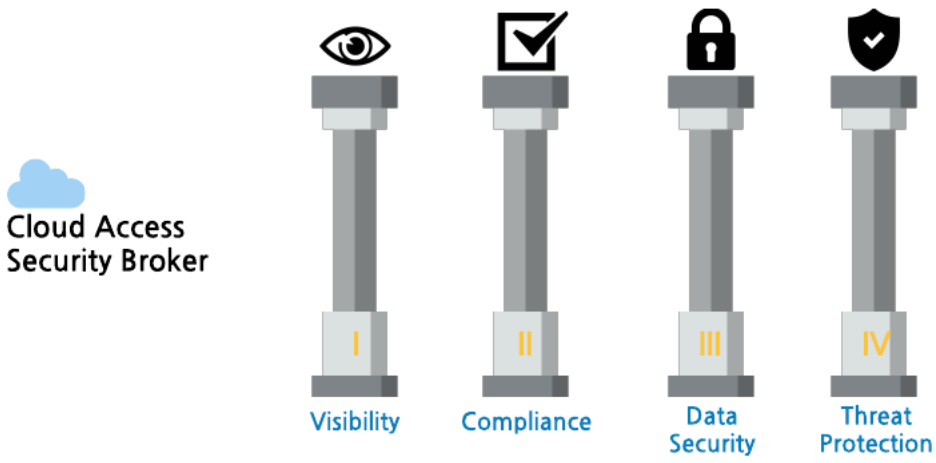
Cloud Access Security Broker – Use Cases

What is a CASB?

A Cloud Access Security Broker (CASB) is a service designed to reduce the risk of an organisation's usage of both IT sanctioned, and unsanctioned cloud applications (so called 'Shadow IT'). Imagine a firewall in the cloud which helps to extend the controls you currently have inside your organisation into the cloud environment.
Each vendor in this space has strengths and weaknesses, but a general consensus is that a CASB must carry out four important functions. Depending on your use cases, and which is the primary driver for looking at CASB, Armadillo can advise on the most suitable vendor to meet your needs.

Pillar I: Visibility

Typically, if you were to ask a CISO how many cloud applications there are in use within an organisation, whatever the number stated, often the real number is four or five times that amount. The first stage of securing your cloud usage is to determine which applications are being used, and what the business risk is associated with each. A CASB should provide a simple means of taking an output from your existing firewall or web proxy and determining the services accessed and the business risk of each. One example is an online document conversion service, whose terms and conditions assume you forfeit the intellectual property rights to any document uploaded. Another might be a file sharing application which is outside the jurisdiction of the EU GDPR regulations.



Pillar II: Compliance

If you have a need to comply with data residency requirements, or storage of data within PCI, HIPAA or other regulatory contexts, a CASB can help in both compliance and audit against these frameworks. CASBs can help fill in the audit visibility gaps, which often exist in sanctioned cloud applications. CASB offers a wide variety of data loss prevention (DLP) capabilities, which ensure that sensitive data is not stored in cloud environments that are not designed for such content. Encryption policies can be applied to data being stored in certain applications to ensure compliance, or even take data outside of the reach of GDPR.

Armadillo Managed Services Ltd
8 The Square, Stockley Park, Heathrow, UB11 1FW
tel: +44 (0)208 0888222 | email: hello@wearearmadillo.com | web: https://www.wearearmadillo.com

Pillar III: Data Security

CASB provides additional visibility and control into how sanctioned cloud applications are being used. Using this metadata, security policies can be created to prevent cloud applications from being accessed from certain locations – for example, making Salesforce accessible from the corporate network only, or only from corporate managed devices. Documents stored on corporate cloud file stores, such as OneDrive or box, can be scanned for over-permissive sharing and automatically remediated by quarantining those files in a secure area, only accessible to the IT team.

Pillar IV: Threat Protection

The final pillar uses rules and machine learning to detect unusual use of cloud applications. The presence of malware can be detected within sanctioned applications and deleted or quarantined to reduce the risk of compromise inside your organisation, or the reputational damage when sharing files with customers or business partners. Unusual behaviour, such as logging on from a different geographical area, or a user who normally changes a few records each day, downloading the whole sales database.

Whatever your primary use case, Armadillo can help you measure your risk with a free cloud risk assessment. We can then support you with advice, set up vendor demos, or even run an RFP on your behalf. Upon selecting a vendor, we can help with the professional managed services required to get maximum value from your investment.