Rubrik Zero Labs

LES IDENTITÉS MENACÉES

MESURER ET RENFORCER LA RÉSILIENCE FACE AUX MENACES BASÉES SUR LES IDENTITÉS

SOMMAIRE

03

Avant-propos

05

Compromission des identités : Le sésame des attaquants pour détourner votre environnement

09

Compromission des identités : l'effet domino

10 Les entreprises contre-attaquent

15

Restauration : pourquoi est-ce si long ?

15 Le MTTR donne une réponse chiffrée

16 Le MTTR en détail

17 L'importance du MTTR

18

Assurer la résilience des identités : Recommandations et capacités de réponse

20 Le cycle de vie de la cyber-résilience

21

Données et méthodologie

AVANT-PROPOS

Rubrik Zero Labs et Wakefield Research ont interrogé 1 625 responsables IT et sécurité du monde entier pour évaluer l'état de préparation de leurs défenses face aux attaques basées sur les identités. Cette étude s'inscrit en complément des quelque 2,2 millions de snapshots que Rubrik scanne chaque jour afin de repérer les menaces tapies au cœur même des données de sauvegarde.

Télétravail, IA agentique, migration vers le cloud… Ces bouleversements ont rendu poreuses les frontières des réseaux telles que nous les connaissons. De simple couche de contrôle, les identités sont devenues le premier vecteur d'attaque, offrant aux adversaires une voie toute tracée vers des environnements IT dont ils n'hésitent pas à détourner les ressources pour leur propre compte. C'est la triste réalité des attaques LOTL, ou Living Off The Land. Ainsi, dans l'écrasante majorité des cas, plutôt que de percer les défenses de votre réseau, les acteurs malveillants exploitent les systèmes de confiance et des identifiants valides pour se faire passer pour des utilisateurs légitimes.

Aujourd'hui, la quasi totalité des offensives impliquent la compromission d'une identité (humaine ou non), que ce soit pour l'accès initial, l'élévation des privilèges ou la latéralisation. C'est donc sans surprise que 90 % des répondants à notre enquête citent les attaques basées sur les identités comme la principale menace pesant sur leur entreprise.

Ce rapport dresse une évaluation chiffrée de la capacité des entreprises à résister face à une cyberattaque. Il met notamment l'accent sur les impératifs à prendre en compte et les projections en termes de délais de réponse.

L'étude passe également en revue les quatre éléments essentiels de la résilience des identités :

- Visibilité, réponse et restauration en temps réel pour les fournisseurs d'identités (IdP) on-prem et cloud et les identités humaines/non humaines
- Confiance dans votre capacité à restaurer de façon rapide et fiable l'infrastructure d'identités à un état antérieur sain
- Renforcement des identités et de la résilience grâce à l'application des principes Zero Trust pour réduire la surface d'attaque et le périmètre d'impact des compromissions
- Intégration de la résilience des identités dans la planification du cycle de vie de la cyber-résilience

Seule une approche holistique réunissant tous ces éléments vous permettra de renforcer votre infrastructure d'identités et de préserver vos revenus, votre image de marque et la continuité de vos activités.

Revenons d’abord sur les tendances qui ont marqué l’année écoulée depuis notre dernier rapport.

2024 vs 2025
LES TENDANCES
(Wakefield)

90 %
des entreprises ont subi une cyberattaque l’an passé

Elles étaient autant à en avoir subi au moins une en 2024

89 %
des victimes de ransomware ont payé la rançon pour récupérer leurs données ou mettre fin à l’attaque

20 %
ont dû faire face à plus de 25 attaques (contre 18 % en 2024)

11 % en ont subi 100 ou plus, soit une légère hausse par rapport à 2024 (8 %)

PERTE DE CONFIANCE DANS LA RAPIDITÉ DE RESTAURATION

En 2025, seulement 28 % des répondants pensent pouvoir se remettre totalement d’un incident cyber en 12 heures ou moins, contre 43 % en 2024

77 %
doivent gérer un environnement cloud plus large que l’année précédente

58 %
sont convaincus que l’IA agentique sera la source de plus de la moitié des cyberattaques l’an prochain

58 %
estiment à 2 jours ou plus le temps nécessaire pour relancer l’intégralité de leurs opérations

COMPROMISSION DES IDENTITÉS :

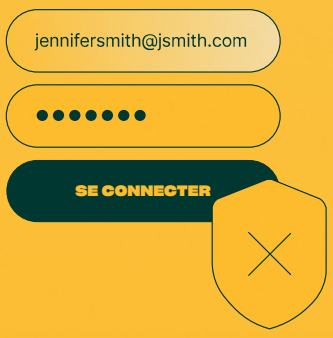
LE SÉSAME DES ATTAQUANTS POUR DÉTOURNER VOTRE ENVIRONNEMENT

Comme nous le soulignions en introduction, la plupart des incidents impliquent à un moment ou à un autre la compromission d'identités.
Or, pour les attaquants, les identités ne sont pas une fin en soi, mais plutôt un moyen d'atteindre leur objectif, quel qu'il soit : espionnage, vol de données, extorsion… La liste est longue.

86 %

des attaques basiques ciblant les applications web utilisent des identifiants volés

(Verizon)[1]



79 %

des incidents détectés par CrowdStrike n'impliquaient aucun malware : les attaquants s'étaient tout simplement authentifiés, sans avoir besoin de déployer un logiciel malveillant

(Crowdstrike 2025)[2]

4,67
MILLIONS $

par compromission

C'est le coût moyen d'une attaque basée sur la compromission d'identifiants

(IBM)[3]

La compromission d'identités ouvre de nombreuses portes à vos adversaires :

Lancer des attaques LOTL, dans lesquelles l'acteur malveillant détourne les processus légitimes (outils admin, services SaaS, voire même les workflows d'identités eux-mêmes) pour déjouer les mécanismes de détection.

Utiliser les identifiants compromis pour organiser d'autres offensives.

Établir une persistance dans l'environnement cible, notamment en créant des plateformes « Shadow Identity », à savoir des tenants ou des infrastructures clandestines échappant à la gouvernance et à la visibilité de l'entreprise.

[1] https://www.verizon.com/business/fr-fr/resources/reports/dbir/
[2] https://www.crowdstrike.com/fr-fr/resources/reports/global-threat-report-executive-summary-2025/
[3] https://www.ibm.com/fr-fr/reports/data-breach

Les identités humaines ne sont pas les seules concernées. Les identités non humaines, ou NHI, représentent une cible tout aussi attractive pour les attaquants. Il s'agit le plus souvent de jetons d'API utilisés pour authentifier les processus informatiques automatisés, mais elles comprennent aussi d'autres éléments comme les certificats, les containers, les outils d'automatisation, les comptes de services ou les agents IA.

Aujourd'hui, les NHI sont 82 fois plus nombreuses que les identités humaines[4]. Une prolifération qui ne fait qu'élargir le terrain de chasse de vos adversaires et qui risque fort de s'accentuer avec l'essor de l'IA agentique.

Les acteurs malveillants ciblent les identités humaines, les NHI, voire les deux, en fonction de leurs objectifs. Il est important de bien comprendre les ressorts de ce ciblage pour mieux défendre ces ressources critiques :

	Identités humaines (Comptes d'employés, identifiants d'administrateurs, etc.)	**Identités non humaines** (Comptes de services, clés d'API, jetons, etc.)
Objectif premier	Accès initial, reconnaissance, détournement des privilèges accordés à l'utilisateur	Déplacement furtif, persistance, accès étendu aux systèmes
Principaux risques	Ingénierie sociale	Erreurs de configuration, prolifération exponentielle
Contournement des défenses	Faciles à gérer – Les comptes humains sont généralement protégés par la MFA, les politiques d'accès et l'analyse des comportements (détection des « voyages impossibles »)	Difficiles à gérer – Les NHI ne sont pas couvertes par la MFA, les contrôles de surveillance sont moins nombreux et les activités automatisées se dissimulent facilement parmi les opérations légitimes
Privilèges	Les privilèges sont généralement liés à un rôle spécifique (ingénieur, commercial, etc.)	Les privilèges sont souvent systémiques et excessifs (par exemple, un compte de service peut lire toutes les bases de données du système)
Persistance	Faciles à révoquer – Les comptes humains peuvent être désactivés, les mots de passe modifiés ou les sessions interrompues en quelques minutes en cas d'incident	Difficiles à révoquer – Les NHI ont une longue durée de vie, tombent dans l'oubli ou deviennent indispensables aux opérations critiques – autant de facteurs qui compliquent leur rotation

[4] https://www.cyberark.com/fr/resources/white-papers/r%C3%A9sum%C3%A9-analytique-du-paysage-de-la-s%C3%A9curit%C3%A9-des-identit%C3%A9s-en-2025

IDENTITÉS : UNE IDÉE FIXE POUR LES ATTAQUANTS

Les identités, humaines ou non, ont beaucoup fait parler d'elles ces derniers temps, notamment en raison de leur rôle central dans plusieurs incidents de cybersécurité très médiatisés.

Latéralisation via Entra ID et n0Auth

En juin 2025, des experts ont repéré une vulnérabilité non corrigée dans Entra ID, le service cloud de Microsoft utilisé pour la gestion des accès et des identités. Cette faille, découverte pourtant deux ans plus tôt, permet aux attaquants d'atteindre les ressources Microsoft 365 d'une entreprise depuis des applications SaaS compromises, et d'accéder à des données sensibles[5].

Il suffit à l'attaquant de modifier l'attribut e-mail dans son propre tenant de façon à ce qu'il corresponde à l'adresse de sa victime, puis d'utiliser la fonctionnalité « Se connecter avec Microsoft » dans l'application SaaS. La vulnérabilité, appelée n0Auth, exploite la logique de vérification des identités au sein des applications concernées, facilitant la latéralisation et l'accès aux outils de productivité clés comme SharePoint et Teams.

Bien qu'elle ait été signalée en 2023, la faille continue d'impacter des dizaines de milliers d'applications SaaS. Problème : la remédiation doit se faire au niveau de chaque tenant concerné. Il est donc impossible à Microsoft de déployer un correctif général. Dans le cas présent, la popularité des outils Microsoft a grandement contribué à accroitre le périmètre d'impact de cette vulnérabilité applicative. Tout au long de l'année 2025, les attaquants ont continué de cibler Entra ID, le plus souvent pour élever leurs privilèges.

Des attaques ToolShell ciblent des serveurs SharePoint on-prem

La vulnérabilité ToolShell, détectée en juillet 2025, met en lumière un autre vecteur d'attaque lié aux identités : l'authentification par clé. Dans cette campagne, des acteurs malveillants suspectés de travailler pour le compte d'une puissance étrangère ont jeté leur dévolu sur des clés machines utilisées pour authentifier les serveurs SharePoint on-prem d'entreprises de premier plan. On peut en déduire qu'ils cherchaient ainsi à établir une présence pour espionner à l'envi les environnements compromis[6].

Preuve que les NHI constituent une cible de choix pour les cyber-espions et autres attaquants. Parce qu'elles sont moins éphémères que les jetons, les clés doivent être rapidement modifiées après un incident de sécurité ou la découverte d'une CVE comme ToolShell.

Scattered Spider piège les humains dans sa toile

Le groupe Scattered Spider aime se faire passer pour des équipes IT ou de support dans le but de soutirer des identifiants à des utilisateurs peu méfiants et ainsi contourner l'authentification multifacteur (MFA). Et pour mettre toutes les chances de son côté, il n'hésite pas à manipuler nos ressorts psychologiques, exploitant l'empathie mais aussi l'empressement d'équipes de support sous pression à résoudre les problèmes toujours plus vite. Scattered Spider serait notamment à l'origine d'une attaque contre Clorox. Un simple appel à son support (géré par un fournisseur externe) lui aurait permis de réinitialiser un mot de passe, provoquant au final une perte totale de 380 millions de dollars pour le géant des produits ménagers[7].

Ainsi, pour s'infiltrer dans votre environnement, Scattered Spider ne mise pas sur les vulnérabilités zero-day mais sur les vulnérabilités humaines, en déployant tout l'éventail des techniques d'ingénierie sociale. Il peut ensuite détourner les outils natifs comme PowerShell et les services SaaS. De toute évidence, les solutions techniques ne suffisent pas pour le tenir à distance. En plus de renforcer la résilience de leurs infrastructures d'identités, les entreprises doivent investir dans une sécurité pensée pour limiter les failles humaines, notamment par une sensibilisation continue et adaptée des collaborateurs.

[5] https://www.infosecurity-magazine.com/news/microsoft-noauth-flaw-2025/
[6] https://www.recordedfuture.com/blog/toolshell-exploit-chain-thousands-sharepoint-servers-risk
[7] https://www.cybersecuritydive.com/news/clorox-380-million-suit-cognizant-cyberattack/753837/

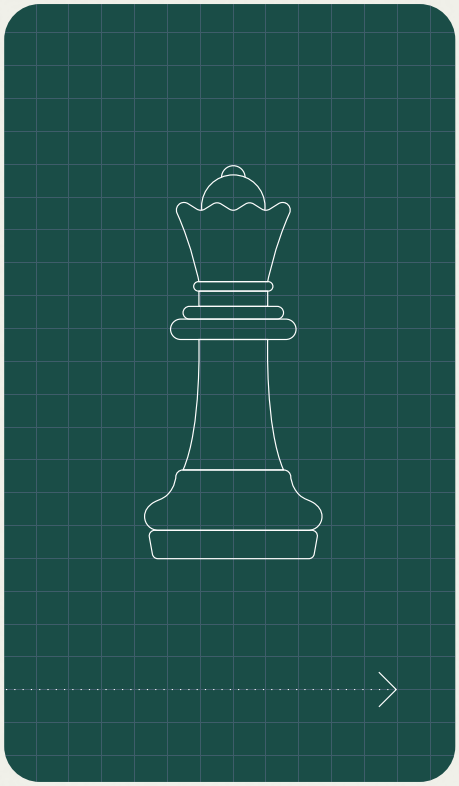
COMPROMISSION DES IDENTITÉS : L'EFFET DOMINO

En compromettant vos identités, les attaquants mettent la main sur les clés du royaume. Ce précieux sésame leur ouvre les portes de votre environnement et leur donne accès à des outils qu'ils peuvent ensuite exploiter à leur guise pour vous espionner ou exfiltrer vos données en masse.

Quand on voit les dégâts causés par une seule compromission, on comprend mieux pourquoi les acteurs malveillants ont fait des identités leur cible de prédilection :

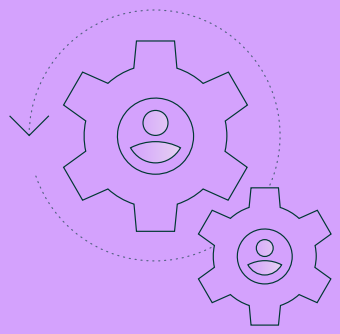
Type d'impact	Conséquence	Assets concernés
Compromission de données	Exfiltration d'informations sensibles (données à caractère sensible, propriété intellectuelle, données financières, etc.)	Données client, données collaborateur, secrets de fabrication, avantage concurrentiel, dossiers financiers
Pertes financières	Fraude, coûts de la réponse à incident, frais juridiques, sanctions réglementaires	Budget, revenus, ressources juridiques
Atteinte à la réputation	Perte de la confiance des clients, érosion de l'image de marque, mauvaise presse	Valeur de la marque, relations avec les clients et partenaires, valeur sur le marché
Perturbations opérationnelles	Interruption des systèmes ou des services, verrouillage des comptes	Revenus, investissements dans l'infrastructure IT, contrôles de sécurité
Persistance et élévation des privilèges	Installation de backdoors (principaux de services, mods de fédération), création de plateformes « Shadow Identity »	Infrastructure IT, gestion des identités et des accès (IAM), contrôles de sécurité
Problèmes de conformité et risque juridique	Violation des règlements sur la confidentialité des données (RGPD, CCPA), actions en justice	Ressources juridiques, équipe de conformité
Compromission de la supply chain	Compromission de partenaires et autres tiers, avec effet domino sur toute la chaîne	Écosystème de partenaires, intégrité de la supply chain, réputation

LES ENTREPRISES CONTRE-ATTAQUENT



90 %

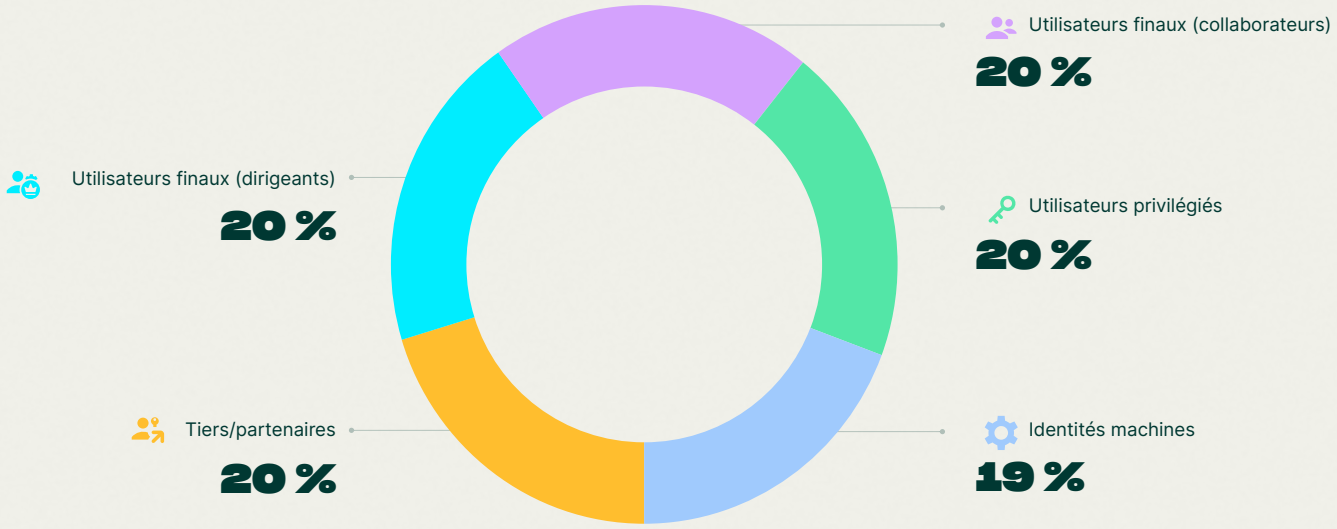
des responsables IT et sécurité interrogés classent les cyberattaques basées sur les identités en tête des menaces pesant sur leur entreprise.



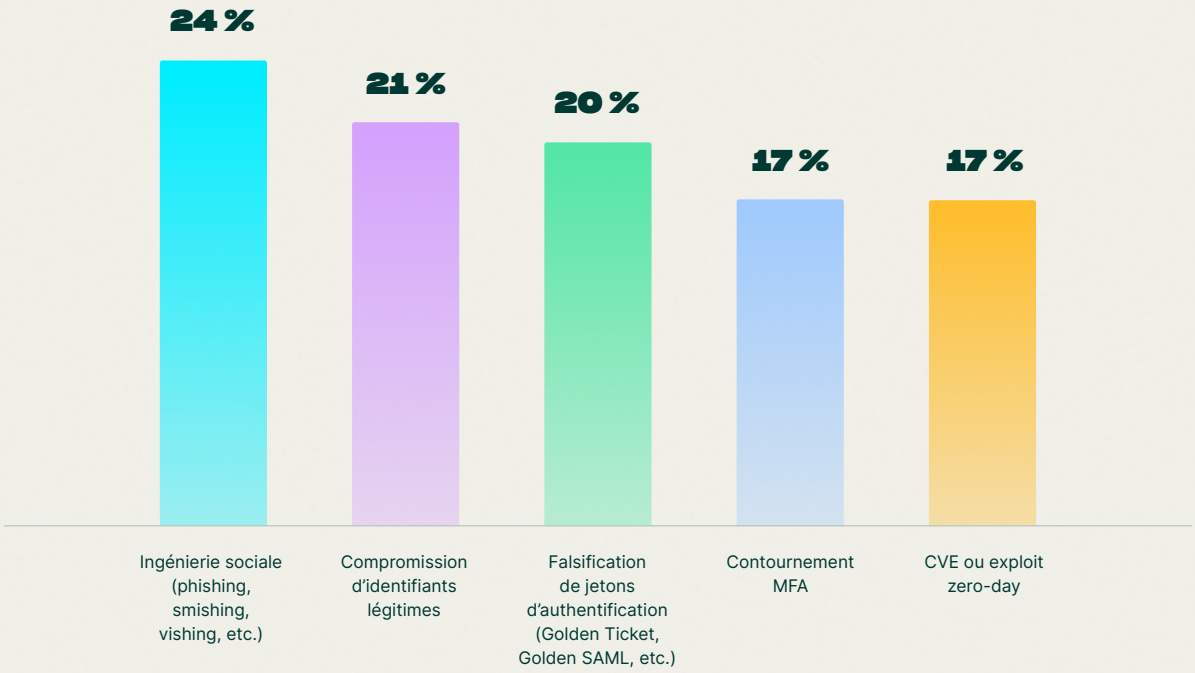
89 %

envisagent de confier à des professionnels externes le pilotage ou le renforcement de la gestion, de l'infrastructure ou de la sécurité des identités au cours des 12 prochains mois

Quels sont les types d'identités les plus exposés aux compromissions ?



Si, auparavant, les dirigeants citaient uniquement les comptes à privilèges au rang des identités critiques, ils comprennent aujourd'hui que chaque identité, même la moins privilégiée, peut servir de porte d'entrée aux attaquants. Une fois introduits, ils peuvent ensuite se latéraliser ou s'octroyer des droits toujours plus élevés.



Les données collectées lors de notre étude montrent également un grand bouleversement dans les priorités de sécurité. Si l'ingénierie sociale reste en tête (24 %), le contournement de la MFA (17 %) et la falsification de jetons d'authentification (20 %) sont désormais au coude à coude avec les exploits zero-day (17 %).

Ce changement majeur montre que les dirigeants ont intégré cette nouvelle réalité : les attaquants n'entrent plus par effraction. Ils utilisent les systèmes d'authentification pour se connecter comme n'importe quel utilisateur légitime.

En 2024, Mandiant est intervenu sur un nombre record de compromissions d'environnements cloud[8]. Un déferlement que l'expert en sécurité attribue au manque de contrôle dans les solutions d'identités. Face à ce nouveau vecteur d'attaque et aux techniques récentes déployées par les acteurs malveillants, les solutions IAM peinent à garder le rythme.

Et ce pour de multiples raisons :

La gestion des identités est un domaine multi-facettes –

PAM (gestion des accès privilégiés), RBAC (contrôle des accès basé sur les rôles), sécurité des API… L'IAM est un domaine complexe, comportant de multiples branches et solutions fournies par différents prestataires. Ce patchwork étend la surface d'attaque des entreprises.

De nouveaux types d'identités apparaissent constamment –

Les bots et agents IA représentent deux nouveaux types de NHI encore inconnues il y a cinq ans. Quant aux API, elles sont plus omniprésentes que jamais dans les entreprises. La prolifération des agents risque fort d'entraîner une explosion du nombre d'identités machine-to-machine qui, pour la plupart, ne sont couvertes par aucun processus de gestion mature (provisionnement, rotation, dé-provisionnement), contrairement aux comptes humains.

Les acteurs malveillants innovent dans l'art d'exploiter les identités –

Face à des mécanismes de protection toujours plus efficaces, que ce soit sur les terminaux ou sur le périmètre, les attaquants doivent trouver d'autres moyens de s'infiltrer. Ils priorisent donc le vol d'identifiants pour s'authentifier via les systèmes légitimes, sans effraction.

Le cloud introduit de nouveaux risques –

La complexité et la granularité des solutions IAM cloud-native les rendent particulièrement susceptibles aux erreurs humaines et aux problèmes de configuration. Les attaquants sont à l'affût de ces failles, en particulier les rôles dotés de droits trop étendus ou les autorisations attribuées par erreur à tous les utilisateurs.

[8] https://services.google.com/fh/files/misc/m-trends-2025-en.pdf

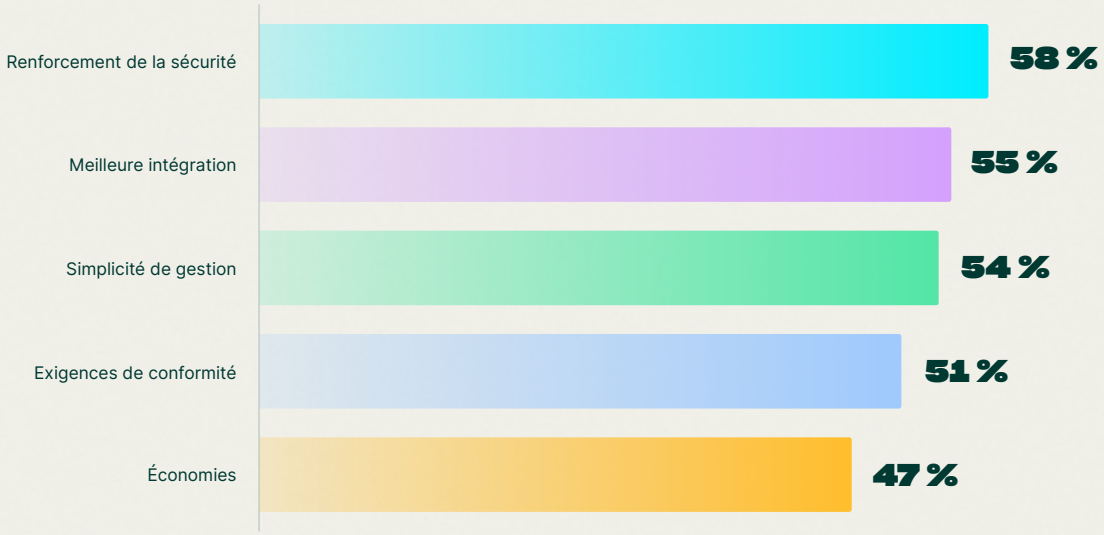
Pas étonnant que :

87 %
des responsables IT et de sécurité envisagent actuellement ou sont déjà en train de changer de fournisseur IAM.

58 %
d'entre eux veulent changer de fournisseur pour renforcer leur sécurité, preuve que les fonctionnalités de protection des identités proposées par la plupart des solutions ne sont pas suffisantes.

60 %
avaient pourtant déjà changé de fournisseur IAM au cours des trois dernières années.

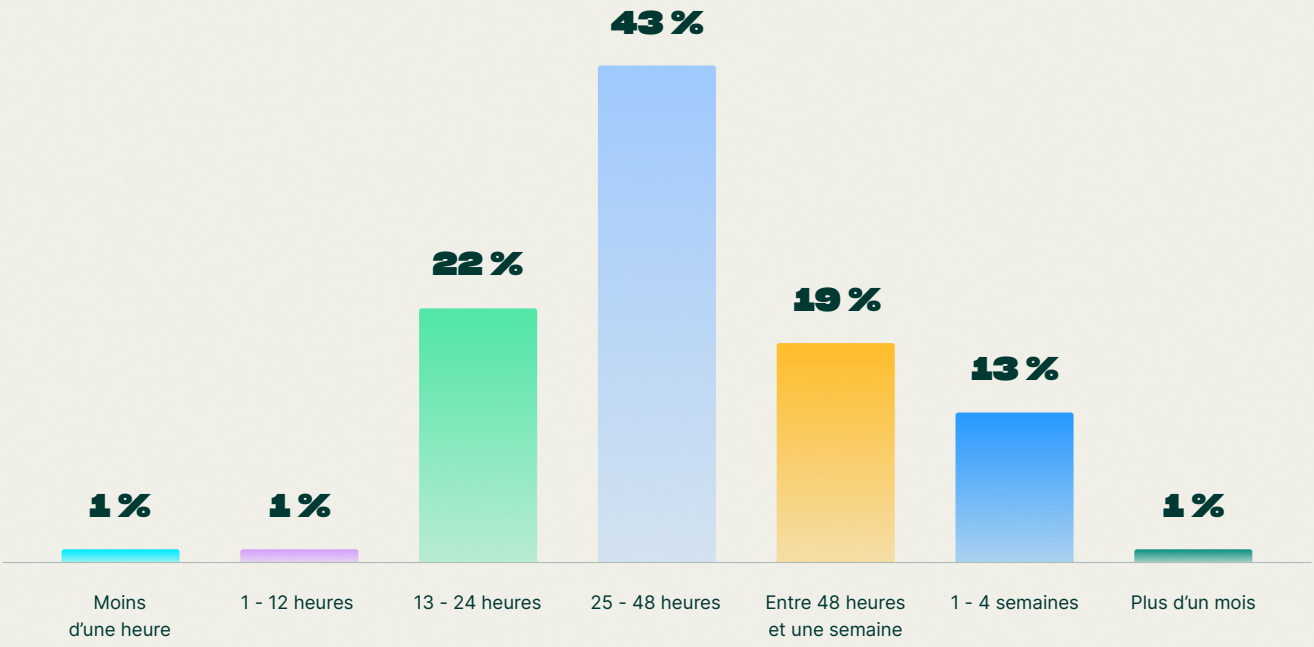
Les principales raisons pour lesquelles les responsables souhaitent changer de fournisseur IAM :



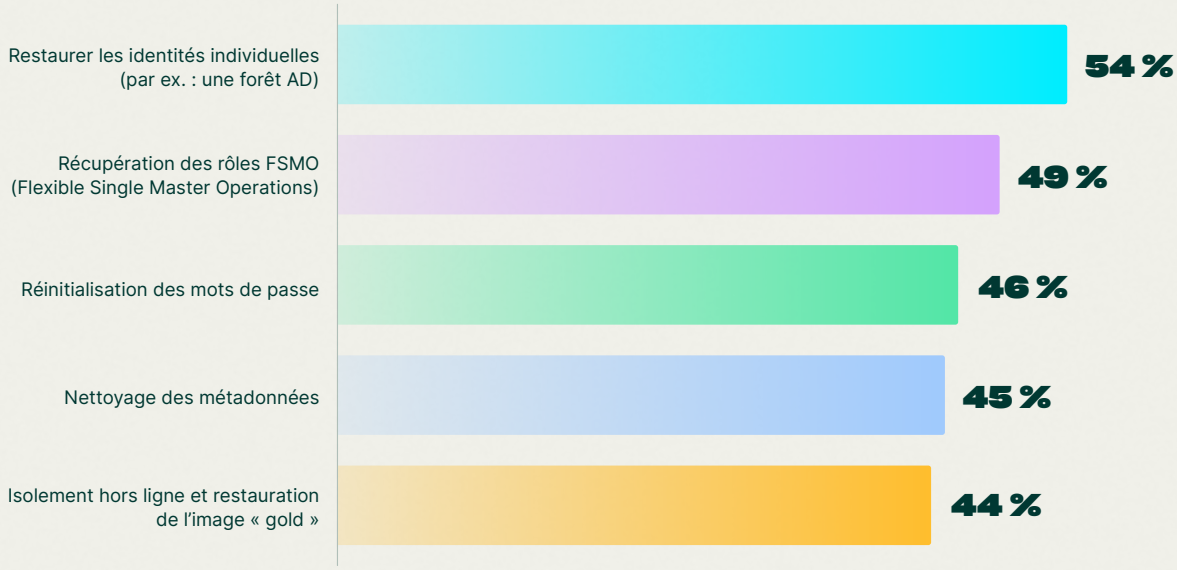
Plus inquiétant encore, le temps nécessaire pour restaurer toute l'infrastructure après une compromission peut être douloureusement long. Quand on sait que chaque interruption peut coûter jusqu'à 6 000 $ par minute[9], les entreprises qui misent uniquement sur des processus de restauration manuels (54 %) subissent souvent des pertes considérables.

[9] https://www.isaca.org/resources/news-and-trends/industry-news/2024/centralized-services-and-their-impact-on-business-continuity

Temps nécessaire aux répondants pour restaurer leur infrastructure d'identités post-compromission :



Processus nécessitant une restauration manuelle :



Chiffre intéressant : 89 % des répondants ont intégré des agents IA à une partie ou à l'intégralité de leur infrastructure d'identités. Ces nouveaux types de NHI devront être protégés à une échelle massive, tout au long de leur cycle de vie, pour éviter qu'ils ne tombent entre de mauvaises mains. Les répondants à notre étude sont déjà sur leurs gardes : 58 % prévoient d'ores et déjà que l'IA agentique sera à l'origine de plus de la moitié des cyberattaques l'an prochain.

Pour mesurer et améliorer les temps de réponse et de restauration, les entreprises doivent avant tout comprendre quels acteurs malveillants ciblent quelles identités, et pourquoi.

RESTAURATION : POURQUOI EST-CE SI LONG ?

LE MTTR DONNE UNE RÉPONSE CHIFFRÉE

La cyber-résilience est pour beaucoup d'entreprises l'objectif à atteindre, mais peu d'entre elles parviennent à le quantifier. Car comment évaluer la faculté d'une entreprise à anticiper les cybermenaces ? À y résister ? À s'en relever ?

Deux métriques étaient jusqu'alors utilisées pour mesurer ces capacités : l'objectif de temps de restauration (RTO) et l'objectif de point de reprise (RPO). Mais celles-ci ne montrent qu'une partie du tableau. Une entreprise peut ainsi définir un RTO de quatre heures pour un incident, mais passer plus d'un mois à restaurer ses activités. À l'opposé, un RPO peut se limiter à quelques minutes, mais une banque peut perdre sur ce court laps de temps des données couvrant des centaines de milliers de transactions. Dans ces deux exemples, on comprend facilement que les équipes de restauration n'ont pas atteint leurs objectifs. Mais impossible de savoir pourquoi.

Autre obstacle à une évaluation précise de la restauration : les entreprises utilisent chacune des métriques différentes pour mesurer leur performance. Pour certaines, le chronomètre s'arrête dès que la menace est détectée. D'autres ne le stopperont qu'une fois l'attaquant éradiqué. Difficile, dans ces conditions, d'obtenir une visibilité complète sur la cyber-résilience d'une entreprise et d'établir une comparaison parlante entre les verticales.

C'est pourquoi Rubrik Zero Labs recommande une nouvelle méthode d'évaluation : le temps moyen de restauration, ou MTTR. Cette métrique standard, basée sur des données concrètes et divisée en plusieurs phases, mesure la capacité de l'entreprise à se relever d'un incident.

LE MTTR EN DÉTAIL

Le MTTR ne se contente pas de mesurer la restauration à un instant t. Il se décompose en plusieurs phases distinctes pour offrir des éclairages précis et identifier les axes d'amélioration. Ce modèle couvre les étapes suivantes :

Détection	C'est le point de départ de tout incident, qu'il s'agisse d'une cyberattaque ou d'une suppression accidentelle.
Définition du périmètre	L'objectif de cette phase est d'identifier tous les systèmes et assets impactés, ainsi que leurs dépendances. Il est en effet essentiel de savoir quelles applications dépendent de quelles bases de données, et vice versa.
Identification d'un point de restauration fiable	C'est la phase la plus importante, et souvent la plus longue. Elle prend fin uniquement lorsque l'entreprise a trouvé une sauvegarde fiable, dénuée de tout malware, à partir de laquelle restaurer ses opérations. Il fallait auparavant des semaines, voire des mois, pour installer un environnement isolé, ou « clean room », dans lequel tester les données. Heureusement, de nouveaux outils comme les infrastructures cloud et l'automatisation accélèrent considérablement le processus.
Rétablissement	Cette phase a pour but la récupération et le rétablissement des données en elles-mêmes. Une restauration trop lente (par ex. : plusieurs semaines) peut indiquer un problème de débit. Il peut alors être judicieux d'investir dans une infrastructure plus performante pour réduire le délai des restaurations les plus urgentes. Compte tenu du nombre croissant de données générées par les entreprises, cette phase pourrait bien un jour durer plus longtemps que la phase d'identification des points de restauration fiables.
Validation	Combien de temps faut-il pour restaurer l'intégralité de l'application et l'accès aux données ? Pour s'assurer que les identités humaines et non-humaines fonctionnent et communiquent parfaitement ?

En prenant des mesures à chacune de ces phases, vous obtenez la visibilité granulaire et contextualisée nécessaire pour repérer les goulets d'étranglement et améliorer vos décisions.

Métrique	Début	Fin	Descriptif
MTTD – Temps moyen de détection	Date et heure du premier signe de l'incident ou de l'alerte	Confirmation du périmètre à restaurer	La détection, l'analyse des anomalies et la corrélation SIEM jouent un rôle déterminant dans cette phase
MTTS – Temps moyen de définition du périmètre	Validation de la détection	Confirmation de la liste des objets à restaurer	Cette phase fait intervenir plusieurs capacités : Global Search, Data Classification et SLA Metadata
MTTCS – Temps moyen d'identification du point de restauration fiable	Validation du périmètre	Identification d'un snapshot propre et non compromis	L'immutabilité, l'analyse des menaces et les scores d'intégrité des snapshots accélèrent le processus
MTTr – Temps moyen de rétablissement	Activation du rétablissement	Le données sont accessibles pour le workload	Les capacités Instant Recovery, Live Mount ou Cloud Disaster Recovery Orchestration facilitent cette phase
MTTV – Temps moyen de validation	Accès aux données établi	Confirmation de l'intégrité de l'application	Grâce à une sauvegarde homogène des applications, à des playbooks d'automatisation et à des analyses de malware post-restauration

MTTR (opérationnel) = MTTD + MTTS + MTTCS + MTTr + MTTV

L'IMPORTANCE DU MTTR

Les données de sauvegarde renferment de précieux éclairages, trop souvent ignorés par les entreprises. Le MTTR transforme ces informations en outil puissant pour non seulement garantir une restauration efficace, mais aussi mesurer la résilience.

Le MTTR s'inscrit dans un cycle continu d'évaluation de la maturité :

1

Évaluation de la résilience

Mesurer la capacité de l'entreprise à résister à une attaque via un système de notation bien conçu, prenant en compte les applications critiques et les scénarios les plus probables, selon un processus similaire à une évaluation des risques.

2

Définition du MVB (Minimum Viable Business)

Cerner et prioriser les applications et bases de données (ainsi que leurs dépendances) essentielles à la continuité des activités, ce que ne permettent pas les enquêtes et inventaires d'applications traditionnels.

3

Confirmation de la restaurabilité

Mettre les défenses à l'épreuve au moyen de simulations de crise réalistes (générées par des logiciels reproduisant les conditions du réel) afin d'obtenir un temps de restauration mesurable dans un contexte serein, plutôt qu'en situation de crise. Ces mesures pourront ensuite servir de base de référence à des améliorations futures.

4

Analyse et amélioration

Analyser et améliorer le processus à chaque phase de la restauration, pour repérer et éliminer les goulets d'étranglement. Par exemple, en réduisant le volume des données critiques à rétablir de 20 To à 2 To, les entreprises peuvent augmenter considérablement la cadence de restauration.

En anonymisant et en agrégeant ces données MTTR, vous créez des benchmarks puissants qui vous permettront de vous comparer aux autres entreprises du secteur ou de la région. Ces informations donnent aux responsables de solides arguments en faveur d'un investissement dans la cyber-résilience. Elles éliminent aussi les silos en offrant aux équipes IT, sécurité et restauration la même visibilité sur des KPI clés (rapidité de la restauration, fiabilité du processus, etc.).

ASSURER LA RÉSILIENCE DES IDENTITÉS :

RECOMMANDATIONS ET CAPACITÉS DE RÉPONSE

Les identités ne doivent plus être considérées comme un simple asset à protéger, mais comme un véritable plan de contrôle nécessitant des mesures adaptées.

Ce changement de paradigme bouleverse complètement le modèle d'investissement dans la sécurité : les défenses focalisées uniquement sur le réseau et les terminaux doivent laisser la place à une gouvernance complète des identités, à une gestion stricte des privilèges d'accès et à des solutions d'authentification avancées. Une identité compromise ouvre un boulevard (souvent indétecté) vers les assets les plus précieux d'une entreprise. Bref, entre de mauvaises mains, les identités peuvent se transformer en une arme aussi puissante que dangereuse.

Face à la prolifération des attaques basées sur les identités, les entreprises doivent prioriser les capacités suivantes :

Visibilité et restauration des identités

Une clé d'API cloud a été compromise. Quels systèmes devez-vous isoler ? Un acteur malveillant a pris le contrôle d'un compte admin Okta ou Active Directory. Pouvez-vous endiguer rapidement l'attaque et déclencher de force la réauthentification des utilisateurs affectés ? Pour répondre à ces questions, vous avez besoin d'une visibilité en temps réel et de capacités solides de restauration dans les environnements hybrides d'identités.

Renforcement de la résilience des identités

La résilience désigne votre capacité à rebondir rapidement et sereinement en cas de crise. Sur ce plan, des sauvegardes sécurisées et hors ligne d'Active Directory ou des répertoires cloud se révèlent essentielles pour rétablir les services d'identités en cas de chiffrement malveillant ou de suppression accidentelle. En planifiant soigneusement les étapes de restauration avec l'équipe de sécurité, les entreprises peuvent réduire considérablement les interruptions et l'impact financier d'une compromission d'identités.

Réduction de la surface d'attaque et du périmètre d'impact grâce au Zero Trust

Les identités représentent un nouveau périmètre à protéger. Chaque demande d'accès, qu'elle provienne de l'intérieur ou de l'extérieur du réseau, doit faire l'objet d'une authentification, d'une autorisation et d'un chiffrement continus. Pour y parvenir, vous devez mettre en place trois mesures clés : MFA, politiques d'accès conditionnels et application par défaut des principes du moindre privilège.

LE ZERO TRUST APPLIQUÉ À LA SÉCURITÉ DES IDENTITÉS

Moindre privilège et RBAC
(contrôle d'accès basé sur les rôles)

Tous les utilisateurs et tous les appareils, où qu'ils se trouvent, disposent du minimum de droits requis pour effectuer leur mission.

Accès JIT (Just-In-Time)

Les autorisations ou les accès étendus ne sont accordés que pour une durée limitée et prédéfinie, en fonction du temps nécessaire pour compléter la tâche requise. Une fois ce délai échu, les permissions sont automatiquement révoquées.

Vérification continue

Outre l'application de la MFA, l'identité de l'utilisateur, la posture de l'appareil et le contexte (lieu, date et heure, etc.) sont constamment surveillés et réévalués pour savoir quand maintenir ou, au contraire, révoquer les accès.

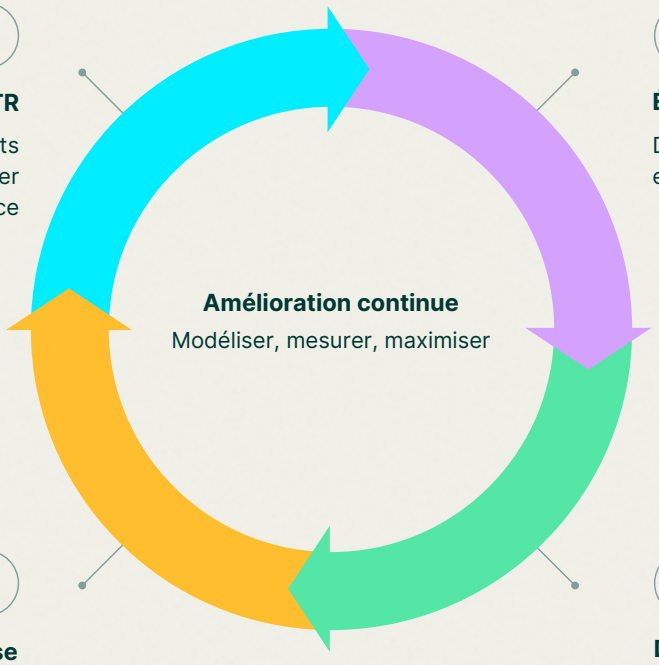
Micro-segmentation

Les réseaux sont divisés en plusieurs segments afin d'endiguer les éventuelles attaques et d'empêcher les utilisateurs non autorisés de se déplacer latéralement d'un segment à l'autre, à la recherche d'assets à compromettre.

LE CYCLE DE VIE DE LA CYBER-RÉSILIENCE

La cyber-résilience, la vraie, va au-delà des principes de cybersécurité. Elle intègre la gestion des risques, la continuité des activités et la réponse à incident dans une stratégie unifiée. L'objectif n'est plus simplement de bloquer l'attaque mais d'y résister et d'en limiter l'impact pour rebondir rapidement.

Le cycle de vie de la cyber-résilience



1

Évaluation de la résilience

Définir et cerner la posture de sécurité et le profil de risque de l'entreprise

2

Définition de la MVB

Identifier les assets et infrastructures critiques aux opérations (Minimum Viable Business)

3

Simulation de crise

Mettre les défenses et la posture de sécurité à l'épreuve pour évaluer les résultats

4

Analyse du MTTR

Identifier et éliminer les goulets d'étranglement pour améliorer la cyber-résilience

Amélioration continue

Modéliser, mesurer, maximiser

Conforme aux recommandations NIST[10] pour la préparation, la protection, la restauration et l'adaptation aux différents schémas de cyberattaques, le framework Rubrik Zero Labs aide les équipes à opérationnaliser la résilience tout en offrant aux responsables des benchmarks et des métriques efficaces pour améliorer le processus.

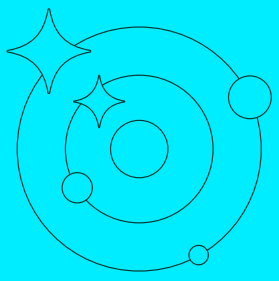
En intégrant la protection des identités dans leur stratégie de cyber-résilience, les entreprises gagnent sur tous les plans : elles limitent les interruptions, défendent leurs assets critiques et gagnent la confiance de leurs parties prenantes.

[10] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-160v2r1.pdf

DONNÉES ET MÉTHODOLOGIE

Rubrik Zero Labs s'engage à fournir aux entreprises des informations concrètes et impartiales pour les aider à renforcer la sécurité de leurs données.

Nous nous appuyons pour cela sur trois grandes sources de données :

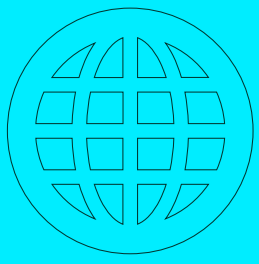


TÉLÉMÉTRIE RUBRIK

La télémétrie Rubrik nous éclaire sur les environnements data des entreprises et les risques associés.

ÉTUDE INDÉPENDANTE

Points de vue de plus de 1 600 responsables IT et sécurité recueillis par Wakefield Research



CONTRIBUTEURS AU RAPPORT

Études menées par des acteurs reconnus dans le monde de la cybersécurité.