The 15 Critical CASB Use Cases

As people and organizations adopt cloud services, **Cloud Access Security Brokers (CASBs)** have become a must-have for any information security team. CASBs provide critical capabilities such as governing access and activities in sanctioned and unsanctioned cloud services, securing sensitive data and preventing its loss, and protecting against internal and external threats. In short, CASBs enable organizations to extend their information protection policies and programs from their on-premises infrastructure and applications to the cloud. For organizations that are considering deploying CASB, it's useful to consider the specific use cases they're likely to address within these broad topic areas as they inform functional and architectural requirements.

Here's a list of the 15 most critical CASB use cases.

GOVERN USAGE

SECURE DATA

PROTECT AGAINST THREATS

1 Monitor or control advanced or cross-service activities in real time

For example, “Edit in Box,” “Save to Dropbox” from Slack, or enforce which services can integrate and share data with your G Suite

Functional Requirements

- Be aware of context, e.g., activities such as “edit,” “sync,” and “save”
- See and control usage in both sanctioned and unsanctioned (including ecosystem) apps
- Identify and control integration with ecosystem services
- Decrypt SSL and decode the API to understand the transaction (for forward proxy)

Deployment Requirements

- Forward proxy (monitor and control)
- TAP mode (monitor only)

2 Govern access to Office 365 and other cloud services by device ownership class

For example, offer web-based email access only to a BYOD device but full suite access to a corporate one

Functional Requirements

- Understand different authentication protocols and federated identity across Office 365 and other cloud services
- Enforce access and activity policies based on device attributes, including classification of “managed” and “unmanaged”
- Decrypt SSL and decode the API to understand the transaction (for forward proxy)

Deployment Requirements

- Forward proxy
- Reverse proxy

3 Monitor or control users' activities even when they are accessing cloud services from a mobile device, native app, or sync client

For example, disallow sharing even when the user is accessing a Cloud Storage service from a mobile device or a sync client

Functional Requirements

- Be aware of context, e.g., activities such as "share" or "download"
- Inspect and control cloud traffic even when it originates from a native app, sync client, or a mobile device
- See and control usage in both sanctioned and unsanctioned services
- Enforce policy action such as block, coach, or justify in real time
- Decrypt SSL and decode the API to understand the transaction (for forward proxy)

Deployment Requirements

- Forward proxy (monitor and control)
- TAP mode (monitor only)

4 Monitor or control users' activities within Collaboration and Social Media services without blocking those cloud services

For example, block any financial employee from posting "guarantee" or "recommend" on any cloud Collaboration or Social Media service such as Slack or Twitter to comply with FINRA, SEC, and other regulations

Functional Requirements

- Integrate CASB with directory services to focus policy on a specific group, e.g., Investment Banking
- Be aware of context, e.g., activities such as "view," "post," and "create"
- See and control usage in both sanctioned and unsanctioned services
- Detect data violations using advanced DLP features including regular expressions, custom keyword dictionaries, and boolean operators to focus on specific risky activities (e.g., for FINRA) Integration with directory services to focus policy on a specific group (e.g., Finance)
- Decrypt SSL and decode the API to understand the transaction (for forward proxy)

Deployment Requirements

- Forward proxy (monitor and control)
- TAP mode (monitor only)

5 Monitor privileged accounts and prevent unauthorized activity in IaaS instances

For example, disallow creation, edit, or delete of cloud instances, "buckets," or "clusters"

Functional Requirements

- Be aware of context, e.g., activities such as "create" and "edit" and objects such as "instances" and "buckets"
- Determine identity and control usage by user, group, and other enterprise directory attributes
- See and control usage in both sanctioned and unsanctioned services
- Decrypt SSL and decode the API to understand the transaction (for forward proxy)

Deployment Requirements

- API
- Forward proxy

6 Prevent data exfiltration from a sanctioned to an unsanctioned service

For example, prevent the download of confidential content from a corporate-sanctioned service such as Salesforce, Box, or even AWS S3 to a personal Dropbox or other file-sharing service

Functional Requirements

- See and control usage in both sanctioned and unsanctioned services
- Detect sensitive data, e.g., “confidential”
- Identify all unique content in motion and track its movement
- Be aware of context, e.g., activities such as “upload” and “download”
- Correlate users’ identities (e.g., bob@netskope.com = bob123@yahoo.com = bobaran@gmail.com)
- Differentiate between internal and external domains
- Know corporate vs. personal accounts
- Recognize and enforce differing policies between service instances, e.g., corporate and personal
- Decrypt SSL and decode the API to understand the transaction (for forward proxy)

Deployment Requirements

- Forward proxy (monitor and control)
- TAP mode (monitor only)

7 Enforce different policies for personal and corporate instances of the same cloud service

For example, prevent the upload of regulated information (such as that beholden to FISMA, NERC, or PCI) to any Dropbox EXCEPT for the corporate-sanctioned instance of Dropbox

Functional Requirements

- Detect sensitive data, e.g., data beholden to FISMA, NERC, or PCI
- Be aware of context, e.g., activities such as “upload” and “download”
- Know corporate vs. personal accounts
- Recognize and enforce differing policies between service instances, e.g., corporate and personal
- See and control usage in both sanctioned and unsanctioned services
- Decrypt SSL and decode the API to understand the transaction (for forward proxy)

Deployment Requirements

- Forward proxy

8 Enforce layered policies that include a “base” and “exception” policy

For example, prevent the upload of confidential data to ANY Cloud Storage services except corporate sanctioned Google Drive

Functional Requirements

- Detect sensitive data, e.g., “confidential”
- Be aware of context, e.g., activities such as “upload” and “download”
- Recognize and enforce differing policies between service instances, e.g., corporate and personal
- See and control usage in both sanctioned and unsanctioned services
- Enforce “set-it-once” policies across categories of services
- Integrate with enterprise directory to enforce policies at a group or organizational unit level
- Decrypt SSL and decode the API to understand the transaction (for forward proxy)

Deployment Requirements

- Forward proxy

9 Enforce an activity- or data-level policy across a category of services

For example, block the download of personally-identifiable information (PII) from ANY HR service if the user is outside of the HR team

Functional Requirements

- Be aware of context, e.g., activities such as “upload” and “download”
- Correlate users’ identities (e.g., bob@netskope.com = bob123@yahoo.com = bobaran@gmail.com)
- See and control usage in both sanctioned and unsanctioned services
- Integrate with enterprise directory to enforce policies at a group or organizational unit level
- Decrypt SSL and decode the API to understand the transaction (for forward proxy)

Deployment Requirements

- Forward proxy

10 Enforce conditional activity-level policies

For example, block the sharing of content by a corporate 'insider' with anyone outside of the organization from ANY Cloud Storage service if it is the organization's financial reporting quiet period

Functional Requirements

- Be aware of context, e.g., activities such as "share"
- See and control usage in both sanctioned and unsanctioned services
- Differentiate between internal and external domains
- Enforce "set-it-once" policies across categories of services
- Detect and enforce policies by IP address, network location, or geo-location
- Integrate with enterprise directory to enforce policies at a group or organizational unit level
- Decrypt SSL and decode the API to understand the transaction (for forward proxy)

Deployment Requirements

- Forward proxy

11 Apply encryption based on conditional factors

For example, apply strong encryption with enterprise key management to confidential intellectual property such as next-generation product designs

Functional Requirements

- Be aware of context, e.g., activities such as “upload”
- See and control usage in both sanctioned and unsanctioned services
- Apply strong encryption to sensitive content with enterprise key management
- Integrate with KMIP-compliant, on-premises key manager
- Decrypt SSL and decode the API to understand the transaction (for forward proxy)

Deployment Requirements

- Forward proxy
- Reverse proxy

12 Detect and alert on user login anomalies

For example, detect users logging into a cloud service from two different locations with the same credentials, indicating a potentially compromised account

Functional Requirements

- Correlate users' identities (e.g., bob@netskope.com = bob123@yahoo.com = bobaran@gmail.com)
- See usage in both sanctioned and unsanctioned services
- Use machine learning to detect cloud behavior anomalies
- Detect IP addresses, network location, or geo-location
- Decrypt SSL and decode the API to understand the transaction (for forward proxy)

Deployment Requirements

- API
- Reverse proxy
- Forward proxy

13 Prevent data infiltration involving new employees

For example, block new employees from uploading confidential data from their previous employer to their new company's sanctioned cloud service

Functional Requirements

- Integrate "new employee" policy with enterprise directory
- Use custom keyword dictionary to delineate sensitive competitor documents
- Decrypt SSL and decode the API to understand the transaction (for forward proxy)

Deployment Requirements

- API
- Forward proxy
- Reverse proxy

14 Block or remediate malware in sanctioned and en route to/from unsanctioned cloud services, even in sync/ native clients and mobile devices

For example, detect, quarantine, and remediate malware being downloaded from unsanctioned cloud services in real time

Functional Requirements

- Inspect, detect, block, and remediate malware in sanctioned cloud services
- Inspect, detect, block, and remediate malware en route to/from unsanctioned cloud services
- Have visibility over cloud traffic even if it's coming from a sync client, native app, or mobile device
- Decrypt SSL and decode the API to understand the transaction (for forward proxy)

Deployment Requirements

- API
- Forward proxy
- Reverse proxy

15 Detect anomalies such as excessive downloads, uploads, or sharing within both sanctioned and unsanctioned services

For example, detect excessive download of sensitive customer data from Salesforce

Functional Requirements

- Be aware of context, e.g., activities such as “download” and “share”
- See and control usage in both sanctioned and unsanctioned services
- Use machine learning and rules to detect anomalies that could signal risky behavior, non-compliance, data exposure, or even malware
- Decrypt SSL and decode the API to understand the transaction (for forward proxy)

Deployment Requirements

- API
- Forward proxy
- Reverse proxy

GOVERN USAGE

- Monitor or control advanced or cross-service activities in real time
- Govern access to Office 365 and other cloud services by device ownership class
- Monitor or control users' activities even when they are accessing cloud services from a mobile device, native app, or sync client
- Monitor or control users' activities within Collaboration and Social Media services without blocking those cloud services
- Monitor privileged accounts and prevent unauthorized activity in IaaS instances

SECURE DATA

- Prevent data exfiltration from a sanctioned to an unsanctioned service
- Enforce different policies for personal and corporate instances of the same cloud service
- Enforce layered policies that include a "base" and "exception" policy
- Enforce an activity- or data-level policy across a category of services
- Enforce conditional activity-level policies
- Apply encryption based on conditional factors

PROTECT AGAINST THREATS

- Detect and alert on user login anomalies
- Prevent data infiltration involving new employees
- Block or remediate malware in sanctioned and en route to/from unsanctioned cloud services, even in sync/native clients and mobile devices
- Detect anomalies such as excessive downloads, uploads, or sharing within both sanctioned and unsanctioned services