Why Guardium?

- Flexibly monitor data across a hybrid multicloud environment with passive and active monitoring delivered via containerized agents
- Adapt to a changing data landscape with scalable architecture
- Identify vulnerabilities and threats with advanced analytics then share data across other critical security teams and tools
- Orchestrate a response to data threats and take immediate action against risky users
- Discover and classify sensitive data wherever it lives
- Centralize data security visibility and policy enforcement
- Leverage prebuilt templates to track progress against various compliance regulations to meet data security standards

Product overview

IBM Security Guardium Data Protection complements and extends native security controls on AWS, discovering and classifying sensitive data, monitoring and securing your entire data landscape, and leveraging analytics to identify and understand how to respond to threats and vulnerabilities.

Product features

**Discover and classify sensitive data**

Sensitive data discovery span critical aspects of enterprise security:

- Discovery: locate the sensitive data that exists anywhere in your environment
- Protection: monitor and alert when sensitive data is accessed, and use automated password provisioning via integration with Amazon Secrets Manager
- Compliance: create audit trails to review the results of sensitive data discovery processes

**Data activity monitoring across the hybrid cloud**

Provide a scalable platform that enables continuous monitoring of structured and unstructured data traffic, allowing the:

- Enforcement of policies around sensitive data access
- Automation of the entire compliance auditing process, including creating and distributing reports
- Ingestion of audit log data from Amazon Kinesis and Amazon CloudWatch to monitor across multiple AWS data sources

**Identify and respond to threats and vulnerabilities**

Analyze hardware and user vulnerabilities and risks then take immediate action:

- Proactively scan for vulnerabilities with more than 3000 assessment tests
- Identify risks with analytics and share risk data with other security tools to orchestrate a response
How it works

Guardium takes a continuous approach to help organizations achieve data security and compliance across on-premises and AWS environments. Through integration with AWS Secrets Manager for cloud security automation and ingestion of audit/log data with Amazon Kinesis and Amazon CloudWatch, Guardium can centralize monitoring and data security visibility across a widely-distributed AWS environment such as AWS RDS, AWS Aurora and AWS S3 data sources housing both structured and unstructured data. This helps to extend AWS’ data security capabilities by consolidating and analyzing logs to quickly address compliance concerns, audit requests, or to uncover anomalous activity.

Differentiators

• **End-to-end data security platform that tackles discovery, classification, data protection, and monitoring.** This helps to deliver a comprehensive platform that not only identifies where sensitive data lives but protects it by proactively monitoring user activity and enforcing security policy aligned to compliance goals.

• **Robust data security threat intelligence and response.** Guardium Data Protection delivers extensive risk and vulnerability identification and analysis capabilities helping organizations to uncover potential security threats and streamline the remediation process.

• **Easy integration with multiple security tools from ticketing platforms to incident response, to support a holistic data security strategy.** Data security is everyone’s business, and Guardium helps to break down siloes by sharing critical data security data with other key tools and systems, keeping the security organization informed and ready to quickly address changes to data security, compliance, or response to an audit.
**What our customers are saying**

"IBM Security Guardium helped the interviewed organization gain visibility into its data environment, enabling it to identify potential internal and external threats and reducing the likelihood of a breach by 40%." **Energy and Utilities Company, The Total Economic Impact Of IBM Security Guardium**

---

**Data Points**

- $1.1m Saved by streamlining compliance
- 1000 Hours saved annually by automating database analysis

---

**Additional Resources**

- [Guardium Data Protection Interactive Demo](#)
- [Guardium Data Protection Website](#)

---

Solution available in [AWS Marketplace](#)