ORACLE CLOUD

ORACLE CASB FOR ORACLE HCM CLOUD

BACKGROUND:

Many businesses depend on business-critical applications such as Oracle HCM Cloud to elevate their business processes and engage better with their employees and contractors. These applications contain business-critical, sensitive and confidential information and security is paramount.

From a business perspective, as the move to HCM Cloud progresses, it is important to actively monitor all activities across all the services to ensure a traceable set of changes across, roles, configurations and business objects. This will help the organization build a baseline of business processes and user privileges faster and help remediate any anomalies sooner. Achieving compliance becomes predictable and less expensive.

From a security perspective, Oracle HCM Cloud by itself is inherently secure, however, it is important to track any user's behavior across organization's cloud spectrum. Some of the things that security teams are interested in are:

- Changes made to the cloud application's security configuration
- User's privilege changes
- Data exfiltration attempts
- Malicious access
- Compromised credentials identification

As with any cloud service, security is a shared responsibility with the cloud service provider and the customer organization. Oracle ensures a secure and stable HCM Cloud solution by carrying out its share of responsibility. Some of the underlying security provided by HCM Cloud include:

- Securing the cloud infrastructure (network, compute and storage etc.)
- Secure the sensitive data by providing encryption at rest and in motion
- Fine-grained access to HCM Cloud features across modules

However, aspects such as configurations, customizations and changes to business objects or users and security of users are the organization's responsibilities.

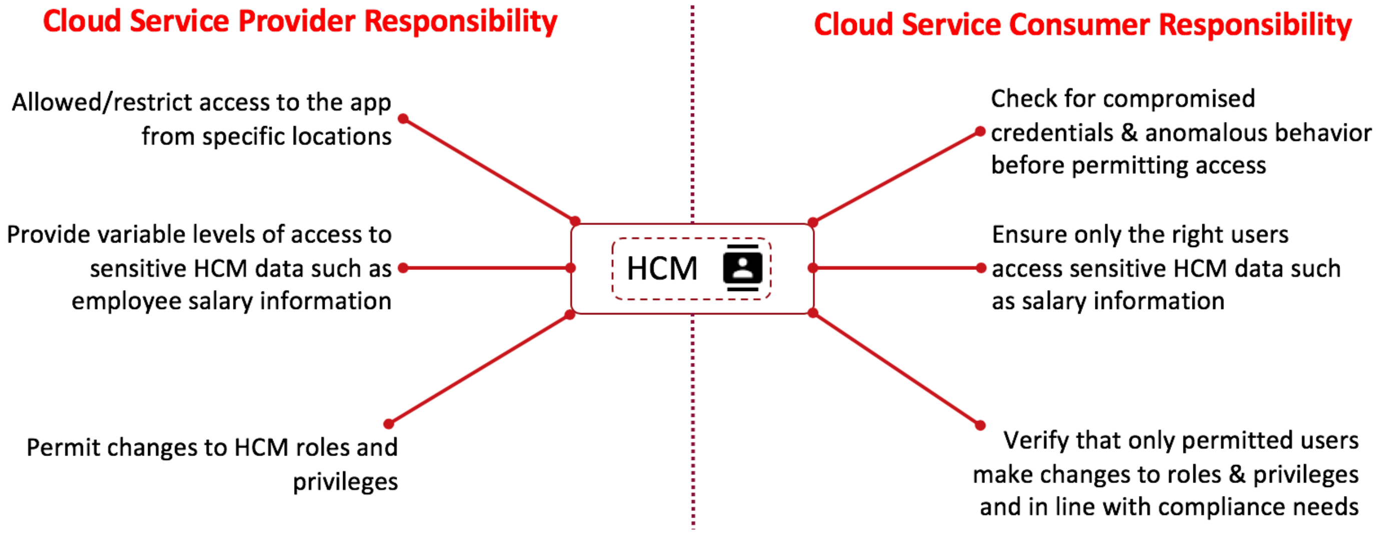
Cloud Service Provider Responsibility
Cloud Service Consumer Responsibility
Allowed/restrict access to the app from specific locations
Provide variable levels of access to sensitive HCM data such as employee salary information
Permit changes to HCM roles and privileges
HCM
Check for compromised credentials & anomalous behavior before permitting access
Ensure only the right users access sensitive HCM data such as salary information
Verify that only permitted users make changes to roles & privileges and in line with compliance needs

Figure 1: Shared Responsibility Model for HCM Cloud

Oracle CASB empowers an organization to carry out their share of security responsibilities. This paper covers the business value of Oracle CASB in enhancing the inherent security posture of Oracle HCM Cloud.

BUSINESS VALUE:

- **Gain visibility into Oracle HCM Cloud usage:** Gain in-depth understanding of users and for the purpose of use. Helps ensure sufficient usage of the service.
- **Achieve continuous compliance**: Ensure that configuration, role and privilege changes do not result in audit failures and non-compliance
- **Detect frauds sooner:** Get notified on changes to business objects that indicate potential fraud
- **Identify risky users:** Leverage network effects of risk across your cloud properties with user behavior analytics

WHY ORACLE CASB FOR ENHANCING ORACLE HCM CLOUD SECURITY

- **Visibility into who is accessing Oracle HCM Cloud**: Oracle CASB integrates closely to provide detailed information on who is using the application and attributes of access such as time and location.
- **Proactive monitoring:** Oracle CASB provides proactive monitoring of administrative user activities and sensitive data changes such as Person, Salary and other related Personally Identifiable Information (PII) modifications.
- **Identify high risk users:** Oracle CASB Cloud computes the risk score for a particular user leveraging machine learning and User Behavior Analytics and identifies high risk users based on their activities and contextual data such as geolocation.
- **Gain detailed proactive insights to business object changes:** Oracle CASB inspects business object level attributes and provides a single point of insight into the changes to these business objects.
- **Track changes to roles and privileges:** Oracle CASB monitors all key role changes. These include changes to privileges and membership for any role change.
- **Single point of visibility across all cloud solutions:** If an organization is using multiple cloud apps, Oracle CASB acts a single pane of glass to monitor all these applications including Oracle HCM Cloud, ERP Cloud and non-Oracle applications such as Office 365, Salesforce etc.

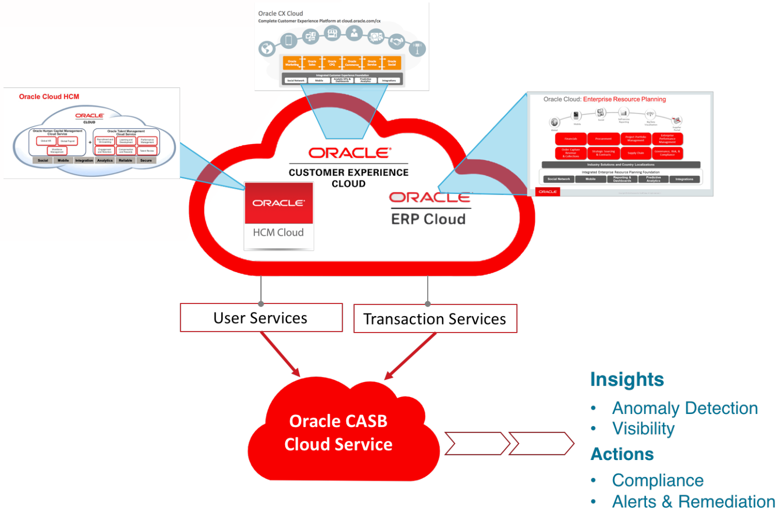

Figure 2: Oracle CASB complementing Oracle Cloud Applications

SAMPLE USE CASES

USE CASE 1 – USER ACCESS MONITORING (VISIBILITY & SECURITY):

CASB identifies who is accessing Oracle HCM Cloud at any given time: Information on all Oracle HCM Cloud users for a particular organization can be tracked by Oracle CASB. You can get information such as the IP address, date/time of login, device type (mobile, desktop etc.), OS, browser type, successful/failed login/logout etc. from Oracle CASB. In addition, password-based attacks like brute force, login attempts from anonymous proxy like Tor etc. can be monitored. A detailed login success and failure report and key security indicators on users with most logins and most login failed attempts are available.

USE CASE 2 - IDENTIFYING ROLE CHANGES (SECURITY & COMPLIANCE):

CASB proactively monitors role, privilege and membership changes made in Oracle HCM Cloud. Oracle CASB monitors all role changes such as role creation, member addition/removal etc. within Oracle HCM Cloud, irrespective of where they originate – administrative or user-initiated and sends notifications through incidents and alerts. In the case of Oracle HCM Cloud specifically, customers can create roles by copying pre-seeded roles. Any changes to these copied roles may result in significant impact downstream. When monitored, these changes help in doing a rapid impact analysis. A comprehensive report for role changes and key security indicators such as users with most role changes is also available.

USE CASE 3 - IDENTIFYING CHANGES TO SENSITIVE BUSINESS OBJECTS (FRAUD DETECTION):

CASB monitors changes to sensitive business objects such as Person and Salary information in Oracle HCM Cloud. Oracle CASB monitors critical business objects in Oracle HCM Cloud such as Person, Salary and raises an alert when any changes occur. A detailed report and key security indicators are available for these object attribute changes.

USE CASE 4 – IDENTIFYING ANOMALOUS USER BEHAVIOUR (SECURITY):

CASB identifies anomalous activity using User and Entity Behavior Analytics (UEBA): Based on machine learning, Oracle CASB builds a profile for a user’s typical behavior, for example, a user may typically log in from San Francisco. However, a login attempt made from New York represents a deviation from the user’s normal behavior and is a potential risk resulting in an alert to the security team. Similarly, Oracle CASB recognizes any deviation in the typical volume of transactions and alerts the security team.

CONCLUSION

The inherent security of Oracle HCM Cloud provides a layer of comfort for organizations. However, given the multi-cloud environments that most organizations operate in, it is imperative that information security teams monitor multiple dimensions of Oracle HCM Cloud in conjunction with other cloud assets. Oracle CASB provides that indispensable layer of visibility and additional security that critical business applications such as Oracle HCM Cloud require.