

# Dispositivo Guardium – Colector

## Solución para la seguridad de bases de datos y el manejo de información.

### Destacados del producto

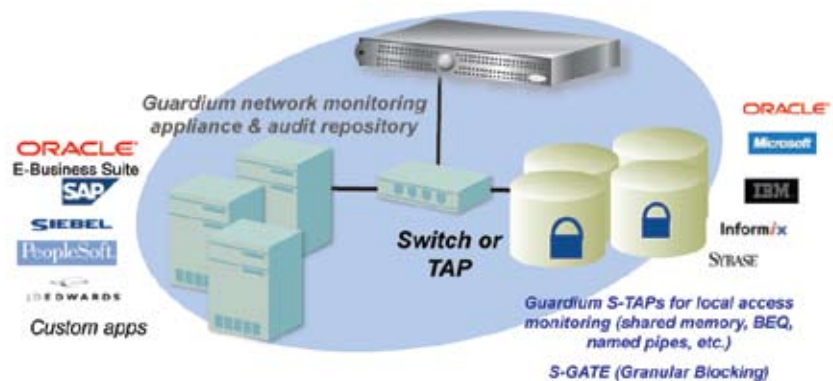
- Solución externa que protege bases de datos en tiempo real y automatiza el proceso total de auditoría de conformidad.
- Tecnología no invasiva, basada en dispositivos que pueden estar funcionando en solo unos minutos, con virtualmente ningún impacto en el rendimiento y desempeño, estabilidad u operaciones.
- Dispositivo fortalecido y construido sobre una plataforma de servidor de nivel industrial de alto rendimiento y gran disponibilidad.
- Solución de plataforma unificada diseñada para ambientes heterogéneos.
- Agente opcional de software liviano (S-TAP) instalado en los servidores de bases de datos para monitorear la red de trabajo y el tráfico local de datos al nivel del OS.
- De arquitectura fácilmente adaptable para responder a cualquier tipo de carga de trabajo y criterio de distribución de monitoreo

A diferencia de las soluciones de registro tradicionales, Guardium provee una solución residente en la red de trabajo que combina, de forma única, seguridad de bases de datos en tiempo real con un proceso totalmente automatizado de auditoría de conformidad. La solución Guardium es un enfoque basado en dispositivos que permiten a las organizaciones responder rápidamente a los requerimientos de los auditores, reducir conformidades, costos y proteger información crítica, sin impactar en aplicaciones, bases de datos o redes de trabajo.

Los dispositivos G1000 y G2000 de Guardium son unidades montables en estantes 1U fortalecidas construidas en una plataforma de servidor de alto rendimiento y nivel industrial. Estos sistemas independientes permiten monitorear, recolectar, informar y manejar todas las actividades de acceso a la base de datos eficientemente; así como el bloquear pasivamente de acceso no autorizado a la base de datos a través del reseteo de TCP. También permite una gama de opciones de despliegue de red: network hub, puerto SPAN, network TAP, y S-TAP (un agente de software liviano instalado en los servidores de base de datos).

El dispositivo inspecciona el flujo de información de manera no invasiva y permite el monitoreo de todas las actividades de acceso a la base de datos, con auditorías continuas e informando alertas en tiempo real y basadas en la política, así como con el bloqueo opcional de acceso no autorizado a la base de datos.

El sistema también monitorea el tráfico local privilegiado – como por ejemplo acceso a la consola SSL, memoria compartida y conductos nombrados – en el nivel del sistema operativo IPC a través de un S-TAP.



Con el fin de reforzar la discriminación de tareas y responsabilidades toda la información de auditoría es guardada en un depósito de almacenamiento interno al dispositivo de Guardium, de carácter seguro y a prueba de alteraciones. No hay acceso de raíz al dispositivo y toda la información de auditoría encriptada cuando es archivada en dispositivos de almacenamiento externos.

La arquitectura de Guardium puede ser adaptada fácilmente para responder a cualquier tipo de trabajo y criterio de monitoreo distribuido. En ambientes de centros de información corporativa, se pueden desplegar dispositivos múltiples en una topología de múltiples niveles. En este caso, un dispositivo central de operaciones – G5000 – agrupa y analiza la información de auditoría, distribuye informes y administra políticas de seguridad corporativa como un único sistema federado.

# Guardium Appliance Specifications (Guardium Version 7.0)

Descripción del Producto	Dispositivo para la auditoria continua y seguridad de base de datos en tiempo real		
Modo operacional	Monitoreo de acceso privilegiado, alerta y auditoria selectivas, auditoria exhaustiva		
Alertas	Mail, SNMP, SYSLOG, notificación de tipo JAVA, alertas de correlación en tiempo real		
Interfase de administración y setup	HTTPS, SSH, y consola		
Característica alta disponibilidad	Multi-LAN, almacenamiento interno protegido por hot-plug RAID1, alimentación hot-plug		
Plataformas de Base de datos admitidas	<b>Plataforma</b>	<b>Versión</b>	<b>Protocolo</b>
	DB2	8, 8.2, 9.1, 9.5	Network/TCP local, memoria compartida
		z/OS	CAF, RRSF, CICS, TSO, IMS, DRDA conectores distribuidos
	Informix	7,8,9,10,11	Network/TCP local, TLI, memoria compartida
	Oracle	8i,9i,10g (r1,r2), 11g,11i	Network/TCP local, Bequeath, IPC
		9i, 10g (r1,r2), 11g, 11i	ASO
	Servidor MS SQL	2000, 2005, 2008	Network/TCP local, Named Pipes, memoria compartida
	MySQL	4.1,5.0,5.1	Network/TCP local, Named Pipes
	Sybase ASE	12, 15	Network/TCP local, TLI
	Sybase IQ	12.6	Network/TCP local, TLI
Teradata	6.01, 6.02	Network TCP (no S-TAP)	
Plataforma OS Admitida (S-TAP)	<b>OS</b>	<b>Versión</b>	<b>32-Bit o 64-Bit</b>
	AIX	5.1, 5.2, 5.3, 6.1	Ambos
	HP-UX	11.00, 11.11, 11.31	Ambos
		11.23 PA	32-Bit
		11.23 IA64	64-Bit
	Red Hat Enterprise Linux	2, 3, 4, 5	Ambos
	Solaris- Sparc	6, 8, 9, 10	Ambos
	SUSE Linux Enterprise	9, 10	Ambos
	Tru64	5.1A, 5.1B	64-Bit
Windows	NT, 2000, 2003	Ambos	
Módulos de Software (opcional)	<b>Modulo</b>	<b>Descripción</b>	
	Aceleradores	Para SOX, PCI y conformidades de privacidad de información	
	Soporte y aplicaciones	Auditoria/monitoreo de usuarios para Oracle EBS, PeopleSoft, SAP R/3, Siebel, y Business Objects	
	Facilitadores de extensión de archivo	Archivo para EMC Centere, y operador de almacenamiento IBM Trivoli	
	Operación central	Crea un sistema federado para el manejo de políticas centrales y la recolección de información y reportes de auditoria	
	Sistema de cambio de auditoria (CAS)	Monitorea cambios a la base de datos y los objetos de configuración de OS del servidor	
	Automatización de conformidades de flujo de trabajo	Agrupa y distribuye resultados de procesos de auditoria con características de escalado y cierre	
	Clasificador de contenido de base de datos (DBCC)	Identifica el lugar de almacenamiento de información sensible, la clasifica y categoriza, y define políticas basadas en resultados automáticamente.	
	Conector de información externa	Integra información de origen externo dentro de reportes y políticas Guardium	
	Monitor de acceso de información no estructurada	Tiene la habilidad de monitorear protocolos de FTP y File Share de Windows	
Evaluación de vulnerabilidad	Autodescubre bases de datos, muestra mapas de acceso de cliente-servidor, evalúa riesgos de configuración y comportamiento, el servicio adicional de suscripción provee actualizaciones frecuentes para vulnerabilidades recientemente descubiertas.		
<b>Hardware</b>	<b>G1000</b>	<b>G2000</b>	
Form Factor	1U, Dell-PE860	1U, Dell-PE1950	
CPU	1 procesador dual core Xenon 3050, 1066MHz FSB	2 procesadores dual core Xenon 5140, cache de 4MB, 2.33GHz, 1333MHz FSB	
Memoria	2GB, 667MHz	4GB, 667MHz	
Tipos de interface network	Cobre/fibra, hasta 6 puertos	Tarjeta de puerto dual Gigabit Ethernet con posibilidad de bypass	
Velocidad de network	10/100/1000Mbps	10/100/1000Mbps	
Almacenamiento interno	Dos 164GB, SAS, 10K RPM de 3.5 pulgadas, RAID1	Dos 164GB, SAS, 10K RPM de 3.5 pulgadas, RAID1	
Alimentación	345 watts simple, 110/220 volts no redundante	670 watts dual, 110/220 volts, redundante, hot-plug, auto encendido	