Oracle CASB for Oracle Cloud Infrastructure

As customer adopt cloud-based infrastructure as part of their digital journey, protecting this infrastructure becomes a critical security imperative to ensure that applications that are built on top of them and the data stored are inherently secure. Oracle's Cloud Access Security Broker (CASB) Cloud Service is a heterogeneous cloud security solution that helps protect cloud-based infrastructure, platforms and applications across vendors. Specifically, for customers adopting Oracle Cloud Infrastructure (OCI), Oracle CASB provides visibility, threat protection, data security and compliance for their OCI deployments.

Oracle CASB for OCI – Key Features

- Provide visibility across OCI services such as Compute, Network, Storage & IAM
- Protect data stored in OCI
- Ensure consistent security posture across services with Smart Policies
- Detect anomalies using behavior analytics and machine learning

Key Business Benefits.

- Continuous security compliance of critical resources in OCI
- Automated anomalous behavior detection with smart policies
- Governance of privileged activities
- Vulnerability detection by monitoring configuration drifts
- Proactive remediation and unified incident management

VISIBILITY, MONITORING & SECURITY INDICATORS

Oracle CASB helps you gain visibility into use of managed and unmanaged OCI instances such as Networking, Compute, Storage and Identity. Various actions performed by users across these

Disclaimer: This document is for informational purposes. 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 in this document remains at the sole discretion of Oracle.

instances are captured providing a strong audit trail of all activities across these resources. Some of the activities that can be monitored are:

- Creation, termination and deletion of compute, network and storage instances
- Creation, addition, modification and deletion of users and groups
- Modification of permissions for any instances
- Most active users and groups

Visibility can be filtered by various attributes such as user, resource or action. Going beyond visibility, Oracle CASB also provides details on the actual activity and possible remediation steps. This enables fast resolution of potential issues and provides the necessary details for forensics.

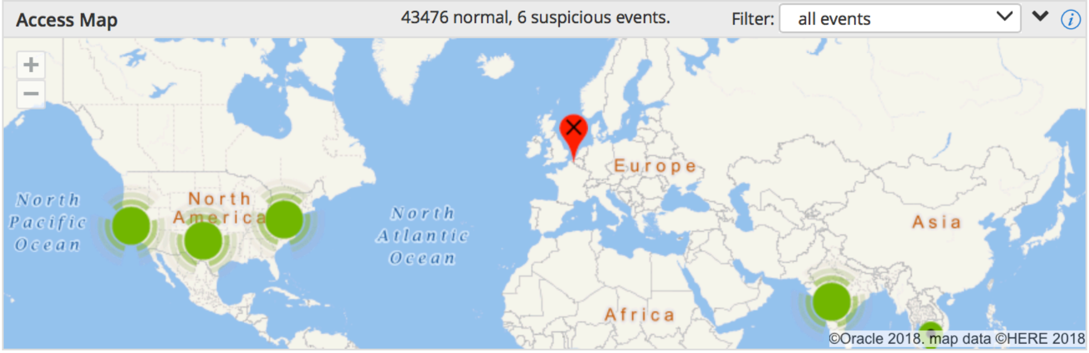


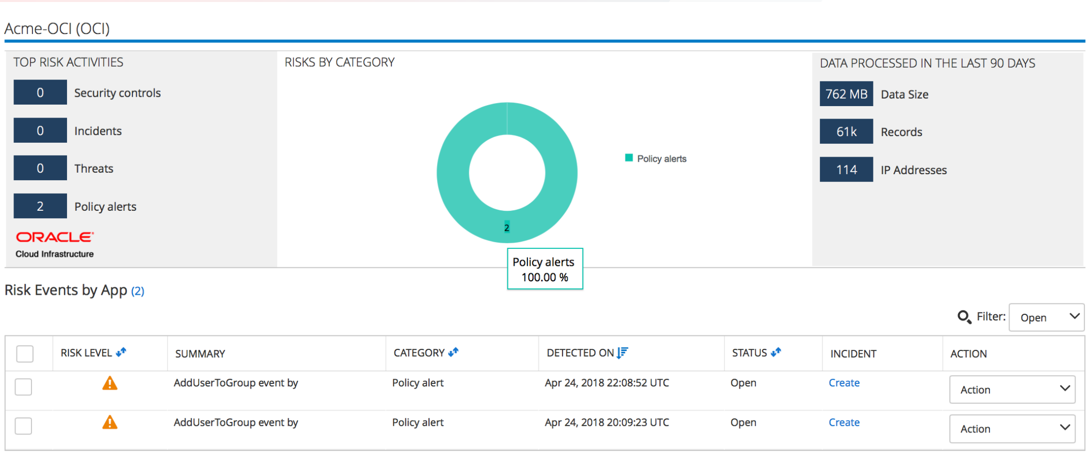
Figure 1: Access map using Oracle CASB

SECURITY CONFIGURATION

Cloud Infrastructure follow the shared responsibility model. While the model provides delineation of responsibilities “of the cloud” and “in the cloud”, optimal security can be achieved with the right configuration of the infrastructure components. Oracle CASB helps detect misconfiguration of various OCI components such as:

- Compute Images and Compute Instances
- Networking and Load Balancers
- Identity Users and Groups
- Database Systems and Object Storage

Further, with Smart Policies, customers benefit from the abundance of security expertise built by experts. These policies are automatically turned off for each customer to ensure predictable and consistent security across all OCI resources.



Acme-OCI (OCI)

TOP RISK ACTIVITIES

0	Security controls
0	Incidents
0	Threats
2	Policy alerts

ORACLE Cloud Infrastructure

RISKS BY CATEGORY

DATA PROCESSED IN THE LAST 90 DAYS

762 MB	Data Size
61k	Records
114	IP Addresses

Risk Events by App (2)

Filter: Open

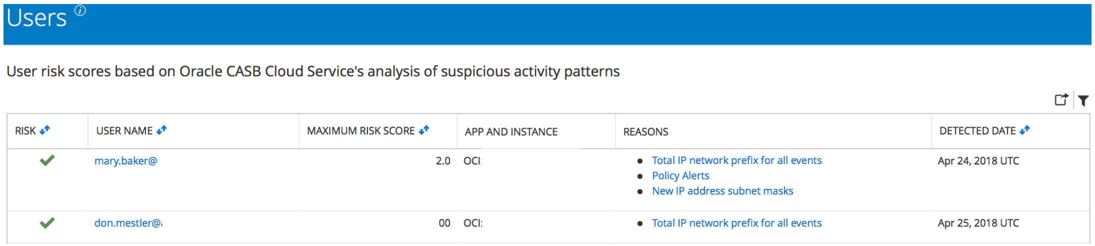
□	RISK LEVEL	SUMMARY	CATEGORY	DETECTED ON	STATUS	INCIDENT	ACTION
□	⚠	AddUserToGroup event by	Policy alert	Apr 24, 2018 22:08:52 UTC	Open	Create	Action
□	⚠	AddUserToGroup event by	Policy alert	Apr 24, 2018 20:09:23 UTC	Open	Create	Action

Figure 2: Risk Events for Oracle OCI

BEHAVIOR ANALYTICS & THREAT PROTECTION

Oracle CASB leverages advanced analytics and machine learning techniques to detect potential security issues. This includes User and Entity Behavior Analytics (UEBA) to determine anomalies and to determine risks to OCI. Oracle CASB automatically creates a baseline of each user and resources' behavior and any deviations from the baseline result in security alerts that can result in action. Some examples are:

- Detect anomalous behavior of users that may result in insider threat
- Compromised accounts that may result in malicious resource usage



Users

User risk scores based on Oracle CASB Cloud Service's analysis of suspicious activity patterns

RISK	USER NAME	MAXIMUM RISK SCORE	APP AND INSTANCE	REASONS	DETECTED DATE
✓	mary.baker@	2.0	OCI	• Total IP network prefix for all events • Policy Alerts • New IP address subnet masks	Apr 24, 2018 UTC
✓	don.mestler@	00	OCI:	• Total IP network prefix for all events	Apr 25, 2018 UTC

Figure 3. User risk for OCI computed using UEBA

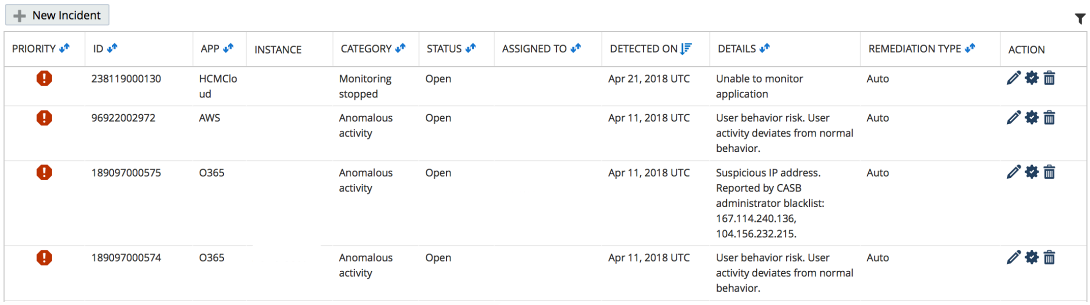
SMART POLICIES

Oracle has leveraged years of expertise in security and combined that with intimate knowledge of Oracle Cloud Infrastructure (OCI) and has published various security policies that are made available to each customer by default. These policies are designed to help customers improve their security posture and provide a consistent security framework. These policies are available in two tiers:

- Tier 1 – Smart Policies that are turned on by default for all customers. For example, policies that ensure that there are no publicly accessible storage buckets
- Tier 2 – Smart Policies that are not turned on by default but are pre-configured. Customers can turn them on based on their individual needs

INCIDENT MANAGEMENT

Oracle CASB provides a robust built in incident management functionality. This ensures that any alert that is generated by CASB is tracked and appropriate action taken. Additional integrations with incident management solutions such as ServiceNow are is also provided.



PRIORITY	ID	APP	INSTANCE	CATEGORY	STATUS	ASSIGNED TO	DETECTED ON	DETAILS	REMEDIATION TYPE	ACTION
❗	238119000130	HCMCloud		Monitoring stopped	Open		Apr 21, 2018 UTC	Unable to monitor application	Auto	✎ ⚙ 🗑
❗	96922002972	AWS		Anomalous activity	Open		Apr 11, 2018 UTC	User behavior risk. User activity deviates from normal behavior.	Auto	✎ ⚙ 🗑
❗	189097000575	O365		Anomalous activity	Open		Apr 11, 2018 UTC	Suspicious IP address. Reported by CASB administrator blacklist: 167.114.240.136, 104.156.232.215.	Auto	✎ ⚙ 🗑
❗	189097000574	O365		Anomalous activity	Open		Apr 11, 2018 UTC	User behavior risk. User activity deviates from normal behavior.	Auto	✎ ⚙ 🗑

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

Copyright © 2018, Oracle and/or its affiliates. All rights reserved. This document is provided for information purposes only, and the contents hereof are subject to change without notice. This document is not warranted to be error-free, nor subject to any other warranties or conditions, whether expressed orally or implied in law, including implied warranties and conditions of merchantability or fitness for a particular purpose. We specifically disclaim any liability with respect to this document, and no contractual obligations are formed either directly or indirectly by this document. This document may not be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without our prior written permission.

This device has not been authorized as required by the rules of the Federal Communications Commission. This device is not, and may not be, offered for sale or lease, or sold or leased, until authorization is obtained.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Xeon are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Opteron, the AMD logo, and the AMD Opteron logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group. 0618

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