



# La historia de Imperva

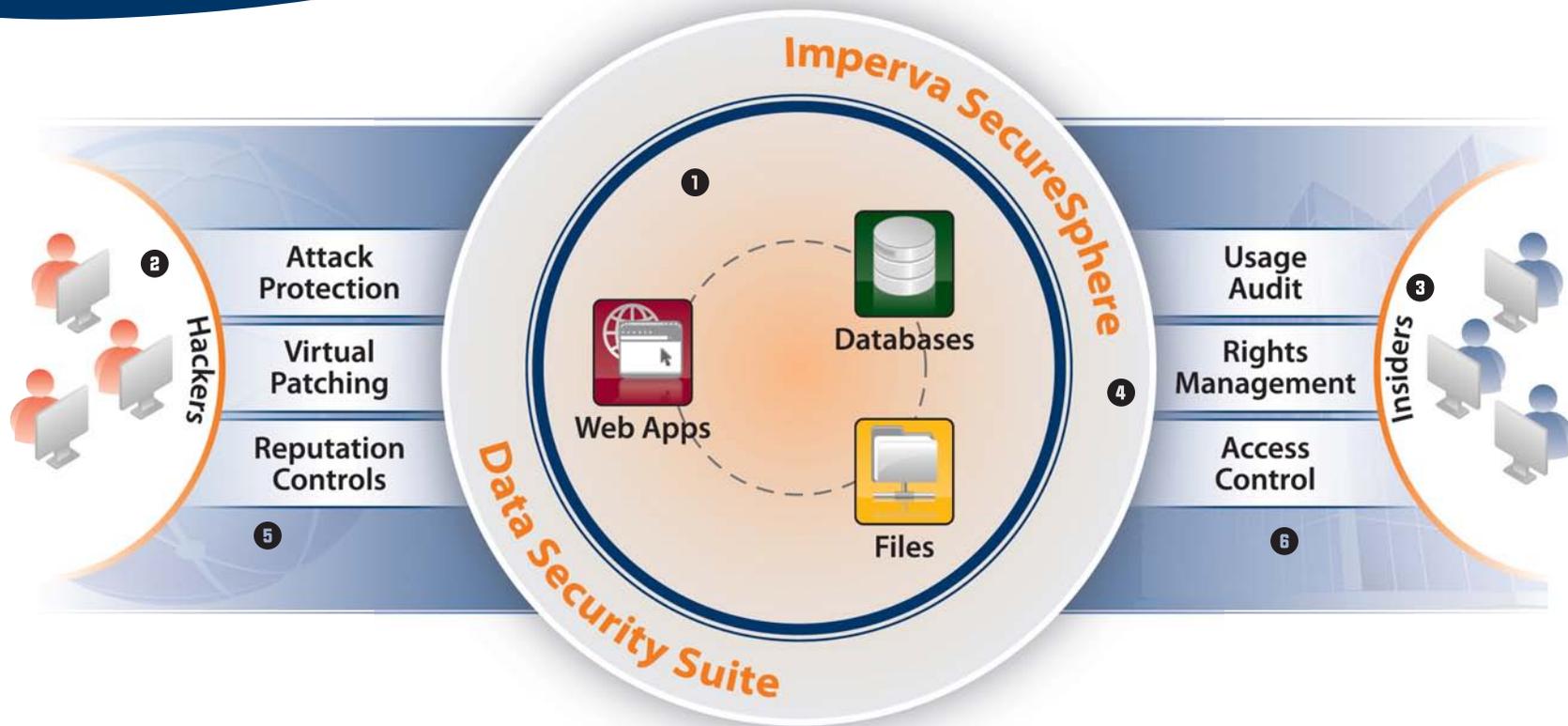


*La misión de Imperva es sencilla:*

**Proteger la información que impulsa a las empresas de nuestros clientes**

*Para lograr eso, Imperva es la empresa líder en la creación de una nueva categoría:*

**La seguridad de la información**



- 1 Su información confidencial se encuentra en bases de datos y en archivos. Las aplicaciones web frecuentemente son una vía para que el mundo entero tenga acceso sus datos confidenciales.
- 2 Su información está en riesgo de ataques de los hackers, de alto nivel tecnológico, automatizados y a gran escala.
- 3 ...y de personas mal intencionadas al interior de su empresa u organización, que pudieran abusar de sus privilegios a fin de obtener ganancias económicas o personales.
- 4 SecureSphere de Imperva es la única solución completa de protección de la información y para cumplimiento de normas para datos sensibles de web, bases de datos y archivos.

- 5 Imperva soluciona el problema de las amenazas externas mediante:
  - » Protección contra los ataques, tanto de los conocidos como los de día cero
  - » Parches virtuales para la mitigación de las vulnerabilidades
  - » Controles basados en la reputación, que detienen el acceso de visitantes malintencionados al sitio web
- 6 Imperva soluciona el problema de las amenazas internas mediante:
  - » Auditorías totales del acceso de las aplicaciones y de los accesos privilegiados a información confidencial
  - » Eliminación de derechos de accesos excesivos y sin uso
  - » Cumplimiento de las directivas de control del acceso y de la separación de funciones

# Comprehensive Data Security

## Quiénes somos

Imperva es la empresa líder mundial en la seguridad de la información. Miles de empresas, organizaciones gubernamentales y empresas de servicio líderes en el mundo se apoyan en las soluciones de Imperva para prevenir robos de la información, satisfacer normas, y administrar los riesgos relativos a la información.

Un factor para reforzar el compromiso de Imperva con la excelencia en la protección de la información es su propio centro ADC (Application Defense Center), una organización de clase mundial dedicada a investigaciones de la seguridad. El centro ADC respalda la protección de primera línea de SecureSphere contra las amenazas nuevas.

## El problema que resolvemos

La información impulsa los negocios y las organizaciones, y eso la convierte en el premio máximo de los hackers y de personas mal intencionadas en el interior de la organización. La información también es objeto de extensos escrutinios legales y normativos. El desafío que se le plantea a las empresas es el de proteger su información y mantener la conformidad con las normas legales y de la industria, y a la vez controlar los costos, la complejidad y el riesgo

## Cómo lo resolvemos

SecureSphere de Imperva es la solución líder del mercado en seguridad y conformidad. SecureSphere protege la información confidencial contra los hackers y personas mal intencionadas en el interior de las empresas, suministra una vía rápida y efectiva en cuanto a costos para el logro de la conformidad con las normas legales y de la industria, y establece un proceso repetible para la mitigación de los riesgos de la información.

### Seguridad de las bases de datos

Soluciones galardonadas para la seguridad y la conformidad de las bases de datos, para la auditoría del acceso a las bases de datos y para proveer de protección en tiempo real contra los ataques a las bases de datos

### Seguridad de los archivos

Máximo nivel tecnológico de administración a auditorías y privilegios para proteger la información no estructurada contenida en servidores de archivos y dispositivos de almacenamiento en la red

### Seguridad de las aplicaciones web

Protección líder del mercado contra ataques web a gran escala, con controles basados en la reputación, administración automática e implementación directa

# Impulsores de negocios

<b>Violación de la información</b>	<b>Prevención</b>	<b>Protección en tiempo real de hackers y de personas mal intencionadas en el interior de la empresa para mitigar el riesgo de violación de la información</b>
Hackers y otras amenazas externas		Protección contra los ataques automatizados a gran escala realizados por hackers
Amenazas internas		Detección e interrupción del abuso de los privilegios de acceso a la información restringida por parte de personas en el interior de la empresa
Desarrollo Web seguro		Mitigación mediante parches virtuales del riesgo de los ataques que aprovechan las vulnerabilidades de las aplicaciones

<b>Conformidad con normas legales y de la industria</b>	<b>Una ruta rápida y efectiva en cuanto a costo al logro de conformidad con las normas mediante una visibilidad completa del uso de la información, las vulnerabilidades y los derechos de acceso</b>
Auditoría del uso de la información restringida	Cadena de auditoría de todos los acceso a la información restringida, conforme a las regulaciones
Monitoreo de usuarios con privilegios	Auditoría de las actividades de los usuarios con privilegios en los servidores host de bases de datos, a efectos de garantizar la separación de tareas
Controles de aplicaciones Web y empresariales	Protección y auditoría de los accesos a la información de las aplicaciones Web y empresariales

<b>Gestión del riesgo de la información</b>	<b>Un proceso automatizado y repetible para analizar el riesgo de la información restringida</b>
Clasificación de la información	Identificación de la información restringida para determinar el alcance de las iniciativas de seguridad y conformidad
Evaluación de vulnerabilidades	Detección y mitigación de las vulnerabilidades de las aplicaciones y del sistema para mitigar el riesgo de violación de la información
Administración de los derechos de usuario	Revisión y restricción de los derechos de acceso a la información para que accedan sólo aquellos que tienen una necesidad operativa de conocerla.

# Soluciones

---

## Prevención de violaciones de la información

SecureSphere de Imperva suministra protección en tiempo real contra las violaciones de la información por parte de hackers y de personas mal intencionadas en el interior de las empresas u organizaciones. SecureSphere permite a los ejecutivos, a los funcionarios a cargo del riesgo, a los auditores y a los profesionales de la seguridad lograr la mitigación de los daños financieros y al prestigio resultantes de las pérdidas de información.

SecureSphere hace lo siguiente:

- » Alerta de o bloquea las solicitudes de acceso cuyas características se desvíen del uso normal de las aplicaciones y de la información, o que violen las directivas corporativas
- » Actualiza las defensas con información proveniente de investigaciones acerca de las amenazas y las vulnerabilidades actuales
- » Hace parches virtuales a las vulnerabilidades de las aplicaciones y de las bases de datos, a fin de reducir la ventana de exposición y el impacto de las correcciones ad-hoc de las aplicaciones

## Conformidad legal y con las normas de la industria

SecureSphere de Imperva reduce enormemente el lapso de tiempo necesario para alcanzar la conformidad, al proveer una visibilidad total del uso de la información, de las vulnerabilidades y de los derechos de acceso. SecureSphere permite a los ejecutivos, a los funcionarios a cargo del riesgo, a los auditores y a los profesionales de la seguridad satisfacer las normas regulatorias en forma rápida y efectiva en cuanto a costos.

SecureSphere hace lo siguiente:

- » Audita todos los accesos a la información confidencial, incluidos los usuarios con privilegios y los usuarios de las aplicaciones
- » Identifica y mitiga las vulnerabilidades de las aplicaciones y de las bases de datos
- » Automatiza la extensa e intensa tarea manual de revisar y aprobar los derechos de acceso de los usuarios

## Administración de los riesgos de la información

SecureSphere de Imperva automatiza los análisis de riesgo de la información confidencial. SecureSphere permite a los ejecutivos, a los funcionarios a cargo del riesgo, a los auditores y a los profesionales de la seguridad establecer procesos continuos y repetibles de reducción de los riesgos de la información.

SecureSphere hace lo siguiente:

- » Analiza continuamente las bases de datos y los sistemas de archivo en busca de información confidencial
- » Establece prioridades en la mitigación de vulnerabilidades, con base en el nivel de restricción de la información y la gravedad de la exposición
- » Acelera el proceso de detección y revocación de derechos excesivos y de usuarios latentes

# SecureSphere Data Security Suite

---

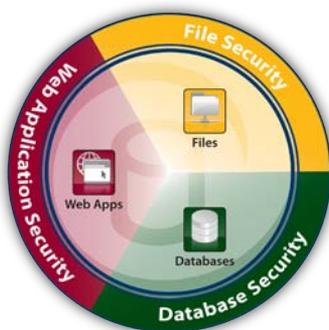
## Seguridad total de los recursos web, de las bases de datos y de los archivos

**SecureSphere Data Security Suite** es la solución líder del mercado en seguridad y conformidad. SecureSphere protege la información confidencial de los hackers y de personas mal intencionadas en el interior de las empresas, suministra una vía rápida y efectiva en cuanto a costos para el logro de la conformidad con las normas legales y de la industria, y establece un proceso repetible para el control de los riesgos de la información.

La base de la solución SecureSphere Data Security Suite es una plataforma común que suministra opciones flexibles de implementación, administración unificada, elementos profundos de análisis y la generación de informes a la medida. La plataforma SecureSphere habilita la escalabilidad a nivel empresarial u organizacional, y reduce el lapso de tiempo en obtener beneficios tangibles.

SecureSphere Data Security Suite hace lo siguiente:

- » Protege a las aplicaciones web de ataques de alta complejidad técnica y a gran escala a través de la Internet
- » Protege y hace auditorías del acceso a las bases de datos y a los archivos cruciales para las operaciones
- » Genera análisis forenses específicos, para una respuesta eficaz ante los incidentes
- » Reduce los riesgos de la información mediante la detección de la información confidencial, la mitigación de vulnerabilidades y la eliminación de los derechos y privilegios excesivos



## Ofrece diversos modos de implementación de los sistemas de información

A medida que la industria de la tecnología de informática se orienta hacia la nube, virtualización y la tercerización, para muchas organizaciones se ha hecho crucial un tercer requerimiento: cubrir un amplio rango de modelos de implementación. A fin de satisfacer dicho requerimiento, Imperva no sólo suministra productos empresariales tradicionales, sino también soluciones a gran escala para proveedores de servicios, infraestructura en la nube, así como opciones de productos y de servicios dirigidos a atender las necesidades de los mercados intermedios y de las pequeñas empresas.

# Seguridad de las bases de datos

---

Las soluciones SecureSphere Database Security protegen la información confidencial almacenada en las bases de datos. SecureSphere suministra una visibilidad total del uso de la información, de las vulnerabilidades y de los derechos de acceso. Permite a los profesionales de la seguridad, de la auditoría y del riesgo mejorar la seguridad de la información y satisfacer las normas legales y de la industria.



## Databases

SecureSphere hace lo siguiente:

- » Audita todos los accesos a la información confidencial, tanto de los usuarios de las aplicaciones como de los usuarios privilegiados
- » Alerta de o bloquea los ataques a las bases de datos y las solicitudes anormales de acceso, en tiempo real
- » Detecta y hace parches virtuales de las vulnerabilidades de bases de datos, basado en las investigaciones del centro ADC de Imperva – a fin de reducir su riesgo
- » Identifica los derechos de acceso excesivos a la información confidencial, y a los usuarios latentes
- » Agiliza la respuesta ante incidentes y las investigaciones forenses, mediante elementos avanzados de análisis

## SecureSphere Database Activity Monitoring (DAM)

Suministra el monitoreo, la auditoría y la generación de informes de manera automatizada y escalable, para entornos heterogéneos de bases de datos. SecureSphere contribuye a que las organizaciones puedan demostrar su conformidad con las normas legales y de la industria, a través de procesos, análisis y generación de informes, todo automáticamente. SecureSphere agiliza la respuesta ante incidentes y las investigaciones forenses, mediante la administración centralizada y elementos avanzados de análisis.

## SecureSphere Database Firewall (DBF)

Suministra protección en tiempo real contra las amenazas internas y los ataques externos, mediante alertas de o el bloqueo de los ataques y de las solicitudes anormales de acceso. SecureSphere hace parches virtuales a las vulnerabilidades en bases de datos, a fin de reducir los riesgos de exposición y el impacto de los prolongados ciclos de desarrollo de parches. DBF incluye las capacidades de auditoría y análisis que ofrece la solución DAM.

## User Rights Management for Databases (URMD)

Habilita la agregación y la inspección automática de los derechos de acceso de los usuarios. SecureSphere contribuye a la identificación de los usuarios con derechos excesivos y de los usuarios latentes, con base en el contexto organizacional y el uso real de la información. Mediante URMD, las organizaciones pueden demostrar su conformidad con normativas legales y de la industria tales como SOX, PCI 7 y PCI 8.5, y reducir el riesgo de violaciones de la información.

## SecureSphere Discovery and Assessment Server (DAS)

Suministra evaluaciones de vulnerabilidades y auditorías de configuración, que permiten a los usuarios medir la conformidad con los estándares de la industria y de las mejores prácticas. El descubrimiento de la información y su clasificación permite a las organizaciones determinar en forma precisa el alcance de los proyectos de seguridad y de conformidad. Mediante un análisis combinado de la información confidencial y de sus vulnerabilidades, SecureSphere contribuye a establecer prioridades y al mejor control de los esfuerzos de mitigación del riesgo.

# Seguridad de los archivos

---

Las soluciones SecureSphere File Security protegen a los archivos confidenciales almacenados en los servidores de archivos, en dispositivos de almacenamiento y en repositorios de contenido. SecureSphere suministra una visibilidad total de la posesión de la información, de su uso y derechos de acceso, y permite a los ejecutivos, auditores, gerentes de seguridad y gerentes de informática mejorar la seguridad de la información y satisfacer las normas legales y de la industria.



**Files**

SecureSphere hace lo siguiente:

- » Audita todos los accesos a los archivos confidenciales, tanto de los usuarios con privilegios como de los usuarios de las aplicaciones
- » Alerta de o bloquea las solicitudes de acceso a archivos en violación de las directivas corporativas
- » Identifica situaciones de derechos excesivos de acceso a archivos confidenciales, y habilita un ciclo total de aprobación de derechos
- » Agiliza la respuesta ante incidentes y las investigaciones forenses, mediante la administración centralizada y elementos avanzados de análisis

## SecureSphere File Activity Monitoring (FAM)

Suministra el monitoreo y la auditoría en tiempo real del acceso a archivos almacenados en servidores de archivos y en dispositivos de almacenamiento de conexión directa a redes (NAS). La auditoría de archivos de SecureSphere permite la generación flexible de alertas, de elementos de análisis y de informes, a fin de que los administradores puedan respaldar y comunicar las actividades de acceso a los principales interesados, y demostrar la conformidad con las normas legales y de la industria. FAM incluye la solución User Rights Management for Files para la auditoría de los derechos de acceso a archivos.

## SecureSphere File Firewall (FFW)

Impide el abuso por parte del personal interno y el acceso no autorizado a información en archivos confidenciales, y contribuye a garantizar la integridad de los archivos. SecureSphere monitorea las actividades de acceso, genera alertas con base en reglas definidas por el usuario y bloquea los accesos que violen las directivas empresariales. La administración centralizada, los elementos de análisis y los informes agilizan las investigaciones forenses y la respuesta ante incidentes de seguridad. FFW incluye la solución User Rights Management for Files para la auditoría de los derechos de acceso a archivos.

## SecureSphere User Rights Management for Files (URMF)

Identifica los derechos de acceso de los usuarios existentes y facilita ciclos totales de inspección de derechos. Las capacidades de SecureSphere de auditoría de los derechos de acceso a archivos garantizan que el acceso a la información de los archivos confidenciales sólo puedan hacerlo aquellos que tienen la necesidad operacional de conocer dicha información. SecureSphere facilita los ciclos de inspección de derechos mediante la creación de una línea base de los derechos existentes, la identificación de derechos excesivos y sin utilizar, y mediante el suministro de capacidades de flujo de trabajo a fin de especificar y comunicar los cambios entre todos los involucrados en el proceso de inspección. URMF es un componente de las soluciones FAM y FFW de SecureSphere.

# Seguridad de las aplicaciones web

---

Las soluciones SecureSphere Web Application Security protegen a las aplicaciones web de los ciberataques. SecureSphere se adapta continuamente a las amenazas en evolución, y permite a los profesionales de la seguridad, a los gerentes de redes y a los desarrolladores de aplicaciones el mitigar los riesgos de violaciones de la información, además de atender requerimientos claves de conformidad tales como PCI 6.6.



## Web Apps

SecureSphere hace lo siguiente:

- » Genera modelos de uso legítimo de las aplicaciones web
- » Alerta de o bloquea solicitudes de acceso que:
  - Se desvíen del uso normal de las aplicaciones y la información
  - Intenten aprovechar vulnerabilidades conocidas y desconocidas
  - Proviengan de fuentes malintencionadas
  - Violan las directivas corporativas
  - Sean parte de un ataque multi-capas de alto nivel tecnológico
- » Actualiza las defensas web con información proveniente de investigaciones relativas a las amenazas actuales
- » Hace parches virtuales a las vulnerabilidades de las aplicaciones mediante exploradores de vulnerabilidades de las aplicaciones web, a fin de reducir la ventana de exposición y el impacto de las correcciones ad-hoc de las aplicaciones

## SecureSphere Web Application Firewall (WAF)

La solución Web Application Firewall, líder del mercado, suministra protección automatizada contra ataques actuales a las aplicaciones, incluyendo las inyecciones SQL, XSS y CSRF. SecureSphere combina el aprendizaje automático de las aplicaciones con directivas de protección y firmas actualizadas, provenientes del centro ADC (Application Defense Center) de Imperva a fin de identificar y detener los ataques en forma precisa. Las reglas de correlación granulares, la seguridad con base en la reputación y una poderosa estructura de generación de informes completan la superior protección multicapa de SecureSphere. Con opciones de configuración multi-gigabit en línea y no en línea, SecureSphere ofrece implementación directa y un desempeño ultra alto, que satisface los requerimientos más exigentes de los centros de datos.

## ThreatRadar

ThreatRadar es un complemento de seguridad para la solución Web Application Firewall, que refuerza las defensas contra ataques automatizados a gran escala. ThreatRadar habilita la protección oportuna ante los riesgos del mundo real, contra fuentes conocidas de ataques tales como direcciones IP de origen de ataques malintencionados y contra URLs de phishing, a la vez que identifica la reputación de la fuente y la ubicación geográfica a efectos de análisis forenses. Al transmitir la información de fuentes de ataque casi en tiempo real a las soluciones WAF de SecureSphere, ThreatRadar puede detener en forma rápida y precisa a los usuarios malintencionados antes de que se puedan iniciar los ataques.

# Plataformas SecureSphere

---

La plataforma SecureSphere es la piedra angular de los galardonados productos de Imperva para la protección de la información. La plataforma SecureSphere incluye la administración centralizada y una estructura de generación de informes, opciones de suministro de máquinas virtuales y físicas y software de agentes de servidores que extienden la seguridad de la información a los sistemas host. La plataforma SecureSphere, gracias a sus opciones de su implementación flexible y las capacidades de administración, suministra a las empresas y organizaciones la implementación creciente según la necesidad, la adaptabilidad y el control necesario para implementar soluciones de la tecnología más avanzada para la protección de la información.

## Administración, elementos de análisis y reportes

El servidor SecureSphere MX Management Server puede controlar simultáneamente las soluciones SecureSphere de bases de datos, archivos y de seguridad web, desde una misma consola. El servidor SecureSphere MX Management Server es una plataforma de administración centralizada para múltiples gateways de SecureSphere. Suministra un punto único para la agregación de las directivas de seguridad, la administración jerárquica de la seguridad, el monitoreo en tiempo real, los registros, las auditorías y los informes de conformidad.

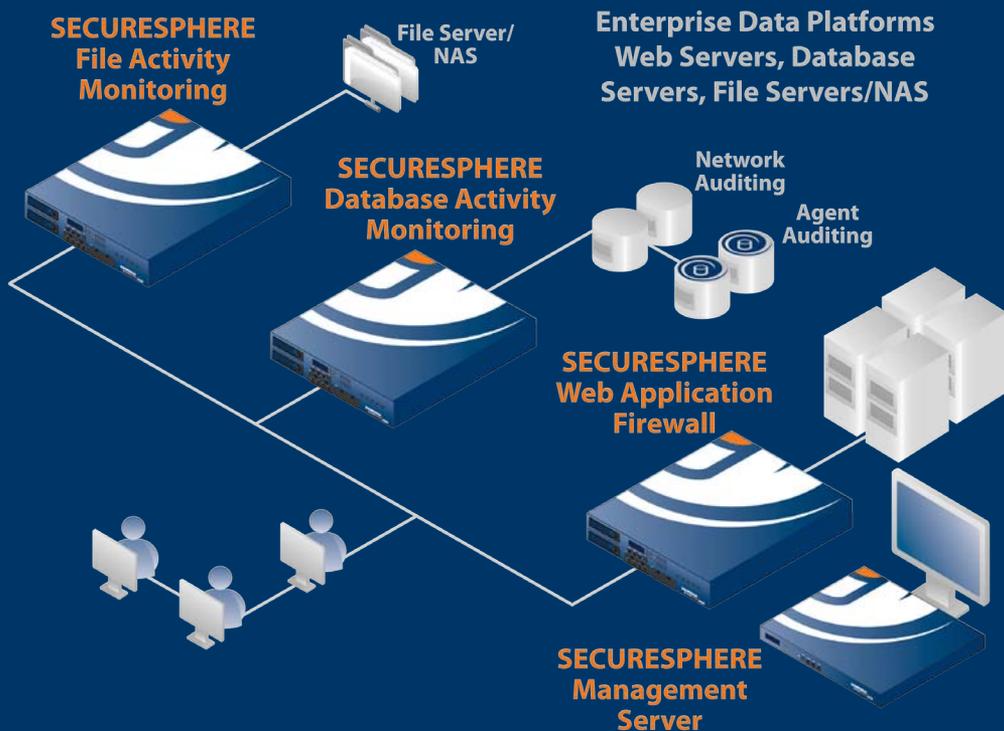
## Máquinas físicas y virtuales

Las máquinas físicas SecureSphere ofrecen un desempeño superior, escalabilidad y resistencia según la necesidad del entorno. Las interfaces 'fail open' de apertura en falla ofrecen soluciones de alta disponibilidad rápidas y efectivas en cuanto a costos. Las máquinas físicas SecureSphere ofrecen un desempeño superior, escalabilidad y resistencia según la necesidad del entorno. Las máquinas virtuales SecureSphere suministran toda la línea de productos de SecureSphere en una solución de software flexible y fácil de instalar. Las máquinas virtuales permiten a las organizaciones utilizar sus servidores existentes y reducir los costos de electricidad, enfriamiento y de soporte técnico.

## Agentes

Para una visibilidad de 360 grados de las actividades de los usuarios, SecureSphere extiende sus capacidades de monitoreo, auditoría y de cumplimiento a los servidores host. El agente SecureSphere de peso liviano se puede utilizar para hacer auditorías de la actividad de las bases de datos y proteger la información confidencial, con un impacto mínimo en el desempeño del servidor. Las comunicaciones del agente a la máquina SecureSphere se almacenan en un búfer y se cifran, a fin de prevenir la pérdida de información y los posibles riesgos. En caso de violaciones de la seguridad, los agentes SecureSphere pueden, como opción, bloquear la actividad de los usuarios y poner en cuarentena las cuentas de usuarios.

# Imperva SecureSphere Data Security Suite



*SecureSphere Data Security Suite es la solución líder del mercado en seguridad y conformidad. SecureSphere protege contra los hackers y personas mal intencionadas en el interior de las empresas a las aplicaciones web, a los archivos y a la información en las bases de datos. También suministra una vía rápida y efectiva en cuanto a costos para la conformidad con las normas legales y de la industria, y establece un proceso repetible para el control de los riesgos de la información.*



**Imperva**

3400 Bridge Parkway, Suite 200  
Redwood Shores, CA 94065  
Tel: +1-650-345-9000

[www.imperva.com](http://www.imperva.com)

© Copyright 2010, Imperva  
All rights reserved. Imperva, SecureSphere, and Protecting the Data That Drives Business are registered trademarks of Imperva. #ImpStory-LS-0910