

Soluciones de Ciberseguridad

Garantiza la integridad y confidencialidad de la información

Configuración y gestión de IBM Guardium Data Protection for Databases

IBM Guardium es una solución de seguridad que ayuda a garantizar la integridad y la confidencialidad de la información de nuestros clientes.

El sistema proporciona un descubrimiento y clasificación automatizada de datos sensibles, supervisión de la actividad de los datos en tiempo real y analítica cognitiva para descubrir actividad poco habitual en torno a datos sensibles.



Protege ante accesos no autorizados a datos aprendiendo los patrones de acceso regular de usuario y proporciona alertas en tiempo real sobre actividades sospechosas.



Bloquea dinámicamente el acceso o pone en cuarentena ID de usuario para proteger ante amenazas internas y externas, además de agilizar y automatizar flujos de trabajo de conformidad.



Se basa en una arquitectura escalable que proporciona visibilidad completa sobre la actividad de los datos en entornos heterogéneos.

Todas las ventajas de Guardium, sin su complejidad.

El equipo de Nologin instala, configura y gestiona toda la solución, y exprimiendo al máximo la funcionalidad, y reduciendo su complejidad en tiempo y costes, gracias a su equipo de técnicos especializados en el producto.

Cumple y supera auditorías

Recibe informes periódicos y alertas a tiempo real del estado de la información y las brechas de seguridad. Además, estos informes son totalmente personalizables, por lo que se pueden generar para que contengan datos técnicos y, por ende, sean revisados por el departamento IT o para ayudar al departamento de Compliance a cumplir con las auditorías pertinentes.



Cree un repositorio para todos los datos

Centralice los datos de auditoría en un repositorio normalizado, para garantizar la conformidad empresarial, los informes y la investigación. Proteja los datos sensibles en entornos heterogéneos

Beneficios de Guardium Gestionado por Nologin

- ▶ Cumple y supera auditorías de GDPR
- ▶ Reducción de la complejidad de la solución
- ▶ No es necesario operar sistemas complejos ni formar al equipo
- ▶ Se transforman costes CAPEX a OPEX
- ▶ Se reduce el pasivo laboral
- ▶ Reducción del tiempo de resolución de incidencias
- ▶ Predictibilidad de costes
- ▶ Evolución del sistema garantizada

“Lo más atractivo de un Guardium gestionado por un grupo especializado, es la economía de conocimiento que genera. Con nuestro equipo de expertos el despliegue es mucho más rápido y ante cualquier incidente que se produzca ya conocemos la solución. Eso, en un equipo interno, llevaría semanas resolverlo.”

Fases del proyecto

El uso de esta solución se basa en la configuración de herramientas que, en su conjunto, permiten securizar aquellos datos de negocio que se consideren sensibles. La configuración se realiza en varias fases:

1. Inicio del proyecto: Toma de requisitos

Toma de requisitos para poder integrarnos en su infraestructura actual.

2. Definición de dato sensible y donde se almacena

Esta fase pretende definir qué datos sensibles son los que han de protegerse y dónde se encuentran almacenados. Es decir, Guardium inspecciona la información de las bases de datos configuradas en base a una lógica preestablecida. Esta lógica puede definirse según requisitos de negocio o puede ser configurada utilizando modelos de datos que Guardium provee, como por ejemplo datos sensibles en PCI o en GDPR.

3. Configuración de reglas de Seguridad

Una vez la información sensible es localizada, es necesario configurar reglas de seguridad para proteger los accesos y evitar así fugas de información o corrupción de datos. Estas reglas de seguridad permiten establecer alertas en tiempo real, reescritura de sentencias SQL o denegación de acceso a datos sensibles entre otros.

4. Almacenamiento y explotación de la información

Toda la información recogida por estas reglas de seguridad se almacena en Guardium con el fin de poder revisarla si sucede algún incidente de seguridad. Para esta tarea, Guardium permite la generación de informes con una amplia gama de consultas. También se pueden configurar informes periódicos o Dashboards para la monitorización a tiempo real.

Impacto mínimo en el rendimiento

La integración de Guardium en los entornos ya existentes tiene un impacto mínimo a nivel de rendimiento debido a que su arquitectura solamente contempla el despliegue de un pequeño agente en las bases de datos a securizar, dejando la mayor parte de la lógica de producto en appliances dedicados.



Céntrese en su negocio, de la seguridad nos encargamos nosotros

Despreocúpese de la seguridad, sabiendo que tiene la infraestructura en manos de expertos.



Nologin ESPAÑA Avda. de Ranillas 1D, Of.3G, 50018 Zaragoza, España.
(+34) 976 512 433 | www.nologin.es.

Si se encuentra fuera de España, puede encontrar información de la oficina más cercana en nuestro sitio web.

Sobre Nologin:

Nologin es una compañía dinámica con un alto grado de conocimiento en el entorno de las Tecnologías de la Información, que ofrece a sus clientes servicios y soluciones de calidad para definir, implantar y administrar sus Sistemas Informáticos y de Comunicaciones.

