HYCU®

Rapport HYCU sur l'état de la résilience SaaS **2025**

Avec l'accélération de l'adoption du SaaS, la résilience des données est-elle laissée pour compte ?

Table des matières

Résumé

Avec l'augmentation des risques liés au SaaS, la protection des données est insuffisante

Les applications SaaS (Software-as-a-Service) sont devenues le pilier des activités numériques. Les organisations, tous secteurs confondus, s'appuient de plus en plus sur le SaaS pour gagner en agilité, collaborer à l'échelle mondiale et évoluer rapidement. Toutefois, à mesure que les portefeuilles SaaS s'étoffent, les risques se multiplient, et la protection des données ne suit pas le rythme. Fondé sur une enquête menée auprès de 500 décideurs informatiques et métiers à travers le monde, notre rapport 2025 sur l'état de la résilience du SaaS met en lumière des constats préoccupants, soulignant la nécessité de renforcer l'efficacité des stratégies de protection des données.

L'adoption du SaaS connaît une croissance rapide

L'usage des applications SaaS augmente dans l'ensemble des secteurs d'activité, s'imposant comme un pilier des activités des organisations.

- Les entreprises utilisent en moyenne 139 applications SaaS.
- 96 % des personnes interrogées ont augmenté leur utilisation du SaaS au cours des dernières années.
- 46 % ont constaté une augmentation significative de l'utilisation du SaaS.

Les menaces pesant sur les données SaaS s'intensifient

Les violations de données liées au SaaS sont de plus en plus courantes et ont des conséquences financières majeures. Pourtant, les organisations déclarent avoir une faible confiance dans leur capacité à prévenir ou à se remettre d'incidents affectant les données SaaS.

- 65 % des personnes interrogées ont subi une violation liée au SaaS au cours des 12 derniers mois.
- 87 % reconnaissent qu'au moins une de leur application SaaS est exposée à des risques en raison d'une protection inadéquate.
- Le coût moyen d'une interruption de service est de 405 770 dollars par jour, soit 2,3 millions de dollars pour une période de restauration de cinq jours.

Résumé

La planification de la résilience des données SaaS ne suit pas le rythme des menaces

Plus de la moitié des organisations interrogées indiquent que les défis liés à la protection des données ont accru leur exposition aux cybermenaces. Les équipes IT ne contrôlent pas toujours les applications SaaS, ce qui limite la visibilité, la sécurité et la conformité.

- 66 % des répondants estiment que les fournisseurs SaaS sont seuls responsables de la protection, alors que plus de la moitié déclarent manquer de confiance dans leurs capacités de protection.
- 43 % indiquent que la sécurité du SaaS n'est réellement attribuée à aucun responsable, créant des lacunes critiques en matière de responsabilité.
- 44 % rencontrent des difficultés à répondre aux audits et aux exigences réglementaires.

La majorité des organisations sont insuffisamment protégées et mal préparées face à ces menaces

Alors que les lacunes en matière de protection sont généralisées, la plupart des organisations interrogées ne parviennent même pas à respecter les exigences minimales en matière de protection des données SaaS.

- Seules 30 % d'entre elles effectuent des sauvegardes pilotées sur des politiques pour certaines de leurs applications SaaS.
- Seules 26 % ont mis en place une conservation des données hors site pour certaines de leurs applications.
- Seules 25 % ont mis en place des tests de résilience pour certaines de leurs applications.

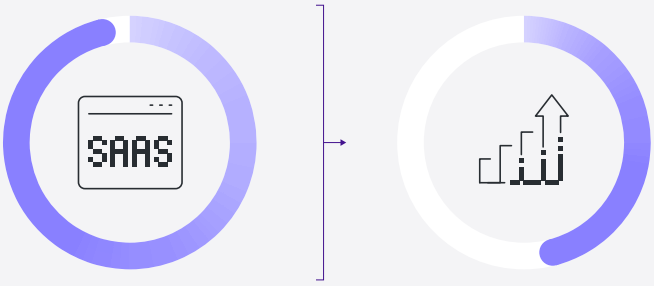
Si les plateformes SaaS ont apporté une valeur ajoutée considérable aux organisations, notre rapport révèle que les stratégies de résilience des données clients restent fragmentées, sous-financées et inadaptées au paysage actuel des risques. Le renforcement de la résilience passe par l'adoption d'une approche plus unifiée, automatisée et proactive de la protection des données SaaS.

L'adoption du SaaS est en plein essor et les risques augmentent

L'adoption du SaaS ne montre aucun signe de ralentissement. Pratiquement toutes les organisations ont ajouté davantage d'applications SaaS au cours des deux ou trois dernières années. Le nombre moyen d'applications utilisées aujourd'hui est **de 139**, mais ce chiffre augmente considérablement parmi les organisations qui ont été confrontées à des violations répétées. Les entreprises touchées par plusieurs incidents ont déclaré utiliser près de **159 applications**, tandis que celles ayant évité les violations n'en utilisaient en moyenne que **116**.

Cette constatation met en évidence un lien direct entre la prolifération du SaaS et la vulnérabilité. Chaque nouvelle application apporte de nouvelles intégrations, de nouvelles autorisations et de nouveaux emplacements où des données sensibles peuvent être stockées. Comme l'a déclaré un membre du conseil d'administration britannique dans le domaine de l'éducation :

> *La surface d'attaque augmente avec le nombre d'applications SaaS utilisées, ce qui multiplie les points d'entrée potentiels pour les cybercriminels.*



96 %

des organisations ont augmenté leur utilisation des applications SaaS au cours des 2-3 dernières

46 %

ont constaté une augmentation significative

139

applications SaaS utilisées en moyenne dans les entreprises

Celles qui ont été victimes de plus d'une violation au cours des 12 derniers mois utilisent en moyenne **159** applications SaaS

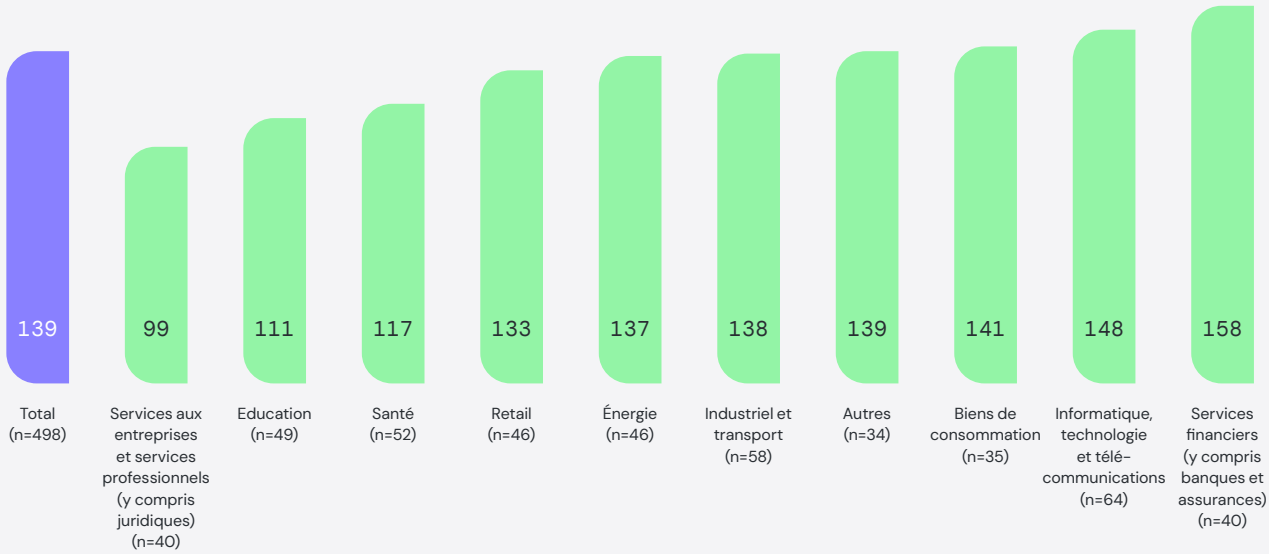
La croissance du SaaS impacte l'ensemble des secteurs d'activité

Tous les secteurs sont confrontés à l'expansion du SaaS. Les secteurs de l'IT et de la vente au détail affichent les niveaux d'adoption les plus élevés, tandis que les secteurs de la santé et des services financiers sont particulièrement sensibles aux enjeux liés à la conformité.

Malgré les différences sectorielles, la tendance sous-jacente est constante. Le SaaS est désormais profondément intégré aux opérations commerciales quotidiennes, et aucun service ou fonction ne dispose d'une vue d'ensemble complète de ce qui est utilisé. Le Shadow IT et l'adoption décentralisée conduisent souvent les équipes IT à devoir sécuriser des applications qu'elles ne contrôlent pas directement.

Pour les responsables informatiques, cela crée un nouveau défi en matière de gouvernance : protéger les données dans des environnements où la visibilité est, au mieux, partielle et où la responsabilité est mal définie.

Nombre moyen d'applications SaaS utilisées, par secteur d'activité



Les incidents de sécurité liés au SaaS sont monnaie courante

65 % des organisations ont subi une violation liée au SaaS au cours des 12 derniers mois. Il ne s'agit plus d'un risque marginal : c'est une réalité vécue par la majorité des organisations, tous secteurs, tailles et régions confondus.

Ce qui est particulièrement préoccupant, c'est la corrélation avec l'adoption du SaaS. Plus une organisation utilise d'applications, plus elle est susceptible de subir une violation. Les organisations disposant des portefeuille SaaS étendus sont non seulement victimes de violations plus fréquentes, mais elles signalent également une gravité des incidents plus élevée.

Cela signifie que le risque lié au SaaS n'est pas seulement théorique. Il s'agit d'une conséquence mesurable de l'expansion du SaaS et d'une planification inadéquate de la résilience.

65 %

ont subi une violation de données liée à une application SaaS au cours de l'année écoulée

2

Nombre moyen d'incidents de violation de données liés aux applications SaaS au cours de l'année écoulée

Ceux qui utilisent **davantage d'applications SaaS** sont plus susceptibles d'avoir subi une violation

1 à 100 applications SaaS — **60 %**

101 à 200 applications SaaS — **66 %**

201 applications SaaS et plus — **77 %**

Le coût élevé des perturbations liées au SaaS

Ces chiffres ne reflètent qu'une partie de la réalité.

Au-delà des coûts directs, les responsables informatiques soulignent des pertes plus difficiles à quantifier : la confiance des clients, les sanctions réglementaires et l'atteinte à la réputation. Dans de nombreux cas, ces impacts dépassent largement les coûts techniques liés à l'indisponibilité des services.

Les conséquences financières des incidents liés au SaaS sont considérables.

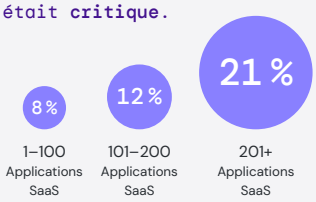
- **Le coût quotidien d'une interruption de service SaaS s'élève en moyenne à 405 770 dollars.**
- La reprise d'activité nécessite généralement **cinq jours ouvrés**, ce qui représente une perte estimée à **2,3 millions de dollars par incident**.
- Pour les organisations qui utilisent 200 applications SaaS ou plus, le coût de la reprise après une panne est près de **cinq fois supérieur à celui** des organisations disposant de portefeuilles plus restreints.

L'impact des violations de données sur les organisations souligne l'urgence d'adopter une stratégie de défense efficace.

Parmi les **65 %** ayant été victimes d'une violation de données au cours de l'année écoulée...

87 % ont subi un certain **niveau de perturbation.**

Les organisations utilisant davantage d'applications SaaS déclarent plus fréquemment que la violation était **critique.**



Impacts financiers et délais de reprise

405,770$
Coût quotidien moyen estimé de l'indisponibilité des données SaaS

1–100 Applications SaaS	101–200 Applications SaaS	201+ Applications SaaS
219,458$	262,976$	999,112$

5 jours ouvrables en moyenne pour **le rétablissement des services**

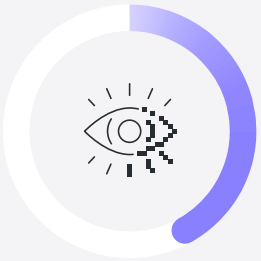
= 2.300,000$ de pertes potentielles

Les lacunes en matière de visibilité et de responsabilité aggravent le risque

Un constat récurrent de l'étude est le manque de visibilité et de responsabilité clairement définie.

- **44 % rencontrent des difficultés à répondre aux audits et aux exigences réglementaires.**
- **55 % déclarent manquer de confiance dans les capacités de protection des fournisseurs.**
- **51 % affirment que leurs défis en matière de protection des données ont accru leur exposition aux cybermenaces.**

Plus révélateur encore : **43 % des organisations indiquent que personne n'est véritablement responsable de la résilience des données SaaS.** Cette absence de responsabilité crée de la confusion, des retards et affaiblit la posture globale. Lorsque personne n'est responsable de la résilience des données, tout le monde est exposé.



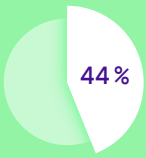
42 %

Visibilité limitée sur la protection des données dans les applications SaaS

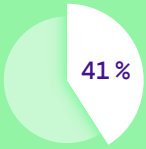
43 %

indiquent que personne n'est véritablement responsable de la résilience des données SaaS, ce qui crée des lacunes en matière de risques et de responsabilité.

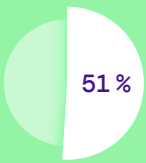
Impact d'une visibilité limitée



Difficulté à répondre aux audits ou aux exigences réglementaires



Perte de données ou impossibilité de récupérer les fichiers supprimés

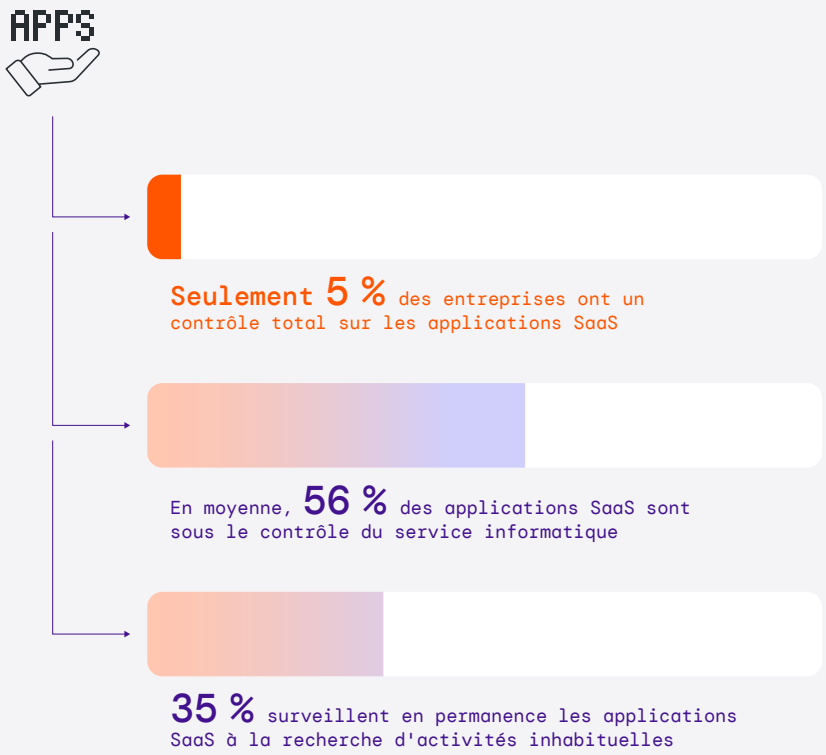


Exposition accrue aux cybermenaces

Le service IT n'est pas toujours aux commandes

La transition vers le SaaS a fondamentalement changé le rôle de l'IT. Auparavant, les applications étaient hébergées dans des centres de données centralisés, où les équipes informatiques exerçait un contrôle total. Aujourd'hui, l'adoption est souvent pilotée par des départements extérieurs à l'informatique. Le Marketing acquiert son propre CRM. Les Ressources Humaines déploient de nouveaux outils collaboratifs. La finance met en place des plateformes cloud natives.

Si cette flexibilité aide les équipes à avancer plus rapidement, elle affaiblit également la visibilité et le contrôle centralisés. Les responsables informatiques sont voient demander de protéger des environnements sur lesquels ils ont eu peu, voire aucune, influence lors du choix des solutions. Il en résulte de nouveaux défis en matière de sécurité, de conformité et d'application des politiques.



Les lacunes en matière de protection sont très répandues

Les résultats de l'enquête confirment que la protection n'a pas suivi le rythme de l'adoption :

- **87 % des organisations disposent d'au moins une application SaaS non protégée**
- **En moyenne, six applications par organisation présentent un niveau de risque**
- **66 % des personnes interrogées pensent à tort que leurs fournisseurs SaaS sont seuls responsables de la protection**

Une dépendance excessive à l'égard des solutions de récupération natives des fournisseurs expose dangereusement les organisations. Comme l'explique un dirigeant d'une entreprise de services publics :

> *Nous n'avons pas une visibilité totale sur les pratiques de sécurité de chaque fournisseur tiers. Il s'agit là d'un angle mort dans notre posture de sécurité globale.*

Cette confiance mal placée crée une réalité dangereuse. Lorsqu'une violation se produit, de nombreuses organisations découvrent trop tard que la responsabilité leur incombait depuis le début.

87 %

ont au moins un type d'application SaaS à risque en raison d'une sauvegarde inadéquate ou d'une dépendance excessive à la récupération native

66 %

estiment que la responsabilité de la protection des données devrait incomber à leur fournisseur SaaS

6

types d'applications SaaS à risque par organisation, en moyenne

Applications sous les projecteurs

Les personnes interrogées ont systématiquement cité les plateformes SaaS d'entreprise comme leur principale source de préoccupation. Les raisons varient, mais le thème est constant : ces applications sont profondément intégrées, largement accessibles et hébergent des données critiques pour l'entreprise.

Application	Raisons fournies par les répondants
salesforce	« Salesforce CRM et nos plateformes de collaboration présentent les risques les plus importants en matière de sécurité. En effet, elles traitent des données sensibles, sont largement accessibles et offrent des capacités d'intégration. Les erreurs de configuration, les contrôles d'accès insuffisants et les accès non autorisés constituent des vecteurs d'attaques. » Membre du conseil d'administration d'une entreprise informatique
GitHub	« GitHub représente le risque de sécurité le plus important pour notre organisation en raison de son rôle dans le stockage et la gestion du code source, des identifiants et des fichiers de configuration qui sont essentiels à nos opérations. » Membre du conseil d'administration d'une entreprise informatique
okta	« En tant que plateforme de gestion des identités et des accès (IAM), Okta sert de passerelle centrale vers pratiquement tous les autres outils SaaS et systèmes internes. Si elle était compromise, elle pourrait permettre à un pirate d'accéder aux applications internes et destinées aux clients, aux outils administratifs et aux systèmes privilégiés. » Cadre supérieur d'une entreprise informatique
Microsoft 365	« Garantir la conformité des applications Microsoft 365 avec la réglementation en matière de protection des données peut s'avérer complexe, ce qui représente le plus grand risque pour la sécurité de mon organisation. »
box	« C'est Box : de nombreuses équipes y déposent des informations importantes. Si quelqu'un de l'extérieur y avait accès, nous ne le saurions même pas immédiatement. »
slack	« Pour de nombreuses entreprises, Slack est un outil de communication essentiel, mais une violation pourrait exposer des discussions internes confidentielles, des pièces jointes et des historiques de discussion. »
Google Workspace	« En raison de sa suite d'applications, Google Workspace présente une large surface d'attaque. Le risque d'attaques par hameçonnage, de violations de données et d'accès non autorisé à des informations sensibles est constant. Nous mettons en œuvre des mesures de sécurité robustes, notamment l'authentification multifactorielle et la prévention des pertes de données, afin de protéger notre environnement Google Workspace. »
zoom	« Les comptes rendus des réunions Zoom contiennent de nombreuses informations internes confidentielles, en particulier le contenu des négociations avec les fournisseurs, et si ces données sont interceptées ou téléchargées, nos pertes peuvent être très importantes. »
zendesk	« Zendesk, car la complexité de la configuration et de la gestion des autorisations pour ces intégrations entraîne des erreurs de configuration de la part du client et accorde un accès trop large à des applications ou services tiers. »
Dropbox	« Sans contrôles de sécurité appropriés, Dropbox pourrait entraîner le partage non autorisé de documents sensibles, ce qui constituerait une menace pour la confidentialité et la conformité de l'entreprise. »
HubSpot	« HubSpot est lié à l'ensemble de notre entonnoir de vente. La perte de données ici serait plus qu'un simple désagrément. »

Insuffisamment protégées et insuffisamment préparées

La majorité des organisations ne respectent pas les exigences minimales en matière de protection des données SaaS :

- 30 % effectuent des sauvegardes basées sur des politiques pour *certaines de leurs applications*
- 26 % disposent d'une conservation des données hors site pour *certaines de leurs applications*
- 25 % ont mis en place des tests de résilience pour *certaines de leurs applications*

30 %

effectuent des sauvegardes basées sur des politiques

26 %

disposent d'une conservation des données hors site

25 %

effectuent des tests de résilience

Méthodologie

Le rapport HYCU sur l'état de la résilience du SaaS en 2025 repose sur une enquête mondiale menée en 2025 auprès de **500 décideurs IT et métiers**. Les personnes interrogées représentaient des organisations utilisant activement des applications SaaS, issues de secteurs d'activité variés.

Les participants comprenaient des membres de conseils d'administration, des dirigeants de niveau C-suite ainsi que des managers seniors et intermédiaires, garantissant une vision équilibrée entre enjeux stratégiques et opérationnels. Pour être éligibles, tous les répondants devaient travailler dans des organisations déployant actuellement des applications SaaS. Les questions de l'enquête portaient sur les tendances en matière d'adoption du SaaS, les incidents de sécurité, les stratégies de protection des données, le niveau de confiance en matière de résilience, ainsi que l'impact métier des interruptions de services ou des violations.

Les réponses ont été analysées à l'échelle mondiale, avec une couverture régionale incluant l'Amérique du Nord, l'Europe et l'Asie-Pacifique. Cette approche permet d'obtenir une vision représentative des dynamiques d'adoption du SaaS et des défis en matière de résilience dans des marchés soumis à des contraintes réglementaires et opérationnelles différentes.

L'objectif de cette étude est de mettre en lumière la manière dont les organisations adaptent leurs stratégies de protection et de sécurité des données dans un monde où le SaaS occupe une place prépondérante, et où son adoption continue de s'accélérer, tandis que la résilience peine encore à suivre.

500 décideurs informatiques

Membres du conseil d'administration, cadres supérieurs et cadres intermédiaires opérant dans les domaines suivants :

Informatique	n=64
Santé	n=52
Retail	n=46
Services financiers	n=40
Biens de consommation courante	n=35
Industriel	n=58
Éducation	n=50
Énergie	n=46
Services aux entreprises et services professionnels	n=40
Secteur Public	n=40

Régions

Amérique du Nord	125
EMEA	225
APAC	150


États-Unis 125


Royaume-Uni 75


Allemagne 75


France 75


Singapour 50


Japon 50


Australie 50

Rapport HYCU sur l'état
de la résilience SaaS **2025**