Baromètre des fuites de données personnelles

ÉDITION 2025

Ce baromètre est élaboré par le Forum INCYBER en partenariat avec Hexatrust et avec la participation de la CNIL pour les données en *open data*.

IN CYBER FORUM EUROPE

HEXATRUST
CLOUD CONFIDENCE & CYBERSECURITY

CNIL.
COMMISSION NATIONALE INFORMATIQUE & LIBERTÉS

édito

Chaque jour en France, 16 fuites de données sont déclarées à la CNIL. En 2024, leur nombre a explosé, atteignant 5 919 notifications, soit une hausse de 29 % par rapport à 2023 (4 564 notifications). Ce chiffre illustre une réalité alarmante : la cybercriminalité ne cesse de gagner du terrain, mettant en péril les données sensibles des entreprises, des collectivités et des citoyens. Face à cette menace, il est urgent d'adopter des stratégies de protection renforcées.

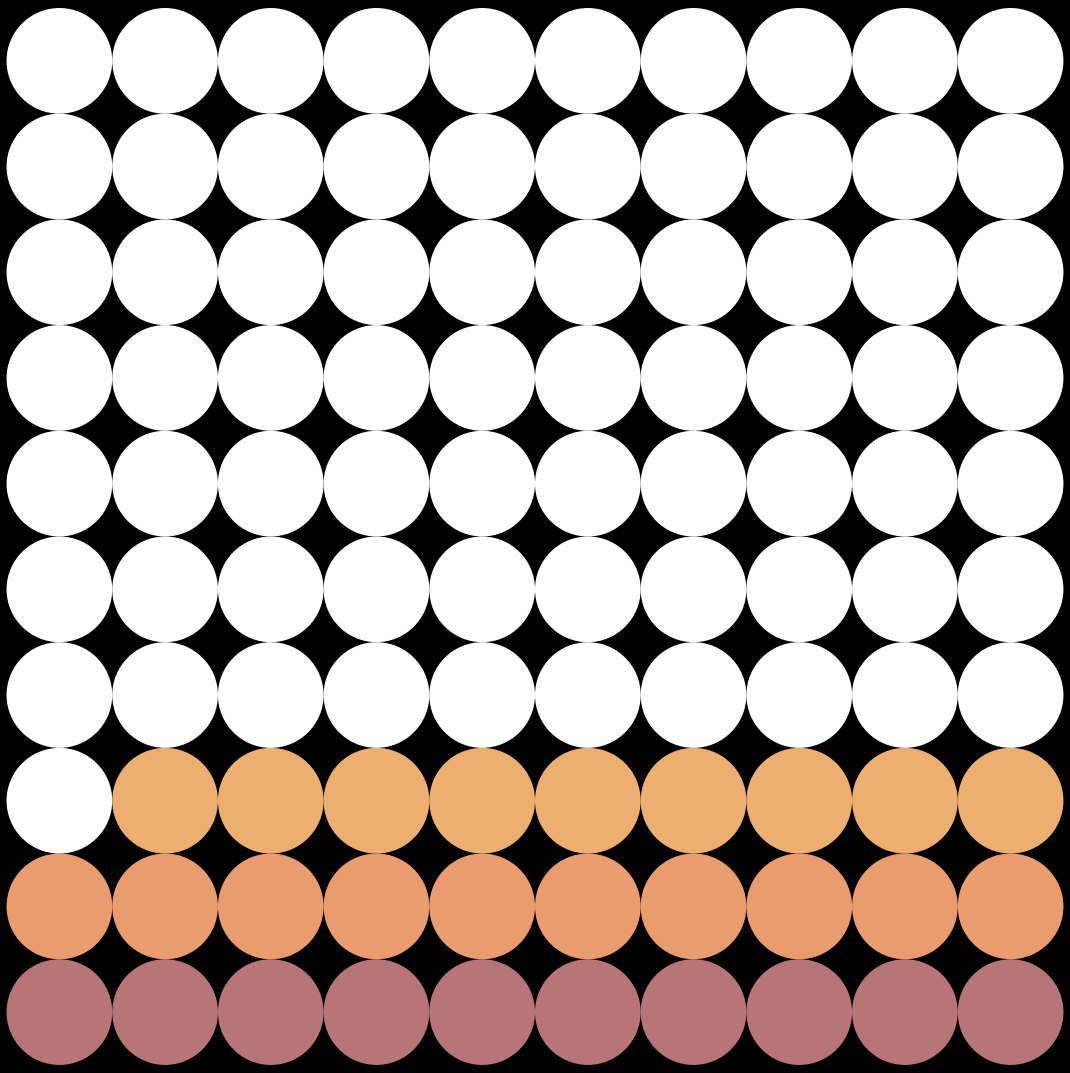
Parmi ces stratégies, le modèle *Zero Trust* s'impose comme une réponse incontournable. Fondé sur le principe du « Ne jamais faire confiance, toujours vérifier », il repose sur une surveillance continue des accès, une authentification forte, la micro-segmentation des réseaux et le chiffrement systématique des données. En appliquant ces principes, les entreprises peuvent réduire considérablement les risques de compromission et empêcher l'exfiltration de données sensibles.

Les entreprises d'Hexatrust, acteur majeur de la cybersécurité en France, proposent aujourd'hui une offre complète de solutions *Zero Trust* couvrant l'ensemble des besoins : gestion des identités (IAM, MFA), protection des données (DLP, chiffrement), sécurisation des accès (ZTNA), détection des menaces (XDR, SIEM) et protection des infrastructures (micro-segmentation, CASB). Ces technologies permettent non seulement de prévenir les intrusions, mais aussi de détecter et bloquer les attaques.

Dans un contexte où les attaques se professionnalisent et se multiplient, le *Zero Trust* n'est plus une option, mais une nécessité. Il est temps pour les organisations de prendre conscience de l'ampleur du risque et d'investir dans des solutions robustes. L'avenir de la cybersécurité se joue aujourd'hui, et il repose sur une approche où chaque accès est contrôlé, chaque donnée est protégée et chaque anomalie est traquée en temps réel.

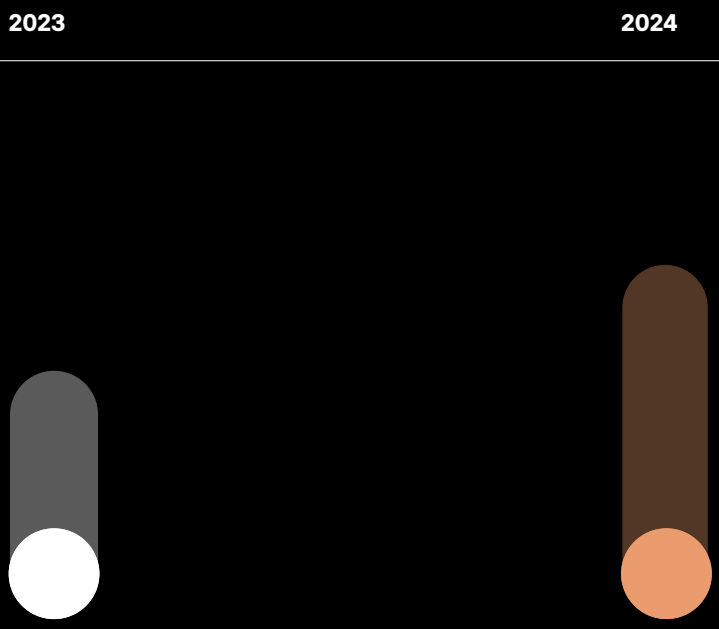
Jean-Noël de Galzain
Président d'Hexatrust

Chaque jour en France, 16 fuites de données sont déclarées à la CNIL



En 2024, leur nombre a explosé, atteignant 5 919 notifications, soit une hausse de 29 % par rapport à 2023

Des fuites de données en augmentation de 29 %

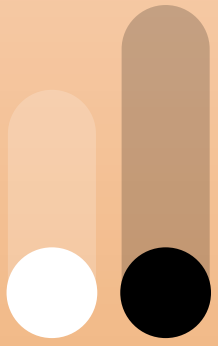


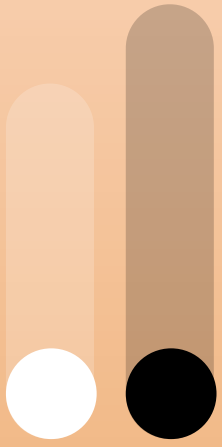
Avec 5 919 notifications en 2024, soit 16 fuites de données par jour, le nombre de fuites de données déclarées à la CNIL est en augmentation de 29 % par rapport à 2023 (4 564 notifications). Cette augmentation est imputable à la fois à une recrudescence des menaces informatiques, à la croissance de notre surface d'exposition aux risques mais également à une meilleure sensibilisation des entreprises face aux obligations qui leur incombent en matière de protection des données personnelles (34 440 DPO référencés auprès de la CNIL en 2024 contre 32 000 en 2023).

Les fuites d’origine malveillantes en progression

Si les fuites de nature accidentelle (envoi de données personnelles à un mauvais destinataire, publication involontaire de données) progressent (+ 11%), c’est surtout le nombre de fuites d’origine malveillante qui explose (+ 25%). L’origine des fuites est également de plus en plus externe (+30%).

2023	2024





1 158
FUITES D’ORIGINE ACCIDENTELLE

1 284 **+11%**
FUITES D’ORIGINE ACCIDENTELLE

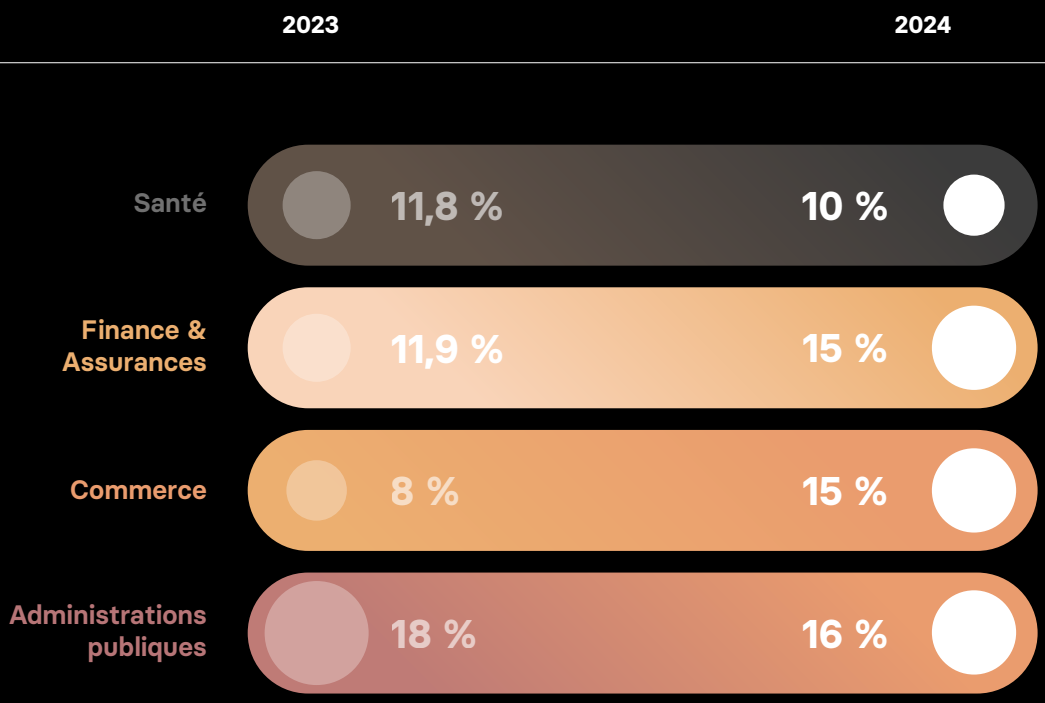
2 911
FUITES D’ORIGINE MALVEILLANTE

3 649 **+29%**
FUITES D’ORIGINE MALVEILLANTE

Les actes d’origine externe en forte progression

Sur le total des fuites, 3 730 ont pour origine des acteurs externes en 2024 (contre 2 857 en 2023), ce qui représente une augmentation de 30 %. Les 1 456 actes d’origine interne enregistrés (contre 1 212 en 2023) sont majoritairement de nature accidentelle (1 284 contre 224 malveillants). La proportion est inverse pour les actes d’origine externe qui sont dans leur grande majorité malveillants (3 441 contre 225 d’origine accidentelle).

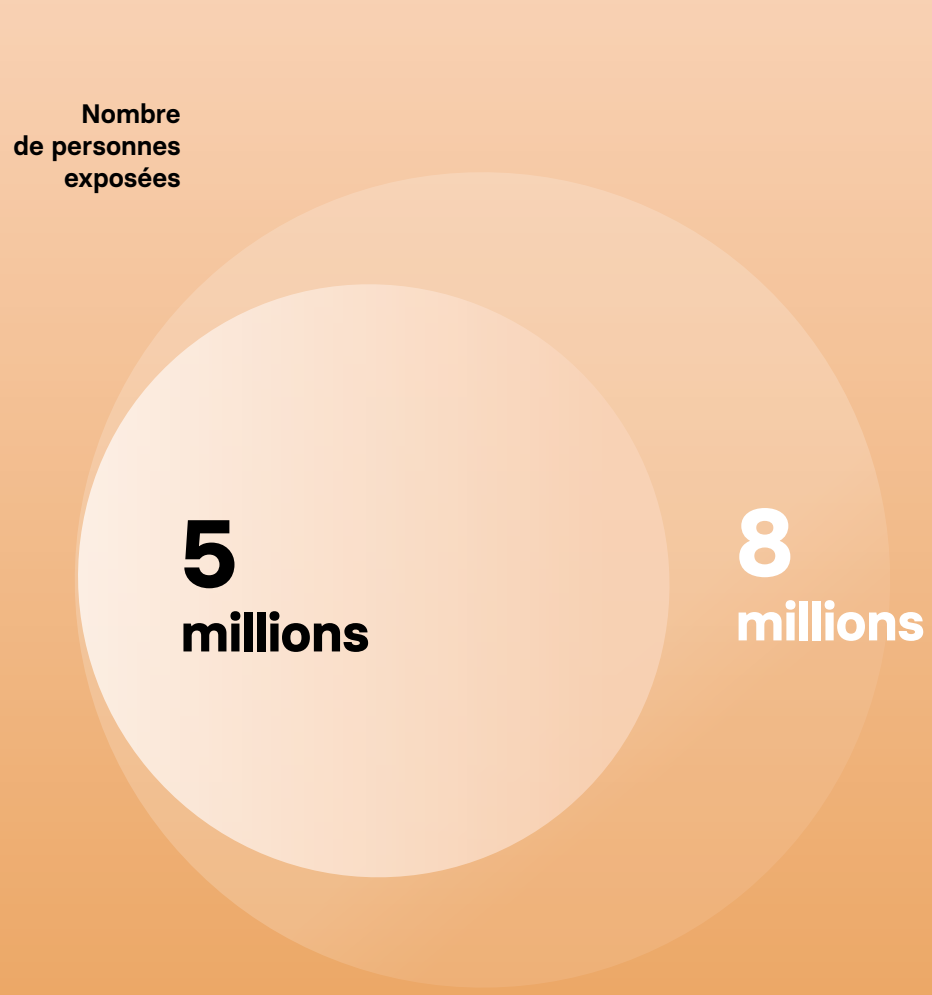
Les administrations et le commerce en tête des secteurs touchés



Les fuites touchant le secteur du commerce ont plus que doublé en 2024, passant de 354 notifications à 915, soit 15 % des notifications totales (en progression de 7 %. Cette forte augmentation est due aux nombreuses attaques ayant visé des acteurs du commerce de détail et de la distribution spécialisée, soit directement, soit par le biais des systèmes de gestion des commandes et des stocks (OMS, WMS). En tête, le secteur des administrations publiques recule légèrement passant de 18 à 16 % des notifications totales, tandis que le secteur financier et assurantiel passe de 11,9 à 15 % du total. Le domaine de la santé reste enfin très affecté par les fuites, même si leur proportion sur le total est en légère diminution (passant de 11,8 à 10 %).

Un impact en forte progression

Les 5 919 fuites ont potentiellement exposé les données de 8 millions de Français, contre 5 millions en 2023, ce qui reflète le caractère très massif de certaines fuites de données.



En plus du préjudice financier et réputationnel subi par les organisations victimes, les individus dont les données ont fuité sont également exposés à des risques de fraude ou d'usurpation d'identité. La fuite de données sensibles, comme les données concernant la santé ou révélant l'origine raciale ou ethnique, est particulièrement dangereuse. 20 % des notifications (pourcentage identique en 2023) concernent ainsi des données sensibles.

Selon l’article 9 du RGPD,

les données sensibles sont des catégories particulières de données personnelles qui révèlent :

- → **L’origine raciale ou ethnique**
- → **Les opinions politiques**
- → **Les convictions religieuses ou philosophiques**
- → **L’appartenance syndicale**
- → **Les données génétiques**
- → **Les données biométriques** (visage, empreintes digitales) utilisées pour identifier une personne
- → **Les données de santé**
- → **Les données concernant la vie sexuelle ou l’orientation sexuelle d’une personne**

Ces données sont **particulièrement protégées** et leur traitement est interdit, sauf exceptions bien encadrées (ex. consentement explicite, nécessité pour la santé publique, obligations légales, etc.).

Le modèle *Zero Trust* : un rempart contre les fuites de données

Le modèle ***Zero Trust*** repose sur un principe fondamental : ***« Ne jamais faire confiance, toujours vérifier ».*** Contrairement aux approches traditionnelles de cybersécurité, qui considèrent le réseau interne comme fiable, le ***Zero Trust*** **suppose que toute connexion peut être compromise,** qu'elle soit interne ou externe.

Dans le contexte des **fuites de données,** les technologies *Zero Trust* permettent de **réduire les risques de compromission, d'empêcher les déplacements latéraux des attaquants et de limiter l'exfiltration des données.**

1. Les principes du *Zero Trust* pour lutter contre les fuites de données

VÉRIFICATION SYSTÉMATIQUE DES IDENTITÉS ET DES ACCÈS (IAM & MFA)

→ Chaque utilisateur, appareil et application doit être authentifié en permanence (via MFA, biométrie, certificats, etc.).

AVANTAGE : Empêche les attaques par usurpation d'identité (*phishing*, vol de mots de passe).

PRINCIPE DU MOINDRE PRIVILÈGE *(LEAST PRIVILEGE ACCESS)*

→ Les utilisateurs et applications n'ont accès qu'aux données strictement nécessaires.

AVANTAGE : Réduit le risque qu'un attaquant utilise un compte compromis pour exfiltrer des données sensibles.

MICRO-SEGMENTATION DU RÉSEAU

→ Les accès sont isolés : un utilisateur ou un service compromis ne peut pas se déplacer librement dans le système.

AVANTAGE : Stoppe la propagation des *ransomwares* et empêche un attaquant de voler un grand volume de données.

SURVEILLANCE ET DÉTECTION CONTINUE DES MENACES (SIEM, UEBA, XDR)

→ Les systèmes *Zero Trust* utilisent l'analyse comportementale pour détecter les activités anormales (exfiltration massive de données, connexion suspecte, etc.).

AVANTAGE : Détection précoce des fuites en cours et réaction automatique en cas de comportement anormal.

CHIFFREMENT DES DONNÉES PARTOUT

→ Les technologies *Zero Trust* chiffrent les données en transit et au repos, ce qui rend leur vol inutile.

AVANTAGE : Même en cas de fuite, les attaquants ne peuvent pas exploiter les données sans la clé de déchiffrement.

CONTRÔLE STRICT DES APPLICATIONS ET SERVICES *CLOUD* (CASB ET ZTNA)

→ Surveillance des accès aux SaaS et *Cloud* tiers pour éviter les fuites accidentelles.

AVANTAGE : Empêche les fuites via des services non approuvés (ex. un employé qui télécharge des fichiers confidentiels sur Google Drive).

2. Les technologies *Zero Trust* contre les fuites de données

1. IAM *(IDENTITY & ACCESS MANAGEMENT)* ET MFA *(MULTI-FACTOR AUTHENTICATION)*

OBJECTIF : Sécuriser l'accès aux systèmes avec une vérification rigoureuse des identités.

IMPACT : Réduit les risques de vol de comptes et d'accès non autorisé.

2. ZTNA *(ZERO TRUST NETWORK ACCESS)*

OBJECTIF : Remplace le VPN traditionnel par un accès sécurisé au cas par cas aux applications.

IMPACT : Empêche un attaquant d'exploiter un accès VPN pour se déplacer dans le réseau.

3. DLP *(DATA LOSS PREVENTION)*

OBJECTIF : Surveiller, bloquer et chiffrer tout transfert anormal de données (ex. copie vers une clé USB, envoi par e-mail).

IMPACT : Stoppe les exfiltrations massives de données.

4. SIEM ET UEBA *(USER & ENTITY BEHAVIOR ANALYTICS)*

OBJECTIF : Détecter les comportements anormaux des utilisateurs et systèmes (ex. téléchargement soudain de gigaoctets de données).

IMPACT : Détection précoce des fuites en cours et réponse automatisée.

5. CASB *(CLOUD ACCESS SECURITY BROKER)*

OBJECTIF : Contrôler et sécuriser les accès aux applications *Cloud* utilisées par les employés.

IMPACT : Empêche les fuites via des services *Cloud* tiers.

6. MICRO-SEGMENTATION ET EDR/XDR

OBJECTIF : Restreindre les accès internes aux systèmes critiques et détecter toute activité suspecte.

IMPACT : Limite la propagation des attaques et empêche l'accès aux bases de données sensibles.

Baromètre des fuites de données personnelles

ÉDITION 2025

IN CYBER FORUM EUROPE

HEXATRUST
CLOUD CONFIDENCE & CYBERSECURITY

CNIL.
COMMISSION NATIONALE INFORMATIQUE & LIBERTÉS