Cloud Access Security Brokerage Services (CASB)

Extend your internal security policies to cloud services

Cloud access security brokerage (CASB) is a series of services which allow for customers to extend their internal security policies to cloud services.

This allows consumers of cloud services to have similar levels of control of the data and access requirements over the usage cloud services as they would for internally hosted services.

CASB is a complimentary technology to existing network infrastructure providing visibility into cloud usage.

Cloud Access Security Brokers (CASB) are security enforcement points between consumers and service providers that apply security controls to access cloud services, usually SaaS services. They may also control access to internal company resources. Security controls may include authentication (credentials and passwords), single sign on, authorisation policy enforcement, device profiling tokenisation, logging, alerting, intrusion prevention, antimalware filters, security logging/auditing, and encryption.

"CASB provide protection for threats related to user behaviour and use of sensitive data threats."

The four pillars of CASB

CASB is not a single solution, but rather a set of security solutions centred around four pillars. They are: Visibility, Compliance, Data Security, and Threat protection.

Pillar One: Visibility

In many sanctioned applications, very few provide basic audit or even activity logs, causing visibility to be a large gap. CASB addresses this by providing audit-level logging, alerts and reports. For example, a CASB will alert you that a user is simultaneously attempting to log into Salesforce from Auckland, and into Box from Sydney – an indication of a potential compromise. CASB enables the ability for an organisation to enumerate cloud services in use and who is using them. CASBs provide both shadow and sanctioned IT discovery, as well as a consolidated view of an organisations cloud service usage and the users who access

data from any device or location. Shadow IT discovery helps a CASB identify high risk traffic leaving the corporate network. Leading CASBs take this further with a cloud service security posture assessment database to provide trust through visibility into the cloud service provider.

Pillar Two: Threat Protection

CASBS provide protection for threats related to user behaviour and use of sensitive data threats. For example, login from geographically diverse locations, or users attempting to download a sensitive database to their BYOD device. CASBs prevent unwanted devices users and versions of applications from accessing cloud services by providing adaptive access controls. Other examples in this category are user and entity behaviour analytics (UEBA) for determining anomalous behaviour, the use of threat intelligence, and malware identification. In some cases, CASB providers have their own analyst teams researching cloud-specific and cloud-native attacks.

Pillar Three: Compliance

Many cloud vendors don't offer the appropriate visibility and data protection tools to remain compliant with regulations. CASB addresses this and can help fill the gaps. For example, CASB can provide audit logs, encrypt sensitive data at rest and enforce data leakage prevention policies. CASB enables the ability for an organisation to comply with governing security standards while consuming the identified cloud services. CASBs assist with data residency and compliance with regulations and standards, as well as identify cloud usage and the risks of specific cloud services. Organisations still need to prove they can meet internal and external compliance mandates and show how they can show the five W's of who, what, when, where, and why. CASBs also help by controlling access to the cloud.

Pillar Four: Data Security

CASBs monitor access to data and vary the level of access to ensure that it is risk appropriate. It enables the ability to enforce data-centric security policies to prevent unwanted activity based on data classification, discovery, and user activity monitoring of access to sensitive data or privilege escalation. Policies are applied through controls, such as audit, alert, block, quarantine, delete and encrypt/tokenise, at the field and file level in cloud services. These policies govern the level of access that a user may have to an application over variables such as role, device, geography. For example, an organisation may allow full access to Office365 from a managed

device but allow only email and web from unmanaged BYOD devices, thereby minimising the amount of sensitive data that can be downloaded on an unmanaged device.

Encryption key management may be integrated with any on-premises product. Data loss prevention (DLP) features are both natively included in CASB products as well as available from on-premises network DLP products via ICAP integration. DLP looks at the data being accessed and makes decisions, in conjunction with an access control engine for example, e.g. a CASB may quarantine a spreadsheet that contains sensitive data and that is being shared outside an organisation. Data-centric audit and protection (DCAP) features are also being addressed natively by some CASBs, as well as traditional on-premises DCAP providers now covering cloud usage use cases.

Visibility

- Shadow IT usage
- Content flowing in and out of cloud
- Audit level logging, alerts and reports

Threat Protection

- Detect and block data
- Adaptive access controls
- User and entity behavioural analytics

Compliance

- Achieve compliance with internal policies and external industry regulation
- Visibility and data protection tools

Data Security

- Protect data from unauthorised access
- Data Loss Prevention
- Encryption Key management
- Data centric Security policies

Cogito Group is an award-winning ICT company specialising in authentication, cloud security, identity management and data protection. Cogito Group protect the authentication methods used to access information through the use of Identity and other security technologies.

Cogito Group
www.cogitogroup.net