

An Oracle White Paper
March 2009

Oracle Audit Vault

Enterprise Security Challenges	3
Oracle Audit Vault	4
Compliance & Security Reports	5
Security and Monitoring Alerts	6
Audit Policies.....	7
Security and Scalability	8
Summary	8

Enterprise Security Challenges

Satisfying compliance regulations and reducing the risk of security breaches are among the top security challenges businesses face today. Examination of numerous security incidents has shown that timely examination of audit data could have helped detect unauthorized activity early and reduced the resulting financial impact. Various studies and surveys conducted by government and academic institutions have concluded that a sizeable percentage of data breaches have been perpetrated by insiders, that is, by those authorized at least some level of access to the system and its data. As a result governments worldwide have enacted a wide range of regulations relating to financial controls, health care, and privacy.

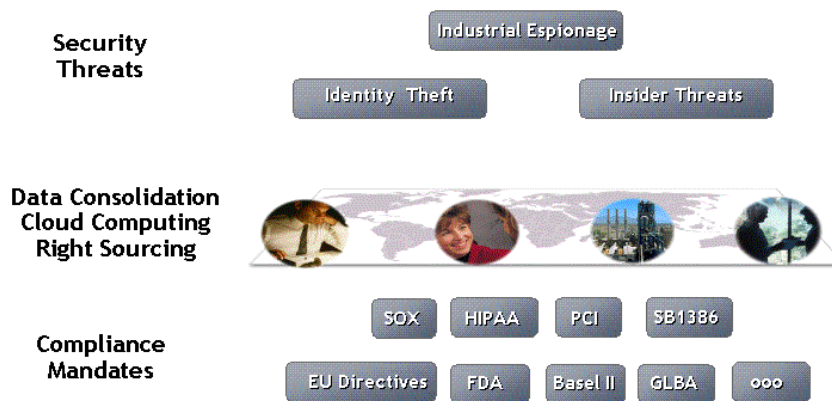


Figure 1.0 – Security Business Drivers

Well known regulations such as Sarbanes-Oxley (SOX), the Health Insurance Portability and Accountability Act (HIPAA) combined with industry driven initiatives such as the Payment Card Industry Data Security Standard (PCI-DSS) have resulted in information protection becoming a top-level issue for the enterprise. As security threats become more sophisticated, monitoring is becoming an increasingly important component of the defense-in-depth architecture. Today, the use of audit data as a security resource remains very much a manual process, requiring administrators and audit personnel to manually collect audit data from multiple locations.

Oracle Audit Vault

Oracle Audit Vault automates the consolidation of audit data into a secure repository, enabling efficient monitoring and reporting. Oracle Audit Vault is a powerful solution providing a secure repository, built-in reporting, event alerting, and separation-of-duty. Built on Oracle's industry leading technology, Oracle Audit Vault uses Oracle data security to protect audit data end-to-end. The latest release of Oracle Audit Vault provides enhanced out-of-the-box compliance reporting and audit collection, including support for Microsoft SQL Server 2000 & 2005, IBM DB2 Unix, Linux, and Windows 8.2 & 9.5, and Sybase ASE 12.5 & 15.0 databases.

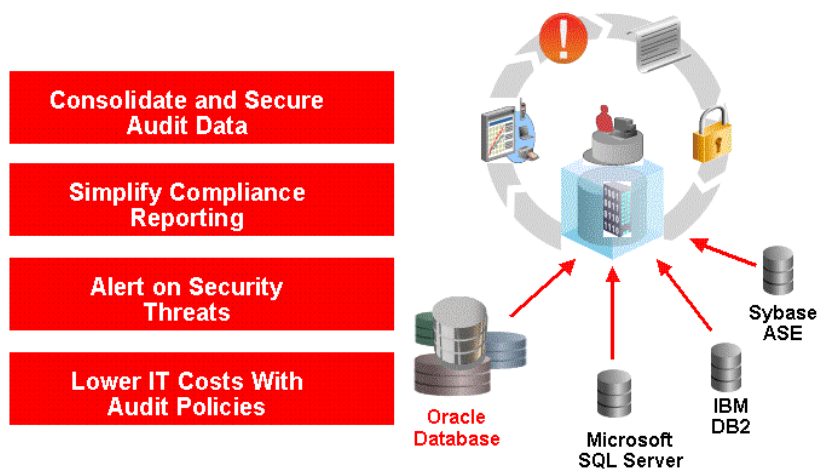


Figure 2.0 – Oracle Audit Vault Overview

Central to Oracle Audit Vault is a secure data repository built on Oracle's industry leading data warehousing technology and secured with Oracle's industry leading security products. Built-in reporting and event alerting help businesses improve their ability to comply with external regulations and internal policies by lessening the time and effort required to detect potential problems and demonstrate that mandated controls are in effect and working. Data security administrators and auditors can manage, compare and provision Oracle database auditing settings across the enterprise directly from the Oracle Audit Vault console, lowering overall maintenance costs.

Compliance & Security Reports

Oracle Audit Vault provides powerful built-in reports to monitor a wide range of activity including privileged user activity and changes to database structures. The reports provide visibility into activities and provide detailed information on *who*, *what*, *when* and *where*. The latest release of Oracle Audit Vault provides an exciting new reports interface built on the widely popular Oracle Application Express technology. The new reports provide an easy-to-use interface with the ability to create colorful charts and graphs as well as the ability to customize the report format. Report columns can be re-ordered as well as removed. Rules can be put in place to automatically highlight specific rows so that report users can quickly spot suspicious or unauthorized activity. Reports will include audit information from Oracle, Microsoft SQL Server, IBM DB2 Unix, Linux, & Windows, and Sybase ASE databases, providing a holistic picture of activity across the enterprise. Oracle Audit Vault provides numerous standard audit assessment reports categorized into areas such as compliance and alerts. Out-of-the-box reports



Figure 3.0 – Oracle Audit Vault Report's Interface

include information on database account management, roles and privileges, object management, and login failures. Oracle Business Intelligence, Oracle BI Publisher and other 3rd party reporting tools can be used to build additional reports to meet specific compliance and security requirements. Detailed information on the repository tables can be found in the Oracle Audit Vault Auditor's guide.

Security and Monitoring Alerts

Oracle Audit Vault provides security personnel with the ability to detect and alert on activities that may indicate attempts to gain unauthorized access and/or abuse system privileges. Oracle Audit Vault can generate alerts for system defined and user defined audit events. Oracle Audit Vault continuously monitors the audit data collected, evaluating the activities against defined alert conditions. Alerts can be associated with any auditable database event including system events such as changes to application tables and creating privileged users.



Figure 4.0 – Oracle Audit Vault Alert's Dashboard

For instance, an alert could be generated when someone attempts to access sensitive business information. The Oracle Audit Vault interface provides graphical summaries of activities causing alerts. These include a summary of alert activity and top sources by number of alerts. Oracle Audit Vault users can click on the summary graphs and drill down to a more detailed report. Alerts for the purpose of reporting are grouped by the sources with which they are associated. Alerts can also be grouped by the event category to which the event belongs, and by the severity level of the alert (warning or critical).

Audit Policies

Oracle Audit Vault provides centralized management of Oracle database audit settings, simplifying the job of the IT security and internal auditors. Many businesses are required to actively monitor systems for specific audit events or audit policies. In most environments the definition and management of these audit settings is a manual process. IT security personnel must work with internal auditors to define audit settings on databases. In addition, internal auditors periodically need to work with IT security personnel to ensure the audit settings have not been changed. The collection of audit settings in use on a given database is sometimes referred to as an *audit policy*.

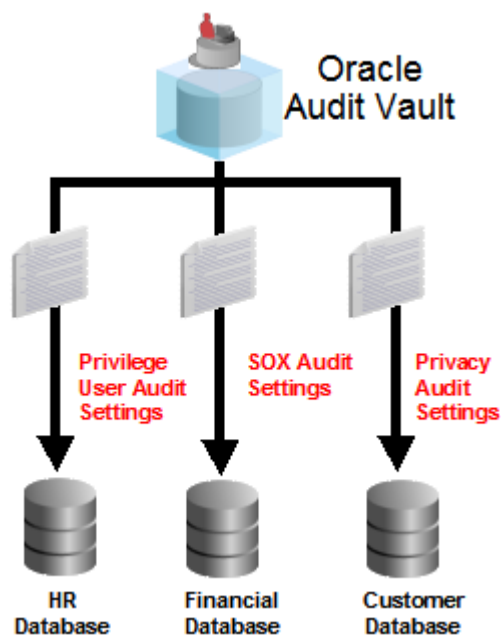


Figure 5.0 – Oracle Audit Vault Policies

Oracle Audit Vault provides the ability to centrally define audit policies from the Audit Vault console. This provides both internal auditors and IT security a much easier way of managing audit settings across the enterprise and demonstrate compliance and repeatable controls to external auditors.

Security and Scalability

Audit data is an important record of business activity. Audit data must be protected against modification to ensure the integrity of reports and investigations based on the audit data. Oracle Audit Vault stores audit data in a secure repository built using Oracle's industry leading database security technology. Timely transfer of audit data from source systems to Oracle Audit Vault is critical to close the window on intruders who may attempt to modify audit data and cover their tracks. Oracle Audit Vault can be configured to transfer audit data on a near real time basis. Oracle Audit Vault protects audit data during transfer over the network and within Oracle Audit Vault. During transfer from the source systems, audit data can be encrypted, preventing anyone from reading or tampering with the data during transmission.

Inside Oracle Audit Vault access to audit data is strictly controlled based on the principle of separation-of-duty. Oracle Real Application Clusters (RAC) can optionally be licensed for Oracle Audit Vault, enabling additional scalability and high availability.

Summary

Audit data is playing an increasingly important role in helping organizations maintain high security and enforce compliance with internal and external policies. Investigations of numerous security incidents have shown that monitoring activity and access to sensitive data could have greatly reduced the financial impact of many security breaches. Oracle Audit Vault helps organizations increase security by automating the consolidation of audit data into a secure and scalable repository. Numerous out-of-the-box reports organized into functional areas such as compliance provide security and compliance personnel with easy access to audit data from Oracle, Microsoft SQL Server, IBM DB2, and Sybase ASE databases. Built-in alerting provides security and compliance personnel with the ability to quickly detect and investigate potential issues. Centralized policies simplify the management of database audit settings across the enterprise and help demonstrate proof of compliance. Oracle Audit Vault provides detailed documentation that can be used to create custom reports using Oracle BI Publisher or other 3rd party reporting tools. Future Oracle Audit Vault releases will include support for additional databases and sources.



Oracle Audit Vault
March 2009
Author: Tammy Bednar, Paul Needham
Contributing Authors:

Oracle Corporation
World Headquarters
500 Oracle Parkway
Redwood Shores, CA 94065
U.S.A.

Worldwide Inquiries:
Phone: +1.650.506.7000
Fax: +1.650.506.7200
oracle.com



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

Copyright © 2009, 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 is a registered trademark of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.