

Les 4 fondamentaux que chaque administrateur Salesforce doit savoir sur la sécurité du cloud

Qu'est-ce que la sécurité du cloud ?

Les infrastructures, plateformes, applications et services cloud gagnent en popularité et les pirates informatiques en profitent : ils voient en ces nouvelles technologies de nouveaux vecteurs d'infiltration. Si vous ne protégez pas votre cloud, vous vous exposez à des vols de données, à des ransomwares et à d'autres attaques. Ces manœuvres malveillantes risquent de perturber vos opérations, de compromettre votre réputation, voire même d'être en infraction au regard des réglementations en vigueur. Le concept de sécurité du cloud renvoie aux technologies, processus et ressources que les entreprises déploient pour rester protégées contre les attaques... mais malheureusement, beaucoup d'entreprises négligent cet aspect de leur protection.

Sécuriser ses systèmes à l'ère du cloud

Réduction des coûts d'exploitation, flexibilité opérationnelle, travail à distance... Les entreprises se tournent vers le cloud pour de nombreuses raisons. Et les exigences de distanciation sociale liées à la pandémie sont venues accélérer les choses. Ce faisant, Salesforce s'est positionné comme l'une des plateformes les plus populaires auprès des entreprises.

La généralisation du cloud semble vouée à se poursuivre. D'après une récente enquête menée par Gartner auprès de directeurs financiers, 74 % des entreprises s'attendent à ce qu'une partie de leurs employés travaillent à distance sur le long terme, et 17% d'entre elles estiment que les télétravailleurs représenteront au moins 20 % de leurs effectifs¹. Les plateformes cloud sont également de plus en plus utilisées pour des opérations critiques, qu'il s'agisse du partage de documents sensibles ou de collaborations avec les clients et partenaires.

Le cloud constitue un atout évident en termes de productivité mais les entreprises peinent à évaluer les risques inhérents à ce nouvel environnement de travail. Du fait de leur popularité croissante, les offres cloud SaaS (Software-as-a-Service) telles que Salesforce, Microsoft 365 et Google Workspace constituent des cibles d'attaques particulièrement attrayantes... et les pirates informatiques se montrent désormais redoutables au moment de cibler les failles de sécurité des entreprises. Bien souvent, ils ne s'attaquent pas directement aux données stockées dans le cloud : ils préfèrent utiliser les services cloud comme tremplin, pour s'introduire ensuite sur des systèmes internes et externes. Nous avons d'ores-et-déjà pu observer des attaques de phishing et de ransomwares menées via des services cloud.

Nos experts vous révèlent ici quatre secrets qui vous aideront à utiliser Salesforce et d'autres services cloud, en toute sécurité.

1. <https://www.gartner.com/en/newsroom/press-releases/2020-04-03-gartner-cfo-surey-reveals-74-percent-of-organizations-to-shift-some-employees-to-remote-work-permanently2>

Secret n°1

Gagnez en visibilité et en contrôle

Lorsque vous transférez des données vers un service cloud comme Salesforce, il vous faut maintenir une visibilité totale et un contrôle absolu : vous devez savoir quelles données vous stockez, comment elles sont classées, d'où elles proviennent, qui peut y accéder, et où elles sont envoyées. Dans le cas de sources externes, inconnues ou non-fiables (via e-mail, par exemple), vous devez pouvoir les bloquer les contenus malveillants ou non-autorisés, avant qu'ils ne parviennent aux utilisateurs internes ou externes.

Vous devez également vous assurer que vous n'êtes pas en infraction vis-à-vis des réglementations relatives aux différents secteurs, marchés et territoires dans lesquels vous exercez votre activité. Pensez, par exemple, au RGPD de l'Union européenne, ou bien à la norme de sécurité des cartes de paiement PCI-DSS.

Vous devez aussi pouvoir détecter tout accès non-autorisé aux données et repérer efficacement les initiés malveillants : pour ce faire, il ne suffit pas de rechercher uniquement les menaces connues : vous devez également assurer un monitoring efficace des activités et des comportements utilisateurs.

Enfin, vous devez monitorer et contrôler l'accès à toute donnée sensible, et conserver une piste d'audit complète.

Secret n°2

Identifiez vos propres responsabilités et comblez les failles de protection de votre environnement cloud

Bien souvent, les entreprises négligent leurs responsabilités en matière de sécurisation cloud. Même si les fournisseurs cloud garantissent généralement la sécurité de leurs plateformes avec des accréditations et des certificats impressionnants, les entreprises clientes ont, elles aussi, certains devoirs. Elles sont pourtant nombreuses à l'ignorer.

Lorsque vous souscrivez à des services cloud comme Salesforce, vous acceptez un modèle de sécurité à responsabilité partagée. Les fournisseurs s'engagent par contrat à garantir la sécurité de leurs systèmes au niveau de l'infrastructure et de la plateforme. De votre côté, vous devez veiller à ce que les contrôles de sécurité cloud fournis par votre fournisseur soient toujours correctement configurés.

Vous devez également veiller à la protection de vos données. Les responsabilités précises peuvent varier d'un fournisseur à l'autre, mais dans l'ensemble, le principe reste le même.

Secret n°3

Assurer une bonne configuration cloud, malgré une complexité croissante

Gérer les services et applications cloud peut vite devenir très complexe. Les mauvaises configurations sont fréquentes, et les contrôles d'accès sont souvent insuffisants. Malheureusement, ces lacunes peuvent conduire à des violations de données.

Les API présentent, elles aussi, des risques : si ces interfaces sont mal configurées ou si elles bénéficient de plus d'autorisations que nécessaire, elles peuvent également déboucher sur un vol de données.

Il s'agit de véritables défis à relever pour les administrateurs de Salesforce, qui sont aussi confrontés à un flux constant de demandes de changements : ils doivent ajouter de nouvelles fonctionnalités, exploiter les fonctionnalités avancées de la plateforme ou encore déployer des applications, des services et des modules complémentaires tiers à partir de Salesforce AppExchange. Pour les aider, il est possible de déployer des solutions de détection des menaces cloud ou encore des outils CSPM (Cloud Security Posture Management), afin de détecter automatiquement les configurations dangereuses ou non-conformes.

Secret n°4

Neutraliser les attaques de la supply chain

Même lorsque votre plateforme ou service cloud est correctement configuré, il existe un risque lié aux intégrations ou applications tierces connectées par API. Vous devez anticiper le fait que des systèmes connectés à votre cloud puissent être piratés, via une vulnérabilité logicielle ou une mauvaise configuration. Attention aux attaques « de la supply chain » : des cybercriminels sont susceptibles de cibler des entreprises tierces pour arriver jusqu'à vous, en infiltrant votre réseau via des techniques de déplacement latéral.

Par exemple, en 2019-2020, une porte dérobée présente sur le système de gestion de réseau SolarWinds a été piratée : les hackers ont ainsi pu infiltrer les systèmes de plusieurs agences gouvernementales américaines. Plus récemment, une vulnérabilité de l'utilitaire de journalisation Java Log4j a exposé environ 93 % des environnements cloud professionnels à un risque d'attaque (source : Wiz/EY). Bien que de nombreux systèmes aient été corrigés depuis, il est probable que la vulnérabilité de Log4j continue de poser problème à l'avenir dans la

mesure où cet utilitaire est extrêmement répandu... Il est même souvent installé de manière invisible par d'autres paquets nécessitant des composants Java particuliers pour fonctionner.

Si l'intégration entre votre cloud Salesforce et un partenaire/client/système tiers contient une vulnérabilité (comme celle de Log4j), un hacker risque de s'en servir pour infiltrer votre entreprise. Il est donc essentiel que vous monitoriez à la fois les menaces connues et les activités anormales qui pourraient indiquer une menace inconnue.

Qui a besoin d'une sécurité complémentaire pour Salesforce ?

WithSecure™ Cloud Protection for Salesforce⁸ offre une protection en temps réel contre les virus, les chevaux de Troie et les ransomwares. Cette solution analyse l'ensemble des contenus uploadés sur Salesforce et vient compléter les contrôles de sécurité intégrés de la plateforme. Toutes les données stockées ou partagées via Salesforce sont protégées : vous assurez ainsi votre conformité aux cadres réglementaires en vigueur.

WithSecure™ Cloud Protection for Salesforce vous permet de prévenir ou de neutraliser les attaques menées par le biais de fichiers malveillants ou de liens de phishing. Cette solution vous offre une visibilité accrue et fournit des analyses complètes. Avec elle, vous disposez d'informations détaillées sur tous les contenus consultés par des utilisateurs, internes ou externes.

Pour de nombreuses entreprises utilisatrices de Salesforce, il devient essentiel de déployer des outils complémentaires de protection comme WithSecure™ Cloud Protection for Salesforce.

Voici trois cas courants d'utilisation.

2. <https://www.withsecure.com/fr/solutions/software-and-services/cloud-protection-for-salesforce>



Cas d'utilisation n°1 : L'administrateur proactif

L'utilisation des systèmes et services cloud se généralise. Face à ce phénomène, certains administrateurs s'efforcent de sécuriser leur plateforme Salesforce. Ils savent que les menaces cloud, comme les ransomwares et les violations de données, sont en augmentation. Ils comprennent également leurs responsabilités partagées en matière de sécurité, même s'ils ne connaissent pas toujours les outils tiers disponibles pour les aider.

Ils se questionnent sur la sécurité de leur environnement Salesforce³ et effectuent des recherches via AppExchange pour connaître les applications de sécurité disponibles. Ils identifient alors des solutions comme WithSecure™ Cloud Protection for Salesforce. Lorsqu'ils comprennent que cette solution peut combler efficacement les failles de sécurité de Salesforce, ils mènent une analyse de rentabilité, puis lancent un exercice d'évaluation et d'acquisition.

3. <https://help.salesforce.com/s/articleView?id=000318378&type=1#FileUpload?>

Scénario d'utilisation n°2 : Le protecteur de portail

L'entreprise élargit son utilisation de Salesforce pour établir des liens avec ses partenaires et/ou clients, par exemple via Experience Cloud (anciennement connu sous le nom de Community Cloud). Elle ne dispose toutefois d'aucune certitude quant à la sécurité mise en place par ces tiers : elle n'est pas en mesure de garantir la sécurité des systèmes et appareils que ces derniers utilisent pour se connecter au portail. Si l'entreprise autorise des utilisateurs externes à uploader des contenus dans Salesforce (documentation, formulaires, liens), elle doit être en mesure d'empêcher des endpoints potentiellement corrompus d'introduire clandestinement des menaces, comme des malwares ou des liens de phishing.

À l'inverse, si - en interne - un fichier malveillant est uploadé dans Salesforce, il risque ensuite d'être téléchargé par un partenaire ou un client, ce qui s'avérerait très dommageable en termes de réputation.

L'entreprise ne peut pas non plus se permettre de mettre ses systèmes hors service en cas d'incident, car ses portails partenaires et clients sont au cœur de son offre commerciale, comme c'est souvent le cas pour les entreprises financières, les sociétés de recrutement, les agences de voyage et les autres prestataires de services professionnels.

Cas d'utilisation n°3 : Le contrôleur de la conformité

Une grande entreprise - ou bien une organisation opérant dans un secteur hautement réglementé comme la santé, les services financiers ou le gouvernement - doit respecter des règles de conformité strictes. Il peut s'agir de dispositions légales et réglementaires sur la protection des données, ou de règles de bonnes pratiques comme la norme de sécurité ISO 27001.

Un cadre supérieur (RSSI, CIO ou CEO) vérifie que les plateformes, applications et services cloud sont bien conformes aux politiques générales de sécurité de l'entreprise. Durant ce processus de vérification, les administrateurs réalisent qu'ils ont besoin d'outils supplémentaires pour protéger Salesforce. Ils choisissent donc de sécuriser les contenus avec des solutions comme WithSecure™ Cloud Protection, ou d'adopter une solution CSPM (Cloud Security Posture Management) pour garantir le respect des politiques et réglementations dans toute l'entreprise.

WithSecure™ Cloud Protection for Salesforce complète les capacités de sécurité natives de Salesforce. Cette solution analyse tous les fichiers, URL et e-mails, pour détecter les malwares au sein des environnements cloud Salesforce.

[Essai gratuit](#)

A propos de WithSecure™

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 environnement 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.

