Automate Your Cloud Security
A shared responsibility.

Although cloud providers include security for their infrastructure, you’re responsible for securing access to your data and applications in the cloud.

A Cloud Access Security Broker (CASB) provides four key functions:

- **Visibility** into who is accessing what applications
- **Compliance** with applicable regulations and policies
- **Data security** that manages who is sharing what data
- **Threat protection** to identify and respond to high-risk activities

“Oracle CASB Cloud Service gives customers consistent and complete governance and policies across a multicloud environment, provides them with visibility and control, and helps them understand what their users are doing at any given point in time.”

– Rohit Gupta, GVP, Product Management
See and respond to security threats.

Your applications are running in the cloud. How do you know they’re secure? Do you have visibility into the real and potential threats to your multivendor cloud footprint?

With Oracle CASB Cloud Service, you gain the visibility you need for the security of your cloud applications. And you can respond to threats quickly and effectively.

Oracle CASB Cloud Service:

- Leverages real-time threat intelligence from your cloud providers and applies machine learning techniques to establish baseline behavior patterns.

- Logs anomalous or suspicious activities, displays them in a dashboard, and responds using forensics, incident management, orchestration, and remediation.
See what’s going on.

While monitoring your cloud applications, you see all activity based on user, network, or device. Oracle CASB Cloud Service provides a view into different types of risks associated with users of your cloud applications, such as

- **User behavior** based on deviations from normal usage history.
- **Suspicious activity** such as a user hopping between geographic locations.
- **Noncompliant security control** such as a password policy that isn’t strong.
- **Policy alerts** based on defined rules about who accesses what resources, how they access them, and from where.
Identify risks. Report compliance.

Oracle CASB Cloud Service comes with predefined security controls. These controls ensure that your cloud applications are checked to a high degree of security. For example, it allows you to specify security control baseline settings for an application and then alerts you to any activity that does not comply with those settings.

To ensure and record compliance with policies and regulations, Oracle CASB Cloud Service provides reports about various types of activities for your cloud applications. You can generate reports such as the rotation status for keys used to access Amazon Web Services (AWS).
Simplified Monitoring

Start monitoring your cloud applications today.

Easy as 1-2-3, quickly begin monitoring your cloud application.

#1 Gather information securely.
Set up a dedicated service user in your cloud application to give Oracle CASB Cloud Service secure access to information, such as logs, needed for monitoring.

#2 Monitor your cloud platforms.
Use the flexibility of the Oracle CASB Cloud Service predefined templates not only to monitor your cloud platforms, but also to support different levels of monitoring (Monitoring Only, for all supported cloud services, or Push Security Controls, for AWS, Box, or Salesforce).

#3 Define security controls.
Define a level of control that’s more secure than the cloud platform defaults. With the simplified monitoring and enforcement of your security policy, you can secure your cloud and ensure that it stays secure.
Protect your sensitive cloud content.

Sensitive data requires more stringent controls. You configure the controls with policies that trigger alerts.

For example, you create a policy that alerts you when email is sent if it meets specified conditions, such as a suspicious IP address, domain destination, or an after-hours time stamp. Then, if an Office365 cloud application user sends Exchange email to a noncorporate recipient, a risk event is generated.

You can also define a policy that generates alerts based on risky administrator actions, such as changing the rules that are applied by the Exchange server before email is sent.

Oracle CASB Cloud Service provides transparency into actions taking place in your cloud applications.

Threat detection happens when activity for your cloud applications is outside the normal bounds, such as these suspicious activities:

- Excessive failed logins from an IP address
- Different user behavior than previous patterns
- Policy alert generated from a policy violation
Remediate threats and alerts in your cloud applications.

Oracle CASB Cloud Service automatically generates incidents in response to detected threats and policy alerts. You remediate incidents in one of the following ways:

- **Manual**: An administrator resolves the issue.
- **Automatic**: For supported incident types, Oracle CASB Cloud Service or another remediation system automatically resolves the issue in the cloud instance; for example, making a password policy stronger.
- **Delegation**: You export the incident to a centralized ticketing system, such as ServiceNow.
Apply **machine learning capabilities** to user behavior.

Oracle CASB Cloud Service uses machine learning capabilities to assign user activity risk scores. Current user activity is compared to the baseline activity to identify anomalous behavior. An incident is created and can include an option for the admin to automatically remediate, such as blocking an IP address and resetting a user’s password.

User behaviors that can cause a high-risk score include activities that are outside the normal behavior for a type of activity, such as the number of downloads, logins, or failed logins. Administrator activity is also scrutinized, because the potential threat is greater. A user who hops between geographical locations is also an indicator of a threat.
Discover unauthorized cloud applications.

Oracle CASB Cloud Service discovers shadow IT applications installed in your monitored cloud instances. (Shadow IT applications are ones that your IT infrastructure doesn’t support.) Applications are discovered either from the registered applications in the cloud instance or from logs.

The generated alert includes such information as the number of unique users, application reputation (if known), vendor name, address and description, vendor ranking, and potential security concerns.

Security concerns for shadow applications include the security of endpoints, network security, leaked information, DNS health, IP reputation, and Cubit Score™.

To manage the remediation cycle, you create incidents from shadow application alerts.
Learn More

- View data sheets, FAQs, pricing, and additional resources on the Oracle CASB Cloud Service product page.
- Sign up for a free trial at Oracle Cloud.
- Purchase a subscription and get started by visiting the Oracle Help Center.

Connect

Twitter: @Oracle Cloud
Facebook: Oracle Cloud
LinkedIn: Official Oracle Cloud Group
YouTube: Oracle Cloud Channel

Visit

Visit our Oracle Cloud community.

Oracle Events
Oracle Cloud Solutions Blog
Safe Harbor

The preceding is intended to outline our general product direction. It is intended for information purposes only, and may not be incorporated into any contract. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions. The development, release, and timing of any features or functionality described for Oracle’s products remains at the sole discretion of Oracle.