

Administrando el ciclo de Vida de la Seguridad de Bases de Datos y el Cumplimiento de Estándares

Más de 1000 organizaciones globales confían en Guardium para proteger la información más importante de su empresa. La realidad es que, nosotros proveemos la más simple y robusta solución para salvaguardar información financiera y del ERP, los datos del cliente y del tarjeta habiente, además de la propiedad intelectual almacenada en los sistemas de su empresa.

La plataforma de seguridad de nuestra empresa, previene actividades no autorizadas o sospechosas de usuarios privilegiados ó posibles piratas informáticos. También monitorea fraudes potenciales por usuarios finales de aplicaciones empresariales como: Oracle E-Business Suite, PeopleSoft, Business Objects y de sistemas hechos en casa.

Al mismo tiempo, nuestra solución optimiza la eficiencia operacional con una arquitectura escalable multi – tarea, que automatiza y centraliza el cumplimiento de controles a través de toda su aplicación y la infraestructura de la base de datos.

Pero tan notable es esta solución por lo que realiza, que por lo que no realiza. Tiene virtualmente cero impacto en el rendimiento, no requiere cambios en sus bases de datos, y no se basa en logs nativos de la base de datos o en utilidades de auditoría.



Solución Unificada

Construida sobre una sola consola unificada y con soporte de almacenamiento de datos, Guardium ofrece una familia de módulos integrados para manejar toda la seguridad de la base de datos y el cumplimiento del ciclo de vida.

Guardium 7 es la única solución que toma en cuenta toda la seguridad de la base de datos y el cumplimiento del ciclo de vida con una consola Web unificada y un sistema automático de flujo de trabajo, lo que le permite:

- **Localizar y clasificar información sensible** en las bases de Datos de toda una organización.
- **Evaluar las vulnerabilidades de la base de datos** y las fallas de configuración.
- **Asegurar que las configuraciones estén bloqueadas** después de que los cambios recomendados sean implementados.
- **Proveer 100% de visibilidad y granularidad a todas las** transacciones de la base de datos - a través de todas las plataformas y protocolos - con una pista de auditoría segura a prueba de manipulaciones que soporta la separación de funciones.

- **Supervisar y hacer cumplir las políticas** de acceso a datos sensibles, acciones privilegiadas de usuarios, control de cambios, actividades de aplicación de los usuarios y excepciones de seguridad como contraseñas fallidas.
- **Automatizar todo el proceso de cumplimiento de auditoría** -incluyendo los reportes de distribución a los equipos de supervisión, cancelaciones y escaladas - con reportes pre-configurados para SOX, PCI-DSS e información privada.
- **Crear un único y centralizado repositorio de auditoría**, para todos los reportes de, cumplimiento, optimización del rendimiento y de las investigaciones forenses.
- **Fácilmente escalable** para pasar de salvaguardar una sola base de datos a proteger miles de bases de datos en centros de datos distribuidos alrededor del mundo.

Descubrir y Clasificar

Automáticamente localiza, clasifica y asegura la información sensible.

En tanto las organizaciones crean y mantienen un aumento en el volumen de la información digital, cada vez es más complicado localizar y clasificar información sensible para ellas.

Esto es especialmente difícil para las organizaciones que han experimentado fusiones y adquisiciones, en ambientes en donde los sistemas heredados se han mantenido más en el tiempo que sus creadores originales. Hasta en el mejor de los casos, cambios actuales en las aplicaciones y en las estructuras de la base de datos - necesarias para apoyar los nuevos requerimientos empresariales - pueden fácilmente invalidar políticas de seguridad estáticas y dejar información sensible sin conocer o proteger.

Para las organizaciones es particularmente difícil:

- Encontrar todos los servidores de base de datos que contienen información sensible y comprender como está siendo accedida por todas las fuentes (aplicaciones empresariales, procesos por lotes, consultas ad hoc, desarrolladores de aplicaciones, administradores, etc.)
- Asegurar información y gestionar el riesgo cuando la sensibilidad de la información almacenada es desconocida.
- Garantizar el cumplimiento, cuando no está claro que la información está sujeta a los términos de un reglamento en particular.

Con Guardiüm, usted utiliza las herramientas de autodescubrimiento de una base de datos y las de clasificación de la información, para identificar donde están guardados los datos confidenciales, después utiliza las etiquetas de clasificación personalizada para automatizar la ejecución de políticas de seguridad que aplican a clases particulares de objetos sensibles. Estas políticas garantizan que la información sensible solo sea observada y/o cambiada por usuarios autorizados.

El descubrimiento de datos sensibles también puede ser programado para ejecutarse regularmente, en orden de prevenir la introducción de servidores no autorizados y asegurarse que la información crítica no sea "olvidada".

Evaluar y Reforzar

Vulnerabilidad, Configuración y Evaluación del Comportamiento

La evaluación de seguridad de base de datos Guardiüm, escanea toda la infraestructura de la base de datos para encontrar vulnerabilidades y proveer una evaluación continua del estado de seguridad de su base de datos, utilizando análisis en tiempo real y también histórico.

Provee una biblioteca amplia de exámenes pre configurados basados en las mejores prácticas de la industria así como vulnerabilidades específicas de cada plataforma, que son actualizados regularmente a través del servicio de suscripción de Guardiüm. Usted también puede definir exámenes personalizados para igualar requerimientos específicos. El modulo de evaluación también marca vulnerabilidades relacionadas con el cumplimiento, tales como acceso no autorizado a tablas reservadas de Oracle EBS y SAP para cumplimiento de SOX y PCI-DSS.

Las evaluaciones se agrupan en dos grandes categorías:

- Pruebas de vulnerabilidad y configuración para encontrar vulnerabilidades tales como: falta de parches, privilegios des configurados y cuentas por defecto.
- Pruebas de comportamiento identifican vulnerabilidades basadas en las maneras en las cuales las bases de datos están siendo accedidas y manipuladas - tales como un número excesivo de claves fallidas, clientes ejecutando comandos administrativos, acceso en horas no permitidas - esto monitoreando todo el tráfico de la base de datos en tiempo real.

Además de producir estos reportes detallados con facilidades de "drill-down", el módulo de evaluación genera un reporte de salud de la seguridad, con una ponderación métrica (basado en las mejores prácticas) y recomienda planes de acción concretos para fortalecer la seguridad de la base de datos.

Bloqueo de Configuración y Seguimiento de Cambios

Una vez que usted implementa las acciones recomendadas generadas por la evaluación de vulnerabilidad, usted puede establecer una línea de configuración de seguridad. Usando el sistema de auditoría de cambios Guardiüm (CAS en ingles), usted puede monitorear cualquier cambio a estas líneas de acción y asegurarse que estos cambios no son realizados afuera de sus políticas autorizadas de control de cambios y de los procesos.

Monitoreo y Cumplimiento

Monitoreo y políticas de seguridad para la base de datos y el control de cambios

Guardiüm provee políticas en tiempo real para prevenir acciones no autorizadas o sospechosas realizadas por cuentas privilegiadas de la base de datos así como ataques por parte de usuarios no autorizados o extraños al sistema.

Usted también puede identificar usuarios de aplicaciones que hacen cambios no autorizados a las bases de datos por medio de aplicaciones multi-tarea que acceden bases de datos a través de una cuenta de servicio común, tales como Oracle, EBS, PeopleSoft, Siebel, SAP y sistemas construidos por el usuario en servidores de aplicación como: IBM WebSphere, BEA WebLogic, y Oracle AS.

La solución puede ser administrada por el personal de seguridad de información sin necesidad de participación de los administradores de la base de datos (DBAs). Usted también puede definir políticas de acceso granular que restringen el acceso a tablas específicas basadas en claves de acceso del sistema operativo, direcciones IP o MAC, aplicaciones fuente, la hora del día, protocolo de red y el tipo de comando SQL.

Continúo análisis contextual de todo el tráfico de la base de datos

Guardium continuamente monitorea todas las operaciones de la base de datos en tiempo real, utilizando análisis lingüístico de patente pendiente para detectar acciones no autorizadas basadas en información contextual detallada - el "quién, qué, dónde, cuándo, dónde y cómo" de cada transacción SQL. Este enfoque único reduce los falsos positivos y negativos, al mismo tiempo proporciona un nivel sin precedentes de control, a diferencia de los enfoques tradicionales que sólo buscan las firmas o patrones predefinidos.

Creando una línea de referencia para la detección de anomalías de comportamiento y automatizar la definición de políticas

Mediante la creación de una línea de referencia e identificando los procesos normales de las empresas y lo que parecen ser actividades anormales, el sistema automáticamente sugiere políticas que pueden utilizar para prevenir ataques como inyección en los SQL. Políticas personalizadas pueden ser fácilmente añadidas a través de intuitivos menús desplegables.

Protección a tiempo real y proactiva

Guardium proporciona un arsenal de controles en tiempo real para responder proactivamente a comportamientos anómalos o no autorizados. Las acciones de protección pueden incluir: alertas de seguridad en tiempo real (SMTP, SNMP Syslog); bloqueo (a través de reseteo de TCP o por medio de técnicas de seguridad a nivel de datos en línea); permite la plena entrada en el sistema; y acciones personalizadas como cierres de cuentas automáticamente, cierres del puerto VPN y la coordinación con sistemas perimetrales IDS / IPS.

Buscando y resolviendo incidentes de seguridad

Regulaciones de cumplimiento requieren que las organizaciones demuestren que todos los incidentes son registrados, analizados, resueltos en poco tiempo y reportados a la gerencia. Guardium provee una interface a los usuarios de negocios y automatización de los flujos de trabajo para resolver incidentes de seguridad, además de un tablero gráfico para buscar elementos métricos o numerales tales como número de incidentes abiertos, nivel de gravedad, y la duración del tiempo que los incidentes han estado abiertos.

Auditar y Reportar.

Capturando Pistas de Auditoría Granular

Guardium crea pistas de auditoría de manera continuo y muy detallada de todas las actividades referentes a las bases de datos que son constantemente analizadas y filtradas en

tiempo real para implementar controles proactivos y producir la información específica requerida por los auditores.

Los resultados de los reportes demuestran el cumplimiento, suministrando una visibilidad detallada a todas las actividades de la base de datos tales como, claves erróneas, asignación de privilegios, cambios en el esquema, acceso en horas prohibidas o en aplicaciones no autorizadas y el acceso a tablas sensibles. Por ejemplo, el sistema monitorea:

- Excepciones de seguridad tales como errores SQL y contraseñas fallidas.
- Comandos DDL tales como Create/Drop/Alter Tables que cambian las estructuras de la base de datos, que son particularmente importantes para las regulaciones de la gestión de datos tales como SOX.
- SELECT queries, que son especialmente importantes para las regulaciones de privacidad de datos como PCI.
- Comandos DML (Insert, Update, Delete) incluyendo variables ocultas.
- Comandos DCL que controlan las cuentas, los roles y los permisos (GRANT, REVOKE).
- Lenguajes de procedimiento soportados por cada plataforma DBMS tales como PL / SQL (Oracle) y SQL / PL (IBM)
- XML ejecutados por la base de datos.

El mejor de su clase reportando

La solución Guardium incluye más de 100 políticas pre configuradas e informes basados en las mejores prácticas y nuestra experiencia de trabajo con más de 1,000 compañías globales, 4 grandes firmas de auditores y asesores de todo el mundo. Estos informes ayudan a abordar los requisitos normativos tales como SOX, PCI, las leyes de privacidad de datos y a racionalizar la gobernanza de datos e iniciativas de protección de datos.

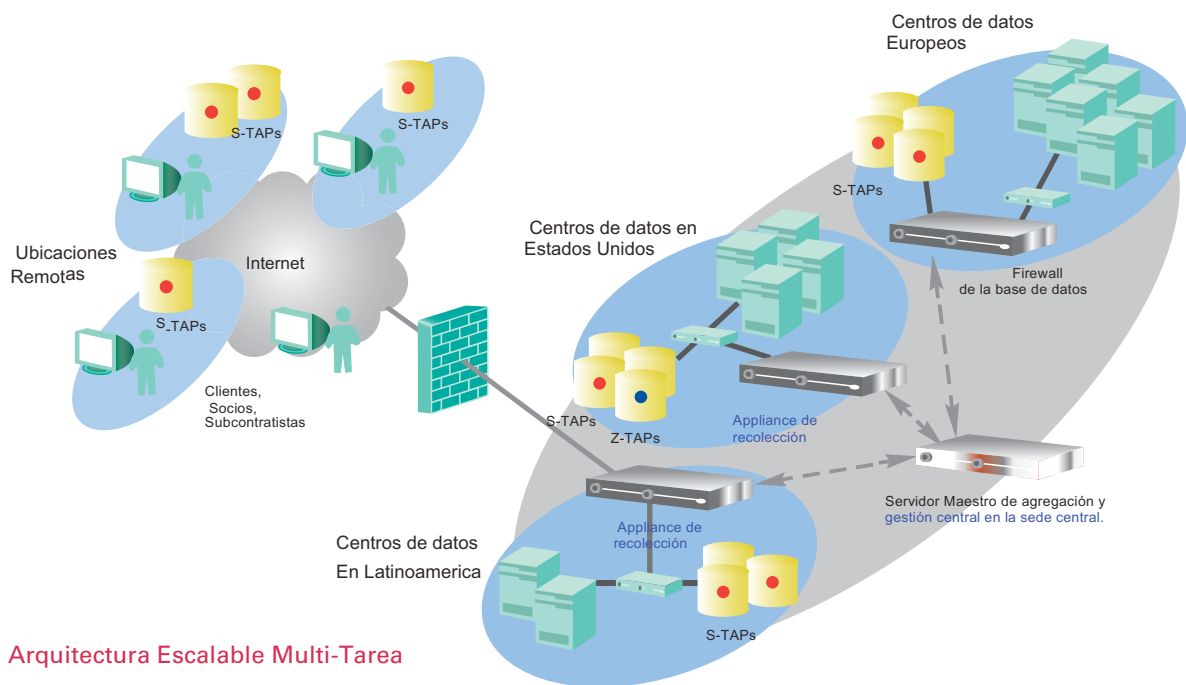
Además de las plantillas de informes pre-empaquetados, Guardium proporciona una interface de representación gráfica de "drag-and drop" para la creación sencilla de reportes o la modificación de reportes existentes. Los reportes pueden ser enviados inmediatamente por correo electrónico en formato PDF (como archivos adjuntos) o como enlaces a páginas HTML. También se pueden ver en línea a través de una interface Web, o exportados a SIEM u otros sistemas de formatos estándar.

Automatización del Flujo de Trabajo para el Cumplimiento

Única en la industria, la aplicación de Automatización del Flujo de Trabajo para el Cumplimiento Guardium, simplifica todo el cumplimiento del proceso de flujo de trabajo, ayudando a automatizar el proceso de generación de reportes de auditorías, la distribución a las principales partes interesadas, firmas electrónicas, y asignaciones de privilegios.

Escalable para Su empresa

- No invasiva: visibilidad del 100% en todas las transacciones de la base de datos - incluidos el acceso local por usuarios privilegiados - sin impacto en el rendimiento o cambios en la base de datos.
- Independiente al - DBMS: Solución Multi- plataforma que no se basa en la explotación de logs nativos de de las bases de datos.
- Basado en un dispositivo de hardware: conjunto de módulos de software, construido sobre un reforzado kernel Linux, para el despliegue rápido a través del dispositivo tipo "caja negra" o appliance (auto-almacenamiento, aplicaciones pre-instaladas, administración incorporada).
- Monitoreo flexible: Por medio de ligeros pulsos instalados en el servidor a monitorear, puertos SPAN, TAPs de red o cualquier combinación de los anteriores.
- Infraestructura Soportada: Soporta SNMP, Syslog, SMTP, LDAP Kerberos, RSA SecurID®, sistemas de control de cambios basados en tickets tales como BMC Remedy, CEF y la integración con todas las principales plataformas SIEM.
- Multi-tarea: Único en la industria, Guardium automáticamente agrega y normaliza la información para la auditoría - de múltiples sistemas y localidades - en un repositorio de auditoría único y centralizado.
- Gestión centralizada: Gestión de las políticas de seguridad en toda la empresa través de la consola Web.
- Escalable: Mientras que el número de seguimiento de los servidores o el volumen de tráfico aumenta, simplemente tiene que añadir más appliances para manejar el aumento de carga. Patentado, almacenamiento de algoritmos inteligentes que proporciona una eficiencia en almacenamiento 100 veces mayor al que proveen los tradicionales enfoques basados en archivos planos.
- Repositorio de Auditoría a Prueba de Falsificación: fuerte autenticación sin acceso a la cuenta root y archivos encriptados.
- Basada en Funciones: el acceso a los módulos y los datos se controla de acuerdo a las funciones de organización.



La arquitectura escalable Guardium soporta tanto ambientes pequeños como grandes y provee la información de auditoría, agregación centralizada y gestión centralizada de las políticas de seguridad, por medio de una consola Web - para toda la empresa.- Las S-TAPs son pulsos ultra livianos, basados en un servidor que monitorea todo el tráfico de la base de datos, incluido el acceso local por usuarios privilegiados, y transmiten esta información al dispositivo colector de información Guardium para su análisis y generación de reportes. Los dispositivos de recolección unen todos los datos que dan las S-TAPs y Z-TAPs (Z- TAPs son los agentes residentes en el mainframe) y / o mediante la conexión directa a los puertos SPAN en conmutadores de red. Los agregadores (Servidor Maestro de Agregación) automáticamente agregan la información de la auditoría de diferentes dispositivos de recolección. Para conseguir la máxima escalabilidad y flexibilidad, usted puede configurar múltiples niveles de agregadores.

Solución Unificada para Ambientes Heterogéneos

Soporte amplio para plataformas DBMS

La solución de multi-plataforma Guardium es compatible con la mayoría de DBMS plataformas y protocolos que funcionan en todos los sistemas operativos (Windows, UNIX, Linux, z/OS):

Plataformas Compatibles	Versiones compatibles
Oracle	8i, 9i, 10g, 11g
Servidor Microsoft SQL	2000, 2005, 2008
IBM DB2 UDB	8, 9
IBM DB2 for z/OS	78,
IBM Informix	7 8, 10, 11,
Sybase ASE	12, 15
Sybase IQ	12.6
My SQL	4, 5
Teradata	6

Monitoreo por Servidor

Único en la industria, los S-TAPs son pulsos de software ultralivianos que monitorean la red y los protocolos locales de la base de datos (shared memory, named pipes, etc.) al nivel del sistema operativo del servidor de la base de datos. Las S-TAPs minimizan cualquier efecto en el rendimiento del servidor mediante el relevo de todo el tráfico hacia los dispositivos Guardium separados para el análisis en tiempo real y reportes, en lugar de confiar en la misma base de datos para procesar y almacenar logs de datos. Las S-TAPs son usualmente preferidas porque eliminan la necesidad de dispositivos de hardware ubicados en lugares remotos o que están disponibles en los puertos SPAN de su centro de datos.

S-TAP Compatibles por OS	Versión
Windows	NT, 2000, 2003
Solaris - SPARC	6, 8, 9,10
Solaris - Intel/AMD	10
IBM AIX	5.1, 5.2, 5.3, 6.1
HP-UX	11.00, 11.11 11.23, 11.31 PA 11.23, 11.31 IA64
Red Hat Enterprise Linux	2, 3, 4, 5
SUSE Linux Enterprise	9, 10
Tru64	5.1A, 5.1B

Monitoreo de la Aplicación

Guardium identifica fraudes potenciales buscando posibles actividades de usuarios finales que acceden a la información tablas críticas a través de múltiples aplicaciones de la empresa asimismo que el acceso directo a la base de datos. Eso es requerido ya que las aplicaciones de la empresa usualmente utilizan un mecanismo de optimización llamado "agrupación de conexiones" (en inglés connection pooling). En un ambiente agrupado, todo el tráfico de usuarios es agregado dentro de unas pocas conexiones de usuario que son identificadas únicamente por un nombre de cuenta genérico para la aplicación, por lo que logra identificar y desenmascarar a los usuarios finales. Guardium soporta el monitoreo de aplicaciones para todas las mayores aplicaciones de software empresariales. Apoya a otras aplicaciones, incluyendo aplicaciones hechas en casa, es proporcionada por medio del monitoreo de las transacciones en el nivel de aplicaciones en el servidor.

Aplicaciones de empresas compatibles	<ul style="list-style-type: none">• Oracle E-Business Suite• PeopleSoft• Siebel• JD Edwards• SAP• Business Objects Web Intelligence
Aplicaciones de Plataformas de servicio compatibles	<ul style="list-style-type: none">• IBM WebSphere• BEA WebLogic• Oracle Application Server (AS)• Microsoft .NET• JBoss Enterprise Application Platform

Acerca de Guardium •

Guardium, la compañía de seguridad de base de datos, provee y ofrece la más amplia solución para garantizar la integridad de la información empresarial y prevenir fugas de información desde la central de datos.

La plataforma de seguridad esta ahora instalada en más de 350 centros de información en todo el mundo, incluyendo más de 60 compañías de "Global 500" y "Fortune 1000", pertenecientes a las más grandes industrias. Los clientes incluidos son 3 de los 4 más grandes bancos mundiales, una de las manufactureras más grandes de computadoras, una marca global de refrescos de soda, 3 líderes globales de venta minorista, una de las marcas mundiales más grandes de tarjetas de crédito, y un proveedor líder de software de inteligencia empresarial.

Guardium tiene alianzas con: Oracle, Microsoft, IBM, Sybase, BMC, EMC, RSA, Accenture, NetApp, McAfee, y NEON, con Cisco como un inversor estratégico, y es miembro del prestigioso Consejo de Administración de los Datos de IBM, y del Consejo de Estándares de Seguridad PCI.

Fundada en 2002, Guardium es la primera compañía en tomar en cuenta el núcleo de los vacíos en la seguridad de datos, suministrando una escalable plataforma para las empresas que protegen tanto la base de datos en tiempo real como la automatización de todo el proceso de auditoría.