

ManageEngine
Log360 Cloud



Améliorer la
sécurité du cloud avec

CASB

<https://www.pgsoftware.fr/siem/log360-cloud>

Table des matières

CASB	1
Naviguer dans le paysage actuel de la sécurité du cloud	2
Qu'est-ce qu'un CASB?	4
La nécessité d'un CASB	6
Comment fonctionne un CASB	7
Adopter la sécurité du cloud avec un CASB	9
Cas d'utilisation d'un CASB	10
Atteindre une GRC critique avec le CASB	11
Identifier la solution CASB idéale	12



Roue de la sécurité du cloud avec **CASB**

Depuis le début de la décennie, les organisations considèrent la migration vers le cloud comme une priorité absolue lorsqu'elles formulent des stratégies commerciales. Cela s'explique par les capacités du cloud telles que l'indépendance géographique, l'accès omniprésent et l'élasticité, qui peuvent être utilisées pour améliorer le business.

L'approche "lift and shift" a permis aux entreprises d'y parvenir plus facilement en les aidant à migrer les données et les applications des sites vers le cloud avec des changements minimes ou nuls. De nombreuses organisations ont migré avec succès et en toute sécurité leurs suites de productivité et leurs applications Web vers le cloud.

Si le cloud offre des avantages concurrentiels et rend les organisations agiles à un coût raisonnable, il a aussi commencé à exposer des vulnérabilités qui ont entraîné d'énormes pertes financières, des fuites de données et des violations de la conformité, ce qui a souvent entraîné une augmentation des coûts.

Aujourd'hui, alors que les experts prévoient que le marché mondial des services de cloud public atteindra **623,3 milliards** de dollars d'ici 2023 et que le nombre d'entreprises qui tentent de transférer leurs applications critiques, telles que les systèmes financiers et de ressources humaines, explose, la nécessité de sécuriser l'environnement de cloud est devenue cruciale.

En outre, lors de la migration, les différences architecturales entre les systèmes sur site et dans le nuage, la sécurité est devenue la principale préoccupation des entreprises, qu'elles utilisent un logiciel en tant que service (SaaS), une plate-forme en tant que service (PaaS) ou une infrastructure en tant que service (IaaS).

En incluant un CASB (Cloud Access Security Broker) dans leur arsenal de sécurité, les entreprises peuvent obtenir une visibilité approfondie de leurs environnements en nuage. Dans cet article, nous expliquons comment le CASB rend la sécurité du cloud complète.

Glisser à travers le courant

Paysage de la sécurité du cloud



Évolution

La sécurité du cloud a fait du chemin depuis le jour où le cloud computing a été conçu pour la première fois. Au départ, lors de l'émergence du cloud computing, l'accent était principalement mis sur la facilitation de la flexibilité, de la collaboration et du partage des ressources. Bien que l'approche "lift and shift" ait permis aux organisations de passer rapidement au cloud, la sécurité est devenue une préoccupation majeure en raison des différences architecturales. En outre, l'utilisation du cloud pour stocker des informations commerciales sensibles a fait monter les enchères.

Cela a incité les fournisseurs de services à élaborer des stratégies pour garantir la sécurité du cloud. De l'autorisation à la vérification des antécédents des utilisateurs qui tentent d'accéder à des informations critiques, les fournisseurs de services en nuage (FSC) ont élaboré une série de politiques de sécurité pour mieux sécuriser les données en nuage et rassurer les utilisateurs sur la sécurité de l'utilisation du nuage.

Étant donné que plusieurs clients utilisent le nuage pour stocker des informations, des frontières virtuelles ont été établies pour garantir l'isolation des données, de sorte qu'aucun client ne puisse accéder aux informations d'un autre client.

Bien que les FSC aient pris le plus grand soin pour sécuriser leurs environnements, les clients ont toujours certaines responsabilités pour assurer la sécurité des mots de passe et de la connexion de leur côté.

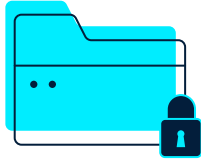
Les cybercriminels et leurs manigances

Les cybercriminels ont profité de l'extension imprévue des périmètres de réseau des organisations et de l'affaiblissement de leur sécurité, ce qui les a incités à élaborer des stratégies pour exploiter les vulnérabilités du cloud.

Les attaques, qui allaient du détournement de comptes à l'injection de logiciels malveillants, étaient de grande ampleur. Comme plusieurs locataires étaient impliqués, les attaquants ont pu mettre la main sur les données de plusieurs organisations, ce qui a rendu difficile la détection et la défense contre ces attaques par le fournisseur de services et le client.



L'énigme de la sécurité



Le partage des responsabilités en matière de sécurité crée une grande confusion entre les FSC et leurs clients, ce qui entraîne des lacunes en termes de contrôle d'accès, de sécurité des données, etc. Bien que la plupart des fournisseurs de services définissent les limites de manière assez définitive, il existe toujours des angles morts qui sont exploités par les attaquants.

Lorsque les organisations adoptent un environnement multi-cloud, elles ne réalisent souvent pas le modèle de responsabilité partagée de chaque fournisseur et se retrouvent avec un environnement cloud à haut risque de sécurité.

De plus, comme plusieurs locataires sont impliqués, il devient difficile d'identifier l'origine d'une cyberattaque. La formulation d'une stratégie commune de réponse aux incidents pour chaque client ne fonctionne pas, car la nature des données traitées doit être prise en compte, ce qui signifie que les stratégies doivent être adaptées à chaque client

En outre, l'utilisation d'applications fantômes et interdites complique la tâche des administrateurs de sécurité et des fournisseurs de services qui doivent faire face à des attaques venant de toutes les directions. En outre, des problèmes majeurs tels que les mauvaises configurations du cloud, l'abus de données et le détournement de session rendent difficile la sécurisation des installations de cloud.

C'est pourquoi il est essentiel de disposer d'une solution complète pour surveiller votre environnement et fournir des informations en temps réel sur les activités du cloud, et c'est là qu'interviennent les CASB (cloud access security brokers).



Qu'est-ce qu'un **CASB**?

En 2012, [Gartner](#) a présenté les CASB au monde entier, en les définissant comme un point d'application de la politique de sécurité sur site ou dans le cloud qui se situe entre les consommateurs de services cloud et les FSC pour surveiller l'accès aux ressources basées dans le cloud.

Depuis sa création, le CASB a considérablement évolué pour devenir une solution plus exhaustive à tous les problèmes de sécurité du cloud.

L'adoption massive du cloud et les rapports continus sur les problèmes de sécurité ont obligé les fournisseurs de services à investir davantage dans la sécurité du cloud et les CASB sont devenus la solution de référence.

Les CASB ont évolué pour devenir des solutions de repérage de l'identité et de l'activité de l'utilisateur du cloud qui traitent les problèmes de visibilité.

Avec un **CASB** complet, vous bénéficiez des capacités suivantes:

1

Analyse des applications en cloud:

Contrairement à la sécurité traditionnelle du cloud, un CASB peut surveiller les applications cloud et fournir des rapports exhaustifs sur les différentes applications fantômes et interdites utilisées dans l'organisation.

2

Surveillance des données et confidentialité:

Un CASB peut surveiller les mouvements de données et s'assurer que seul le personnel autorisé a accès aux informations sensibles. Cela garantit la confidentialité des données et protège les organisations contre les fuites de données.

3

Détection des menaces et gestion des incidents:

Les CASB sont également capables de détecter les menaces internes et externes. Ils se situent entre une organisation et son environnement en nuage et surveillent le trafic entre eux. La solution identifie les activités malveillantes et aide à se défendre contre les menaces courantes telles que le détournement de compte, la prise de contrôle de session, etc.

4

Gestion intégrée de la conformité:

Un CASB aide à se conformer aux mandats réglementaires tels que l'HIPAA, le GDPR et d'autres en surveillant sans cesse les plateformes cloud et en fournissant des alertes en temps réel et des rapports exhaustifs sur les différentes activités du réseau.

La nécessité d'un CASB

L'explosion de la croissance du SaaS

Les experts ont prédit que 85 % des logiciels utilisés par les organisations seront des SaaS d'ici 2025. En outre, le SaaS a commencé à jouer un rôle important dans la majorité des secteurs, notamment la finance, l'éducation, la santé, la défense et d'autres secteurs dans lesquels des informations sensibles sont traitées.

85%

Les logiciels utilisés par les organisations seront des SaaS d'ici 2025.

Périmètre étendu du réseau

L'adoption du cloud computing étend le périmètre du réseau des organisations, ce qui peut laisser des angles morts en matière de sécurité. Ces angles morts peuvent être exploités par des attaquants.

Adoption du multi-cloud

Les organisations ont commencé à adopter des stratégies multi-cloud. Les différents fournisseurs de services suivent des directives de sécurité différentes. Cela rend la surveillance du cloud difficile.

Comment fonctionne un CASB

Par rapport à la surveillance traditionnelle du cloud, un CASB facilite la surveillance et la sécurisation de l'installation du cloud. Le processus de déploiement est simple et la solution est assez facile à utiliser. Toutefois, certains facteurs doivent être pris en compte lors de l'adoption d'un CASB.



Un CASB peut être déployé sur site ou dans le nuage.
Cependant, le SaaS est en tête de liste des méthodes de déploiement.

Modèles de déploiement

Modèle	Description	Avantages
API	<p>La plupart des applications SaaS utilisent des API pour surveiller les applications. Cependant, les API ne fournissent souvent pas de logique de politique ou de flux de travail utiles aux équipes de sécurité ou aux SOC.</p> <p>Les CASB exploitent les API et permettent de surveiller les activités du cloud à partir d'une console unique. En outre, un CASB annule également les différences entre les API des différents fournisseurs de services en établissant des fonctions API natives. L'un des principaux inconvénients des API est qu'elles peuvent ne pas fournir une protection en temps réel.</p>	<ul style="list-style-type: none"> ✔ Assurer l'intégrité des données au repos: Assurer l'intégrité des données au repos en contrôlant et en classant les données en fonction de leur sensibilité et en mettant en œuvre des politiques pertinentes. ✔ Facile à déployer: Ce modèle peut être déployé facilement et ne modifie pas l'expérience utilisateur des applications. ✔ Valeur immédiate: Les avantages du déploiement d'un modèle d'API peuvent être perçus immédiatement, car le processus de mise en œuvre est simple.
Proxy avant	<p>Dans ce modèle, le trafic passe par un CASB avant d'accéder à une application ou une ressource en nuage. Le CASB fait office de passerelle vers le réseau et assure une sécurité complète en établissant un contrôle d'accès et en bloquant le trafic malveillant. En outre, le CASB garantit l'intégrité des données en utilisant des capacités de prévention des pertes de données et d'inspection approfondie des paquets.</p>	<ul style="list-style-type: none"> ✔ Sécurité en temps réel: Un proxy avancé fournit des informations en temps réel sur les activités du cloud. ✔ Déploiement simple: Le processus de déploiement est simple ; la solution surveille les téléchargements et notifie à l'administrateur système les violations de la politique. ✔ Flexibilité: Le forward proxy offre une meilleure flexibilité par rapport au modèle API.
Proxy inversé	<p>Dans ce modèle, l'utilisateur est redirigé vers le CASB, qui valide ensuite l'identité de l'utilisateur à l'aide de SAML et fournit l'accès requis. Un avantage marqué du modèle de proxy inverse, notamment par rapport au proxy direct, est qu'il n'est pas nécessaire de contrôler le point d'extrémité pour diriger le trafic à travers le proxy.</p>	<ul style="list-style-type: none"> ✔ Contrôle en ligne: Fournit une sécurité en ligne et en temps réel pour les services en nuage, en limitant l'accès aux applications ou aux données sensibles en fonction du contexte de l'appareil et de l'utilisateur. ✔ Sans agent: Fournit une sécurité sans agent aux appareils personnels et d'entreprise en fonction de leur contexte. ✔ Omniprésente: surveille plusieurs applications en nuage indépendamment de leur cadre..

Adopter la sécurité du cloud avec un CASB

L'adoption d'un CASB rend la sécurité du cloud complète en donnant une vue approfondie des différents événements qui se produisent dans l'environnement cloud d'une organisation, ce qui permet aux administrateurs d'identifier plus facilement les activités malveillantes.

En outre, les CASB aident également les organisations à :

1 Établir une sécurité spécifique à l'application:

Les organisations formulent souvent une stratégie de sécurité commune pour les différentes applications de leur environnement. Cependant, un CASB est capable d'exploiter les API de la plupart des applications en nuage et de surveiller les activités, d'analyser le contenu et d'ajuster les paramètres des comptes sur ces applications.

2 Créez une passerelle concurrente:

Un CASB s'interpose entre une organisation et son environnement en nuage et agit comme une passerelle qui contrôle l'accès aux ressources dans le nuage. Il facilite également l'application des politiques et assure la protection des informations en transit.

3 Contrôlez les TI fantômes:

Un CASB aide à analyser l'informatique fantôme en surveillant en permanence les applications en nuage et en identifiant l'utilisation des applications fantômes et interdites. et des applications interdites.

4 Pratiquez le contrôle d'accès:

Avec un CASB, il est possible d'établir un contrôle d'accès, limitant ainsi l'accès non autorisé aux ressources sensibles du nuage.



Cas d'utilisation d'un CASB

Protection contre les menaces



- ☑ **Détection des anomalies:** Le CASB apprend les modèles comportementaux des utilisateurs et développe une ligne de base. En cas d'écart par rapport à cette ligne de base, la solution alerte l'administrateur. Par exemple, un employé se connecte régulièrement vers 10 heures du matin. Un jour, il se connecte à 11 heures du soir et accède à certaines ressources critiques. Bien que cela puisse être normal, la possibilité d'une fuite de données ne peut être négligée. C'est pourquoi le CASB alerte l'administrateur de cet incident et garde trace de toutes les activités de l'employé. Il attribue également un score de risque sur la base duquel l'administrateur peut prendre des mesures.
- ☑ **Shadow IT:** Le CASB assure également la sécurité contre le shadow IT en surveillant l'accès aux sites web malveillants et aux applications interdites. En outre, il surveille également les téléchargements en amont et en aval, afin de s'assurer qu'aucune charge utile ne pénètre dans le réseau.

Protection des données



- ☑ **Prévention des pertes de données:** Le CASB assure la sécurité des données tant en transit qu'en stockage. Il surveille également les mouvements de données et s'assure qu'aucun utilisateur non autorisé n'a accès à des informations critiques. Par exemple, un utilisateur du département financier tente de modifier un fichier particulier qui appartient au département des ressources humaines. Le CASB signale immédiatement cet incident et alerte l'administrateur de l'accès non autorisé. Le CASB protège également les fichiers en filigrane, par cryptage ou par mot de passe, en fonction de leur sensibilité, afin d'éviter que les données ne soient exposées.
- ☑ **Contrôle de sécurité:** Le CASB est capable d'aider les organisations à appliquer des contrôles de sécurité pour empêcher le transfert de données non autorisées sur Internet. De plus, il peut bloquer les téléchargements de fichiers vers des applications Internet malveillantes, sécurisant ainsi les données sensibles.

Sécurité de l'identité



- ☑ **Application des politiques:** Le CASB permet aux organisations d'appliquer des politiques pour sécuriser leur réseau. Chaque fois que la solution détecte une violation de politique, elle alerte l'administrateur et lui fournit des informations en fonction du risque et de la sensibilité de la violation.
- ☑ **Gestion des utilisateurs:** La solution fournit également des informations sur les utilisateurs et leurs activités, ce qui permet d'identifier les initiés malveillants.

Atteindre une **GRC** critique avec le **CASB**

Les CASB aident les organisations à réaliser la GRC (gouvernance, gestion des risques et conformité) en fournissant des rapports exhaustifs sur les différentes activités en nuage. Voyons maintenant comment un CASB réalise la GRC :



Gouvernance:

Un CASB peut aider à définir des politiques et des procédures pour établir un contrôle d'accès aux sites Web et aux applications. Cela permet d'aligner les opérations informatiques de manière à ce qu'elles contribuent à la réalisation de l'objectif commercial global. En outre, il offre une meilleure visibilité sur l'utilisation des différentes applications et sites Web du cloud, ce qui facilite la gestion du cloud.

Gestion des risques:

Un CASB permet de garantir la sécurité des données et d'assurer une protection contre les menaces, contribuant ainsi à la gestion des risques. Il alerte également les administrateurs en cas d'interactions malveillantes avec le réseau de l'entreprise.



Conformité:

La mise en conformité est l'une des fonctions intégrales d'un CASB. Elle aide les organisations à se conformer à un large éventail de normes de conformité telles que la loi HIPAA, le GDPR, PCI DSS, etc.

Identifier la solution idéale du CASB

**1**

Trouver le bon ajustement:

Pour identifier le CASB idéal, il faut trouver la bonne solution. Pour cela, les organisations doivent connaître leur position actuelle en matière de sécurité du cloud et leurs exigences de sécurité. Pour ce faire, elles peuvent effectuer des recherches en interne, obtenir un rapport détaillé d'un analyste ou surveiller des organisations similaires dans le secteur. Une fois que les objectifs sont clairs, les entreprises peuvent rechercher la solution qui leur permettra de répondre parfaitement à leurs besoins.

2

Répondre à l'évolution des exigences de sécurité:

Les exigences en matière de sécurité ne cessent de changer à mesure que le volume d'activité augmente. Un CASB doit être capable de résister aux exigences changeantes des organisations et doit pouvoir se défendre contre les attaques provenant du paysage étendu des menaces.

3

Architecture sous-jacente:

Un CASB se décline principalement en trois architectures différentes, à savoir l'approche API, le proxy direct et le proxy inverse. Les proxys avancés garantissent la confidentialité et la sécurité des utilisateurs du côté client en interceptant les demandes adressées aux services en nuage sur le chemin de leur destination. Les proxys inversés, quant à eux, se placent devant un service en nuage et assurent la sécurité en ligne. C'est l'idéal pour les appareils qui se trouvent en dehors du champ d'action du réseau. L'approche API fonctionne en dehors de la bande et ne fournit pas de sécurité en temps réel. Il est essentiel de choisir l'architecture qui correspond aux besoins de l'entreprise.

4

Sécurité de l'infrastructure informatique:

Lors du choix définitif d'un fournisseur, il est essentiel de savoir si la solution peut également surveiller l'ensemble de l'infrastructure informatique, y compris les adoptions IaaS. Cela est essentiel pour les grandes entreprises qui préfèrent souvent le IaaS.

En un mot, les CASB sont devenus un élément vital de la sécurité du cloud et il est essentiel que chaque organisation ait un CASB dans son arsenal de sécurité. Cependant, il est également important qu'une organisation évalue sa position actuelle en matière de sécurité et s'assure que le fournisseur de CASB peut répondre à ses exigences en matière de sécurité avant de décider du fournisseur à retenir.

A propos de l'auteur



Raghav Iyer est un expert en cybersécurité au sein de l'équipe de marketing produit de ManageEngine. Il est un conseiller de confiance en matière de gestion de la sécurité des réseaux et étudie régulièrement les tactiques adoptées par les cybercriminels. Il rédige régulièrement des articles et des guides sur des sujets clés en matière de sécurité informatique afin d'aider les organisations à résoudre leurs problèmes de sécurité. Consultez ses blogs [ici](#).

ManageEngine
Log360 Cloud

ManageEngine Log360 Cloud, une solution cloud SIEM unifiée avec des fonctionnalités CASB intégrées, aide les entreprises à sécuriser leur réseau contre les cyberattaques. Grâce à ses fonctions d'analyse de la sécurité, de renseignement sur les menaces et de gestion des incidents, Log360 Cloud aide les analystes de la sécurité à repérer, hiérarchiser et résoudre les menaces dans les environnements sur site et dans le cloud. menaces dans les environnements sur site et en nuage.

La solution est hautement évolutive et permet de réduire les coûts d'infrastructure et de stockage.

Pour plus d'informations sur Log360 Cloud, visitez le site <https://www.pgsoftware.fr/siem/log360-cloud>

S'INSCRIRE GRATUITEMENT