des signaux de risque (état de l'appareil, localisation) avant d'autoriser l'accès.
Identité Décentralisée (DID)	Modèle où les individus contrôlent leurs données et justificatifs, vérifiés via des technologies distribuées.
Services D'annuaire	Systèmes centralisés de gestion d'identité (Microsoft Entra ID, Active Directory).
Identity and Access Management (IAM)	systèmes/politiques pour gérer les identités numériques et contrôler l'accès aux ressources.
Identity-as-code	Rôles/politiques traités comme du code pour l'automatisation, l'auditabilité et l'intégration dans les pipelines DevOps.
Identity Governance and Administration (IGA)	Outils/processus pour gérer le cycle de vie des accès : revues, approbations, application de politiques.
Cycle de vie D'identité	Onboarding, mobilité, offboarding des identités au fil du temps.
Identity Threat Detection and Response (ITDR)	Capacités qui surveillent et répondent aux menaces identitaires (abus, escalade, anomalies).
Just-in-Time (JIT) Access	Granting privileged access temporarily and only when needed, to minimise standing risk.

Terme	Définition
Least Privilege	A principle ensuring users and systems have only the access necessary to do their job – nothing more.
Machine Identity	Non-human accounts used by software, APIs, services, or devices, which require identity controls and governance.
Multifactor Authentication (MFA)	An authentication approach requiring two or more forms of verification, improving resistance to account compromise.
Passwordless Authentication	Login methods that eliminate the need for passwords, using biometrics, device trust, or cryptographic keys.
Privileged Access Management (PAM)	Controls and tools that secure administrator and other sensitive accounts through vaulting, monitoring, and JIT access.
Role-Based Access Control (RBAC)	A method of assigning access rights based on a user's job function or role.
Self-Sovereign Identity (SSI)	A model where users own and manage their digital identities independently of central authorities.
Service Account	A digital identity used by systems or software to perform automated tasks, often requiring elevated privileges.
Single Sign-On (SSO)	A system that allows users to log in once and gain access to multiple systems or applications.
Token-Based Authentication	Authentication that relies on secure tokens (e.g. JWTs) rather than re-entering usernames and passwords.
Zero Trust	A modern security philosophy where access is never assumed and always verified, based on context and continuous assessment.

Next Steps

Contact Insight to build your comprehensive identity security programme. With identity now the primary attack vector for enterprises, securing every user, service account, and connection is mission-critical. Our holistic approach protects your digital identities, reduces risk, and enables Zero Trust principles. We help you ensure only the right people get the right access, whilst streamlining productivity. Trust Insight's deep expertise and Microsoft partnership to turn your identity security from a complex challenge into a business enabler.

- **fr.insight.com**
- **0344 846 3333**