The 20 Most Common CASB Use Cases

Govern +

Secure +

+ Protect

netskope

As people and organizations adopt cloud applications and services, Cloud Access Security Brokers (CASBs) have become a must-have for any information security team. CASBs are a key component of an overall Security Service Edge (SSE) solution and they provide critical capabilities such as governing access and activities in managed and unmanaged cloud services, securing sensitive data and preventing its loss, and protecting against internal and external threats. CASBs enable organizations to extend their information protection policies and programs from their on-premises infrastructure and applications to the cloud. When used with a Secure Web Gateway (SWG), CASB provides an integrated SSE solution for cloud and web security. 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 20 most common CASB use cases.

Govern Usage

1. Govern access to Microsoft 365 and other cloud services by device ownership class
2. Monitor privileged accounts and prevent unauthorized activity in IaaS instances
3. Monitor or control users' activities within Collaboration or Social Media without blocking those services
4. Monitor or control advanced or cross-service activities in real time
5. Protect against password email abuse
6. Monitor or control users' activities even when they are accessing cloud services from a mobile or desktop app or sync client

Secure Data

7. Prevent data exfiltration from an IT-lmanaged to any cloud service
8. Enforce different policies for personal and corporate instances of the same cloud service
9. Monitor sensitive data in Amazon S3 buckets
10. Enforce an activity- or data-level policy across a category of cloud services
11. Enforce conditional activity-level policies
12. Enforce layered policies that include a "base" and "exception" policy
13. Apply encryption based on conditional factors

Protect Against Threats

14. Block or remediate malware in IT-managed and in motion to/from from business-led cloud services
15. Detect and alert on user login anomalies
16. Detect anomalies such as excessive downloads, uploads, or sharing within both IT-managed and business-led services
17. Find and protect sensitive data embedded in images
18. Block and quarantine zero-day malware in the cloud
19. Detect encrypted data movement as part of ransomware attacks
20. Prevent data infiltration involving new employees

Govern access to Microsoft 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 Microsoft 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 unpublished API to understand the transaction (for forward proxy)

Deployment Requirements

- Forward proxy, for example, Netskope Next Gen Secure Web Gateway (NG-SWG)
- Reverse proxy (IT-managed only, browser only), for example, Netskope NG-SWG deployed as a reverse proxy

2

Govern Usage +

< Back to TOC

+

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 IT-managed and business-led services
- Decrypt SSL and decode the unpublished API to understand the transaction

Deployment Requirements

- API (IT-managed only)
- Forward proxy, for example, Netskope Next Gen Secure Web Gateway (NG-SWG)

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

For example, block any financial employee from posting "guarantee" or "recommend" alongside a stock ticker or company name on any Collaboration or Social Media service like Slack or Twitter to comply with FINRA 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 IT-managed and business-led services
- Detect data violations using advanced data protection and DLP features including regular expressions, custom keyword dictionaries, and Boolean operators to focus on specific risky activities (e.g., for FINRA) or to set policies for a specific group (e.g., Finance)
- Decrypt SSL and decode the unpublished API to understand the transaction

Deployment Requirements

- Forward proxy (monitor and control), for example, Netskope Next Gen Secure Web Gateway (NG-SWG)

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 IT-managed and business-led (including ecosystem) apps
- Identify and control integration with ecosystem services
- Decrypt SSL and decode the unpublished API to understand the transaction

Deployment Requirements

- Forward proxy (monitor and control), for example, Netskope Next Gen Secure Web Gateway (NG-SWG)

Protect against password email abuse

For example, block passwords being sent via any webmail app

Functional Requirements

- Cloud DLP with custom keyword dictionaries to incorporate any variation of keyword that may signal that a password is being shared
- Cloud DLP support for business-led webmail accounts (hundreds)
- Support for category-level policies with specific support for webmail
- Decrypt SSL and decode the unpublished API to understand the transaction

Deployment Requirements

- Forward proxy, for example, Netskope Next Gen Secure Web Gateway (NG-SWG)
- Reverse proxy (IT-managed only, browser only), for example, Netskope Next Gen Secure Web Gateway (NG-SWG)

Monitor or control users' activities (even when they are accessing cloud services from a mobile or desktop app or sync client)

For any of the real-time use cases that require a forward proxy, support should be extended to mobile apps, desktop apps, and sync clients

Functional Requirements

- Inspect and control cloud traffic even when it originates from a mobile or desktop app or sync client
- See and control usage in both IT-managed and business-led services
- Enforce policy action such as block, coach, or justify in real time
- Decrypt SSL and decode the unpublished API to understand the transaction (for forward proxy)

Deployment Requirements

- Forward proxy (monitor and control), for example, Netskope Next Gen Secure Web Gateway (NG-SWG)

7

Secure Data +

< Back to TOC

Prevent data exfiltration from an IT-managed to any cloud service

For example, prevent the download of confidential content from a corporate-IT-managed 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 IT-managed and business-led services
- Detect sensitive data, e.g., “confidential”
- Identify all unique content in motion and track data movement
- Be aware of context, e.g., activities such as “upload” and “download”
- Visibility into each user’s identities in use (e.g., bob@netskope.com = bob123@yahoo.com = bobaran@gmail.com)
- Differentiate between internal and external domains
- Know and seecorporate vs. personal account use
- Recognize and enforce differing policies between service instances, e.g., corporate and personal
- Decrypt SSL and decode the unpublished API to understand the transaction
- Visiblity into data exfiltration activities in a user interface that is easy to understand

Deployment Requirements

- Forward proxy (monitor and control) , for example, Netskope Next Gen Secure Web Gateway (NG-SWG)

8

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- IT-managed 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 IT-managed and business-led services
- Decrypt SSL and decode the unpublished API to understand the transaction

Deployment Requirements

- Forward proxy (monitor and control), for example, Netskope Next Gen Secure Web Gateway (NG-SWG)

9

Secure Data +

< Back to TOC

+

Monitor sensitive data in public cloud storage, including Amazon S3 buckets

For example, alert when PCI data is discovered in AWS S3 buckets

Functional Requirements

- Cloud DLP that can scan public cloud storage, including S3 buckets
- Specify all or individual S3 buckets
- Incident management workflow

Deployment Requirements

- API (IT-managed only)

Enforce an activity- or data-level policy across a category of cloud 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”
- Visibility into each user’s identities (e.g., bob@netskope. com = bob123@yahoo.com = bobaran@gmail. com)
- See and control usage in both IT-managed and business-led services
- Integrate with enterprise directory to enforce policies at a group or organizational unit level
- Decrypt SSL and decode the unpublished API to understand the transaction

Deployment Requirements

- Forward proxy, for example, Netskope Next Gen Secure Web Gateway (NG-SWG)

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 IT-managed and business-led 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 geolocation
- Integrate with enterprise directory to enforce policies at a group or organizational unit level
- Decrypt SSL and decode the unpublished API to understand the transaction

Deployment Requirements

- Forward proxy, for example, Netskope Next Gen Secure Web Gateway (NG-SWG)
- Reverse proxy (IT-managed only, browser only), for example, Netskope NG-SWG deployed as a reverse proxy

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

For example, prevent the upload of confidential data to ANY Cloud Storage service except corporate IT-managed Google Drive

Functional Requirements

- Support for policies with “allow” and “block” actions
- Support for category-level policies
- Differentiate between instances of cloud services

Deployment Requirements

- Forward proxy, for example, Netskope Next Gen Secure Web Gateway (NG-SWG)
- Reverse proxy (IT-managed only, browser only), for example, Netskope NG-SWG deployed as a reverse proxy

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 IT-managed and business-led services
- Apply strong encryption to sensitive content with enterprise key management
- Integrate with KMIP-compliant, on-premises key manager
- Decrypt SSL and decode the unpublished API to understand the transaction

Deployment Requirements

- Forward proxy, for example, Netskope Next Gen Secure Web Gateway (NG-SWG)
- Reverse proxy (IT-managed only, browser only), for example, Netskope NG-SWG deployed as a reverse proxy

Block or remediate malware in IT-managed and in motion to/from business-led cloud services

For example, detect, quarantine, and block malware being downloaded from any cloud service in real time

Functional Requirements

- Inspect, detect, block, and remediate malware in IT-managed cloud services
- Inspect, detect, block, and remediate malware in motion to/from business-led cloud services
- Decrypt SSL and decode the unpublished API to understand the transaction

Deployment Requirements

- API (IT-managed only)
- Forward proxy, for example, Netskope Next Gen Secure Web Gateway (NG-SWG)
- Reverse proxy (IT-managed only, browser only), for example, Netskope NG-SWG deployed as reverse proxy.

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 IT-managed and business-led services
- Use artificial intelligence and machine learning to detect behavior anomalies
- Detect IP addresses, network location, or geo-location
- Decrypt SSL and decode the unpublished API to understand the transaction

Deployment Requirements

- API (IT-managed only)
- Reverse proxy (IT-managed only, browser only), for example, Netskope NG-SWG deployed as a reverse proxy
- Forward proxy, for example, Netskope Next Gen Secure Web Gateway (NG-SWG)

Detect anomalies such as excessive downloads, uploads, or sharing within both IT-managed and business-led 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 IT-managed and business-led services
- Use artificial intelligence, machine learning and rules to detect user and entity behavior anomalies that could signal risky behavior, non-compliance, data exposure, or even malware
- Decrypt SSL and decode the unpublished API to understand the transaction

Deployment Requirements

- API (IT-managed only)
- Forward proxy, for example, Netskope Next Gen Secure Web Gateway (NG-SWG)
- Reverse proxy (IT-managed only, browser only), for example, Netskope NG-SWG deployed as a reverse proxy

Find and protect sensitive data embedded in images

For example, find and stop patient data embedded in an x-ray image or a screenshot of a zoom video conference being uploaded to a personal cloud service

Functional Requirements

- Cloud DLP with AI/ML-enhanced image detection and OCR (Optical Character Recognition) capability
- Ability to scan IT-managed cloud services with cloud DLP features including AI/ML-enhanced image detection and OCR capability
- Ability to apply image detection and OCR to cloud traffic to and from business-led cloud services

Deployment Requirements

- API (IT-managed only)
- Forward proxy, for example, Netskope Next Gen Secure Web Gateway (NG-SWG)
- Reverse proxy (IT-managed only, browser only), for example, Netskope NG-SWG deployed as a reverse proxy

Block and quarantine zero-day malware in the cloud

For example, detect and quarantine new strains of malware present in IT-managed cloud services and block this type of malware en route to and from business-led cloud services

Functional Requirements

- Support for cloud-based inspection with dynamic analysis using a cloud-based sandbox
- Support for multiple threat intelligence mechanisms including external and internal
- Support quarantine workflows that are malware-centric

Deployment Requirements

- API (IT-led only)
- Forward proxy, for example, Netskope Next Gen Secure Web Gateway (NG-SWG)
- Reverse proxy (IT-managed only, browser only), for example, Netskope NG-SWG deployed as a reverse proxy

Detect encrypted data movement as part of ransomware attacks

For example, alert when advanced User and Entity Behavior Analytics (UEBA) detects unusual encrypted data movement, often an indicator of ransomware.infection

Functional Requirements

- Integration with advanced User and Entity Behavior Analytics and the AI/ML encrypted data classifier to detect unusual encrypted data movement
- Use and integrate with Netskope Private Access (ZTNA), Advanced Analytics, and CSPM/SSPM to reduce exposure to ransomware

Deployment Requirements

- Forward Proxy

Prevent data infiltration involving new employees

For example, block new employees from uploading confidential data from their previous employer to their new company's IT-managed 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 unpublished API to understand the transaction

Deployment Requirements

- API (IT-managed only)
- Forward proxy, for example, Netskope Next Gen Secure Web Gateway (NG-SWG)
- Reverse proxy (IT-managed only, browser only), for example, Netskope NG-SWG deployed as a reverse proxy

Govern Usage

1. Govern access to Office 365 and other cloud services by device ownership class
2. Monitor privileged accounts and prevent unauthorized activity in IaaS instances
3. Monitor or control users' activities within Collaboration or Social Media without blocking those services
4. Monitor or control advanced or cross-service activities in real time
5. Protect against password email abuse
6. Monitor or control users' activities even when they are accessing cloud services from a mobile or desktop app or sync client

Secure Data

7. Prevent data exfiltration from an IT-managed to any cloud service
8. Enforce different policies for personal and corporate instances of the same cloud service
9. Monitor sensitive data in Amazon S3 buckets
10. Enforce an activity- or data-level policy across a category of cloud services
11. Enforce conditional activity-level policies
12. Enforce layered policies that include a "base" and "exception" policy
13. Apply encryption based on conditional factors
14. Find and protect sensitive data embedded in images

Protect Against Threats

15. Block or remediate malware in IT-managed and en route to/from business-led cloud services
16. Detect and alert on user login anomalies
17. Detect anomalies such as excessive downloads, uploads, or sharing within both IT-managed and business-led services
18. Block and quarantine zero-day malware in the cloud
19. Detect encrypted data movement as part of ransomware attacks
20. Prevent data infiltration involving new employees

Netskope, a global cybersecurity leader, is redefining cloud, data, and network security to help organizations apply Zero Trust principles to protect data. The Netskope Intelligent Security Service Edge (SSE) platform is fast, easy to use, and secures people, devices, and data anywhere they go. Netskope helps customers reduce risk, accelerate performance, and get unrivaled visibility into any cloud, web, and private application activity. Thousands of customers, including more than 25 of the Fortune 100, trust Netskope to address evolving threats, new risks, technology shifts, organizational and network changes, and new regulatory requirements.

Learn how Netskope helps customers be ready for anything on their SASE journey, visit netskope.com.