Oracle CASB Cloud Service protects your entire cloud footprint with automated security monitoring. A pioneering, Multimode cloud access security broker (CASB) that simplifies configuration settings and prevents configuration drift, detects anomalous behavior with user behavior analytics, and secures against threats that span multiple cloud services.

**Modern Security Concerns**

As enterprises continue to adopt new cloud services, they require more sophisticated capabilities to secure their entire cloud footprint. CASBs have emerged as the go-to solution for cloud security, but a modern CASB must go beyond simple shadow IT discovery to secure your sanctioned services. You need a solution that protects your entire cloud footprint—including infrastructure as a service (IaaS), software as a service (SaaS), and platform as a service (PaaS)—provides optimal performance with no user impact, and integrates with your existing security investments through a simple deployment. Oracle CASB Cloud Service meets modern, cloud security requirements to protect your business.

**Complete Visibility of Your Cloud Environment**

Oracle CASB Cloud Service protects your employee-facing SaaS applications as well as the foundations of your cloud infrastructure, including IaaS and PaaS services. It delivers a holistic view of the entire cloud environment, including all users and devices. Rather than manually investigating incidents separately in each application, your enterprise can quickly identify threats across multiple cloud services and take remedial action to address the source of the problem. Oracle CASB Cloud Service also gives you an advantage in shadow IT discovery. In addition to exposing unsanctioned SaaS applications downloaded by employees, Oracle CASB Cloud Service provides visibility into previously unknown applications downloaded from enterprise app stores and custom applications.
Oracle CASB Cloud Service protects an enterprise’s business critical cloud services by combining visibility, threat detection, compliance management, and automated incident response for cloud services into a single platform that can be deployed in minutes.

Threat Detection with User Behavior Analytics

User behavior analytics (UBA) in Oracle CASB Cloud Service go beyond noticing simple incongruences, such as logging in from different parts of the country in a short amount of time. Instead, Oracle CASB Cloud Service builds a baseline of typical behavior—down to the individual user and application—and logs when and how a user deviates from the baseline. Predictive analytics identify risky users, including behavior such as changing folder permissions, changing user privileges, or altering configuration settings. This allows you to stop an incident before it occurs. Because it pulls information from third-party threat feeds, you can rest assured that Oracle’s CASB solution is armed with the most up-to-date information on the threat landscape.

Compliance for the Cloud

Your enterprise has specific security configuration requirements. Oracle CASB Cloud Service offers configuration settings based on best practices and allows you to customize settings to fit your unique needs. Additionally, Oracle’s CASB solution can automatically seed the configuration settings in each cloud application.

Once specific values are established, Oracle CASB Cloud Service monitors your cloud service settings and alerts you to any changes. To prevent configuration drift, the solution can restore your settings back to the approved configuration, eliminating the hours of investigation spent preparing for compliance audits. Through this approach, Oracle CASB Cloud Service provides the flexibility you need to run your business while ensuring that the proper rules are in place to protect it.

Data Security Designed for the Cloud

Data security is of utmost importance to organizations adopting cloud services. Oracle CASB Cloud Service addresses the three key components of data security in the cloud:

- **Data visibility.** Oracle CASB Cloud Service monitors whether certain data has been accessed, moved, copied, renamed, edited, deleted, or locked.
- **Data accessibility.** Oracle’s CASB solution monitors collaboration settings so you know who has access to what information and whether they’ve used that access.
- **Data inspection.** Oracle CASB Cloud Service integrates with the data inspection tools available from cloud service providers to ensure data inspection is applied close to where the data resides.

Integrating with Existing Investments

Oracle’s CASB solution integrates with your existing solutions to extend their benefits to your cloud environment. You already have enterprise security tools such as secure web gateways (SWG), next-generation firewalls (NGF), identity as a service (IDaaS), data loss prevention (DLP), and security information and event management (SIEM). Oracle CASB Cloud Service builds upon those investments for maximum efficiency with minimal investment. Current integrations include PAN, Fortinet, Check Point, Sophos, Okta, and Ping Identity.
CONTACT US
For more information about Oracle CASB Cloud Service, visit oracle.com or call +1.800.ORACLE1 to speak to an Oracle representative.

Integrated Cloud Applications & Platform Services

Copyright © 2017, 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.

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.