ManageEngine
Log360

Cloud access security broker (CASB)

manageengine.com/log-management

What is a cloud access security broker (CASB)?

- ✓ A CASB is a security solution that acts as a gatekeeper to monitor the interaction between users and cloud applications.
- ✓ It provides visibility into user activity, cloud applications, and file uploads to ensure security policies are enforced.

Why do you need a CASB?

- ✓ **Regulate user access:** Enforces security policies to control cloud access.
- ✓ **Protect sensitive data:** Monitors and encrypts data in transit.
- ✓ **Stop data exfiltration:** Identifies and restricts unauthorized data transfers.
- ✓ **Monitor shadow IT:** Detects and manages unsanctioned cloud applications.
- ✓ **Ensure compliance:** Helps meet industry data security and access requirements.
- ✓ **Stop app duplication:** Audits cloud service usage to optimize costs.
- ✓ **Secure collaboration:** Protects resource-sharing platforms from exploitation.

Use cases of CASB

Shadow IT monitoring

Detect unauthorized cloud applications and ensure compliance with security policies.

Monitor sensitive data uploads

Monitors and prevents unauthorized data uploads to the cloud.

User risk tracking

Tracks risky user behavior, such as accessing banned applications.

Pillars of CASB

Visibility

Provides insights into user activity, including app usage and data transfer.

Data security

Monitors and protects sensitive data moving to/from the cloud.

Compliance

Helps organizations meet regulatory requirements like PCI DSS, HIPAA, and GDPR.

Threat detection

Identifies unusual patterns and flags potential security threats.

Use cases of CASB

CASBs operate in three deployment modes:

Forward proxy

All traffic from the organization is routed through the CASB for monitoring.

Reverse proxy

User requests to cloud apps are validated via CASB before access is granted.

API scanning

Directly connects with cloud apps to scan data at rest for security issues.

CASB architecture

Forward proxy

Intercepts outbound traffic for deep packet inspection (DPI) and policy enforcement.

Reverse proxy

Redirects user requests to cloud apps through the CASB, ensuring security checks.

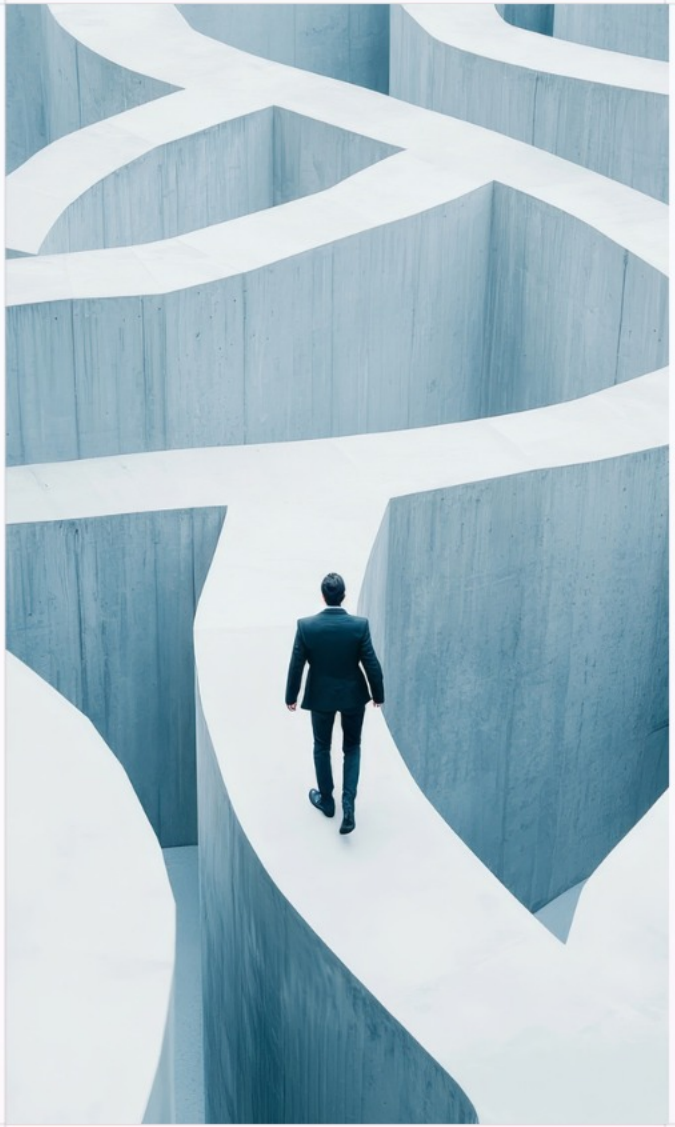
API scanning

Monitors cloud data interactions via API integrations, ensuring content security.

Choosing a CASB solution

When evaluating a CASB, consider the following:

- ✓ Security needs and goals
- ✓ Integration with existing tools like SIEM
- ✓ Visibility into shadow IT
- ✓ Scalability and reporting features
- ✓ Actionable data and cost-effectiveness



CASB in action with Log360

ManageEngine Log360 integrates CASB features to:

- ✓ Provide visibility into cloud app usage
- ✓ Enhance identity and access management
- ✓ Ensure compliance and data security
- ✓ Detect and respond to cloud-based threats

CASB in healthcare

CASBs protect sensitive patient data, ensure compliance with HIPAA, and monitor cloud-based medical apps to prevent unauthorized access and data breaches.

CASB in banking and finance

CASBs safeguard financial data, prevent unauthorized cloud access, and ensure compliance with regulatory standards like PCI DSS, GLBA, and GDPR.

CASB in education

CASBs help educational institutions manage user access to cloud services, prevent shadow IT, and ensure secure collaboration for students, faculty, and staff.

CASB and Zero Trust

CASBs complement Zero Trust principles by securing cloud access, monitoring user behavior, and integrating with SIEM solutions for granular control over cloud-based resources.

ManageEngine
Log360

Thank you

manageengine.com/log-management