ORACLE AUDIT VAULT AND DATABASE FIREWALL

SCALABLE DATABASE ACTIVITY MONITORING AND AUDITING

KEY FEATURES

- Activity monitoring and blocking on the network combined with consolidation of audit data for Oracle, MySQL, Microsoft SQL Server, SAP Sybase, IBM DB2, and Oracle Big Data Appliance
- White list, black list, and exception list based enforcement on the network
- Extensible audit collection framework with templates for XML and table-based audit data
- Dozens of built-in customizable compliance reports combined with proactive alerting and notification
- Interactive, PDF, and Excel reports
- Fine grained source-based authorizations for auditors and administrators
- Highly scalable architecture to support large number of databases with high traffic volume
- Pre-configured Software appliance for convenience and reliability
- High availability support
- External storage support for audit data repository and audit archives

KEY BENEFITS

- First line of defense that transparently blocks unauthorized traffic, provides a complete view of database activity, and consolidates audit data
- Achieve compliance quickly with packaged and customizable reports
- Meet both security and compliance requirements with a single deployment
- Lower cost of ownership with highly accurate SQL analysis, out-of-the-box reports, and proactive alerts

Oracle Audit Vault and Database Firewall provides a first line of defense for databases and consolidates audit data from databases, operating systems, and directories. A highly accurate SQL grammar-based engine monitors and blocks unauthorized SQL traffic before it reaches the database. Database activity data from the network is combined with detailed audit data for easy compliance reporting and alerting. With Oracle Audit Vault and Database Firewall, auditing and monitoring controls can be easily tailored to meet enterprise security requirements.

Detective and Preventive Controls

Perimeter firewalls play an important role in protecting data centers from unauthorized, external access, but database attacks have grown increasingly sophisticated. They bypass perimeter security, take advantage of trusted middle tiers, and even masquerade as privileged insiders. As a result, database activity monitoring and enforcing security controls in and around the database have become critical. Effective monitoring and auditing can alert and block attempted policy violations, as well as provide comprehensive reports for compliance.

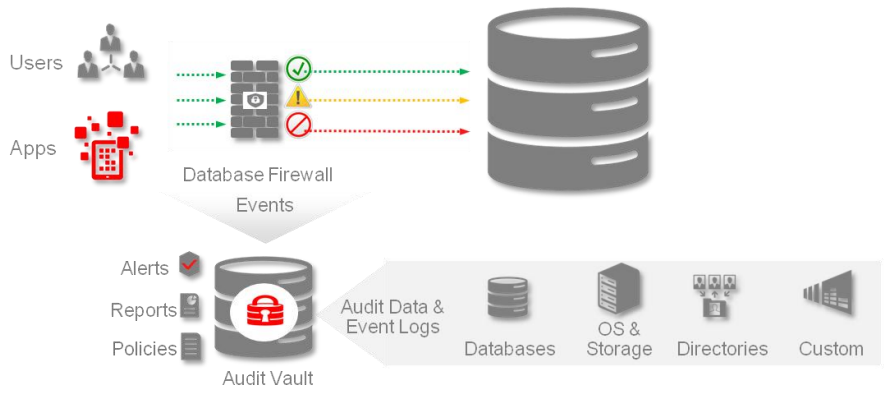

Figure 1. Oracle Audit Vault and Database Firewall

Oracle Audit Vault and Database Firewall consolidates database activity monitoring events and audit logs. Policies enforce expected application behavior, helping prevent SQL injection, application bypass, and other malicious activities from reaching the database while also monitoring and auditing privileged users, and other activities, inside the database. Oracle Audit Vault and Database Firewall can also consolidate audit data from Microsoft Active Directory, Microsoft Windows, Oracle Solaris, Oracle Linux, and Oracle ASM Cluster File System. A plug-in architecture consolidates custom audit data from application tables and other sources.

Database Firewall for Activity Monitoring and Blocking

Oracle Database Firewall provides a sophisticated next-generation SQL grammar analysis engine that inspects SQL statements going to the database and determines with high accuracy whether to

allow, log, alert, substitute, or block the SQL. Oracle Database Firewall supports white list, black list, and exception list based polices. A white list is simply the set of approved SQL statements that the database firewall expects to see. These can be learned over time or developed in a test environment. A black list includes SQL statements from specific users, IP addresses, or specific types that are not permitted for the database. Exception list-based policies provide additional deployment flexibility to override the white list or black list policies. Policies can be enforced based upon attributes, including SQL category, time of day, application, user, and IP address. This flexibility, combined with highly accurate SQL grammar analysis, enables organizations to minimize false alerts, and only collect data that is important. Database Firewall events are logged to the Audit Vault Server enabling reports to span information observed on the network alongside audit data.

Enterprise Audit Data Consolidation and Lifecycle Management

Native audit data provides a complete view of database activity along with full execution context irrespective of whether the statement was executed directly, through dynamic SQL, or through stored procedures. In addition to consolidating audit data from databases, operating systems, and directories, the Audit Collection Plugin can be used to collect audit data from application tables or XML files, and transfer them to the Audit Vault Server. Audit data from databases is automatically purged after it has been moved to the Audit Vault Server. Audit Vault Server supports data retention policies spanning days, weeks, or years on a per source basis, making it possible to meet internal or external compliance requirements**.**

Fine Grained, Customizable Reporting and Alerting

Dozens of out-of-the-box reports provide easy, customized reporting for regulations such as SOX, PCI DSS, and HIPAA. The reports aggregate both the network events and audit data from the monitored systems. Report data can be easily filtered, enabling quick analysis of specific systems or events. Security Managers can define threshold based alert conditions on activities that may indicate attempts to gain unauthorized access and/or abuse system privileges. Fine grained authorizations enable the Security Manager to restrict auditors and other users to information from specific sources, allowing a single repository to be deployed for an entire enterprise spanning multiple organizations.

Deployment Flexibility and Scalability

Security controls can be customized with in-line monitoring and blocking on some databases and monitoring only on other databases. The Database Firewall can be deployed in-line, out-of-band, or in proxy mode to work with the available network configurations. For monitoring remote servers, the Audit Vault Agent on the database server can forward the network traffic to the Database Firewall. Delivered as a soft appliance, a single Audit Vault Server can consolidate audit logs and firewall events from thousands of databases. Both Audit Vault Server and the Database Firewall can be configured in a HA mode for fault tolerance.

Contact Us

For more information, visit oracle.com or call +1.800.ORACLE1 to speak to an Oracle representative.

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

Hardware and Software, Engineered to Work Together