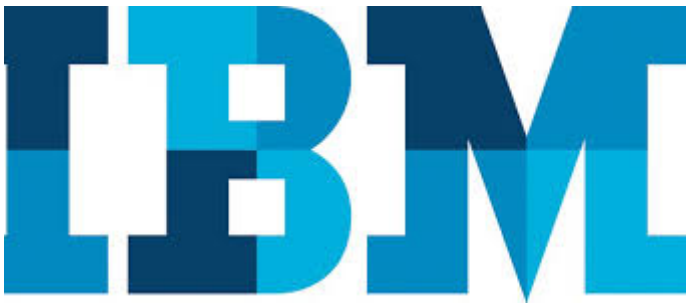

IBM Guardium prevents leaks from databases, data warehouses and Big Data environments such as Hadoop, ensures the integrity of information and automates compliance controls across heterogeneous environments.
It protects structured and unstructured data in databases, big data environments and file systems against threats and ensures compliance.
It provides a scalable platform that enables continuous monitoring of structured and unstructured data traffic as well as enforcement of policies for sensitive data access enterprise-wide.

A secure, centralized audit repository combined with an integrated workflow automation platform streamlines compliance validation activities across a wide variety of mandates.
It leverages integration with IT management and other security management solutions to provide comprehensive data protection across the enterprise.
They are intended to enable continuous monitoring of heterogeneous database and document-sharing infrastructures, as well as enforcement of your policies for sensitive data access across the enterprise, utilizing a scalable platform. A centralized audit repository designed to maximize security, combined with an integrated compliance workflow automation application, enables the products to streamline compliance validation activities across a wide variety of mandates.

IBM Security Guardium is designed to help safeguard critical data. Guardium is a comprehensive data protection platform that enables security teams to automatically analyze what is happening in sensitive-data environments (databases, data warehouses, big data platforms, cloud environments, files systems, and so on) to help minimize risk, protect sensitive data from internal and external threats, and seamlessly adapt to IT changes that may impact data security. Guardium helps ensure the integrity of information in data centers and automate compliance controls.

The IBM Security Guardium solution is offered in two versions:

- IBM Security Guardium Database Activity Monitoring (DAM)
- IBM Security Guardium File Activity Monitoring (FAM) - Use Guardium file activity monitoring to extend monitoring capabilities to file servers.
  The IBM Guardium products provide a simple, robust solution for preventing data leaks from databases and files, helping to ensure the integrity of information in the data center and automating compliance controls.
  Guardium products can help you:
- Automatically locate databases and discover and classify sensitive information within them;
- Automatically assess database vulnerabilities and configuration flaws;
- Ensure that configurations are locked down after recommended changes are implemented;

- Enable high visibility at a granular level into database transactions that involve sensitive data;
- Track activities of end users who access data indirectly through enterprise applications;
- Monitor and enforce a wide range of policies, including sensitive data access, database change control, and privileged user actions;
- Create a single, secure centralized audit repository for large numbers of heterogeneous systems and databases; and
- Automate the entire compliance auditing process, including creating and distributing reports as well as capturing comments and signatures.

  The Guardium solution is designed for ease of use and scalability. It can be configured for a single database or thousands of heterogeneous databases located across the enterprise.

  This solution is available as preconfigured appliances shipped by IBM® or as software appliances installed on your platform. Optional features can easily be added to your system after installation.

  These are the key functional areas of Guardium's database security solution:
- Vulnerability assessment. This includes not just discovering known vulnerabilities in database products, but also providing complete visibility into complex database infrastructures, detecting misconfigurations, and assessing and mitigating these risks.
- Data discovery and classification. Although classification alone does not provide any protection, it serves as a crucial first step toward defining proper security policies for different data depending on its criticality and compliance requirements.
- Data protection. Guardium addresses data encryption at rest and in transit, static and dynamic data masking, and other technologies for protecting data integrity and confidentiality.
- Monitoring and analytics. This includes monitoring of database performance characteristics and complete visibility in all access and administrative actions for each instance. On top of that, advanced real-time analytics, anomaly detection and security information and event management (SIEM) integration can be provided.
- Threat prevention. This refers to methods of protection from cyberattacks such as distributed denial-of-service (DDoS) or SQL injection, mitigation of unpatched vulnerabilities and other database-specific security measures.
- Access management. This goes beyond basic access controls to database instances. The rating process focused on more sophisticated, dynamic, policy-based access management capable of identifying and removing excessive user privileges, managing shared and service accounts, and detecting and blocking suspicious user activities.
- Audit and compliance. This includes advanced auditing mechanisms beyond native capabilities, centralized auditing and reporting across multiple database environments, enforcing separation of duties, and tools supporting forensic analysis and compliance audits.
- Performance and scalability. Although not a security feature per se, it is a crucial requirement for all database security solutions to be able to withstand high loads, minimize performance overhead and support deployments in high-availability configurations.