What is a cloud access security broker (CASB)?

Learn how cloud access security brokers provide visibility, data control, and analytics to identify and combat threats.

Discover Microsoft Defender for Cloud Apps

CASB defined | Key benefits of CASBs | Four cornerstones of CASBs | How to implement a CASB | Top use cases for CASBs | The role of CASBs for businesses

Cloud access security broker (CASB) defined

A cloud access security broker, often abbreviated (CASB), is a security policy enforcement point positioned between enterprise users and cloud service providers. CASBs can combine multiple different security policies, from authentication and credential mapping to encryption, malware detection, and more, offering flexible enterprise solutions that help ensure cloud app security across authorized and unauthorized applications, and managed and unmanaged devices.

Key benefits of CASBs

CASBs offer a range of security benefits that allow enterprises to mitigate risk, enforce policies across various applications and devices, and maintain regulatory compliance.

Shadow IT assessment and management
CASBs deliver visibility into all cloud applications, sanctioned and unsanctioned. Enterprises can employ a CASB to obtain a comprehensive picture of cloud activity and enact security measures accordingly.

Granular cloud usage control
CASBs offer detailed management of cloud usage with strong analytics. Enterprises can limit or allow access based on employee status or location, and can govern specific activities, services, or applications.

Data loss prevention (DLP)
A CASB's DLP capabilities help security teams protect sensitive information like financial data, proprietary data, credit card numbers, health records, or social security numbers. A CASB solution can enable policies that prevent unauthorized sharing of this data.

Risk visibility
CASBs allow enterprises to assess the risk of unsanctioned applications and make access decisions accordingly.

Threat prevention
CASBs detect unusual behavior across cloud applications, identifying ransomware, compromised users, and rogue applications. CASBs can analyze high-risk application use and automatically remediate threats, limiting an organization's risk.

Understanding CASBs

Why use a CASB?

In the modern work era, enterprises are responsible for increasingly complex security enforcements between users and cloud-based applications. Traditional binary security systems only block or allow access, and no longer serve a cloud-based enterprise contending with multiple locations and devices. A CASB allows an organization to take a nimble, flexible approach to security policy enforcement, providing tailored options for the contemporary workforce and balancing access with data security.

Four cornerstones of CASBs

Visibility
CASBs allow IT departments to identify all cloud services in use and assess subsequent risk factors. For enterprises grappling with shadow IT, CASBs offer a comprehensive understanding of all cloud-based applications employees are accessing. Risk assessments then provide information to shape IT's access policy, including more detailed controls based on specific employee and device criteria.

Data security
A core component of a CASB system, data loss prevention (DLP) extends an enterprise's security to all data traveling to, within, and stored in the cloud, reducing the risk of costly data leaks. A CASB protects both the data itself as well as the data's movement.

Threat protection
By aggregating and understanding typical usage patterns, CASBs can identify anomalous behavior and recognize malicious activities. Adaptive access control, malware mitigation, and other capabilities help protect the enterprise from third party or internal threats. CASB threat protection defends against all modern threats, whether malicious or negligent.

Compliance
CASBs help ensure compliance with data privacy and safety regulations, and monitor compliance for enterprises requiring adherence to regulatory standards like HIPAA or PCI DSS.

How does a CASB work?

CASBs use a three-part process to offer visibility across sanctioned and unsanctioned applications and control over enterprise data in the cloud.

Discovery

The CASB identifies all cloud applications in use as well as affiliated employees.

Classification

The CASB assesses each application, identifies its data, and calculates a risk factor.

Remediation

The CASB creates a tailored policy for the enterprise based on its security needs. From there the CASB identifies and remediates any incoming threats or violations.

How to implement a CASB

CASBs are easy to deploy and use. While most CASBs are deployed in the cloud, on-premise options are available. CASBs operate with three different deployment models, and multimode CASBs that utilize all three offer the most flexibility and robust protection.

API scanning

Available for sanctioned enterprise applications, API scanning is an unobtrusive security measure for data at rest in the cloud, but it does not offer real-time prevention.

Forward proxy

Forward proxy offers DLP in real time for both sanctioned and unsanctioned applications, but only applies to managed devices, and cannot scan data at rest.

Reverse proxy

A reverse proxy redirects all user traffic, and therefore works for both managed and unmanaged devices. It offers DLP in real time, but only on sanctioned applications.

Top use cases for CASBs

Discover all cloud apps and services in use

Shadow IT can comprise up to 60 percent of an enterprise's cloud services. A CASB offers a full picture of all cloud-based applications in use.

Assess risk and compliance in cloud-based apps

Assess general security, regulatory compliance, and legal factors for any cloud-based app your enterprise uses.

Enable monitoring to detect new and risky cloud apps

A CASB's continuous monitoring policies help to ensure your enterprise is alerted to new cloud-based services and spikes in usage.

Enforce DLP and compliance policies for sensitive data stored in your cloud apps

CASBs enforce DLP policies as soon as data arrives in the cloud, and help enterprises locate sensitive files in the cloud and provide remediation options.

Protect data on unmanaged devices

Configure granular access to prevent downloads or apply protection labels on unmanaged devices.

Detect and remediate malware in cloud apps

CASBs monitor and identify malicious files in cloud-based apps, offering remediation options to enable enterprises to react quickly.

Learn more use cases for CASBs

The role of CASBs for businesses

In the evolving cloud-based workplace, CASBs will continue to play a vital role in enterprise security. Multiple vendors offer multimode CASB security services—when evaluating options, consider the changing security landscape, and determine if a given CASB will continue to progress along with your enterprise's needs. A CASB should work in tandem with other elements of your enterprise's security strategy to help protect your users and data, so make sure your CASB integrates with your enterprise's security architecture.

What to consider when weighing CASB options:
- Existing enterprise security architecture
- What capabilities and features the enterprise requires
- Implementation time
- Ease of use
- Compliance certification needs

Products and services available with CASBs:
- Data loss prevention
- Malware detection
- Adaptive access control
- Behavior analytics
- Web application firewalls
- Authentication
- Collaboration control
- Encryption

Learn more about Microsoft cloud security

Cloud security solutions
Get integrated protection for multicloud apps and resources.
Learn more >

Microsoft Defender for Cloud
Strengthen cloud security and monitor and protect workloads across multicloud environments.
Learn more >

Microsoft Defender for Cloud Apps
Gain comprehensive DLP in real time and view user activity across multiple cloud services.
Learn more >

Frequently asked questions

Expand all | Collapse all

- What is a CASB solution?
- What types of integrations does a CASB have?
- What is a CASB used for?
- How do you choose a CASB?