ORACLE

Data Sheet

Oracle Audit Vault and Database Firewall 20

Oracle Audit Vault and Database Firewall (AVDF) goes beyond database activity monitoring to manage your Oracle Database's security posture, enhancing AVDF's best-in-class activity monitoring capabilities with visibility into security configuration, user entitlements, stored procedures, and how much and what types of data are in the database.

AVDF collects audit data from Oracle and non-Oracle databases, operating systems, and directories, whether on the cloud or on-premises. AVDF protects the aggregated audit data in a secure repository, where the audit data is safe from tampering. Capable of working with almost anything that produces an audit trail, AVDF is your enterprise-level audit platform with scalability, security, and automation.

The Database Firewall offers network-based SQL inspection, making it easy to identify anomalies and block unauthorized SQL, including SQL injection attacks.

AVDF's fleet-level view gives you insight into all of your systems and enables you to detect issues across your IT estate. With its powerful reporting and alerting, AVDF supports compliance audits and incident investigations and provides a modern, scalable platform for a full 360-degree view of database activity and security posture.

Key features

Database Security Posture Management (Oracle)

- Assess database security configuration and develop an actionable mitigation plan
- Understand your users, privileges, and their drift
- Track security configuration drift against the baseline
- Discover types of sensitive data, where, and how much
- Map assessment results to CIS, DISA STIG, and EU-GDPR security benchmarks

Database Auditing & Audit Collection

- Know who has accessed your data
- Audit user activity, including privileged users
- Audit policy and stored procedure changes
- Audit account and entitlement changes
- Audit sensitive data access
- Correlate database and OS activity, including SUDO
- Track how many rows were selected from sensitive tables
- Track before/after values (Oracle Database, Microsoft SQL Server and MySQL)
- Centrally manage audit policies (Oracle Databases)

Figure 1: Comprehensive view of user activities

Assess and Discover

Oracle Database security posture management finds your sensitive data, assesses how it is protected, and monitors who access the data.

Security assessment gives you a simplified fleet-wide view of the security configuration for all your Oracle databases, along with the security findings and associated risks. Detailed remarks help you better understand risk and evaluate strategies to minimize that risk. With Database Security Posture Management, you can detect and track security configuration drift and define a security baseline and monitor deviations from your baseline security posture.

User entitlements give you insight into your users, their roles, privileges, activities, and how those entitlements may have drifted over time.

Data discovery helps you understand how much and what types of sensitive data are stored in your Oracle databases. AVDF also identifies users who access that data.

AVDF can help you validate that the security posture is appropriate for that data and develop mitigation plans to close gaps. For example, you could create policies to audit access to the data or create Database Firewall policies that restrict access to well-known and trusted paths.

SQL Traffic Monitoring

- Monitor and analyze incoming SQL with the database firewall
- Accurately detect threats using AVDF's patented SQL grammar engine
- Detect and block SQL injection attempts or anomalous access
- Alert on exfiltration attempts using SELECT (Oracle Databases)
- Global sets to use across multiple DBFW policies and databases

Powerful Reporting and Alerting

- Out-of-the-box reports for security and compliance
- Audit Insights for the top user activities
- Customizable reports and filtering for investigation
- PDF/XLS reports
- An open schema for third-party reporting tools
- Powerful alert builder

Supported Target Types

- Databases: Oracle, Microsoft SQL Server, MySQL, IBM Db2, PostgreSQL, SAP Sybase, MongoDB (see custom collector below)
- Operating systems: Linux, Windows, Solaris, AIX
- Custom collector to collect data from application audit tables, XML/JSON data, MongoDB, CSV, REST
- QuckCSV collectors for Databases like MariaDB, EnterpriseDB (Postgres), and other systems that create audit data in CSV
- Microsoft Active Directory
- Oracle Cluster File System (ACFS)
- On-premises and cloud targets

Enterprise Deployment

- Highly scalable architecture

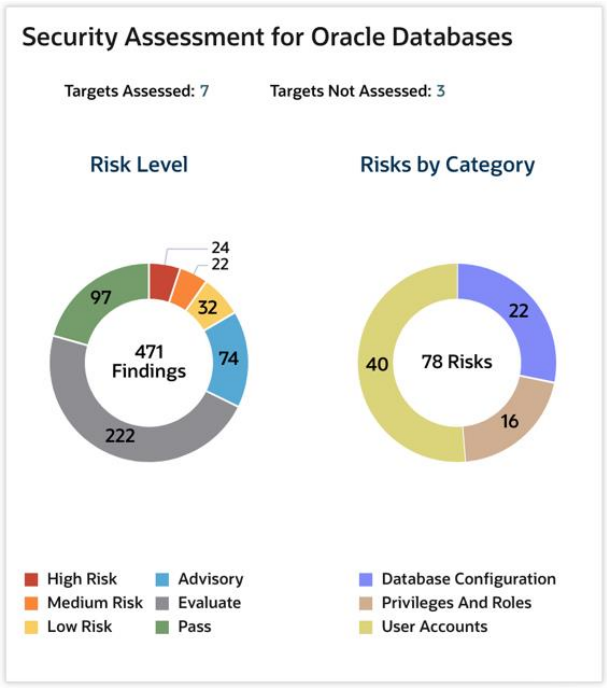

Figure 2: Database security posture management

Audit and Monitor

AVDF gives you visibility into database activity by collecting and aggregating audit data and network-based monitoring of SQL statements for the most popular relational databases. AVDF aggregates audit/activity data into Audit Vault - a secure repository where the data is available for analysis, alert generation, and reporting. Audit Vault captures activity from database users and applications, including privileged users, critical changes, user account modifications, authorization changes, and login/logout events. AVDF also monitors the returned number of rows from SQL SELECT statements to identify potential data exfiltration attempts.

In addition to out-of-the-box supported sources, AVDF collects audit data from application tables or audit files, maps them to the standard format, and includes them in a single report across all sources. No matter what the source, if it produces an audit trail, chances are good that AVDF can work with it. For Oracle databases, users can centrally manage and publish audit policies from AVDF.

Report and Alert

AVDF includes a powerful interactive reporting engine with dozens of out-of-the-box activity reports like login/logout, sensitive data access and modification, stored procedure changes, and many more. These reports can be scheduled, downloaded, and saved. Report data can be easily filtered with different conditions to expedite after-incident investigations.

The audit insights dashboard offers a bird's eye view and provides immediate insight into the top user activities across one or multiple databases. There are three different insight views – audit events, network-collected monitoring events, and a combined that shows a holistic view of all collected events.

- High availability and disaster recovery
- Automated audit data archival
- Security Technical Implementation Guidelines (STIG) compliant audit policies (Oracle Databases)
- Separation of duties (SoD), including support for the read-only auditor
- Active Directory authentication
- SAML 2.0 integration
- SIEM/Syslog integration
- FIPS 140-2 mode support
- Automation through command-line-interface
- Auto-updateable agents
- Agentless and/or remote audit collection for Oracle and Microsoft SQL server databases
- Full-stack software appliance on your x86 server with periodic updates
- Deployable in an Oracle Cloud tenancy within minutes

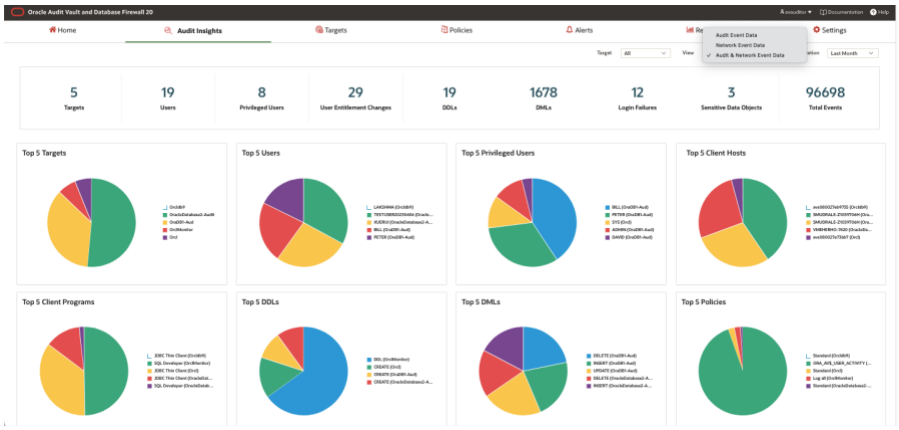

Figure 3: Audit Insights Dashboard

The self-service compliance dashboard gives auditors easy access to pre-defined reports for GDPR, PCI, GLBA, HIPAA, IRS 1075, SOX, and UK DPA, helping organizations manage ongoing audits efficiently. Third-party reporting tools can connect to the Audit Vault for further analysis.

Policy-based alerts raise notifications on suspicious activity. The alert policy engine is flexible and intuitive, enabling targeted policies that reduce false positives. Customizable thresholds monitor tables containing sensitive data, generating an alert when SQL queries return more rows than policy permits.

Prevent and Protect

Finally, to prevent and protect unauthorized activities on the database, AVDF Database Firewall inspects SQL traffic before it reaches the database. Database firewall policies determine if the SQL can be forwarded to the database or if it should be blocked. The database firewall records activity, forwarding events to the Audit Vault for analysis, reporting, and alerting.

Unlike other database activity monitors, AVDF does not rely on regular expressions to detect suspicious activity. Instead, AVDF uses a patented grammar-based engine to parse and evaluate SQL statements. Understanding the context of the SQL in much the same way that the database does, AVDF can identify database actions like select, insert, and delete. AVDF is also aware of database objects like tables and views. This approach to activity monitoring reduces false positives to near zero and gives your teams actionable alerts.

Because AVDF is SQL-aware, firewall policies can profile normal application behavior. If an application suddenly begins executing abnormal SQL (for example, due to an SQL injection attack) the database firewall alerts on the activity and can block it.

Firewall policies go beyond just inspecting the SQL – they also consider the session context – what location did the connection come from? What program is being used? Who are the database and operating system users? This information lets you develop firewall policies that create a trusted path to the data, and block attempts to access data from outside of that path – even if the attacker knows the application's credentials!

Enterprise Deployment

AVDF's Audit Vault Server can consolidate audit data and firewall events from thousands of databases, operating systems, and applications. AVDF can be deployed in active/standby mode, ensuring availability. Oracle Audit Vault and Database Firewall lets you monitor cloud and on-premises databases in a single dashboard. AVDF gives you independent insight into activity on your databases - even when a cloud vendor or other third party manages those databases.

Administrators can use AVDF's rich command-line interface to automate operations, reducing the risk of error and simplifying repetitive or large-scale operations.

Audit data lifecycle management is automated. Retention policies that meet your organizational requirements can be configured, with different policies supported for different sources. Historical data is automatically archived, helping you reduce storage costs. Archived data can be retrieved as needed.

AVDF can integrate with identity providers (IDP) such as Azure, Active Directory Federation Services (ADFS), and Oracle Access Manager (OAM) through SAML 2.0 integration. This feature allows AVDF console users to be authenticated by IDP using mechanisms such as single sign-on (SSO) and multi-factor authentication (MFA).

Delivered as a pre-configured software appliance, AVDF can be installed on your x86-64 hardware of choice, giving you the scale you need. If you are using the Oracle Cloud Infrastructure, you can deploy AVDF in minutes using images from the Oracle Cloud marketplace. AVDF on OCI can monitor targets deployed on-premises and on the Oracle Cloud, including Oracle Autonomous Database services.

The AVDF repository is encrypted at rest using Oracle Transparent Data Encryption. Collected data is also encrypted in motion as it moves from the collection agent to the repository. AVDF uses Oracle Database Vault to restrict access to data, and provide separation of duties between AVDF administrators and auditors.

Periodic release updates for AVDF include updates to the embedded operating system, Oracle database, and the AVDF application, simplifying maintenance. Audit Vault automatically updates agents, saving valuable time and eliminating administrator involvement. Agentless audit collection expedites AVDF implementation and makes it easy to begin protecting your Oracle and Microsoft SQL Server database fleet.