CLOUDFLARE

LIVRE BLANC

Simplifier la façon dont nous protégeons les applications SaaS

Comment protéger les utilisateurs et les données à l'aide d'une approche Zero Trust

Contenu

Introduction

Dans l'environnement distribué d'aujourd'hui, les applications SaaS (Software as a Service) ont offert davantage de flexibilité aux entreprises, leur permettant de soutenir leur personnel et leurs sous-traitants à travers le monde. Parmi les suites d'applications SaaS les plus remarquables figurent actuellement les applications de communication (envoi d'e-mails, plateformes de chat), les applications de productivité (documents, tableurs) et les applications collaboratives (stockage en ligne). D'ici 2025, Gartner prévoit que 85 % des entreprises adopteront une approche orientée cloud pour gérer leur activité, et que l'approche SaaS deviendra le véhicule privilégié des déploiements de gestion des accès[1].

Si les applications SaaS permettent aux entreprises de rester plus agiles, l'adoption du cloud comporte toutefois certains risques en matière de sécurité et de performances, notamment pour les entreprises qui jonglent avec plusieurs solutions dédiées, conçues pour fonctionner indépendamment les unes des autres. Chargées de déployer et de gérer des dizaines, voire des centaines, de ces applications, les équipes responsables de la sécurité, des réseaux et de l'informatique manquent souvent de temps, peinent à obtenir une visibilité à l'échelle de l'organisation et luttent pour maîtriser les failles de sécurité et de connectivité résultant de services qui ne sont pas intrinsèquement conçus pour fonctionner ensemble.

De nombreuses entreprises se trouvent donc contraintes de trouver de meilleures manières de consolider les produits de sécurité de leur environnement SaaS, afin d'améliorer l'efficacité, de réduire les complexités liées à la gestion et au déploiement, mais aussi de bénéficier d'un support consolidé.

Gartner prédit que d'ici 2025, 80 % des entreprises adopteront des solutions à fournisseur unique permettant d'unifier l'accès au web, aux services de cloud et aux applications privées depuis une plateforme SSE (Security Services Edge)[2].

La migration vers une sécurité SaaS simplifiée s'accompagne de plusieurs considérations importantes. La façon dont le personnel communique et travaille aujourd'hui exige une approche simple et évolutive de la sécurité, conçue pour devancer les risques émergents, réduire les incidents résultant des applications SaaS et permettre aux équipes de sécurité de surveiller et prévenir facilement les menaces affectant leurs entreprises.

Lisez la suite pour découvrir comment une plateforme Zero Trust, intégrant des fonctionnalités de CASB (Cloud Access Security Broker) et de sécurité des e-mails dans le cloud (CES, Cloud Email Security), offre l'approche la plus simple pour mettre un terme aux pertes de données, au phishing, aux rançongiciels, à l'informatique fantôme (Shadow IT) et aux mouvements latéraux à l'échelle de votre entreprise.

[1] Gartner, « Forecast Analysis: Information Security and Risk Management, Worldwide. » Analystes : Shailendra Upadhyay, Mark Driver, Christian Canales, Ruggero Contu, Lawrence Pingree, Elizabeth Kim, John A. Wheeler, Nat Smith, Rahul Yadav, Swati Rakheja, Dave Messett, Mark Wah, Shawn Eftink. 12 août 2021. Gartner. [2] Gartner, « Predicts 2022 : Consolidated Security Platforms Are the Future. » Analystes : Charlie Winckless, Joerg Fritsch, Peter Firstbrook, Neil MacDonald, Brian Lowans. 1er décembre 2021. Gartner.

L'évolution des CASB

Une sécurité SaaS exhaustive nécessite plusieurs technologies cruciales, permettant aux équipes de sécurité d'obtenir une visibilité sur l'ensemble de leur environnement SaaS, de surveiller et d'atténuer facilement les menaces et de sécuriser l'accès aux données et systèmes sensibles. Un des composants les plus importants de toute stratégie de sécurité SaaS est un CASB (Cloud Access Security Broker), qui fournit des contrôles de sécurité des données, ainsi que de la visibilité sur les applications et les services hébergés au sein du cloud d'une entreprise.

Fondamentaux de la sécurité SaaS : les CASB

Un CASB permet aux équipes informatiques et de sécurité d'afficher tous les paramètres des données et l'activité des utilisateurs depuis un tableau de bord unique. Ses fonctionnalités varient selon les fournisseurs, mais incluent habituellement les attributs suivants[3] :

- **Protection des données :** les CASB protègent les données sensibles et les empêchent de quitter les systèmes contrôlés par l'entreprise.
- **Contrôle des accès :** les CASB permettent de contrôler plus facilement ce que les utilisateurs peuvent voir et faire dans les applications contrôlées par l'entreprise. Ils peuvent également fournir des fonctionnalités de vérification d'identité, afin d'assurer que les utilisateurs sont bien les personnes qu'ils prétendent être.
- **Détection de l'informatique fantôme :** les CASB aident à identifier les systèmes et services non autorisés (informatique fantôme ou « shadow IT ») utilisés par le personnel à des fins professionnelles. En cataloguant ces systèmes, les CASB peuvent détecter et atténuer des risques de sécurité précédemment inconnus.
- **Protection contre les menaces :** les CASB s'appuient sur des fonctionnalités de détection des logiciels malveillants, de sandboxing, d'inspection des paquets et d'autres technologies pour bloquer les fuites de données et les attaques externes.
- **Gestion du niveau de sécurité :** les CASB fournissent aux équipes de sécurité des données analytiques sur le comportement des utilisateurs et un contrôle du niveau de sécurité des applications, afin de leur permettre de surveiller facilement les mouvements et de traquer les menaces au sein de leur environnement SaaS.
- **Conformité :** les CASB aident les entreprises à se conformer aux exigences réglementaires (par exemple, SOC 2, HIPAA, GDPR, etc.) en identifiant les erreurs de configuration, et ainsi, à éviter les pénalités et amendes associées aux violations de la conformité.

[3] Il ne s'agit pas d'une liste exhaustive des fonctionnalités pouvant être incluses dans une offre de CASB.

Comprendre les défis des CASB modernes

À mesure que l'adoption du SaaS augmente, la surface d'attaque que doivent protéger les entreprises augmente également. À la place d'une base de données unique contenant des données précieuses, ces données sont maintenant disséminées dans des applications gérées par des tiers (par ex. Dropbox, Google Drive, etc.), qu'elles aient ou non été déployées dans un sandbox pour l'entreprise.

Si les CASB aident à protéger les données des entreprises et des utilisateurs dans les applications SaaS, ils ne constituent pas pour autant une panacée parfaite contre les menaces. Puisque le volume de données précieuses traité à l'aide d'applications SaaS devient plus important, les acteurs malveillants ciblent de plus en plus ces applications afin de perpétrer des violations de données et d'autres menaces. Par ailleurs, de simples erreurs de configuration et d'utilisation peuvent également ouvrir la porte à ces attaques :

Gartner prédit que plus de 99 % des violations du cloud d'ici 2025 seront dues à des erreurs de configuration ou à des erreurs commises par les utilisateurs[4].

Lorsqu'il s'agit d'anticiper et de remédier aux erreurs de configuration des utilisateurs et aux attaques contre les applications SaaS modernes, de nombreux CASB ne sont toujours pas à la hauteur. Pour remédier à ce problème, certains fournisseurs ont commencé à proposer des services de gestion du niveau de sécurité du cloud ou des applications SaaS (CSPM ou SSPM[5]), conçus pour identifier les erreurs de configuration et de conformité au niveau du plan de contrôle. Cependant, cette protection ne s'étend pas à tous les niveaux, ce qui laisse de nombreuses entreprises dépourvues de fonctionnalités de détection et de résolution indispensables.

Par ailleurs, certaines offres de CASB ne permettent pas d'identifier les violations de données avant qu'elles ne se produisent, entraînant une augmentation des coûts de résolution ainsi que des pertes de données, contraignant les équipes de sécurité à traquer inlassablement les auteurs d'attaques.

[4] Gartner, « Hype Cycle for Cloud Security, 2021. » Analystes : Tom Croll, Jay Heiser. 27 juillet 2021. Gartner.
[5] Ces services et fonctionnalités sont souvent proposés parallèlement à l'offre de produits CASB ou, plus couramment, sous forme de partie intégrante de l'offre, afin d'assurer aux applications une protection à la fois interne et orientée API.

Les difficultés liées à la mise en œuvre et à l'intégration des CASB

Tandis que les fournisseurs d'applications SaaS renforcent les fonctionnalités de leurs offres de sécurité intégrée, deux obstacles majeurs subsistent : l'intégration et la visibilité. Avec ces fournisseurs, les données deviennent accessibles et faciles à consommer, mais il incombe toujours aux entreprises de consolider les fonctionnalités de sécurité d'une manière facile à gérer. Pour les entreprises qui adoptent plusieurs solutions dédiées, le suivi des menaces sur différentes plateformes devient plus difficile lorsque ces solutions ne sont pas conçues pour s'intégrer les unes aux autres, ou lorsqu'elles offrent différents niveaux de visibilité.

Cette situation accroît la complexité de l'environnement des applications, rendant même les attaques basiques plus difficiles à anticiper et à atténuer, puisqu'il suffit aux acteurs malveillants d'identifier les failles entre les plateformes de sécurité pour lancer des attaques sans être détectés. Grâce à un CASB, les entreprises peuvent accéder aux produits de sécurité depuis un même endroit et ainsi bénéficier d'une meilleure visibilité, ainsi que de fonctionnalités d'atténuation sur l'ensemble de leur pile de sécurité.

Les CASB ne représentent néanmoins qu'un élément d'une stratégie de sécurité SaaS plus vaste. Pour couvrir l'ensemble de l'environnement SaaS, les entreprises doivent faire converger les fonctionnalités du CASB avec d'autres technologies Zero Trust, sans ajouter de complexité inutile ni contraindre les équipes de sécurité à configurer et gérer manuellement chaque outil. Le contrôle à grande échelle d'une application SaaS ne peut pas reposer sur un processus manuel. L'automatisation se révèle indispensable pour compléter les plateformes de gestion SaaS et les outils CASB, et permet aux entreprises d'atténuer efficacement de nombreuses menaces différentes sans risquer d'épuiser leurs équipes ni de devoir remédier à des configurations erronées et des erreurs d'utilisateurs.

L'évolution de la sécurité des e-mails

À l'image de la plupart des services SaaS, les communications par e-mail ont évolué, devenant une application professionnelle essentielle pour les entreprises de toutes tailles. Avec l'adoption du cloud et du télétravail, un nombre croissant d'entreprises se tournent vers les solutions d'e-mail dans le cloud intégrées à Microsoft 365 et Google Workspace (jusqu'à 70 % des entreprises dans le monde, selon Gartner)[6].

Par voie de conséquence, les e-mails constituent aujourd'hui l'application SaaS la plus largement adoptée et présentent l'une des plus vastes surfaces d'attaque, attirant les attaques par phishing, par logiciels malveillants, par usurpation d'identité, par compromission du courrier électronique professionnel (BEC) et d'autres menaces modernes.

Protéger l'entreprise contre les attaques véhiculées par e-mail peut toutefois s'avérer être une tâche fastidieuse et accablante pour les équipes de sécurité, d'autant plus que les acteurs malveillants continuent d'employer des tactiques de plus en plus sophistiquées contre des employés peu méfiants. Pour protéger les utilisateurs et les données contre ces menaces, les responsables de la sécurité devraient envisager d'intégrer les e-mails à leur plateforme de sécurité SaaS, d'une manière qui améliore la visibilité et offre une protection plus robuste et simplifiée.

Fondamentaux de la sécurité SaaS : la sécurité des e-mails

Le concept moderne de sécurité des e-mails englobe un ensemble d'outils, de processus et de techniques visant à protéger les comptes de messagerie et le contenu des e-mails contre les attaques malveillantes et les accès non autorisés. Parmi les technologies de sécurité des e-mails les plus répandues figurent les suivantes :

- **Passerelles de messagerie sécurisées (SEG, Secure Email Gateway) :** les passerelles de messagerie sécurisées traitent et filtrent le trafic SMTP. Elles contraignent les entreprises à modifier leur enregistrement MX, afin que ce dernier pointe vers leur agent de transfert d'e-mails.
- **Sécurité des e-mails dans le cloud (CES) :** une solution de sécurité des e-mails dans le cloud analyse le contenu des e-mails (via un accès par API aux fournisseurs d'e-mails dans le cloud) sans qu'il soit nécessaire de modifier l'enregistrement MX. (Remarque : Gartner désigne cette catégorie sous le nom de « ICES »
ou « CES intégrée ».)
- **DMARC (Domain-based Message Authentication Reporting and Conformance) :** le protocole DMARC authentifie les e-mails en vérifiant les enregistrements SPF (Sender Policy Framework) et DKIM (DomainKeys Identified Mail) d'un domaine. Dans ce système, les e-mails qui ne passent pas les vérifications SPF ou DKIM sont marqués comme indésirables ou bloqués et ne parviennent pas à leur destinataire.
- **Protection des données des e-mails (EDP, Email Data Protection) :** les solutions de protection des données des e-mails emploient le chiffrement pour éviter la perte accidentelle de données et interdire les accès non autorisés au contenu des e-mails.

---

[6] Gartner, « Market Guide for Email Security. » Analystes : Mark Harris, Peter Firstbrook, Ravisha Chugh, Mario de Boer. 7 octobre 2021. Gartner.

Comprendre les défis modernes en matière de sécurité des e-mails

Proposées à l'origine via des plateformes logicielles déployées sur site, les solutions de messagerie s'orientent de plus en plus vers des systèmes de diffusion cloud-native. De nombreuses entreprises ont adopté des suites de productivité dotées de fonctionnalités riches, telles que Microsoft 365 et Google Workspace, qui permettent aux utilisateurs de travailler et collaborer plus efficacement.

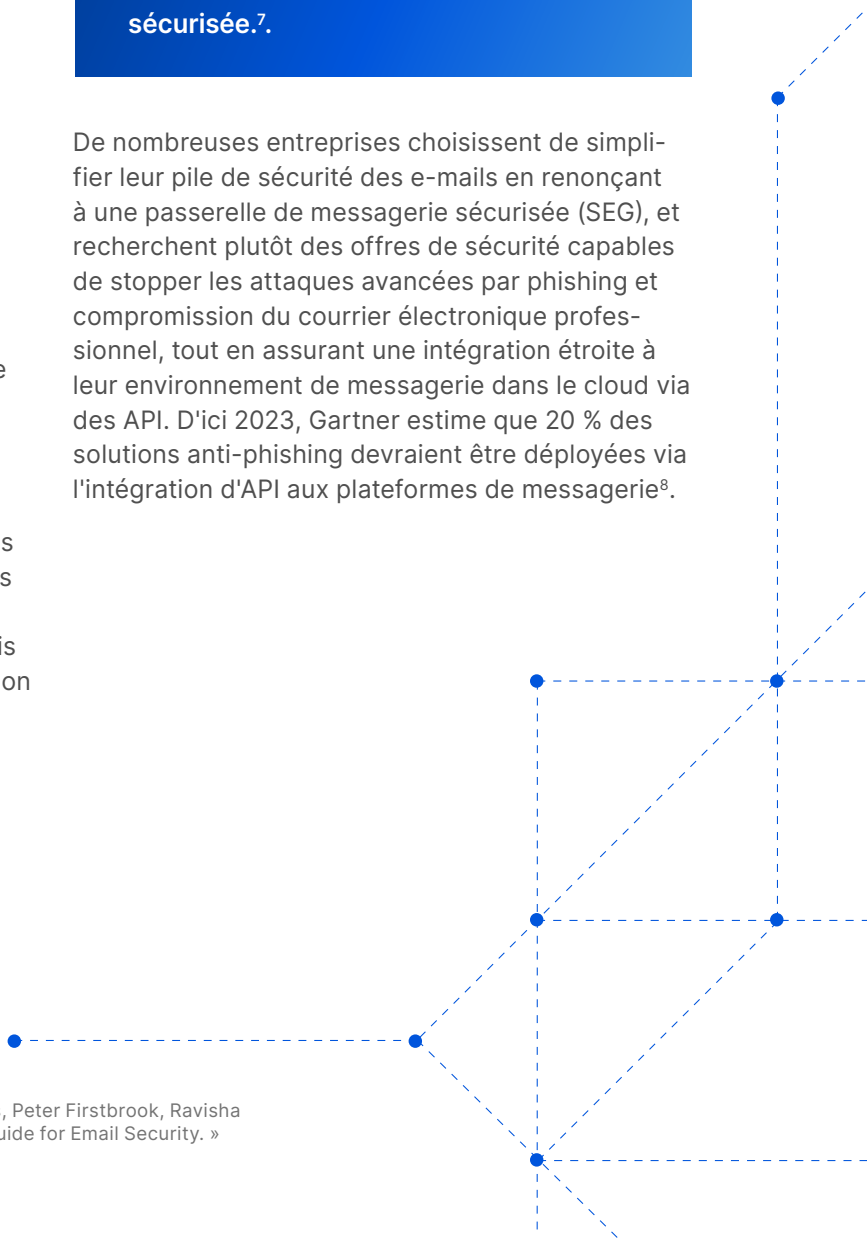
Les e-mails existent maintenant depuis longtemps. Même les utilisateurs occasionnels ont aujourd'hui conscience de certaines des menaces les plus courantes auxquelles ils peuvent être exposés par e-mail, notamment les e-mails suspects, les liens malveillants, etc. Les auteurs d'attaques ont donc fait évoluer leurs stratégies, et il devient désormais plus difficile de différencier les messages légitimes des messages malveillants. Ces menaces mixtes sont diffusées sur différents canaux de communication, afin de paraître plus légitimes (par exemple, vishing, smishing, etc.), et parviennent souvent à inciter les utilisateurs à divulguer des informations sensibles.

L'augmentation de l'utilisation des e-mails expose également les entreprises au risque de violations : lorsqu'un acteur malveillant a accès au compte de messagerie d'un utilisateur, il lui est souvent facile de se déplacer latéralement au sein d'une organisation et de compromettre ou voler des données sensibles. Toutefois, si les fournisseurs de messagerie dans le cloud proposent des fonctionnalités limitées de sécurité intégrée, conçues pour atténuer les menaces courantes, comme le courrier indésirable, les logiciels malveillants et le phishing, leur faiblesse face aux attaques provenant d'expéditeurs internes compromis (qui se déplacent latéralement d'une boîte de réception à l'autre) n'est plus à démontrer.

Pour combattre ces menaces, les solutions de sécurité des e-mails évoluent, elles aussi. Les plateformes de messagerie dans le cloud offrent un niveau basique de fonctionnalités de sécurité intégrée, permettant de gérer le courrier indésirable et les attaques courantes lancées par des logiciels malveillants.

D'ici 2023, Gartner estime qu'au moins 40 % des entreprises s'appuieront sur cette protection intégrée, plutôt que d'adopter des outils distincts, comme une passerelle de messagerie sécurisée.[7].

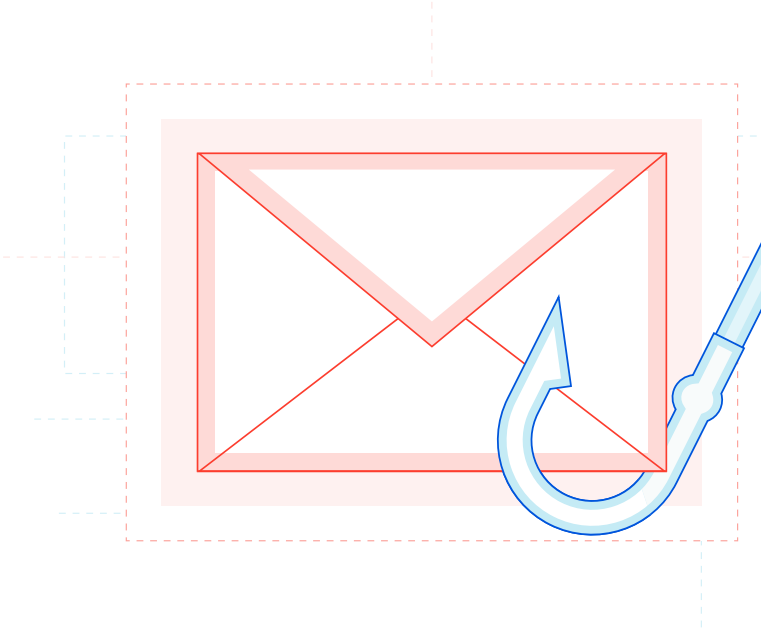
De nombreuses entreprises choisissent de simplifier leur pile de sécurité des e-mails en renonçant à une passerelle de messagerie sécurisée (SEG), et recherchent plutôt des offres de sécurité capables de stopper les attaques avancées par phishing et compromission du courrier électronique professionnel, tout en assurant une intégration étroite à leur environnement de messagerie dans le cloud via des API. D'ici 2023, Gartner estime que 20 % des solutions anti-phishing devraient être déployées via l'intégration d'API aux plateformes de messagerie[8].



[7] Gartner, « Market Guide for Email Security. » Analystes : Mark Harris, Peter Firstbrook, Ravisha Chugh, Mario de Boer. 7 octobre 2021. Gartner. [8] Gartner, « Market Guide for Email Security. »

Les difficultés liées à la mise en œuvre et à l'intégration de solutions de sécurité des e-mails

Si ces fonctionnalités intégrées offrent aux entreprises une certaine sérénité, elles sont loin d'être suffisantes pour lutter contre les menaces modernes liées aux e-mails. Des catégories entières d'attaques, telles que le spear phishing, les attaques BEC et bien d'autres, nécessitent des plateformes de sécurité dédiées que les fournisseurs de messagerie ne proposent pas. Par ailleurs, les solutions existantes de sécurité des e-mails ne sont pas conçues pour être évolutives, pour relever les défis propres au cloud ou pour contrer les attaques très ciblées.



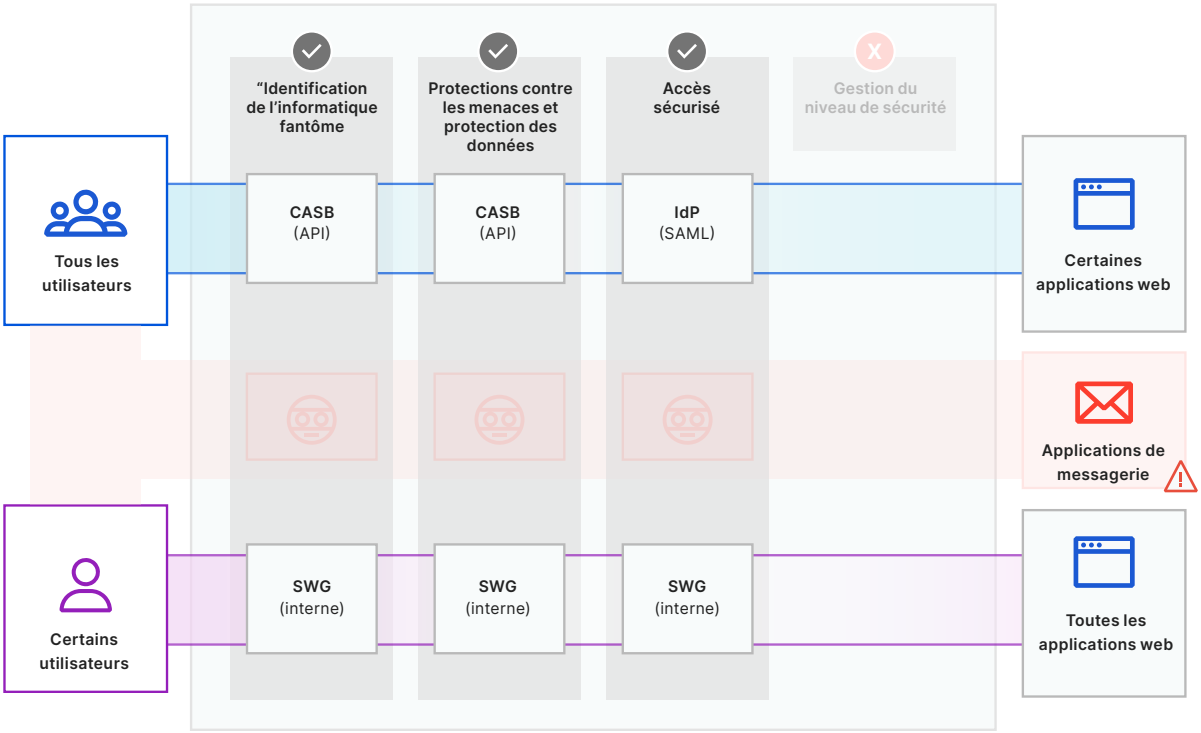
Même lorsque les équipes de sécurité identifient des outils de sécurité des e-mails conçus pour intercepter les menaces modernes, elles peuvent se heurter à d'autres problèmes : des exigences de configuration complexes, des processus de déploiement chronophages et des défis fastidieux liés à la maintenance des politiques. Par exemple, les produits de passerelle de messagerie sécurisée sont notoirement difficiles à déployer contre les attaques par e-mail, car la maintenance d'une liste toujours plus longue de politiques destinées à arrêter chaque variante d'attaque n'est pas toujours possible (ou réalisable dans le temps). La détection d'attaques avancées nécessite l'utilisation d'algorithmes à grande échelle, que seuls les services cloud-native sont capables de gérer.

Pour protéger les systèmes de messagerie pour entreprises contre ces attaques (sans pour autant surcharger les équipes de sécurité, superposer des solutions matérielles existantes ou compter sur le personnel pour intercepter chaque message malveillant), les entreprises doivent adopter une approche Zero Trust qui intègre des fonctionnalités de sécurité des e-mails cloud-native et réduisent la confiance implicite accordée aux communications par e-mail.

Une meilleure approche de la sécurité SaaS

Qu'il s'agisse de plateformes de communication ou de systèmes d'acheminement d'e-mails, les applications SaaS représentent une part importante des opérations actuelles des entreprises. Cependant, la protection de ces applications contre des menaces toujours plus complexes peut devenir un véritable cauchemar pour les équipes responsables de la sécurité, qui doivent souvent s'accommoder de différents outils, qui ne sont pas conçus pour s'intégrer nativement les uns aux autres et s'avèrent incapables d'offrir une visibilité sur l'ensemble de l'environnement SaaS d'une entreprise.

La sécurité SaaS traditionnelle

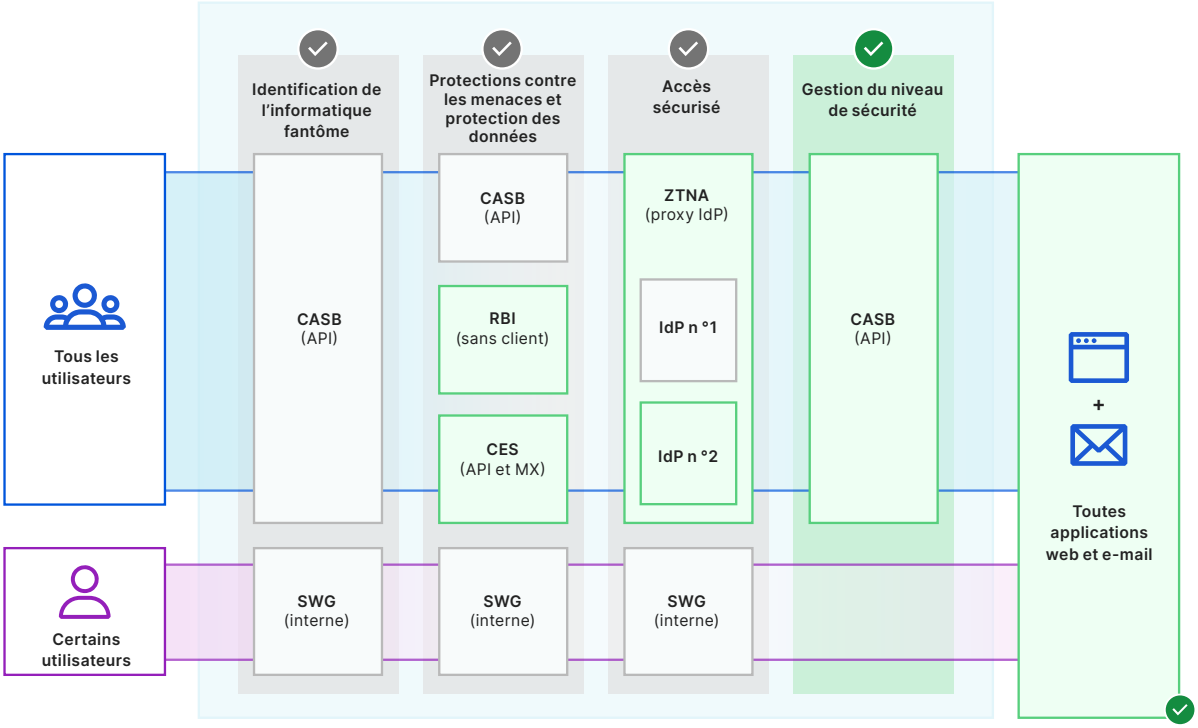


SWG = passerelle web sécurisée | CASB = Cloud Access Security Broker | IdP = fournisseur d'identité

À mesure que les fournisseurs ont élaboré des outils de sécurité SaaS plus robustes, les équipes informatiques et de sécurité ont été chargées d'assembler ces solutions ultra-performantes afin de sécuriser leurs applications et leurs données. Le déploiement et la gestion de ces solutions nécessitaient souvent beaucoup de temps et de ressources internes. En outre, si les solutions dédiées étaient capables de gérer les menaces au niveau individuel, il n'existait pas de plateforme globale offrant une prise en charge multi-fournisseurs et une visibilité à l'échelle de l'entreprise.

Souvent, les mesures de sécurité SaaS traditionnelles ne parvenaient pas non plus à étendre pleinement leurs protections aux plateformes de messagerie. Elles laissaient ainsi les entreprises vulnérables aux attaques ciblées qui imitaient les flux de travail essentiels à l'activité, usurpaient l'identité des partenaires et des utilisateurs de confiance, et contournaient facilement les systèmes de classification des e-mails et les contrôles intégrés existants. De même, en l'absence d'intégration native entre ces solutions (ou de visibilité sur l'ensemble de l'environnement des menaces), la protection des applications contre les menaces modernes entraînait finalement une nécessité pour les équipes de sécurité de combler un nombre encore plus grand de lacunes.

La sécurité SaaS moderne



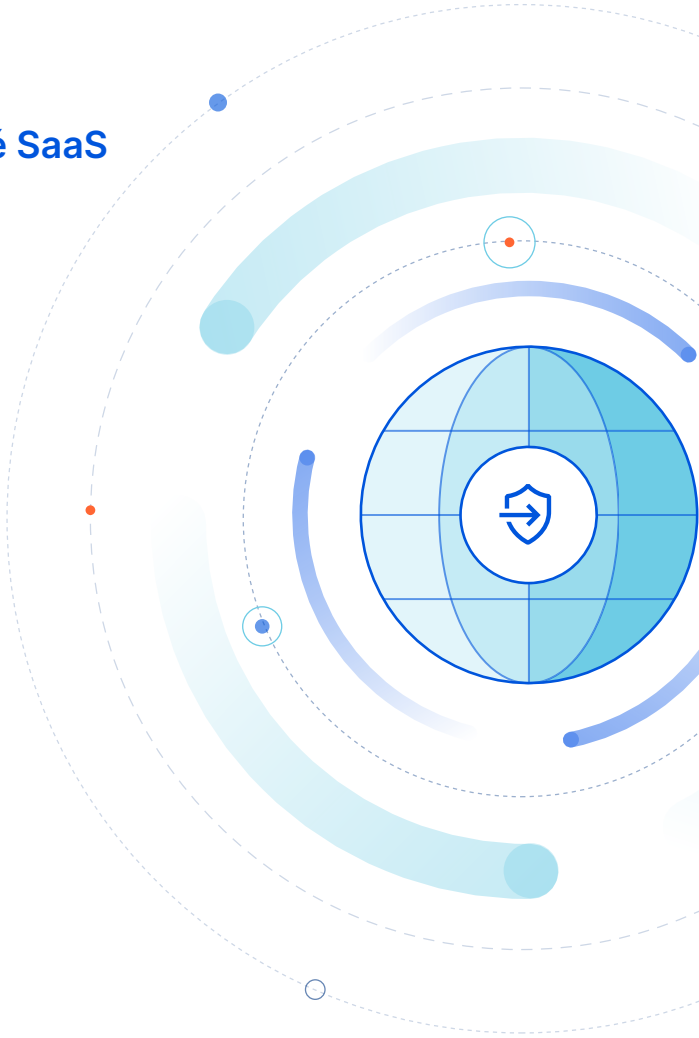
SWG = passerelle web sécurisée | CASB = Cloud Access Security Broker | IdP = fournisseur d'identité | RBI = isolation de navigateur à distance CES = sécurité des e-mails dans le cloud | ZTNA = accès réseau Zero Trust

Pour combler les lacunes laissées par les solutions traditionnelles de sécurité et de gestion des applications SaaS, les entreprises doivent disposer d'une protection moderne contre les menaces, conçue pour sécuriser les applications et les données depuis une plateforme unique, native d'Internet. Une composante vitale de cette approche moderne est la gestion robuste du niveau de sécurité, qui permet aux équipes de sécurité de mieux déterminer de quelle manière les utilisateurs accèdent aux ressources vitales, tout en bénéficiant d'une visibilité et d'un degré de contrôle sur les menaces externes et internes.

Au lieu d'exiger des entreprises qu'elles gèrent des outils dédiés pour remédier aux menaces individuelles, une plateforme de sécurité SaaS peut analyser les applications afin de détecter les anomalies dans la configuration, les autorisations et le partage, puis permettre aux équipes de sécurité de gérer l'accès aux applications, d'atténuer les attaques véhiculées par e-mail, de bloquer les menaces internes et les partages de données risqués, etc.

Cette approche assure non seulement une protection plus solide et plus complète des applications SaaS, mais permet également aux entreprises de gagner du temps lors de la gestion des tickets, d'automatiser les processus de sécurité et de se concentrer sur des initiatives stratégiques, plutôt que de se préoccuper des fuites de données, des attaques ou des opérations manuelles de configuration et d'entretien.

Appliquer l'approche Zero Trust à la sécurité SaaS



L'élaboration d'une approche adéquate de la sécurité SaaS nécessite une vue d'ensemble des menaces modernes liées à l'architecture SaaS et au cloud. L'adaptation des solutions existantes aux besoins d'une entreprise peut toutefois représenter une lourde tâche pour les équipes informatiques et de sécurité. Au lieu de combattre les menaces au niveau individuel (ou de se fier à un assemblage hétéroclite d'outils cloisonnés), les entreprises doivent disposer d'une plateforme de sécurité simplifiée, facile à gérer et capable d'anticiper et d'atténuer les menaces modernes.

Si les fonctionnalités de sécurité du CASB et de la messagerie dans le cloud constituent des éléments essentiels d'une stratégie de sécurité des applications SaaS, elles sont conçues pour s'exécuter de manière optimale dans le cadre d'une architecture Zero Trust, dans laquelle chaque composant technologique fonctionne mieux avec d'autres que seul. Correctement mise en œuvre, cette superposition contribue également à atténuer les problèmes adjacents en éliminant les failles de sécurité, en conservant la bande passante de l'équipe de sécurité et en automatisant la surveillance des menaces.

Comment Cloudflare protège les applications SaaS

Cloudflare propose le moyen le plus facile de protéger l'ensemble du paysage SaaS afin de permettre aux entreprises de contrôler la façon dont les utilisateurs accèdent aux ressources vitales, mais aussi dont elles protègent ces ressources contre les attaques externes ou internes, ainsi que la manière dont elles surveillent et atténuent les risques en temps réel.

*Rejoignez la liste d'attente de notre solution de prévention des pertes de données

Sécuriser les applications SaaS avec Cloudflare Zero Trust

Pour sécuriser les données en transit, Cloudflare Zero Trust place les mesures de contrôle de l'accès Zero Trust (ZTNA), de la passerelle web sécurisée (SWG) et de l'isolation de navigateur en amont de vos applications SaaS, afin qu'elles se comportent comme une architecture de déploiement de CASB interne.

Pour sécuriser les données au repos dans les applications SaaS, des intégrations orientées API et faciles à configurer analysent continuellement vos applications les plus fréquemment utilisées, à la recherche de vulnérabilités et de menaces potentielles.

Réunir la sécurité des e-mails de Cloudflare Area 1 et Cloudflare Zero Trust

La solution de sécurité des e-mails Cloudflare Area 1 fournit des solutions de sécurité intégrée des e-mails dans le cloud, afin d'assurer davantage de flexibilité aux entreprises en fonction de leurs besoins en matière de sécurité des e-mails. Pour ce faire, elle s'intègre via une API et se comporte comme une passerelle permettant de vérifier, de filtrer, d'inspecter et d'isoler le trafic de messagerie interne, via des modifications d'enregistrements MX.

Area 1 sonde Internet de manière préventive afin d'identifier les infrastructures utilisées pour lancer des attaques et des campagnes de phishing, afin de protéger les clients contre ces dernières avant qu'elles n'atteignent leurs boîtes de réception.

Pour en savoir plus sur la façon dont Cloudflare contribue à sécuriser les applications SaaS, rendez-vous sur https://www.cloudflare.com/fr-fr/products/zero-trust/.

Sources

1. Gartner, « Forecast Analysis: Information Security and Risk Management, Worldwide. » Analystes : Shailendra Upadhyay, Mark Driver, Christian Canales, Ruggero Contu, Lawrence Pingree, Elizabeth Kim, John A. Wheeler, Nat Smith, Rahul Yadav, Swati Rakheja, Dave Messett, Mark Wah, Shawn Eftink. 12 août 2021. Gartner.

2. Gartner, « Predicts 2022: Consolidated Security Platforms Are the Future. » Analystes : Charlie Winckless, Joerg Fritsch, Peter Firstbrook, Neil MacDonald, Brian Lowans. 1er décembre 2021. Gartner.

4. Gartner, « Hype Cycle for Cloud Security, 2021. » Analystes : Tom Croll, Jay Heiser. 27 juillet 2021. Gartner.

6. Gartner, « Market Guide for Email Security. » Analystes : Mark Harris, Peter Firstbrook, Ravisha Chugh, Mario de Boer. 7 octobre 2021. Gartner.

7. Gartner, « Market Guide for Email Security. » Analystes : Mark Harris, Peter Firstbrook, Ravisha Chugh, Mario de Boer. 7 octobre 2021. Gartner.

8. Gartner, « Market Guide for Email Security. » Analystes : Mark Harris, Peter Firstbrook, Ravisha Chugh, Mario de Boer. 7 octobre 2021. Gartner.

+33 7 57 90 52 73 | enterprise@cloudflare.com | www.cloudflare.com/fr-fr/

RÉV. : BDES-3303.2022JUN24