IBM InfoSphere Guardium

Cómo administrar toda la seguridad de base de datos y el ciclo de vida del cumplimiento

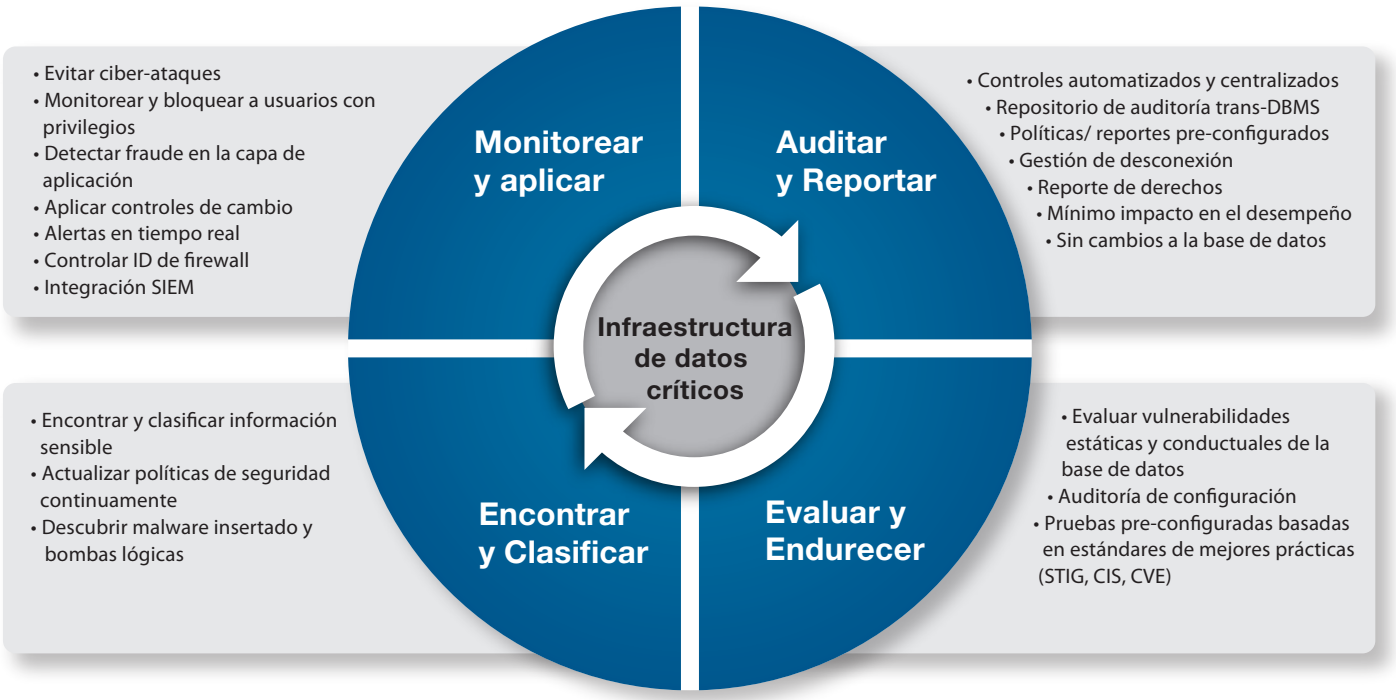
Organizaciones líderes de todo el mundo confían en IBM para que asegure su información empresarial crítica. El hecho es que proveemos una solución simple y robusta para salvaguardar una gran cantidad de sistemas empresariales usados para almacenar información financiera y de ERP, información sobre clientes y tarjeta-habientes, y propiedad intelectual.

Nuestra plataforma de seguridad empresarial evita actividades no autorizadas o sospechosas por parte de personas con privilegios de acceso a información confidencial y hackers potenciales. También monitorea el potencial de fraude por parte de usuarios de aplicaciones empresariales como Oracle, E-Business Suite, PeopleSoft, SAP y sistemas internos.

Al mismo tiempo, nuestra solución optimiza la eficiencia operativa con una arquitectura multi-capa, escalabe, que automatiza y centraliza los controles de cumplimiento a lo largo de toda la infraestructura de aplicaciones y base de datos.

Pero además de lo notable que resulta esta solución en lo que hace, resulta igualmente notable en cuanto a lo que no hace. Tiene un impacto mínimo en el desempeño, no requiere cambios a la base de datos y no se apoya en bitácoras de base de datos o funciones de auditoría nativas.

Seguridad y monitoreo de la base de datos en tiempo real



Solución unificada: Construida en una única y unificada consola y almacén de datos administrativos, InfoSphere Guardium ofrece una familia de módulos integrados para administrar toda la seguridad de la base de datos y el ciclo de vida de cumplimiento.

La solución de IBM® InfoSphere® Guardium® abarca toda la seguridad de base de datos y ciclo de vida de cumplimiento con una consola web unificada, almacenamiento de información administrativa y sistema de automatización de flujo de trabajo, que le permite:

- Encontrar y clasificar información sensible en bases de datos corporativas.
- Evaluar vulnerabilidades de la base de datos y defectos de configuración.
- Asegurar que las configuraciones queden integradas una vez implementados los cambios recomendados.
- Capturar y examinar todas las transacciones de bases de datos, incluyendo acceso local de usuarios con privilegios para todas las plataformas y protocolos soportados ‘ con un rastro de auditoría seguro, a prueba de manipulación, que soporte la separación de tareas.
- Realizar actividades de rastreo en las principales plataformas para compartir archivos.
- Monitorear y aplicar políticas de acceso a información sensible, acciones de usuarios privilegiados, control de cambio, actividades de usuarios de aplicaciones y excepciones de seguridad, como fallas en el registro.
- Automatizar todo el proceso de auditoría de cumplimiento ‘ incluyendo la distribución de reportes para supervisión de equipos, desconexión y escalamiento‘ con reportes pre-configurados para SOX, PCI Data Security Standard (DSS) y privacidad de información.
- Crear un repositorio único, centralizado para reporte de cumplimiento, optimización de reporte, investigaciones y rastros forenses a nivel de toda la empresa.
- Escalar fácilmente la protección de una sola base de datos a miles de ellas, en bases de datos y centros de datos distribuidos en todo el mundo.

Encontrar y clasificar

A medida que las organizaciones crean y mantienen un volumen de información digital cada vez mayor, les resulta más y más difícil ubicar y clasificar información sensible.

Localizar y clasificar información

Localizar y clasificar información sensible resulta especialmente difícil para las organizaciones que han atravesado fusiones y adquisiciones, o para ambientes donde los sistemas existentes han durado más que sus desarrolladores originales. Incluso en el mejor de los casos, los cambios continuos a estructuras de aplicación y base de datos ‘ necesarios para soportar los nuevos requerimientos del negocio ‘ pueden con facilidad invalidar políticas de seguridad y dejar información sensible desconocida y desprotegida.

A las organizaciones les resulta particularmente difícil:

- Mapear todos los servidores de base de datos que contienen información sensible y entender cómo se accede a ella desde todas las fuentes (aplicaciones de línea de negocios, procesos en lote, búsquedas ad-hoc, desarrolladores de aplicación, administradores y otros).
- Asegurar información y administrar el riesgo cuando se desconoce la sensibilidad de la información almacenada.
- Garantizar cumplimiento cuando no resulta claro qué información está sujeta a los términos de regulaciones particulares.

Automáticamente localizar, clasificar y asegurar información sensible

Con InfoSphere Guardium, puede utilizar la función de autodescubrimiento e información confidencial a la base de datos para identificar dónde se almacenan los datos y luego utilizar etiquetas de clasificación personalizables para automatizar la aplicación de políticas de seguridad aplicables a clases particulares de objetos sensibles. Estas políticas aseguran que la información sensible sea vista y cambiada sólo por usuarios autorizados. El descubrimiento de datos sensibles puede también programarse para que se ejecute regularmente y para prevenir la introducción de servidores rogue y asegurar que no se ’olvide÷ ninguna información crítica.

Evaluar y endurecer

Los ambientes para base de datos son altamente dinámicas, con cambios en cuentas, configuraciones y parches que ocurren regularmente. La mayoría de las organizaciones carecen de recursos capacitados para revisar cambios sistemáticamente y determinar si han introducido huecos en la seguridad.

Evaluación automática de configuración de vulnerabilidad y conductual

La capacidad de evaluación para la seguridad de bases de datos de InfoSphere Guardium escanea toda la infraestructura de base de datos en cuanto a vulnerabilidades y proporciona una evaluación constante de la postura de seguridad de su base de datos, usando información en tiempo real e histórica.

Proporciona una biblioteca extensa de pruebas pre-configuradas basadas en las mejor prácticas de la industria (CVE, CIS, STIG), junto con vulnerabilidades específicas a la plataforma, que son constantemente actualizadas por el servicio de Base de Conocimientos de InfoSphere Guardium. También puede definir pruebas a la medida para ajustarse a requisitos específicos. El módulo de evaluación señala vulnerabilidades relacionadas con el cumplimiento, como acceso no autorizado a tablas reservadas de Oracle E-Business Suite y SAP para cumplimiento con SOX y PCI DSS.

Las evaluaciones se agrupan en dos categorías amplias:

- Revisión de pruebas de vulnerabilidad y configuración para buscar vulnerabilidades como parches pendientes, privilegios mal configurados y cuentas predeterminadas.
- Las pruebas conductuales identifican vulnerabilidades con base en la manera que se accesan y manipulan las bases de datos ‘ como número excesivo de fallas de registro, clientes que ejecutan comando administrativos o conexión fuera de horario ‘ al monitorear todo el tráfico en la base de datos en tiempo real.

Además de producir reportes detallados, junto con datos de soporte, el módulo de evaluación genera una boleta de calificación de salud de seguridad. Esta boleta no sólo incluye métricas ponderadas basadas en mejores prácticas y cifras de referencia estándar de la industria, sino también recomienda planes de acción concretos para fortalecer la seguridad de la base de datos.

Integración de la configuración y rastreo de cambios

Después de implementar las acciones recomendadas en la evaluación de vulnerabilidad, puede establecer una línea de base de configuración segura. El Sistema de Auditoría de Configuración de InfoSphere Guardium puede monitorear los cambios a esta línea de base y asegurarse que no se hagan fuera de sus políticas y procesos de cambio autorizados.

Monitorear y aplicar

Las crecientes amenazas a información sensible, sumadas a ordenamientos de cumplimiento cada vez mayores, están llevando a las organizaciones a buscar medios efectivos para monitorear actividades de la base de datos a nivel de toda la empresa y evitar actividades no autorizadas en tiempo real.

Monitorear y aplicar políticas para la seguridad de bases de datos y control de cambio

InfoSphere Guardium proporciona políticas granulares, en tiempo real, para evitar acciones no autorizadas o sospechosas por parte de cuentas de base de datos con privilegios y ataques de usuarios rogue u otras personas externas. También puede identificar usuarios de aplicaciones que hagan cambios no autorizados a bases de datos con aplicaciones multi-capa que acceden a las bases de datos a través de una cuenta de servicio común, como Oracle E-Business Suite, PeopleSoft, Siebel, SAP, software IBM Cognos® y sistemas a la medida construidos en servidores de aplicaciones como Oracle WebLogic, Oracle AS y los de la familia WebSphere de IBM.

La solución puede administrarla el personal de seguridad sin involucrar a los administradores de las bases de datos (DBA).

También puede definir políticas de acceso detalladas que limiten el acceso a tablas específicas basadas en ingreso al sistema operativo, direcciones IP o MAC, aplicación de fuente, hora del día, protocolo de red y tipo de comando SQL.

Monitorear y aplicar políticas para la seguridad de bases de datos y control de cambio

InfoSphere Guardium monitorea continuamente todas las operaciones en la base de datos en tiempo real, usando análisis lingüístico para detectar acciones no autorizadas, basadas en información contextual detallada ”el ’quién, qué, dónde, cuándo y cómo÷ de cada transacción SQL. Este enfoque contextual minimiza los falsos positivos y negativos, al tiempo que proporciona un nivel significativo de control, a diferencia de los enfoques tradicionales que sólo buscan patrones o firmas predefinidos.

Monitorear y aplicar políticas para la seguridad de bases de datos y control de cambio

Al crear una línea de base e identificar procesos de negocios normales y lo que parecen ser actividades anormales, el sistema sugiere automáticamente políticas que puede usar para evitar ataques como inyección de código SQL. Los menús intuitivos facilitan la adición de políticas a la medida.

Seguridad proactiva en tiempo real

InfoSphere Guardium proporciona controles en tiempo real para responder a comportamientos no autorizados o anormales antes de que puedan causar un daño significativo.

Las acciones basadas en políticas pueden incluir alertas de seguridad en tiempo real (SMTP, SNMP, Syslog); bloqueo de Software; registro completo, cuarentenas de usuario y acciones a la medida, como cierre de los puertos VPN y coordinación con sistemas perimetrales IDS/IPS.

Rastreo y resolución de incidentes de seguridad

Las regulaciones de cumplimiento requieren que las organizaciones demuestren que todos los incidentes se registran, analizan y resuelven de manera oportuna y se reportan a la gerencia. InfoSphere Guardium proporciona una interfaz de usuario de negocios y automatización de flujo de trabajo para resolver incidentes de seguridad, junto con un tablero para rastrear métricas clave, como el número de incidentes abiertos, niveles de severidad y tiempo que dura abierto un incidente.

Auditoría y reporte

Volúmenes crecientes de datos, con frecuencia distribuidos físicamente a lo largo de una empresa, hacen cada vez más difícil que las organizaciones capten y analicen los rastros de auditoría requeridos para validar el cumplimiento.

Captar un rastro de auditoría granular

InfoSphere Guardium crea un rastro de auditoría continuo, detallado, de las actividades en la base de datos, el cual se analiza contextualmente y se filtra en tiempo real para implementar controles y producir la información específica que requieren los auditores.

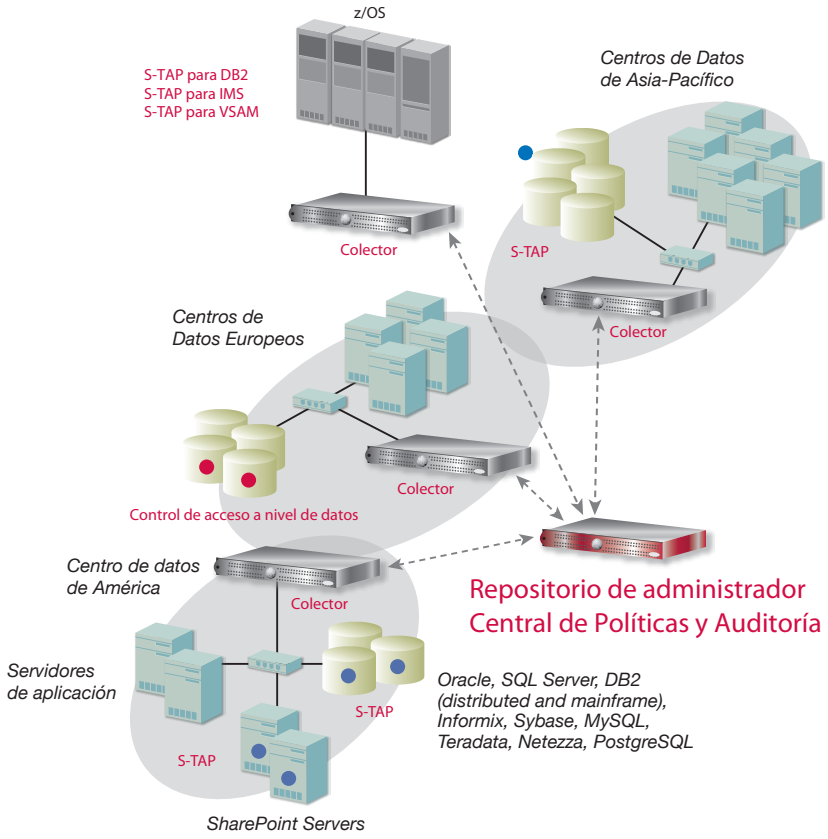
Los reportes resultantes demuestran cumplimiento, al posibilitar visibilidad en detalle las actividades de la base de datos como fallas de registro, escalamiento de privilegios, cambios de esquema, acceso fuera de horario o de aplicaciones no autorizadas y acceso a tablas sensibles. El sistema monitorea, por ejemplo:

- Excepciones de seguridad como errores SQL
- Comandos como CREAR/QUITAR/ALTERAR que cambian estructuras particularmente importantes para regulaciones de gobernabilidad de información como SOX
- Comandos SELECCIONAR/ LEER/ ABRIR, que resultan particularmente importantes para regulaciones sobre privacidad de información como PCI DSS
- Comandos de manipulación de datos (por ejemplo, INSERTAR, ACTUALIZAR, ELIMINAR) incluyendo variables de binding
- Comandos para lenguaje de control de datos que controlan cuentas, roles y permisos (OTORGAR, REVOCAR)
- Lenguajes de procedimiento soportados por cada plataforma DBMS como PL/SQL (Oracle) y SQL/PL (IBM)
- XML ejecutado por la base de datos
- Cambios a objetos Microsoft SharePoint

Escalabilidad a nivel de toda la empresa con costos minimizados

InfoSphere Guardium se escala con facilidad, usando funciones integradas de automatización e integración para reducir los costos operativos, al tiempo que se adaptan los cambios en requerimientos de auditoría y el ambiente. Independientemente del tamaño del sistema, InfoSphere Guardium simplifica las operaciones al proporcionar:

- **Una solución única.** Amplio soporte a la plataforma y amplia funcionalidad, incluyendo protección proactiva que permite el despliegue de una solución única a todo lo largo de la empresa.
- **Diseño no invasivo.** No se requieren cambios a la configuración de la base de datos, aplicación o red y no hay dependencia de registro nativo, lo que minimiza el impacto al desempeño.
- **Protección de la inversión.** A medida que crece el número de servidores que han de monitorearse, puede simplemente añadir capacidad para preservar las compras existentes de InfoSphere Guardium e inversiones de configuración como políticas y flujo de trabajo de cumplimiento.
- **Administración simple.** Se utiliza un solo interfaz para administrar dispositivos y detectores, incluyendo configuración, gestión de usuarios y actualizaciones de software. La interfaz única se utiliza para administrar dispositivos y detectores, incluyendo actualizaciones de configuración, gestión y software. Los detectores se actualizan sin reiniciarlos.
- **Análisis y reporte a nivel de toda la empresa.** La información de auditoría — de múltiples plataformas de bases de datos y colectores— se normaliza automáticamente y es agregada a un repositorio de auditoría único, seguro y centralizado con reporte y analítica avanzada.
- **Automatización de tareas.** En el sistema se incluyen capacidades que eliminan las tareas manuales, como automatización del flujo de trabajo para cumplimiento integrado, soporte API total para automatización basada en script, plantillas de configuración y auditoría, compartición de información automatizada entre funciones y más.
- **Flexibilidad de despliegue.** La entrega como dispositivos pre-configurados en forma de software y hardware soporta una amplia gama de estrategias de reducción de costos. Resulta posible soportar el monitoreo con detectores ligeros basados en web, sobre la red, o cualquier combinación, lo que maximiza la visibilidad.
- **Integración de infraestructura.** La interacción automática con sistemas, incluyendo LDAP, bases de datos administrativas, correo electrónico, etiquetado de cambio y Syslog, eliminan el intercambio manual de información de seguridad.



Una arquitectura multicapa escalable soporta ambientes grandes y pequeños, con agregación centralizada, normalización de datos de auditoría y gestión centralizada de políticas de seguridad a nivel de toda la empresa. Los S-TAP son detectores ligeros, basados en el host, que pueden monitorear el tráfico de la base de datos, incluyendo acceso local por parte de usuarios con privilegios, y transmitirlo a los dispositivos colectores de InfoSphere Guardium para análisis y reporte. Los dispositivos colectores reúnen información de monitoreo de los S-TAP o mediante la conexión directa con puertos SPAN en switches de red. Los agregadores ensamblan de manera automática la información de auditoría de múltiples dispositivos colectores. Múltiples capas de agregadores pueden configurarse para tener mayor flexibilidad y escalabilidad. Implementado como una extensión de S-TAP, el control de acceso a nivel de datos de InfoSphere Guardium refuerza la seguridad y aplica la separación de deberes al evitar que los administradores de las bases de datos puedan crear nuevas cuentas de bases de datos, elevar los privilegios para cuentas existentes y más.

El mejor reporte en su clase

La solución de InfoSphere Guardium incluye más de 150 políticas y reportes pre-configurados, basados en mejores prácticas y en nuestra experiencia trabajando con empresas de la lista Global 1000, importantes auditores y asesores en todo el mundo. Estos reportes ayudan a responder a requerimientos regulatorios como SOX, PCI DSS y leyes sobre privacidad de información, y ayudan a agilizar las iniciativas de gobernabilidad y privacidad de información.

Además de las plantillas de reporte pre-empaquetadas, InfoSphere Guardium proporciona un interfaz gráfico de arrastrar y soltar que permite construir nuevos reportes o modificar los reportes existentes con facilidad. Los reportes pueden enviarse automáticamente a los usuarios en formato PDF (como documentos adjuntos de correo electrónico) o como ligas a páginas HTML. También pueden verse en línea en la consola web o exportarse a SIEM y otros sistemas en formatos estándar.

Automatización del flujo de trabajo de cumplimiento

La aplicación para automatización del flujo de trabajo de cumplimiento de InfoSphere Guardium agiliza todo el proceso de flujo de trabajo de cumplimiento, ayudando a automatizar la generación de reportes de auditoría, distribución entre los principales interesados, aprobación y escalamiento electrónico. Los procesos de flujo de trabajo son completamente personalizables por cada usuario; es posible enrutar y rastrear hasta la aprobación puntos de auditoría específicos.

Soluciones unificadas para ambientes heterogéneos

La mayoría de las organizaciones tienen bases de datos de una variedad de proveedores, instaladas en una variedad de sistemas operativos, lo que dificulta la aplicación de políticas de seguridad y la recolección de información de auditoría consistente a nivel de toda la empresa. Los ambientes heterogéneos también pueden ocasionar que se tome un enfoque de silo hacia la seguridad y actividades de cumplimiento, elevando los costos de operación y consumiendo recursos escasos.

Amplio soporte a plataformas

Se soportan las principales plataformas DBMS y los protocolos que corren en la mayoría de los sistemas operativos, junto con una variedad creciente de ambientes para compartir archivos y documentos.

Plataforma soportada	Versiones soportadas
Oracle Database	8i, 9i, 10g (r1, r2), 11g, 11gr2
Oracle Database (ASO, SSL)	9i, 10g (r1, r2), 11g
Microsoft SQL Server	2000, 2005, 2008
Microsoft SharePoint	2007, 2010
IBM DB2® (Linux, UNIX, Linux for System z)	9.1, 9.5, 9.7
IBM DB2 (Windows)	9.1, 9.5, 9.7
IBM DB2 pureScale®	9.8
IBM DB2 for z/OS	8.1, 9.1, 10.1
IBM IMS™	9, 10, 11, 12
IBM VSAM	See OS support table
IBM DB2 for IBM iSeries®	V5R2, V5R3, V5R4, V6R1
IBM Informix®	7, 9, 10, 11,11.50, 11.7
Sun MySQL and MySQL Cluster	4.1, 5.0, 5.1
Sybase ASE	12, 15, 15.5
Sybase IQ	12.6, 12.7, 15
IBM Netezza®	NPS 4.5, 4.6, 4.6.8, 5.0, 6.0
PostgreSQL	8,9
Teradata	6.X, 12, 13, 13.10
FTP	

Monitoreo basado en host

Los S-TAP son detectores de software de peso ligero que monitorean los protocolos de red y base de datos locales (por ejemplo, memoria compartida, conexiones de software compartidas con nombre) en el nivel de sistema operativo del servidor de base de datos. Los S-TAP minimizan cualquier efecto en el desempeño del servidor, al apoyarse en la base de datos misma para procesar y almacenar los datos de bitácoras. Con frecuencia se prefieren los S-TAP porque eliminan la necesidad de dispositivos de hardware dedicados en ubicaciones remotas o puertos SPAN disponibles en su centro de datos

Tipo de OS	Versión	32-bit y 64-bit
IBM AIX®	5.2, 5.3,	Ambos
	6.1, 7.1	64-bit
HP-UX	11.11, 11.23, 11.31	Ambos
Red Hat Enterprise Linux	3, 4, 5	Ambos
Red Hat Enterprise Linux for System z	5.4	
SUSE Enterprise Linux	9, 10, 11	Ambos
SUSE Enterprise Linux for System z	9, 10, 11	
Solaris — SPARC	8, 9, 10, 11	Ambos
Solaris — Intel/AMD	10	Ambos
	11	64-bit
Tru64	5.1A, 5.1B	64-bit
Windows	2000, 2003, 2008	Ambos
iSeries	IBM i5/OS®*	
z/OS	1.10 (5694-A01) or later	

** Soporta monitoreo de actividad de red, soporte local de actividad con Enterprise Integrator*

Monitoreo de aplicaciones

InfoSphere Guardium identifica fraude potencial al rastrear actividades de usuarios que acceden a tablas críticas con aplicaciones empresariales multi-capa en lugar del acceso directo a la base de datos. Esto resulta necesario porque las aplicaciones empresariales típicamente utilizan un mecanismo de optimización llamado 'pooling de conexión÷. En un ambiente en pool, todo el tráfico de usuarios se agrega en unas pocas conexiones de bases de datos, que son identificadas sólo por un nombre de aplicación genérico, enmascarando de esta forma las identidades de los usuarios. InfoSphere Guardium soporta el monitoreo de aplicaciones para las principales aplicaciones listas para usarse. Se proporciona soporte para otras aplicaciones, incluidas las de desarrollo interno, mediante monitoreo de las transacciones a nivel del servidor de aplicaciones o estableciendo un interfaz con la alimentación universal de InfoSphere Guardium. IBM proporciona documentación sobre el protocolo de alimentación universal que permite a las organizaciones implementar un interfaz para soportar cualquier subconjunto de las funciones de monitoreo y protección soportadas por InfoSphere Guardium que resulten apropiadas para sus ambientes únicos.

Aplicaciones Empresariales soportadas	• Oracle E-Business Suite • PeopleSoft • Siebel • SAP • Cognos • Business Objects Web Intelligence
Plataformas de servidor de aplicaciones soportadas	• IBM WebSphere • BEA WebLogic • Oracle Application Server (AS) • JBoss Enterprise Application Platform

Sobre IBM InfoSphere Guardium

InfoSphere Guardium es parte de la plataforma integrada InfoSphere de IBM para definir, integrar, proteger y administrar información de confianza en sus sistemas. La Plataforma InfoSphere proporciona todos los bloques de construcciones fundamentales para la información de confianza, incluyendo integración de datos, almacenamiento de datos, gestión de información maestra y gobernabilidad de la información, todo ello integrado con un núcleo de metadatos y modelos compartidos. El portafolios es modular, por lo que se puede empezar desde cualquier punto y mezclar y compaginar los pilares de construcción del software InfoSphere con componentes de otros proveedores, o elegir desplegar múltiples bloques de construcción juntos para una mayor aceleración y valor. La plataforma InfoSphere es una base de clase empresarial para proyectos con uso intensivo de información, que proporciona el desempeño, escalabilidad, confiabilidad y aceleración necesarios para simplificar los retos difíciles y entregar información de confianza a su negocio con mayor rapidez.

IBM Corporation
Route 100
Somers, NY 10589

Producido en Los Estados Unidos de América
Agosto 2011

InfoSphere
software

IMD14286-CAEN-02