ORACLE DATA SHEET

ORACLE AUDIT VAULT AND DATABASE FIREWALL

ORACLE
AUDIT VAULT
AND
DATABASE FIREWALL

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 collected at the network level 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.

KEY BUSINESS BENEFITS

- Manage data risks by detecting and blocking attempts to compromise data in application databases
- Decrease the operational costs of compliance with governance and regulatory policies
- Provide visibility into system use and activity tracking for on-premise and cloud systems across the hybrid data center
- Address compliance initiatives quickly with pre-packaged and customizable reports
- Reduce cost of ownership with a secure appliance form factor

Detective and Preventive Controls

While perimeter firewalls play an important role in protecting data centers from unauthorized external access, 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, monitoring database activity and enforcing security controls in and around the database have become critical imperatives. Effective monitoring and auditing can alert on, and block, attempted policy violations as well as provide comprehensive reports for compliance.

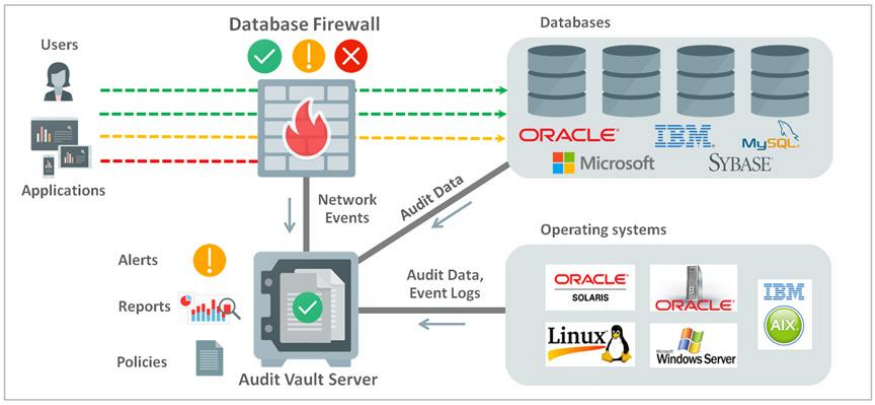

Figure 1. Oracle Audit Vault and Database Firewall

Oracle Audit Vault and Database Firewall continuously monitors application behavior, recognizing unexpected or unauthorized behavior and helping prevent SQL injection, application bypass, and other malicious activities from reaching the database. The solution also monitors and audits the activities of privileged and application users inside the database.

KEY FEATURES

- Performs activity monitoring and blocking on the network and consolidates audit data from Oracle, MySQL, Microsoft SQL Server, SAP Sybase, and IBM DB2 databases
- White list, black list, and exception list based enforcement on the network
- Collects audit data from systems deployed on-premise and in the cloud
- Built with an extensible audit collection framework with templates for XML and table-based audit data
- Includes dozens of built-in customizable compliance reports and delivers proactive alerting and notification
- Supports interactive, PDF, and Excel reports
- Incorporates a fine grained audit data access authorization model
- Highly scalable architecture supports large number of databases with high traffic volumes
- Delivered as a secure, pre-configured software appliance for convenience and reliability
- Supports high availability deployment options

RELATED PRODUCTS

Oracle Database 12c Defense-in-Depth Security Solutions:

- Oracle Advanced Security
- Oracle Data Masking and Subsetting
- Oracle Database Vault
- Oracle Key Vault
- Oracle Label Security

Oracle Audit Vault and Database Firewall can also consolidate audit data from Microsoft Active Directory, Microsoft Windows, Oracle Solaris, Oracle Linux, Oracle ASM Cluster File System, and IBM AIX. A plug-in architecture enables deployment of custom agents to consolidate audit data from application tables and other sources.

Database Firewall for Activity Monitoring and Blocking

Oracle Database Firewall incorporates 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 of statements that are not permitted for the database. Exception list-based policies provide additional deployment flexibility by overriding white list or black list policies. Policies can be enforced based on a number of query attributes, including SQL category, program name, user, and IP address. This flexibility, combined with highly accurate SQL grammar analysis, enables organizations to minimize false alerts and collect only important data. Database Firewall events are logged to the Audit Vault Server, enabling reports to span information observed on the network in combination with audit data.

Enterprise Audit Data Consolidation and Lifecycle Management

By collecting and managing native audit data, Oracle Audit Vault provides a complete view of database activity along with full execution context irrespective of whether statements were executed directly, through dynamic SQL, or through stored procedures. In addition to consolidating audit data from databases, operating systems, and directories, the Audit Collection Plug-in can be used to collect audit data from application tables or XML files and securely transfer them to the Audit Vault Server. Audit data from databases is automatically purged after it has been moved to the Audit Vault Server freeing up space on the system. Audit Vault Server's repository is encrypted and protected by Oracle Database Vault, ensuring security and integrity of the audit data while enforcing separation of duties for Audit Vault administration. Audit Vault supports data retention policies spanning months, 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 network events and audit data from the monitored systems. For detailed analysis of trends, specific systems, or events consolidated data can be combined, filtered and presented interactively or in PDF and Excel formats. 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 to information from specific sources, allowing a single repository to be deployed for an entire enterprise spanning multiple organizations.

Deployment Flexibility and Scalability

A flexible deployment architecture allows security controls to 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 a variety of network configurations. Alternatively, a Host Monitor installed on a database server can forward network traffic to the remote Database Firewall. Delivered as a pre-configured software 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 high availability mode for fault tolerance.

ORACLE

CONTACT US

For more information about Oracle Audit Vault and Database Firewall, visit oracle.com or call +1.800.ORACLE1 to speak to an Oracle representative.