Guide d'achat de la

sécurité CASB nouvelle génération

Sommaire

L'adoption du SaaS évolue à un rythme soutenu

La pandémie n'a fait qu'intensifier l'adoption des applications SaaS, qui continuent de transformer les usages en entreprise.

Pour rester compétitives et asseoir leur position sur le marché, les entreprises cherchent à atteindre le plus rapidement possible une rentabilité et une productivité optimales. En ce sens, la simplicité, l'intelligence et la disponibilité universelle des applications SaaS (Software as a Service) les aident à atteindre ces objectifs.

Vue sous cet angle, la croissance accélérée du marché des produits SaaS sur cloud (Salesforce, HubSpot, Google Apps, Zoom, etc.) n'a donc rien d'étonnant. Comme le SaaS fut le premier service cloud à s'être réellement démocratisé, il possède une bonne longueur d'avance sur les autres services dématérialisés. Ainsi, d'après Gartner, le SaaS devrait rester le plus grand poste de dépense des budgets IT à l'échelle mondiale dans les années à venir.

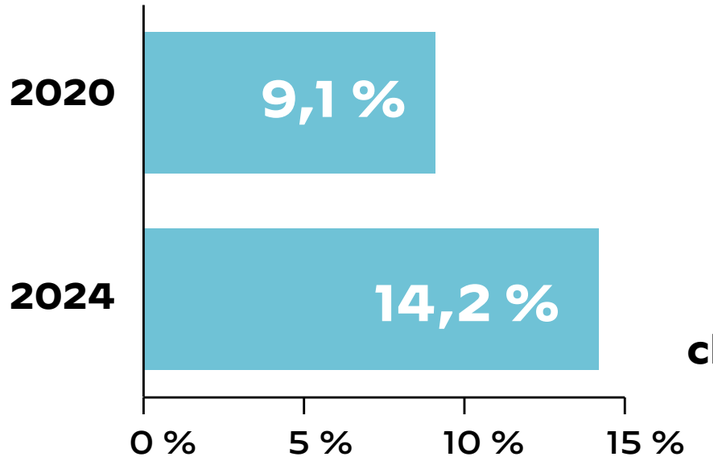
Le cabinet évalue à **23,1 %** l'augmentation des dépenses en services cloud publics en 2021, soit un total de **332,3** milliards de dollars, contre 270 milliards en 2020, d'après son précédent rapport prévisionnel. Le SaaS d'entreprise représente encore le plus large segment de marché pour les dépenses IT mondiales et devrait atteindre **145,3 milliards** de dollars en 2022.

50 %

Taux d'augmentation des dépenses globales en produits SaaS par entreprise en 2020.

30 %

Pourcentage annuel d'augmentation du nombre d'applications autorisées utilisées par entreprise en 2020.



Estimation mondiale de la hausse des dépenses IT d'entreprise consacrées au cloud d'ici 2024.

Le cloud du futur restera placé sous le signe de la disruption. Il permettra aux entreprises d'adopter la containerisation, la virtualisation et l'edge computing, autant de technologies émergentes sur le point de se généraliser.

Sources :

– Rapport Blissfully sur les tendances du SaaS, 2020
– « Gartner Forecasts Worldwide Public Cloud End-User Spending to Grow 23% in 2021 »

L'explosion du SaaS sème le chaos

La multiplication des applications SaaS au sein des différents départements fait apparaître de sérieuses difficultés de gestion.

Alors que le SaaS transforme peu à peu les méthodes de travail des entreprises de toutes tailles, le phénomène s'étend aujourd'hui à l'échelle de l'organisation tout entière. Hormis l'IT et la sécurité, les fonctions métiers concernées vont du support client aux RH, en passant par les équipes produits, l'ingénierie, le DevOps, la comptabilité-finance, le marketing ou encore le service commercial.

En conséquence, les responsabilités et l'administration de ces applications sont de plus en plus réparties entre différents départements et environnements. Autrefois, le rôle principal des équipes IT était de sélectionner les technologies adéquates pour l'ensemble de l'entreprise, tout en gérant la plupart des aspects comme la budgétisation, l'achat, l'onboarding, l'offboarding et la sécurité des logiciels.

Aujourd'hui, la tendance à la décentralisation du SaaS complique la tâche des équipes IT, notamment sur toutes les questions sécuritaires (suivi, évaluation, maintenance et protection). En moyenne, les entreprises utilisent des centaines d'applications autorisées, ce qui implique des milliers de connexions à sécuriser.

Dépenses et usages du SaaS par segment de marché en 2020

Statistiques SaaS (par entreprise)	Global	Grandes entreprises	Entreprises de taille intermédiaire	Petites et moyennes entreprises
Dépenses	+50 %	4,16 M$	2,47 M$	202 k$
Applis SaaS uniques	137	288	185	182
Connexions applis-utilisateurs	–	21 580	4 406	624
Taux de churn (applis SaaS)	30 %	46 %	29 %	35 %
Doublons d'applications	3,6	7,6	5,8	2,3
Abonnements SaaS laissés en déshérence	2,6 (+100 %)	7,1	4,3	1,4
Nombre de collaborateurs facturés par entreprise	–	98	32	10

Sources :

– Blissfully

Shadow IT : une menace plus durable et plus sérieuse qu'on ne le croit

Pour garantir la sécurité des données, les entreprises doivent surveiller, gouverner et restreindre l'utilisation d'applications SaaS non autorisées.

Souvent, les membres de différentes équipes préfèrent recourir à leurs propres solutions SaaS, tant pour des usages professionnels que privés. D'où l'émergence d'un phénomène de **Shadow IT**, dont une part prépondérante concerne l'utilisation non autorisée d'applications SaaS et autres services cloud. Or, l'explosion du télétravail n'a fait qu'amplifier les risques de cette pratique, étant donné que les collaborateurs distants se connectent depuis des réseaux non sécurisés. Nombre d'entre eux ont en effet tendance à contourner le VPN d'entreprise afin d'accéder directement aux applications souhaitées, sans parler des équipements personnels non gérés. Autant de phénomènes qui rendent le Shadow IT plus difficile à détecter et à bloquer.

LE SHADOW IT NUIT À LA SÉCURITÉ DES DONNÉES

Il est impossible pour l'équipe IT d'exercer un contrôle centralisé sur le stockage et la circulation de données métiers sensibles et propriétaires à l'échelle de milliers d'applications et de services cloud qui ne sont ni validés, ni approuvés. Les référentiels de données non gérés, situés hors du périmètre de sécurité de l'entreprise, élargissent la surface d'attaque à l'insu des responsables IT.

LE SHADOW IT VA À L'ENCONTRE DES RÉGLEMENTATIONS SUR LA PROTECTION ET LA CONFIDENTIALITÉ DES DONNÉES

L'équipe IT possède peu voire aucune visibilité sur les répercussions de ces applications non autorisées sur la conformité, pas plus que sur la nature des données qui y sont transférées ou stockées. Le Shadow IT implique donc la création de points d'audit visant à prouver que les réglementations sont bien respectées.

LE SHADOW IT PERMET AUX UTILISATEURS DE SE SOUSTRAIRE AUX BONNES PRATIQUES DE SÉCURITÉ

La plupart du temps, le recours au Shadow IT n'a rien de malveillant ni de négligent. Mais comme le dit l'adage, l'enfer est pavé de bonnes intentions. En effet, ce phénomène ouvre la voie aux compromissions de données, aux menaces internes, ainsi qu'à l'apparition de nouveaux points d'entrée pour les malwares et autres types de cyberattaques.

D'après Gartner, le Shadow IT représente 30 % à 40 % des dépenses IT globales au sein des grandes entreprises. Autrement dit, près de la moitié de votre budget informatique est consacré à des technologies qui n'ont pas obtenu l'aval de la DSI. Gartner prévoit en outre qu'en 2022, un tiers des attaques réussies contre les entreprises passeront par des ressources inconnues (Shadow IT).

Source :

– « Don't Let Shadow IT Put Your Business At Risk », Smarter with Gartner

Les entreprises doivent répondre à trois questions clés

Face à l'essor du cloud, les décideurs reconnaissent que la sécurité de ces environnements est une priorité absolue, et ce quelles que soient la taille et l'implantation géographique de leur entreprise.

Applications

Quelles applications les salariés utilisent-ils, et comment ?

Les entreprises confrontées à une expansion massive du télétravail poursuivent une stratégie SaaS multicloud audacieuse. Mais le manque de supervision des comportements d'utilisation crée une zone d'ombre autour de la confidentialité des données sensibles, synonyme de risques et de menaces potentiels.

Données

Comment protéger nos données sensibles dans le cloud ?

De par leur nature même, certains types de données doivent être consultés et utilisés par un grand nombre de collaborateurs, tandis que l'accès aux informations sensibles est en règle générale plus restreint. La disparité des usages dans les différentes équipes de l'entreprise crée des niveaux de complexité sans précédent en matière de protection des données.

Utilisateurs

Pouvons-nous contrôler et sécuriser l'accès aux applications SaaS ?

Certes, les fournisseurs de services cloud (CSP) assument leur part de responsabilité dans les domaines de la sécurité et de la conformité. Mais celle-ci ne doit pas soustraire l'entreprise à son devoir de protection des données, des utilisateurs et des applications. Entre l'entreprise et son CSP, la question de la responsabilité de la sécurité du cloud est souvent source de désaccord.

Sécurité SaaS, un sujet de préoccupation majeur pour les RSSI

Malgré tous les avantages des solutions SaaS pour les métiers, bon nombre d'entreprises se refusent à sauter le pas pour des questions de sécurité.

Côté pile, nul ne contredira la capacité des solutions SaaS à rendre n'importe quelle structure rapidement opérationnelle et performante à grande échelle. Mais côté face, ces applications soulèvent aussi des problématiques complexes et de nombreuses incertitudes auxquelles les RSSI doivent se confronter. Par exemple, ces produits nécessitent d'abandonner un certain degré de contrôle et de visibilité au fournisseur SaaS. Or, il est difficile de lâcher prise lorsque les données représentent un tel enjeu. De plus, les RSSI doivent composer avec une protection disparate – voire inexistante – d'une application à l'autre, ce qui crée des incohérences dans leur stratégie de sécurité SaaS.

Principaux enjeux de sécurité des applications SaaS

SHADOW IT

Des applications non autorisées sont utilisées et gérées à l'insu des équipes IT.

EXPOSITION DES DONNÉES

L'exposition accidentelle entraîne un risque de vol de données.

COMPORTEMENT DES UTILISATEURS

Entre partage trop permissif de données et présence de menaces en interne, l'équipe IT a du mal à surveiller le comportement des utilisateurs.

MANQUE DE VISIBILITÉ

Les responsables IT manquent de visibilité sur les données qui résident ou circulent dans les applications, y compris les informations sensibles et les fichiers malveillants.

MENACES ET MALWARES

Les applications SaaS, les utilisateurs et les données sont la cible de malwares et de menaces avancées.

CONFORMITÉ RÉGLEMENTAIRE

Les équipes IT sont dans l'incapacité d'étendre leurs mesures de conformité à leurs environnements SaaS.

Menaces liées au SaaS les plus préoccupantes pour les RSSI

Infections par malware **77 %**

Perte ou vol de données **72 %**

Vols d'identifiants ou compromissions de comptes **69 %**

Compromission de données cloud **45 %**

Compromission du réseau d'entreprise via le cloud **35 %**

Sources :

– Cybersecurity Insiders, The CISO Cloud SaaS Security Report, 2020

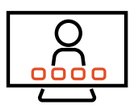
Types de SaaS les plus préoccupants sur le plan sécuritaire

Applications d'hébergement et de transfert de fichiers **72 %**

Applications de messagerie cloud **57 %**

Applications de messagerie instantanée **52 %**

Applications de communication et de collaboration **42 %**



Visioconférences **35 %**

Gestion de projet **23 %**

Limites des approches CASB traditionnelles

Les entreprises ont aujourd'hui besoin d'une approche évoluée du CASB pour faire face à la croissance exponentielle du SaaS.

Les solutions CASB sont devenues un outil incontournable pour assurer la protection des applications cloud et des données sensibles qui y sont partagées. Cependant, les entreprises doivent se départir des modèles opérationnels propres aux CASB de première génération, dont les lacunes sont aujourd'hui flagrantes.

1 **Visibilité incomplète sur les applications :** les solutions CASB de première génération se concentrent sur le HTTP/S, omettant au passage près de la moitié du trafic provenant des applications non-web. Par ailleurs, ces systèmes continuent de se fier exclusivement aux bases de données statiques de signatures applicatives, et ne peuvent détecter des applications qu'après ouverture d'un ticket de support. Or, cette approche affecte leur capacité à identifier ou contenir de nouvelles applications SaaS avant qu'elles ne deviennent un risque. Quant à l'absence d'API, elle empêche toute sécurisation des applications collaboratives plébiscitées par les équipes distribuées.

2 **Protection inadaptée des données :** leurs méthodologies de protection des données sont dépassées par le volume et la prolifération de données sensibles. Côté prévention des pertes de données (DLP), le recours quasiexclusif aux expressions régulières et aux méthodes traditionnelles d'empreintes digitales des données se traduit par une protection lente et imprécise. Mais la lacune la plus criante se situe dans leur incapacité à détecter des fuites de données sur des applications collaboratives de type Slack, Teams et Zoom, qui utilisent de nouveaux modes de communication basés sur des messages brefs et non structurés.

3 **Sécurité inefficace :** malheureusement, les solutions CASB traditionnelles relèguent souvent la sécurité à une simple case à cocher. En effet, la plupart d'entre elles ne présentent qu'une efficacité très limitée face aux menaces urgentes, aux malwares inconnus et aux compromissions – généralement à l'aide d'outils de sandboxing tiers. Par ailleurs, leur approche basée sur les proxys inline apporte uniquement de la visibilité sur le HTTP/S, ce qui signifie que les clients ne sont que partiellement protégés.

4 **Couverture disparate :** ces solutions CASB cloisonnées contraignent les entreprises à employer différentes technologies et méthodes de déploiement afin de couvrir le siège, les filiales et les télétravailleurs, ce qui crée d'énormes disparités en matière de protection. Séparées du reste de l'infrastructure de sécurité, elles imposent en outre des modifications au niveau du réseau, ainsi qu'une architecture difficile à déployer, ce qui rend leur gestion à la fois inefficace et fastidieuse dans le contexte du travail hybride.

L'heure est venue d'adopter une nouvelle approche du CASB. Pour enfin faire rimer SaaS et protection, vous devez miser sur une solution connectée au reste de votre environnement de sécurité, synonyme de contrôle et de visibilité sur l'ensemble des applications, des utilisateurs et des données.

5 fonctionnalités indispensables d'un CASB nouvelle génération

1 Votre solution CASB nouvelle génération doit opérer à l'échelle du cloud et tenir le rythme face à l'explosion du SaaS

Une visibilité complète sur votre environnement SaaS est indispensable pour déterminer précisément le niveau de sécurité des données et du cloud. L'utilisation de produits cloud hors du champ de contrôle de l'équipe IT signifie que les politiques de gouvernance, risque et conformité (GRC) de l'entreprise ne sont pas appliquées. Les données ne sont donc plus protégées. Une solution CASB nouvelle génération doit automatiquement détecter et sécuriser toutes les applications, autorisées ou non, y compris les outils SaaS collaboratifs, afin de tenir la cadence face à l'explosion exponentielle du SaaS.

Un CASB nouvelle génération doit en outre analyser l'ensemble du trafic, des ports et des protocoles, tout en assurant la découverte automatique des nouvelles applications. Une telle solution doit aussi prendre en charge un très large éventail d'API d'applications SaaS, y compris celles d'outils de collaboration modernes tels que Slack® et Teams. Chaque application sous surveillance doit en outre être soumise à des scores et des attributs de risque précis et personnalisables, avec blocage automatique des activités utilisateurs dangereuses et porteuses de risques. La visibilité complète en temps réel et les scores de risque permettront à vos équipes IT de gérer automatiquement la croissance du SaaS, appliquer des contrôles de risque granulaires sur les applications connues et inconnues, et éviter que ces dernières ne deviennent un vecteur de pertes de données.

Ces fonctionnalités sont le signe que votre solution CASB opère à l'échelle du cloud :

- ✓ Couverture de sécurité étendue à l'ensemble des applications SaaS, avec connectivité par API permettant d'assurer la maîtrise et la sécurité des applications SaaS autorisées.
- ✓ Détection continue des applications à l'aide d'un moteur cloud basé sur les identités applicatives, permettant ainsi de mieux lutter contre les risques du Shadow IT.
- ✓ Classification automatisée des risques, avec plus de 30 attributs pour mieux déterminer le niveau de risque de l'entreprise.
- ✓ Fonctionnalités d'étiquetage par lot pour faciliter le classement des applications et afficher leur statut d'autorisation, et étiquetage personnalisé pour une classification sur mesure.
- ✓ Contrôles inline intégrés pouvant être déployés sur l'ensemble des équipements et des utilisateurs.

2 Votre solution CASB nouvelle génération doit être simple à déployer et reposer sur une architecture Lean

Dans les entreprises hautement distribuées d'aujourd'hui, qui comptent de multiples sites et de nombreux utilisateurs mobiles, le rôle d'intermédiaire que jouent les solutions CASB traditionnelles n'est pas viable, tant en termes de coûts élevés que de manque d'évolutivité. Les CASB standard sont fastidieux à déployer, car ils ajoutent une passerelle cloud (généralement un proxy) inutile et requièrent une redirection complexe du trafic issu des collecteurs de journaux tels que le pare-feu réseau et les agents d'autoconfiguration des proxys (PAC). Pour compliquer un peu plus l'équation, ces solutions impliquent l'ajout d'un connecteur Active Directory (AD) en vue d'appliquer les politiques selon l'ID d'utilisateur ou le groupe AD. Et cette infrastructure doit être dupliquée sur autant de sites que compte l'entreprise. Enfin, l'essor du télétravail impose l'ajout de terminaux sur lesquels il faut installer les fichiers PAC, voire des agents VPN pour faire passer le trafic des utilisateurs distants par le proxy cloud. Bien que l'architecture proxy soit incontournable pour ceux qui en dépendent, elle représente pour les autres un fardeau à configurer et ne devrait pas être la seule option.

Une solution CASB nouvelle génération doit éliminer tous les composants intermédiaires et soulager vos budgets IT d'investissements supplémentaires en infrastructure. Elle doit simplifier les opérations de vos équipes informatiques en exploitant conjointement le SASE et le CASB sur une plateforme unifiée de sécurité, de réseau et de protection des données couvrant l'ensemble des environnements. Enfin, elle doit pouvoir tirer parti de vos pare-feu nouvelle génération (NGFW) actuels pour une surveillance et une posture de sécurité complètes et intégrées de votre portefeuille SaaS.

Ces fonctionnalités sont le signe que votre solution CASB est simple et facile à déployer :

- ✓ Solution gérée à 100 % dans le cloud, proposant des options de déploiement flexibles et compatibles avec le travail hybride.
- ✓ Tableau de bord unique offrant une visibilité sur l'ensemble des politiques relatives aux applications cloud.
- ✓ Configuration simplifiée grâce à des workflows optimisés et une automatisation basée sur le ML.
- ✓ Visibilité automatique et actualisée sur le Shadow IT à l'aide d'intégrations natives.
- ✓ Intégration directe aux solutions de prévention des pertes de données (DLP), de protection contre les menaces et de contrôles inline pour l'application des politiques définies. Aucun ajout de fichiers PAC ou de proxys nécessaire pour compléter le déploiement.

3 Votre solution CASB nouvelle génération doit détecter les menaces connues et inconnues, efficacement et en amont

L'hétérogénéité des applications SaaS crée un environnement hautement distribué, constitué de centaines d'applications provenant de différents CSP – soit autant de points de compromission en puissance. Une posture de sécurité SaaS efficace nécessite des éclairages concrets sur la détection et la prévention des menaces qui pèsent sur votre environnement SaaS. Une solution CASB nouvelle génération doit prévenir les menaces zero-day à l'aide de modèles ML inline intégrés nativement, sans recours à des outils tiers. Elle doit neutraliser de façon immédiate les menaces nouvelles et inconnues grâce à des signatures résistant aux techniques de contournement, puis distribuer les mises à jour en quelques secondes à l'échelle mondiale pour empêcher toute propagation de l'infection. Au-delà des analyses de malwares traditionnelles, une telle solution doit s'appuyer sur un moteur de Threat Intelligence alimenté par l'un des plus grands ensembles de données de la planète. Vous puisez ainsi dans la force du collectif pour bloquer rapidement et facilement les menaces à l'aide d'une protection zero-day inline en temps réel. Cette nouvelle approche permettra d'adapter continuellement votre posture de sécurité afin de défendre votre réseau contre les menaces issues du SaaS, tout en épargnant un temps précieux à vos équipes IT.

Ces fonctionnalités sont le signe que votre solution CASB offre une prévention des menaces efficace :

- ✓ Protection continue contre les malwares et autres menaces à l'aide d'un moteur cloud de prévention et d'analyse des malwares, pour favoriser la détection et la prévention de nouvelles menaces inconnues basées sur des fichiers.
- ✓ Workflow de résolution des incidents avec remédiation automatique.
- ✓ Surveillance de l'activité des utilisateurs et réponse adaptée.

4 Votre solution CASB doit assurer une protection et une conformité complètes de vos données à l'aide de techniques de détection ultraprécises

La plupart des CASB n'offrent que des fonctionnalités basiques de protection et de mise en conformité des données, tout en se limitant aux environnements cloud. Bien que les solutions de prévention des pertes de données déployées sur site s'appuient sur des techniques et des fonctionnalités plus avancées, elles créent une approche déséquilibrée entre l'infrastructure des environnements sur site et sur cloud. Une solution CASB nouvelle génération doit fournir des contrôles de protection et de conformité des données fiables et complets à l'échelle de l'entreprise, des environnements cloud, des réseaux sur site… c'est-à-dire partout où se trouvent vos utilisateurs et vos données. Une telle solution doit être capable de découvrir, classer et protéger toutes les données stockées et transmises par l'intermédiaire d'applications SaaS inline et d'applications SaaS hors bande via des API. Ainsi, les infractions aux politiques, les problèmes d'exposition de données et les questions de conformité sont traités de façon appropriée. Plus important encore, un CASB nouvelle génération doit s'adapter aux applications collaboratives comme Slack, Teams et Zoom, où les utilisateurs communiquent par messages brefs, non structurés, voire par captures d'écran. Moteur de détection cloud efficace, profils de données descriptifs, correspondance exacte des données, reconnaissance d'images, traitement automatique du langage naturel, modèles IA… un CASB qui intègre toutes ces fonctionnalités sera en mesure de détecter précisément les données sensibles, structurées ou non, au repos et en transit.

Ces fonctionnalités sont le signe que votre solution CASB assure une protection et une conformité complètes de vos données :

- ✓ Prévention des pertes de données au repos et en transit, avec découverte des données sensibles au sein des applications SaaS, détection de l'exposition des données grâce à l'EDM, à l'OCR et aux profils de données inclus, et prévention de l'exfiltration de données.
- ✓ Protection des données pour les applications de collaboration critiques (Slack, Teams, Zoom, Jira, Confluence, etc.), avec possibilité d'identifier automatiquement les informations sensibles en temps réel dans le contexte d'échanges non structurés grâce au deep learning, au traitement automatique du langage naturel et aux modèles IA.
- ✓ Reporting de conformité clé en main, avec notamment un rapport RGPD en temps réel pour les données au repos, un rapport d'évaluation des risques des données au repos (à la demande), et un rapport de sécurité SaaS pour les applications Shadow IT (à la demande).

5 Votre solution CASB doit fournir une sécurité intégrée et homogène sur tous les sites

Détachés de l'architecture centrale de l'entreprise, les CASB sont limités dans leur capacité à fournir des contrôles de sécurité homogènes sur l'ensemble de l'infrastructure (cloud, sur site, à distance). Or, ceci complique la tâche des équipes de sécurité qui doivent synchroniser les risques, les politiques et les contrôles entre plusieurs environnements. Une solution CASB nouvelle génération doit prendre la forme d'un outil intégré, capable de sécuriser le travail hybride (à distance ou dans l'enceinte de l'entreprise), en plus de protéger l'ensemble des applications et des données qui y sont stockées ou transmises. En éliminant la complexité inhérente aux produits spécialisés, cette solution permettra de protéger de façon homogène les données au repos et en transit dans les applications cloud et sur le réseau physique. D'autre part, ce nouveau CASB multimode doit sécuriser à la fois les applications (approuvées ou non) et le trafic (web et non-web) à partir d'une console unifiée dans le cloud. Enfin, il doit être capable de détecter les applications SaaS non autorisées et de gérer les risques tout en recourant aux API pour élargir la sécurité aux applications autorisées hors bande, et ce afin de garantir la détection de données au repos, l'inspection et la remédiation sur l'ensemble des activités relatives aux utilisateurs, aux dossiers et aux fichiers.

Ces fonctionnalités sont le signe que votre solution CASB est un outil intégré et multimode :

- ✓ Contrôles inline granulaires sur l'ensemble des applications, pour tous les utilisateurs et équipements.
- ✓ Contrôles de sécurité et mise en conformité des données sur l'ensemble des applications SaaS, des réseaux et des utilisateurs, sans aucun outil tiers.
- ✓ Prévention des menaces sur l'ensemble des applications, des réseaux et des équipements avec WildFire, sans aucun outil tiers.
- ✓ Utilisation de l'infrastructure de sécurité existante. Aucun changement d'architecture, ni d'ajout de fichiers PAC ou d'agents VPN supplémentaires.

SaaS Security par Palo Alto Networks

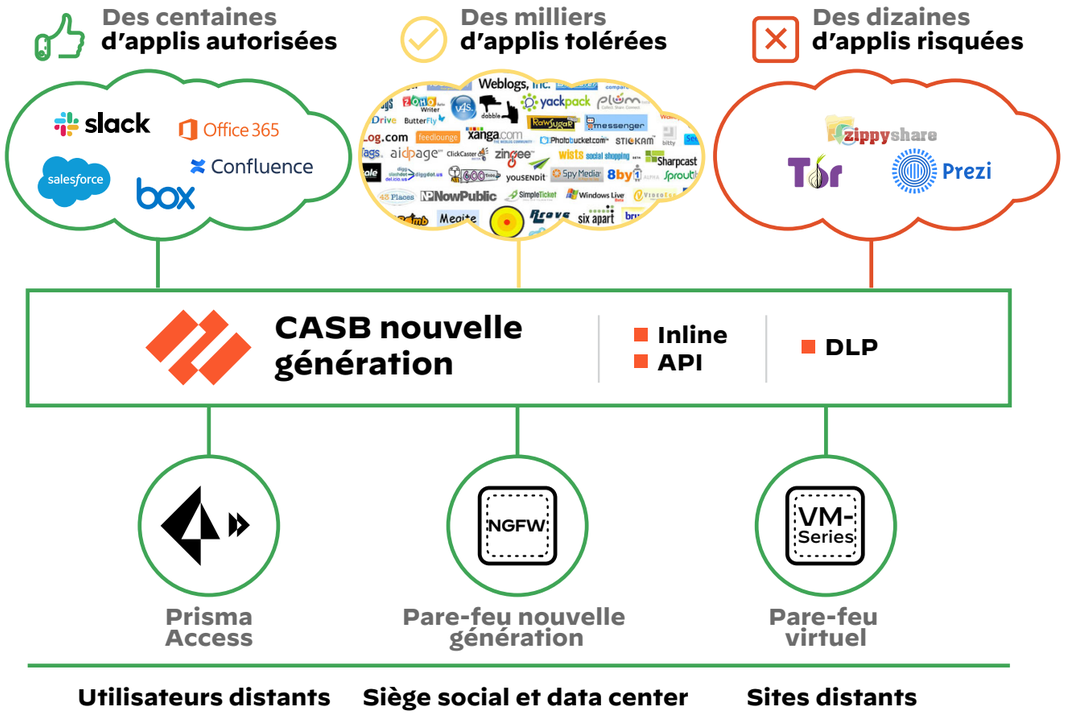
Le premier CASB nouvelle génération capable de faire rimer SaaS et sécurité

Pour adopter le cloud en toute sérénité, les entreprises ont besoin d'une seule et même solution de sécurité capable d'assurer une protection homogène de leurs utilisateurs, applications et données sur l'ensemble de leurs environnements. SaaS Security relève les défis de l'explosion du SaaS en assurant la découverte automatique et la protection de vos applications, tout en s'intégrant efficacement à vos propres architectures et workflows. Découvrez tout ce que SaaS Security peut faire pour vous.

- Notre solution est la seule capable de détecter et de contrôler automatiquement les nouvelles applications SaaS à l'aide d'App-ID, notre technologie brevetée qui exploite toute la puissance du machine learning et toute la force collective de la communauté mondiale de Palo Alto Networks.

- Par rapport aux outils basés sur proxy, l'architecture Lean de notre CASB nouvelle génération élimine les composants intermédiaires. Ainsi, notre solution peut être déployée et mise en service sur nos plateformes SASE et nos NGFW en l'espace de quelques minutes, ce qui divise par cinq le délai de rentabilisation. Meilleure efficacité opérationnelle, réduction du coût total de possession (TCO), accélération du ROI… les avantages de notre CASB nouvelle génération ont de quoi convaincre.

- Notre réseau de milliers de clients à travers le monde permet de neutraliser instantanément les menaces et de distribuer des signatures résistant aux techniques de contournement seulement quelques secondes après la détection.
SaaS Security aide à prévenir tout type de danger, y compris les menaces zero-day, en temps réel et sans aucun outil de sécurité tiers.



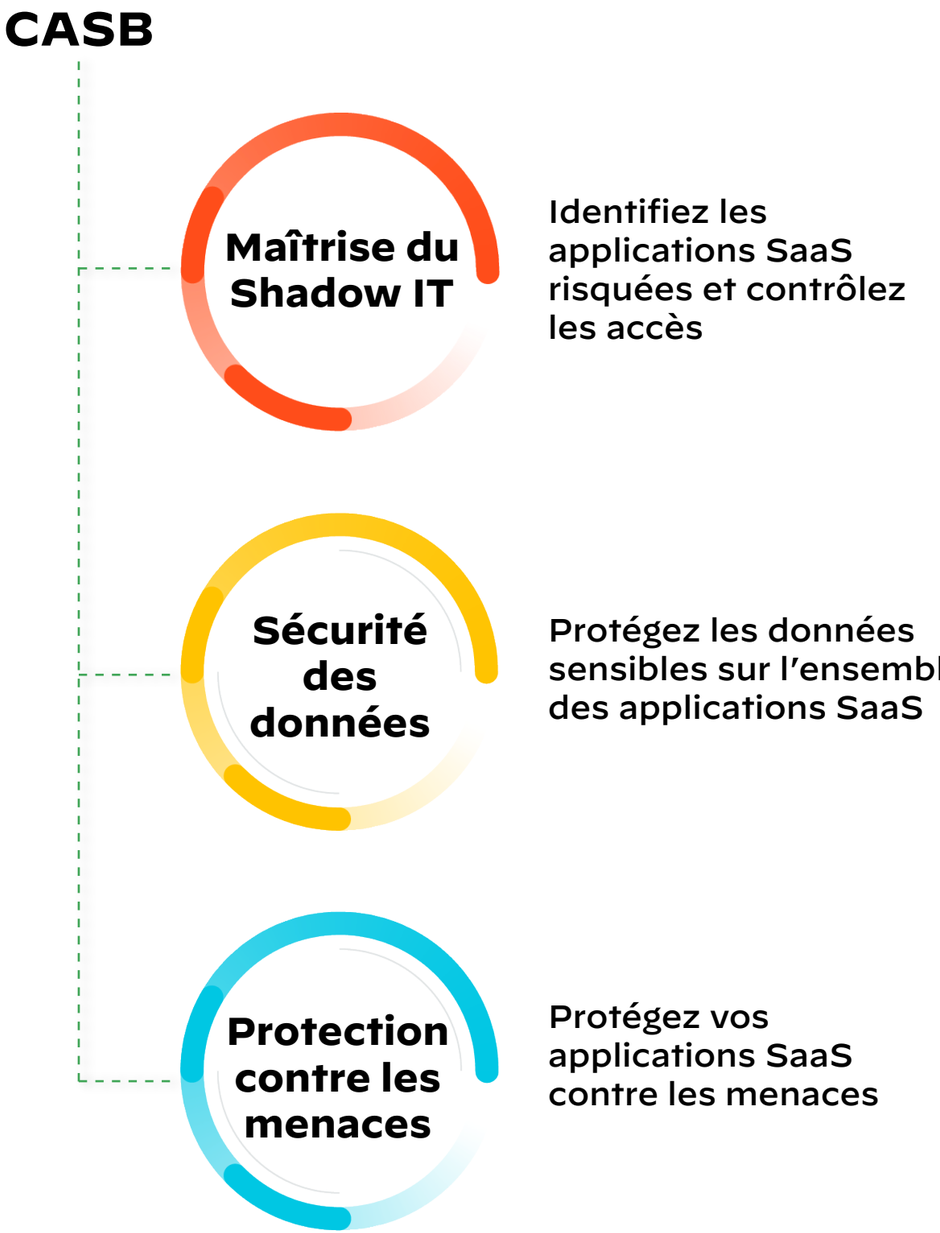
Palo Alto Networks réinvente le CASB pour l'entreprise d'aujourd'hui

- SaaS Security utilise **Enterprise DLP**, le système de prévention des données cloud le plus complet du marché, sur l'ensemble des applications SaaS (inline et au repos via les API hors bande) – dont les derniers outils collaboratifs – ainsi que sur le reste de votre environnement (cloud, infrastructure sur site, télétravailleurs). Pour vous, c'est la garantie d'une protection et d'une conformité homogènes, où que soient situés vos utilisateurs et vos données.

- SaaS Security veille au respect des réglementations (PCI DSS, HIPAA, RGPD, etc.) grâce à des rapports de conformité prêts à l'emploi, ainsi qu'à une protection complète des applications SaaS (**Enterprise DLP**, prévention des menaces pilotée par ML et surveillance continue de l'activité des utilisateurs et des configurations administratives).

- Grâce à son implémentation cloud-native, notre solution s'intègre directement à votre plateforme **SASE** et à vos **pare-feu nouvelle génération**. SaaS Security est conçu pour détecter et protéger toutes les applications utilisées (web et non-web) ainsi que pour offrir une protection homogène de l'ensemble des applications, réseaux, données, workloads et utilisateurs, peu importe leur lieu de travail.

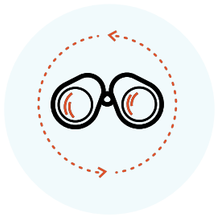
SaaS Security de Palo Alto Networks apporte une réponse aux entreprises à la recherche d'une solution plus simple et plus sûre que les CASB traditionnels. **Les études montrent que cette approche complète et intuitive aboutit à une réduction de 45 % des compromissions sur trois ans.**



SaaS Security couvre tous les cas d'usage d'un CASB

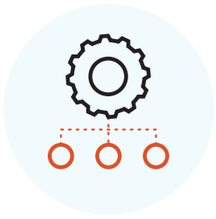
Offrez à votre équipe IT les avantages d'une solution CASB intégrée

Misez sur notre CASB intégré pour placer l'adoption croissante du SaaS sous le signe de la maîtrise et de la sécurité.



Solution complète pour une visibilité et une maîtrise inégalées du SaaS

- Découverte et contrôle automatiques des nouvelles applications avec la technologie cloud App-ID™
- Aucun composant intermédiaire, faible TCO
- Sécurité étendue basée sur des API pour les applications autorisées



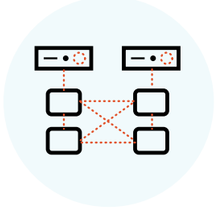
Architecture Lean avec déploiement facile dans tous les formats

- Secure Access Service Edge (SASE)
- Pare-feu matériels
- Pare-feu logiciels

Prévention des pertes de données et prévention des menaces basée sur ML

- Protection des données sensibles sur l'ensemble des applications SaaS et tous les sites où sont situés vos utilisateurs et vos données
- Identificateurs descriptifs, correspondance exacte des données, traitement automatique du langage naturel et reconnaissance des images pour une détection ultraprécise des données
- Prévention des menaces via des modèles ML inline
- Distribution immédiate de signatures de détection des menaces neutralisant les techniques de contournement

Console unifiée dans le cloud (inline + API + Enterprise DLP)



Déploiement intégral sur notre plateforme SASE ou nos pare-feu nouvelle génération

Mise en conformité réglementaire (PCI DSS, HIPAA, RGPD…) par une protection renforcée des applications SaaS

Pensez CASB intégré.
Pensez Palo Alto Networks.

Chez Palo Alto Networks, nous avons pour mission de protéger les modes de vie numériques contre les cyberattaques. Nous sommes présents en première ligne pour assurer la sécurité de dizaines de milliers d'entreprises sur le cloud, les réseaux et les terminaux. Intelligence artificielle, analytique, automatisation, orchestration… nous innovons sur tous les fronts pour vous aider à relever les défis de sécurité les plus sensibles.

Fondée en 2005, Palo Alto Networks est basée à Santa Clara, en Californie, et accompagne des clients dans le monde entier.

Pour plus d'informations, rendez-vous sur : www. paloaltonetworks.fr

Envie d'en savoir plus ? **Demandez votre démo de SaaS Security !**

SaaS Security, ce sont nos clients qui en parlent le mieux :

> ***« Nous sommes convaincus d'avoir choisi le partenaire idéal pour propulser notre entreprise vers l'avenir. Palo Alto Networks propose une vision claire de la sécurité des environnements SaaS, qui couvre tous les aspects critiques de ce type de déploiement. »***
>
> – Juan Carlos Alzate Garcia, VP Technologies

CIUDAD CELESTE SAMBORONDÓN

Lire l'étude de cas

www.paloaltonetworks.fr

Oval Tower, De Entrée 99 – 197
1101HE Amsterdam, Pays-Bas

Téléphone : +31 20 888 1883