



# CASB Architecture

Proxy or API

## CASB Architecture

There are two primary methods of providing a CASB service and when organisations adopt a CASB they must decide between:

- Proxy, or
- API

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; they process traffic like web Gateway vendors. This is a more difficult engineering exercise than that of using API's. Therefore, it is relatively easy for a proxy vendor to begin supporting API's, but not 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 going through it, and then make policy enforcement decisions, depending on what the enterprise wants. The primary benefit of the proxy approach is the notion of real-time protection, where traffic goes through the proxy in real time, the proxy inspects the information and then makes real-time enforcement decision, such as blocking a user from going to a site or preventing them from sharing or emailing a document.

*“Both proxy and API architecture will provide organisations with control and visibility into data in cloud applications.”*

## 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 right client who made the request. The 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.



*“The API approach is an out of band approach that leverages APIs to connect to the cloud provider.”*

## Reverse Proxy

A reverse proxy aims at securing the 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 i.e. it hides the identities of the services. The reverse proxy supports both managed and unmanaged devices. The reverse proxy also balances the load, and this feature is important for high availability of the services. A reverse proxy can distribute all the 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, stopping the compromise from occurring in the first place

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

There is no need for endpoint configuration changes on Enterprise, BYO or CYO Devices

### Disadvantages

URLs are rewritten with reverse-proxy method; this makes 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 because all traffic from managed endpoints goes through the CASB

Hard to address BYOD scenarios and unmanaged devices in general



**Cogito Group**

[www.cogitogroup.net](http://www.cogitogroup.net)



## Advantages

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. Some are 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 for example.

## Disadvantages

### 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 be able to 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 it does not provide inline protection. Rather than preventing a breach of policy it notifies the organisation that one has occurred.



## Advantages

Smaller footprint within and organisations premises and smaller impact on changes within the environment.

Less resource utilisation in terms of bandwidth and CPU usage

Non-intrusive solution that is not in the data path of the SaaS application

Can be used in a complementary manner with the proxy approaches

Allows for content-based controls for activities involving data that has already been uploaded to the cloud

Provides reliable information on what data is in the cloud, permissions associated with that data, and activity logs of all activity by both administrators and users

## Disadvantages

Reactive not proactive solution. Data is reported on, not acted on meaning you would get a report of a compromise rather than stopping the compromise from occurring in the first place.

May mean that the organisation's existing controls such as firewalls are circumvented by direct API connections resulting in less protection of data such as privacy data.

TLS sessions are not inspected. This must be done by existing methods

Not all SaaS applications offer API support and, of those that do, capabilities differ across providers

SaaS applications that do have APIs may not yet support a full feature set for implementing CASB features

Enterprise, BYO and CYO device endpoints may require additional configuration

Cannot provide for some basic CASB features, for example, DLP, encryption and tokenization

Applications and appliances must support the API based approach. This means that many new and most older services may not support this approach and those that do may do so to varying degrees depending on the manufacturer/provider.