

Guardium Aggregator Enterprise.

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

Destacados del producto

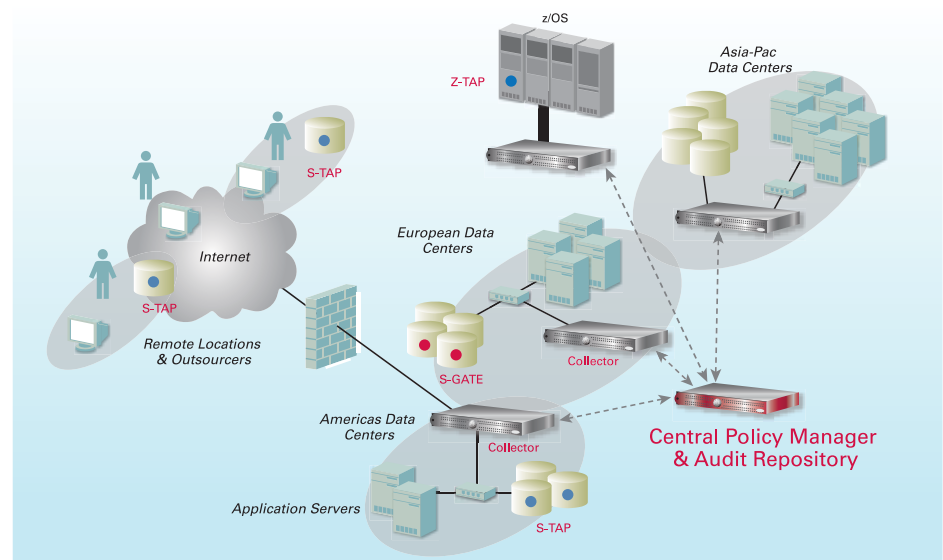
- Agrupador: produce reportes de datos en su conjunto de alcance corporativo.
- Gerenciador central: maneja todos los dispositivos federados desde una única consola.
- Solución externa que protege bases de datos en tiempo real y automatiza el proceso total de auditoría de conformidad.
- Tecnología no 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.

Única en la industria, la arquitectura de niveles múltiples de Guardium agrupa y normaliza información de auditoría - de múltiples sistemas y orígenes - en un depósito central y único. Esto facilita los reportes de conformidad a nivel corporativo, la correlación, asuntos forenses y análisis de carácter avanzado focalizados en las bases de datos.

El G5000 es el agrupador Guardium. Recauda información de lugares múltiples. Con el G5000 el cliente puede obtener reportes en conjunto a nivel corporativo. Además, los agrupadores pueden ser utilizados en una arquitectura de escalones múltiples en la cual la información puede ser sustraída de agrupadores de escalones medios.

Un agrupador puede ser seteado, como lo es en muchos casos, como un operador central para manejar todos los dispositivos Guardium desde un solo punto de acceso. Una consola gráfica Web provee el manejo centralizado de políticas, definiciones de reporte, procesos de conformidad de flujo de trabajo, seteo de dispositivos (como por ejemplo programación de archivado), y la aplicación de parches o la mejora (o upgrade) de productos en el sistema federado.



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 la auditoría es encriptada cuando es archivada en dispositivos de almacenamiento externos, o exportada a un agrupador. De manera similar, todas las comunicaciones entre componentes federados son encriptadas.

Guardium Aggregator. Especificaciones del dispositivo (Guardium 7.0)

Descripción del Producto	Dispositivo fortalecido para el monitoreo de información corporativa	
Modo operacional	Servidor recolector, programable como unidad de operación central	
Alertas	Mail, SNMP, SYSLOG, notificación JAVA customizada, alertas de correlacion	
Interfase de administración y setup	HTTPS, SSH, y consola	
Características alta disponibilidad	Multi-LAN, almacenamiento interno protegido hot-plug RAID-1	
Modos de Software (opcional)	Modulo	Descripción
	Aceleradores	Para SOX, PCI y conformidades de privacidad de información
	Soporte de aplicaciones	Auditoria/monitoreo de usuario 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	Agrupar 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 Protege S-TAP (S-GATE)	Integra información de origen externo dentro de reportes y políticas Guardium Provee protección con firewall a través de S-TAP tanto para la red como para los conectores locales
	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.	
Hardware G5000	Componente	Descripción
	Factor de Forma	1U, Dell-PE1950
	CPU	Dos procesadores dual core Xeon 5420, cache de 2x6MB, 2.5GHz, 1333MHz FSB PE1950
	Memoria	4GB, 667MHz
	Interface de red	Gigabit Ethernet NIC de doble puerto
	Almacenamiento interno	Dos 400GB, SAS, 3.5 pulgadas 10K RPM, Hot Plug, RAID-1
	Alimentación	670Watt dual, 110/220 Volt, redundante, hot-plug, autoencendido

¹ Esta aplicación solo es para los colectores. Sin embargo, puede ser instalada en el recolector si este es también operador y su licencia es transferida al colector operado.