# Sécuriser Salesforce en 2023

Identifier les risques, évaluer les enjeux

W / T H
secure

# Introduction

L'année 2022 a été une année mouvementée pour le secteur de la cybersécurité. Des groupes de hackers très actifs comme Lapsus$ et Conti ont fait parler d'eux en lançant des attaques contre des entreprises de premier plan et des infrastructures d'envergure nationale. Dans le même temps, d'autres groupes criminels moins médiatisés ont gagné en dangerosité en recourant aux ransomwares ciblés.

Les cyberattaques se propagent principalement par les systèmes informatiques et les endpoints traditionnels, mais de plus en plus d'entreprises migrent vers le cloud et les pirates informatiques tentent d'en tirer parti : ils concentrent désormais leurs efforts sur les environnements cloud comme Salesforce.

Salesforce est un environnement particulièrement collaboratif et personnalisable. Il prend en charge un large éventail de plug-ins tiers et offre de nombreuses options de connectivité.

Plus de 150 000 entreprises utilisent la plateforme Salesforce pour des activités essentielles comme la gestion de la relation client (CRM). Cette plateforme renferme donc de vastes volumes de données clients potentiellement sensibles et de grande valeur.

Salesforce est donc devenu une cible particulièrement attrayante pour les pirates informatiques. Bien qu'aucun piratage majeur n'ait encore été signalé sur la plateforme, ce n'est d'après nous qu'une question de temps.

Salesforce dispose d'un grand nombre de contrôles de sécurité. Cependant, pour protéger efficacement leurs données, les clients doivent eux-mêmes configurer de nombreux contrôles. C'est la nature même du modèle de responsabilité partagée.

Nous vous présenterons ici les grands axes de sécurisation de Salesforce pour 2023. Tout au long de ce rapport, trois experts en sécurité de Salesforce partageront leur expertise, pour vous aider à sécuriser votre environnement Salesforce. Leurs propos seront illustrés par les données produites par l'étude de marché 2022 de WithSecure™ sur la sécurité du cloud et de Salesforce*.

## Les grands dossiers de la sécurité, en 2022

- Les préoccupations des professionnels IT et des administrateurs de Salesforce en matière de sécurité
- Les mauvaises configurations et les actifs non-monitorés
- L'augmentation des fichiers et des liens malveillants dans Salesforce
- Les contrôles de sécurité à mettre en place
- Nos sept grandes recommandations pour sécuriser Salesforce en 2023

*Étude de marché WithSecure™ : Étude B2B menée auprès de 3072 décideurs et influenceurs informatiques dans 12 pays entre avril et mai 2022 : Royaume-Uni, France, Allemagne, Belgique/Pays-Bas, Finlande, Norvège, Suède, Danemark, États-Unis, Canada et Japon.

# Nos experts

**Dmitriy Viktorov**
Head of Product and Technology, Cloud Protection,
WithSecure™

Dmitriy est spécialiste des produits de sécurité. Passionné par la résolution de problèmes complexes, il s'est donné pour mission d'aider les clients à sécuriser leurs services cloud et autres services numériques. Il a occupé différents postes dans la R&D, la gestion des produits et les technologies. Il dirige actuellement le développement des produits Cloud Protection pour Salesforce.

**Pankaj Paryani**
Salesforce Technical Lead,
WithSecure™

Pankaj est développeur et consultant certifié Salesforce. Il mène plusieurs projets Salesforce avec des clients aux États-Unis, au Royaume-Uni et en région APAC. Il dirige l'équipe de développement CRM chez WithSecure™ : il veille à ce que les ventes et services restent opérationnels et adaptés aux besoins des clients.

**Doug Merrett**
Salesforce Security, Compliance,
Privacy and Resilience Specialist, Platinum7

Doug est un passionné de la sécurité. Il a travaillé durant 13 ans chez Salesforce en tant que Platform and Security Specialist, au Royaume-Uni et en Australie. Durant cette période, il a aidé les entreprises à bien comprendre l'approche de sécurité de Salesforce, afin qu'elles puissent mieux protéger leurs données stockées sur la plateforme. En juin 2021, Doug a créé sa propre société de conseil, Platinum7, centrée exclusivement sur la sécurité, la conformité et la résilience de Salesforce.

# Les principales préoccupations des professionnels IT et des administrateurs en sécurité Salesforce

## Les 5 grands enjeux de la sécurité

1. Prévenir les violations de données
2. Assurer une protection efficace contre les malwares et les ransomwares.
3. Détecter les attaques ayant pu contourner d'autres mesures de sécurité.
4. Prévenir les menaces avancées par e-mail comme les attaques de phishing et les attaques BEC (Business Email Compromise)
5. Assurer la sécurité des applications de collaboration cloud, comme Office 365 et Salesforce.

## * Cloud et collaboration

Les plateformes cloud comme Salesforce jouent désormais un rôle fondamental. Elles servent de socle au travail à distance et au travail hybride, adoptés en masse durant la pandémie.

En permettant une véritable optimisation des ressources, les environnements cloud offrent des avantages clairs en termes d'efficacité. Ils renferment toutefois des lacunes de sécurité et abritent de nombreux composants mobiles, dont beaucoup échappent à tout contrôle direct.

« Durant des décennies, l'approche on-premise a dominé : tout était sous le contrôle direct des entreprises. Le nombre de connexions externes à surveiller était limité. Désormais, tout se passe dans le cloud, et de nombreux systèmes critiques échappent à tout contrôle direct. »

Pankaj Paryani, Salesforce Technical Lead, WithSecure™

## Au cours des 18 derniers mois, quels ont été les trois principales difficultés que vous avez rencontrées dans le processus de sécurisation de vos données ?

(Extrait du rapport Salesforce Top Security Trends for 2022)

| | |
|---|---|
| *59% | Gestion de la sécurité des composants tiers |
| **53% | Respect des règles de conformité |
| 49% | Sécurité des appareils mobiles |
| 38% | Contraintes liées aux ressources |
| 37% | Gestion des vulnérabilités |
| 28% | Gestion des mesures de prévention proactive |
| 15% | Audit |
| 5% | Comportement des utilisateurs |

## *Gestion de la sécurité des composants tiers

La plateforme Salesforce est conçue pour être hautement personnalisable. Elle permet d'implémenter facilement de nouvelles fonctionnalités en fonction des besoins.
Sur le seul site Salesforce AppExchange, il existe plus de 3 400 applications. D'innombrables API et plug-ins tiers sont par ailleurs facilement accessibles en ligne. Si cette approche est particulièrement intéressante du point de vue de l'intégration et de l'accessibilité, elle crée également une chaîne d'approvisionnement étendue, qui peut rapidement devenir incontrôlable. Chaque ajout augmente l'exposition aux attaques de la supply chain, qui dominent le paysage de la cybersécurité depuis vingt ans. Ces menaces représentent donc un réel danger pour la sécurité de Salesforce. Pour en savoir plus, lisez notre dernier rapport sur la gestion des composants tiers de Salesforce.

## **Régulation et conformité

Les exigences réglementaires ne cessent d'évoluer et il devient de plus en plus difficile d'y répondre. À mesure que la migration vers le cloud s'accélère, les règles se complexifient. Chaque région promulgue ses propres lois ; chaque organisme de réglementation édicte ses propres normes. Désormais, les entreprises doivent impérativement savoir où sont transférées, stockées et traitées leurs données. Elles doivent aussi être attentives aux réglementations spécifiques à leur secteur, notamment si elles opèrent dans le monde de la santé ou de la finance.

Des changements sont à venir. Certains textes vont être modifiés, et de nouvelles réglementations vont être introduites. La Commission européenne s'apprête à publier la nouvelle directive NIS2 (Network and Information Systems) qui devrait entrer en vigueur dans les 18 prochains mois.

## Quelles sont vos trois principales préoccupations en matière de sécurité informatique ?


## Ransomwares et phishing

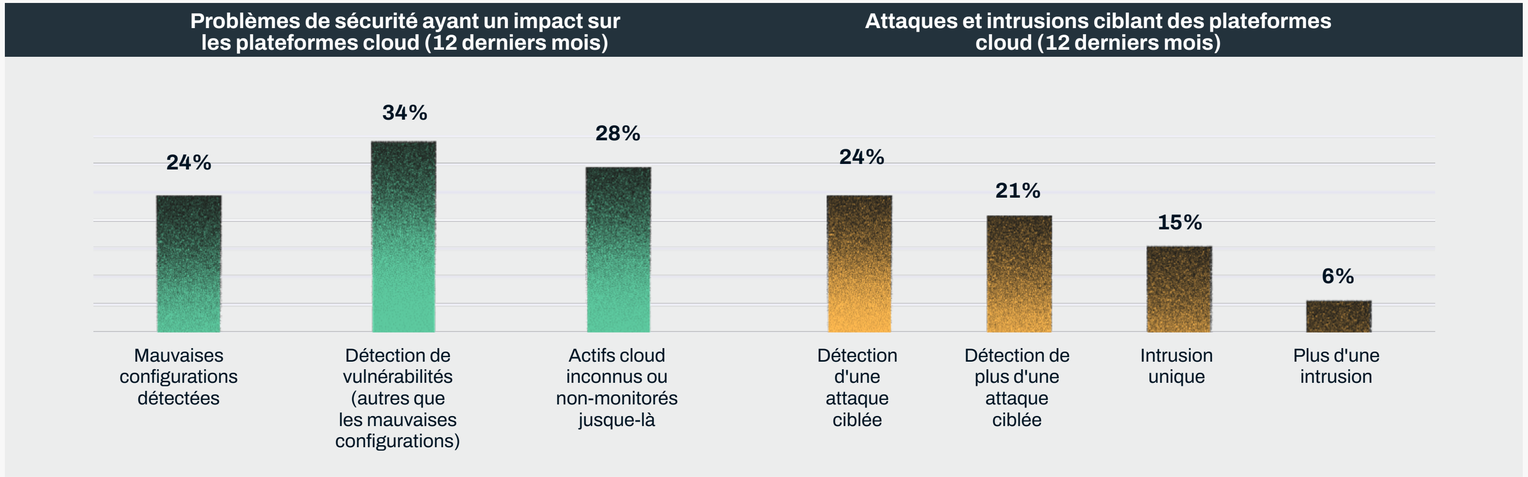
Le phishing (ou hameçonnage) est considéré comme une attaque par e-mail. S'il est vrai que les pirates informatiques utilisent principalement la messagerie pour lancer ce type d'attaque, Salesforce n'est pas pour autant à l'abri : la plateforme fournit en effet différents flux e-mails, comme email-to-case ou email-to-Chatter. De plus, avec Slack, Chatter et d'autres options tierces, Salesforce offre un certain nombre de canaux de communication et de collaboration pouvant également être exploités dans des attaques de phishing.

Du côté des ransomwares, la situation est plus complexe qu'il n'y paraît : l'environnement Salesforce lui-même est relativement inaccessible aux ransomwares standard, mais il reste possible de l'utiliser pour transmettre des fichiers et liens malveillants à des systèmes cibles. Il ne faut pas non plus oublier que les ransomwares et autres programmes malveillants évoluent rapidement. Les fonctions de communication très flexibles proposées par Salesforce pourraient créer un terrain favorable à l'émergence de menaces nouvelle-génération.

## Visibilité et contrôle des accès

La visibilité et le contrôle sur les connexions réseau constituent également des enjeux majeurs. Les entreprises doivent impérativement contrôler les accès (internes et externes) aux données et aux systèmes critiques. Et elles doivent savoir comment leur plateforme Salesforce se connecte et interagit avec d'autres systèmes.

# La menace des mauvaises configurations et des actifs non-monitorés.




Un quart des professionnels que nous avons interrogés estiment avoir été victimes d'une attaque ciblée au cours des 12 derniers mois. Ce chiffre montre à quel point les pirates informatiques sont devenus redoutables. Il n'en reste pas moins que beaucoup d'entreprises leur facilitent la tâche : elles ne configurent pas correctement leur environnement cloud, et ne le monitorent pas correctement non plus.

Les erreurs de configuration sont d'autant plus fréquentes que les possibilités offertes par les environnements cloud sont généralement immenses. Sur Salesforce, les problèmes de configuration les plus fréquents concernent les politiques d'accès. Les utilisateurs et les applications disposent souvent par défaut de droits d'accès trop élevés. Ces problèmes de configuration exposent aux menaces externes et aux attaques d'initiés, tout en augmentant les risques d'erreur humaine.

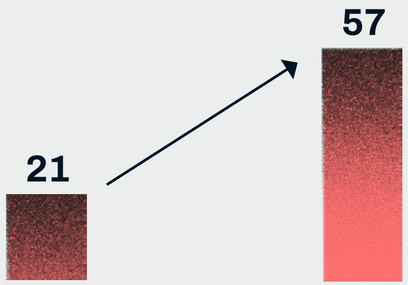
Par ailleurs, les entreprises ont souvent des difficultés à assurer le monitoring de leurs systèmes. Via le modèle SaaS (Software-as-a-Service), les employés tendent à acheter et à implémenter trop facilement de nouvelles extensions et applications, sans en avertir le service informatique. Salesforce peut rapidement se retrouver truffé de composants qui ne sont ni vérifiés, ni monitorés pour rechercher les vulnérabilités ou les activités suspectes.

« La complexification est l'ennemi de la sécurité. Plus un environnement est complexe, plus il est probable qu'un composant soit négligé ou mal configuré. Salesforce est une plateforme hautement personnalisable. Les mauvaises configurations possibles sont donc nombreuses. »

Dmitriy Viktorov, Head of Product and Technology, Cloud Protection, WithSecure™

# Les fichiers et liens malveillants dans Salesforce sont en augmentation

**Détection de fichiers / URL par client et par mois**




**Au cours des 6 derniers mois, le volume de détection de fichiers et de liens malveillants a augmenté de 250 %.**

**Top 5 des détections malveillantes, par type de fichier**

1. HTML 49 %
2. Archives rar/zip 23 %
3. Microsoft Office 10%
4. Exe/com 4 %
5. PDF 3%

*6 derniers mois

**Les 5 principaux types de malwares**

1. Chevaux de Troie 54%
2. Adwares 15%
3. Exploits 12%
4. Autres 12%
5. Téléchargeurs 2%

*6 derniers mois

Les tentatives d'attaques sont en constante augmentation. Ce constat, largement partagé, est confirmé par nos données issues du monitoring des environnements Salesforce. Au cours des six derniers mois, nous avons détecté en moyenne 57 fichiers ou liens malveillants, par client et par mois. Ce chiffre représente une augmentation de 274 % par rapport à la moyenne des six mois précédents.

Les fichiers HTML malveillants constituent la méthode d'attaque la plus populaire : ils représentent plus de la moitié des fichiers détectés. Parmi les tentatives d'attaques par malware que nous avons identifiées, la majorité sont des chevaux de Troie.

Nous avons également relevé plusieurs tendances qui semblent indiquer que les pirates informatiques assurent une veille des actifs Salesforce. Par exemple, si un client implémente Salesforce Experience Cloud et crée un portail pour l'upload de contenus, le nombre de fichiers et de liens détectés augmente rapidement par la suite.

Il est intéressant de noter que les liens malveillants sont plus nombreux que les fichiers. Les hackers savent que de plus en plus d'entreprises analysent efficacement les fichiers, mais travaillent encore à détecter les URL malveillantes.

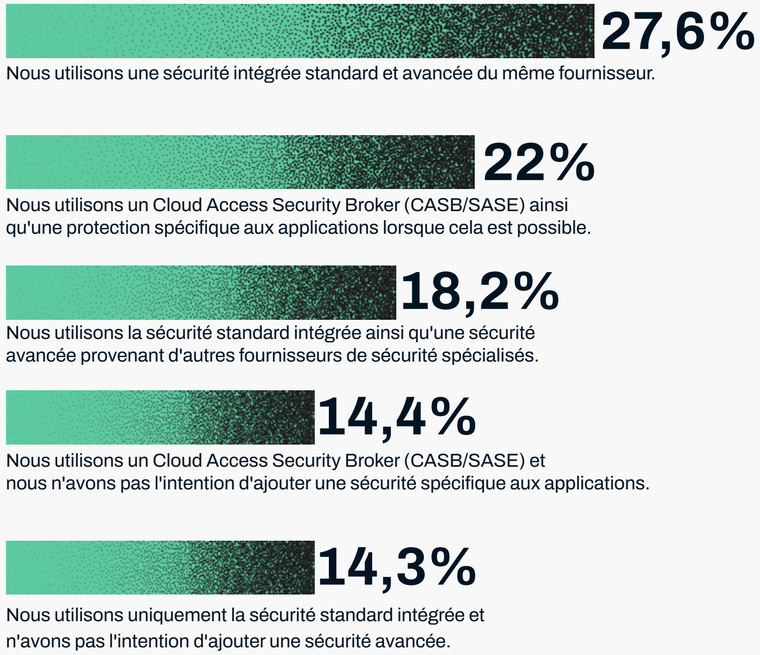
« Tout le monde sait qu'il faut rechercher des fichiers malveillants. Pour autant, l'analyse des URL ne constitue pas toujours une pratique standard, surtout hors-messagerie. »

Doug Merrett, Salesforce Security, Compliance, Privacy and Resilience Specialist, Platinum7

# Choisir les contrôles de sécurité adéquats

**Parmi les énoncés suivants concernant la sécurité des applications cloud, lesquels s'appliquent le mieux à votre entreprise/ organisation ?**

(ex : Office 365, Google Workspace, Salesforce)




D'après nos recherches, les organisations présentent des capacités de sécurisation du cloud extrêmement disparates. La plupart des professionnels interrogés affirment utiliser plusieurs applications de sécurité spécifique, mais d'autres misent uniquement sur les capacités de sécurité natives de leur plateforme ou application cloud.

Les outils intégrés constituent un bon point de départ. Ils ont l'avantage d'être souvent conçus par le fournisseur de l'application mais ils présentent généralement des lacunes importantes. Par exemple, Salesforce n'assure pas la sécurité des données non-structurées et ne dispose d'aucune fonctionnalité native permettant d'analyser les téléchargements et les uploads.

Pour bien faire, les entreprises doivent associer la sécurité native de Salesforce à des outils de sécurité spécialisés d'au moins un fournisseur tiers, afin de combler les lacunes. Mieux vaut se limiter à un seul fournisseur tiers. Dans le cas contraire, les équipes doivent gérer de multiples flux de données non-corrélées et des alertes de menaces de tout venant. Les CASB (Cloud Access Security Broker) fonctionnant comme des proxies peuvent être difficiles à implémenter car ils doivent être configurés spécifiquement pour chaque produit SaaS. Les CASB par API et les solutions conçues de manière intégrée sont plus utiles, et offrent une plus grande polyvalence.

« Les outils intégrés des fournisseurs couvrent rarement tous les besoins, mais ils peuvent être très efficaces car les développeurs connaissent très bien le système. Le fait de disposer d'un outil spécialisé supplémentaire permet d'atteindre un certain équilibre en couvrant les différentes lacunes. »

Pankaj Paryani, Salesforce Technical Lead, WithSecure™

# Nos huit principales recommandations pour sécuriser Salesforce en 2023

Les grands dossiers 2022 de la sécurité permettent de définir les priorités pour l'année à venir. Voici les aspects qui, d'après nos experts, méritent votre attention :

## 1. La gestion des identités et des accès

Une meilleure gestion des accès offre très rapidement des avantages significatifs. L'authentification multifactorielle (MFA) réduit immédiatement le risque de violation de données. Cette fonctionnalité est désormais incluse en standard dans Salesforce et peut donc être déployée rapidement et sans coût supplémentaire.

Vous devez mettre en place une politique du moindre privilège pour accéder au système, tant pour les utilisateurs que pour l'intégration des API : vous réduirez ainsi considérablement votre surface d'attaque. Bien que ce processus soit plus lent, il n'en est pas moins extrêmement important.

## 2. Le monitoring des menaces entrantes

Les pirates informatiques ne se contentent plus de mener des attaques par e-mail. La fonction d'upload dans Salesforce et les canaux de communication intégrés comme Chatter peuvent être exploités à des fins malveillantes, dans des attaques de malware ou de phishing. La plateforme Salesforce ne dispose pas de capacités natives pour le monitoring des contenus. WithSecure™ Cloud Protection for Salesforce a été conçu en collaboration avec Salesforce pour analyser en temps réel tous les contenus entrants et sortants, pour identifier et bloquer les fichiers et liens malveillants.

## 3. Suivre l'évolution des réglementations en matière de confidentialité et de conformité

Le paysage réglementaire ne cesse d'évoluer. Respecter les réglementations en perpétuel changement peut s'avérer difficile, surtout face au grand nombre de composants mobiles présents dans les environnements Salesforce. Commencez par adopter une approche stricte du moindre privilège, avec un accès minimal par défaut. Et pour les réglementations impliquant des tiers, un contrôle strict doit être mis en place pour prévoir les responsabilités de chacun.

## 4. Ne négligez pas les outils intégrés

Salesforce inclut par défaut un certain nombre d'outils très utiles. Assurez-vous d'en tirer le meilleur parti avant d'investir dans des solutions tierces. Health Check et Optimizer, par exemple, peuvent vous aider à mettre en évidence les mauvaises configurations et contrôles d'accès perdus.

« Salesforce s'efforce de sécuriser son infrastructure mais les utilisateurs doivent reconnaître leur part de responsabilités et sécuriser leurs instances cloud. Salesforce est chaque jour ou presque la cible d'attaques. Il n'y a donc pas de temps à perdre. »

Doug Merrett, Salesforce Security, Compliance, Privacy and Resilience Specialist, Platinum7

« Un monitoring efficace des utilisateurs est indispensable. Il permet non seulement de stopper les pirates informatiques et les initiés malveillants, mais aussi d'empêcher les accidents et les mauvaises configurations. »

Doug Merrett, Salesforce Security, Compliance, Privacy and Resilience Specialist, Platinum7

## 5. Des sauvegardes efficaces

Les ransomwares cherchent à endommager ou à détruire vos données CRM. Face à ces attaques, les sauvegardes fiables sont votre plus grand atout. Si vous êtes en mesure de restaurer votre instance Salesforce, l'impact sera drastiquement réduit. Les sauvegardes offrent également un niveau supplémentaire de protection contre l'erreur humaine : si une mauvaise configuration ou une mauvaise intégration d'application pose problème, vous pourrez activer la procédure de restauration.

## 6. Faites preuve de discernement

Votre environnement Salesforce va continuer de s'étendre. Au moment d'implémenter une nouvelle application ou un nouveau plug-in tiers, renseignez-vous sur son fournisseur. Vérifiez s'il est fiable et digne de confiance. Pour vous aider, la communauté Salesforce publie des rapports précis sur la boutique AppExchange. Les avis des clients peuvent être mis à jour : il peut donc être utile de les consulter régulièrement.

## 7. Activez le monitoring des événements

Le monitoring des événements joue un rôle essentiel : il vous permet de bien comprendre comment fonctionne votre environnement Salesforce. Vous pouvez voir comment les utilisateurs et les applications accèdent à vos données stratégiques. Cette visibilité est essentielle pour protéger votre plateforme Salesforce contre les tentatives d'attaques externes et contre les risques internes, malveillants ou accidentels. Les données forensiques issues de ce monitoring ne sont utiles que si elles peuvent être correctement interprétées. Des outils comme Splunk et Imprivata FairWarning peuvent donc vous être d'une aide précieuse.

## 8. Protégez les données sensibles

Les données de votre entreprise sont d'une importance capitale. Chaque bit, chaque octet mérite d'être protégé. Accordez une attention particulière aux données clients et aux données sensibles. Utilisez Salesforce Shield ou d'autres solutions tierces pour identifier, chiffrer, monitorer et conserver les données sensibles.

« Salesforce améliore continuellement ses capacités de lutte contre les menaces comme le phishing grâce à de nouvelles fonctionnalités intégrées. Mais les utilisateurs ont aussi un rôle à jouer pour implémenter et utiliser correctement ces outils. »

Pankaj Paryani, Salesforce Technical Lead, WithSecure™

« Ces deux dernières années, les attaques de la supply chain ont constitué un problème majeur. Elles ne vont pas disparaître du jour au lendemain. Les entreprises doivent mieux comprendre leurs environnements numériques étendus, et mieux les sécuriser. »

Dmitriy Viktorov, Head of Product and Technology, Cloud Protection, WithSecure™

WithSecure™ Cloud Protection for Salesforce complète les capacités de sécurité natives de Salesforce en maîtrisant les risques liés aux fichiers et liens uploadés.

Nous contacter

salesforce PARTNER SINCE 2016

## Sources des données

L'étude de marché B2B WithSecure™ 2022 a été menée auprès de 3072 professionnels, en mai 2022, par le biais d'une enquête en ligne dans 12 pays, dont 9 pays européens (le Royaume-Uni, la France, l'Allemagne, la Belgique, les Pays-Bas, les Danemark, la Finlande, la Norvège, la Suède), les États-Unis, le Canada, et le Japon. Tous les professionnels interrogés sont des décideurs ou des influenceurs en sécurité informatique/réseau/cloud. Ils influencent ou décident de l'achat de produits et de services de sécurité informatique/réseau/cloud au sein de leur organisation.

Les chiffres mentionnés sont tirés de données internes anonymes. Ces données ont été recueillies via des demandes d'analyse de menaces reçues dans des environnements Salesforce protégés par WithSecure™.

Salesforce's Top Data Trends for 2022 – Rapport basé sur une enquête menée par Salesforce et Pulse auprès de 300 responsables InfoSec et informatiques.

# Qui sommes-nous ?

WithSecure™ est le partenaire européen de référence en matière de cybersécurité depuis plus de 30 ans. Nous accompagnons les fournisseurs de services informatiques, les MSSP et des multinationales, qui nous font confiance, à travers des modèles commerciaux flexibles et adaptés au marché. Nous leur fournissons une cybersécurité axée sur les résultats, pour les protéger en toutes circonstances et garantir le bon fonctionnement de leurs activités.
Notre protection basée sur l'IA sécurise les endpoints et protège les environnements cloud. Nos outils intelligents de détection et de réponse sont pilotés par des experts qui identifient les risques, assurent une recherche proactive des menaces et neutralisent les attaques en temps réel. Un service de consulting expert est également disponible pour les entreprises qui souhaitent renforcer leur résilience.

WithSecure™, anciennement F-Secure Corporation, a été fondée en 1988 et est cotée au NASDAQ OMX Helsinki Ltd.

W / T H®
secure