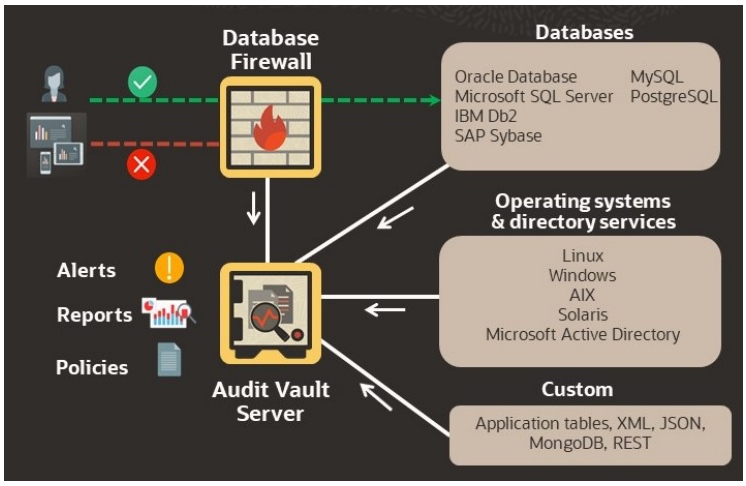
ORACLE

Oracle Audit Vault and Database Firewall 20

Oracle Audit Vault and Database Firewall (AVDF) consolidates activity audit data from Oracle and non-Oracle databases, operating systems, and directories, and provides security and compliance reports. Through an accurate SQL grammar-based engine, the Database Firewall monitors SQL traffic and blocks unauthorized SQL. Now with a modern and simplified UI, and an extensible audit platform, Oracle Audit Vault and Database Firewall 20 is your first line of defense with enterprise-level scale, security, and automation.



DATABASE ACTIVITY AUDITING & AUDIT DATA COLLECTION

Audit Vault collects audit/activity data from database users and applications, including those with high administrative privileges. It collects audit data on all

Key business benefits

- Lowers security risks by auditing and monitoring database activity across enterprise databases
- Blocks unauthorized SQL traffic from reaching the database
- Provides out-of-the-box audit and activity reports for compliance and security investigations
- Provides enterprise-level scale, security, automation, and extensibility

Key features

Database Auditing & Audit Collection

- Audit privileged user activity
- Audit configuration changes
- Audit user account management
- Audit security changes
- Audit logon/logoff events
- Audit sensitive data access
- Track how many rows of data were selected from sensitive tables
- Audit stored procedure and entitlement changes, along with before/after values (for Oracle)
- Create seeded policies (for Oracle)
- Correlate with OS activity

SQL Traffic Monitoring

- Analyze incoming SQL with a multi-stage database firewall
- Accurately detect and log threats using AVDF's SQL grammar engine
- Monitor database traffic
- Block SQL injection attempts
- Monitor and alert on exfiltration attempts using SELECT operations on sensitive tables (for Oracle)

database-wide critical changes, user account modifications, authorization changes, and login/logout events. In addition to the out-of-the-box supported sources, it can also collect audit data from application tables or files, map them to the standard format, and include them in a single report across all sources.

For Oracle databases, it additionally captures before/after values, and changes to user entitlements and stored procedures. With support for pre-seeded audit policies, it is now easy to implement best practices for auditing.

SQL TRAFFIC MONITORING WITH DATABASE FIREWALL

Database Firewall provides a multi-stage firewall that inspects SQL traffic going into the database and determines with high precision whether to allow, log, alert, substitute, or block the SQL. The SQL traffic goes through multiple stages, including checks for the IP address, database/OS user, program name, SQL statement category (DDL, DML), and database tables being accessed. It blocks and/or alerts both SQL that is in the deny-list and SQL that is not in the allow-list, helping prevent SQL injection attacks. The Database Firewall can capture the returned number of rows from a SQL SELECT statement (for Oracle) and this value can be used to monitor and alert on exfiltration attempts. The SQL grammar engine ensures that a firewall policy defined on a SQL statement is applicable to equivalent SQL statements, making it easy to develop robust policies.

Database Firewall events are stored in the Audit Vault Server and consolidated with the audit data giving customers a unified view into all activities.

POWERFUL REPORTING AND ALERTING CAPABILITIES

Audit Vault provides several out-of-the-box reports on changes to database configuration, security, and user entitlements. It also provides reports on login/logout, sensitive data access and modification, stored procedure changes, and many more. AVDF reports also provide the returned number of rows from SQL SELECT statements which can be used for analyzing data exfiltration attempts. Report data can be easily filtered and searched for investigations.

Through compliance reports for GDPR, PCI, GLBA, HIPAA, IRS 1075, SOX, and UK DPA, customers can easily provide needed reports to auditors. Third-party reporting tools can connect to the Audit Vault schema for further analysis.

Audit Vault raises alerts on user-specified events such as multiple failed login attempts, sensitive table access by unauthorized users, and data export operations. Additionally, for Oracle databases, returned number of rows from SQL SELECT statements can be used for monitoring and alerting on data exfiltration attempts.

ENTERPRISE DEPLOYMENT

Delivered as a pre-configured software appliance, Oracle AVDF can be installed on an x86 hardware of choice, giving customers the scale they need. It is also available from the Oracle Cloud Marketplace and can be deployed in an OCI tenancy within minutes. Oracle AVDF on OCI can monitor targets deployed on-premises and on the Oracle Cloud, including Oracle Autonomous Database services.

Periodic release updates for Oracle AVDF include updates to the embedded operating system, Oracle database, and the AVDF application itself, simplifying its maintenance. Further, Audit Vault automatically updates the agents used for collecting audit data and eliminates administrator involvement. Customers can use the rich command-line interface to automate their operations.

Audit Vault Server can consolidate audit data and firewall events from hundreds or thousands of databases and operating systems. It can be deployed in active/standby

Powerful Reporting and Alerting

- Out-of-the-box reports for security and compliance
- Customizable reports
- Intuitive charts
- Easy filtering for investigation
- An open schema for integration with third-party reporting tools
- Powerful custom alert builder

Enterprise Deployment

- Highly scalable architecture
- Full-stack software appliance that can be deployed on X86 hardware
- Deployable in an OCI tenancy within minutes from the Oracle Cloud Marketplace
- High availability
- Auto updateable agents
- Audit data archival/restore
- Separation of duties (SoD)
- Active Directory authentication
- SIEM/Syslog integration
- On-premises and cloud targets

Supported Target Types

- Databases: Oracle, Microsoft SQL Server, MySQL, IBM Db2, PostgreSQL, SAP Sybase
- Operating systems: Linux, Windows, Solaris, AIX
- Custom collector to collect data from application audit tables, XML/JSON data, MongoDB, REST
- Microsoft Active Directory
- Oracle Cluster File System (ACFS)

Related Products

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

mode, ensuring availability. Customers can configure the data archival policies to automatically archive historical data to low-cost storage and retrieve it as needed.

Beyond hardened configuration, Oracle AVDF encrypts the collected data using Transparent Data Encryption, encrypts the network traffic, uses Database Vault to restrict access to data, and provides separation of duties between the administrator and the auditor.

Oracle Audit Vault and Database Firewall 20 supports both cloud and on-premises databases with one single dashboard giving customers independent insight into the activities on their databases even if they are managed by a cloud vendor.

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 facebook.com/oracle twitter.com/oracle