Cloud Access Security Broker (CASB)

Author: Parul Chaudhary, Cloud Security Architect

This document provides a comprehensive overview of the top use cases for Cloud Access Security Brokers (CASBs). As organizations migrate workloads to the cloud, securing access and protecting sensitive data becomes paramount. CASBs offer a strategic layer of control and visibility across cloud environments, enabling organizations to enforce policies, detect threats, and maintain compliance. This guide outlines six key use cases to help decision-makers evaluate the relevance and value of CASB solutions within their cloud security strategy.

Do you actually need a CASB?

Everyone is focused on securing their cloud environments, but the real question is: do you actually need a CASB? And the only way to answer that is by evaluating your specific use cases. Before jumping into solutions, it's important to step back and consider the top six use cases where CASBs truly add value.

Choosing a CASB can be challenging. While the functions it offers may not seem unique, many of them overlap with existing cybersecurity tools—the difference lies in how those functions are delivered.

CASBs are exceptional in enabling visibility and control across cloud access environments, something traditional tools often lack. Your decision should be driven by whether your use cases require that level of cloud-native control and integration.

Use Case 1: Personal Device Security and Control

One of the most critical use cases for a Cloud Access Security Broker (CASB) is securing access from personal or unmanaged devices. This aligns with the core principle of Secure Access Service Edge (SASE), as defined by Gartner—enabling users to access workloads from any device, any location, and any network.

The Challenge

Allowing employees, contractors, or vendors to access cloud environments using personal devices offers flexibility and productivity benefits. However, these devices are typically not managed by the organization, meaning:

- No corporate agent can be installed
- Limited visibility into device posture
- Increased risk of data leakage and malware

How CASB Solves challenges.

CASBs address this challenge using a reverse proxy architecture:

- When a user attempts to access a cloud application, they are redirected through the CASB.
- The CASB intermediates the connection, enforcing security policies without needing an agent on the device.

Security Benefits

- Privacy Respect: CASB only monitors traffic to the cloud app, avoiding intrusion into personal device activity.
- Context-Aware Access: CASB evaluates device context and adjusts authorization levels (e.g., read-only vs. full access).
- Data Leakage Prevention: Policies can restrict downloading sensitive data to personal devices while allowing it on corporate devices.
- Malware Scanning: CASB inspects traffic between the device and cloud to detect and block malware uploads.

Use Case 2: Data Protection

At its core, a **Cloud Access Security Broker (CASB)** is designed to protect sensitive data across cloud environments. It does this by understanding the **context and classification** of the data it interacts with.

Intelligent Data Awareness

CASBs can identify and classify:

- **Personally Identifiable Information (PII)**
- **Payment Card Information (PCI)**
- **Healthcare Data (PHI)**
- Other regulated or sensitive data types

Based on this classification, CASBs can apply **context-aware protection levels** to sensitive data points ensure data is handled appropriately.

Data Manipulation & Privacy Techniques

One of the most commonly used techniques is **pseudonymization**:

- Replaces identifiable data (e.g., full birth date) with generic data (e.g., birth year)
- Maintains analytical value while reducing privacy risk

CASBs also support:

- **Tokenization**: Replacing sensitive data with non-identifiable tokens
- **Minimization**: Removing unnecessary sensitive data

- **Encryption**: Securing data at rest and in transit

Access Control & Rights Management

CASBs enforce granular access policies:

- Control whether data can be **viewed, edited, downloaded, or deleted**
- Adjust permissions based on **user role, device type, and location**

With **API integration**, CASBs can encrypt data within cloud applications while still allowing analytics and search functionality.

Data in Transit Protection

Even data sent via email or shared externally can be scanned:

- CASBs inspect content for sensitive information
- Apply **Digital Rights Management (DRM)** to enforce authentication before access

Use Case 3: Guard Against Account Takeover

In today's cloud-first environments, organizations often manage **dozens to thousands of cloud applications and services**, each with its own user accounts and access controls. This scale introduces a significant risk of **account compromise**, especially when monitoring and behavioral baselines are inconsistent across platforms.

The Challenge

- High volume of cloud accounts across multiple environments
- Limited visibility into user behavior across platforms
- Difficulty detecting subtle anomalies that signal account takeover

How CASB Helps

CASBs use **User Behavioral Analytics (UBA)** and **detailed activity logging** to establish behavioral baselines and detect deviations. They can:

- Monitor user activity patterns over time
- Identify abnormal behavior (e.g., unusual file downloads, access to rarely used directories)
- Trigger **adaptive authentication** or **access restrictions** when anomalies are detected

Security Actions

- Enforce additional authentication for suspicious sessions
- Limit access to sensitive data during anomalous behavior
- Prevent excessive file downloads or unusual browsing activity
- Redirect users to secure workflows or challenge mechanisms before continuing access

This proactive approach helps prevent unauthorized access even when credentials are valid, significantly reducing the risk of **account takeover** in cloud environments.

Use Case: Data Encryption

Data encryption is a critical capability of CASBs, especially when they integrate via **API interfaces** with cloud applications. This allows organizations to:

- **Independently encrypt data** within cloud environments, rather than relying solely on the cloud provider's native encryption.
- Prevent cloud service providers from viewing or accessing sensitive data, even under legal requests or warrants.

Benefits of CASB-Driven Encryption

- **Encryption at rest and in transit** using CASB algorithms
- **Preserves analytics and search functionality** on encrypted data
- **Enhances privacy and control** over sensitive information

This ensures that even if the cloud provider is compelled to share data, the encrypted content remains inaccessible without your keys.

Use Case 5: Identifying Unsanctioned Applications (Shadow IT)

One of the earliest and most valuable CASB use cases is detecting **Shadow IT**—unauthorized cloud applications used by employees.

What CASBs Do

- Identify users accessing unsanctioned apps
- Assign **risk scores** to those applications
- Provide visibility into usage patterns and potential threats

Response Options

- **Educate and coach users** on safe practices
- Allow limited access to low-risk apps (e.g., social media for passive use)
- Monitor posts and interactions for **keywords or sensitive content**
- Maintain an **audit trail** for future investigations or compliance actions

CASBs help balance flexibility with control, ensuring that unsanctioned app usage doesn't compromise organizational security.

Use Case 6: Compliance

Compliance is one of the most common drivers for CASB adoption. CASBs help organizations meet regulatory requirements like:

- **GDPR**
- **CCPA**
- **HIPAA**
- Other global and industry-specific frameworks

CASB Compliance Capabilities

- Provide **policy templates** for major regulations
- Record **data access and movement** across cloud environments
- Support **data subject rights** (e.g., right to be forgotten)
- Enable **pseudonymization**, **minimization**, and **tokenization** of sensitive data

These capabilities ensure that user data is protected and handled in accordance with privacy laws, even in complex multi-cloud environments.

Key Takeaways

1. **CASB adoption is becoming essential**: While still a relatively new concept for many organizations, the shift of over 80% of workloads to the cloud (as per Gartner) makes CASB a critical component of modern cloud security strategies.

2. **Use case-driven decisions are vital**: CASBs are not one-size-fits-all. With over 20 different offerings available, each with unique capabilities, organizations must evaluate solutions based on their specific use cases and security needs.
3. **CASBs are not yet commoditized**: Unlike traditional security tools, CASBs vary significantly in architecture, features, and integrations. This makes vendor evaluation and proof-of-value exercises crucial.
4. **Support for both proxy models is key**: Ensure your CASB supports both **forward proxy** (for managed devices) and **reverse proxy** (for unmanaged or personal devices). This ensures secure access regardless of device ownership.
5. **API integration unlocks deeper control**: Look for CASBs that offer robust API integrations with your cloud platforms. This enables enhanced visibility, automated policy enforcement, and greater control over sensitive data across environments.