AYI NEDJIMI Consultants

CASB : Guide Comparatif Cloud Access Security Broker 2026

Catégorie : Cloud Security Lecture : 8 min Publié le : 12/03/2026 Auteur : Ayi NEDJIMI

Guide comparatif CASB Cloud Access Security Broker : architectures proxy et API, DLP cloud, Shadow IT, comparatif Netskope Zscaler et intégration.

L'adoption massive des applications SaaS a créé un défi de visibilité et de contrôle que les solutions de sécurité traditionnelles, conçues pour protéger un périmètre réseau défini, ne peuvent pas adresser. Les utilisateurs accèdent à des dizaines d'applications cloud depuis des réseaux variés et des appareils multiples, partageant des données sensibles dans des services que l'équipe de sécurité ne supervise pas toujours. Les **Cloud Access Security Brokers** (CASB) se positionnent comme intermédiaires entre les utilisateurs et les services cloud pour appliquer les politiques de sécurité de l'organisation. En 2026, le CASB a évolué d'une solution standalone vers une composante intégrée des architectures SASE (Secure Access Service Edge), tout en conservant une pertinence fonctionnelle propre pour le contrôle granulaire des applications SaaS. Ce guide comparatif analyse les architectures de déploiement, les fonctionnalités de sécurité essentielles, les solutions leaders du marché et les stratégies d'intégration dans les architectures de sécurité modernes.

Résumé exécutif

Guide comparatif CASB Cloud Access Security Broker : architectures de déploiement, fonctionnalités de sécurité, comparatif des solutions leaders, intégration dans les architectures SASE et Zero Trust.

Retour d'expérience : le déploiement d'un CASB pour un cabinet d'avocats international a révélé l'utilisation non autorisée de 47 services cloud de partage de fichiers par les collaborateurs, dont 12 contenant des documents clients confidentiels. La mise en place de politiques DLP contextuelles a permis de bloquer les transferts de données sensibles vers des services non approuvés tout en maintenant la productivité des utilisateurs via une migration encadrée vers les services autorisés. Le nombre d'incidents de fuite de données a diminué de 94 % en six mois. Face à la complexité croissante des environnements cloud hybrides et multi-cloud, les organisations doivent adopter des stratégies de sécurité adaptées aux spécificités de chaque fournisseur tout en maintenant une cohérence globale. Les équipes sécurité sont confrontées à des défis inédits : surfaces d'attaque dynamiques, configurations éphémères, gestion des identités à grande échelle et conformité réglementaire multi-juridictionnelle. Ce guide technique présente les approches éprouvées en environnement de production, les erreurs fréquentes à éviter et les stratégies de durcissement prioritaires. Chaque recommandation est issue de retours d'expérience concrets en entreprise et a été validée sur des architectures cloud de production à grande échelle.

Architectures de déploiement CASB

Les CASB se déploient selon trois modes architecturaux complémentaires. Le **mode proxy forward** intercepte le trafic des utilisateurs vers les applications cloud en se positionnant entre le client et le service. Il offre un contrôle inline en temps réel de toutes les interactions, incluant le blocage des actions non autorisées et l'application de politiques DLP sur les données en transit. Le déploiement nécessite la configuration du proxy sur les terminaux (via un agent ou un fichier PAC) et la gestion des certificats TLS pour l'inspection du trafic chiffré. Le **mode proxy reverse** se positionne devant l'application cloud sans nécessiter de configuration client, particulièrement adapté aux accès depuis des appareils non gérés (BYOD, partenaires).

Le **mode API** se connecte directement aux applications cloud via leurs APIs pour scanner les données existantes, appliquer des politiques sur les partages et détecter les comportements anormaux. Ce mode est non intrusif (pas d'interception de trafic) mais fonctionne en mode détection plutôt qu'en mode blocage temps réel, avec une latence variable selon les APIs des applications. La plupart des déploiements modernes combinent le mode proxy (pour le contrôle inline) avec le mode API (pour le scan rétroactif et la gouvernance des données existantes). L'*agent endpoint* ajoute une visibilité locale sur les activités de téléchargement et de synchronisation qui échappent au proxy réseau. Consultez CIS Benchmarks pour les intégrations CASB avec les services AWS. Notre article sur Livre Blanc Nis 2 Directive Guide détaille les stratégies de protection d'accès complémentaires. Les recommandations de ANSSI couvrent l'intégration CASB avec l'écosystème Azure.

Fonctionnalités CASB essentielles

Un CASB complet couvre quatre piliers fonctionnels. La **visibilité** identifie toutes les applications cloud utilisées dans l'organisation (Shadow IT discovery), classifie le risque de chaque application selon des critères de sécurité (chiffrement, certifications, localisation des données) et fournit des métriques d'utilisation par utilisateur et par service. Le **contrôle d'accès** applique des politiques contextuelles basées sur l'identité de l'utilisateur, le type d'appareil, la localisation et la sensibilité de l'action demandée. La *protection des données* (DLP) détecte et protège les données sensibles partagées dans les applications cloud via des classifieurs automatiques, des regex, des fingerprints de documents et du machine learning. La **détection des menaces** identifie les comportements anormaux dans les applications cloud : téléchargements massifs, accès depuis des localisations inhabituelles, partages excessifs et activité de comptes compromis.

Les fonctionnalités avancées incluent le **chiffrement sélectif** des données stockées dans les applications SaaS avec des clés contrôlées par le client, la *tokenisation* qui remplace les données sensibles par des jetons non réversibles, et l'**adaptive access control** qui ajuste les niveaux d'accès en fonction du risque contextuel en temps réel. L'intégration avec les **Identity Providers** (Azure AD, Okta, Google Workspace) permet l'application cohérente des politiques d'accès conditionnel. Le support de l'**API security** étend le CASB à la protection des communications inter-applications cloud. Notre guide sur Kubernetes Offensif Rbac explore les stratégies de gestion des identités qui sous-tendent les politiques CASB. Les benchmarks de Azure Defender for Cloud fournissent des critères d'évaluation complémentaires.

Solution CASB	Forces	Mode principal	Intégration SASE
Netskope	Performance inline, DLP avancé, SSE leader	Proxy + API	Netskope One
Microsoft Defender for Cloud Apps	Intégration M365, coût Azure AD	API + proxy reverse	Microsoft Entra
Zscaler	Architecture cloud-native, scale	Proxy forward	Zscaler Zero Trust
Palo Alto Prisma Access	Intégration pare-feu, DLP unifié	Proxy + API	Prisma SASE
Skyhigh Security	DLP hérité McAfee, MVISION	Proxy + API	Skyhigh SSE
Lookout CASB	Mobile security, data-centric	API + proxy	Lookout SSE

CASB dans l'architecture SASE et SSE

L'évolution du marché a intégré le CASB dans des architectures plus larges. Le *Secure Access Service Edge* (SASE) unifie le réseau (SD-WAN) et la sécurité (CASB, SWG, ZTNA, FWaaS) dans une plateforme cloud-native distribuée. Le *Security Service Edge* (SSE) regroupe les composantes de sécurité du SASE sans le SD-WAN, ce qui correspond au périmètre fonctionnel des CASB étendus. Les leaders du marché SSE en 2026 sont **Netskope**, **Zscaler**, **Palo Alto Networks** et **Microsoft**, chacun proposant une intégration native du CASB dans leur plateforme SSE/SASE.

L'intégration CASB/SSE offre des avantages considérables. La **politique unifiée** applique les mêmes règles de sécurité quel que soit le mode d'accès (web, SaaS, IaaS, accès privé). La **visibilité consolidée** corrèle les événements de sécurité à travers les canaux web, SaaS et réseau. L'**inspection unique** du trafic évite les dégradations de performance liées aux solutions chaînées. La **gestion simplifiée** réduit le nombre de consoles et de politiques à maintenir. Pour les organisations qui débutent leur parcours SSE, le CASB constitue souvent le premier composant déployé car il adresse le besoin le plus urgent de visibilité et de contrôle sur les applications SaaS. Notre article sur Cspm Cloud Security Posture Management explore les aspects réseau complémentaires de la sécurité cloud. L'ANSSI via Azure Defender for Cloud fournit des recommandations sur la sécurisation des accès aux services cloud.

Mon avis : le CASB standalone est en voie de disparition, remplacé par la composante CASB des plateformes SSE/SASE. Les organisations qui achètent un CASB en 2026 devraient privilégier une solution intégrée dans une plateforme SSE qui couvrira également les besoins SWG et ZTNA à moyen terme. La valeur ajoutée du CASB reste cependant intacte pour la visibilité Shadow IT, le contrôle granulaire des actions SaaS et la protection DLP contextuelle, des fonctionnalités que les solutions réseau classiques ne couvrent pas.

Comment choisir un CASB adapté aux besoins de son organisation ?

Le choix d'un CASB doit être guidé par une évaluation multicritère adaptée à votre contexte. **Couverture applicative** : vérifiez que les applications SaaS critiques de votre organisation sont couvertes en mode API et en mode proxy, avec des connecteurs natifs offrant une granularité de contrôle supérieure aux connecteurs génériques. **Capacités DLP** : évaluez la précision des classifieurs pour vos types de données sensibles (données financières, données de santé, propriété intellectuelle) et la capacité à gérer les faux positifs sans bloquer la productivité. **Mode de déploiement** : le proxy forward nécessite un déploiement client mais offre un contrôle temps réel, le mode API est non intrusif mais limité en blocage. **Intégration IdP** : la qualité de l'intégration avec votre fournisseur d'identité détermine la fluidité de l'expérience utilisateur et la richesse des politiques d'accès conditionnel. **Feuille de route SSE** : privilégiez un éditeur avec une stratégie SSE claire si vous prévoyez d'étendre votre périmètre de sécurité cloud. Notre article sur Escalades De Privileges Aws fournit des perspectives complémentaires sur l'évaluation des solutions de sécurité cloud. Consultez CIS Benchmarks pour les intégrations disponibles avec les services AWS.

Pourquoi un CASB reste-t-il pertinent avec le Zero Trust ?

Le Zero Trust et le CASB sont complémentaires, non redondants. Le Zero Trust définit un **modèle d'architecture** basé sur la vérification continue de chaque accès, tandis que le CASB fournit les **capacités techniques** nécessaires pour implémenter ce modèle spécifiquement pour les applications cloud. Le Zero Trust vérifie l'identité et autorise l'accès à l'application, mais ne contrôle pas ce que l'utilisateur fait à l'intérieur de l'application. Le CASB ajoute un *contrôle granulaire intra-application* : autoriser l'accès à OneDrive mais bloquer le partage externe de documents confidentiels, permettre la consultation de Salesforce mais interdire l'export massif de contacts. La **détection du Shadow IT** est une capacité unique du CASB que le Zero Trust ne couvre pas. La **protection DLP contextuelle** sur les données en mouvement vers et depuis les applications SaaS nécessite l'inspection du contenu que seul le CASB réalise à cette granularité. L'intégration du CASB dans une architecture Zero Trust renforce la profondeur de la protection au niveau de la couche applicative.

Quelles sont les différences entre CASB et SASE ?

Le CASB et le SASE opèrent à des niveaux d'abstraction différents qu'il est important de distinguer. Le **CASB** est un composant fonctionnel qui contrôle l'accès et l'utilisation des applications cloud via l'inspection du trafic et les APIs. Il couvre la découverte du Shadow IT, le contrôle d'accès contextuel, la protection DLP et la détection des menaces spécifiques aux applications SaaS. Le **SASE** (Secure Access Service Edge) est une *architecture convergée* qui intègre six composantes : le SD-WAN pour l'optimisation réseau, le CASB pour le contrôle des applications cloud, le SWG (Secure Web Gateway) pour la protection de la navigation web, le ZTNA (Zero Trust Network Access) pour l'accès sécurisé aux applications privées, le FWaaS (Firewall as a Service) pour la protection réseau et le RBI (Remote Browser Isolation) pour

l'isolation des sessions web risquées. Le CASB est donc une pièce du puzzle SASE, la plus spécifique aux applications cloud. Les organisations n'ont pas à choisir entre CASB et SASE mais à décider si elles déploient le CASB en standalone ou dans le cadre d'une adoption progressive du SASE.

À retenir : le CASB reste indispensable pour la visibilité Shadow IT, le contrôle granulaire des applications SaaS et la protection DLP contextuelle. Son intégration dans les architectures SSE/SASE est la trajectoire naturelle pour les organisations qui cherchent à unifier leur sécurité réseau et cloud. Le choix doit privilégier une plateforme avec une feuille de route SSE claire et une couverture native des applications SaaS critiques.

Connaissez-vous le nombre exact d'applications SaaS utilisées dans votre organisation, ou le Shadow IT reste-t-il un angle mort de votre sécurité ?

Sources et références : CISA · Cloud Security Alliance

Perspectives et prochaines étapes

L'évolution du CASB vers le SSE est irréversible, mais les fonctionnalités CASB restent un différenciateur clé entre les plateformes. L'intégration de l'IA générative dans les CASB permet une classification DLP plus précise et une détection comportementale plus sophistiquée. L'émergence de nouveaux risques liés à l'utilisation d'applications d'IA générative (ChatGPT, Copilot, Claude) crée un nouveau cas d'usage pour le CASB : le contrôle des données partagées avec les services d'IA. Les organisations doivent anticiper cette évolution en évaluant les capacités de leur CASB à gérer les interactions avec les applications d'IA générative.

Ayi NEDJIMI Consultants — Expert cybersécurité offensive & intelligence artificielle

ayinedjimi-consultants.fr · ayi@ayinedjimi-consultants.fr