

¿Qué es Oracle Database Firewall?

UN CORTAFUEGOS DE BASES DE DATOS EMPRESARIALES POTENTE Y ESCALABLE

Oracle Database Firewall es una solución única que proporciona a las organizaciones una **primera línea de defensa para todas sus bases de datos**. Supervisa el acceso a datos, hace cumplir las políticas de acceso, destaca las posibles anomalías y ayuda a proteger contra los ataques a la red originados dentro o fuera de la organización.

Oracle Database Firewall previene los ataques comunes a bases de datos, como la inyección SQL y otras, mediante el bloqueo de tráfico SQL anormal. También genera alertas inteligentes y precisas, supervisando la actividad de base de datos, y reduciendo así costes administrativos y de gestión.

Se instala de forma transparente entre la aplicación y la base de datos que se está supervisando, y es una solución autónoma **compatible con bases de datos Oracle y no-Oracle**.

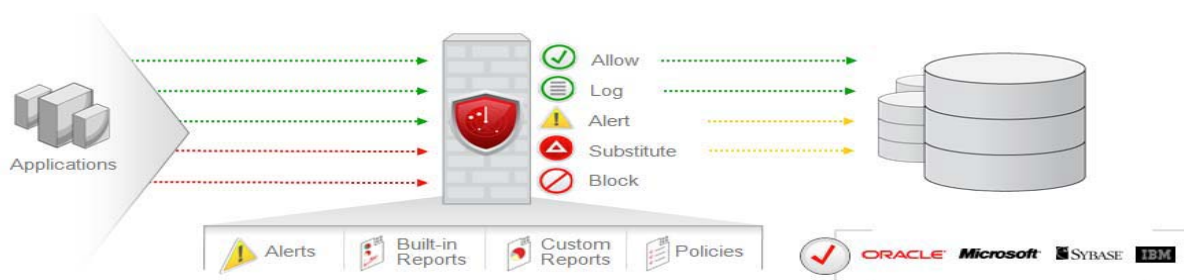


Figura 1: Oracle Database Firewall

¿Para qué empresas es relevante Oracle Database Firewall?

- Aquellas que, por motivos de seguridad o rendimiento, quieran filtrar, sustituir o reemplazar dinámicamente, en función de su política, determinadas consultas a sus bases de datos.
- Empresas o servicios con aplicaciones que dispongan de formularios o pantallas que, al recoger datos, generen instrucciones SQL de manera dinámica.
- Organizaciones con necesidades de control, clasificación y auditoría de las consultas generadas contra la base de datos.

Empresas de comercio electrónico o particularmente expuestas en aplicaciones web que, potencialmente, puedan acceder a datos sensibles mediante formularios susceptibles de ser atacados con técnicas de inyección SQL.

- Aquellas organizaciones que necesiten cumplir normativas de seguridad como PCI, SOX, HIPAA, ... cuyos informes de control están ya implementados en Oracle Database Firewall.

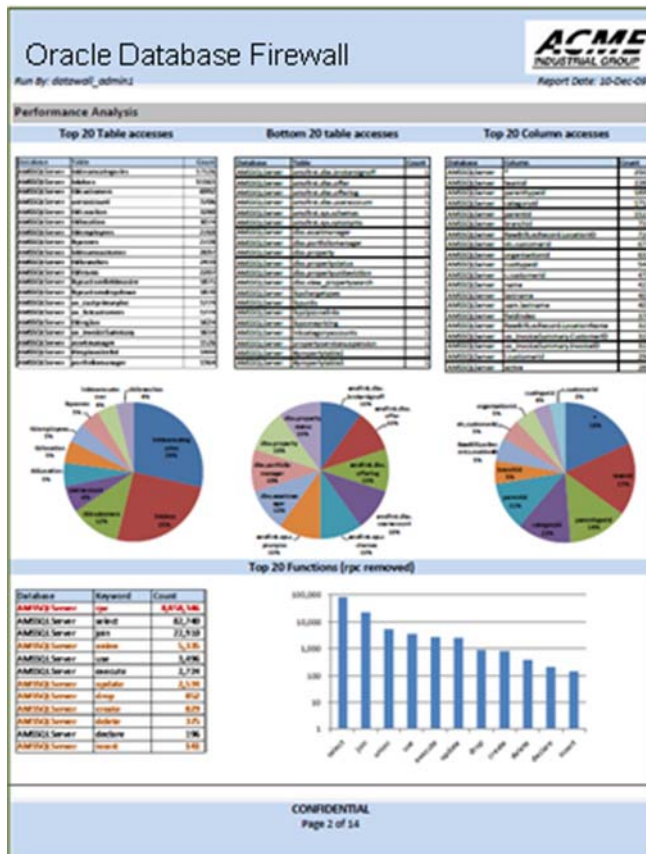


Figura 2: Más de 150 informes pre construidos y adaptables

CARACTERÍSTICAS CLAVE

- Modelos de implementación flexibles que incluyen monitorización y bloqueo
- Políticas basadas en listas blancas, listas negras y listas de excepciones
- Arquitectura altamente escalable para aplicaciones empresariales
- Docenas de informes de conformidad integrados y personalizables
- Alertas de seguridad en tiempo real
- Compatible con bases de datos Oracle, Microsoft SQL Server, Sybase e IBM DB2 LUW

¿Cómo funciona Oracle Database Firewall?

Cuando el programador de una aplicación incorpora en una sentencia SQL una variable cuyo valor es suministrado por el usuario final y su contenido no es correctamente filtrado, es posible que el usuario final pueda introducir valores que puedan ser interpretados como parte de una sentencia SQL. Por ejemplo:

“SELECT * FROM users WHERE name = '' + userName + '";”

Usando un nombre de usuario “ilegal” se puede conseguir (ataque *SQL Injection*) que la sentencia se transforme en :

```
SELECT * FROM users WHERE name = '' OR '1'='1';  
SELECT * FROM users WHERE name = 'a'; DROP TABLE users; SELECT * FROM  
userinfo WHERE 't' = 't';
```

Mediante SQL Injection se obtienen datos no permitidos de las bases de datos o se realizan ataques de denegación de servicio. (En el caso indicado, por ejemplo, podría destruirse la tabla de identificación de usuarios).

A diferencia de otros proveedores de seguridad de bases de datos que identifican eventos fuera de la política de seguridad mediante expresiones regulares, comparando cadenas de texto o comparando esquemas, Oracle Database Firewall entiende el significado, los motivos y las intenciones del SQL.

Oracle Database Firewall implementa un enfoque basado en “listas blancas” que sólo permite que se envíen a la base de datos las sentencias SQL correctas, y aprende de las sentencias SQL que desea controlar. El motor gramatical de Oracle Database Firewall va más allá de la sintaxis y se acerca al significado, la intención o los motivos de la sentencia SQL antes de que se envíe a la base de datos.

Cuando el SQL se analiza, se clasifica en un “cluster” según la estructura de la sentencia y se proporciona un valor hash único que identifica de manera eficiente si el SQL se ha registrado o puesto en la lista blanca. Sólo se registra el SQL una vez para leer múltiples veces.

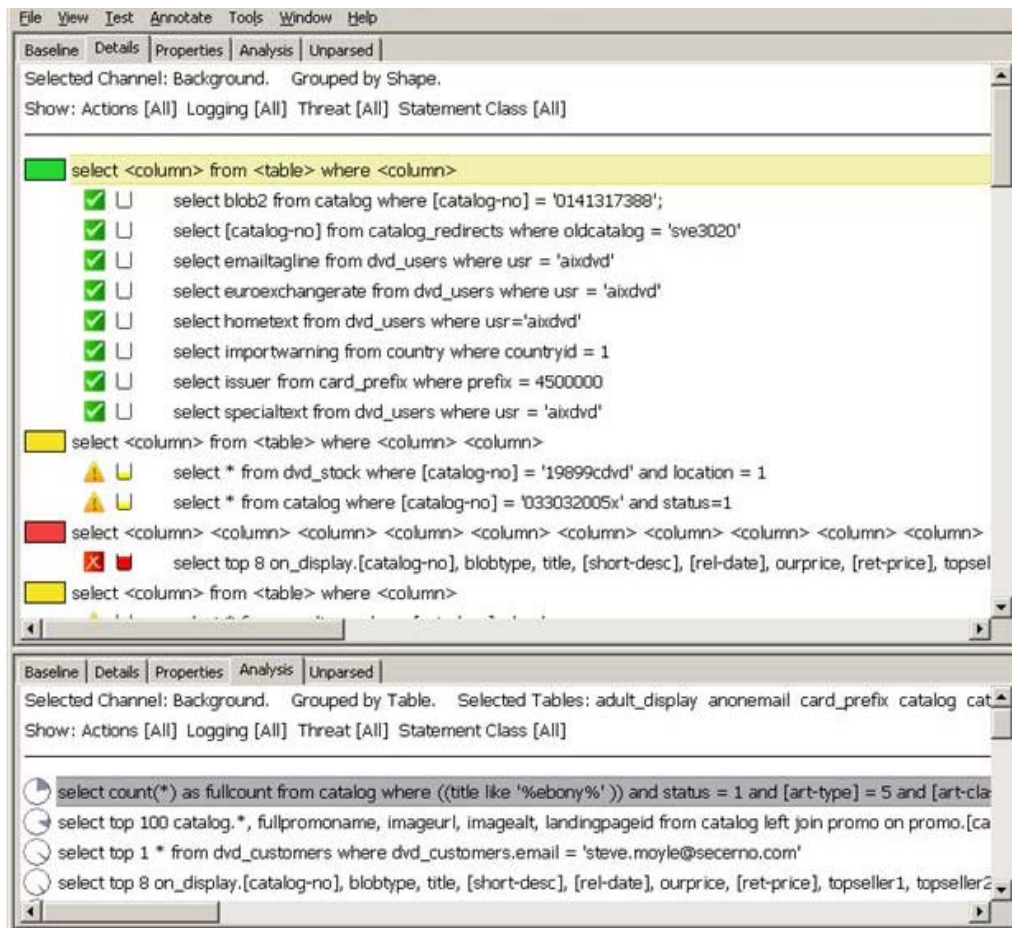


Figura 3: Clustering SQL

Si se usa únicamente expresiones regulares para establecer una política de filtrado, sucede lo siguiente:

- La comparación de patrones no entiende la intención del SQL
- Puede generar falsos positivos y ausencia de detección
- Necesita un alto nivel de mantenimiento

Por otro lado, Oracle Database Firewall analiza el SQL que se registra en los archivos de “log”, de modo que:

- Se generan agrupaciones (clusters) que son deterministas, y facilitan la aplicación de políticas precisas,
- La velocidad de búsqueda para validación es constante en todos los grupos de la política,
- Mediante la comprensión de la gramática SQL, la inyección SQL, y otros SQL que no cumplan con la política se detectan como anomalías.

Componentes de Oracle Database Firewall

- Oracle Database Firewall - interroga y aplica la política de SQL a la base de datos.

- Management Server (gestión centralizada, alertas e informes).
- Analyzer (Analiza la sesión de SQL para establecer las líneas de base de la política).

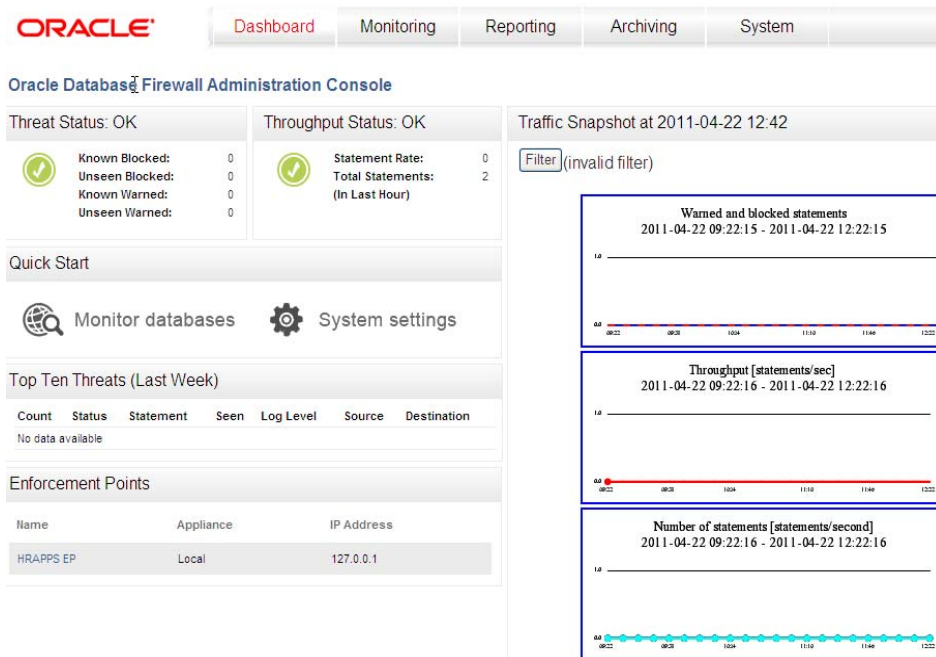


Figura 4: Consola de Administración de Oracle Database Firewall

Más información:

Portal Técnico principal: (White Papers, documentación, descargas)

<http://www.oracle.com/technetwork/database/databasefirewall/overview/index.html>

Preguntas más frecuentes:

<http://www.oracle.com/technetwork/database/database-firewall/oracle-database-firewall-faq-291222.html>

Ejemplo de instalación y uso en Youtube (no oficial)

http://www.youtube.com/watch?v=ljRv8GgruFA&feature=channel_video_title

Contacta con Oracle:

Para obtener más información, llama al **900 95 29 02**.

www.oracle.com/es