IBM InfoSphere Guardium

Managing the entire database security and compliance life cycle

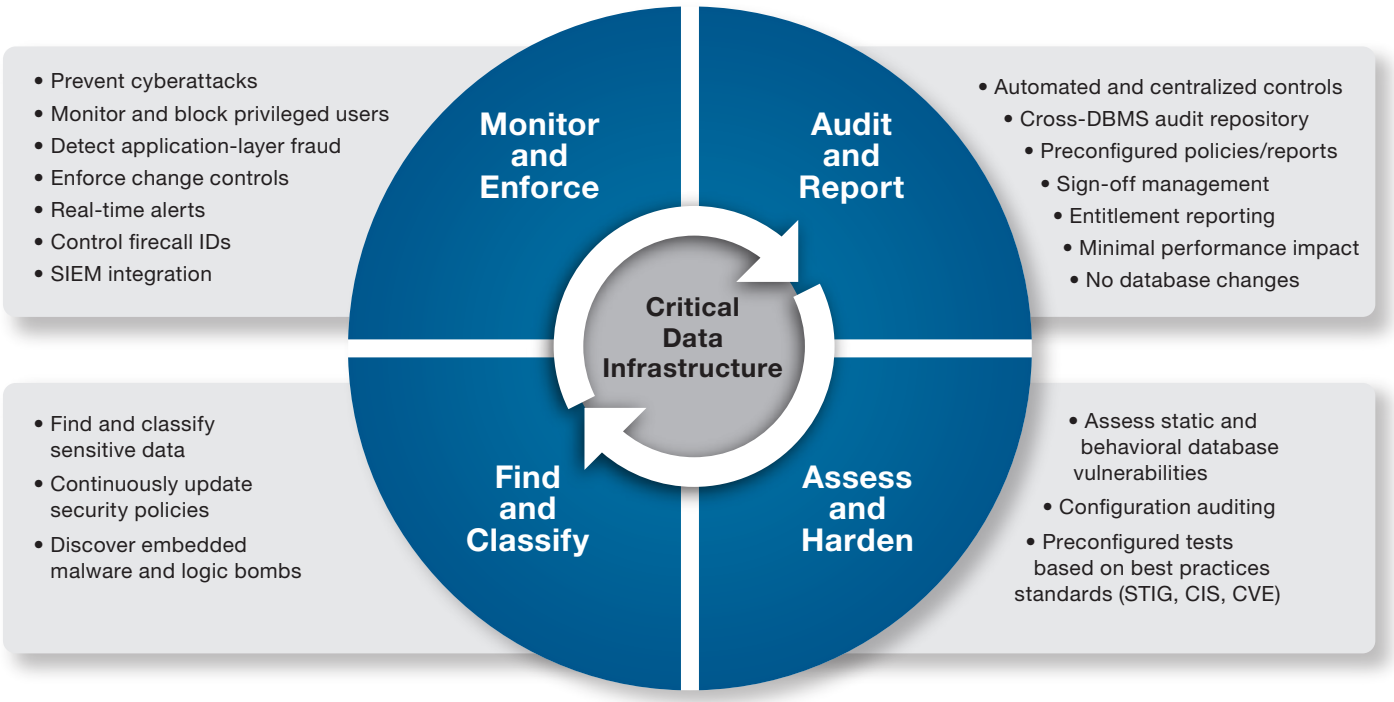
Leading organizations across the world trust IBM to secure their critical enterprise data. The fact is, we provide a simple, robust solution for safeguarding a broad range of enterprise systems used to store financial and ERP information, customer and cardholder data, and intellectual property.

Our enterprise security platform prevents unauthorized or suspicious activities by privileged insiders and potential hackers. It also monitors potential fraud by users of enterprise applications such as Oracle E-Business Suite, PeopleSoft, SAP and in-house systems.

At the same time, our solution optimizes operational efficiency with a scalable, multi-tier architecture that automates and centralizes compliance controls across your entire application and database infrastructure.

But as remarkable as this solution is for what it does, it's equally remarkable for what it doesn't do. It has negligible impact on performance, does not require changes to your databases and does not rely on native database logs or auditing utilities.

Real-time database security and monitoring



Unified Solution: Built on a single unified console and back-end data store, InfoSphere Guardium offers a family of integrated modules for managing the entire database security and compliance life cycle.

The IBM® InfoSphere® Guardium® solution addresses the entire database security and compliance life cycle with a unified web console, back-end data store and workflow automation system, enabling you to:

- Find and classify sensitive data in corporate databases.
- Assess database vulnerabilities and configuration flaws.
- Ensure that configurations are locked down after recommended changes are implemented.
- Capture and examine all database transactions, including local access by privileged users — for all supported platforms and protocols — with a secure, tamper-proof audit trail that supports separation of duties.
- Track activities on major file sharing platforms.
- Monitor and enforce policies for sensitive data access, privileged user actions, change control, application user activities and security exceptions such as login failures.
- Automate the entire compliance auditing process — including report distribution to oversight teams, sign-off and escalations — with preconfigured reports for SOX, PCI Data Security Standard (DSS) and data privacy.
- Create a single, centralized audit repository for enterprise-wide compliance reporting, performance optimization, investigations and forensics.
- Easily scale from safeguarding a single database to protecting thousands of databases in distributed data centers around the world.

Find and classify

As organizations create and maintain an increasing volume of digital information, they are finding it harder and harder to locate and classify sensitive information.

Locating and classifying information

Locating and classifying sensitive information is especially challenging for organizations that have experienced mergers and acquisitions or for environments where existing systems have outlasted their original developers. Even in the best of cases, ongoing changes to application and database structures — required to support new business requirements — can easily invalidate static security policies and leave sensitive data unknown and unprotected.

Organizations find it particularly difficult to:

- Map out all database servers containing sensitive information and understand how it is being accessed from all sources (line-of-business applications, batch processes, ad hoc queries, application developers, administrators and others).
- Secure information and manage risk when the sensitivity of stored information is unknown.
- Ensure compliance when it isn't clear which information is subject to the terms of particular regulations.

Automatically locate, classify and secure sensitive information

With InfoSphere Guardium, you use database auto-discovery and information classification to identify where confidential data is stored and then use customizable classification labels to automate enforcement of security policies that apply to particular classes of sensitive objects. These policies ensure that sensitive information is only viewed and changed by authorized users. Sensitive data discovery can also be scheduled to execute regularly to prevent the introduction of rogue servers and ensure that no critical information is "forgotten."

Assess and harden

Database environments are highly dynamic, with changes in accounts, configurations and patches occurring regularly. Most organizations lack the skilled resources to review changes systematically to determine if they have introduced security gaps.

Automated vulnerability, configuration and behavioral assessment

The database security assessment capability of InfoSphere Guardium scans your entire database infrastructure for vulnerabilities and provides an ongoing evaluation of your database security posture, using both real-time and historical data.

It provides a comprehensive library of preconfigured tests based on industry best practices (CVE, CIS, STIG), along with platform-specific vulnerabilities, which are updated regularly by the InfoSphere Guardium Knowledge Base service. You can also define custom tests to match specific requirements. The assessment module flags compliance-related vulnerabilities such as unauthorized access to reserved Oracle E-Business Suite and SAP tables for compliance with SOX and PCI DSS.

Assessments are grouped into two broad categories:

- Vulnerability and configuration tests check for vulnerabilities such as missing patches, misconfigured privileges and default accounts.
- Behavioral tests identify vulnerabilities based on how databases are being accessed and manipulated — such as an excessive number of login failures, clients executing administrative commands or after-hours login — by monitoring all database traffic in real time.

In addition to producing detailed reports, along with supporting data, the assessment module generates a security health report card. The report card not only includes weighted metrics based on best practices and industry standard reference numbers, but it also recommends concrete action plans to strengthen database security.

Configuration lock-down and change tracking

After you have implemented the actions recommended in the vulnerability assessment, you can establish a secure configuration baseline. The InfoSphere Guardium Configuration Audit System can monitor changes to this baseline and make sure they are not made outside of your authorized change control policies and processes.

Monitor and enforce

Escalating threats to sensitive data, along with growing compliance mandates, are driving organizations to seek effective means of monitoring database activities enterprise-wide and preventing unauthorized activities in real time.

Monitor and enforce policies for database security and change control

InfoSphere Guardium provides granular, real-time policies to prevent unauthorized or suspicious actions by privileged database accounts and attacks from rogue users or outsiders. You can also identify application users that make unauthorized changes to databases with multi-tier applications that access databases from a common service account, such as Oracle E-Business Suite, PeopleSoft, Siebel, SAP, IBM Cognos® software and custom systems built on application servers such as Oracle WebLogic, Oracle AS and those in the IBM WebSphere family.

The solution can be managed by information security personnel without involving database administrators (DBAs). You can also define granular access policies that restrict access to specific tables based on operating system login, IP or MAC address, source application, time of day, network protocol and type of SQL command.

Continuous contextual analysis of all database traffic

InfoSphere Guardium continuously monitors all database operations in real time, using linguistic analysis to detect unauthorized actions based on detailed contextual information — the "who, what, where, when and how" of each SQL transaction. This contextual approach minimizes false positives and negatives while providing a significant level of control, unlike traditional approaches that only look for predefined patterns or signatures.

Baselining to detect anomalous behavior and automate policy definition

By creating a baseline and identifying normal business processes and what appear to be abnormal activities, the system automatically suggests policies you can use to prevent attacks such as SQL injection. Intuitive menus make it easy to add custom policies.

Proactive, real-time security

InfoSphere Guardium provides real-time controls for responding to unauthorized or anomalous behaviors before they can do significant harm. Policy-based actions can include real-time security alerts (SMTP, SNMP, Syslog); software blocking; full logging; user quarantines; and custom actions such as shutting down VPN ports and coordinating with perimeter IDS/IPS systems.

Tracking and resolving security incidents

Compliance regulations require organizations to demonstrate that all incidents are recorded, analyzed, resolved in a timely manner and reported to management. InfoSphere Guardium provides a business user interface and workflow automation for resolving security incidents, along with a dashboard for tracking key metrics such as number of open incidents, severity levels and length of time incidents have been open.

Audit and report

Growing volumes of data, often physically distributed throughout an enterprise, are making it increasingly difficult for organizations to capture and analyze the detailed audit trails required for validating compliance.

Capturing a granular audit trail

InfoSphere Guardium creates a continuous, fine-grained trail of database activities that is contextually analyzed and filtered in real time to implement controls and produce the specific information required by auditors.

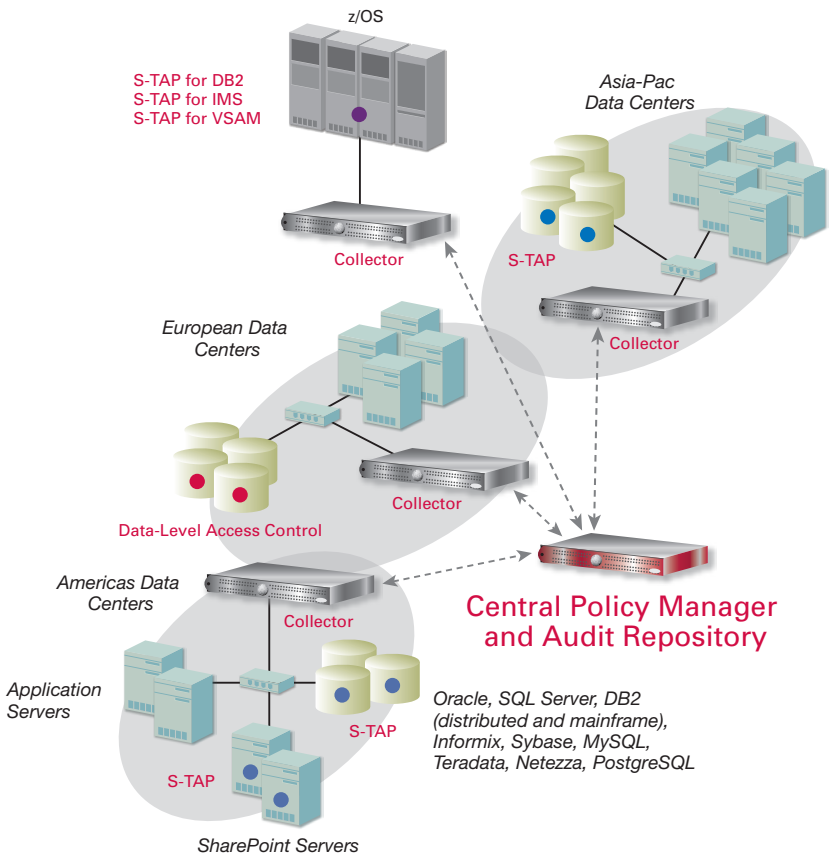
The resulting reports demonstrate compliance by making it possible to view database activities in detail, such as login failures, escalation of privileges, schema changes, access during off-hours or from unauthorized applications and access to sensitive tables. For example, the system monitors:

- Security exceptions such as SQL errors
- Commands such as CREATE/DROP/ALTER that change structures, which are particularly important for data governance regulations such as SOX
- SELECT/READ/OPEN commands, which are particularly important for data privacy regulations such as PCI DSS
- Data manipulation commands (for example, INSERT, UPDATE, DELETE), including bind variables
- Data Control Language commands that control accounts, roles and permissions (GRANT, REVOKE)
- Procedural languages supported by each DBMS platform such as PL/SQL (Oracle) and SQL/PL (IBM)
- XML executed by the database
- Changes to Microsoft SharePoint objects

Enterprise-wide scalability with minimized costs

InfoSphere Guardium scales easily, using built-in automation and integration functions to reduce operational costs while adapting to changes in audit requirements and the environment. Irrespective of system size, InfoSphere Guardium simplifies operations, providing:

- **A single solution**. Comprehensive platform support and broad functionality, including proactive protection, enables deployment of a single solution enterprise wide.
- **Noninvasive design**. No changes to existing database, application or network configurations are required and there is no reliance on native logging, minimizing performance impact.
- **Investment protection**. As the number of servers to monitor increases, you can simply add capacity to preserve existing InfoSphere Guardium purchases and configuration investments such as policies and compliance workflow.
- **Simple administration**. A single interface is used to manage appliances and probes, including configuration, user management and software updates. Probes are updated without reboot.
- **Enterprise-wide analysis and reporting**. Audit information — from multiple database platforms and collectors — is automatically normalized and aggregated into a single, secure, centralized audit repository with advanced reporting and analytics
- **Task automation**. Capabilities that eliminate manual tasks, such as integrated compliance workflow automation, extensive API support for script based automation, configuration auditing templates, automated information sharing between functions and more, are included in the system.
- **Deployment flexibility**. Delivery as preconfigured appliances, in hardware and software form, supports a range of cost reduction strategies. Monitoring with lightweight host-based probes, over the network, or any combination is supported, maximizing visibility.
- **Infrastructure integration**. Automated interaction with systems, including LDAP, administrative databases, email, change ticketing and Syslog, eliminates manual exchanges of security information.



A scalable multi-tier architecture supports large and small environments, with centralized aggregation and normalization of audit data and centralized management of security policies enterprise wide. S-TAPs are lightweight, host-based probes that are able to monitor database traffic, including local access by privileged users, and relay it to InfoSphere Guardium collector appliances for analysis and reporting. Collector appliances gather monitored data from S-TAPs or by connecting directly to SPAN ports in network switches. Aggregators automatically assemble audit data from multiple collector appliances. Multiple tiers of aggregators can be configured for greater flexibility and scalability. Implemented as an extension to S-TAP, the InfoSphere Guardium Data-Level Access Control strengthens security and enforces separation of duties by blocking DBAs from creating new database accounts, elevating privileges for existing accounts and more.

Best-in-class reporting

The InfoSphere Guardium solution includes more than 150 preconfigured policies and reports based on best practices and our experience working with Global 1000 companies, major auditors and assessors around the world. These reports help address regulatory requirements such as SOX, PCI DSS and data privacy laws, and they help streamline data governance and data privacy initiatives.

In addition to prepackaged report templates, InfoSphere Guardium provides a graphical drag-and-drop interface for easily building new reports or modifying existing reports. Reports can be automatically sent to users in PDF format (as email attachments) or as links to HTML pages. They can also be viewed online in the web console or exported to SIEM and other systems in standard formats.

Compliance workflow automation

The InfoSphere Guardium Compliance Workflow Automation application streamlines the entire compliance workflow process, helping automate audit report generation, distribution to key stakeholders, electronic sign-off and escalations. Workflow processes are completely user customizable; specific audit items can be individually routed and tracked through sign-off.

Unified solution for heterogeneous environments

Most organizations have databases from a variety of vendors deployed on a range of operating systems, making it difficult to enforce uniform security policies and gather consistent audit information enterprise-wide. Heterogeneous environments can also result in taking a silo approach to security and compliance activities, driving up operational costs and consuming scarce resources.

Broad platform support

All major DBMS platforms and protocols running on major operating systems, along with a growing range of file and document-sharing environments, are supported.

Supported Platform	Supported Versions
Oracle Database	8i, 9i, 10g (r1, r2), 11g, 11gr2
Oracle Database (ASO, SSL)	9i, 10g (r1, r2), 11g
Microsoft SQL Server	2000, 2005, 2008
Microsoft SharePoint	2007, 2010
IBM DB2® (Linux, UNIX, Linux for System z)	9.1, 9.5, 9.7
IBM DB2 (Windows)	9.1, 9.5, 9.7
IBM DB2 pureScale®	9.8
IBM DB2 for z/OS	8.1, 9.1, 10.1
IBM IMS™	9, 10, 11, 12
IBM VSAM	See OS support table
IBM DB2 for IBM iSeries®	V5R2, V5R3, V5R4, V6R1
IBM Informix®	7, 9, 10, 11,11.50, 11.7
Sun MySQL and MySQL Cluster	4.1, 5.0, 5.1
Sybase ASE	12, 15, 15.5
Sybase IQ	12.6, 12.7, 15
IBM Netezza®	NPS 4.5, 4.6, 4.6.8, 5.0, 6.0
PostgreSQL	8,9
Teradata	6.X, 12, 13, 13.10
FTP	

Host-based monitoring

S-TAPs are lightweight software probes that monitor both network and local database protocols (for example, shared memory, named pipes) at the operating system level of the database server. S-TAPs minimize any effect on server performance by relaying all traffic to separate InfoSphere Guardium appliances for real-time analysis and reporting, rather than relying on the database itself to process and store log data. S-TAPs are often preferred because they eliminate the need for dedicated hardware appliances in remote locations or available SPAN ports in your data center.

OS Type	Version	32-bit and 64-bit
IBM AIX®	5.2, 5.3,	Both
	6.1, 7.1	64-bit
HP-UX	11.11, 11.23, 11.31	Both
Red Hat Enterprise Linux	3, 4, 5	Both
Red Hat Enterprise Linux for System z	5.4	
SUSE Enterprise Linux	9, 10, 11	Both
SUSE Enterprise Linux for System z	9, 10, 11	
Solaris — SPARC	8, 9, 10, 11	Both
Solaris — Intel/AMD	10	Both
	11	64-bit
Tru64	5.1A, 5.1B	64-bit
Windows	2000, 2003, 2008	Both
iSeries	IBM i5/OS®*	
z/OS	1.10 (5694-A01) or later	

** Supports network activity monitoring, local activity support with Enterprise Integrator*

Application monitoring

InfoSphere Guardium identifies potential fraud by tracking activities of users who access critical tables with multi-tier enterprise applications rather than direct access to the database. This is required because enterprise applications typically use an optimization mechanism called "connection pooling." In a pooled environment, all user traffic is aggregated in a few database connections that are identified only by a generic application account name, thereby masking the user identities. InfoSphere Guardium supports application monitoring for all major off-the-shelf enterprise applications. Support for other applications, including in-house applications, is provided either by monitoring transactions at the application server level or by interfacing them to the InfoSphere Guardium universal feed. IBM provides documentation of the universal feed protocol, which enables organizations to implement an interface to support any subset of the monitoring and protective features supported by InfoSphere Guardium appropriate for their unique environments.

Supported Enterprise Applications	• Oracle E-Business Suite • PeopleSoft • Siebel • SAP • Cognos • Business Objects Web Intelligence
Supported Application Server Platforms	• IBM WebSphere • BEA WebLogic • Oracle Application Server (AS) • JBoss Enterprise Application Platform

About IBM InfoSphere Guardium

InfoSphere Guardium is part of the IBM InfoSphere integrated platform for defining, integrating, protecting and managing 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.

IBM Corporation
Route 100
Somers, NY 10589

Produced in the United States of America
August 2011

Please Recycle

InfoSphere.
software

IMD14286-CAEN-02