ORACLE DATABASE

ORACLE DATABASE FIREWALL

A POWERFUL, SCALABLE, ENTERPRISE DATABASE FIREWALL

KEY FEATURES

- Flexible deployment models include monitoring, and blocking
- White list, black list, and exception list based policies
- Highly scalable architecture for enterprise applications
- Dozens of built-in customizable compliance reports
- Real-time security alerts
- Supports Oracle, MySQL, Microsoft SQL Server, Sybase, and IBM DB2
- Supports Oracle Advanced Security TDE

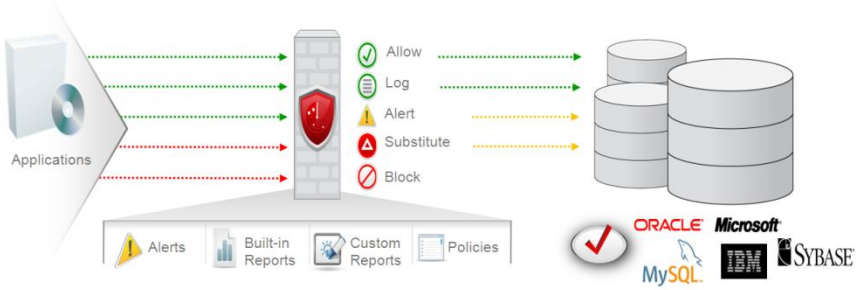
RELATED PRODUCTS

- Oracle Audit Vault
- Oracle Database Vault
- Oracle Advanced Security

Oracle Database Firewall acts as the first line of defense for databases, helping prevent internal and external attacks from reaching the database. Highly accurate SQL grammar-based technology monitors and blocks unauthorized SQL traffic on the network before it reaches the database. Oracle Database Firewall is easy to configure and can be deployed with no changes to existing applications.

Database Firewall for Security and Compliance

Network firewalls play an important role today in protecting data centers from unauthorized, external access. Data center attacks, however, have grown increasingly sophisticated, by-passing perimeter security, taking advantage of trusted middle tiers, and even masquerading as privileged insiders. As a result, enforcing security controls around the database has become critical. Oracle Database Firewall creates a defensive inner-perimeter that monitors and enforces normal application behavior, helping prevent SQL injection, application bypass, and other malicious activity from reaching the database.



Next-Generation Network-based Database Security

Oracle Database Firewall examines the grammar of the SQL statements being sent to the database, analyzes their meaning, and determines the appropriate security policy to apply. Grammatical classification and session-factor profiling provide a powerful method for tracking database access, and enables the Oracle Database Firewall to recognize changes in normal behavior, such as SQL injection attacks on applications, and block them before they reach the database. This highly accurate approach provides a significantly higher degree of protection than first-generation database monitoring technologies that rely on recognizing the signature of known security threats.

Flexible Security Policies

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 firewall expects to see. These can be learned over time or developed in a test environment. A black list includes schemas, tables, users, and SQL statements that are not permitted to be sent to the database. Exception list based policies provide additional deployment flexibility that can be used 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. Oracle Database Firewall can log queries, raise alerts, block the incoming SQL statement, or substitute it with a harmless SQL

statement. This flexibility, combined with advanced SQL grammar analysis, provides organizations graceful application handling of unauthorized requests.

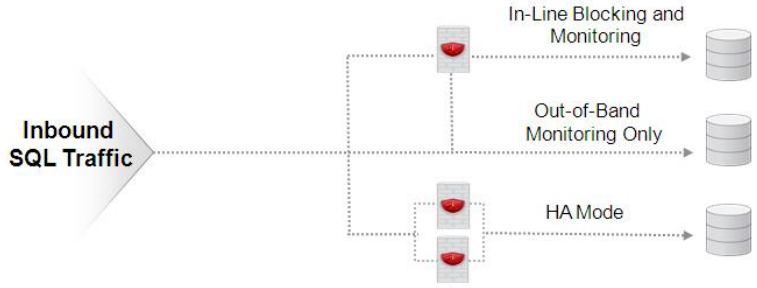
Customizable Reporting and Alerting

Oracle Database Firewall includes dozens of out of the box reports that can be easily customized for regulations such as the Sarbanes-Oxley (SOX) Act, Payment Card Industry Data Security Standard (PCI DSS), and Health Insurance Portability and Accountability Act (HIPAA). Real-time alerts can also be set up for fast response to any policy exception. For privacy and compliance requirements, personally identifiable information contained in logged SQL can be easily masked.

Multiple Deployment Models

Oracle Database Firewall resides on the network, transparent to database servers and applications. Customers can choose from several deployment models to meet their business requirements:

- In-line blocking and monitoring mode
- In-line monitoring only mode
- Proxy blocking and monitoring mode
- Out-of-band monitoring only mode



Remote database servers can be monitored with optional low impact host based agents. Oracle Database Firewall supports deploying parallel firewall devices for high availability. Oracle Database Firewall Management Server centrally manages the policies for multiple database firewalls, consolidates the activity data, and generates reports. Oracle Database Firewall works seamlessly with existing Oracle Database security solutions including privileged user controls, transparent data encryption and native database auditing.

Contact Us

For more information about Oracle Database Firewall, 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

SOFTWARE. HARDWARE. COMPLETE.

ORACLE