Bases de datos

Protecting the Data That Drives Business®

Seguridad de las bases de datos

Auditoría y Protección de las Bases de Datos Críticas

Productos SecureSphere de Imperva, los mejores de su clase para la seguridad de las bases de datos:

- Hace auditoría de todos los accesos a información restringida
- Alerta y bloquea los ataques a las bases de datos y las actividades no autorizadas relacionadas con las bases de datos, en tiempo real
- Detecta y aplica parches virtuales a las vulnerabilidades de las bases de datos
- Identifica los derechos de usuario excesivos y los usuarios latentes, y habilita ciclos totales de examen de los derechos
- Agiliza la respuesta ante incidentes y las investigaciones forenses, gracias a elementos avanzados de análisis

Productos

SecureSphere Database Activity Monitoring

SecureSphere Database Firewall

SecureSphere Discovery and Assessment Server

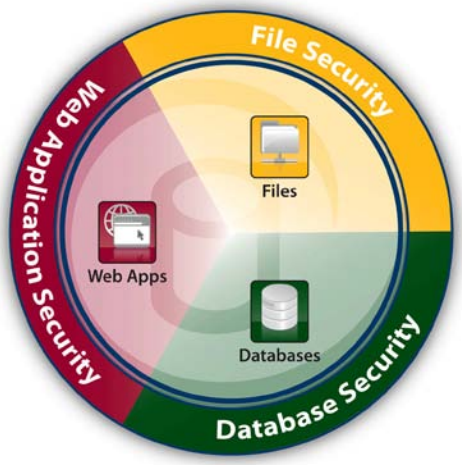
User Rights Management for Databases

ADC Insights

La mejor auditoría y protección de las bases de datos del mercado

Las bases de datos almacenan información extremadamente valiosa y confidencial. Una cantidad creciente de regulaciones de conformidad obligan a las organizaciones a hacer auditorías del acceso a dicha información restringida y a protegerla de los ataques y del mal uso.

Los galardonados productos SecureSphere Database Security de Imperva automatizan las auditorías de las bases de datos, e identifican de inmediato los ataques, las actividades malintencionadas y el fraude. En combinación con las soluciones Web Application Security y File Security de Imperva, SecureSphere es la primera opción para la protección de la información empresarial restringida.



Auditoría continua del uso de la información restringida

SecureSphere monitoriza de forma continua y en tiempo real todas las operaciones de las bases de datos, proporcionando a las organizaciones cadenas detalladas de auditoría que indican el 'quién, qué, cuándo, dónde y cómo' de todas las transacciones. SecureSphere hace auditorías de los usuarios con privilegios que tienen acceso directo a los servidores de bases de datos, así como a los usuarios sin privilegios que tienen acceso a las bases de datos a través de diversas aplicaciones. SecureSphere también monitoriza las respuestas de las bases de datos a fin de alertar y detener las fugas de información restringida.

Elementos de análisis de auditoría para la investigación de incidentes y los análisis forenses

SecureSphere proporciona un profundo discernimiento de las actividades auditadas, a través de elementos interactivos de análisis de auditoría. SecureSphere permite que los equipos de seguridad y los auditores de las bases de datos puedan visualizar, analizar y correlar rápidamente las actividades de las bases de datos, desde cualquier ángulo y a través de un sencillo interfaz de usuario, sin necesidad de scripts SQL. Los elementos interactivos de análisis de auditoría simplifican las investigaciones forenses y habilitan la identificación de tendencias y de patrones, que podrían señalar riesgos de seguridad.

Detección de accesos no autorizados y de actividades fraudulentas

SecureSphere identifica los patrones normales de acceso de los usuarios a la información, mediante la tecnología de perfiles dinámicos de patente en curso. Establece una línea base de toda la actividad de los usuarios, incluyendo DML, DDL, DCL, actividades de sólo lectura (SELECTs) y del uso de procedimientos almacenados. SecureSphere detecta variaciones materiales cuando los usuarios ejecutan consultas no esperadas, y además alerta y bloquea a los usuarios que violen las directivas de acceso. También se puede poner en cuarentena a los usuarios que ejecuten solicitudes SQL no autorizadas, hasta que sus derechos de usuario hayan sido examinados y aprobados.

Bloqueo en tiempo real de las inyecciones SQL, de los ataques DoS y de otros

A la vez que hace auditorías selectivas de la información restringida, SecureSphere monitoriza en tiempo real toda la actividad de las bases de datos a fin de detectar fugas desconocidas de información, transacciones SQL no autorizadas, y ataques a los protocolos y a los sistemas. Tando si se originan en aplicaciones como en usuarios con privilegios, dentro de la red o en los mismos servidores de bases de datos, SecureSphere puede alertar y, como opción, bloquear los ataques malintencionados.

Cumplimiento de directivas e informes ágiles de la conformidad

SecureSphere incluye un conjunto completo de directivas de seguridad y auditoría predefinidas y personalizables. El conocimiento incorporado de fábrica de aplicaciones empresariales tales como SAP, Oracle EBS y PeopleSoft, y de las normativas principales incluyendo SOX, PCI DSS e HIPAA, simplifican la implementación y los lapsos requeridos para alcanzar la conformidad. Las alertas de seguridad pueden ser enviadas a SIEM, a sistemas de tickets y a otras soluciones de terceros, lo que agiliza los procesos empresariales.

Cumplimiento de los requerimientos de conformidad

SecureSphere contribuye a que las organizaciones atiendan múltiples regulaciones de conformidad, incluyendo PCI DSS, SOX e HIPAA.

- Cumple 8 de 12 requisitos PCI de alto nivel, incluyendo las secciones 10, 7 y 8.5
- Satisface los requisitos de auditoría de información financiera de las secciones 302 y 404 de SOX
- Cumple con la separación de tareas
- Garantiza la integridad de la información de auditoría
- Detecta el acceso no autorizado a información financiera y de titulares de tarjetas
- Ofrece informes predefinidos que agilizan la conformidad

Clasificación del alcance de la información a efectos de la conformidad y de la seguridad

SecureSphere detecta todos los sistemas de bases de datos a fin de determinar el alcance de los proyectos de seguridad y de conformidad, a través del descubrimiento y la clasificación automáticas de la información restringida. La combinación de las evaluaciones de las vulnerabilidades junto con la funcionalidad de descubrimiento y clasificación permite a las organizaciones establecer prioridades en sus esfuerzos de mitigación.

Evaluación y parches virtuales para las vulnerabilidades de las bases de datos

Las más de mil evaluaciones de vulnerabilidades en las configuraciones, bases de datos y en las plataformas incluidas en SecureSphere contribuyen a que las organizaciones identifiquen y solucionen las vulnerabilidades. Para una protección inmediata, la funcionalidad de parches virtuales de SecureSphere puede bloquear los intentos de aprovechamiento de las vulnerabilidades descubiertas. Los parches virtuales minimizan la ventana de riesgo y reducen drásticamente el riesgo de infracciones de la información, mientras se prueban e implementan los parches de las bases de datos.

Control eficaz de los derechos de usuario en todas las bases de datos

SecureSphere agrega automáticamente los derechos de usuario, aún entre bases de datos heterogéneas. Con la solución User Rights Management, las organizaciones pueden establecer un proceso automático para la revisión de los derechos de acceso, la detección de derechos de usuario excesivos y comprobar su conformidad con normas tales como las SOX, PCI 7 y PCI 8.5.

Auditoría y protección locales de las bases de datos con el uso de agentes ligeros

Para la total visibilidad y control de todas las actividades de los usuarios, SecureSphere extiende sus capacidades de monitorización, auditoría y de conformidad a los servidores host. Los agentes ligeros SecureSphere hacen auditorías de la actividad de las bases de datos, y protegen la información restringida con un impacto mínimo en el desempeño de los servidores.

Implementación de impacto cero y de rendimiento ultra alto

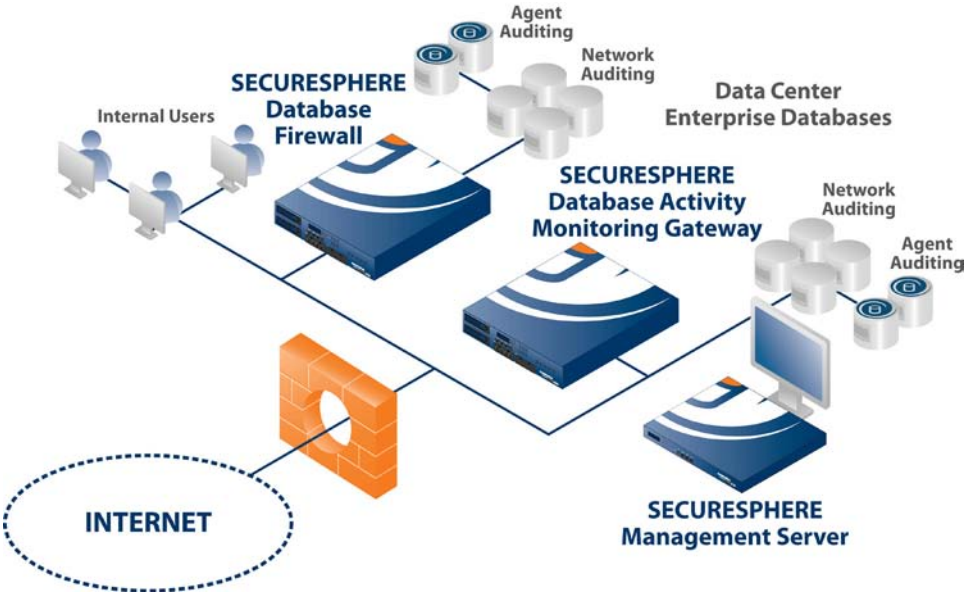
- **Máquinas de hardware**: Ofrecen anchos de banda de múltiples Gigabits y latencias por debajo del milisegundo
- **Máquinas virtuales**: Proporcionan una protección adaptable, confiable y de administración sencilla, que puede crecer con su organización

Seguridad y conformidad inigualada de las bases de datos

SecureSphere atiende todos los aspectos de la seguridad y de la conformidad de las bases de datos, mediante las capacidades de auditoría y la protección en tiempo real, mejores de la industria, sin afectar el rendimiento ni la disponibilidad . Gracias a su arquitectura de múltiples capas, SecureSphere puede crecer para dar apoyo a instalaciones de bases de datos de gran tamaño. Debido a la automatización de la seguridad y de la conformidad, no sorprende que muchas organizaciones hayan elegido a SecureSphere de Imperva para la protección de sus activos más valiosos.

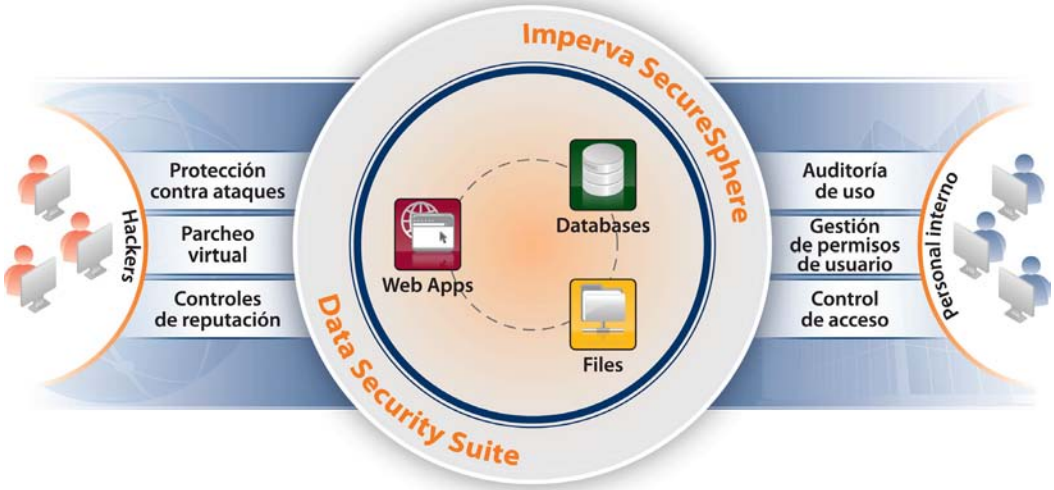
Implementación

- **Monitorización fuera de línea de redes**: Monitorización de las actividades, con cero impacto en el rendimiento y en la disponibilidad de las bases de datos
- **Protección transparente en línea**: Implementación directa y el mejor rendimiento de la industria
- **Monitorización basada en agentes**: Agentes ligeros de software que monitorizan las actividades con privilegios directos y tráfico de red
- **Recopilación de los registros de auditoría**: Aprovecha los registros de terceros de las bases de datos a efectos de elementos de análisis de auditoría, alertas e informes heterogéneos
- **Plataformas compatibles de bases de datos**: Oracle, Microsoft SQL, IBM DB2 (que incluye DB2 para z/OS y DB2/400), Informix, Sybase, MySQL, Teradata y Netezza



Bases de datos

SecureSphere Data Security Suite de Imperva



SecureSphere Data Security Suite es la solución líder del mercado en seguridad y conformidad de la información. SecureSphere protege, de los hackers y de personas mal intencionadas dentro de las empresas, a las aplicaciones web y a la información restringida contenida en bases de datos y en archivos, ofrece una ruta rápida y efectiva en cuanto a coste al logro de la conformidad con las normas legales y de la industria, y establece un proceso repetible para la administración del riesgo de la información.

Familia	Producto SecureSphere
Bases de datos	**Database Activity Monitoring** Capacidades totales de auditoría y de visibilidad del uso de la información de las bases de datos
	Database Firewall Monitoreo de la actividad y protección en tiempo real de las bases de datos cruciales
	Discovery and Assessment Server Evaluación de las vulnerabilidades, administración de las configuraciones y clasificación de la información de las bases de datos
	User Rights Management for Databases Inspección y administración de los derechos de acceso de usuario a bases de datos restringidas
	ADC Insights Informes y reglas predefinidas para la seguridad y la conformidad de SAP, Oracle EBS y PeopleSoft
Archivos	**File Activity Monitoring** Capacidades totales de auditoría y de visibilidad del uso de la información de los archivos
	File Firewall Monitorización de la actividad y protección en tiempo real de los archivos cruciales
	User Rights Management for Files Inspección y administración de los derechos de usuario de acceso a archivos con información restringida
Web	**Web Application Firewall** Protección precisa y automatizada contra ataques a través de Internet
	ThreatRadar Seguridad de las aplicaciones web, con base en la reputación y pionera de la industria

Imperva es la empresa líder en seguridad de la información

Miles de las principales empresas, organizaciones gubernamentales y proveedores de servicio del mundo se apoyan en las soluciones de Imperva a fin de prevenir las violaciones de la información, lograr la conformidad con las normas legales y de la industria, y para la administración del riesgo de la información.

SAP Certified Integration

ICSA labs CERTIFIED Web Application Firewall

Imperva Spain
Edificio Torre Europa
Paseo de la Castellana, 95 – planta 15 A
28046 Madrid
Tel: +34 91 418 69 02

www.imperva.com