IBM InfoSphere Guardium

Managing the Entire Database Security and Compliance Lifecycle

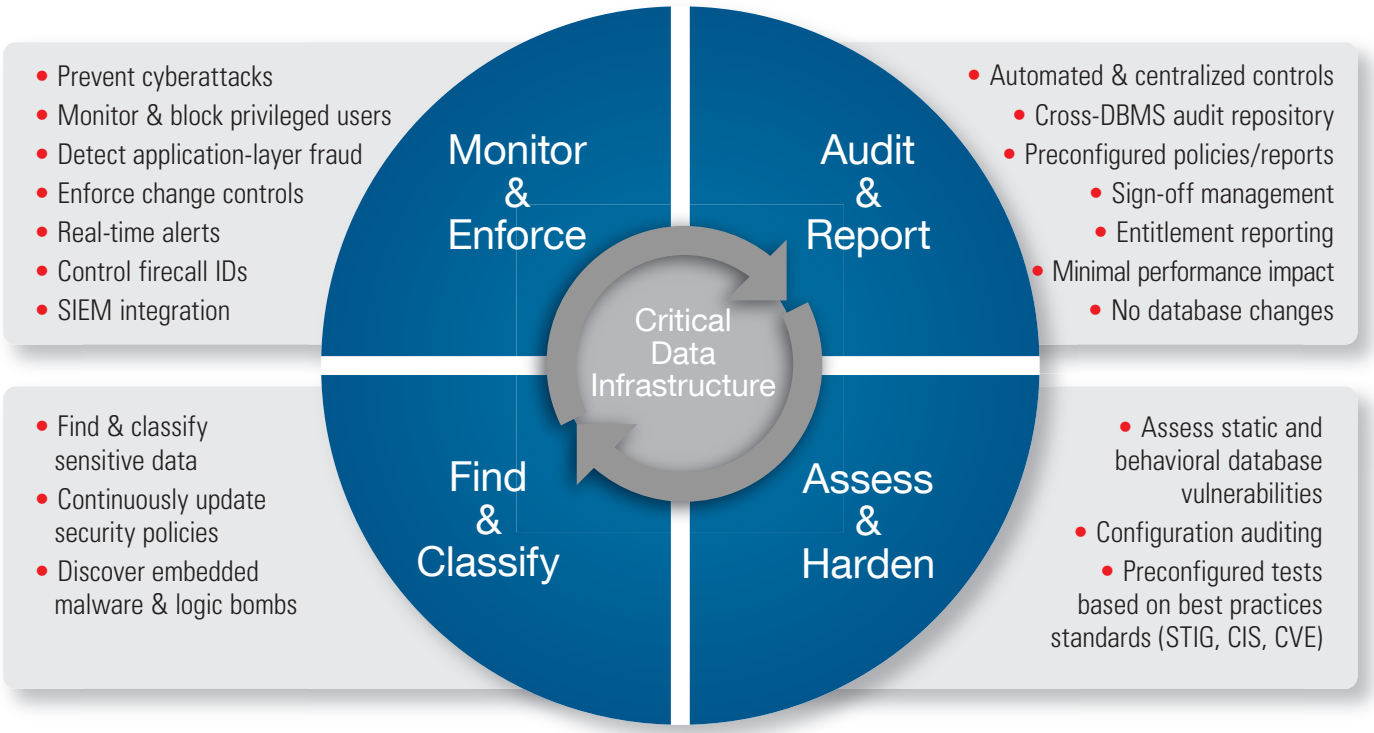
More Global 1000 organizations trust IBM to secure their critical enterprise data than any other technology provider. The fact is, we provide the simplest, most robust solution for safeguarding financial and ERP information, customer and cardholder data, and intellectual property stored in your enterprise systems.

Our enterprise security platform prevents unauthorized or suspicious activities by privileged insiders and potential hackers. It also monitors potential fraud by end-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 virtually zero 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 & Monitoring



Unified Solution: Built upon 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 lifecycle.

InfoSphere Guardium is the only solution that addresses the entire database security and compliance lifecycle with a unified Web console, back-end data store and workflow automation system, enabling you to:

- Locate and classify sensitive information in corporate databases.
- Assess database vulnerabilities and configuration flaws.
- Ensure configurations are locked down after recommended changes are implemented.
- Provide 100% visibility and granularity into all database transactions – across all platforms and protocols – with a secure, tamper-proof audit trail that supports separation of duties.
- Track activities on major file sharing platforms like Microsoft SharePoint.
- Monitor and enforce policies for sensitive data access, privileged user actions, change control, application user activities and security exceptions such as failed logins.
- Automate the entire compliance auditing process – including report distribution to oversight teams, sign-offs and escalations – with pre-configured reports for SOX, PCI 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 & Classify

Automatically locates, classifies and secures sensitive information

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

This is especially challenging for organizations that have experienced mergers and acquisitions, or environments where legacy 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, etc.).
- 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.

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/or changed by authorized users.

Sensitive data discovery can also be scheduled to execute on a regular basis, in order to prevent the introduction of rogue servers and ensure that no critical information is "forgotten."

Assess & Harden

Vulnerability, configuration and behavioral assessment
InfoSphere Guardium's database security assessment 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) as well as platform-specific vulnerabilities, which are updated on a regular basis via InfoSphere Guardium's Knowledge Base service. You can also define custom tests to match specific requirements. The assessment module also flags compliance-related vulnerabilities such as unauthorized access to reserved Oracle EBS 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 the ways in which databases are being accessed and manipulated — such as an excessive number of failed logins, clients executing administrative commands, or after-hours logins — by monitoring all database traffic in real-time.

In addition to producing detailed reports with drill-down capabilities, the assessment module generates a security health report card with weighted metrics (based on best practices), industry standard reference numbers, and recommends concrete action plans to strengthen database security.

Configuration lock-down and change tracking
Once you have implemented the recommended actions generated by the vulnerability assessment, you can now establish a secured configuration baseline. Using InfoSphere Guardium's Configuration Audit System (CAS), you can monitor any changes to this baseline, and make sure that changes are not made outside of your authorized change control policies and processes.

Monitor & Enforce

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 as well as attacks from rogue users or outsiders. You can also identify application users that make unauthorized changes to databases via multi-tier applications that access databases via a common service account, such as Oracle EBS, PeopleSoft, Siebel, SAP, Cognos and custom systems built on application servers such as IBM WebSphere, Oracle WebLogic, and Oracle AS.

The solution can be managed by information security personnel without requiring involvement by database administrators (DBAs). You can also define granular access policies that restrict access to specific tables based on OS 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 patent-pending linguistic analysis to detect unauthorized actions based on detailed contextual information – the "who, what, where, when and

how" of each SQL transaction. This unique approach minimizes false positives and negatives while providing an unprecedented 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 both 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. Custom policies can easily be added via intuitive drop-down menus.

Proactive, real-time security

InfoSphere Guardium provides an arsenal of real-time controls for proactively responding to unauthorized or anomalous behaviors. Policy-based actions can include real-time security alerts (SMTP, SNMP, Syslog); software blocking; enable full logging; quarantine users; and custom actions such as VPN port shut-downs and coordination 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 & Report

Capturing a granular audit trail

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

The resulting reports demonstrate compliance by providing detailed visibility into all database activities such as failed logins, escalation of privileges, schema changes, access during off-hours or from unauthorized applications, and access to sensitive tables. For example, the system monitors all:

- Security exceptions such as SQL errors and failed logins.
- DDL commands such as Create/Drop/Alter Tables that change database structures, which are particularly important for data governance regulations such as SOX.
- SELECT queries, which are particularly important for data privacy regulations such as PCI DSS.
- DML commands (Insert, Update, Delete) including bind variables.
- DCL 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 SharePoint objects.

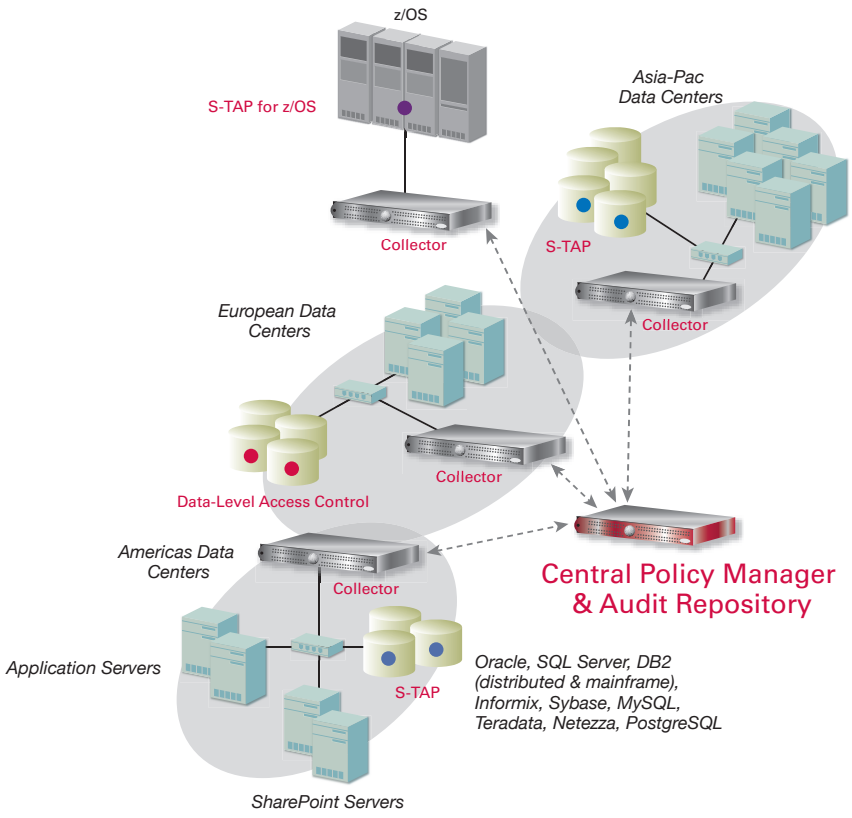
Best-in-class reporting

The InfoSphere Guardium solution includes more than 150 preconfigured policies and reports based on best practices and our experience working with Global 1000 companies, Big 4 auditors and assessors around the world. These reports help address regulatory requirements such as SOX, PCI DSS, and data privacy laws, and 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 e-mailed to users in PDF format (as attachments) or as links to HTML pages. They can also be viewed online via the Web console interface, or exported to SIEM and other systems in standard formats.

Scalable for Your Enterprise

- **Non-Invasive:** 100% visibility into all database transactions – including local access by privileged users – with minimal performance impact and no database or application changes.
- **DBMS-Independent:** Cross-platform solution that does not rely on native logging or auditing.
- **Appliance-Based:** Modular software suite, built on a hardened Linux kernel, for rapid deployment via "black box" appliances (self-contained storage, preinstalled applications, built-in management). Also available as a virtual appliance to support hardware consolidation strategies.
- **Flexible Monitoring:** Via lightweight host-based probes, SPAN ports, network TAPs or any combination.
- **Infrastructure-Ready:** Supports SNMP, SMTP, Syslog, LDAP, Kerberos, RSA SecurID®, change ticketing systems such as BMC Remedy, CEF and integration with all major SIEM platforms.
- **Multi-Tier:** Unique in the industry, InfoSphere Guardium automatically aggregates and normalizes audit information – from multiple database platforms and locations – into a single centralized audit repository.
- **Centralized Management:** Enterprise-wide management of cross-DBMS security policies via Web console.
- **Scalable:** As the number of monitored servers or traffic volume increases, simply add appliances to handle the increased load. Patented, intelligent storage algorithms provide 100x better storage efficiency than traditional flat file-based approaches.
- **Tamper-Proof Audit Repository:** Strong authentication with no root access and encrypted archives.
- **Role-Based:** Access to modules and data is controlled according to organizational roles.



Scalable Multi-Tier Architecture

InfoSphere Guardium's scalable architecture supports both large and small environments, with centralized aggregation and normalization of audit data, and centralized management of security policies via a Web console – enterprise-wide. S-TAPs are lightweight, host-based probes that monitor all 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 and/or by connecting directly to SPAN ports in network switches. Aggregators automatically aggregate audit data from multiple collector appliances. For maximum scalability and flexibility, you can configure multiple tiers of aggregators. Implemented as an extension to S-TAP, InfoSphere Guardium's Data-Level Access Control also strengthens security and enforces separation of duties by blocking DBAs from performing security functions such as creating new database accounts and elevating privileges for existing accounts.

Compliance workflow automation

Unique in the industry, InfoSphere Guardium's Compliance Workflow Automation application streamlines the entire compliance workflow process, helping to automate the process of audit report generation, distribution to key stakeholders, electronic sign-offs, and escalations. Workflow processes are completely user customizable at a detailed level, enabling specific audit items to be individually routed and tracked through sign-off.

Unified Solution for Heterogeneous Environments

Broad platform support

InfoSphere Guardium's cross-platform solution supports all major DBMS platforms and protocols running on all major operating systems (Windows, UNIX, Linux, z/OS), as well as Microsoft SharePoint and FTP environments:

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, 9.2, 9.5, 9.7
IBM DB2 for z/OS	7, 8, 9
IBM DB2 for iSeries	V5R2, V5R3, V5R4, V6R1
IBM Informix	7, 9, 10, 11,11.50
Sun MySQL and MySQL Cluster	4.1, 5.0, 5.1
Sybase ASE	12, 15, 15.5
Sybase IQ	12.6, 15
Netezza	4.5
PostgreSQL	8
Teradata	6.X, 12, 13
FTP	

Host-based monitoring

Unique in the industry, S-TAPs are lightweight software probes that monitor both network and local database protocols (shared memory, named pipes, etc.) at the OS 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 & 64-Bit
AIX	5.2, 5.3	Both
	6.1	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	Both
Solaris - Intel/AMD	10	Both
Tru64	5.1A, 5.1B	64-Bit
Windows	2000, 2003, 2008	Both
iSeries	i5/OS*	

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

Application monitoring

InfoSphere Guardium identifies potential fraud by tracking activities of end-users who access critical tables via 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 within a few database connections that are identified only by a generic application account name, thereby masking the identity of end-users. InfoSphere Guardium supports application monitoring for all major off-the-shelf enterprise applications. Support for other applications, including in-house applications, is provided by monitoring transactions at the application server level.

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

Guardium is part of IBM InfoSphere, an integrated platform for defining, integrating, protecting and managing trusted information across 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 around a core of shared metadata and models. The portfolio is modular, allowing you to 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 provides 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

May 2010

Please Recycle

InfoSphere.
software