Cloud Security – CASB Requirements

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.

CASB OVERVIEW

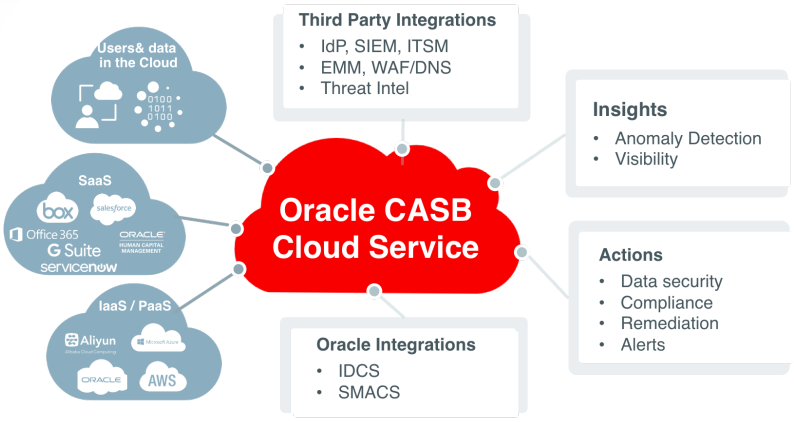

Figure 1: Typical CASB Solution

According to Gartner, "**Cloud Access Security Brokers (CASBs)** are on-premises, or cloud-based security policy enforcement points, placed between cloud service consumers and cloud service providers to combine and interject enterprise security policies as the cloud-based resources are accessed. CASBs consolidate multiple types of security policy enforcement."

With the rapid adoption of cloud services across the stack (Infrastructure, Platform and Software), the role of a CASB has become all the more important. While initial use cases of CASB were predominantly focused on obtaining visibility into what cloud resources were being used by users within an organization, more recent use cases have expanded beyond that into securing the state of the cloud services, monitoring user activities and locking down data in the cloud services.

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 servi es that will reduce the barrier to adoption, improve time to value and enhance the overall security posture.

User & Entity Behavior 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 defense-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

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 behavior 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.

CONCLUSION

While capabilities across the CASB market is evolving, the above factors should provide a broad overview of CASB functionality for most organizations. Given that most organizations are adopting a multi-cloud strategy, it is critical that a CASB provides comprehensive support to multiple cloud services across IaaS, PaaS and SaaS with fast time to value. Oracle CASB Cloud Service provides all the elements to help you make a secure transition to the cloud. It acts a first line of defense and provides security controls and policies to ensure that any cloud service has the appropriate configuration and control. It leverages the industry's best user and entity behavior analytics (UEBA) capabilities to deliver insights into cloud usage and take appropriate mitigating action. In summary, Oracle CASB Cloud Service is the most comprehensive CASB in the market that helps you rapidly improve your cloud security posture.

CONNECT WITH US

Call +1.800.ORACLE1 or visit oracle.com.
Outside North America, find your local office at oracle.com/contact.

blogs.oracle.com/oracle facebook.com/oracle twitter.com/oracle

Integrated Cloud Applications & Platform Services

Oracle is committed to developing practices and products that help protect the environment

ORACLE®