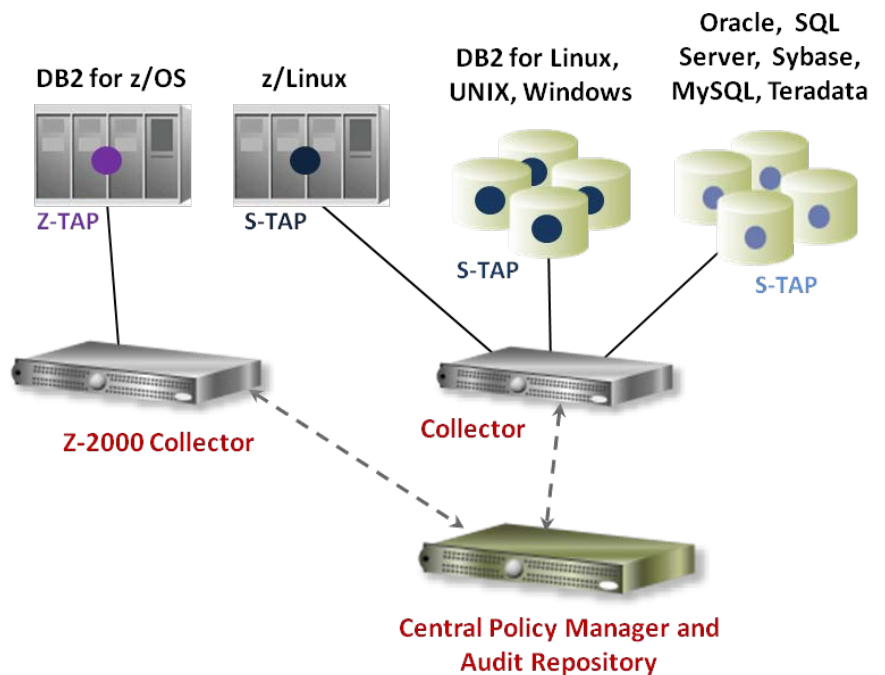


# Guardium for Mainframes

## 100% Auditing Visibility for DB2 – Without Performance Impact of Native Logging

### Highlights

- 100% visibility at a granular level into all critical operations, including:
  - SELECTS, DML and DDL
  - DB2 utilities
  - Access grants and revokes
- Uses zIIP specialty processors, reducing general CPU usage
- Monitors and audits all activity for privileged users, mainframe-resident applications and network clients
- All analysis, reporting and storage of log data is performed off-mainframe
- Provides fine-grained audit information, real-time security alerts and separation of duties not available with traditional log-based approaches—with minimal performance impact
- Integrates with the Guardium architecture to provide a unified solution for both mainframe and distributed database environments
- Centralized cross-DBMS audit repository for enterprise-wide compliance reporting, investigations and forensics
- Secure tamper-proof audit trail
- Automates entire compliance process including report distribution to oversight teams, sign-offs and escalations
- Preconfigured reports for SOX, PCI DSS and data privacy regulations
- Scalable multi-tier architecture with centralized cross-DBMS policies
- Chosen by more Global 1000 organizations than any other database security and compliance solution
- IBM Information On Demand Specialty Accreditation
- IBM Advanced Industry-Optimized status for Financial Markets
- Member of IBM Data Governance Council
- Seamless integration tested at IBM Innovation Centers



**Figure 1:** Guardium uses a lightweight mainframe-resident probe (Z-TAP) to capture all database activities by privileged users, mainframe-resident applications and network clients. Both mainframe and distributed environments can be managed from a single console; in addition, all audit data is automatically aggregated and normalized into a single centralized repository.

### Burgeoning DB2 Security and Compliance Requirements

Many organizations host extensive amounts of information in mainframe databases which are both sensitive and mission critical. Financial, personnel and customer records are among the information commonly found in these environments.

As a result, compliance requirements and audits often involve mainframe data; compelling IT security organizations to ensure their DB2 data is secure from unauthorized access and tampering by both internal and external parties.

Guardium offers a simple yet powerful means of securing critical data across the enterprise. It provides real-time detection of anomalous activities that violate corporate policies, policy-based responses such as alerts, auditable workflow to ensure appropriate resolution, along with automated reporting features which simplify validation of compliance with regulations such as SOX, Data Privacy and PCI DSS.

Guardium for Mainframes provides these capabilities for DB2 on z/OS. The solution can be used independently for the mainframe environment only, or integrated with other Guardium database security and compliance components across the enterprise (see Figure 1), to provide a secure, centralized audit repository and management point.

## Avoid Performance and Security Penalties Typically Associated With Monitoring DB2 Data on z/OS

Historically organizations seeking to monitor and secure their valuable DB2 data on z/OS have utilized logging utilities such as trace or transaction logs. These solutions, as well as others built upon them, such as log and audit management products, suffer from a variety of limitations, including:

- Significant performance impact on the mainframe
- Reliance on mainframe DBA's for administration; failing to provide the separation of duties (SOD) required by auditors
- Failure to capture all critical activities required by auditors (such as read operations when using Logging or SQL statements when using Trace)
- Lack of real-time capability; eliminating the possibility of prevention and containment

Guardium for Mainframes eliminates these limitations, while providing important additional capabilities such as automated reporting and workflow.

## Simple, Scalable Enterprise Database Security and Compliance Platform

Guardium for Mainframes does not rely on any native Log or Trace capabilities in z/OS, nor does it require any changes to the database. Lightweight software probes called Z-TAPs capture all database activities by privileged users, mainframe-resident applications and network clients, including those connecting via services such as JDBC or DB2 Connect. This means that all critical operations such as SELECTS, DML, DDL and access grants are captured without sacrificing performance or availability. Z-TAPs send information specified by user defined policies to Z-2000 Collector appliances, ensuring the mainframe is not burdened with incremental storage or processing requirements, network traffic is limited and a full audit trail is stored securely.

Guardium for Mainframes Requirements	
Software	Version
IBM z/OS	V1.6 or later (64-bit mode required)
IBM TCP/IP	V3.1 or later
DB2 for z/OS	V7, 8, 9, 9.5

Unique in the industry, Guardium's multi-tier architecture (see Figure 1) can optionally aggregate and normalize audit information – from multiple systems and locations – into a single centralized repository. This provides comprehensive enterprise-wide compliance reporting, correlation, forensics, and advanced database-focused analytics. Users starting with a mainframe implementation can easily scale up to support any mix of databases and systems, simply by adding appropriate Probes, Collectors and Aggregators, which work together in a federated model.

## Comprehensive Policy-Based Monitoring and Auditing Simplifies Compliance Validation

Guardium's graphical Web console provides centralized management of policies, report definitions, compliance workflow processes, and appliance settings (such as archiving schedules) without the involvement of DBAs, providing required SOD. Features include the ability to:

- Define granular access policies using indicators of possible risk appropriate for your particular environment, including data object, type of SQL command, user ID, client IP address, source application or time-of-day
- Automatically create a baseline of normal activities to suggest policies which will detect anomalous activities such as SQL injection attacks
- Define actions in response to policy violations, such as generating alerts and logging incident details
- Automate compliance workflow for routine activities as well as incident responses, including steps such as sign-offs, commenting and escalation
- Run hundreds of out-of-the box reports including those required for SOX, PCI DSS and data privacy laws, as well as create customized reports

**Figure 2:** Granular access policies can be easily built with Guardium's web-based Centralized Policy Manager.

With Guardium, you gain full visibility into your DB2 environment, enabling activities like data tampering or hacking to be identified and addressed in real-time. Automation of the entire security and compliance lifecycle reduces labor costs, facilitates communication across the organization, and streamlines audit preparation.

Start Date: 2008-07-08 05:30:00		End Date: 2008-07-08 23:59:59						
Timestamp	Server Type	Client IP	OS User	Source Program	Server IP	Network Protocol	DB User Name	Full Sql
2008-07-08 03:25:04.0	DB2	10.37.100.26	NESQA	NSUQAG	10.37.100.26	LOCAL	NESQA/NESQA	SELECT FIRSTNME, MIDINIT, LASTNAME FROM NSUQA1.EMP WHERE EMPNO = 'TSTJ40'
2008-07-08 03:25:04.0	DB2	10.37.100.26	NESQA	NSUQAG	10.37.100.26	LOCAL	NESQA/NESQA	SELECT FIRSTNME, MIDINIT, LASTNAME FROM NSUQA1.EMP WHERE EMPNO = 'TSTDD0' FOR FETCH ONLY
2008-07-08 03:25:04.0	DB2	10.37.100.26	NESQA	NSUQAG	10.37.100.26	LOCAL	NESQA/NESQA	UPDATE NSUQA1.EMP SET FIRSTNME = 'NEWTESTFNAME', LASTNAME = 'NEWTESTLNAME', MIDINIT = 'N' WHERE EMPNO = 'TSTJ20'
2008-07-08 03:25:04.0	DB2	10.37.100.26	NESQA	NSUQAG	10.37.100.26	LOCAL	NESQA/NESQA	UPDATE NSUQA1.EMP SET FIRSTNME = 'NEWTESTFNAME', LASTNAME = 'NEWTESTLNAME', MIDINIT = 'N' WHERE EMPNO = 'TSTJ40'
2008-07-08 04:57:46.0	DB2	11.100.37.10	DGD1DIS	DGD1DIST	10.37.100.26	DRDA	SAS1/SAS1	ALTER DATABASE NSUJC4DA BUFFERPOOL BP0
2008-07-08 04:57:46.0	DB2	11.100.37.10	DGD1DIS	DGD1DIST	10.37.100.26	DRDA	SAS1/SAS1	ALTER DATABASE NSUJ2DA BUFFERPOOL BP0

**Figure 3:** Guardium provides full visibility into DB2 data usage, capturing both mainframe and network access with key details such as user name, client IP, SQL statements executed and accessing programs.

## Guardium for IBM Environments

Guardium provides comprehensive support for the most popular IBM database platforms and applications including:

- IBM DB2 UDB 9 for z/OS
- IBM DB2 for IBM i (AS/400)
- IBM DB2 8, 9, 9.5 for Linux, UNIX and Windows
- Cognos 8, for which Guardium identifies fraud and other unauthorized activities via application-layer monitoring, in addition to previous support for enterprise applications such as SAP, PeopleSoft and SOA applications developed for IBM WebSphere Application Server and other middleware platforms.
- IBM Informix 9, 10, 11, 11.5
- System z Red Hat Enterprise Linux and SUSE Linux Enterprise Server for System z, providing coverage for all major DBMS platforms (Oracle, MySQL, etc.) running in the IBM z/VM hypervisor.

## About the Guardium Platform

Guardium's real-time database security and monitoring solution monitors access to sensitive data, across all major DBMS platforms and applications, without impacting performance or requiring changes to databases or applications.

The solution prevents unauthorized or suspicious activities by privileged insiders, potential hackers, and end-users of enterprise applications such as SAP, Oracle EBS, PeopleSoft, Siebel, Business Intelligence and in-house systems. Additional modules are available for performing database vulnerability assessments, change and configuration auditing, data-level access control and blocking, data discovery and classification, and compliance workflow automation.

Forrester Research recently named Guardium "a Leader across the board," with "dominance and momentum on its side." Guardium earned the highest overall scores for Architecture, Current Offering and Corporate Strategy ("The Forrester Wave: Enterprise Database Auditing And Real-Time Protection, Q4 2007" by Noel Yuhanna, October 2007).

## About Guardium

Guardium, [the database security company](#), delivers the most widely-used solution for preventing information leaks from the data center and ensuring the integrity of enterprise data.

The company's enterprise security platform is now installed in more than 450 data centers worldwide, including 5 of the top 5 banks; 3 of the top 5 insurers; top government agencies; 2 of the top 3 retailers; 15 of the world's top telcos; 2 of the world's favorite beverage brands; the most recognized name in PCs; a top 3 auto maker; a top 3 aerospace company; and a leading supplier of business intelligence software.

Guardium has partnerships with Accenture, ArcSight, BMC, EMC/RSA, IBM, McAfee, Microsoft, Oracle, Sybase and Teradata, with [Cisco as a strategic investor](#), and is a member of IBM's prestigious [Data Governance Council](#) and the [PCI Security Standards Council](#).

Founded in 2002, Guardium was the first company to address the core data security gap by delivering a scalable, cross-DBMS enterprise platform that both protects databases in real-time and automates the entire compliance auditing process.

