VARONIS

The Great SaaS Data Exposure

The Great SaaS Data Exposure
The Great SaaS Data Exposure
The Great SaaS Data Exposure
The Great SaaS Data Exposure
The Great SaaS Data Exposure

En moyenne, le risque de fuite de données SaaS pour une organisation se chiffre à plus de 28 M$.

2022

Table of contents

Termes clés

Comptes administrateur (admin)

Comptes utilisateur dotés de droits supplémentaires pour permettre à l'équipe informatique d'effectuer des tâches comme l'installation de logiciels.

Accès public

Désigne des enregistrements, des fichiers et des dossiers ouverts à tous via Internet.

Objets sensibles

Les données, comme la métadonnée de fichiers, stockées et accessibles dans le cloud.

Comptes utilisateur obsolètes (« utilisateurs fantômes »)

Comptes activés semblant inactifs, souvent liés à des utilisateurs qui ne sont plus employés par l'organisation.

Enregistrements ou fichiers sensibles

Instances de données à caractère personnel ou autrement sensibles. Un seul fichier de feuille de calcul peut contenir plusieurs enregistrements. Les enregistrements et fichiers sensibles peuvent inclure des données de cartes de paiement, des dossiers médicaux, ou des données à caractère personnel soumises à des réglementations comme la norme PCI, le HIPAA, le RGPD, etc.

Accès à l'ensemble de l'organisation

Désigne les enregistrements, fichiers et dossiers ouverts à tous les employés.

Données obsolètes

Informations qui ne sont plus nécessaires pour les opérations quotidiennes.

Comptes privilégiés

Dotés d'autorisations élevées pour accéder aux systèmes et aux données sensibles.

Liens de partage

Permettent aux utilisateurs de partager rapidement et facilement des données avec d'autres.

À propos du rapport

Notre équipe de recherche a analysé :

10 milliards d'objets

15 pétaoctets de données

717 organisations

Cette métadonnée est issue de plusieurs applications et services SaaS et IaaS tels que Microsoft 365, Box et Okta.

Analyse firmographique

Ce rapport analyse les données de nombreux secteurs :

- Services financiers
- Pharmacie et biotechnologies
- Énergie et services publics
- Technologie
- Administrations nationales et locales
- Santé
- Fabrication
- Vente au détail
- Éducation

Les données ont été recueillies auprès d'entreprises du monde entier, notamment aux États-Unis, au Canada, au Royaume-Uni, en France, en Allemagne, en Espagne, au Brésil et en Australie.

Résultats clés

Une entreprise lambda compte une quantité alarmante de données sensibles exposées à tous ses employés, voire, dans nombre de cas, à tous les utilisateurs d'Internet. Cette situation peut à tout moment engendrer une fuite de données catastrophique.

81 % des organisations évaluées ont des données sensibles SaaS exposées.

Une entreprise lambda compte :

10 % de données cloud exposées à chaque employé

– un risque interne considérable.

4 468 comptes utilisateur sans MFA (authentification multifactorielle)

(authentification multifacteur) activée, ce qui permet aux hackers de compromettre plus facilement les données exposées en interne.

Plus de 40 millions de droits uniques

sur l'ensemble des applications SaaS, un cauchemar pour les équipes informatique et de sécurité chargées de gérer et de réduire les risques liés aux données cloud.

Plus de 12 000 liens de partage Microsoft 365

qui exposent les données de toute l'organisation à chaque employé.

157 000 enregis-trements sensibles exposés à tous sur Internet

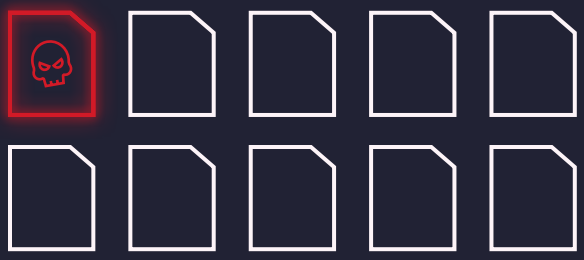
via des fonctionnalités de partage SaaS – soit 28 M$ de risques de fuite de données.

33 comptes superadministrateur

– plus de la moitié d'entre eux sans MFA activée. En compromettant ces comptes, les hackers peuvent voler plus de données, créer des portes dérobées et semer le chaos.

6 % des données cloud exposées à tous sur Internet.

Pourquoi cette situation peut engendrer une catastrophe à tout moment :



Un enregistrement sur 10 dans le cloud est exposé à tous les employés.

Le rayon d'exposition interne d'une organisation lambda est incroyablement vaste ; n'importe quel employé a la capacité de voler 10 % de ses données cloud.

L'absence de MFA facilite la tâche des hackers.

Les comptes dépourvus de contrôles de sécurité de base tels que la MFA – y compris des comptes administrateur malveillants – facilitent la violation des applications SaaS et le vol des données exposées en interne.

L'identification des données exposées au sein du SaaS est une tâche titanesque.

Les applications SaaS sont conçues pour créer automatiquement plus d'exposition, mais beaucoup n'incluent aucune fonctionnalité permettant de détecter et de réduire cette exposition. Le nombre de droits SaaS à gérer augmente exponentiellement par rapport aux droits sur site.

IBM Security, **« Cost of a Data Breach Report »,** page 5. D'après ce rapport, les données à caractère personnel des clients sont le type d'enregistrement le plus coûteux : 180 $ par enregistrement perdu ou volé. Nous avons constaté qu'une organisation lambda compte 157 000 enregistrements exposés, ce qui représente pour elle un risque évalué à 28 M$.

Un téraoctet dans le cloud

611 478 Fichiers	**6 116** Fichiers sensibles
3 998 dossiers partagés en externe	**4 324** fichiers sensibles obsolètes
1 924 canaux privés Microsoft Teams (par org.)	**295** Microsoft Teams (par org.)
2 152 543 Droits	

En moyenne, chaque téraoctet dans le cloud contient plus de 6 000 fichiers sensibles, près de 4 000 dossiers partagés avec des contacts externes et plus de 2,1 millions de droits (entrées de contrôle d'accès).

Avec autant de contenus et d'accès dans un seul téraoctet, on comprend aisément comment les données peuvent échapper à tout contrôle.

7 %

des entreprises comptaient plus de 10 000 fichiers exposés

10

entreprises comptaient plus de 100 000 fichiers exposés

1

organisation comptait plus d'1,5 million de fichiers exposés

Des données exposées à l'échelle de l'organisation dans Microsoft 365

Chaque employé peut créer, lire, mettre à jour et supprimer des données critiques et sensibles sur le réseau s'il dispose d'un accès à l'ensemble de l'organisation. En offrant à tout le personnel l'accès aux données, les organisations créent une large surface d'attaque, hautement vulnérable aux cyberattaques comme les ransomwares et les menaces internes.

Dans une organisation lambda utilisant Microsoft 365 :

Un fichier sensible sur 10 est exposé à chaque utilisateur.

Un dossier sur 10 est exposé à l'ensemble de l'organisation.

1 000 fichiers sensibles (9 %) sont exposés à l'ensemble de l'organisation.

97 638 dossiers (8 %) sont exposés à l'ensemble de l'organisation.

En moyenne, il faut environ **six heures** par dossier pour localiser et supprimer manuellement les groupes à accès global, créer et appliquer de nouveaux groupes, puis renseigner ces groupes avec les utilisateurs qui ont besoin d'accéder aux données. Pour 1 000 dossiers, cela représente 6 000 heures de gestion manuelle !

Étude de cas

Si la collaboration impliquant le partage de données fait partie intégrante de chaque organisation, elle se fait rarement de manière sécurisée. Aux États-Unis, un comté a découvert que des informations sensibles sur des affaires pénales en cours étaient exposées à tous les employés dans son environnement Microsoft 365. Confrontée à des milliers d'employés et à la prolifération des droits, l'équipe informatique ne réussissait pas à verrouiller les données de manière fiable. La visibilité, l'automatisation et les fonctions d'alerte se sont avérées essentielles pour protéger leurs données dans le cloud Microsoft.

Des droits hors de contrôle

Une entreprise lambda accorde plus de 40 millions de droits uniques sur l'ensemble des applications SaaS, un cauchemar pour les équipes informatique et de sécurité qui tentent de gérer et de réduire les risques liés aux données cloud.

En matière d'analyse de l'accessibilité, la plupart des DSI ne réalisent pas combien de dossiers, de fichiers et d'enregistrements devront être examinés. Un seul téraoctet de données contient habituellement des dizaines de milliers d'objets dotés de droits spécifiques et uniques qui déterminent quels utilisateurs et groupes y ont accès. Or, les organisations comptent désormais des milliers de téraoctets de données. Toutes les relations entre les utilisateurs et les groupes doivent également être analysées. Facteur aggravant, chaque application SaaS met en œuvre des mécanismes de droits différents.

Étude de cas

Une société immobilière internationale avait accordé un accès à son instance Salesforce à une douzaine de sous-traitants. Des mois plus tard, après la fin de leur projet, ces anciens sous-traitants pouvaient toujours se connecter et accéder à tous les dossiers de la société. Deux d'entre eux étaient des superadministrateurs, et l'un s'était récemment connecté. En outre, 182 utilisateurs standard pouvaient exporter chaque enregistrement, et un responsable de vente a été surpris en train d'exporter des informations commerciales et des comptes après avoir donné sa démission.

Étude de cas

Dans une banque nationale, l'équipe de sécurité manquait de visibilité sur l'instance Salesforce de l'institution. Les administrateurs Salesforce locaux avaient cloné dix instances « shadow » sans que l'équipe de sécurité le sache. Au sein de ces instances, 23 utilisateurs réguliers disposaient de droits masqués qui leur permettaient de réinitialiser des mots de passe pour d'autres utilisateurs, de créer de nouveaux utilisateurs et d'afficher, de supprimer et d'exporter toutes les données. De plus, l'équipe de sécurité n'était pas au courant des tentatives de piratage par force brute que subissait continuellement l'une de ces instances.

Les liens de partage en interne surexposent les données

Plus de 27 000

liens de partage vers des informations dans Microsoft 365

12 803

liens de partage ouverts à tous les employés

Si les liens de partage sont utiles pour collaborer, ils constituent également un risque important pour la sécurité.

La protection des données sensibles s'avère plus complexe lorsque le partage en interne est facilité. Si des personnes internes ou des hackers accèdent à des données auxquelles ils ne devraient pas avoir accès, celles-ci deviennent immédiatement la cible potentielle d'un vol ou d'une attaque de ransomware.

Partagés à l'excès, les liens vers des données sensibles peuvent exposer ces dernières à tous les membres de l'organisation. Même une erreur de configuration mineure peut créer une faille de sécurité importante et entraîner une fuite de données.

Notre étude a montré qu'une entreprise lambda comptait des milliers de liens de partage vers des données dans Microsoft 365, et que près de la moitié de ces liens étaient ouverts à tous les employés.

Étude de cas

Une **université privée** devait atténuer les risques posés par des menaces comme le ransomware. Son environnement hybride sur site et dans le cloud s'était complexifié, rendant difficile la gestion du partage externe et de l'exposition des données. Grâce à la visualisation des structures de droits existants pour les fichiers Microsoft 365, la petite équipe informatique de l'université a pu gérer le partage externe pour les utilisateurs dotés d'un accès important.

Des données accessibles à tous sur Internet

Aussi terrifiant que cela puisse paraître, le partage public rend les données accessibles à tous sur Internet.

L'utilisation d'applications et de services SaaS et IaaS peut accroître le risque de manière exponentielle : au lieu de simplement exposer les données sensibles à chaque employé, elle peut les exposer à tous et partout via Internet.

Nombre d'organisations peinent à verrouiller les accès. Une organisation standard compte plus de 150 000 enregistrements et fichiers partagés publiquement. En moyenne, nous avons trouvé près de 50 000 enregistrements sensibles dans Microsoft 365 et plus de 113 000 dans des applications SaaS ouvertes à tous sur Internet. Ces dossiers sensibles comprenaient des informations protégées aux termes des réglementations HIPAA, CCPA, GLBA et RGPD, notamment des numéros de sécurité sociale, des données de carte bancaire et même des mots de passe en texte brut.

En moyenne, une organisation compte :

157 181

Fichiers partagés publiquement

6 %

de liens de partage ouverts à tous sur Internet

18 763

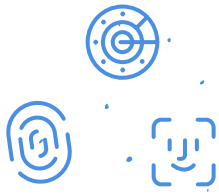
dossiers partagés publiquement

48 896

enregistrements sensibles partagés publiquement dans Microsoft 365

113 632

enregistrements sensibles partagés publiquement dans les applications SaaS



En activant la MFA, vous êtes

99 %

moins susceptibles d'être piratés.

4 468

comptes utilisateur sans MFA activée.

Absence de MFA

L'authentification multifacteur (MFA) est une mesure de sécurité essentielle qui permet de protéger les utilisateurs même si leurs mots de passe sont divulgués ; néanmoins, la MFA n'est utile que si elle est activée et appliquée.

D'après Jen Easterly, directrice de la CISA, l'activation de la MFA rend votre organisation 99 % moins susceptible d'être piratée.

En moyenne, dans notre étude, les entreprises comptaient 4 468 comptes utilisateur sans MFA activée – autrement dit, plus de 4 000 comptes requéraient uniquement les identifiants de connexion d'un utilisateur. Les organisations disposaient en moyenne de 33 comptes administrateur, dotés de privilèges élevés en matière de gestion et de modification des comptes utilisateur, des systèmes et des paramètres. Parmi ces comptes, 18 (55 %) n'utilisaient pas la MFA.

Sans MFA, il est bien plus facile d'attaquer et de compromettre une organisation. Les groupes criminels comme BlackMatter sont connus pour s'emparer de noms d'utilisateurs et de mots de passe issus de la mise en ligne massive de données volées sur le dark Web. Pour obtenir l'accès, ils essaient tous les identifiants lors d'attaques par force brute sur les systèmes connectés à Internet.

33

comptes administrateur

41

comptes privilégiés

55 %

de comptes administrateur sans MFA

44 %

de comptes privilégiés sans MFA

La MFA ne suffit pas toujours : elle peut être contournée par des hackers de diverses manières. Les chercheurs de Varonis Threat Labs ont découvert des techniques pour contourner la **MFA basée sur le mot de passe temporaire à usage unique de Box,** et une technique pour contourner la **MFA basée sur l'envoi d'un SMS de Box.** Avant que Box ne résolve ces problèmes, les hackers pouvaient utiliser des identifiants volés provenant du dark Web pour infiltrer discrètement les comptes Box, même lorsque la MFA était activée.

Comptes utilisateur obsolètes

Les comptes utilisateur obsolètes (on parle parfois d'« utilisateurs fantômes ») sont des comptes activés en apparence inactifs, souvent liés à des utilisateurs qui ont quitté l'organisation.

Ces comptes obsolètes restent souvent activés mais peuvent être facilement ignorés, car inactifs. Ils donnent accès à des applications et à des données, et peuvent permettre aux hackers de « tester le terrain » en toute discrétion ou de tenter une attaque par force brute sans faire de remous ni déclencher d'alarme.

1 197

Utilisateurs inactifs

1 322

utilisateurs invités

56 %

d'utilisateurs invités obsolètes toujours activés à 90 jours

33 %

d'utilisateurs invités obsolètes toujours activés à 180 jours

Étude de cas

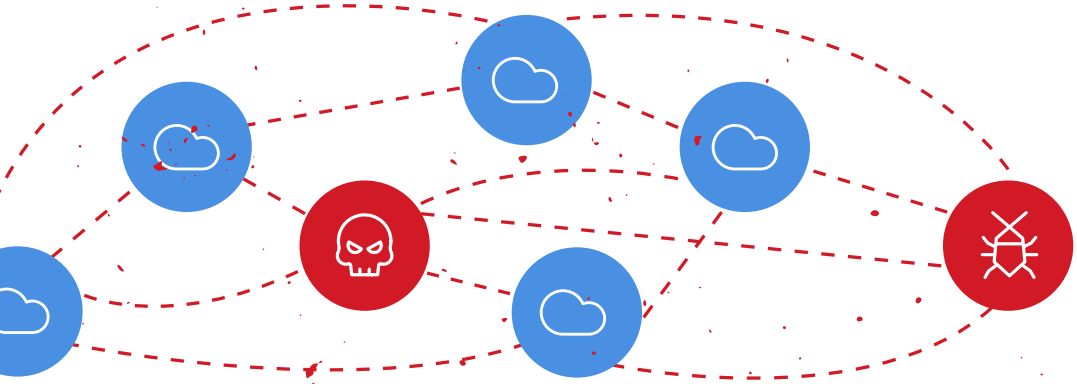
Chez un **grand fabricant** de l'industrie automobile, les attaques successives de ransomware avaient mis en évidence la nécessité d'adopter des solutions de cybersécurité modernes. En étant en mesure de visualiser l'activité des utilisateurs sur site et dans Microsoft 365, l'entreprise a identifié et désactivé plus de 500 utilisateurs obsolètes et réduit le nombre de groupes Microsoft 365 de 280 à 31.

État de Sécurité du cloud

Les applications et services cloud créent une surface d'attaque étendue et interconnectée qui peut être compromise de nouvelles manières par des acteurs internes et externes. Les attaques sont devenues plus efficaces et plus dévastatrices. Les hackers commandités par un État sont plus sophistiqués, et leurs techniques se répandent dans le monde des entreprises, comme elles l'ont déjà fait maintes fois.

Le cloud libère une valeur ajoutée considérable pour les organisations. Mais parallèlement aux atouts qu'elle présente en matière de collaboration et de commodité, cette technologie rend la détection des menaces beaucoup plus difficile. Chaque terminal peut servir de point d'accès à des environnements numériques contenant des données critiques et sensibles. En outre, les applications SaaS constituent souvent des angles morts majeurs pour les organisations qui cherchent à protéger leurs données.

Compte tenu de la disponibilité d'exploits et de la perspective de gains considérables dans le cas des ransomwares, les attaques ne cesseront pas. Tout système, compte ou personne peut à tout moment constituer un vecteur d'attaque potentiel . Avec une surface d'attaque aussi vaste, vous devez partir du principe que les hackers parviendront à compromettre au moins un vecteur, si ce n'est déjà fait.



Liste de contrôle de la sécurité des données cloud

- [ ] **Comprenez et réduisez votre rayon d'exposition SaaS.**

  Si un hacker compromettait un utilisateur, quels seraient les dégâts potentiels ? En réduisant le rayon d'exposition de votre cloud – tout ce à quoi un hacker peut accéder avec un seul compte ou système compromis – avant toute attaque, vous rendez la tâche du cybercriminel plus difficile.

- [ ] **Surveillez les activités inhabituelles dans votre environnement cloud.**

  Les hackers sont plus susceptibles de déclencher des alertes s'ils rencontrent plus d'obstacles pour accéder à vos données sensibles. Gardez un œil sur l'activité des utilisateurs et guettez les anomalies et les activités non respectueuses de la politique en place.

- [ ] **Adoptez une approche Zero Trust.**

  Le modèle Zero Trust est probablement votre meilleure défense contre les attaques liées aux données, tels les ransomwares. Aucune personne, application ou système ne devrait être en mesure d'accéder à ou de faire plus que le nécessaire. Limitez l'accès aux systèmes, applications et données, en particulier aux données sensibles.

- [ ] **Vérifiez les paramètres de votre application SaaS.**

  Une seule erreur de configuration suffit pour exposer des données sensibles. Si vos configurations ne sont pas parfaites, vous pouvez exposer vos applications – et vos données – à des risques considérables. Revérifiez les paramètres pour vous assurer que les mises à jour ne laissent pas de données exposées, limitez les partages externes et vérifiez les paramètres de configuration de partage du cloud.

- [ ] **Activez l'authentification multifacteur pour tous vos employés.**

  Cette étape simple est essentielle mais souvent négligée. Activez la MFA sur l'ensemble des applications et services cloud et pour les comptes de service/admin. Rendez la MFA obligatoire et n'autorisez pas les utilisateurs à la désactiver. Trop d'entreprises autorisent l'authentification à facteur unique pour les services connectés à Internet.

- [ ] **Mettez en place et appliquez des processus d'offboarding.**

  Alors que les entreprises utilisent de plus en plus d'applications et de services SaaS, les risques liés aux « utilisateurs fantômes » (comptes actifs mais inutilisés) augmentent. Ne manquez pas de révoquer les droits d'accès sur l'ensemble de vos services cloud chaque fois qu'un employé ou un sous-traitant quitte l'organisation.

- [ ] **Trouvez le juste équilibre entre productivité et sécurité.**

  Les applications SaaS offrent souvent un intérêt d'autant plus important qu'elles s'intègrent à d'autres applications, mais cette interconnectivité via des API facilite également le déplacement latéral des attaquants. Guettez les erreurs de configuration et veillez à avoir une bonne posture en matière de sécurité cloud.

- [ ] **Donnez la priorité à vos données.**

  Au lieu de commencer par défendre votre périmètre (terminaux, vecteurs), il est bien plus judicieux de protéger vos grands référentiels centralisés dans un premier temps, puis d'opérer de l'intérieur vers l'extérieur.

Recommandations

Une fois que vous avez « présumé l'intrusion », réfléchissez à l'endroit où un cybercriminel se rendrait le plus probablement s'il voulait maximiser ses profits. Si votre organisation ressemble aux autres, il se dirigera tout droit vers vos dépôts de données les plus critiques. Votre mission consiste à réduire au maximum votre rayon d'exposition, de sorte que les utilisateurs ne puissent accéder qu'aux éléments dont ils ont besoin, et à détecter les accès anormaux susceptibles d'indiquer qu'une attaque est en cours.

Chaque étape supplémentaire qui contraint un hacker ou un collaborateur à ralentir vous donne la possibilité de détecter et de contrer une attaque.

Imaginons qu'un hacker ou un employé malveillant s'en prenne à votre organisation. Vous accusez déjà un retard critique si vous ne pouvez pas voir instantanément ce que cette personne pourrait prendre – ou a déjà pris – dans vos applications et services SaaS.

Il est crucial d'axer votre approche sur les données.

Répondez à ces questions essentielles :

1. Savez-vous **où sont stockées vos données importantes ?**
2. Êtes-vous sûr(e) **que seules les personnes appropriées y ont accès ?**
3. Êtes-vous sûr(e) **qu'elles utilisent ces données correctement ?**

Ces trois questions abordent les trois dimensions fondamentales de la protection des données : l'importance des données, leur accessibilité et leur utilisation. Pour prendre des décisions significatives et améliorer votre posture face aux risques, vous devez voir où les données critiques sont concentrées et exposées (à risque) et qui les utilise, ou non (comptes obsolètes).

Donnez la priorité à vos données. Au lieu de commencer par défendre votre périmètre (terminaux, vecteurs), il est bien plus judicieux de protéger vos grands référentiels centralisés dans un premier temps, puis d'opérer de l'intérieur vers l'extérieur.

Étude de cas

Une société immobilière sécurise Salesforce grâce à Varonis.

Une société immobilière de premier plan a adopté DatAdvantage Cloud pour protéger les données sensibles dans ses applications SaaS les plus utilisées, notamment Salesforce. Grâce à une meilleure visibilité et à des alertes fiables qui s'intègrent parfaitement aux solutions de sécurité existantes, l'entreprise a réduit les délais de confinement et de réponse et gagné en sérénité, en sachant que ses données étaient protégées.

« Nous pouvons facilement exécuter des rapports et identifier qui a des droits de superadministrateur ou d'administrateur, ainsi que les points de chevauchement. DatAdvantage Cloud se révèle particulièrement pratique en ce qui concerne la visibilité sur l'ensemble des services cloud, car il est quasiment impossible de faire de même manuellement. Ce serait comme une gigantesque toile d'araignée, et il ne fait aucun doute que des informations passeraient au travers. »

Tony Hamil, société immobilière américaine

Lire l'étude de cas

Vous souhaitez savoir si vos données cloud sont exposées ?

Demandez à Varonis une évaluation gratuite des risques sur vos données cloud. Identifiez rapidement les risques cachés auxquels sont exposées vos données les plus importantes, sans alourdir votre charge de travail.

Obtenir votre évaluation des risques

À propos de Varonis

Varonis est un pionnier en sécurité et analyse des données, spécialisé dans les logiciels de protection des données, de détection des menaces et de mise en conformité. Varonis protège les données des entreprises en analysant l'activité liée aux données, la télémétrie du périmètre et le comportement des utilisateurs, évite les sinistres en verrouillant les données et maintient un état sécurisé grâce à l'automatisation.

www.varonis.com