Security
Data Sheet

IBM Security Guardium Data Protection for Databases

Continuously monitor data access and protect sensitive data across the enterprise

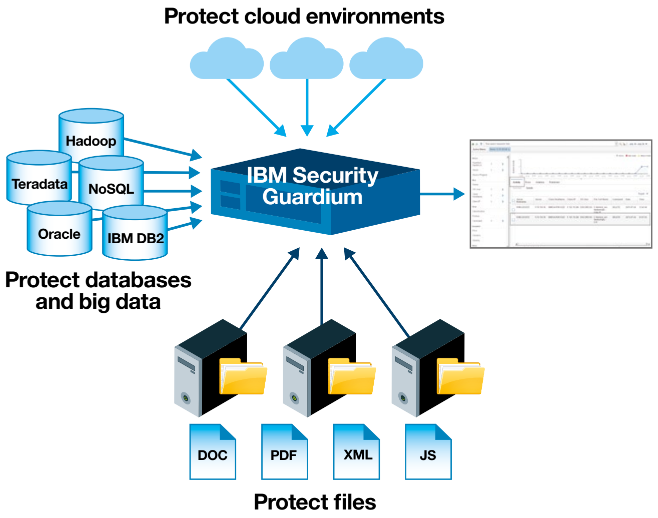
Highlights

- Uncover risks to sensitive data through data discovery, classification and privileged access discovery to automatically take action or report for compliance
- Reduce data breach risk and extend security intelligence with in-depth data protection
- Provide a streamlined and adaptable solution for real-time monitoring access to high-value databases, data warehouses, files, cloud and big-data environments
- Minimize total cost of ownership with robust scalability, simplification, automation, analytics and transparency for a range of deployments—whether they are small, large or enterprise-wide

IBM® Security Guardium® Data Protection for Databases and Big Data environments (Guardium Data Protection) empowers security teams to analyze, protect and adapt for comprehensive data protection in heterogeneous environments, including databases, data warehouses, files, file shares, cloud, and big-data platforms such as Hadoop and NoSQL.

The solution continuously monitors all data access operations in real time to detect unauthorized actions, based on detailed contextual information—the “who, what, where, when and how” of each data access. Guardium Data Protection reacts immediately to help prevent unauthorized or suspicious activities by privileged insiders and potential hackers. It automates data security governance controls in heterogeneous enterprises.

Guardium Data Protection improves security and supports compliance requirements through a set of core capabilities that help reduce risk and minimize cost of ownership.



Guardium Data Protection for Databases and Big Data platforms provides comprehensive protection. It makes it easy to see which databases and big-data platforms contain sensitive data, monitor data access, and take action to help protect against internal and external threats.

Risk reduction

For any given organizational action or activity, there is the potential risk of sensitive data exposure or loss. The probability or threat of damage, liability or data loss caused by external or internal vulnerability can be avoided through quick response or preemptive action. Guardium Data Protection reduces data breach risk by providing real-time data security and intelligence with features such as:

- **Automatic identification of risky data or configurations**—Uses data discovery, classification, entitlement reports and audit records to identify data at risk, such as dormant sensitive data or outdated entitlements and over-privileges to data.
- **Real-time data activity monitoring with application end-user translation**
  - Provides 100 percent visibility and granularity into all database, files, file share, data warehouse, Hadoop and NoSQL transactions across all platforms and protocols—with a secure, tamper-proof audit trail that supports segregation of duties.
  - Monitors and enforces a wide range of policies for sensitive-data access, privileged-user actions, change control, application-user activities and security exceptions.
  - Monitors all data transactions to create a continuous, fine-grained audit trail of all data sources that identifies the “who, what, when, where and how” of each transaction, including execution of all SQL commands on all database objects.
  - Audits all logins/logouts, security exceptions such as login failures and SQL errors and extrusion detection (identifying sensitive data returned by queries).
  - Creates a single, centralized audit repository for enterprise-wide compliance reporting, performance optimization, investigations and forensics.
- **Real-time security alerts**—Creates alerts in real time when a security policy is violated—including alerts to enterprise-wide security information and event management (SIEM) systems. IBM Security QRadar® provides bidirectional communications to Guardium, so you can take immediate action.
- **Real-time data masking (via the Guardium S-GATE agent)**—Helps ensure that critical data does not fall into the wrong hands. Guardium Data Protection for Databases looks at the data content leaving the data sources and obfuscates non-authorized fields according to the requestor privileges.

- **Real-time blocking (via S-GATE), including user quarantine and firewall IDs**
  - Establishes preventive controls across the enterprise. Guardium Data Protection provides automated, real-time controls that help prevent privileged users from performing unauthorized actions such as executing queries on sensitive tables, changing sensitive data values, adding or deleting critical tables (schema changes) outside the change management process, and creating new user accounts and modifying privileges.
  - Reacts to suspicious activity by blocking activity or quarantining the requestor.
  - 6.6.15 Implements firewall IDs that allow specified users to access certain servers for a particular time period to accommodate certain activities such as maintenance windows without affecting database security configurations.
- **Custom report builder with drill-down capabilities**—Customizes and filters security reports to display the parameters that are relevant to your organization. Some common reports include: SQL errors, failed logins, terminated users and policy violations.
- **Best-practice recommendations in predefined reports and alerts**—Provides a variety of predefined reports with different views of entitlement data, enabling organizations to quickly and easily identify security risks such as inappropriately exposed objects, users with excessive rights and unauthorized administrative actions. Examples of the numerous predefined reports include: system, administrator and object privileges with SQL-level detail drill-downs by user and all objects. Entitlement information is stored in a forensically secure and tamper-proof repository, along with all data source audit information. Custom reports can be easily built by using an intuitive drag-and-drop interface.

Streamlined graphical user interface provides centralized control

IT organizations today are under high pressure to maximize the use of their resources and time. Low-level security operations or manual processes are wasteful, risky and error-prone. As your business data needs grow, the scope of the data security and compliance projects increases. You need security solutions to become more streamlined and adaptable as your needs change. In the era of big data, Guardium Data Protection provides key capabilities to help organizations streamline and adapt data protection and security management without impacting data sources, networks, or applications, such as:

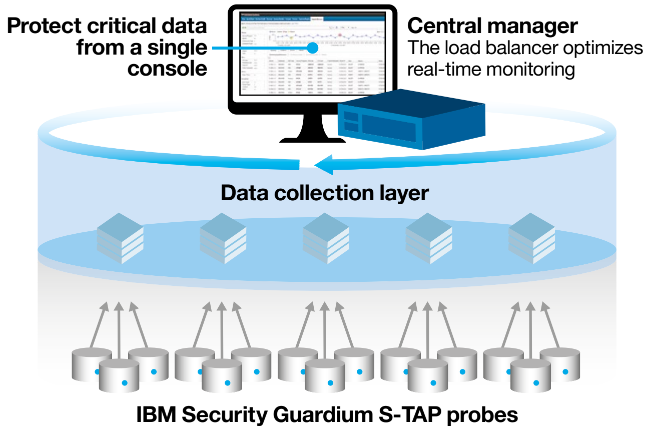
- **Dynamic graphical user interface (GUI) helps build and update data and user groups**—Maximizes the protection delivered by Guardium. With one click, groups, policies, tests and other configurable parameters can be updated to adapt to the constantly evolving nature of the IT environment, database infrastructure and associated threats. Automated group management is used in audit reports, alerts and real-time policies to facilitate maintenance—despite constant changes in the IT environment. Whitelists or blacklists can be 6.6.15 generated on any auditable item, for example, users, IP addresses, table names and so forth. Group maintenance can be done manually through the GUI or automated with Lightweight Directory Access Protocol (LDAP) integration. Groups can be populated using queries or GuardAPIs. You can synchronize with user groups in Microsoft Active Directory, IBM Security Directory Server, Novell, OpenLDAP, Sun ONE, IBM z/OS® and more. Handling policies, reporting and auditing indirectly through groups helps to keep a consistent management process, despite the constant change in the environment.

- **Centralized management automates the deployment of Guardium**—Provides centralized management through a single web-based console. The scalable multi-tier architecture supports large and small environments with built-in health-check dashboards. Software updates are handled centrally and automatically without having to involve the change management team or resource owners.
- **Database discovery, data classification and entitlement reports**—Discovers and classifies sensitive data. The discovery process can be configured through the Guardium GUI to probe specified network segments on a schedule or on demand. Once instances of interest are identified, the content is examined to identify and classify sensitive data. Entitlement reports provide an automatic risk assessment on who is configured to access the sensitive data.
- **Powerful analytic insights**—Enables organizations to centrally visualize and analyze data activity from a heterogeneous data environment using a single format. The Guardium GUI includes leading-edge analytic tools—such as connection profiling, Quick Search real-time forensics, outlier detection algorithms and an investigative dashboard—that provide actionable insights on data access behavior.
- **Predefined security policies**—Allows you to create and manage your own data security policies based on audit data or leverage out-of-the-box predefined policies. The policies can be built to detect any threat scenario against the data utilizing the most common audit constructs such as who, from where, when, where to, on what, what action and other contextual information. Examples of security policies include:
  - Access policies that identify anomalous behavior by continuously comparing all data activity to a baseline of normal behavior. An example of anomalous behavior would be an SQL injection attack, which typically exhibits patterns of data access that are uncharacteristic of standard line-of-business applications.
  - Exception policies that are based on definable thresholds, such as an excessive number of failed logins or SQL errors.
  - Extrusion policies that examine data leaving the data repository for specific data value patterns, such as credit card numbers.
- **Guardium GUI has customizable compliance workflows with preset compliance accelerators for common compliance requirements**—Centralizes and automates oversight processes enterprise-wide, including report generation, distribution, electronic sign-offs and escalations. It creates custom processes without sacrificing security. It ensures that some team members see only data and tasks related to their own roles and stores process results in a secure centralized repository. It supports compliance with Sarbanes-Oxley (SOX), Payment Card Industry (PCI), Health Insurance Portability and Accountability Act (HIPAA) and other regulations with predefined reports. An easy-to-use GUI allows a wide variety of processes to be created to match the unique needs of the tasks and individuals involved. Reports can be exported in varying formats, including PDF, comma-separated values (CSV), common event format (CEF), Syslog forwarding, Security Content Automation Protocol (SCAP) or custom schemas.
- **Secure and self-sustained platform through the Guardium GUI**—Audits all operations, including administration and configuration tasks, to maintain compliance controls, segregation of duties, and compliance with the latest security mandates and Federal Information Processing Standards (FIPS) 140-2.

Performance

Business moves fast and clients demand continual access to data. As a result, IT environments with diverse databases, transactional applications, analytics platforms, file systems and emerging big-data applications are required to meet aggressive service level agreements for availability, performance and responsiveness. Compliance requirements need to be addressed and security strategies implemented without impacting performance. Guardium Data Protection can be implemented with negligible performance impact—less than 1 percent overhead in most cases—using key capabilities, such as:

- **An operating system-based agent**—Provides full visibility of data traffic without affecting the performance of the data source or application, as in the case of native audit logging.
- **Filtering of database traffic**—Avoids unnecessary database audit traffic by monitoring only what is required, such as the data traffic already going from the operating system to the data source, and sending it out of band for analysis.
- **Centralized load balancing for multi-tier architecture**—Enables Guardium agents (STAPs) to be automatically distributed, so they can automatically find the most optimal configuration to send their data activity traffic.
- **Support for 64-bit architecture**—Provides the ability to handle and store more data traffic data with fewer resources.


Protect critical data from a single console
Central manager
The load balancer optimizes real-time monitoring
Data collection layer
IBM Security Guardium S-TAP probes

With automated load balancing, Guardium Data Protection for Databases enables organizations to easily adapt to IT changes that affect data security.

Scalability

Driven by a rapidly changing business landscape that includes mergers, outsourcing, cloud deployments, workforce adjustments and accelerating business automation, data sources continue to proliferate over geographical and organizational boundaries. In addition, data is growing in terms of volume, variety and velocity, and it now resides in new types of data stores, such as Hadoop and NoSQL databases. Given current IT resource constraints, the complexity of environments and escalating workloads, many organizations want to increase automation in their data security and compliance operations.

Guardium Data Protection is equipped to seamlessly scale from one data source to tens of thousands without disrupting operations. Automation capabilities include:

- **Guardium Grid automates adaptation to changes in the data**—Automatically balances the load and handles changes or additions to the environment without impacting the performance or availability of the data monitoring infrastructure. Guardium Data Protection dynamically adds or drops data sources without altering configurations. Guardium Grid provides elasticity for supporting large deployments in frequent change. Load balancing scalability and performance features help clients reduce management costs, minimize the need to manage detailed configuration information (IP addresses or hostnames) as data sources are added or removed, and simplify data capacity expansion projects.
- **GuardAPI support for batch operations**—Facilitates integration of any IT process with Guardium Data Protection. GuardAPI is a script-based command-line interface (CLI) to Guardium, which allows any operation to be performed remotely.
- **Centralized aggregation**—Merges and normalizes audit reports from multiple data sources to produce enterprise-wide reports and a forensics source.
- **Centralized management**—Controls operations and policy setting from a central location, including hands-off agent updates, policy control, Guardium environment health and load balancing.

Integration

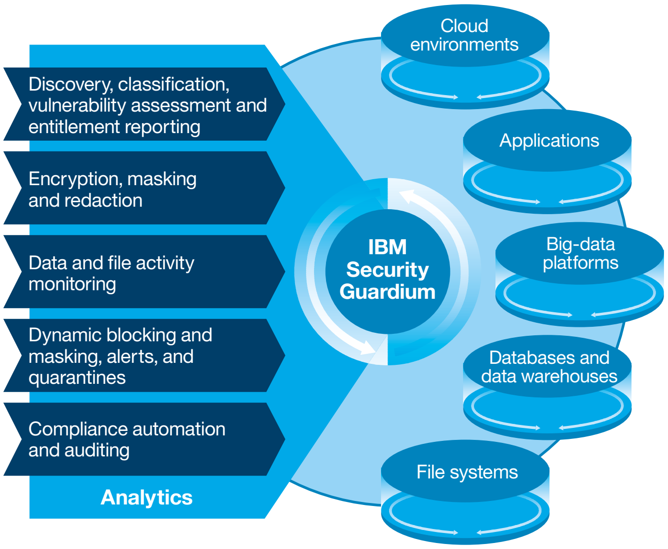
Most organizations have a diverse set of IT and security solutions in place today, such as ticketing systems or SIEM solutions. All of these solutions eventually require interaction with data security. Most existing security solutions lack the complete visibility into data access patterns required by regulatory mandates. Guardium Data Protection for Databases provides analytics-based, in-depth insight while seamlessly integrating into existing security solutions, such as QRadar or ArcSight. In addition, Guardium Data Protection for Databases provides a modular integration model with existing IT systems, such as data management, ticketing and archiving solutions.

The goal is to streamline IT and security operations by complementing and extending them with data security capabilities, including:

- **Integration with IT operations**—Guardium Data Protection includes built-in, ready-to-use support for Oracle, IBM DB2®, Sybase, Microsoft SQL Server, IBM Informix®, mySQL, Teradata, IBM PureSystems®, Hadoop, IBM InfoSphere® BigInsights™, PostgreSQL, NoSQL, MongoDB, SAP HANA and more across all major protocols, including: HTTP, HTTPS, FTP, SAMBA and IBM iSeries connections to CSV text file data sources. It can also seamlessly share information with common IT operations tools, such as ticketing systems, where Guardium tracks ticket IDs within data access audit records.
- **Integration with security systems and standards (QRadar, HP ArcSight, Radius, LDAP)**—Changes to users, groups, roles and authentication to data sources and applications can be updated automatically and directly from directories such as LDAP, Radius and Active Directory. Organizations can automatically handle any staff or user changes while keeping the policies and reports intact, avoiding the need to constantly modify them. In addition, IT staff can send alerts and all audit information to a SIEM. QRadar users experience bidirectional integration, allowing QRadar to issue alerts and change policies for immediate data protection.
- **Guardium Universal Feed and Enterprise Integrator**—Simplifies and automates the integration of data from external data sources or text files into the Guardium repository. With data housed in the repository, the full array of Guardium policy, analysis, reporting and workflow tools can be leveraged. It allows input data from other sources to participate in the correlation analysis from change ticketing systems. Organizations can import descriptive information such as full names and phone numbers corresponding to user names to streamline investigation of exceptions; integrate information from identity and access management systems, such as roles and departments, to enable fine-grained security policies; and connect to IBM Spectrum Protect™, formerly known as IBM Tivoli® Storage Manager, and EMC Centera to archive audit data and oversight process results.

Why Guardium?

Guardium is part of IBM Security Systems Framework and IBM Data Security Privacy Platform. Guardium provides end-to-end data protection capabilities to discover and analyze, protect, integrate and manage the critical data in your environment. Guardium provides all the building blocks you need for data protection—from meeting compliance requirements all the way through to broader data protection. The portfolio is modular, so you can start anywhere and mix and match security software building blocks with components from other vendors or choose to deploy multiple building blocks together for increased acceleration and value. The security platform is an enterprise-class foundation for information-intensive projects providing the performance, scalability, reliability and acceleration needed to simplify difficult challenges and deliver trusted information to your business faster. For clients with other data security needs, IBM Security Guardium also provides capabilities including: Data Protection for Files, Vulnerability Assessment, Encryption, Express Data Protection for Databases, and more.


Discovery, classification, vulnerability assessment and entitlement reporting
Encryption, masking and redaction
Data and file activity monitoring
Dynamic blocking and masking, alerts, and quarantines
Compliance automation and auditing
Analytics
IBM Security Guardium
Cloud environments
Applications
Big-data platforms
Databases and data warehouses
File systems

IBM Security Guardium is a comprehensive data security platform that helps security teams secure and manage all types of sensitive data consistently, whether it is in big-data platforms, databases or file systems, across distributed and mainframe (IBM z Systems™) environments.

Why IBM?

IBM Security offers one of the most advanced and integrated portfolios of enterprise security products and services. The portfolio, supported by world-renowned IBM X-Force® research and development, provides security intelligence to help organizations holistically protect their people, infrastructures, data and applications, offering solutions for identity and access management, database security, application development, risk management, endpoint management, network security and more. These solutions enable organizations to effectively manage risk and implement integrated security for mobile, cloud, social media and other enterprise business architectures. IBM operates one of the world's broadest security research, development and delivery organizations, monitors 15 billion security events per day in more than 130 countries, and holds more than 3,000 security patents.

For more information

To learn more about IBM Security Guardium Data Protection for Databases and Big Data environments, please contact your IBM representative or IBM Business Partner, or visit: **ibm.com**/guardium

Additionally, IBM Global Financing provides numerous payment options to help you acquire the technology you need to grow your business. We provide full lifecycle management of IT products and services, from acquisition to disposition. For more information, visit: **ibm.com**/financing

IBM Security
Route 100
Somers, NY 10589

Produced in the United States of America
December 2016

This document is current as of the initial date of publication and may be changed by IBM at any time. IBM Business Partners set their own prices, which may vary.

The performance data discussed herein is presented as derived under specific operating conditions. Actual results may vary. It is the user's responsibility to evaluate and verify the operation of any other products or programs with IBM products and programs.

THE INFORMATION IN THIS DOCUMENT IS PROVIDED "AS IS" WITHOUT ANY WARRANTY, EXPRESS OR IMPLIED, INCLUDING WITHOUT ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OR CONDITION OF NON-INFRINGEMENT. IBM products are warranted according to the terms and conditions of the agreements under which they are provided.

The client is responsible for ensuring compliance with laws and regulations applicable to it. IBM does not provide legal advice or represent or warrant that its services or products will ensure that the client is in compliance with any law or regulation.

Statements regarding IBM's future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only.

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful, comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM DOES NOT WARRANT THAT ANY SYSTEMS, PRODUCTS OR SERVICES ARE IMMUNE FROM, OR WILL MAKE YOUR ENTERPRISE IMMUNE FROM, THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.

♲ Please Recycle