RAPPORT

L'état de la sécurité des identités 2026

Perspectives de 5 000 responsables informatiques et cybersécurité de 17 pays

SOPHOS

Introduction

L'identité constitue le périmètre de la cybersécurité, et ce périmètre s'élargit à mesure que les systèmes d'IA obtiennent accès de plus en plus aux données d'entreprise par le biais des emails, des fichiers, des applications SaaS, ainsi que des identités humaines et non humaines. Cela se traduit par une exposition accrue, les informations sensibles étant désormais plus facilement accessibles et plus faciles à transférer.

Alors que les organisations continuent d'accélérer leur transition vers le cloud, le télétravail et l'utilisation de multiples applications et services reposant sur des connexions entre machines, le nombre d'identités numériques — humaines et non humaines — a explosé. Chaque identifiant, clé API, compte de service et jeton OAuth constitue un point d'entrée potentiel pour les adversaires. Cela fait de la sécurité des identités l'un des enjeux les plus critiques et les plus complexes de la cyberdéfense moderne.

Les attaquants ont bien pris conscience de ce tournant. Le vol d'identifiants, la compromission de comptes de service et les attaques d'ingénierie sociale visant les employés comptent désormais parmi les vecteurs d'accès initiaux les plus courants dans les violations partout dans le monde. Les adversaires ont recours à l'IA et à l'automatisation pour agir plus rapidement et sur un plus grand nombre de systèmes. Les conséquences vont du vol de données avec extorsion aux attaques de ransomware à grande échelle, susceptibles de paralyser les activités de l'entreprise pendant plusieurs jours, voire plusieurs semaines.

Afin de mieux cerner l'ampleur réelle et l'impact des menaces liées à l'identité, Sophos a commandé une enquête indépendante menée auprès de 5 000 responsables informatiques et cybersécurité dans 17 pays, portant sur leurs expériences en matière de menaces liées à l'identité et sur les répercussions qu'elles ont entraînées en 2025. Ce rapport présente les conclusions de l'étude, qui examine la fréquence des attaques liées à l'identité, la capacité des organisations à les détecter et à les neutraliser, leurs conséquences, les causes premières des violations réussies, leur coût financier, ainsi que les pratiques de gestion de sécurité des identités.

Les résultats dressent un tableau alarmant : omniprésentes, les menaces liées à l'identité ont des conséquences graves et sont très largement associées à des attaques de ransomwares. Les organisations qui négligent d'investir dans la sécurité des identités s'exposent à des risques considérables pour leurs activités, leurs finances ainsi que leur réputation.

5 000

responsables informatiques et cybersécurité issus de 17 pays ont participé à une enquête indépendante mondiale

Aperçu des principales découvertes

- **71 % des organisations ont subi au moins une violation de sécurité liée à l'identité** au cours des 12 derniers mois, avec une moyenne de 3 attaques par organisation touchée.
- **14 % des organisations victimes d'une violation n'ont pas été en mesure de détecter et de contrer** l'attaque liée à l'identité la plus critique avant qu'elle ne fasse des dégâts.
- **Le coût moyen de remédiation d'une violation d'identité s'élevait à 1,64 million de dollars**, le coût médian s'établissant à 750 000 dollars.
- **Le vol de données (49 %) et les ransomwares (48 %) ont été les conséquences** les plus fréquentes lors d'attaques d'identité réussies.
- **Les deux tiers (67 %) des victimes de ransomware ont indiqué que l'attaque de ransomware correspondait également à l'attaque basée sur l'identité la plus grave** ; établissant un lien direct entre identité et ransomware.
- **Une gestion défaillante des identités non humaines (NHI) a été citée dans 41 % des cas de violation d'identité**, ce qui en fait la deuxième cause individuelle la plus fréquente, après l'erreur humaine (43 %).
- **Les organisations dotées d'une stratégie de gestion des NHI insuffisante ont 22 % plus de risques de subir un vol financier, 24 % plus de risques d'être victimes d'une extorsion** et de déclarer des coûts de rétablissement supérieurs de près de 150 000 dollars à la moyenne.
- **Seule une organisation sur trois (34 %) procède régulièrement à des rotations ou des audits de leurs comptes de service et de leurs identités non humaines**, et seuls 11 % le font de manière continue, ce qui crée des failles de sécurité que les attaquants peuvent exploiter.
- **Seuls 24 % des organisations surveillent en continu les tentatives de connexion inhabituelles**, et plus de la moitié ne procèdent à ces vérifications que tous les trois mois, voire moins souvent.
- **Les fournisseurs d'énergie, de pétrole/gaz et de services d'utilité publique (80 %) et l'administration publique centrale (78 %) ont enregistré les taux les plus élevés de violations d'identité**, tandis que les secteurs de l'informatique, des technologies et des télécommunications (63 %) ainsi que celui de la santé (63 %) ont affiché les taux les plus bas.
- **Les petites organisations (comptant entre 100 et 250 employés) avaient 72 % moins de chances de détecter une attaque** liée à l'identité que celles comptant entre 1 001 et 3 000 employés (19 % contre 11 %).

Résultats détaillés

Fréquence des attaques basées sur l'identité

L'enquête révèle que les violations liées à l'identité, loin d'être des cas isolés, sont désormais monnaie courante. Plus de sept organisations sur dix (70,9 %) ont subi au moins une telle violation au cours des 12 derniers mois. Seuls 22,6 % ont déclaré formellement n'en avoir subi aucune, tandis que 6,4 % ont admis que des violations pouvaient avoir eu lieu à leur insu.

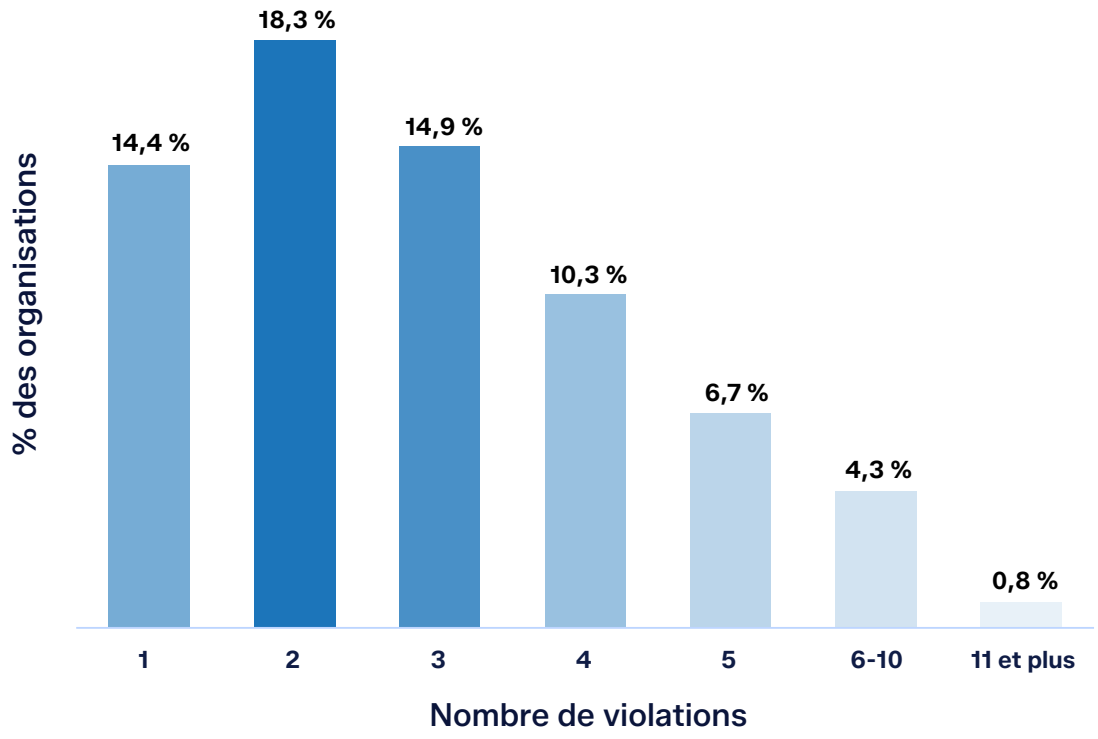
Parmi les victimes de ces violations, le nombre moyen d'incidents s'élevait à 3,1. Un chiffre qui montre que les attaques visant l'identité sont rarement des événements isolés. 5 % des répondants ont déclaré avoir subi au moins six violations au cours de l'année écoulée.

67 %

des incidents examinés en 2025 par Sophos Incident Response et Sophos MDR étaient liés à des attaques basées sur l'identité.

Information Sophos X-Ops

Distribution de fréquence des violations



Votre organisation a-t-elle subi des violations de sécurité liées à l'identité au cours des 12 derniers mois ? Si oui, combien ? n = 5 000

Tendances par pays

Les taux de violation varient considérablement d'un pays à l'autre. La Suisse (88,7 %) a enregistré le taux le plus élevé, soit 18 points de pourcentage au-dessus de la moyenne mondiale, suivie du Mexique (83,3 %) et de l'Italie (80,0 %). L'Allemagne (62,6 %), la Colombie (62,7 %) et le Japon (64,7 %) ont été les moins touchés, même si les taux les plus bas dépassent tout de même les 60 %.

Pays	Taux de violation	vs Mondial (70,9 %)
Suisse	88,7 %	+17,8 pp
Mexique	83,3 %	+12,4 pp
Italie	80,0 %	+9,1 pp
Australie	79,7 %	+8,8 pp
Inde	76,8 %	+5,9 pp
Afrique du Sud	75,0 %	+4,1 pp
Brésil	74,0 %	+3,1 pp
EAU	73,3 %	+2,4 pp
Singapour	72,0 %	+1,1 pp
Espagne	70,0 %	-0,9 pp
Chili	66,7 %	-4,2 pp
États-Unis	66,1 %	-4,8 pp
France	66,0 %	-4,9 pp
Royaume-Uni	65,3 %	-5,6 pp
Japon	64,7 %	-6,2 pp
Colombie	62,7 %	-8,2 points
Allemagne	62,6 %	-8,3 pp

Votre organisation a-t-elle subi des violations de sécurité liées à l'identité au cours des 12 derniers mois ? Si oui, combien ? n = 5 000.

Tendances par secteur

Si l'on examine les données sous l'angle sectoriel, ce sont les secteurs de l'énergie, du pétrole/gaz et des services d'utilité publique (80,3 %) et l'administration publique centrale (78,4 %) qui ont enregistré les taux de violation les plus élevés. Les secteurs de l'informatique, des technologies et des télécommunications (63,1 %), ainsi que celui de la santé (63,4 %), ont été les moins touchés. Cette tendance s'explique peut-être par une plus grande maturité des investissements en matière de cybersécurité dans ces secteurs.

Secteur d'activité	Taux de violation
Énergie, pétrole/gaz, services d'utilité publique	**80,3 %**
Administration publique centrale	78,4 %
Construction et immobilier	76,1 %
Manufacture et production	73,6 %
Retail	72,0 %
Enseignement des 1er et 2nd degrés	71,1 %
Services financiers	71,0 %
Médias, loisirs, divertissement	70,9 %
Administration publique locale	69,6 %
Distribution et transport	67,6 %
Enseignement supérieur	65,9 %
Services aux entreprises et professionnels	64,5 %
Santé	63,4 %
IT, technologies et télécoms	63,1 %

Votre organisation a-t-elle subi des violations de sécurité liées à l'identité au cours des 12 derniers mois ? Si oui, combien ? n = 5 000.

La conformité, révélateur du niveau de risque

Les organisations qui ont qualifié le respect des exigences de conformité de « très difficile » affichaient un taux de violation de 82,4 %, soit 14 points de pourcentage de plus que celles qui considéraient que la mise en conformité était « peu ou pas du tout difficile » (68,3 %). Cela montre que les problèmes de conformité peuvent être le signe avant-coureur de violations de sécurité plus larges.

Les bases de la sécurité des identités

Quatre types d'identité sont à prendre en compte

Chaque organisation accorde l'accès à différents types d'identités. Chacune comporte ses propres risques.

Catégorie 1 : identités du personnel

Il s'agit des membres de l'organisation ayant besoin d'un accès aux systèmes et aux données pour exercer leurs fonctions.

- Employés
- Sous-traitants
- Administrateurs IT et infosec (collaborateurs dont les fonctions nécessitent un accès privilégié au système)
- Cadres supérieurs (collaborateurs dont le rôle présente une valeur particulière pour les adversaires)

Catégorie 2 : identités externes

Il s'agit des membres extérieurs à l'organisation auxquels un accès est accordé, à titre temporaire ou permanent, afin qu'ils puissent remplir une fonction ou une intervention spécifique.

- Partenaires
- Fournisseurs
- Clients

Catégorie 3 : identités non humaines (NHI)

Il s'agit des logiciels, systèmes et processus automatisés autorisés à effectuer des tâches sans intervention humaine.

- Comptes de service (par exemple, sauvegardes planifiées)
- Clés API (par exemple, intégrations d'applis)
- Agents IA (par exemple, tâches autonomes)
- Appareils IoT (par exemple, capteurs, caméras)

Catégorie 4 : identités privilégiées (risque maximal)

Toute entité, humaine ou non, disposant de droits d'accès étendus lui permettant d'accéder en profondeur à des systèmes et à des données sensibles.

- Super-administrateurs (c'est-à-dire les personnes disposant d'un contrôle total sur le système)
- Comptes root (par exemple, accès administrateur au cloud)
- Comptes partagés (par exemple, identifiants d'équipe)
- Comptes d'accès d'urgence (dits « break-glass »)

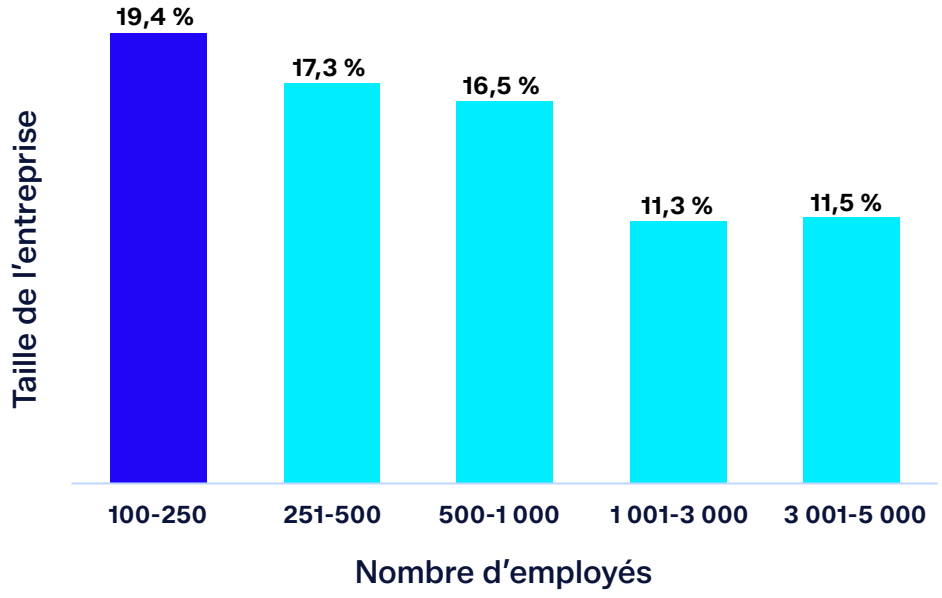
Chaque identité constitue un point d'entrée potentiel. Gérer les personnes et les éléments ayant accès à vos systèmes, et veiller à ce que ces accès soient appropriés et contrôlés, est l'une des mesures les plus importantes qu'une organisation puisse prendre pour garantir sa sécurité.

Capacité à détecter et à bloquer les attaques visant les identités

Sur les 3 545 répondants ayant subi au moins une violation liée à l'identité en 2025, 85,4 % ont réussi à détecter et à neutraliser l'attaque la plus grave avant que des dommages ne soient causés. Si ce taux montre que la majorité dispose d'une certaine capacité de détection, les 14,4 % qui n'ont pas pu empêcher l'attaque représentent un risque substantiel non négligeable et, comme le révèlent les conclusions suivantes, les conséquences pour ces organisations sont graves.

Échec de détection par taille de l'organisation

Les organisations de petite taille étaient nettement moins susceptibles de détecter les attaques. Parmi les plus petites entreprises interrogées (100 à 250 salariés), 19,4 % n'ont pas réussi à neutraliser l'attaque, soit près du double du taux observé chez les organisations comptant entre 1 001 et 3 000 salariés (11,3 %). Cet écart met en évidence les difficultés des petites entreprises en matière de ressources et de capacités.



S'agissant de l'attaque ciblant les identités la plus marquante vécue par votre organisation au cours des 12 derniers mois, avez-vous été en mesure de détecter et d'arrêter l'attaque avant qu'elle ne cause des dommages ? Base : l'organisation a été victime d'une violation de sécurité liée à l'identité. n = 3 545

Échec de détection par pays

Le Brésil (21,6 %) et la Suisse (21,1 %) ont enregistré les taux d'échec de détection les plus élevés. A contrario, c'est le Mexique (9,6 %) et le Royaume-Uni (7,1 %) qui ont obtenu les meilleurs résultats. Il convient de noter que le taux élevé de violations en Suisse, associé à un taux élevé d'échecs de détection, en fait un marché particulièrement vulnérable.

Pays	N'a pas été détecté
Brésil	**21,6 %**
Suisse	21,1 %
Japon	19,6 %
Espagne	18,1 %
Chili	18,0 %
Singapour	17,6 %
Allemagne	17,4 %
France	14,6 %
Italie	14,6 %
Australie	13,8 %
Colombie	13,8 %
États-Unis	12,8 %
EAU	11,8 %
Inde	11,2 %
Afrique du Sud	10,7 %
Mexique	9,8 %
Royaume-Uni	7,1 %

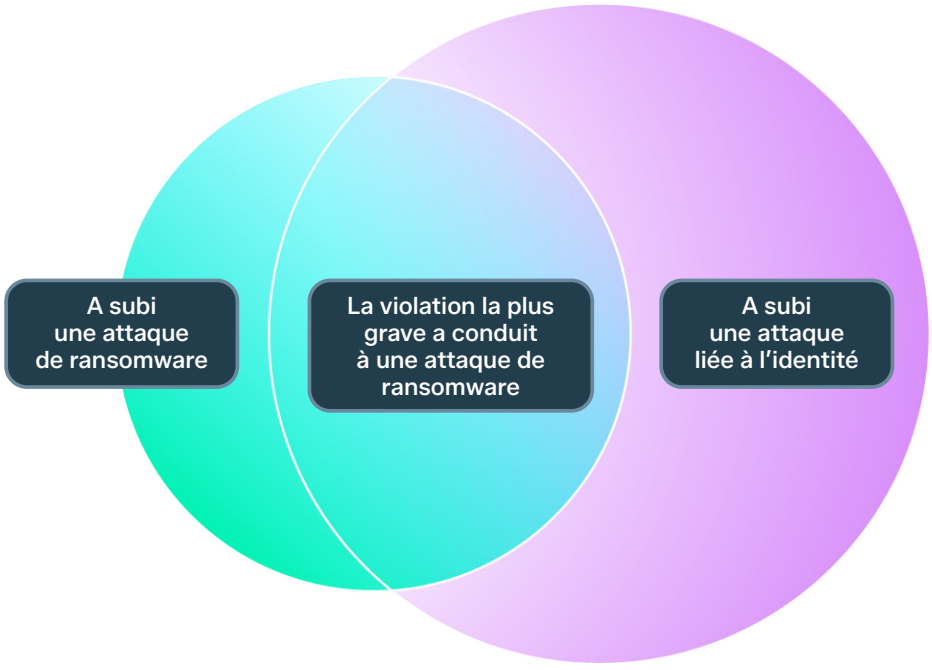
S'agissant de l'attaque ciblant les identités la plus marquante vécue par votre organisation au cours des 12 derniers mois, avez-vous été en mesure de détecter et d'arrêter l'attaque avant qu'elle ne cause des dommages ? Base : l'organisation a été victime d'une violation de sécurité liée à l'identité. n = 3 545

Échec de détection par secteur

Les secteurs des médias, des loisirs et du divertissement (22,4 %) ont affiché le taux d'échec de détection le plus élevé, suivi par l'industrie manufacturière (18,4 %) et les services financiers (17,9 %). Le secteur de la santé (8,1 %) a obtenu les meilleurs résultats en matière de détection, ce qui s'explique peut-être par la pression réglementaire incitant à investir dans la surveillance des menaces.

Le lien entre l'usurpation d'identité et les ransomwares

L'une des conclusions les plus frappantes de cette enquête est le lien direct qui existe entre les attaques liées à l'identité et les ransomwares. Parmi les organisations victimes d'un ransomware en 2025, les deux tiers (66,5 %) ont confirmé que cet incident correspondait à leur attaque liée à l'identité la plus grave. Même si toutes les attaques n'ont pas donné lieu à un chiffrement des données, ce constat montre que le vol d'identité est l'un des principaux mécanismes utilisés pour propager les ransomwares.



Au cours de l'année passée, votre organisation a-t-elle été touchée par un ransomware ? (n=5 000) Votre organisation a-t-elle subi des violations de sécurité liées à l'identité au cours des 12 derniers mois ? Si oui, combien ? (n = 5 000) [Si vous avez répondu oui aux deux questions] Cet incident lié à un ransomware correspondait-il à votre attaque basée sur l'identité la plus grave ?

Lien entre les ransomwares et les attaques liées à l'identité, par taille d'organisation

Le lien entre les attaques liées à l'identité et les ransomwares était le plus marqué dans les organisations comptant entre 1 001 et 3 000 employés (71,6 %) et le plus faible parmi celles comptant entre 100 et 250 employés (62,4 %). Cette variation peut s'expliquer par des différences de complexité des infrastructures, de niveau de visibilité ou de capacité à établir un lien entre le vecteur d'attaque et l'impact sur la cible au sein des segments.

Taille de l'organisation	Ransomware = Attaque basée sur l'identité
100-250 employés	62,4 %
251-500 employés	68,2 %
501-1 000 employés	62,5 %
1 001 à 3 000 employés	**71,6 %**
3 001-5 000 employés	64,6 %

Au cours de l'année passée, votre organisation a-t-elle été touchée par un ransomware ? (n=5 000) Votre organisation a-t-elle subi des violations de sécurité liées à l'identité au cours des 12 derniers mois ? Si oui, combien ? (n = 5 000) [Si vous avez répondu oui aux deux questions] Cet incident lié à un ransomware correspondait-il à votre attaque basée sur l'identité la plus grave ?

Tendances par secteur

C'est dans l'enseignement supérieur (76,8 %) et la distribution/les transports (75,0 %) que le lien entre les ransomwares et les violations liées à l'identité était le plus fort. À l'inverse ce lien était moins marqué dans les services financiers (57,6 %) et dans les secteurs de l'informatique, des technologies et des télécommunications (61,1 %) (même s'il restait bien supérieur au seuil de la majorité).

Conséquences des violations liées à l'identité non détectées

Pour les 510 organisations qui n'ont pas pu empêcher leur attaque basée sur l'identité la plus grave, les conséquences ont été lourdes et multiples, les victimes ayant signalé en moyenne deux répercussions liées à cet incident.

Conséquence	% d'organisations victimes d'une violation
Vol de données : les attaquants ont volé des données sensibles	**48,8 %**
Ransomware : des identifiants volés ont été utilisés pour exécuter l'attaque de ransomware	48,4 %
Extorsion : les attaquants ont réclamé de l'argent en menaçant l'organisation	43,9 %
Sabotage : les attaquants ont utilisé des identifiants pour nuire à l'organisation	30,0 %
Vol financier : paiements détournés	28,0 %
Vol financier : vol d'argent sur des comptes	25,5 %
Résumé : Vol financier (toute forme)	**46,7 %**

Quelles ont été les conséquences de cette violation liée à l'identité pour votre organisation ? Base : l'organisation n'a pas pu empêcher la violation de sécurité. n = 510.

Près de la moitié des organisations victimes d'une violation ont fait l'objet d'un vol de données (48,8 %) et une proportion presque identique a subi une attaque de ransomware (48,4 %). Près de la moitié (46,7 %) ont été victimes d'une forme ou d'une autre de vol financier direct (paiement détourné, vol de fonds, ou les deux). Si l'on ajoute à cela les cas d'extorsion (43,9 %), ces résultats montrent que les attaques visant l'identité qui ne sont pas détectées à temps ont presque toujours de graves conséquences.

Pourquoi les organisations sont victimes

Il est essentiel de comprendre pourquoi les attaques aboutissent pour pouvoir les prévenir. L'enquête a identifié les défaillances humaines, opérationnelles et techniques qui ont conduit les organisations à être victimes d'attaques liées à l'identité. Ses conclusions montrent également qu'il y a rarement une seule raison, les personnes interrogées citant en moyenne deux causes premières ayant contribué à l'incident.

Cause racine	% d'organisations victimes d'une violation
Erreur humaine : un employé a été piégé et a transmis ses identifiants	**42,7 %**
Gestion insuffisante des identités non humaines (par exemple, des clés API stockées dans le code, des identifiants statiques, des comptes de service orphelins qui reliaient auparavant des applications aux systèmes, etc.)	40,6 %
Gestion insuffisante des identités des employés	38,6 %
Manque de visibilité sur les accès et les autorisations accordés aux applications externes	35,7 %
Gestion insuffisante des identités des fournisseurs et des sous-traitants	31,4 %
Manque de contrôle sur les accès et les autorisations accordées aux applications externes	30,8 %
Employé malveillant : un employé a délibérément facilité l'attaque	26,7 %
Résumé : Gestion insuffisante des identités humaines (toute forme)	**60,2 %**
Résumé : Problèmes liés à des accès et autorisations accordées à des applications externes (toute forme)	**56,1 %**

Pourquoi votre organisation a-t-elle été victime d'une attaque liée à l'identité ? Sélectionnez toutes les réponses appropriées. Base : l'organisation n'a pas pu empêcher la violation de sécurité. n = 510.

L'erreur humaine a été la principale cause des violations d'identité, citée par 42,7 % des victimes. En deuxième position figure la gestion insuffisante des identités non humaines (40,6 %), ce qui est particulièrement préoccupant, car cela concerne aussi bien les clés API stockées dans le code, les identifiants statiques que les comptes de service orphelins, qui sont plus difficiles à auditer et à surveiller.

Des actes malveillants commis par des initiés, dans lesquels des employés ont délibérément facilité l'attaque, ont été signalés dans plus d'un quart (26,7 %) des attaques, ce qui révèle combien il est important de maintenir des contrôles internes rigoureux et une vigilance constante.

Dans l'ensemble, la gestion insuffisante des identités humaines (60,2 %) est la raison la plus fréquente pour laquelle les organisations ont été victimes d'attaques basées sur l'identité, tandis que les problèmes liés aux accès et aux autorisations accordés aux applications externes ont joué un rôle dans 56,1 % des incidents.

59,5 %

L'authentification multifacteur MFA, qui existe depuis plusieurs décennies, n'était pas disponible sur le système ciblé dans 59,5 % des dossiers MDR analysés dans le cadre du rapport Sophos 2025 Active Adversary.

Information Sophos X-Ops

Tendances par taille d'organisation

Les grandes organisations rencontrent davantage de difficultés que les petites dans plusieurs domaines liés à la protection des identités, ce qui s'explique sans doute par la taille et la complexité accrues des environnements qu'elles doivent surveiller et sécuriser.

Plus de la moitié (55,6 %) des entreprises comptant entre 1 001 et 3 000 salariés ont cité l'erreur humaine comme cause principale, contre seulement 29,0 % de celles comptant entre 251 et 500 salariés. De même, 68,6 % des organisations comptant entre 3 001 et 5 000 employés ont déclaré qu'une gestion insuffisante des identités avait contribué à leur vulnérabilité, contre 58,5 % de celles comptant entre 100 et 250 employés.

Les identités non humaines en bref

Une identité non humaine (NHI) est un identifiant numérique attribué à un logiciel, un système ou un processus automatisé qui lui permet d'accéder à des ressources sans intervention humaine. Au lieu de mots de passe, les NHI utilisent des codes d'accès non humains pour prouver leur identité, notamment :

- Clés API connectant les applications
- Comptes de service exécutant des sauvegardes
- Jetons OAuth pour les intégrations SaaS
- Agents d'IA accédant à des bases de données

Les identifiants NHI peuvent être volés et utilisés à mauvais escient de la même manière que les codes d'accès de connexion d'un utilisateur. Cela pose d'autant plus de problèmes lorsque les organisations ne procèdent pas régulièrement à des audits des autorisations NHI, lesquelles sont très souvent étendues et importantes.

Les NHI sont nettement plus nombreuses que les identités humaines, certaines organisations faisant état de ratios supérieurs à 100 pour 1. L'IA agentique est l'un des principaux facteurs à l'origine de cette augmentation du ratio ces dernières années.

96 %

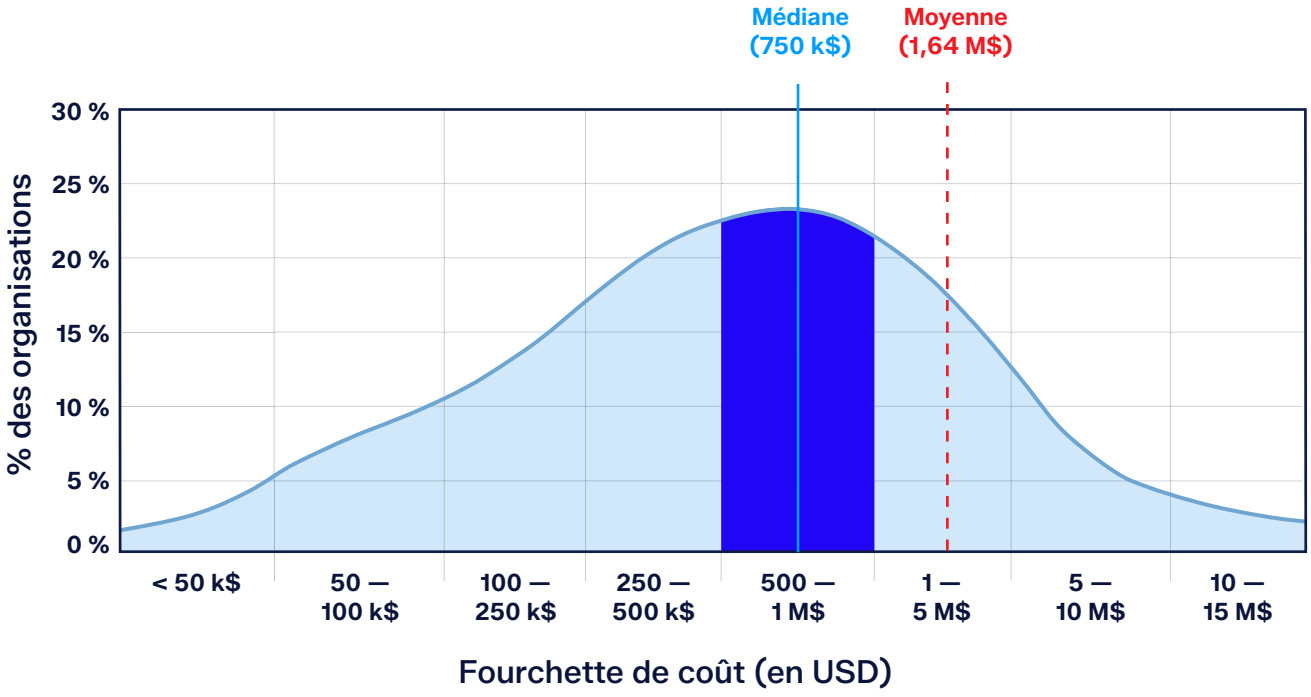
des environnements clients Sophos ITDR comportent des applications multi-locataires. Identifier et contrôler les identités non humaines impliquées dans ces relations peut s'avérer difficile.

Information Sophos X-Ops

Le coût financier des violations d'identité

Les organisations ayant été victimes d'une violation d'identité ont fait état de coûts de remédiation considérables. Le coût moyen global de rétablissement s'élevait à 1 637 363 dollars, et la médiane à 750 000 dollars. 73 % des organisations victimes d'une violation ont estimé leurs coûts à 250 000 dollars ou plus, et près d'un quart (23,7 %) se situaient dans la fourchette comprise entre 500 000 et 1 million de dollars.

Distribution des coûts



À combien estimez-vous le coût total que devra supporter votre organisation pour remédier à cette violation liée aux identités ? Base : l'organisation n'a pas pu empêcher la violation de sécurité. n = 510.

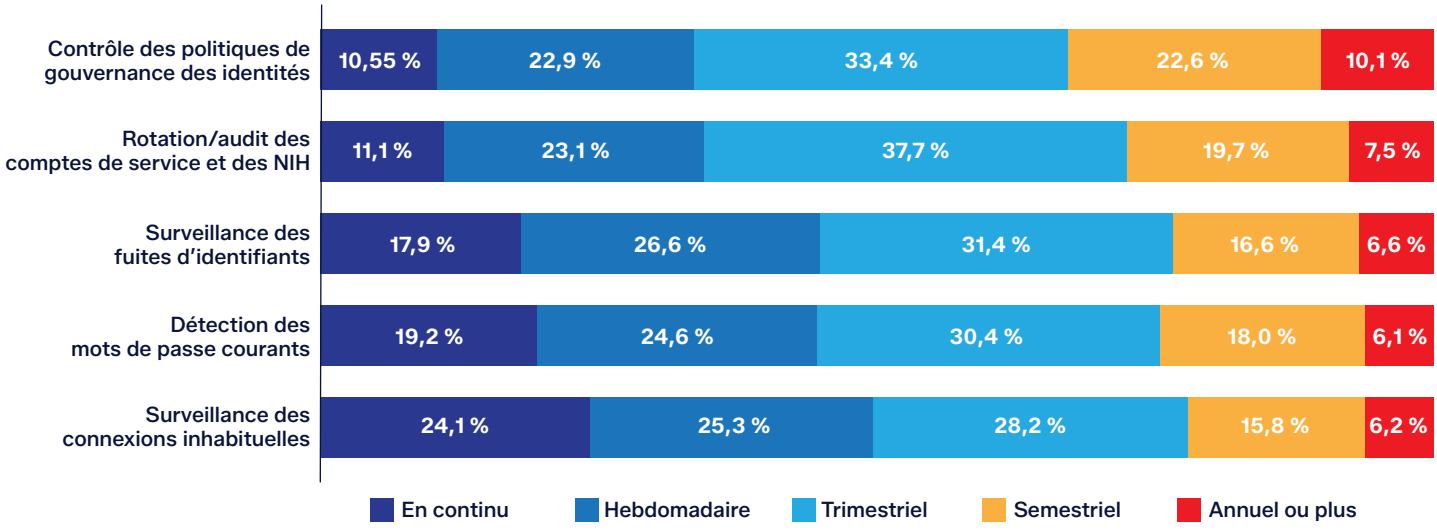
Coûts en fonction de la taille de l'organisation

Taille de l'organisation	Coût moyen	Coût médian
100-250 employés	1 125 562 $	375 000 $
251-500 employés	1 978 043 $	750 000 $
501-1 000 employés	1 009 205 $	375 000 $
1 001 à 3 000 employés	1 907 594 $	750 000 $
3 001-5 000 employés	2 452 929 $	750 000 $

À combien estimez-vous le coût total que devra supporter votre organisation pour remédier à cette violation liée aux identités ? Base : l'organisation n'a pas pu empêcher la violation de sécurité. n = 510.

Hygiène de la sécurité des identités

L'enquête a porté sur cinq activités fondamentales de gestion des identités et sur la fréquence à laquelle les organisations les mettent en œuvre. Les résultats révèlent des écarts importants entre les bonnes pratiques et la réalité du terrain — des écarts qui accroissent l'exposition aux attaques basées sur l'identité.



À quelle fréquence votre organisation mène-t-elle les activités suivantes en matière de gestion des identités ? n = 5 000

La surveillance des tentatives de connexion inhabituelles est l'activité la plus couramment menée en temps réel (24,1 % en continu). Pour autant, plus de la moitié des organisations (50,6 %) ne procèdent à ces vérifications que tous les trois mois au maximum. En ce qui concerne la rotation ou l'audit des identités non humaines, une activité essentielle dans la mesure où il s'agit de la deuxième cause première de violations, seuls 34,3 % des entreprises procèdent à ces opérations au moins une fois par semaine.

La révision des politiques de gouvernance des identités est l'activité la moins fréquemment menée de manière continue (10,5 %), un tiers des organisations (33,3 %) ne révisant leurs politiques qu'au maximum une fois par trimestre et 22,6 % seulement tous les semestres. Compte tenu de l'évolution rapide des menaces liées à l'identité, les bilans annuels, semestriels, voire trimestriels, créent de dangereuses lacunes.

IA agentique : aggravation de la problématique NHI

L'IA agentique a considérablement compliqué la gestion des NHI : les identités sont toujours plus nombreuses, créées plus rapidement, bénéficient d'un accès plus large et font l'objet d'une surveillance humaine bien moindre. Parmi les principaux défis liés aux NHI, on peut citer :

- **Les agents d'IA multiplient automatiquement les NHI**
  Chaque agent d'IA requiert sa propre identité et ses propres identifiants. Surtout, les agents peuvent créer de manière autonome de nouveaux agents pour accomplir des sous-tâches, chacun d'entre eux générant davantage d'identifiants sans aucune intervention ni supervision humaine.
- **Les agents d'IA nécessitent un accès étendu et permanent**
  Pour accomplir leur travail, les agents d'IA doivent pouvoir accéder à de nombreux systèmes : calendriers, bases de données, CRM, référentiels de fichiers et API. Contrairement aux comptes utilisateur, ces droits d'accès expirent rarement et font rarement l'objet d'un contrôle.
- **Les agents d'IA sont plus difficiles à surveiller que les NHI traditionnelles**
  Un compte de service de sauvegarde exécute la même tâche à la même heure chaque nuit, ce qui facilite son suivi. Les agents d'IA, pour leur part, prennent des décisions de manière autonome, agissent de façon imprévisible et fonctionnent 24 h/24 et 7 j/7, ce qui complique fortement l'identification d'éventuelles compromissions.
- **Les agents d'IA tiers comportent des risques inconnus**
  Les études montrent que lorsque les organisations ont recours à des capacités d'agents d'IA tiers, elles héritent de l'ensemble des identifiants et des autorisations d'accès dont disposent ces agents, tout en ayant une visibilité limitée sur leur niveau de sécurité ou sur les ressources auxquelles ils ont accès.
- **Les règles de sécurité n'ont pas été conçues pour les agents d'IA**
  La plupart des systèmes de sécurité des identités ont été conçus pour des utilisateurs humains et des comptes machine simples. Ils ne prennent pas en compte les agents capables de créer, de déléguer et de supprimer leurs propres identifiants de manière autonome au cours d'un workflow, ce qui entraîne une lacune importante en matière de gouvernance.

L'IA agentique est l'une des principales raisons pour lesquelles la sécurité des NHI est désormais une priorité absolue pour les RSSI.

Conséquences d'une gestion inadéquate des identités non humaines

Comme nous l'avons déjà indiqué, une gestion défaillante des identités non humaines (NHI) était à l'origine de 40,6 % des attaques ayant abouti. Par ailleurs, les données montrent que la compromission des NHI aggrave considérablement les répercussions financières d'une violation.

Particulièrement, les organisations ayant une gestion inadéquate des NHI sont nettement plus exposées aux vols financiers (lorsque des adversaires détournent des paiements de comptes), avec un taux supérieur de 27,9 % à la moyenne, et aux extorsions (lorsque des attaquants ont recours à des menaces pour obtenir de l'argent), avec un taux supérieur de 24,4 % à la moyenne. Les seules catégories dans lesquelles les organisations ayant une gestion inefficace des NHI ont obtenu des résultats légèrement supérieurs à la moyenne sont celles du vol de données et des ransomwares, même si ces écarts sont minimes.

Conséquence	% de l'ensemble des organisations victimes d'une violation	% d'organisations victimes d'une violation dont la gestion des ressources non humaines est défaillante	Variation en % en cas de gestion insuffisante des NHI
Vol de données : les attaquants ont volé des données sensibles	48,8 %	47,8 %	-2,1 %
Ransomware : des identifiants volés ont été utilisés pour exécuter l'attaque de ransomware	48,4 %	46,4 %	-4,1 %
Extorsion : les attaquants ont réclamé de l'argent en menaçant l'organisation	43,9 %	**54,6 %**	**+24,4 %**
Sabotage : les attaquants ont utilisé des identifiants pour nuire à l'organisation	30,0 %	33,8 %	+12,7 %
Vol financier : paiements détournés	28,0 %	**35,8 %**	**+27,9 %**
Vol financier : vol d'argent sur des comptes	25,5 %	29,9 %	+15,7
Résumé : Vol financier (toute forme)	**46,7 %**	**57,0 %**	**+22 %**

Quelles ont été les conséquences de cette violation liée à l'identité pour votre organisation ? Base : l'organisation n'a pas pu empêcher la violation de sécurité. n = 510 (toutes les violations), n = 207 (violations impliquant des NHI)

Compte tenu de l'impact financier accru lié à la faiblesse des NHI, il n'est guère surprenant que les organisations dont les NHI sont mal administrés déclarent des coûts globaux de rétablissement après une violation d'identité nettement plus élevés, la facture typique s'élevant à près de 150 000 dollars de plus que la moyenne.

Coût moyen de rétablissement après une violation d'identité

Il existe une corrélation évidente entre une mauvaise hygiène de sécurité des NHI et la probabilité de subir une violation basée sur les NHI. Si un tiers (34 %) de l'ensemble des organisations effectue une rotation ou un audit des comptes de service et des NHI en continu ou chaque semaine, cette proportion tombe à un quart (24 %) parmi celles dont la violation était due à des NHI compromis.

Conclusion

Les résultats de cette enquête appellent à redoubler de vigilance. Au cours de l'année écoulée, plus de 7 organisations sur 10 ont été victimes de violations liées à l'identité, avec une moyenne de plus de trois incidents par entreprise concernée. Il ne s'agit pas d'un risque théorique ni d'un problème limité à certains secteurs ou à certains pays. Il s'agit d'une menace universelle et omniprésente qui touche les organisations de toutes tailles, de tous secteurs et de tous pays. Les données démontrent que les attaques ciblant les identités ouvrent la voie aux ransomwares, aux vols de données et aux tentatives d'extorsion : 67 % des victimes de ransomware ont attribué cet incident directement à une compromission de leur identité.

Lorsque les attaques visant l'identité aboutissent, leurs répercussions sont graves et multidimensionnelles. Près de la moitié des organisations victimes d'une violation ont subi un vol de données ou une attaque de ransomware, et le coût moyen de la remédiation, qui s'élève à 1,64 million de dollars, fait de chaque incident un événement financier majeur.

Les causes premières révèlent des faiblesses systémiques : l'erreur humaine (42,7 %), une gestion inadéquate des identités non humaines (40,6 %) et une visibilité insuffisante sur les autorisations des applications tierces (35,7 %) sont autant de problèmes qui peuvent être résolus, mais uniquement moyennant des investissements et une attention soutenus. Le fait que les petites organisations aient près de deux fois plus de chances de ne pas détecter les attaques que les grandes met en évidence une fracture en matière de cybersécurité qui mérite toute l'attention de la communauté de la cybersécurité.

Mais le plus préoccupant est peut-être l'état des pratiques d'hygiène en matière de sécurité des identités. Seul environ un quart des organisations surveillent en continu les activités de connexion inhabituelles, et moins d'une sur trois effectuent régulièrement une rotation des identifiants non humains — précisément les failles que les attaquants vont chercher à exploiter.

Les organisations doivent prendre conscience que la sécurité des identités doit moins être envisagée comme un effort ponctuel que comme une discipline opérationnelle continue. Les organisations qui adopteront cette approche seront en bien meilleure posture pour se défendre contre les menaces qui ont marqué l'année 2025 et qui ne manqueront pas de prendre de l'ampleur en 2026 et au-delà.

Recommandations

Comme l'a montré l'enquête, une sécurité solide des identités est un élément essentiel d'une stratégie efficace de réduction des cyber-risques. Afin d'être moins vulnérables face aux attaques basées sur l'identité, les organisations devraient s'efforcer de mettre en place un système de défense à plusieurs niveaux pour les identités humaines et non humaines. Commencez par les mesures essentielles, puis évoluez progressivement vers des actions recommandées dans le cadre d'un programme d'amélioration continue.

Étapes essentielles

Identités humaines

- Appliquez l'authentification multifacteur (MFA) pour tous les comptes utilisateur.
- Utilisez des identifiants distincts pour les opérations privilégiées et non privilégiées.
- Implémentez le verrouillage du compte et la protection par force brute.
- Centralisez la gestion des identités avec l'authentification unique (SSO).
- Assurez-vous que votre formation de sensibilisation des utilisateurs reflète les dernières techniques de phishing et de vol d'identifiants.

Identités non humaines

- Répertoriez et classez périodiquement de toutes les identités non humaines.
- Utilisez des identifiants de courte durée plutôt que des clés secrètes de longue durée.

Identités humaines et non humaines

- Appliquez l'accès avec le moindre privilège.
- Sécurisez et gérez les identifiants correctement.
- Désactivez ou supprimez rapidement les identités inactives.
- Appliquez un processus d'onboarding formel qui audite et révoque l'accès aux ressources de l'entreprise.
- Journalisez et surveillez toutes les activités d'authentification, et conservez les journaux pendant au moins 30 jours.

Étapes recommandées

Identités humaines

- Implémentez des politiques d'accès conditionnel et basées sur les risques.
- Déployez des clés d'accès (matérielles ou logicielles) comme méthode d'authentification principale.
- Fédérez les identités en utilisant des protocoles d'identité largement reconnus, tels que Security Assertion Markup Language (SAML) ou le plus récent OpenID Connect (OIDC).

Identités non humaines

- Utilisez la fédération d'identités de charges de travail plutôt que des clés secrètes statiques.
- Adoptez une plateforme de gestion des clés secrètes pour gérer les NHI à grande échelle.
- Activez le contrôle des clés secrètes dans les plateformes prises en charge (GitHub, GitLab).

Identités humaines et non humaines

- Déployez une solution de gestion des accès privilégiés (PAM).
- Adoptez un modèle de sécurité Zero Trust.
- Procédez à des contrôles périodiques des droits d'accès et à la re-certification des droits.
- Déployez des capacités de détection et de réponse aux menaces liées aux identités (ITDR).
- Segmentez l'accès au réseau par identité et par rôle.
- Définissez et testez un ou plusieurs manuels de réponse aux incidents liés à l'identité, destinés à traiter les incidents de ce type, tels que ceux décrits dans le présent rapport.

En savoir plus

Consultez notre guide des bonnes pratiques en matière de sécurité des identités

Méthodologie

Cette enquête a été réalisée par Vanson Bourne pour le compte de Sophos au premier trimestre 2026. 5 000 responsables informatiques et de la cybersécurité ont été interrogés dans 17 pays : Afrique du Sud, Allemagne, Australie, Brésil, Chili, Colombie, Espagne, Émirats arabes unis, États-Unis, France, Italie, Inde, Japon, Mexique, Singapour, Suisse, et Royaume-Uni. Les répondants provenaient d'organisations comptant entre 100 et 5 000 employés, réparties dans 15 secteurs d'activité.

SOPHOS

Pour discuter de vos besoins en matière de sécurité des identités et découvrir comment Sophos peut vous aider, rendez-vous sur notre site Web ou contactez l'un de nos conseillers.

Sophos France
Tél. : 01 34 34 80 00
Email : info@sophos.fr

2026-05-08 FR (TA) CRE-5312