ManageEngine
Log360 Cloud

Greasing the cloud security wheel with CASB

www.manageengine.com/cloud-log-management/

Table of contents

Cloud security wheel with **CASB**

Organizations have been considering cloud migration a top priority while formulating business strategies since the start of the decade. This is because of the capabilities of the cloud such as location independence, ubiquitous access, and elasticity that can be used to enhance business.

The lift and shift approach made it easier for organizations to achieve this by helping them migrate data and applications from on-premises to cloud with minimal or no changes. Many organizations securely and successfully migrated their productivity suites and web applications to the cloud.

While the cloud provides competitive advantages and makes organizations agile at a reasonable cost, on the other side, it started exposing vulnerabilities that resulted in huge financial losses, data leakages, and compliance violations, often resulting in increased costs.

Now, with experts anticipating the public cloud service market to reach $623.3 billion by 2023 worldwide, and with an explosive rate of enterprises trying to shift their business-critical applications like finance and HR systems, the need to secure the cloud environment has become critical.

Further, while migrating, the architectural differences between on-premises and cloud, security has become the major concern for organizations irrespective of whether they're using Software as Service (SaaS), Platform as Service (PaaS), or Infrastructure as Service (IaaS).

By including a cloud access security broker (CASB) in their security arsenal, organization can gain thorough visibility into their cloud environments. In this paper, we discuss how CASB makes cloud security comprehensive.

Gliding through the current **cloud security landscape**

Evolution

Cloud security has come a long way since the day cloud computing was first conceived. Initially, during the emergence of cloud computing, the focus was predominantly on facilitating flexibility, collaboration, and resource sharing. Though the lift and shift approach enabled organizations to move to the cloud quickly, due to the architectural differences, security became a huge concern. Further, the usage of cloud to store sensitive business information upped the ante.

This prompted service providers to devise strategies to ensure cloud security. From authorization to background verification of users trying to access critical information, cloud service providers (CSPs) came up with a range of security policies to better secure cloud data and reassure users that using the cloud is safe.

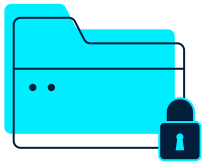
Since multiple clients use the cloud to store information, virtual boundaries were established to ensure data isolation, ensuring that no client could access the information of another client.

Though CSPs took utmost care to secure their environments, clients still have certain responsibilities to ensure security of passwords and connection at their end.

Cybercriminals and their shenanigans

Cybercriminals have enjoyed the unanticipated extension of oranizations' network perimeters and their weakened security, which motivated them to come up with strategies to exploit vulnerabilities in the cloud.

Attacks ranged from account hijackings to malware injections and were large in scale. Since multiple tenants were involved, attackers were able to get their hands on data of several organizations, making it difficult for the service provider and the client to detect and defend against these attacks.



The security conundrum

Shared security responsibilities create a lot of confusion amongst CSPs and their clients, leading to gaps in terms of access control, data security, and so on. Though most service providers define the boundaries quite definitively, there are still blind spots that get exploited by attackers.

When organizations adopt a multi-cloud environment, they often fail to realize the shared responsibility model of each vendor and end up with a high security risk cloud environment.

Further, since multiple tenants are involved, it becomes a challenge to identify the origin of a cyberattack. Formulating a common incident response strategy for every client won't work, since the nature of data processed has to be considered, meaning strategies have to be custom-made for every client.

Further, the usage of shadow and banned applications makes it difficult for security administrators and service providers to keep up with attacks coming from every direction. Also, major issues such as cloud misconfigurations, data abuse, and session hijacking make it difficult to secure cloud installations.

This is why a comprehensive solution to monitor your environment and provide real-time insights on cloud activities is essential, which is where cloud access security brokers (CASBs) come into play.

What is a **CASB?**

In 2012, Gartner introduced CASBs to the world, defining it as an on-premises or cloud-based security policy enforcement point that sits between cloud service consumers and CSPs to monitor access to cloud-based resources.

Since its inception, CASB has evolved drastically to be a more exhaustive solution to all cloud security issues. The massive adoption of the cloud and continuous reports of security issues forced service providers to invest more in cloud security and CASBs became the go-to solution.

CASBs have evolved to be cloud user identity and activity mapping solutions that address issues with visibility.

With a comprehensive **CASB,** you get the following capabilities:

1

Cloud application analytics:

Unlike traditional cloud security, a CASB can monitor cloud applications and provide exhaustive reports on the different shadow and banned applications used in the organization.

2

Data monitoring and privacy:

A CASB can monitor data movement and ensure that only authorized personnel have access to sensitive information. This ensures data privacy and protects organizations from data leakage.

3

Threat detection and incident management:

CASBs are also capable of detecting internal and external threats. They sit between an organization and its cloud environment monitoring the traffic between them. The solution identifies malicious activities and helps defend against common threats like account hijacking, session takeover, etc.

4

Integrated compliance management:

A CASB helps comply with regulatory mandates such as HIPAA, the GDPR, and others by monitoring cloud platforms incessantly and providing real-time alerts and exhaustive reports on different network activities.

The need for a **CASB**

Exploding growth of SaaS

Experts have predicted that 85% of software used by organizations will be SaaS by 2025. Moreover, SaaS has started playing a prominent role in the majority of industries including finance, education, health, defense, and others in which sensitive information is handled.

85%

Software used by organizations will be SaaS by 2025.

Extended network perimeter

The adoption of cloud extends the network perimeter of organizations, which can leave blind spots in security. These blind spots can be exploited by attackers.

Multi-cloud adoption

Organizations have started adopting multi-cloud strategies. Different service providers follow different security guidelines. This makes cloud monitoring difficult.

How a **CASB works**

Compared to traditional cloud monitoring, a CASB makes it easier to monitor and secure cloud installation. The deployment process is straightforward and the solution is pretty easy to use. Still, there are certain factors to consider while adopting a CASB.

A CASB can be deployed either on-premises or in the cloud. However, SaaS tops the list of deployment methods.

Deployment models		
Model	**Description**	**Advantages**
API	Most SaaS applications use APIs to monitor applications. However, APIs often fail to provide policy logic or workflows that are useful for security teams or SOCs. CASBs leverage APIs and help monitor cloud activities from a single console. Further, a CASB also nullifies the differences in the APIs of different service providers by establishing native API functions. One major drawback of API is that it may not provide real-time protection.	**Ensure integrity of data at rest:** Ensure the integrity of data at rest by monitoring and classifying data based on its sensitivity and implementing relevant policies. **Easy to deploy:** This model can be deployed easily and doesn't modify the user experience of any applications. **Immediate value:** The benefit of deploying an API model can be enjoyed immediately since the implementation process is easy.
Forward proxy	In this model, the traffic goes through a CASB before accessing any cloud application or resource. Here, the CASB acts as a gateway to the network, ensuring complete security by establishing access control and blocking malicious traffic. Further, the CASB ensures data integrity using data loss prevention and deep packet inspection capabilities.	**Real-time security:** A forward proxy provides real-time insights on cloud activities. **Straightforward deployment:** The deployment process is straightforward; the solution monitors uploads and notifies the system administrator of policy violations. **Flexibility:** The forward proxy provides better flexibility compared to the API model.
Reverse proxy	In this model, the user is redirected to the CASB, which then validates the user's identity using SAML and provides the required access. A marked advantage of the reverse proxy model, particularly over that of the forward proxy, is that there is no need to have control over the endpoint to drive traffic through the proxy.	**Inline control:** Provides real-time, in-line security for cloud services, limiting access to applications or sensitive data based on the context of the device and user. **Agentless:** Provides agentless security to both corporate and personal devices based on their context. **Ubiquitous:** Monitors several cloud applications irrespective of their framework.

Embracing cloud security with a **CASB**

The adoption of a CASB makes cloud security comprehensive by giving an in-depth view of the different events that happen in an organization's cloud environment, making it easier for administrators to identify malicious activities.

Further, CASBs also helps organizations to:

1 **Establish application-specific security:**

Organizations often formulate a common security strategy for the different applications in their environment. However, a CASB is capable of leveraging the APIs of most cloud applications and monitoring activities, analyzing content, and adjusting settings within accounts on those applications.

2 **Create a concurrent gateway:**

A CASB sits in between an organization and its cloud environment and acts as a gateway that scrutinizes access to resources in the cloud. It also facilitates policy enforcement and ensures protection of information in transit.

3 **Control shadow IT:**

A CASB helps analyze shadow IT by monitoring cloud applications incessantly and identifying the usage of shadow and banned applications.

4 **Practice access control:**

With a CASB, access control can be established, thereby restricting unauthorized access to sensitive cloud resources.

Use cases for a **CASB**

Threat protection

- **Anomaly detection:** The CASB learns behavioral patterns of users and develops a baseline. If there are any deviations from this baseline, the solution alerts the administrator. For instance, an employee regularly logs in around 10 in the morning. One day they logged in at 11 in the evening and accessed certain critical resources. Though this could be a normal thing, the possibility of data leakage cannot be overlooked. This is why the CASB alerts the administrator about this incident and keeps record of all the activities the employee carries out. It also assigns a risk score based on which the administrator can take actions.

- **Shadow IT:** The CASB also provides security against shadow IT by monitoring access to malicious websites and banned applications. Further, it also monitors uploads and downloads, ensuring that there are no payloads coming into the network.

Data protection

- **Data loss prevention:** The CASB ensures the security of data both in transit and in storage. It also keeps tabs on data movement, making sure that no unauthorized user gets access to critical information. For instance, a user from the finance department tries to modify a particular file that belongs to the HR department. The CASB immediately reports this incident and alerts the administrator about the unauthorized access. The CASB also watermarks, encrypts, or password protects files based on their sensitivity to prevent data from getting exposed.

- **Security control:** The CASB is capable of helping organizations enforce security controls to prevent unauthorized data from being transferred over the internet. Further, it can block file uploads to malicious internet applications, thereby securing sensitive data.

Identity security

- **Policy enforcement:** The CASB lets organizations enforce policies to secure their network. Whenever the solution detects a policy violation, it alerts the administrator, providing insights based on the risk and the sensitivity of the violation.

- **User management:** The solution also provides insights on users and their activities, thus aiding in identifying malicious insiders.

Achieving critical **GRC with CASB**

CASBs help organizations achieve GRC (governance, risk management, and compliance) by providing exhaustive reports on different cloud activities. Let's now see how a CASB achieves GRC:

Governance

A CASB can help set policies and procedures to establish access control to websites and applications. This helps align IT operations in such a way that it supports achieving the overall business objective. Further, it also provides deeper visibility into different cloud application and website usage, making cloud management easier.

Risk management

A CASB helps ensure data security and provides protection from threats, thus aiding in risk management. It also alerts administrators whenever there are malicious interactions with an organization's network.

Compliance

Achieving compliance is one of the integral functions of a CASB. It helps organizations meet a wide range of compliance standards such as HIPAA, the GDPR, PCI DSS, etc.

Identifying the **perfect CASB solution**

1

Finding the right fit:

Identifying the perfect CASB is about finding the right fit. For this, organizations must be aware of their current cloud security posture and their security requirements. This can be done by conducting in-house research, getting a detailed report from an analyst, or monitoring similar organizations in the industry. Once the goals are clear, organizations can look for the solution that perfectly helps achieve their requirements.

2

Meeting changing security requirements:

Security requirements keep changing as the volume of business grows. A CASB should be able to withstand the changing requirements of organizations and must be able to defend from attacks originating in the extended threat landscape.

Lorem Ipsum

3

Underlying architecture:

A CASB comes predominantly in three different architectures, namely API approach, forward proxy, and reverse proxy. Forward proxies ensure users' privacy and security from the client side by intercepting requests to cloud services on the way to their destination. Reverse proxies, on the other hand, sit in front of a cloud service and provide in-line security. This is ideal for devices outside the purview of the network. The API approach works out of band and doesn't provide real-time security. It's essential to select the architecture that fits an organization's requirements.

4

Security of the IT infrastructure:

While finalizing a vendor, it is essential to know whether the solution can also monitor the entire IT infrastructure including IaaS adoptions. This is critical for bigger organizations who often prefer IaaS.

In a nutshell, CASBs have become a vital part of cloud security and it is essential for every organization to have a CASB in their security arsenal. However, it is also important that an organization evaluates their current security posture and ensures the CASB vendor can meet their security requirements before making the call on which vendor to go with.

About the author

Raghav Iyer is a cybersecurity expert on ManageEngine's product marketing team. He is a trusted advisor in network security management and regularly studies the tactics adopted by cybercriminals. He routinely writes IT security articles and guides on key security topics to help organizations solve their security challenges. Check out his blogs here.