**Cloud Access Security Broker (CASB)**

A cloud access security broker (CASB - often pronounced cas-bee) is a software application that resides between cloud applications and cloud service users to monitor all activity and enforce security policies. A CASB can perform multiple functions including user activity monitoring, issuing warning signals to administrators regarding potentially hazardous actions, security policy compliance check and enforcement, and automatic detection and prevention of malware.

**What are Cloud Access Security Brokers?**

A CASB delivers security management. In this sense, "security" is the prevention of high-risk events, and "management" is the monitoring and mitigation of high-risk activities.

CASBs that provide security must be located along the data access path between the cloud or data center and the user. You can achieve this with proxy agents on each end-point device, or in agentless fashion without requiring any configuration on each device.

Agentless CASBs offer rapid deployment and deliver security on both company-managed and unmanaged [Bring Your Device](https://www.simplilearn.com/how-to-avoid-byod-pitfalls-at-work-article) (BYOD) hardware. Besides, an agentless CASB also respects user privacy, inspecting only corporate data. In contrast, Agent-based CASBs are challenging to deploy and valid only on devices that are managed by the corporation. Agent-based CASBs typically examine both corporate and personal data depending on the access rights on a device (for instance, Apple's iOS restricts CASBs from accessing private data).

CASBs that deliver management can use APIs to inspect data and activity in the cloud to alert of risky events. Another management capability of a CASB is to check firewall or proxy logs for the usage of cloud applications.

API-only CASBs offer management using APIs provided by the major software as a Service, SaaS, applications.

Finally, multi-mode CASBs offer both management and security. Some multi-mode CASBs may also offer Zero-Day capabilities to protect against threats, both known and unknown.

Now that we have understood what are Cloud Access Security Brokers, let us next understand their use cases.

How Do You Use CASB?

There are four main reasons why you will use CASB. They are:

* Visibility: a CASB will offer a view of the entire Cloud service usage throughout a company. This view is a way to verify the services being used in IT and identify cloud services outside of IT. Some companies leverage CASB to test shadow-IT work.
* Data Security: You can use CASB to enforce security policies.
* Threat Protection: On the flip side of security policies is the ability to identify threats to your data.
* Compliance: you can use CASB to verify that you comply with your data.

Organizations are using CASB vendors to address cloud service risks, enforce security policies, and comply with regulations, even when cloud services are beyond their perimeter and out of their direct control.

After having learned so much about Cloud Access Security Brokers, let us next understand how they are disrupting the cloud security industry.

How are CASB Disrupting the Cloud Security Industry

Leading think tanks such as Gartner are now recommending that you implement a CASB in your organization. The rationale is sound: when your company is working with a [Cloud provider](https://www.simplilearn.com/selecting-the-right-cloud-provider-article), your data must, at some point, leave your company. The challenge to Cloud providers is to prove that your data is secure, has not been intercepted, and complies.

A good example can be seen with companies managing data in countries such as Russia with substantial data restrictions. With a CASB, you can monitor the data in Russia and verify if the data stays in compliance. An example of this is that the data is stored in Russia.

As you can imagine, companies now see a CASB as an additional cost. There are three types of vendors looking to serve you with a CASB as your company interacts with Cloud providers. They are:

* Start-Ups
* Security Firms
* Cloud Vendors

There are several good startups you can review for CASB support. The leading companies include:

* Netskope
* Bitglass
* Cipher Cloud
* Proofpoint

The security firms that implement CASB solutions include:

* Symantec
* McAfee

The leading cloud provider for CASB solution is Microsoft. AWS does not have a CASB solution and relies on third-party vendors in their AWS Marketplace to fill the gap.

After going through on how Cloud Access Security Brokers are disrupting the cloud security industry, let us look at the acceptance of CASB by cloud companies.

How Cloud Companies are Embracing CASB

Cloud companies such as AWS, Azure, Google Cloud, and IBM want you to know that your data is secure and compliant. The need for Cloud Access Security Brokers is a service that meets the need to ensure security with a cloud provider. To this end, you will find all leading CASB providers offered in cloud provider marketplaces for third party products. Indeed, companies such as AWS will even go to the level of providing [training on how to implement CASB](https://pages.awscloud.com/AWSMP-H2-SEC-McAfee-CASB.html) with your AWS cloud services. All participants must agree that the end goal is that no matter where the data is in your company, you are providing every means possible to secure the data.

For your next steps, if you have not implemented a CASB, but you do leverage cloud services, then you will want to consider developing a CASB implementation plan.