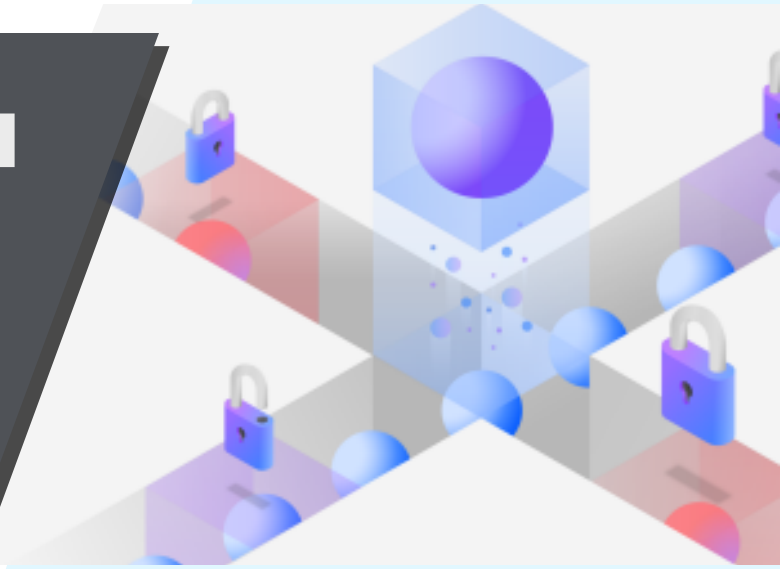
OptimaTech

Guardium Data Protection

Wide visibility, compliance and protection throughout the data security lifecycle



Solution overview

IBM Guardium Data Protection provides comprehensive visibility and control over your sensitive data across on-premises, cloud, and hybrid environments. It helps organizations enforce data security policies, monitor database activities in real time, and respond swiftly to potential threats. With robust integration capabilities, Guardium ensures compliance with industry regulations and helps safeguard critical information from unauthorized access and breaches.

Cost of Data Breach

US4.88M

The global average cost of a data breach in 2024—a 10% increase over 2023 and the highest total ever.

292 days

Breaches involving stolen or compromised credentials took the longest to identify and contain (292 days) of any attack vector.

1 in 3

Share of breaches that involved shadow data, showing the proliferation of data is making it harder to track and safeguard.

Benefits

50%

Discover

When using Guardium, the average client's accuracy of data classification improved by 50%.

43%

Protect

Guardium increased the ability to detect threats with accuracy on average by 43%.

67%

Analyze

Investigate anomalies to understand what activities are creating risk, better uncover data source vulnerabilities by 67%.

42%

Respond

The time spent on identifying and remediating data security issues decreased 42% in the area of data threat response.

89%

Comply

Simplify compliance tasks, clients are spending less time to prepare for an audit by 89%. In person-hours, that's 1,250 hours down to 478 hours.

(*Source: Ponemon Report: client Insights on Data Protection with IBM Security Guardium, Ponemon Institute)

Features

Discover and classify sensitive data across on-premises and cloud environments

- Automatically discover databases or import assets manually. Define & map applications to their data sources
- 100+ data discovery patterns help to identify regulated data in your environment

Comply with regulations and simplify auditing and reporting through automation

- Automate tracking and reporting for regulatory compliances with pre-built templates for a quick start
- Track progress towards compliance on all selected regulations from a single interface
- Accelerate audit activities and confirm separation of duties through a continuous, fine-grained audit trail

Protect sensitive assets with data activity monitoring

- Define rule-based policies to monitor, log, report & alert on unauthorized data access
- Customize or use predefined policy templates to meet your audit & compliance requirements
- Variety of agent-based and agentless options to protect data on-premises & in the cloud

Respond to threats in real-time

- Quickly uncover and respond to suspicious user activity and external threats by blocking or quarantining suspicious users in real-time
- Initiate remediation of security gaps by integrating with security operations solutions to close the loop on exposures

Analyze and harden your environments for vulnerabilities

- Proactively scan for vulnerabilities across heterogenous platforms using more than 3000 assessments
- Investigate user risk details to determine the “Who?” , “What?”, “When?”, and “Where?” of an event with threat analytics

Supported Data Sources

Databases

The solution supports data on IBM Db2®, Oracle, Teradata, Sybase, Microsoft® SQL Server, Windows®, UNIX®, Linux®, AS/400 and z/OS®, and Hadoop NoSQL. It also supports key enterprise resource planning, CRP and custom applications.

Files

Provides automated discovery and classification of unstructured data in files and file systems, including NAS, SharePoint, Windows, Unix and Linux, to help you better understand and control unstructured data risks.

DBaaS

Provides automated data discovery and classification, near real-time activity monitoring, and machine learning analytics to sensitive data stored in database-as-a-service (DBaaS) platforms and cloud-native platforms, such as IBM Cloud Pak for Data, including AWS RDS and Azure Database-Platform-as-a-Service.

Big Data

It accelerates compliance workflows through a prebuilt regulation template and supports both Hadoop and NoSQL environments. Provides full visibility on data activity, detecting unusual activity around sensitive data with near real-time data monitoring and machine learning analytics.

Use Cases

Data protection across the hybrid cloud

Secure sensitive data by discovering, classifying, and protecting it in real-time with features like dynamic masking, redaction, quarantining and blocking. It offers centralized control for both modern and legacy systems, allows policy management from one location, and enforces least privileged access to ensure data is only accessed on a need-to-know basis.

Simplify compliance

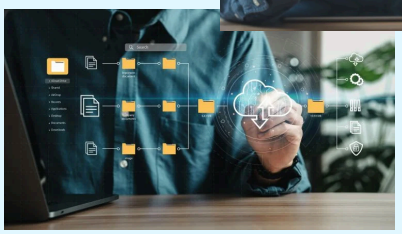
Offering preinstalled and customizable policies, streamlined audits, and quick reporting. It provides predefined templates for policies and reports to help meet regulations like PCI DSS, GDPR, and CCPA efficiently.

Find and respond to threats faster

Enables rapid threat response by blocking access and redacting data in real time, opening tickets, and integrating with other security tools. It offers detailed, AI-powered risk views for investigating threats like SQL injection and data leakage, with click-through and drill-down features for deeper analysis.

Flexible database monitoring

Offers scalable, flexible database monitoring for both structured and unstructured data across public clouds, data warehouses, and SaaS apps. Provides full visibility into data activity with options for at-source monitoring via Guardium agents and non-sensitive data monitoring through Universal Connector plug-ins, simplifying integration with modern cloud environments.



+64 9 889 889 0 www.OptimaTech.co.nz info@OptimaTech.co.nz