WALLIX Guide

Comment protéger les entreprises contre les attaques basées sur l'identité



WALLIX Guide :

Comment protéger les entreprises contre les attaques basées sur l'identité

1. Introduction

La sécurité des identités consiste à protéger les identités numériques, c'est-à-dire les comptes, les identifiants et les droits d'accès par lesquels les personnes, les machines et les services accèdent aux systèmes d'une organisation. C'est un enjeu majeur car l'identité est devenue la principale surface d'attaque. La plupart des violations de sécurité ne commencent plus par une intrusion dans le périmètre : elles débutent par un identifiant volé, une session hameçonnée (phishing) ou un compte disposant de privilèges excessifs discrètement exploité.

Le vol d'identifiants et le phishing demeurent les points d'entrée les plus courants, contournant de plus en plus souvent l'authentification multifacteur (MFA) de base grâce à des techniques d'attaque de type « adversaire au milieu » (ou *adversary-in-the-middle).* Une fois à l'intérieur, les attaquants exploitent des droits d'accès excessifs ou dormants pour se déplacer latéralement et élever leurs privilèges. Ce problème est aggravé par le développement d'un phénomène de plus en plus courant aujourd'hui : les identités non humaines, les comptes de service, les clés API et les connexions machine-à-machine sont aujourd'hui plus nombreux que les identités humaines dans la plupart des organisations, souvent non gérés et rarement contrôlés. Chaque identité non vérifiée et chaque droit d'accès superflu constituent un risque latent.



Fig. 1 : le déroulement d'une attaque basée sur l'identité

Si l'identité est le point de départ des attaques, alors le contrôle des accès doit être le point de départ de la défense. Ce rôle est exercé par la gestion des accès aux identités (*identity access management*) : la couche opérationnelle de la sécurité des identités qui vérifie qui se connecte, impose la manière dont les utilisateurs s'authentifient, et régit ce qu'ils sont autorisés à faire et ce, de façon continue, et non pas uniquement lors de la connexion. Avant qu'une organisation puisse envisager des contrôles avancés ou une maturité en matière de gouvernance, elle doit d'abord disposer de ce socle fondamental : une authentification forte, un accès basé sur le principe du moindre privilège, et un cycle de vie des identités géré de bout en bout, de l'arrivée au départ.

2. Les problèmes auxquels les organisations font face

2.1. Dispersion et fragmentation des identités

Peu de paysages identitaires sont le fruit d'une conception délibérée. Ceux-ci ont tendance à se développer au fil du temps, façonnés par les besoins de l'organisation à chaque étape : une nouvelle application par-ci, une plateforme cloud par-là, une acquisition qui arrive avec son propre annuaire et ses propres conventions d'octroi d'accès. Des années de cette évolution laissent derrière elles ce que l'on appelle généralement une « dispersion des identités » (*identity sprawl*) : un même employé détenant une dizaine de comptes déconnectés les uns des autres, des droits d'accès disséminés à travers différents systèmes sans aucune cohérence entre eux, et aucun moyen fiable de répondre à une question aussi élémentaire que « qui a accès à quoi ? ».

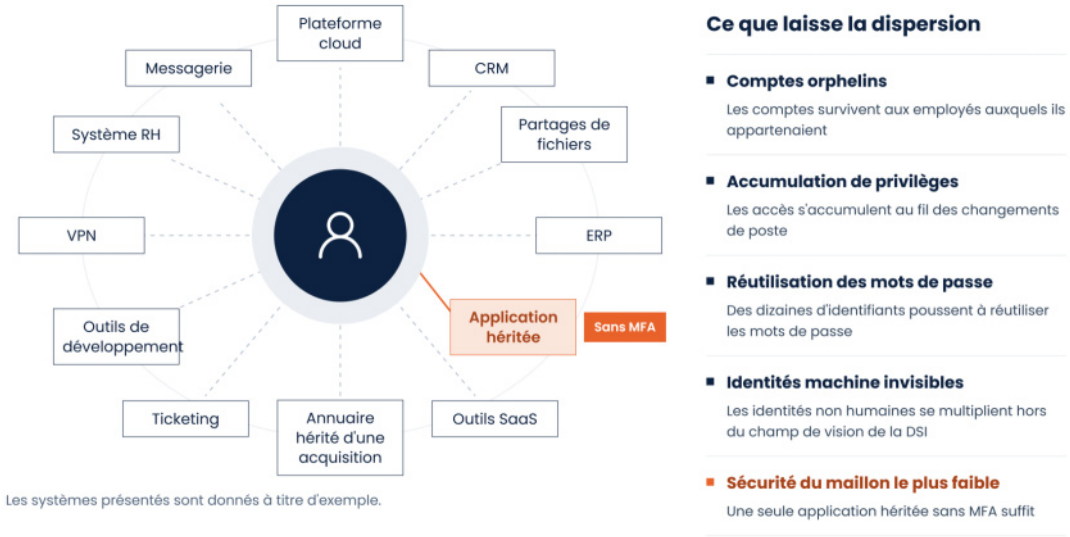


Fig. 2 : La dispersion des identités (un employé, une douzaine de comptes déconnectés)

Les risques associés à cette dispersion sont bien documentés, et la plupart d'entre eux découlent d'un même problème sous-jacent : rien n'est géré à partir d'un point central. La désactivation des accès doit se faire système par système, si bien qu'il n'est pas rare que des comptes continuent à exister même après le départ de l'employé auxquels ils appartenaient. Les droits d'accès s'accumulent au fil des changements de poste, car les permissions sont accordées en fonction des besoins et rarement réexaminées par la suite. Confrontés à des dizaines d'identifiants distincts, les utilisateurs se rabattent sur des mots de passe réutilisés, personne ne pouvant raisonnablement gérer autant d'identifiants forts et uniques. Parallèlement, la population des identités non humaines (comptes de service, clés API, identifiants d'intégration, agents d'intelligence artificielle et autres identités machines) augmente plus rapidement que toute autre catégorie, souvent créée en dehors du champ de vision de l'IT et fonctionnant pendant des années avec des identifiants statiques.

La fragmentation complique encore davantage la résolution de ces problèmes. Lorsque l'authentification est appliquée séparément dans chaque système, le niveau de sécurité global s'aligne sur celui de l'implémentation la plus faible. Concrètement, une seule application héritée dépourvue de MFA peut suffire à compromettre l'ensemble. Lorsque les politiques d'accès résident dans des consoles différentes, en assurer la cohérence devient un exercice manuel, et se préparer à un audit signifie reconstituer l'image globale système par système. Les équipes de sécurité se retrouvent responsables d'une surface d'attaque qu'elles ne peuvent percevoir que partiellement, alors que ce sont précisément les zones de jonction entre systèmes que les attaquants ont tendance à cibler.

Il convient également de noter que cette dispersion ne prend que rarement la même forme d'une organisation à l'autre. La plupart des environnements sont hybrides par nécessité, combinant applications cloud et infrastructures sur site et, dans les secteurs réglementés ou soucieux de souveraineté, des systèmes qui ne peuvent en aucun cas quitter le périmètre propre de l'organisation. Une réponse sérieuse à la fragmentation des identités doit donc prendre en compte l'ensemble de ce paysage, et pas uniquement les composantes les plus simples à connecter.

2.2. L'industrialisation des attaques par identifiants

Le phishing n'est plus une activité artisanale ou hautement spécialisée. Les plateformes de phishing-as-a-service fournissent aux attaquants une infrastructure clé en main pour imiter les pages de connexion des entreprises, collecter des identifiants et contourner certaines formes courantes d'authentification multifacteur. Des services tels que Tycoon 2FA ont permis de déployer ces capacités à grande échelle, abaissant la barrière technique pour les attaquants et transformant des techniques de phishing avancées en services disponibles dans le commerce.

Une évolution particulièrement significative est le phishing de type « adversaire au milieu » (*adversary-in-the-middle*, ou AiTM). Dans une attaque AiTM, l'attaquant place un proxy entre l'utilisateur et le service d'authentification légitime. La victime effectue le processus de connexion authentique, y compris la saisie d'un code à usage unique ou l'approbation d'une notification push, tandis que l'attaquant intercepte le jeton de session ou le cookie résultant. Cela peut permettre à l'attaquant d'accéder au compte sans avoir à répéter le processus d'authentification, même lorsqu'une MFA classique est activée. Microsoft a signalé une augmentation de 146 % des attaques de phishing AiTM observées au cours de l'année 2024.



Fig. 3 : Anatomie d'une attaque de type "Adversary-in-the-Middle" (Le MFA est bien mis en place, mais contourné)

D'autres formes de MFA présentent également des limites. Les notifications push peuvent être exploitées par le biais de demandes d'approbation répétées, tandis que les mots de passe à usage unique peuvent être interceptés ou relayés en temps réel. La question pertinente n'est donc pas simplement de savoir si une MFA est en place, mais si la méthode d'authentification est résistante au phishing. Les méthodes reposant sur des secrets partagés, des codes ou une approbation de l'utilisateur offrent une protection sensiblement différente de celle des méthodes cryptographiques telles que les clés de sécurité FIDO2 et les passkeys.

Le détournement d'identifiants n'en demeure pas moins une voie d'accès importante aux environnements d'entreprise. Le rapport 2026 sur les enquêtes relatives aux violations de données (*Data Breach Investigations Report*) de Verizon a révélé que les identifiants volés

représentaient 13 % de l'activité d'accès initial observée. Une fois que les attaquants ont obtenu un accès via une identité légitime, leurs actions peuvent initialement ressembler à celles d'un utilisateur autorisé, ce qui rend plus difficile la distinction entre activité suspecte et comportement normal.

2.3. Pression réglementaire

Les régulateurs de tous les grands marchés convergent vers la même exigence : les organisations doivent être en mesure de démontrer qu'elles maîtrisent qui a accès à leurs systèmes, et d'en apporter la preuve. En Europe, NIS2 étend les obligations de cybersécurité à un plus grand nombre de secteurs. Elle inclut le contrôle des accès et l'authentification multifacteur parmi les mesures que les entités concernées pourraient devoir mettre en œuvre. Dans le même temps, DORA impose aux entités financières de renforcer la gouvernance des risques liés aux technologies de l'information et de la communication (notamment le contrôle des accès, les comptes à privilèges et l'accès des tiers). Le RGPD continue quant à lui d'exiger une protection appropriée des données personnelles, faisant de la gouvernance documentée des accès, des revues régulières des permissions et de la suppression rapide des comptes des éléments de conformité importants.

Ce schéma se répète bien au-delà de l'Europe. Aux États-Unis, SOX et HIPAA exigent des contrôles d'accès démontrables dans leurs secteurs respectifs, et les directives fédérales de zero trust poussent les agences et leurs fournisseurs vers une MFA résistante au phishing. Le Royaume-Uni associe son RGPD retenu (« UK GDPR ») aux règles de résilience opérationnelle de la FCA et au label Cyber Essentials, ce qui fait du contrôle des accès et de la MFA une condition d'accès à une grande partie des marchés publics. Au Moyen-Orient, les lois sur la protection des données telles que la PDPL saoudienne évoluent rapidement, des régulateurs comme la SAMA imposant des exigences explicites en matière d'identité pour le secteur financier. La région Asie-Pacifique suit la même trajectoire, de l'APPI japonaise et du PDPA singapourien aux lignes directrices de la MAS sur les accès à privilèges. Et au-dessus de la couche nationale, PCI DSS et ISO 27001 accompagnent l'activité des entreprises elles-mêmes, faisant de la gestion des accès une attente aussi bien contractuelle que réglementaire.

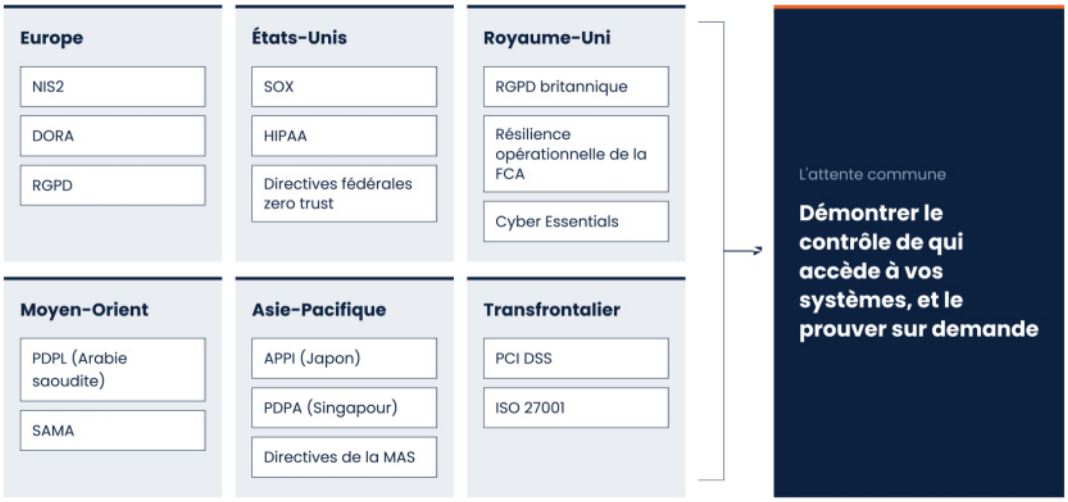


Fig.4 : Différents cadres réglementaires, une même attente

Pris individuellement, chaque cadre réglementaire possède son propre périmètre et son propre calendrier. Pris ensemble, ils convergent tous vers une même direction : les contrôles d'identité et d'accès ne relèvent plus d'une préférence interne en matière de sécurité, mais constituent une obligation externe : une obligation que les organisations doivent être en mesure de justifier sur demande.

2.4. Le piège de l'expérience-utilisateur

Enfin, les contrôles de sécurité qui génèrent une friction excessive sont souvent contournés. Des demandes d'authentification trop fréquentes incitent les utilisateurs à chercher des raccourcis. Des exigences de mots de passe trop complexes conduisent à la réutilisation, à des variations prévisibles et à un stockage peu sécurisé. Des processus de demande d'accès trop lents augmentent la probabilité de recours à des identifiants partagés ou à des solutions de contournement non maîtrisées.

Il ne s'agit pas simplement d'une question de discipline des utilisateurs, mais d'un problème de conception. La sécurité des accès pour les collaborateurs est la plus efficace lorsque le chemin sécurisé est aussi le plus simple. Les utilisateurs devraient pouvoir s'authentifier une seule fois, accéder aux applications nécessaires à leur fonction, utiliser des facteurs d'authentification plus rapides et plus sûrs que les mots de passe, et répondre à leurs besoins d'accès courants sans délai inutile. Une solution qui relègue l'ergonomie au second plan finira par engendrer les comportements mêmes qu'elle cherchait à prévenir.

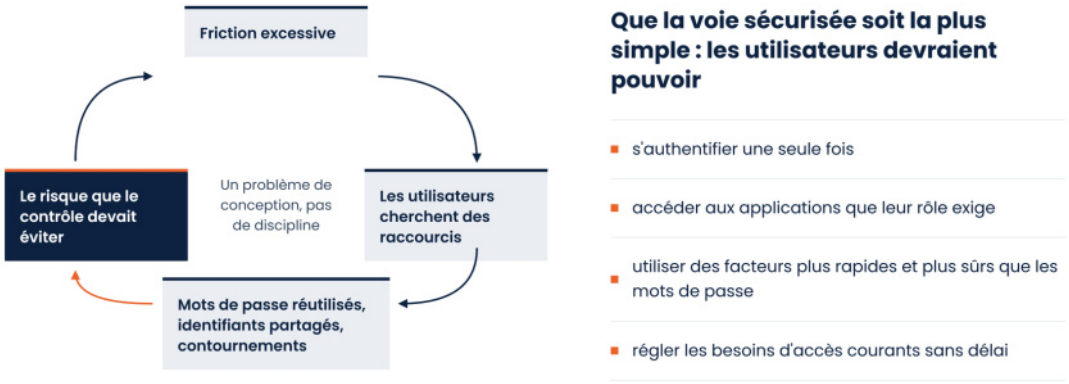


Fig. 5 : La friction engendre le comportement même qu'elle était censée prévenir : il faut donc la concevoir pour l'éliminer.

3. Là où la pression est la plus élevée

Ces défis concernent la majorité des organisations, mais ils sont incontournables dans les secteurs qui combinent environnements complexes, systèmes sensibles et exigences réglementaires strictes.

Services publics et administrations

Les administrations publiques exploitent des parcs applicatifs vastes et hétérogènes, allant des services cloud modernes aux systèmes utilisés depuis des décennies. Ces systèmes sont accessibles par des ministères, des agences et des collectivités locales, souvent sous des exigences strictes en matière d'auditabilité, de souveraineté et de maîtrise du lieu de stockage des données d'identité.

Pour ces organisations, la priorité consiste à assurer une authentification cohérente sur l'ensemble du parc applicatif, à introduire des facteurs d'authentification forts conformément aux exigences applicables au secteur public, et à conserver une traçabilité complète de l'activité d'accès sous le contrôle de l'organisation.

Infrastructures critiques et industrie

Les opérateurs de l'énergie, des transports, de l'eau, de l'industrie manufacturière et d'autres secteurs industriels doivent sécuriser des environnements où la disponibilité est essentielle. Ils peuvent exploiter des réseaux de technologie opérationnelle (OT) segmentés, des sites distants à connectivité limitée, ainsi que des systèmes hérités difficiles à remplacer ou à modifier.

L'authentification dans ces environnements doit rester fiable sans dépendre entièrement de services externes. Elle doit également s'intégrer aux systèmes industriels et hérités existants,

tout en générant les journaux nécessaires à l'audit et à la surveillance réglementaire. L'objectif est d'assurer une authentification cohérente des collaborateurs à travers les bureaux, les usines et les sites distants, sans introduire de dépendance opérationnelle inacceptable.

Services financiers

Les institutions financières opèrent sous des exigences étendues en matière de gestion des risques liés aux TIC, de résilience et de supervision des tiers. Employés, prestataires, fournisseurs de services et partenaires technologiques peuvent tous nécessiter un accès contrôlé aux systèmes sensibles.

Une approche efficace doit prendre en compte chaque identité, appliquer une authentification adaptée, restreindre et surveiller les accès à privilèges et les accès tiers, et rendre les preuves disponibles en cas de besoin. L'enjeu ne se limite pas à empêcher les accès non autorisés, mais consiste aussi à démontrer que ces accès sont gouvernés de manière continue.

Santé

Les environnements de santé combinent des données personnelles hautement sensibles avec des flux de travail où les délais peuvent affecter la prise en charge des patients. Les soignants peuvent se déplacer entre plusieurs sites, utiliser des postes de travail partagés et avoir besoin d'un accès rapide à de multiples systèmes cliniques.

L'authentification doit donc être suffisamment rapide pour soutenir le travail clinique, tout en garantissant que l'accès aux informations des patients reste contrôlé, attribuable et auditable. L'objectif n'est pas de choisir entre ergonomie et sécurité, mais de concevoir des contrôles d'accès qui garantissent les deux à la fois.

proxy à une session d'authentification légitime et intercepter le jeton de session qui en résulte, même lorsque certaines formes de MFA sont activées. La simple présence d'une MFA ne garantit donc pas une résistance au phishing.

L'authentification résistante au phishing permet de pallier cette faiblesse. Les méthodes FIDO2 et WebAuthn, notamment les clés de sécurité physiques et les passkeys, lient l'authentification au service légitime grâce à la cryptographie à clé publique. Il n'existe aucun code réutilisable ni secret partagé que l'utilisateur pourrait divulguer à un site frauduleux. L'authentification par certificat, y compris les cartes à puce (smartcards), offre une protection similaire et demeure largement utilisée dans les secteurs gouvernemental, de la défense et dans d'autres environnements à haut niveau d'exigence.



Fig. 7 : Toutes les MFA ne se valent pas : positionnement des méthodes courantes face au phishing

Les recommandations réglementaires et techniques reconnaissent de plus en plus cette distinction. L'ANSSI recommande des méthodes d'authentification cryptographiques lorsqu'un niveau d'assurance renforcé est requis, et met en garde contre le recours à des canaux plus faibles pour la transmission de codes à usage unique. La CISA décrit la MFA résistante au phishing, incluant l'authentification FIDO/WebAuthn et basée sur PKI, comme la norme à privilégier. Les orientations européennes accompagnant la mise en œuvre de NIS2 encouragent également les organisations à adopter des méthodes résistantes au phishing pour les accès sensibles.

Le déploiement doit être fondé sur une approche par les risques. Les administrateurs, les utilisateurs à privilèges et ceux accédant à des systèmes critiques devraient être prioritaires, une adoption plus large étant introduite au fur et à mesure que les équipements et les flux

de travail le permettent. La solution doit accompagner cette progression au moyen d'un cadre de politiques commun, plutôt que d'imposer une migration immédiate à l'échelle de l'ensemble de l'organisation.

4.3. Fédération sur l'infrastructure existante (sans nécessité de tout remplacer)

Les organisations ont investi des années dans leur infrastructure d'annuaire. Active Directory et LDAP détiennent le référentiel faisant autorité sur qui travaille où et dans quelle fonction, un référentiel intégré aux processus des RH, de l'IT et de la sécurité. Une solution d'accès des collaborateurs qui exigerait de migrer hors de ce socle échoue avant même d'être évaluée.

L'exigence est donc la fédération : la solution s'appuie sur les annuaires existants en tant que sources d'identité faisant autorité, se synchronise avec eux, et étend leur portée aux applications par le biais de protocoles standards (SAML et OpenID Connect pour les applications web modernes, RADIUS pour les équipements et infrastructures réseau, ainsi que SCIM pour le provisionnement automatisé des utilisateurs vers les services compatibles). Les identités, groupes et logiques organisationnelles existants sont conservés intégralement. Le parc applicatif, y compris les systèmes qui n'ont jamais été conçus pour la fédération, devient accessible par le biais d'une couche d'authentification unique.



Fig. 8 : La fédération étend les annuaires que vous possédez déjà, par le biais de protocoles standards

C'est également ce qui rend le déploiement réaliste au regard des échéances de conformité. Les obligations réglementaires assorties de délais fixes ne laissent pas de place à des migrations d'annuaires s'étalant sur plusieurs années ; une solution qui se superpose à l'infrastructure existante permet d'imposer une authentification forte sur l'ensemble du parc en quelques mois.

4.4. Le cycle de vie des identités sans la charge manuelle

Chaque identité a un cycle de vie (arrivée, changements de rôle, départ) et chaque étape constitue un point où les accès peuvent discrètement s'écarter de ce qu'ils devraient être. La solution doit rendre ce cycle de vie administrable depuis un point unique : des comptes créés dès le premier jour avec des accès adaptés à leur rôle, des permissions ajustées au fil des changements de fonction, et un départ qui révoque l'ensemble des accès simultanément. Une politique fondée sur les groupes et les rôles, appliquée de façon centralisée, remplace l'administration application par application.

Cela permet d'éliminer les deux modes de défaillance chroniques de l'administration manuelle : la dérive des privilèges (*privilege creep*) et les comptes orphelins qui survivent au départ de leurs titulaires. Cela transforme également un coût opérationnel récurrent en un processus gouverné : les accès dont dispose une personne correspondent exactement à ceux que définit son rôle, de façon démontrable et à tout moment.

4.5. Des preuves d'audit intégrées

Chaque réglementation évoquée dans ce document converge vers les mêmes questions : qui a accès à quoi, comment cet accès est-il protégé, et pouvez-vous le prouver ? Une solution d'accès des collaborateurs doit pouvoir répondre à partir de ses propres registres : des journaux d'authentification complets, une cartographie en temps réel des droits d'accès des utilisateurs aux applications, ainsi que des rapports adaptés aux auditeurs et non pas seulement aux administrateurs. L'intégration avec les plateformes SIEM permet de faire remonter les événements liés à l'identité vers les capacités plus larges de détection et de réponse de l'organisation.

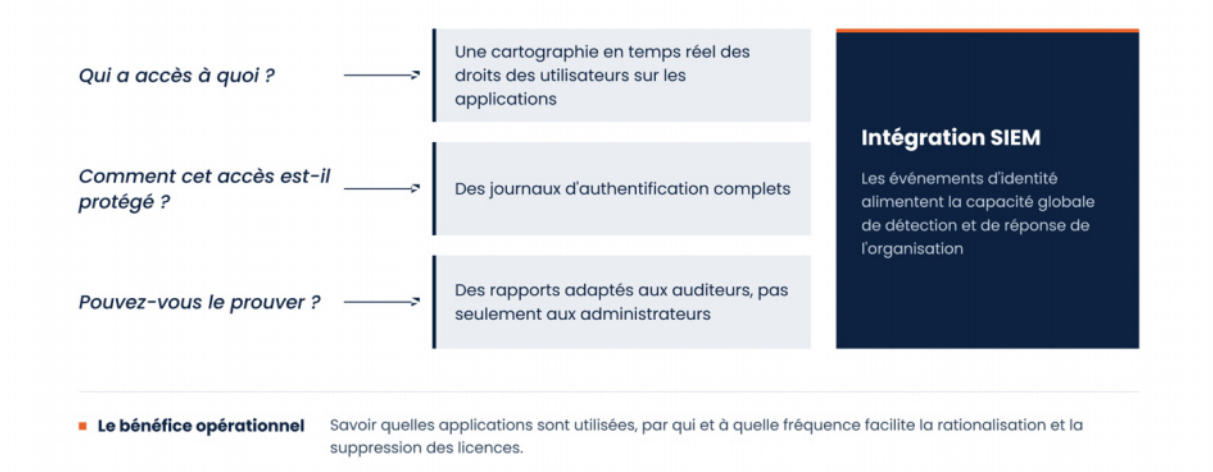


Fig. 9 : Les trois questions de l'auditeur, auxquelles la solution répond à partir de ses propres registres

Au-delà de la conformité, cette visibilité procure un bénéfice opérationnel : savoir quelles applications sont réellement utilisées, par qui et à quelle fréquence, fournit aux équipes IT les éléments nécessaires pour rationaliser les licences et retirer les outils que l'organisation a dépassés.

5. Une plateforme, votre modèle de déploiement

Les capacités présentées ci-dessus définissent ce qu'une solution d'accès des collaborateurs doit accomplir. La question de savoir où elle s'exécute relève d'une décision distincte : une décision qui dépend du contexte réglementaire, de l'infrastructure et de la posture de risque de l'organisation, et non des capacités elles-mêmes.

En mode service (SaaS) : C'est la voie la plus rapide vers ces capacités : aucune infrastructure à provisionner, exploitation et mises à jour prises en charge par l'éditeur, montée en charge gérée de manière transparente. Conçue pour les organisations souhaitant déployer la sécurité des accès des collaborateurs en quelques semaines et préférant consommer ce service plutôt que l'exploiter elles-mêmes.

Sous forme de solution clé en main sur site : Ce sont les mêmes capacités, déployées au sein de l'infrastructure propre de l'organisation. Les données d'identité, les flux d'authentification et les journaux demeurent entièrement sous le contrôle de l'organisation (au sein de son périmètre, de sa juridiction et de sa responsabilité opérationnelle). Conçue pour les organisations soumises à des exigences de souveraineté, à des appels d'offres réglementés excluant une identité délivrée par le cloud, ainsi que pour les environnements industriels, isolés (*air-gapped*) ou à connectivité limitée, où l'authentification doit fonctionner sans dépendance externe.

Deux questions déterminent le modèle à retenir. Où les données d'identité doivent-elles résider ? Si la réglementation, la politique interne ou la sensibilité des opérations exige que l'identité demeure sous le contrôle direct de l'organisation, la solution clé en main apporte structurellement une réponse là où de simples garanties contractuelles ne répondent que partiellement à cette exigence. À quoi l'authentification doit-elle pouvoir résister ? Si l'environnement doit continuer à fonctionner en cas de perte de connectivité externe (une usine, un navire, un réseau classifié), l'authentification ne peut pas dépendre de l'accessibilité d'un service cloud.

Aucun des deux modèles ne constitue un compromis. Ce sont deux modes de déploiement d'une même plateforme, et le bon choix est celui que l'environnement de l'organisation a déjà, de fait, déterminé.

6. WALLIX Sovereign Identity Access

Notre solution assure la sécurité des identités telle que décrite dans ce document :

- Authentification unique (single sign-on) sur l'ensemble des applications ;
- Authentification multifacteur, y compris des méthodes résistantes au phishing ;
- Synchronisation des utilisateurs et fédération des identités avec les environnements Microsoft Entra ID, Google Workspace, Active Directory et LDAP existants ;
- Authentification déléguée vers les applications cibles ; administration centralisée du cycle de vie ; et visibilité d'audit complète.

Elle est disponible en mode service (SaaS) ou sous forme de solution clé en main sur site, avec un même ensemble de capacités gouvernées de la même manière.

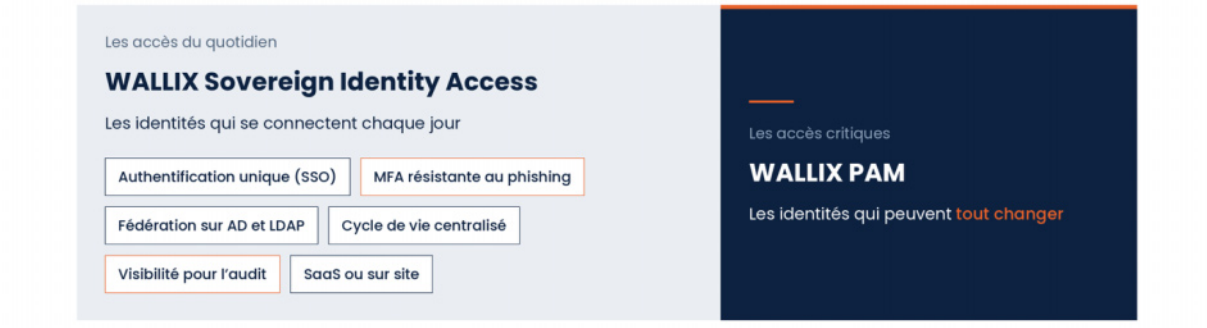


Fig. 10 : Deux facettes d'un même problème, un seul plan de contrôle

WALLIX Sovereign Identity Access fait partie de la plateforme WALLIX, aux côtés de WALLIX PAM. La sécurité des identités et l'accès à privilèges constituent deux facettes d'un même problème : les identités qui se connectent chaque jour (et celles qui peuvent tout changer) et le fait de les sécuriser. Réalisée grâce à un éditeur européen, cela offre aux organisations un plan de contrôle unique et cohérent sur l'ensemble des accès, du quotidien au plus critique d'entre eux.

7. Conclusion

L'accès aux identités est le terrain sur lequel se joue le sort de l'organisation moderne : c'est à la fois ce qui permet le travail au quotidien et ce par quoi commencent les violations. Les organisations qui parviennent à le sécuriser partagent une même approche : une identité centralisée plutôt que dispersée, une authentification que le phishing ne peut vaincre, une infrastructure existante étendue plutôt que remplacée, et une preuve de maîtrise disponible sur demande.

Les capacités existent. Les échéances réglementaires sont fixées. Ce qui reste à faire, c'est de décider de traiter l'accès des collaborateurs comme le périmètre de sécurité qu'il est déjà devenu, et de déployer ce contrôle partout où l'organisation en a besoin.

À propos de WALLIX

WALLIX (Euronext : ALLIX, coté depuis 2015) est un éditeur européen de cybersécurité des identités et des accès, leader dans la gestion des accès privilégiés (PAM), qui aide les organisations à renforcer leur sécurité et leur souveraineté numérique. Ancrée dans les valeurs européennes de sécurité et de liberté, et reconnue pour l'excellence technologique de sa plateforme WALLIX One par les plus grandes sociétés d'analyse, WALLIX soutient plus de 4 000 organisations à travers le monde. WALLIX protège les identités, les accès et les privilèges dans les environnements IT et OT afin de permettre aux organisations d'évoluer en toute confiance dans un monde numérique plus sécurisé.

WWW.WALLIX.COM