Fact Sheet

Cogito Group

Cloud Access Security Brokerage Architecture

CASB Architecture

There are two primary methods of providing a Cloud Access Security Brokerage (CASB) service. When organisations adopt a CASB they must decide between proxy or API services. Architecture is foundational and therefore difficult to change. Both proxy and API types of architecture will provide organisations with control and visibility into data in cloud applications. Proxy-based CASBs are networking vendors who process traffic like web Gateway vendors. This is a more difficult engineering exercise than that of using APIs. Therefore, it is relatively easy for a proxy vendor to begin supporting API's, but not in the reverse.

Proxy-Based CASB

The proxy approach is an inline services approach or an inline gateway, that is, a control point that sits between the enterprise and the service provider. The control point leverages traditional packet inspection techniques to inspect the traffic travelling through the control point, and then makes policy enforcement decisions dependent the needs of the enterprise. The primary benefit of the proxy approach is real-time protection, where traffic goes through the proxy in real-time, the proxy then inspects the information and makes real-time enforcement decisions, such as blocking a user from going to a site or preventing them from sharing or emailing documents.

Forward Proxy

A forward proxy setup aims at securing the client computers. In most cases, the client's requests come from the internal network behind the proxy servers. The service views the request as originating from the proxy server rather than the client, i.e. it hides the identities of the clients. The response received by the proxy server is then redirected to the client who made the request. A forward proxy can only support managed devices. Forward proxy servers are used with a firewall to improve the internal network security and to control the traffic directed to the services.

Reverse Proxy

A reverse proxy aims at securing services. In most cases, client requests that go through the proxy server originate from the internet. The reverse proxy receives all the requests (from the client) for the services. The client will have no knowledge of the service servers behind the proxy server as it hides the identities of the services.

The reverse proxy supports both managed and unmanaged devices. The reverse proxy also balances the load, important for a high availability of services. A reverse proxy can distribute all incoming requests to a group of servers providing the same kind of service and will have one or two firewalls set up to control the traffic.

Advantages

- Proactive not reactive solution. Data can be reported and acted upon, meaning data loss doesn't occur as it would in the API-based solution, preventing compromise.
- Ability to alter rulesets in real time.
- Can maintain organisational control over some data, such as personal privacy data, as an organisation can still maintain existing controls such as firewalls.
- No need for endpoint configuration changes on Enterprise, BYO, or CYO Devices.
- All traffic from managed devices goes through the CASB, giving IT more visibility into unsanctioned SaaS usage.
- Covers RESTful and JSON-based access.
- Transport-layer encryption is handled reasonably well in the forward-proxy architecture.
- Existing Secure Web Gateway (SWG) deployment can be used to redirect traffic to the CASB via proxy chaining.

Unlike the API approach, the proxy approach does not require the manufacture/service provider to support CASB services. It can support many applications and services that do not provide an interface for CASB. This allows it to support older services and services that have no wish to integrate with CASB offerings. There may be many reasons why some service providers do not support CASB services, such as concerns about performance, the effort involved in supporting these applications on top of existing resource limitations, and their own competing products or those of their partners. Office 365 is one example where the vendor (Microsoft) provides limited or no support for third party CASB offerings for encryption and tokenisation services.

Disadvantages

- URLs are rewritten with reverse-proxy method, making it hard to enforce for mobile SaaS apps that use hard-coded URLs.
- CASB becomes single point of failure, making the SaaS usage vulnerable to DDoS risk and latency.
- Personal data privacy concerns exist as all traffic from managed endpoints goes through the CASB.
- Hard to address BYOD scenarios and unmanaged devices in general.

Cloud Access Security Brokerage Architecture

Fact Sheet

API Based CASB

The API approach is an out-of-band approach that leverages APIs to connect to the cloud provider. It inspects the state, health, and compliance of the cloud service on behalf of the enterprise. It may also determine what is happening in the cloud service itself. APIs ensure you have complete coverage and visibility of web-based or SaaS applications like Salesforce or Office 365, and of IaaS providers like AWS, Azure, or Rackspace. The main disadvantage of the API approach is that is does not provide inline protection. Rather than preventing a breach of policy, it notifies the organisation that one has occurred.

About Cogito Group

Cogito Group is an award-winning, Australian owned and operated 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 protect data not only from unauthorised access and disclosure, but also from being altered by an unauthorised third party or a trusted insider with malicious intent. This assists in the detection and prevention of fraud or other malicious activities by third parties or trusted insiders.