# Top 6 Use Cases for Cloud Access Security Brokers (CASB)

By Parul Chaudhary

Cloud Access Security Brokers (CASBs) play a critical role in securing cloud environments. While many security tools offer overlapping capabilities, CASBs are uniquely positioned to provide visibility, control, and protection across cloud applications. Below are six high-impact use cases that demonstrate the value of CASBs.

## 1. Personal Device Security and Control

CASBs enable secure access from unmanaged or personal devices without requiring agents. Using reverse proxy architecture, CASBs intercept cloud access requests and enforce security policies.

* Key Benefits:
* • Enforce access control without installing agents
* • Respect user privacy by monitoring only cloud-bound traffic
* • Prevent data leakage by restricting downloads to personal devices
* • Scan for malware in traffic between device and cloud

## 2. Data Protection

CASBs are designed to protect sensitive data by understanding its context and applying appropriate controls. They can detect PII, PCI, PHI, and other sensitive data types, and apply techniques like pseudonymization.

* Key Capabilities:
* • Identify and classify sensitive data
* • Apply pseudonymization, tokenization, and minimization
* • Enforce access restrictions based on user context
* • Encrypt data while preserving analytics functionality
* • Scan emails and file transfers for sensitive content

## 3. Guard Against Account Takeover

With organizations managing hundreds of cloud environments, the risk of account compromise is high. CASBs use user behavior analytics to detect anomalies and enforce adaptive security measures.

* Key Features:
* • Monitor user behavior for deviations from baseline
* • Trigger additional authentication for suspicious activity
* • Restrict access to sensitive data during anomalies
* • Prevent excessive downloads or unusual directory browsing

## 4. Data Encryption

CASBs can independently encrypt data within cloud applications via API integration, ensuring that even cloud providers cannot access the data.

* Advantages:
* • Encrypt data at rest and in transit
* • Maintain control over encryption keys
* • Prevent unauthorized access by cloud providers or third parties

## 5. Identifying Unsanctioned Applications (Shadow IT)

CASBs help detect and manage the use of unauthorized cloud applications by employees. They provide visibility and risk scoring to inform policy decisions.

* Key Functions:
* • Detect usage of unsanctioned cloud apps
* • Assign risk scores to applications
* • Monitor content for sensitive keywords
* • Maintain audit trails for compliance and investigations

## 6. Compliance

CASBs support compliance with regulations like GDPR, CCPA, and HIPAA by enforcing data protection policies and enabling data subject rights.

* Compliance Support Includes:
* • Pre-built policy templates for major regulations
* • Logging and auditing of data access
* • Identification of data across cloud environments
* • Support for data deletion, pseudonymization, and tokenization