Whitepaper 9/2018 (C) Dr. Dipl. Ing. Bernhard Bowitz

Almost every platform has its own version of a CASB:

AWS CASB - CASB DLP – NETSCOPE CASB – ORACLE CASB – MICROSOFT CASB – IBM QRADAR – SYMANTEC CASB – BITGLASS CASB …..

The Cloud Access Security Broker (CASB) is a service or application that secures cloud applications. The CASB is located between the user and the cloud and is able to monitor, log and control communications.

The Cloud Access Security Broker is designed to protect the applications of a company or organization that have been moved to the cloud. It is a special software or service that can analyze, control and log the communication between the user and the cloud application. This allows the CASB to monitor communications, prevent unwanted traffic, and alerted to suspicious actions.

Using a Cloud Access Security Broker extends and enforces internally enforced security policies on external services. For example, this may be necessary to comply with the compliance guidelines of an organization or regulated industry. Unwanted use of cloud services, such as those caused by shadow IT, is prevented by the CASB.

The CASB also makes it possible to create secure access requirements by allowing users to authenticate and encrypt all traffic. These security policies are defined in advance and then enforced by the Cloud Access Security Broker. Other areas of application include the logging of all actions in the cloud and the verification of cloud usage for billing purposes with the provider.

The different implementation types of a Cloud Access Security Broker

The technical implementation of the Cloud Access Security Broker may vary. Many of the systems are based on one of the two basic CASB architectures. These are:

- The Cloud Access Security Broker as a central gateway
- The Cloud Access Security Broker as an API application

If the Cloud Access Security Broker is implemented as a central gateway, it is located between the cloud applications and the users. It can be located directly in front of the cloud, monitoring all communication with the services, or being installed on the edge of a company's on-premise network and analyzing all outside traffic. It is powered on in the data stream and can control and influence access to cloud services. Unwanted cloud usage can be blocked directly by the CASB. The disadvantage of this architecture is that the performance of the communication may suffer and the CASB has to be scaled with the number of users and applications.

The API-based Cloud Access Security Broker is outside the actual communication between the user and the application. It is connected to the cloud application via an application programming interface (API). Through this he receives information about the use of the services and the connected users. Direct blocking of data is usually not possible. The advantage of this configuration is that the performance of the cloud applications is not influenced by the CASB. API-based Cloud Access Security Brokers are suitable for installations with a large number of users and applications.

Typical functions of the CASB

The typical features of a Cloud Access Security Broker are:

- Analysis and monitoring
- enforcement of security policies
- Alerting to initiate incident actions
- Monitoring and reporting

Thanks to the monitoring and analysis of the communication, the CASB knows which users are using which cloud applications. He can determine if a user is authorized for the application. According to the pre-established security policies, it allows or excludes users from the cloud applications. In addition, user rights within the application can be checked or the sending and receiving of unencrypted data can be prohibited. Monitoring and reporting provide comprehensive reports that can be used for capacity planning, billing for services or subsequent analysis of cloud usage.

In the event of suspicious actions or detected misconduct, the CASB automatically alerts. This will enable administrators to take manual incident action and adjust security policies or block dangerous traffic.