

COHESITY

LA COUCHE D'IDENTITÉ

EST AU COEUR MÊME DES CYBERATTQUES



*Pourquoi les responsables de la sécurité et des technologies de l'information doivent **démontrer** leur capacité à restaurer l'infrastructure d'identité*

INTRODUCTION

L'identité d'entreprise était censée vous simplifier la vie. Les entreprises ont commencé à centraliser l'accès numérique à la fin des années 60 et au début des années 70, pour disposer d'un point unique permettant de décider qui pouvait entrer dans les systèmes et à quoi ils pouvaient accéder. Le protocole LDAP et des plateformes telles qu'Active Directory ont ensuite transformé ce concept en une source unique de vérité pour l'ensemble du réseau. Cela a fonctionné à merveille.

Et c'est justement là que réside le problème.

Cette source unique de vérité est désormais le point d'accès le plus facile. Les attaquants ne forcent plus l'entrée. Ils se connectent à l'aide d'identifiants volés et d'un accès légitime, et accèdent directement à vos systèmes les plus critiques. Rien ne déclenche d'alerte. Aucune alarme ne retentit. Ils empruntent la même porte que vos employés chaque matin, ce qui constitue un problème fondamentalement différent de celui pour lequel la plupart des programmes de sécurité ont été conçus.

Pendant des années, vous avez construit vos défenses autour d'un périmètre : un mur destiné à tenir les intrus à l'écart.

Ce mur est toujours là, mais les attaquants ont cessé de l'escalader. **Il est plus facile, plus discret et plus fiable de compromettre votre infrastructure d'identité. C'est pourquoi le champ de bataille principal est désormais l'identité et non plus le périmètre du réseau.** La plupart des solutions de sécurité n'ont jamais été conçues pour lutter sur ce terrain.

Les chiffres ne laissent aucune place au doute. En 2024, 79 % des attaques étaient exemptes de logiciels malveillants : pas de virus à attraper, seulement de l'ingénierie sociale, des identifiants volés et des outils de gestion à distance de confiance qui échappaient à la détection. En 2025, ce chiffre a grimpé à 82 %, les attaquants s'appuyant encore davantage sur des identifiants valides, des flux d'identité fiables et des intégrations SaaS approuvées pour se déplacer d'un domaine à l'autre sans être détectés (CrowdStrike Global Threat Report). La tendance est claire.

Tout programme de sécurité sérieux doit désormais commencer par là, même si cela peut sembler inconfortable. Le système que vous avez conçu pour contrôler l'accès à tout est subrepticement devenu le moyen le plus simple d'accéder à tout. Ce n'est pas une raison de paniquer, mais c'est une raison pour protéger l'identité avant tout, et pour être capable de prouver que vous pouvez la restaurer, avant toute autre chose.

Pourquoi l'identité d'entreprise est attaquée

Pour un attaquant, l'identité constitue la cible la plus précieuse et la plus facile à attaquer au sein de votre entreprise, car un seul identifiant compromis peut lui donner accès à tout ce qui se cache derrière. L'identité n'est pas un simple vecteur parmi d'autres. De nos jours, c'est le seul vecteur que les attaquants recherchent activement.

Mais voici le problème : pratiquement aucun élément de votre infrastructure n'a été conçu pour empêcher cela. Les solutions EDR, les pare-feu et la segmentation du réseau sont tous conçus pour détecter les intrusions, et non pour remettre en question l'identité d'une personne qui s'est connectée avec des identifiants valides. Pour vos défenses, l'attaquant ressemble comme deux gouttes d'eau à votre employé.

Et cette faille ne cesse d'augmenter. La plupart des environnements Active Directory remontent à plusieurs dizaines d'années. Des années de solutions de fortune, de comptes oubliés et d'erreurs de configuration passées inaperçues se sont accumulées en arrière-plan, là où personne ne regarde. Cette accumulation ne se résume pas à une simple dette technique. C'est une fenêtre laissée ouverte, et c'est précisément ce que les pirates recherchent en premier lieu.

L'identité hybride ne fait qu'aggraver ce problème. La plupart des entreprises exécutent désormais une combinaison d'Active Directory en local et de fournisseurs d'identité cloud comme Entra ID et Okta, et chaque connexion entre ces solutions élargit la surface d'attaque. Pire encore, une faiblesse présente dans Entra ID ou Okta provient souvent directement d'Active Directory, car Active Directory est généralement la source unique d'informations sur laquelle tout le reste s'appuie. Si les fondations sont fissurées, c'est toute la structure qui s'effondre.

ACTIVE DIRECTORY EST AU CŒUR DE L'IDENTITÉ D'ENTREPRISE

Active Directory exécute des fonctions d'identité d'entreprise depuis plus de 25 ans et est toujours en place dans 90 % des entreprises du monde entier. La plupart des fournisseurs d'identité dans le cloud sont fédérés ou synchronisés avec Active Directory, ce qui signifie que même lorsque vous adoptez de nouvelles plateformes, Active Directory reste le pilier sur lequel reposent toutes ces dernières.

En réalité :

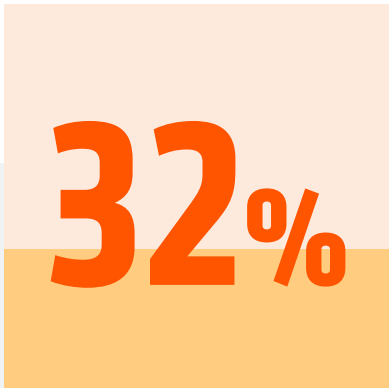
- Les adversaires compromettent un contrôleur de domaine dans plus de 78 % des intrusions menées par des humains.
- Dans 35 % de ces cas, le contrôleur de domaine devient le point à partir duquel le ransomware se propage dans l'ensemble de l'environnement.

En cas d'attaque, Active Directory est souvent la seule ligne de défense entre vous et la restauration. Réfléchissez à ce que cela signifie : si vous ne pouvez plus vous connecter à votre propre solution de sauvegarde, vous ne pouvez pas commencer à restaurer quoi que ce soit. Les attaquants le savent parfaitement, c'est pourquoi ils s'attaquent de plus en plus souvent simultanément à vos systèmes de sauvegarde et à votre Active Directory. S'ils parviennent à mettre les deux hors service, votre journée tourne au cauchemar. Vous êtes alors confrontés à ce qui semble être une prise d'otages.

Et le temps presse, impitoyablement. La restauration complète d'une forêt Active Directory peut prendre plusieurs jours, voire plusieurs semaines, et chaque temps d'arrêt peut coûter aux entreprises jusqu'à 730 000 USD par heure (*Forrester, The Total Economic Impact™ of Quest Recovery Manager for Active Directory Disaster Recovery Edition*).

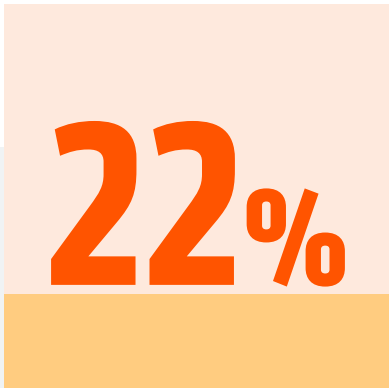
Face à une telle situation, les outils de sauvegarde ne vous seront d'aucune utilité. Ils permettent certes de copier des contrôleurs de domaine et des fichiers individuels, mais ils ne sont pas en mesure d'orchestrer les étapes précises et ordonnées nécessaires à la reconstruction d'une forêt Active Directory dans son intégralité. Sauvegarder des éléments individuels n'est pas la même chose qu'avoir la capacité de les réassembler.

DONNÉES JUSTIFICATIVES

A vertical bar chart with a light orange top half and a darker orange bottom half. The number '32%' is displayed in large orange font across the middle.

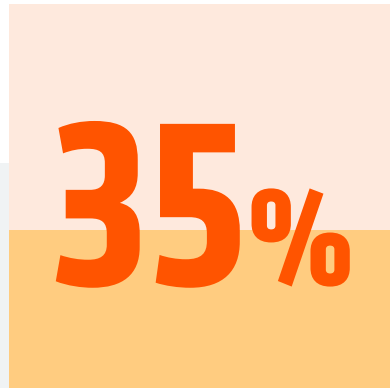
Hausse de 32 % des attaques ciblant l'identité au premier semestre 2025. 97 % d'entre elles étaient des attaques par diffusion de mot de passe ou par force brute

(Microsoft Digital Defense Report 2025)

A vertical bar chart with a light orange top half and a darker orange bottom half. The number '22%' is displayed in large orange font across the middle.

des violations impliquaient globalement un vol d'informations d'identification ; 88 % des attaques sur les applications web de base impliquaient spécifiquement un vol d'informations d'identification

(Verizon 2025 Data Breach Investigations Report)

A vertical bar chart with a light orange top half and a darker orange bottom half. The number '35%' is displayed in large orange font across the middle.

des incidents liés au cloud étaient dus à un abus de comptes valides

(CrowdStrike 2025 Global Threat Report)

L'identité est la base de la EVM et de la confiance, aujourd'hui et à l'avenir

Une Entreprise Viable Minimale (EVM) est la version la plus réduite et la plus allégée d'une entreprise nécessaire pour assurer sa survie et maintenir ses opérations essentielles. Lorsqu'une entreprise est victime d'un cyberincident, ce n'est pas parce que ses sauvegardes sont défectueuses qu'elle ne parvient pas à restaurer. Elle échoue souvent parce qu'elle tente de tout restaurer en même temps ou dans le mauvais ordre.

L'aspect que la plupart des entreprises négligent concerne la confiance et le contrôle, et l'identité se situe précisément à la croisée de ces deux éléments. C'est la clé passe-partout de l'entreprise. Si vous ne pouvez pas établir une identité de confiance, vous ne pourrez rien restaurer d'autre de façon sécurisée.

La gestion des identités et des accès (IAM) est responsable de trois fonctionnalités principales :

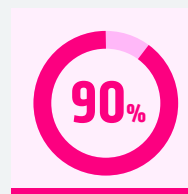
- **Gestion du cycle de vie de l'identité :** automatise l'intégration, la mise à jour des rôles et la suppression des droits d'accès afin que les droits d'accès restent à jour lorsque des collaborateurs rejoignent l'entreprise, changent de rôle ou quittent l'entreprise.
- **Authentification :** vérifie que l'identité d'une personne correspond bien à ce qu'elle prétend être, généralement grâce à l'authentification multifactorielle (MFA) et à l'authentification unique (SSO).
- **Autorisation :** accorde à chaque utilisateur authentifié les droits d'accès spécifiques dont il a besoin pour exercer ses fonctions, tout en limitant l'accès à tout le reste.

En combinant ces trois fonctionnalités, Active Directory, Entra ID et Okta ne sont plus de simples éléments d'infrastructure, mais deviennent la colonne vertébrale opérationnelle de votre entreprise. Elles authentifient chaque employé, chaque application et chaque transaction. Cela nous amène à une vérité simple, mais dérangement : si l'infrastructure d'identité tombe en panne, l'entreprise s'effondre avec elle.

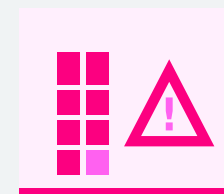
Et cette colonne vertébrale opérationnelle est sur le point d'être beaucoup plus exposée. Alors que les entreprises se précipitent pour adopter l'IA et les flux de travail automatisés, ces agents s'appuient sur une infrastructure d'identité pour fonctionner en toute sécurité, et cette évolution est déjà visible dans les données : 93 % des entreprises utilisent déjà ou prévoient d'utiliser des agents IA pour des tâches sensibles en matière de sécurité, telles que la réinitialisation des mots de passe ou l'accès à un VPN (Semperis, mai 2026).

Voici ce qui devrait retenir votre attention : ces agents usurpent souvent l'identité des employés qui leur demandent d'effectuer des tâches et d'accéder à des données sensibles. Chacun d'entre eux correspond à un nouvel ensemble de clés. Les enjeux de la sécurisation, de la protection et de la restauration de l'identité n'ont jamais été aussi élevés.

DONNÉES JUSTIFICATIVES



Active Directory et Entra ID sont utilisés par plus de 90 % des entreprises dans le monde (Semperis).



Active Directory est impliqué dans 9 cyberattaques sur 10, non pas en raison d'un défaut inhérent, mais à cause de son omniprésence ([Cohesity CERT](#)).

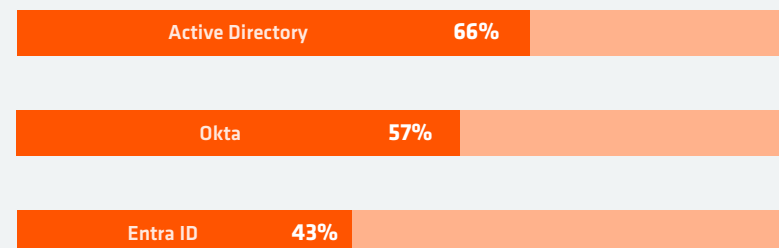
L'intersection de l'identité, de la continuité des opérations et de la cyber-résilience

La planification traditionnelle de la continuité des opérations traite l'identité exactement comme elle traite le réseau électrique : comme une infrastructure qui est censée être opérationnelle dès l'actionnement de l'interrupteur. C'est précisément ce qui entraîne la ruine des entreprises. L'identité ne peut plus être considérée comme acquise. Elle nécessite son propre plan de restauration.

La cyber-résilience bouleverse complètement cette idée reçue. Elle considère que l'identité est le premier élément qui sera attaqué et qu'il s'agit de la première chose que vous devez être en mesure de restaurer (de façon indépendante, testée, isolée et fiable), même lorsque tout ce qui l'entoure est compromis. C'est précisément dans l'écart entre « nous pensons que cela va fonctionner » et « nous avons déjà prouvé que cela fonctionnera » que les entreprises perdent des jours, voire des semaines, après une attaque. Elles ont pourtant la capacité de très bien restaurer leurs fichiers. Mais personne ne peut se connecter pour les utiliser.

Pour les responsables de la sécurité, de l'informatique et de la direction, la conclusion est inévitable : la continuité des activités et la cyber-résilience ne réussissent que lorsque la sécurité proactive de l'identité et la restauration de l'identité sont planifiées, testées et dotées de ressources comme s'il s'agissait de disciplines à part entière. Ne supposez jamais se produiront automatiquement pendant que vous restaurez tout le reste. L'espoir n'est pas un plan de restauration.

DONNÉES JUSTIFICATIVES



Les plans de reprise après sinistre n'incluent Active Directory que pour 66 % des entreprises, Entra ID pour 43 % et Okta pour 57 % d'entre elles, ce qui laisse une grande partie des plans de continuité avec un angle mort au niveau même de la couche d'identité

(Semperis, Nov 2025).



90 % des entreprises analysent les vulnérabilités d'identité, mais seules 51 % d'entre elles mettent en place des procédures de remédiation, et seulement 57 % automatisent la restauration d'identité (Semperis, Nov 2025).

Le coût de l'inaction

Parlons du coût qu'implique d'attendre, car attendre est aussi un choix, et c'est le plus coûteux de tous. Non seulement sur le plan financier, mais aussi sur le plan opérationnel et en termes de réputation.

Ce coût ne se résume pas à une seule facture. Il y en a trois, et leurs effets s'additionnent :

- **La facture liée à la violation** : réponse aux incidents, amendes réglementaires et risques juridiques
- **La facture liée aux temps d'arrêt** : perte de productivité, manque à gagner et attaques répétées tant que la couche d'identité reste exposée
- **La facture liée à la confiance** : hausse des primes d'assurance cyber, responsabilité des dirigeants et risque lié aux opérations

Et le fait d'attendre n'arrête pas le compteur. La surface d'attaque liée à l'identité est l'une des plus ciblées en entreprise, et les défenses traditionnelles ne peuvent pas suivre le rythme. Par conséquent, le coût de l'inaction n'est pas figé. Il augmente chaque trimestre où vous n'agissez pas. Attendre n'est pas synonyme de prudence. C'est comme des intérêts composés sur une dette que vous n'avez jamais choisi de contracter.

DONNÉES JUSTIFICATIVES



Sur une période de trois ans, les entreprises peuvent faire face à une attaque d'identité réussie coûtant **1,2 million USD**, à une surveillance manuelle des identités hybrides coûtant **109 000 USD**, et à une perte de productivité et à des temps d'arrêt liés à la restauration manuelle d'Active Directory coûtant **3,9 millions USD**. (Étude Forrester Total Economic Impact).



Le coût moyen mondial d'une violation de données s'élève à **4,44 millions USD**, mais les violations basées sur les informations d'identification coûtent environ **4,67 millions USD**, et il faut environ 292 jours pour les identifier et les contenir, ce qui représente le plus long délai parmi tous les vecteurs d'attaque (IBM Cost of a Data Breach 2025).



L'économie des ransomwares évolue, mais non sans douleur : le paiement moyen d'une rançon a chuté à **115 000 USD**, et **64 %** des victimes ont refusé de payer, ce qui signifie que davantage d'entreprises absorbent le coût opérationnel de la restauration plutôt que celui de la rançon elle-même, ce qui fait monter la pression en termes de vitesse de récupération de l'identité (Verizon DBIR 2025).



Désormais, **8 cyberassureurs majeurs sur 8** demandent à voir et valident la sécurité et la résilience liées à l'identité lors de la souscription de polices d'assurance cyber, et le fait d'être capable de démontrer un renforcement solide de l'identité est directement corrélé à une baisse des primes et à une couverture supérieure (Cohesity, "Identity resilience is critical for cyber insurance").

Ces données ne sont pas sans rapport les unes avec les autres. Il s'agit du coût détaillé des violations de données et des temps d'arrêt, suivis de près par le coût lié à la perte de confiance, les assureurs liant désormais directement leurs primes à votre niveau de protection de l'identité. Chacun de ces points devient plus coûteux à mesure que l'identité reste non traitée. Vous devrez payer cette facture quoi qu'il arrive. La seule question est de savoir si vous préférez payer une petite partie dès maintenant, selon vos conditions, ou la totalité plus tard, selon celles de l'attaquant.

CONCLUSION

La compromission basée sur l'identité fait désormais partie de la quasi-totalité des violations majeures, et le schéma est toujours le même. Les attaquants ne forcent pas l'entrée. Ils se connectent à l'aide d'informations d'identification valides et de flux d'identité fiables et se déplacent sans être repérés dans des environnements qui n'ont jamais été conçus pour les détecter. Ils volent ensuite vos données, confisquent vos systèmes et déploient leur ransomware.

Rien de tout cela n'est inévitable.

Ce qui distingue les entreprises qui se rétablissent en quelques heures de celles qui mettent des semaines à restaurer la confiance dans leurs services d'identité n'a rien à voir avec la chance, ni avec le montant des investissements réalisés. Tout se résume à une décision unique : ont-elles mis en place une résilience des identités en tant que discipline à part entière, couvrant l'ensemble du cycle de vie d'une attaque, avant même d'en avoir besoin ?

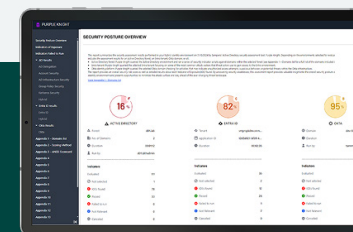
Considérez donc la résilience des identités pour ce qu'elle est devenue : non pas une option, mais une exigence fondamentale de la sécurité d'entreprise. L'identité est à la fois votre porte d'entrée, votre fondement et le frein à votre restauration. Un ensemble disparate d'outils ponctuels ne suffira jamais. Il en va de même pour tout plan de continuité qui part simplement du principe que l'identité sera bien là le moment venu. La seule stratégie qui résiste à une attaque réelle est celle que vous avez testée et validée avant d'en avoir besoin.

La bonne nouvelle, c'est que vous pouvez prendre les devants. Vous pouvez accélérer la cyber-résilience pour vos systèmes d'identité les plus critiques.

Et nous pouvons vous y aider.

En savoir plus sur la façon dont Cohesity peut vous aider à développer et à renforcer la résilience de l'identité

Recevez une évaluation gratuite de la sécurité des identités pour identifier les vulnérabilités et les lacunes dans Active Directory, Entra ID et Okta





© 2026 Cohesity, Inc. All rights reserved. Cohesity, the Cohesity logo, SnapTree, SpanFS, DataPlatform, DataProtect, Helios, and other Cohesity marks are trademarks or registered trademarks of Cohesity, Inc. in the US and/or internationally. Other company and product names may be trademarks of the respective companies with which they are associated. This material (a) is intended to provide you information about Cohesity and our business and products; (b) was believed to be true and accurate at the time it was written, but is subject to change without notice; and (c) is provided on an "AS IS" basis. Cohesity disclaims all express or implied conditions, representations, warranties of any kind.

6100036-001 FR 8-2026