Mitigate the Top Nine Cloud Threats with a Cloud Access Security Broker (CASB)

How to encourage cloud usage while protecting applications and data.

Today's enterprises run 41 percent of their workloads in a public cloud, and 38 percent in a private cloud.[1] According to a survey by 451 Research, this number is expected to grow to 60 percent by 2018. And it's no wonder, with the cloud promising greater efficiency, flexibility, and cost savings.

For all their benefits, cloud services can also expose your organization to significant security risks, some of which IT professionals fail to recognize—or simply don't have the resources to deal with.

The Cloud Security Alliance published a report in 2016 highlighting "The Treacherous 12" threats to cloud computing security. Of the 12 cloud security challenges identified in the report, the good news is that you can address nine with a single CASB solution.

The Top Nine Cloud Threats: CASB Is Your Solution

1. Mitigate data breaches.

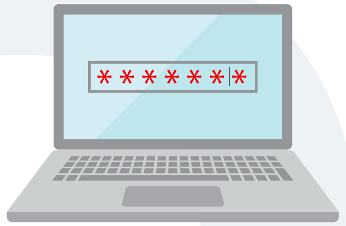
Top-tier cloud providers typically do a good job of securing their infrastructure. But the shared security model means customers are responsible for protecting their own data in the cloud.

The problem is that monitoring users, data, and encryption policies across a huge enterprise IT estate can be a challenge for even the largest of IT teams. Monitoring all of it manually is simply not possible in many cases.

With an automated security solution such as a CASB, the entire data center—and any clouds connected to it—can be monitored in real time. Everything from user behavior to the flow of data itself can be monitored simultaneously and reported to IT staff if any suspicious activity is detected.

More importantly, leading CASB solutions are equipped with the latest machine learning technologies to ensure they improve over time, and are better equipped to secure data in your organization's unique hybrid IT environments.

[1] Kim Weins, "Cloud Computing Trends: 2017 State of the Cloud Survey," *Cloud Management Blog*, RightScale, February 15, 2017, rightscale.com/blog/cloud-industry-insights/cloud-computing-trends-2017-state-cloud-survey.



2. Manage identities, credentials, and access.

Data breaches and attacks are more likely to occur when companies have insufficient identity- and access-management systems.

Many organizations permit the use of weak passwords for authentication, fail to use multifactor authentication, or lack automated rotation of cryptographic keys, passwords, and certificates.

You need to be able to monitor and manage identities, implement strong password policies, and eliminate noncompliant cryptographic keys—all things the right CASB solution can help with.

3. Secure APIs.

APIs are an essential part of leading cloud solutions, enabling the integrations that break down silos and enhance efficiency. But APIs also have IP addresses that can be accessed from outside trusted organizational boundaries. API tokens, such as client OAuth tokens, are also used to connect to cloud services. These tokens are increasingly compromised and used in cyberattacks.

Because they are exposed, these assets can be the target of attacks through the internet. You need adequate controls to monitor API usage and detect unusual activities originating from API calls in the cloud.

CASBs can also help here—but only those with the ability to score external APIs and applications based on activity, and address the cloud apps that don’t measure up. CASBs can be used to monitor all third-party clients connecting to cloud services to make sure they are approved clients.

Again, CASBs with machine learning capabilities are at an advantage here, because they have the ability to improve the accuracy of their API scoring over time.

4. Monitor system and application vulnerabilities.

With application estates expanding, attackers now have more bugs and vulnerable programs they can exploit to infiltrate data centers. Once they gain access, they can move on to steal data, take control of systems, or disrupt operations.

Closing these security gaps is a top priority for IT staff, but they must be able to identify where these gaps are before they can act.

An automated CASB solution can continuously monitor systems, scan for vulnerabilities, and send alerts about suspicious activity instantly—without any manual searching or effort.

A CASB can also automatically install security patches and upgrades, to ensure vulnerabilities are kept to the absolute minimum. The right CASB can even review application code to scan for weaknesses, closing security gaps before they can pose a risk.

5. Detect account-hijacking threats.

Attackers can steal credentials to gain access to critical parts of a cloud service, allowing them to compromise IT integrity, privacy, and availability. Intruders can use existing accounts to steal data, disrupt cloud services and systems, and damage your corporate reputation.

You need to rigorously monitor all users, accounts, and APIs, and be ready to alter your monitoring strategy as user behavior—and IT threats—change.

A leading CASB and the machine learning algorithms it provides can help automate this process and relieve the pressure of manual monitoring by IT.

For example, CASBs can alert you to unusual account behavior automatically, in real time. If a user logs in from a location they couldn't possibly be in, you'll get immediate insight into what has happened, and what you can do about it.

For more information, get the white paper "The Importance of User Behavior Analytics for Cloud Service Security."

ORACLE

6. Stop malicious insiders.

The 2016 Cyber Security Intelligence Index found that 60 percent of all IT attacks were carried out by insiders.

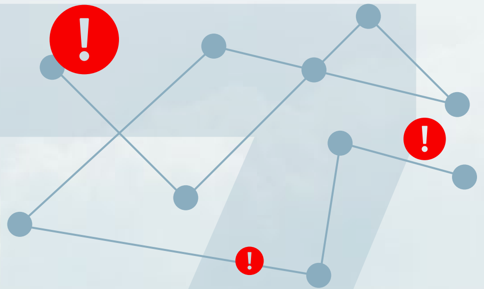
A malicious insider can wreak havoc on sensitive systems and data. But how can you pick out malicious user activities from the stream of genuine user traffic and behavior?

To properly monitor for insider activity, enterprise IT teams need to screen highly privileged user accounts, while monitoring user profiles, roles, and privileges.

But this kind of manual monitoring can be time-consuming, and stretch already scarce IT resources and skills to their limits.

Leading CASBs can automate much of this process, freeing up valuable IT resources. More importantly, a fully-featured CASB can build up a baseline of behavior for each user, and send alerts when they act outside their expected usage patterns. This can help you and your IT teams foil even the most complex account-hijacking efforts, without demanding more time and expertise from IT staff.

For more information, get the white paper "Hiding in Plain Sight: How a Cloud Access Security Broker with Built-In User Behavior Analytics Unmasks Insider Threats in the Cloud."



7. Detect advanced persistent threats.

An advanced persistent threat (APT) is a network attack where an unauthorized person gains access to a network and remains undetected for a long time. Using phishing emails or brute-force password-cracking, the APT attacker will get a foothold in the data center before deploying additional tools to help keep them in the system over the long term.

The purpose of an APT attack is to monitor and steal data, rather than to cause damage to the network or organization. Attackers will leave little or no trace of their presence to ensure they can continue their malicious activities.

While proactive security measures can stop APTs, it's ultimately up to you to educate your users on how to avoid the fraudulent practices, such as phishing emails, that attackers use to gain access to your systems.

CASBs can help your security team detect anomalies in inbound and outbound data. CASBs can also help proactively monitor for—and alert you to—potentially weak configurations and abnormal user behavior. The proactive monitoring and alerting can help you secure public clouds, avoiding potential phishing attacks in the future.

With visibility of all data going into and out of the organization, you can determine when your network has been targeted by an APT attack, and take timely action to mitigate its impact.

8. Thwart nefarious use of cloud services.

Free cloud trials and fraudulent cloud account signups can expose your network to attacks on infrastructure, platform, and application services.

All CSPs should allow customers to monitor the health of their cloud workloads. But if they don't, a CASB can detect abnormal launches and terminations of compute instances, as well as identify sudden changes to network and firewall configurations.

Similarly, cloud services can be co-opted by hackers to execute distributed denial of service (DDoS) attacks that stop users from accessing cloud services. Most cloud service providers (CSPs) are equipped to handle this kind of attack, but some CASBs can actually add to the problem, and disrupt cloud services on their own.

By choosing an API-based CASB, you can ensure it won't put additional strain on cloud services, helping reduce DDoS attack risk.

9. Minimize shared-technology issues.

CSPs deliver services at scale by sharing infrastructure, platforms, and applications. It's an efficient model, but one that potentially opens up your own cloud services to risk. A breach in one part of a shared infrastructure can quickly give hackers the platform they need to launch attacks on other cloud resources.

Advanced security tactics, such as multifactor authentication, on all hosts can help reduce the risks to shared cloud resources. A host-based intrusion detection system (HIDS) and network-based intrusion detection systems (NIDS) on internal networks can also help eliminate attacks across different levels of shared cloud resources.

A CASB can monitor and enforce security policies and processes like these on shared resources at the compute, storage, network, application, and user levels. The CASB can tie together other security processes, protocols, and tools to help you secure shared cloud systems more effectively.

CASB: The Answer to Your Cloud-Security Threats

CASBs address many of the Treacherous 12 cloud security threats through four fundamental capabilities:

Visibility: CASBs give administrators visibility into cloud usage throughout the organization. This includes discovery tools to detect unauthorized cloud services, as well as visibility into the activities of end users who access cloud services. A CASB can also provide insight into programmatic or cloud-to-cloud access activity.

Compliance: CASBs impose controls on cloud usage to enforce compliance with industry regulations such as HIPAA. They can also detect when cloud service usage and configurations are at risk of falling out of compliance.

Data security: CASBs enforce corporate security policies to restrict access to sensitive data and to make sure that data is encrypted appropriately—while still allowing application functions to work effectively. Most CASBs can also prevent unauthorized data downloads and redact sensitive data.

Threat protection: CASBs detect network threats, unusual activity, and malware attacks. In addition, they prevent unauthorized devices and users from accessing corporate cloud services.

For more help building the business case for CASBs, take a look at the white paper "Making the Case for a Cloud Access Security Broker."

Automating Cloud Security with a CASB

All enterprises must take personal responsibility for cloud security. But because of the unique, changeable, and agile nature of cloud services, manual security efforts simply aren't enough to protect cloud data and services over the long term.

For example, as part of the adoption of cloud services, IT administrators typically define key configuration settings for each service. These settings are initially well defined, but configurations can drift away from their original settings as cloud usage patterns evolve.

Automation can help ensure your cloud security policies and processes keep up with the changing world of cloud services. CASBs bring this new level of automation to cloud security.

These software tools reside between your on-premises infrastructure and your cloud infrastructure, acting as a gatekeeper that extends your security policies beyond the data center and into the cloud. CASBs can automate visibility, compliance, data security, and threat protection for software-, platform-, and infrastructure-as-a-service (SaaS, PaaS, and IaaS) deployments.

ORACLE

Choosing the Right CASB

The best CASBs use industry standards such as next-generation firewall (NGFW) and secure web gateway (SWG) protocols to integrate with your existing security solutions—so you don't have to create a new security silo.

Leading CASBs also enforce data loss prevention (DLP) strategies to ensure end users don't send critical information outside the corporate network.

Finally, security information and event management (SIEM) integration enables CASBs to manage incidents and alerts from an existing SIEM system.

The patented CASB, **Oracle CASB Cloud Service**, offers these features, and more. With Oracle CASB Cloud Service, IT and security teams can get:

- Advanced threat analytics from user-behavior analytics and third-party feeds
- Configuration seeding, monitoring, and alerts
- Shadow IT discovery, including custom applications
- Integration with existing security solutions, including SWG, SIEM, NGFW, DLP, and IDaaS

Oracle CASB Cloud Service can help organizations of any size, in any industry:

- **Secure the entire cloud stack** including IaaS, PaaS, and SaaS
- **Identify high-risk users** and the use of compromised credentials
- **Autorespond** to incidents
- **Identify anomalous behavior** with superior UBA
- **Eliminate configuration drift** with custom alerts and remediation action
- **Maximize existing security investments** through partnership and integration

To learn more about how Oracle CASB Cloud Service can help you safely enhance your use of cloud services while increasing visibility and control, visit Oracle CASB Cloud Service.

ORACLE®