IBM Security Guardium Data Protection

Continuously monitor data access and protect sensitive data across the enterprise

IBM® Security Guardium® Data Protection empowers security teams to safeguard sensitive data through automated discovery, classification, vulnerability assessments, activity monitoring and advanced threat detection — extending comprehensive data protection across heterogeneous environments, including databases, data warehouses, mainframes, file systems, file shares, cloud and big-data platforms.

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 automatically 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 helps accelerate compliance through a set of core capabilities that help reduce operational risk and total cost of ownership.

Highlights

- Uncover data risk through data discovery, classification and vulnerability scans
- Automatically take action or report regulatory compliance
- Monitor in real time access to high-value databases, data warehouses, mainframes, files, cloud and big-data environments
- Minimize total cost of ownership with robust scalability, analytics simplification, and automation

Risk reduction

Guardium Data Protection reduces the risk of a data breach by providing real-time data security intelligence, with features that

enable organizations to uncover data risks by providing data discovery and classification for compliance and privacy regulations, enabling proactive assessment of database vulnerabilities and providing granular visibility into database entitlements, dormant accounts and excessive privileges for effective access governance processes.

Database discovery, data classification and entitlement reports can be configured to probe specified network segments on a schedule or on demand allowing you to examine content to identify and classify sensitive data. You can also build custom reports with drill-down capabilities using an intuitive drag-and-drop interface.

Vulnerability assessments can proactively scan databases for vulnerabilities, misconfigurations, authentication controls and missed patches before they can be exploited. Quarterly data protection subscriptions (DPS) and rapid response DPS let you keep ahead of the zero-day vulnerabilities. Results can be actioned by opening a ticket in IT Service Management platforms such as ServiceNow.

Predefined security policy templates can be customized based on your own audit requirements. The policies can be built to detect any threat scenario against the data utilizing the most common audit constructs and other contextual information.

Real-time data activity monitoring, security alerts, and blocking (via S-GATE) monitors and enforces a wide range of policies, data transactions to create a detailed audit trail and creates profiles based on risky user behavior coupled with advanced threat detection use cases. Creates alerts in real-time when a security policy is violated and enables blocking or quarantining users for suspicious activity to remediate threats quickly.

Advanced Threat Detection uses machine-learning (M/L) algorithms, which use a combination of rules-based policies and symptom analysis to detect patterns of behaviors that map to known industry attack vectors, to identify insider and external threats. Identified cases are categorized by severity for investigative analysis and response.

Streamlined graphical user interface provides centralized control

IT and security professionals are under high pressure to maximize the use of their resources and time. Through an automated deployment, Guardium Data Protection provides key capabilities to help you streamline data security management without impacting data sources, networks, or applications, such as:

Dynamic graphical user interface (GUI) helps build and update data and user groups. Whitelists or blacklists can be generated on any auditable item, such as users, IP addresses and table names. Groups can be populated using queries or using Guardium APIs (GuardAPIs).

Powerful analytic insights includes leading-edge analytic tools—such as connection profiling, search engine for real-time forensics, outlier detection algorithms and an investigative dashboard—that provide actionable insights on data access behavior.

Customizable workflows with preset accelerators for common compliance requirements creates custom processes without sacrificing security, by ensuring that some team members see only data and tasks related to their own roles and by storing process results in a secure centralized repository.

Secure and self-sustained platform through the Guardium GUI allows for audits of 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

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% overhead in most cases—using key capabilities, such as:

- An operating system-based agent without affecting the performance of the data source or application
- Filtering of database traffic, avoiding unnecessary database audit traffic
- Centralized load balancing for multi-tier architecture
- Support for 64-bit architecture

Scalability

As enterprises adapt to changes in the business and technological landscapes, data sources continue to proliferate over geographical and organizational boundaries. An organization's data—stored across on premise and hybrid multicloud environments—is increasing in volume, variety and velocity. Guardium Data Protection is equipped to scale seamlessly from one data source to tens of thousands without disrupting operations. Automation capabilities include:

Guardium Grid automates adaptation to changes in the data

Load balancing scalability and performance features help you reduce management costs, minimize the need to manage detailed configuration information and simplify 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 and management

Merges and normalizes audit reports from multiple data sources to produce enterprise-wide reports and a forensics source. Controls operations and policy setting from a central location.

Deployment options

Guardium Data Protection can be deployed to protect structured, semi-structured and unstructured files. Some of the deployment models include:

Guardium Data Protection for Databases and Big Data

Supports enterprise databases or data warehouses running on major operating systems including IBM DB2, Oracle, Teradata, Sybase, Microsoft SQL Server, running on Windows, UNIX, Linux, AS/400, and z/OS as well as Hadoop and NoSQL environments. In addition to the capabilities detailed on the previous pages, this deployment monitors: all executions of SQL commands on database objects; audits all logins/logouts and security exceptions such as login failures; and SQL errors and extrusion detection.

Guardium Data Protection for Databases Services

Provides all the functions and features of Guardium Data Protection for Databases; however, this offering is optimized for protecting databases deployed in cloud-native platforms such as IBM Cloud Pak for Data as well as databases consumed as a service from cloud, like AWS RDS, Azure Database-Platform-as-a-Service (DBaaS, or DPaaS).

Guardium Data Protection for Files

Guardium Data Protection for Files helps support the security and integrity of unstructured data—documents, spreadsheets, web pages, presentations, chat logs, and more—in heterogeneous environments. The solution can be deployed in unstructured data repositories, such as NAS, SharePoint, Windows and Unix. It protects critical configuration and application files and back-end access to application documents. This deployment supports many data file types, including PDF documents, text, Microsoft Office files, comma-separated values (CSV) files, logs, source code (Java, C++, C#, Perl, XML) and more.

Guardium Data Protection for z/OS

Organizations that deploy IBM z Systems™ mainframes have protection built in—including security in the processor, operating system, storage and applications—but even mainframe environments need to protect against threats increasing in volume and sophistication and to meet compliance regulations.

Guardium Data Protection for z/OS provides comprehensive data security and compliance capabilities for DB2, IMS and Data Sets on z/OS. The solution can be used for the mainframe environment only, or it can be integrated with Guardium data security and monitoring components on distributed systems —providing a robust, centralized data security solution.

Guardium Data Protection for z/OS is scalable and flexible, using lightweight software sensors called S-TAPs to capture DB2, IMS and Data Set activities by privileged users, mainframe-resident applications and network clients, including those connecting through services such as Java Database Connectivity, DB2 or IMS. Proven IBM event-capture technologies ensure that all critical operations are captured, without the use of expensive audit traces.

Guardium Data Protection for SAP HANA

Organizations need a solution that can secure dispersed data, detect database vulnerabilities and security blind spots and monitor user access while having minimal impact on performance. Guardium Data Protection provides real-time protection for your SAP HANA database environments.

Guardium Data Protection for SAP HANA enables all the functions and features of Guardium Data Protection for Databases including IBM Security Guardium Vulnerability Assessment, which scans SAP HANA deployments to detect potential exposures (such as such as missing patches, weak passwords, unauthorized changes and misconfigured privileges) and generates reports with suggested remedial actions. Users can integrate results with ServiceNow for remediation and closed-loop feedback

The solution does not require modifications to your existing SAP database environment and can be scaled effortlessly to meet larger deployment needs. Deployed as a lightweight S-TAP agent onto the SAP HANA appliance, Guardium Data Protection enables parsing, analysis and logging needed to apply the security and compliance workflows, requiring minimal resources from the SAP HANA cluster.

Guardium Data protection is available on cloud-market places. Supports deployment of the entire infrastructure in the cloud across major providers such as AWS, Azure, Google Cloud, IBM Cloud and Oracle Cloud.

Integration

Most existing security solutions lack the complete visibility into data access patterns required by regulatory mandates. Guardium Data Protection provides analytics-based, in-depth insight while seamlessly integrating into existing security solutions, such as

QRadar, Splunk, Resilient, CyberArk, DUO, HP ArcSight to name a few. In addition, Guardium Data Protection provides a modular integration model with existing IT systems, such as data management, ticketing and archiving solutions such as IBM Cloud Pak for Data, ServiceNow and Amazon S3.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 can seamlessly share information with common IT operations tools, such as ticketing systems
- Integration with security systems and standards (Active Directory, Radius and 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

Why IBM Security

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, provides security solutions to help organizations drive security into the fabric of their business so they can thrive in the face of uncertainty.

IBM operates one of the broadest and deepest security research, development and delivery organizations. Monitoring more than one trillion events per month in more than 130 countries, IBM holds over 3,000 security patents. To learn more, visit ibm.com/security.

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

For more information

Discover how IBM Security Guardium solutions can help you take a smarter, integrated approach to safeguarding critical data across your hybrid, multicloud environments. Visit ibm.com/security/data-security/guardium