IBM Security Guardium Data Protection

Continuously monitor data access to protect sensitive data and align with zero trust principles

IBM Security Guardium Data Protection empowers security teams to safeguard sensitive data through discovery and classification, data activity monitoring, vulnerability assessments, 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.

Guardium Data Protection helps organizations to adopt a zero trust approach that never assumes anyone or anything is trustworthy, but continuously verifies whether access to data should be granted based on contextual information. Guardium continuously monitors all data access operations in real-time to detect unauthorized actions based on detailed context — the "who, what, where, when and how" of each data access. It reacts automatically to help prevent unauthorized or suspicious activities by privileged insiders and potential hackers.

Reduce risk with a data-centric approach

Guardium Data Protection reduces the risk of a data breach by providing real-time data security visibility and intelligence that enables organizations to address increasingly complex data security and privacy regulations, while stopping threats and risky users in their tracks. Capabilities include data discovery and data classification, which can be configured to probe network segments or scan data

Highlights

- Monitor data activity from high-value databases, data warehouses, mainframes, files, cloud and big data environments
- Uncover and take action on risky users, vulnerabilities, and other threats
- Address regulatory compliance with automated workflows
- Minimize total cost of ownership with robust scalability and automation

sources on a schedule or on-demand, allowing you to examine content and metadata to identify and classify sensitive data.

Predefined security and compliance policy templates can be customized based on your audit and regulatory requirements. Policies can be built to detect any threat scenario against the data utilizing the most common audit constructs and other contextual information. To automate compliance tracking and reporting, policies and rules can be easily created, updated and tagged for specific data security and privacy regulations and standards, without duplicating administrative efforts. Guardium Data Protection offers numerous quick starts to reduce the time it takes to audit and report on compliance, from months down to weeks, with compliance accelerators and automated workflows.

These policies instruct real-time data activity monitoring and security alerts, which inform detailed audit trails and risky user profiles. Guardium Data Protection notifies security analysts with alerts in real-time when a security policy is violated. To help discern and stay alert of suspicious user access or connections to data sources, as well as identify in real-time the presence of sensitive objects in the traffic of monitored data sources, Guardium helps analysts evaluate risks more efficiently with built-in advanced analytics for increased visibility and context that promotes zero trust security. This enriched understanding of risk helps security teams to block or quarantine users or sessions for suspicious activity and to remediate threats quickly.

You can also build custom reports with drill-down capabilities using an intuitive drag-and-drop interface to support your audit processes and regulatory compliance needs. Guardium Data Protection provides granular visibility into user entitlements, dormant accounts and excessive privileges so that your organization can prove that it has effective access governance controls in place.

Guardium's 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 help you keep ahead of zero-day vulnerabilities. Results can be actioned by opening a ticket in IT Service Management platforms such as ServiceNow.

Lastly, Guardium offers advanced analytical tools based on machine-learning (ML) 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 further investigation and response.

Centralize control to streamline data security

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

- Centralized policy management and enforcement across hybrid multicloud deployments simplifies data protection even as your data landscape and IT infrastructure change and grow. The self-sustained platform through the Guardium graphical user interface (GUI) allows for audits of all operations, including administration and configuration tasks to maintain security controls, segregation of duties and compliance with the latest security mandates and Federal Information Processing Standards (FIPS) 140-2

- Through the user interface, you can easily build and update data and user groups for closer monitoring and auditing. Blocklists and allowlists can be generated on any auditable item, such as users, IP addresses and table names. Groups can be populated using queries or Guardium APIs (GuardAPIs)
- Actionable insights from leading-edge analytical capabilities help to quickly prioritize and respond to threats. Capabilities include user access profiling, search engine for real-time forensics, outlier detection algorithms and an investigative dashboard

Secure data sources without performance impact

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 that does not affect the performance of the data source or application
- Filtering of data source traffic to avoid unnecessary data audit traffic
- Centralized load balancing for multi-tier architectures
- Support for 64-bit architectures

Scale and adapt data protection as needed

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-premises and cloud 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 due to the following capabilities:

- Automated adaptation to changes in the data center with load balancing scalability to support large deployments in frequent change. This helps to reduce management costs, minimize configuration information management, and simplify data capacity expansion projects
- Batch integration of IT processes with Guardium with the help of GuardAPI, a command-line interface (CLI) to Guardium that allows any operation to be performed remotely
- Centralized management of operations, policies, and auditing that simplifies the aggregation and normalization of multiple data sources for enterprise reporting
- Agent and agentless connections to data sources that help reduce the workload on infrastructure teams. Use at-source monitoring for sensitive data with Guardium S-TAP and external S-TAP agents. Monitor less-sensitive data sources with Universal Connector plugins, which offer an agentless architecture that imports native audit logs and normalizes the data to prepare it for reporting and analytics, making it fast and easy to connect to modern, cloud-based data environments

Deploy data security through multiple options

Guardium Data Protection can be deployed to protect structured and unstructured data sources and platforms. 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 and 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, all logins/logouts and security exceptions such as login failures, and SQL errors and extrusion detection.

Guardium Data Protection for Database 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, such as AWS RDS and Azure Database-Platform-as-a-Service (DBaaS or DPaaS). Some of the environments supported by this version include IBM DB2 and DB2 Warehouse, Netezza Performance Server and BigSQL.

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 others.

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 comply with security and privacy 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. It 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
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. It 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 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 for cloud deployment
Guardium Data Protection supports deployment of the entire infrastructure in the cloud across major providers such as AWS, Azure, Google Cloud, IBM Cloud and Oracle Cloud. For organizations

that use AWS, Guardium Data Protection is available on AWS Marketplace to provide unified data protection across a hybrid AWS cloud environment.

Integrate your tools for connected security

Most existing security solutions lack the complete visibility into data access patterns required by regulations or a zero trust framework. Guardium Data Protection seamlessly integrates and provides in-depth, analytics-based insights to your existing security solutions such as QRadar, IBM Security Verify, Splunk and ArcSight, to name a few. Guardium Data Protection also provides a modular integration model with IT operations and systems such as data management, ticketing and archiving solutions that include IBM Cloud Pak for Data, IBM Security SOAR, ServiceNow and Amazon S3 – to seamlessly share critical information. The goal is to streamline IT and security operations by complementing and extending them with data security capabilities.

In addition, Guardium Data Protection supports identity security systems and standards such as Active Directory, RADIUS, LDAP and other third-party solutions such as CyberArk, DUO and HashiCorp's Vault for streamlined authentication and centralized management of data source credentials and privileged access, performed automatically and directly from such directories. By protecting data and identities, in collaboration with a broad range of security tools, Guardium Data Protection can help organizations remove silos to achieve a zero trust approach to security.

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, 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.

This document contains information pertaining to the following IBM products which are trademarks and/or registered trademarks of IBM Corporation:

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 https://www.ibm.com/products/ibm-guardium-data-protection to learn more about Guardium Data Protection.