National Conference on Communication Technology & Network Security In association with International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2019 IJSRCSEIT | Volume 4 | Issue 7 | ISSN : 2456-3307

CASB - Cloud Access Security Broker

Jyoti Bolannavar
Asst. Professor, Department of Computer Science, Govt. First Grade College, Naregal, Tq: Ron Dist: Gadag, State: Karnataka, India

ABSTRACT

With cloud technology becoming a larger and more important part of running a digital business, cloud computing platforms are rapidly limiting the effectiveness of the traditional security model. The cloud has required organizations to rethink security. Since data and applications in the cloud reside outside the old enterprise boundaries, they must now be protected in new ways. As more and more users connect directly to public cloud applications, and as workloads continue to shift to leverage Infrastructure-as-a-Service and Platform-as-a-Service capabilities from providers, a category of products called Cloud Access Security Brokers (CASB) has emerged to prominence and has become the go-to solution to address challenges in cloud security. Over the years, CASBs have evolved to keep pace with the rapid cloud adoption trends. This paper is an attempt to define some of the key capabilities that organizations look for in a CASB solution.

I. INTRODUCTION

Cloud computing has brought a variety of services to potential consumers. Many companies typically access around 600 services, mostly of the SaaS type. Those companies also have internal resources and governing access to external and internal resources can be a complex logistic problem in that access to those services need to be controlled because they may provide access to highly sensitive enterprise data. Although the service provider (SP) may have a strong security infrastructure, it does not understand the semantics of the applications running on it and the consumer must control access to its sensitive information. A new type of system software has recently appeared that can organize the management of these applications; this is the Cloud Access Security Broker (CASB). A CASB becomes a key part of the IT governance structure of the institution. Access to the company resources may come from portable devices such as smartphones, tablets, and laptops, and there is also a need to grant some user's temporary access to cloud applications; all this variety can be conveniently handled by CASBs. A CASB is also an important part of cloud ecosystems. An ecosystem is the expansion of a software product line architecture to include systems outside the product which interact with the product.

What is CASB?

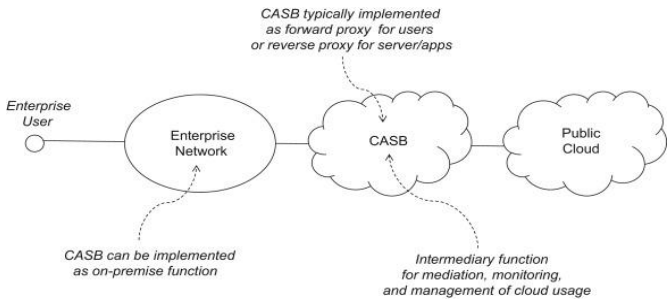
A cloud access security broker (CASB) is a software tool or service that sits between an organization's on-premises infrastructure and a cloud provider's infrastructure. A CASB acts as a gatekeeper, allowing the organization to extend the reach of their security policies beyond their own infrastructure.

CASBs typically offer the following:

- **Firewalls:** to identify malware and prevent it from entering the enterprise network.

- **Authentication:** to checks users' credentials and ensure they only access appropriate company resources.
- **Web application firewalls (WAFs):** to thwart malware designed to breach security at the application level, rather than at the network level.
- **Data loss prevention (DLP):** to ensure that users cannot transmit sensitive information outside of the corporation.

Architecture of CASB and working of CASB



How CASBs work

There are two key ways that a CASB can work. It can be set up as a proxy — either a forward or a reverse proxy — or it can work in API mode, using cloud providers' APIs to control cloud access and apply corporate security policies. Increasingly CASBs are becoming "mixed mode" or "multi-mode," using both proxying and API technology. That's because each approach offers pros and cons.

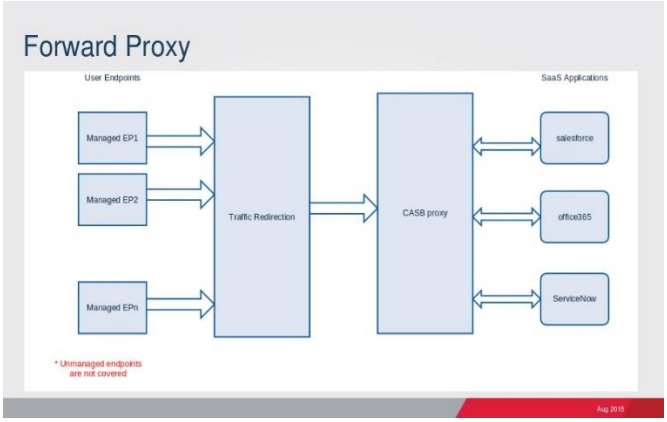
Proxy mode

A CASB deployed in proxy mode is “inline”; network traffic between users and cloud applications flows through the CASB proxy.

This is achieved in one of two ways:

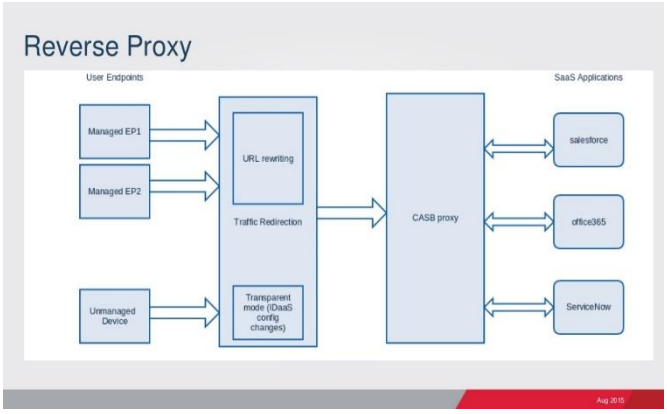
Forward proxy

For example, a forward proxy can be used for all types of cloud applications and all data passes through the proxy, but to use a forward proxy you need to install self-signed certificates on every single device that accesses the proxy. This can be difficult to deploy in a distributed environment or one with a large number of employee-owned mobile devices.



Reverse proxy

A reverse proxy system is easier in that respect because it is accessible from any device, anywhere, without the need for special configuration or certificate installation. The drawback is that a reverse proxy can't work with client-server type apps, which have hard-coded hostnames.



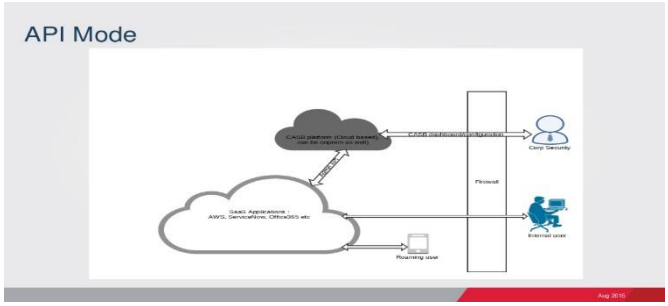
Proxy mode allows CASBs to implement very granular access controls. Proxy mode also gives the CASB visibility into data in motion and allows it to enforce policies in real time. For example, the CASB can ensure that files being uploaded are encrypted, and can block the download of sensitive files to noncompliant devices. It can also generate alerts in real time, allowing security teams to react

immediately to security incidents, policy violations, and anomalous behaviours.

However, proxy mode takes longer to implement. To route traffic to the CASB proxy, changes need to be made to network devices and endpoints (for forward proxy), or to applications (for reverse proxy). Also, some implementations of forward proxies require the installation of software agents on endpoint devices, which may be impossible with unmanaged devices. Further, some reverse proxies can break application functionality

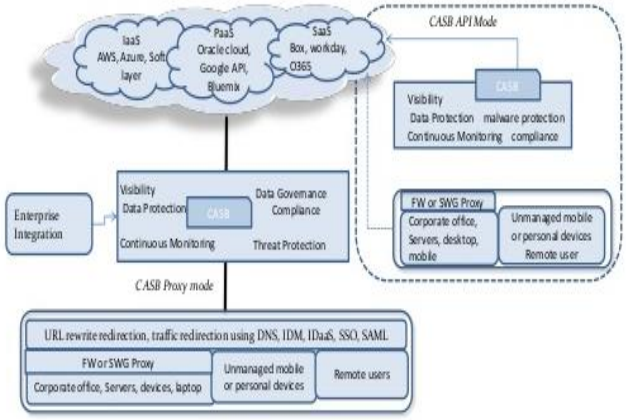
API mode

A CASB deployed in API mode is "out of band"; users communicate directly with cloud applications, and the CASB obtains data from the applications through their APIs. This approach provides very detailed visibility into data at rest and user activities, including logins and logouts, file uploads and downloads, information sharing, and administrative actions. CASBs deployed in API mode can also perform administrative tasks and enforce governance policies. For example, if a user violates policies by publicly sharing files containing sensitive information, administrators can use the CASB to change the access permissions on the files, or to take file ownership away from the offending user. A major advantage of API mode is speed: a CASB can be implemented literally in minutes because no changes to networks, endpoint devices, or applications are needed.



Hybrid mode

Some CASBs offer a hybrid mode that combines API mode and proxy mode. This allows the CASB to support a wide range of use cases with visibility, policy enforcement, and ways to deal with unmanaged devices.



Key CASB capabilities

- **Discovery, visibility and security across all cloud applications and resources** A CASB solution must provide a complete view into cloud access, irrespective of where users are located.

The solution should streamline security assessment across your cloud ecosystem:

- SaaS apps in use
- IaaS and PaaS providers your business relies on.

It should enable a security-first approach to compliance with support for pre-built and customizable compliance reports. It needs to provide means to remediate risks as they arise. Proactive monitoring of the entire cloud stack is an important consideration.

Most organizations today have adopted the cloud, and a majority of them have adopted a multi-cloud strategy. While BYOD policy at these organizations have increased productivity and lowered costs, Infrastructure-as-a-Service (IaaS) services and Software-as-a-Service (SaaS) apps need cloud app security to prevent threats, protect sensitive data and meet regulatory compliance needs. A Cloud Access Security Broker (CASB) solution must provide cloud security with visibility and control over sanctioned

and unsanctioned cloud services to enable safe and productive use. In addition, any CASB should be able to ensure that the initial or discovered state of the cloud service meets all the requirements of the organization to achieve the minimum acceptable security posture and standards.

- **Continuous Security Assessment for IaaS, SaaS & PaaS** The growth and rapid adoption of Infrastructure-as-a-Service (IaaS) has introduced the need for a Cloud Security solution to also cover the same. A Cloud Access Security Broker solution must be able to provide protection and security for all cloud use, whether SaaS, IaaS or PaaS, specifically by continuously monitoring security configuration for these environments, CASB should ensure that the services are configured appropriately and any change in configuration that results in a state change of the cloud service is captured and appropriate users are alerted. A CASB may also provide sensitive data discovery, protection and cloud Data Loss Prevention capabilities. Additionally, as the number of cloud services increase, it is very difficult to identify and manage the ongoing configuration changes that the service provider makes. Getting specific talent to manage these complexities are not easy either. A good CASB solution should provide a rich set of policies out of the box that will help organizations get an assured security posture right away, without the dependence on service expertise. For example, as enterprises adopt IaaS services, they need to have the expertise to understand not just the IaaS provider's compute, network, storage and security capabilities, but also need to understand the underlying infrastructure components and configuration. Not doing so may result in accidentally opening up the infrastructure to vulnerabilities. Ideally a CASB solution should have readily deployable security policies across cloud services that will reduce the barrier to adoption, improve time to value and enhance the overall security posture.
- **User & Entity Behaviour Analytics (UEBA) with Machine Learning & Threat Protection** By their very nature, cloud services, particularly the control plane of these services, are accessible via the internet. It is not only necessary to understand who is using these services but also to ensure that the vast threat surface opened up as a result is constantly monitored. That is where UEBA brings profiling and anomaly detection based on machine learning to security. UEBA essentially maps what legitimate processes look like when they take place in an enterprise and learns how to distinguish and stop threats. A CASB solution must incorporate UEBA to deliver actionable intelligence and provide protection against internal and external threats. The solution should be able to detect unusual user activity and data movement and compromised credentials that could indicate internal or external threat to a cloud environment.
- **Integration with Identity and Access Management** **Identity and Access Management** is a key element in the security of an operating cloud and is usually the first level in a defence-in-depth strategy of an organization. Understanding and defining user authentication and authorization among cloud actors is an important aspect of cloud security. A CASB solution as an open platform must provide seamless and standards-based integration with existing Identity and Access Management solutions or Identity-as-a-Service solutions.
- **Data Security and Application Security** typically covers integration aspect with SaaS applications. Risks to data security is the exposure of data at rest and data in motion. A CASB solution should be able to address Data Security for the cloud. Further, any CASB must provide cloud service specific insights, this includes the risk posture of the app, usage patterns and risky behaviour within the apps. While multi-modal CASBs support the

use of proxies, introduction of such infrastructure components complicate the deployment and increase adoption time.

- **Cloud Delivered – Responsive & Reliable For businesses,** the increasing sophistication of attacks means traditional approaches to security no longer provide adequate protection. Many organizations have now started to agree that cloud security as-a-service offerings can provide better security than on premise hardware or software security offerings. A CASB solution must be fast, responsive and highly reliable.
- **Non-Intrusive & Frictionless User Experience** A CASB solution must provide bullet-proof security without impacting productivity. It must provide required protection without causing slowdown and without affecting device performance. Additionally, the CASB solution should have sufficient APIs to integrate with other security solutions to facilitate remediation. Ideally, a CASB solution should be agentless hence reducing any friction to adoption by users.

Advantages of CASB include:

- Policy-based services--consumers can define security policies, e.g., RBAC, to apply to the services they use in order to restrict the access of their employees and customers to cloud data.
- Secure channel—the channel to access cloud services can be encrypted. Data encryption—CASBs can let consumers encrypt their data using their own keys.
- Compliance—consumers can demonstrate compliance with specific regulations because CASBs normally include security loggers/auditors.
- Discovery—users at the company are able to find out what services they have available through the CASB.
- Transparency—security is transparent to the application consumers when they use the CASB, they would only know about the CASB if an attempted access is rejected.
- Access unification—Consumers do not need to deal with a variety of credential types and protocols.
- Heterogeneity—access to the cloud can be made from any type of device.
- Malware detection—access to the cloud application through a CASB can guarantee that no malware will be found in the accessed service.
- Logging/auditing—the CASB keeps logs for security and compliance reasons; these can be later audited.
- Identity—the CASB can provide identification services.

Liabilities of CASB include:

- Complexity due to using different types of credentials. It can be fixed by using some standard such as SAML for all the credentials.
- If the consumers encrypt their data with their own keys, the SP cannot search that data and cannot apply its procedures to it.
- The CASB may incur in possible privacy violations, but careful use of its security controls can improve users' privacy.

II. Conclusion

In this paper we have presented the know-how about the Cloud Access Security Broker (CASB), which the ongoing and a go to market solution for protection of sensitive data being hosted by different vendors' trough cloud applications on different cloud platforms. And we also discussed about working modes of CASB along with its capabilities, advantages and disadvantages.

III. REFERENCES

[1]. [Sky14] Skyhigh Networks, "What is a cloud access security broker?",2014 http://www.skyhighnetworks.com/cloud-

university/what-is-cloud-access-security-broker/

[2]. [McV13] Lori McVittie, “The mounting case for cloud access brokers”, Virtualization Journal, Feb. 8, 2013.

[3]. https://pdfs.semanticscholar.org/fecb/163673cb5f87a40826dec5b1b4a796b60e8a.pdf

[4]. https://4b0e0ccff07a2960f53e707fda739cd414d8753e03d02c531a72.ssl.cf5.rackcdn.com/w-content/uploads/2015/12/Definitive-Guide-to-CASB_HPE-eBook.pdf

[5]. https://blog.cloudsecurityalliance.org/2016/08/11/api-vs-proxy-get-best-protection-casb/

[6]. https://www.slideshare.net/cisoplatform7/workshop-on-casb-part-2

Cite this article as :

Jyoti Bolannavar, "CASB - Cloud Access Security Broker", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 4 Issue 7, pp. 171-176, September-October 2019.
Journal URL : http://ijsrcseit.com/CSEIT194732