IBM InfoSphere Guardium Data Activity Monitor

Continuously monitor data access and protect sensitive data across the enterprise

Highlights

- Provides a simple, robust solution for continuously monitoring access to high-value databases, data warehouses, file shares, document-sharing solutions and big data environments.
- Reduces risk and extends security intelligence with in-depth database security and protection.
- Lowers total cost of ownership with robust scalability for large enterprise-wide deployments.

Lowers total cost of ownership with robust scalability for large enterprise-wide deployments.

IBM® InfoSphere® Guardium® Data Activity Monitor provides the simplest, most robust solution for assuring the security and integrity of data in heterogeneous environments such as databases, data warehouses, file shares and big data platforms including Hadoop, Cloudera, IBM InfoSphere BigInsights™ and NoSQL databases. 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. InfoSphere Guardium Data Activity Monitor prevents unauthorized or suspicious activities by privileged insiders and potential hackers, and automates governance controls in heterogeneous enterprises.

InfoSphere Guardium Data Activity Monitor lowers the total cost of ownership, improves security, and supports compliance requirements through a set of core capabilities. These capabilities are available in three simple offerings: *Data Activity Monitor Standard Edition*, *Data Activity Monitor Advanced Edition and Central Management*. Figure 1 demonstrates core capabilities and the value that they provide. All core capabilities are included in the Standard Edition, except for those marked with a "*", which are available in the Advanced Edition. Central Manager can be purchased separately, and the capabilities included in Central Management are marked with a "c."

Streamlined Management	TCO	Security	Compliance
Automatic update of reports and policies to adapt to IT changes and security events	x	x	
[C]Single console to manage, use and update InfoSphere Guardium	x		
Database discovery and data classification	x	x	x
Automated management through groups (white lists, black lists)	x	x	x
Secure and self sustained platform (self monitoring, internal audit, secure appliance)	x		x
Predefined security policies	x	x	x
Built-in compliance workflow (review, escalations, sign-offs)	x		x
[C]Advanced compliance workflow (row-level auditing and customizable workflow)	x		x
Quick search and real time analytic reporting	x		x
Performance			
OS based agent (SOD)	x	x	x
Filtering of DB traffic	x		
scalable 64-bit appliance platform	x		
Integration			
Integration with IT operations	x	x	x
Integration with security systems (QRadar, HP Arcsight, Radius, LDAP, etc.)	x	x	
Flexible, customizable integration platform (Universal Feed, Enterprise Integrator)	x	x	x
Integration with IT operations (Master Data Management, Change Data Capture, etc)	x		x
Scalability			
Automatically adapt to changes in the data center (Grid)	x		
Support for batch operations (GuardAPI)	x		
[C]Aggregation–merge audit reports from multiple sources to produce enterprise-wide reports	x		x
Risk Reduction			
Custom report builder with drill-down capabilities	x		x
Best practice recommendations–predefined reports and alerts	x		x
Real-time data activity monitoring with application end-user translation		x	x
Real-time security alerts		x	
**Real-time data masking (S-GATE)		x	
**Real-time blocking (S-GATE), including quarantine and fire ids		x	

[C]Also available in InfoSphere Guardium Central Management
**Available in InfoSphere Guardium Data Activity Monitor Advanced Edition Only

Figure 1: InfoSphere Guardium Data Activity Monitor lowers total cost of ownership, improves security and supports compliance requirements through a set of core capabilities available in three simple offerings: Data Activity Monitor Standard Edition, Data Activity Monitor Advanced Edition and Central Management.

Streamlined management

No organization has the time or resources to spend time on low-level security operations or manual processes. Not only do manual approaches slow down the business, but they are risky and error-prone. As your business grows and the scope of security projects increase, you need security solutions to become more streamlined. In the era of big data where data is growing in volume, variety and velocity, security strategies should be optimized and transparent, not more complex or obscure.

InfoSphere Guardium Data Activity Monitor provides key capabilities to help organizations streamline data security management without changes to databases, networks or applications.

- **Automatic update of reports and policies to adapt to IT changes and security events** — Maximizes the protection afforded by InfoSphere Guardium. With one click, groups, policies, tests and other configurable parameters can be updated to adapt to the constantly evolving nature of the database infrastructure and associated threats.
- **Single console to manage, use and update InfoSphere Guardium** — Provides centralized management through a single web-based console. The scalable multitier 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 and data classification** — Discovers and classifies sensitive data. The discovery process can be configured 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.
- **Automated management through groups (white lists, black lists)** — Automates group management for security policies and compliance reports. Groups are used in audit reports, alerts and real-time policies to facilitate the maintenance — despite the constant change in the IT environment. White lists or black lists can be 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 be automated with LDAP integration. Populate groups from query, or GuardAPIs. You can synch with user groups in Active Directory, IBM Tivoli® DS, Novell, Open LDAP, SunOne, 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.
- **Secure and self sustained platform (self monitoring, internal audit, secure appliance)** — Audits all operations, including administration and configuration to maintain compliance controls and supportability.
- **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, such an SQL injection attack typically exhibits patterns of database access that are uncharacteristic of standard line-of-business applications. Exception policies 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.

- **Built-in compliance workflow (review, escalations, sign-offs)**—Supports SOX, PCI, HIPAA and more with pre-defined reports for top regulations. An easy-to-use graphical user interface allows a wide variety of processes to be created to match the unique needs of the tasks and individuals involved. Many different audit tasks are supported, including reviewing the results of automatically generated vulnerability assessments, asset discovery and data classification. Export reports in varying formats, which include PDF, CSV, CEF, Syslog forwarding, SCAP or custom schemas.
- **Advanced compliance workflow (row-level auditing and customizable workflow)**—Centralizes and automates oversight processes enterprise-wide, including report generation, distribution, electronic sign-offs and escalations; creates custom processes by specifying your unique combination of workflow steps, actions and user and enable automated execution of oversight processes on a report line-item basis, maximizing process efficiency without sacrificing security; ensures that some team members see only data and tasks related to their own roles, and stores process results in a secure centralized repository.
- **Quick search and real time analytic reporting**—Obtain responsive forensic information from the most relevant data access activity with the data security datamart pivot-table-like capability.

Performance

Business moves fast and clients demand continual access to data. As a result, IT environments including databases, transactional applications, analytics platforms 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. InfoSphere Guardium Data Activity Monitor can be implemented with negligible performance impact—less than 1% overhead in most cases using key capabilities.

- **OS based agent (Separation of Duties)**—Monitors only what is required, such as the data traffic already going from the OS to the data source. As a result, monitoring does not affect the performance of the data source or application since native audit logging does not need to be enabled.
- **Filtering of DB traffic**—Avoids unnecessary DB audit traffic at the source.
- **A scalable 64-bit appliance platform**—Leverage an appliance platform that can grow with your implementation and delivers the throughput to handle traffic analysis for thousands of data sources.

Integration

Most organizations have some security solutions in place today. For example, a Security Information and Event Management (SIEM) solution or application-level access controls. However, most existing security solutions do not provide the 100 percent visibility into data access patterns required by regulatory mandates. InfoSphere Guardium Data Activity Monitor provides this insight, while seamlessly integrating into existing security solutions such as IBM Security QRadar® or HP ArcSight. In addition, InfoSphere Guardium Data Activity Monitor provides a "snap it" integration model with existing IT systems such as data management, ticketing and archiving solutions. The goal is to complement existing IT solutions and extend your security posture.

- **Integration with IT operations**—Exploits existing data management environments. 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, MongoDB and more across all major protocols including: HTTP, HTTPS, FTP, SAMBA and IBM iSeries® connections to CSV text file data sources. Additionally support the data governance toolsets that accompany these backend technologies, such as Master Data Management, Change Data Capture, or Archival solutions.
- **Integration with security systems and standards (QRadar, HP Arcsight, Radius, LDAP)**—Adapts to changes automatically. Users, groups, roles and authentication to databases and applications can be updated automatically and directly from directories like LDAP, Radius and Active Directory. You can automatically handle any staff or user change while keeping the policies and reports intact, avoiding the need to constantly modify them. In addition, send all audit information to a SIEM such as IBM Security QRadar.
- **Flexible, customizable integration platform (Universal Feed, Enterprise Integrator)**—Simplifies and automates the integration of data from external databases or text files into the InfoSphere Guardium repository. With data housed in the repository, the full array of InfoSphere Guardium policy, analysis, reporting and workflow tools can be leveraged: Allows input data from other sources to participate in the correlation analysis; creates unified audit reports, including external information that enhances security and improves operational efficiency such as approved modifications from change ticketing systems; imports descriptive information such as full names and phone numbers corresponding to user names to streamline investigation of exceptions; integrates information from IAM systems, such as roles and departments, to enable finer-grained security policies; interfaces with IBM Tivoli Storage Manager and EMC Centera to archive audit data and oversight process results.

Scalability

Managing database security and compliance has become increasingly challenging. Not only has the rate of cyber attacks continued to grow, but the complexity of the environments has increased dramatically. Driven by a rapidly changing business landscape that includes mergers, outsourcing, workforce adjustments and accelerating business automation, databases continue to proliferate over geographical and organizational boundaries. In addition, data is growing in terms of volume, variety and velocity introducing new types of data stores, for example Hadoop and NoSQL databases. Given the current resource-constrained environment, the complexity of environments being managed and escalating workloads, organizations are now seeking means to increase automation in their database security and compliance operations. InfoSphere Guardium Data Activity Monitor is equipped to scale from one database to tens of thousands without disrupting operations.

- **Automatically adapts to changes in the data center (Grid)** — Balances the load and handles changes or additions to the environment without impacting performance or availability of the data monitoring infrastructure. Dynamically adds or drops data sources without altering configurations. The InfoSphere Guardium Grid provides elasticity for supporting large deployments in frequent change. Load balancing scalability and performance benefits help clients reduce management costs, minimize the need to manage detailed configuration information (IP addresses and so on) as data sources are added or removed and simplify data capacity expansion projects.
- **Support for batch operations (GuardAPI)** — Facilitates integration of any IT process with InfoSphere Guardium Data Activity Monitor. GuardAPI is a script-based CLI interface to InfoSphere Guardium allowing any operation to be done remotely.
- **Aggregation** — Merges audit reports from multiple sources to produce enterprise-wide reports.

Risk reduction

Risk is the potential that a chosen action or activity, including the choice of inaction, will lead to sensitive data exposure. A probability or threat of damage, liability, data loss, or any other negative occurrence that is caused by external or internal vulnerability must be avoided through preemptive action. InfoSphere Guardium Data Activity Monitor reduces risk by providing real time data security and intelligence.

- **Custom report builder with drill-down capabilities** — Customizes and filters security reports to display the parameters that are relevant to you. Some common reports include: SQL errors, failed logins, terminated users and policy violations.
- **Best practice recommendations–predefined reports and alerts** — Provides a variety of predefined reports from 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: accounts with system privileges, all system and administrator privileges, shown by user and role, object privileges by user and all objects with PUBLIC access. All entitlement information is stored in a forensically secure and tamper-proof repository along with all database audit information. Custom reports can be built easily by way of an intuitive drag-and-drop interface.

- **Real-time data activity monitoring with application end-user translation** — Creates an audit trail of all database activities 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); provides 100 percent visibility and granularity into all database, file share, data warehouse, Hadoop and NoSQL transactions across all platforms and protocols—with a secure, tamper-proof audit trail that supports separation of duties; monitors and enforces wide range of policies for sensitive-data access, privileged-user actions, change control, application-user activities and security exceptions; creates a single, centralized audit repository for enterprise-wide compliance reporting, performance optimization, investigations and forensics; monitors all data transactions to create a continuous, fine-grained audit trail that indentifies the "who, what, when, where and how" of each transaction.
- **Real-time security alerts**—Receives alerts in real time when a security policy is violated so you can take action.
- **Real-time data blocking (S-GATE) including quarantine and firecall ids**—Establish preventative controls across the enterprise. InfoSphere Guardium Data Activity Monitor provides automated, real-time controls (blocking or quarantining users) that 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 change windows and creating new user accounts and modifying privileges. Implement firecall IDs which allows specified users to access certain server for a particular time period to accommodate certain activities such as maintenance windows without affecting DB security configuration.
- **Real-time masking (S-GATE)**—Take action on suspicious activity. Prevent leakage of sensitive data by dynamically masking it according to the requester's role.

About IBM InfoSphere Guardium

InfoSphere Guardium is part of the IBM InfoSphere integrated platform and the IBM Security Systems Framework. The InfoSphere Integrated Platform defines, integrates, protects and manages trusted information in your systems. The InfoSphere Platform provides all the foundational building blocks of trusted information, including data integration, data warehousing, master data management and information governance, all integrated with a core of shared metadata and models. The portfolio is modular, so you can start anywhere and mix and match InfoSphere software building blocks with components from other vendors, or choose to deploy multiple building blocks together for increased acceleration and value. The InfoSphere 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 more information

To learn more about IBM InfoSphere Guardium solutions, contact your IBM sales representative or visit:
ibm.com/guardium

IBM Corporation
Route 100
Somers, NY 10589

Produced in the United States of America
October 2013

Please Recycle

IMD14433-USEN-01