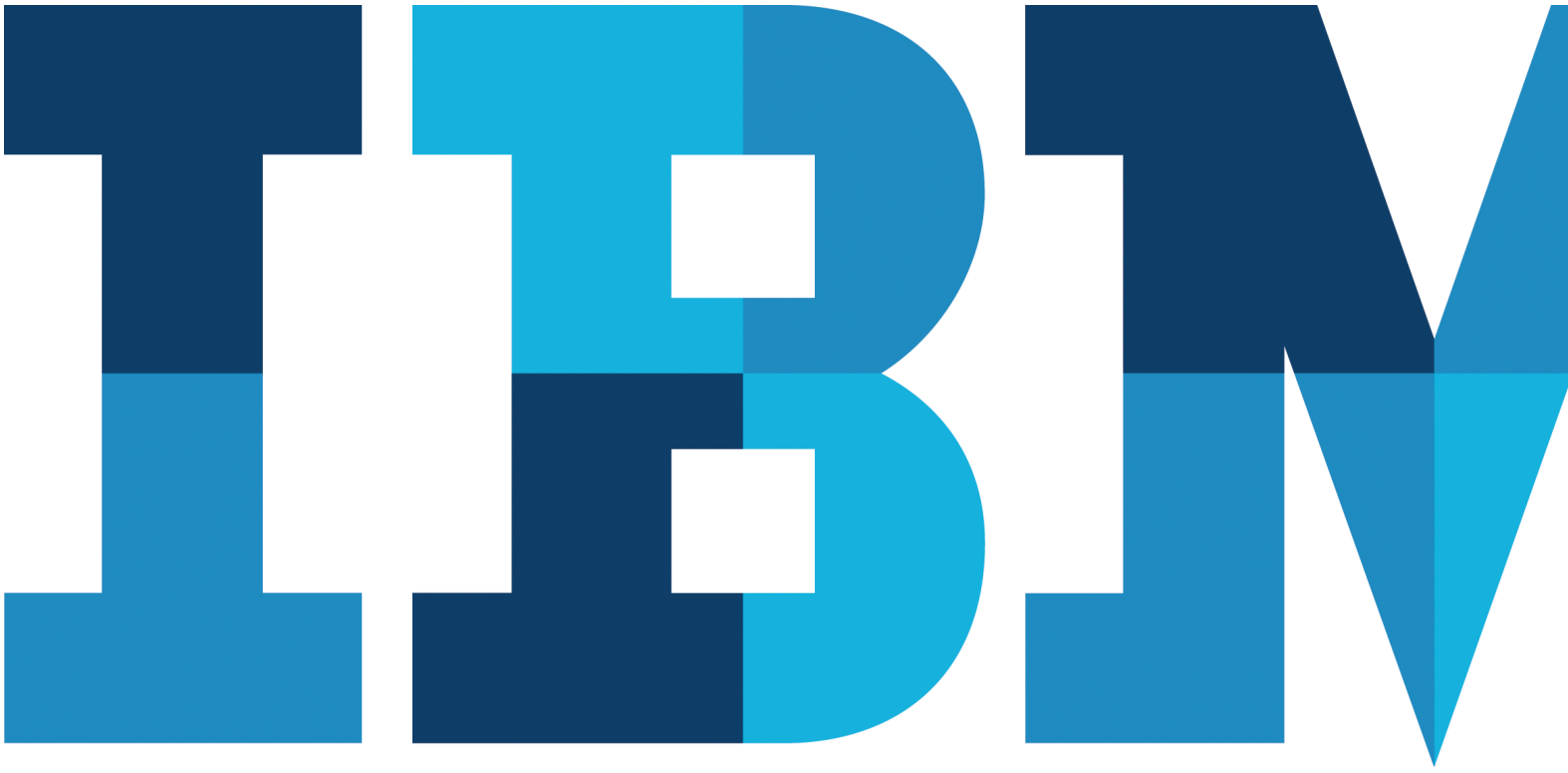
IBM InfoSphere Guardium Optional Capabilities



IBM

Contents

InfoSphere Guardium Overview	**3**
Advanced Compliance Workflow Automation	**5**
Database Vulnerability Assessment	**8**
Database Protection Knowledge Base	**12**
Data-Level Access Control	**15**
Entitlement Reports	**18**
Configuration Audit System for Database Servers	**21**
Application End-User Identifier	**26**
Enterprise Integrator	**30**
IBM InfoSphere Guardium for z/OS	**34**
IBM InfoSphere Guardium Collector Hardware Unit	**37**
IBM InfoSphere Guardium Aggregator Hardware Unit	**38**

InfoSphere Guardium Overview

InfoSphere Guardium provides the simplest, most robust solution for safeguarding your entire application and database infrastructure, including:

- Real-time database activity monitoring (DAM) for proactively identifying unauthorized or suspicious activities, preventing attacks and blocking unauthorized access by privileged users.
- Auditing and compliance solutions for automating and simplifying validation activities related to PCI DSS, SOX, SAS70, ISO 27001/2, NIST 800-53 and data privacy regulations.
- Change control solutions for preventing unauthorized changes to databases, privileges and configurations.
- Vulnerability management solutions for identifying and resolving database vulnerabilities such as missing patches, misconfigured privileges and default accounts.
- Fraud prevention solutions with application layer monitoring to identify unauthorized activities by application users (SAP, PeopleSoft, Oracle EBS, Cognos, etc.).
- Database leak prevention for locating sensitive data and thwarting data center breaches.

The solution is now installed in more than 400 customers worldwide, including 5 of the top 5 global banks; 4 of the top 6 insurers; top government agencies; 2 of the top 3 retailers; 20 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. InfoSphere Guardium was the first solution to address the core data security gap by delivering a scalable enterprise platform that both protects databases in real-time and automates the entire compliance auditing process.

This solution brief provides an overview of a variety of optional capabilities available for InfoSphere Guardium. For a more complete overview of the core InfoSphere Guardium solution, please see the InfoSphere Guardium brochure.

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.

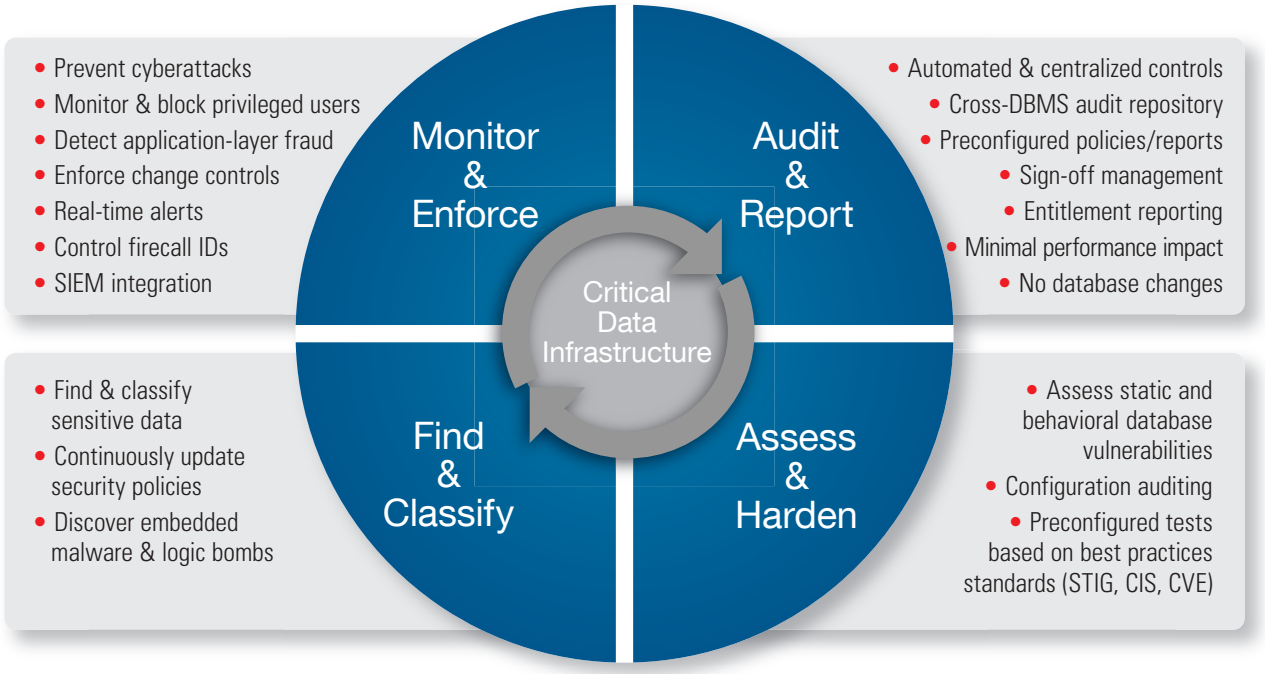


Figure 1: Built upon a single unified console and back-end data store, InfoSphere Guardium offers a family of integrated modules for managing the entire database security and compliance lifecycle.

Advanced Compliance Workflow Automation

Automate Oversight Processes to Reduce Operational Costs

- Centralize and automate oversight processes enterprise-wide, including report generation, distribution, electronic sign-offs and escalations
- Easily create custom processes by specifying your unique combination of workflow steps, actions and users
- Enable automated execution of oversight processes on a report line item basis, maximizing process efficiency without sacrificing security
- Ensure oversight team members only see data and tasks related to their own roles
- Improve process efficiency with real-time tools for centralized process management
- Store process results in a secure centralized repository, along with granular audit data for compliance and forensic use

Managing Enterprise-wide Oversight Processes

Driven by growing compliance mandates and increased focus on data security and privacy, organizations have put in place a variety of processes to review the results of regularly scheduled monitoring activities, as well as to investigate and remediate incidents of controls violations. For example, an organization may review incident reports on a daily basis, while database vulnerability assessments and database discovery processes are run and reviewed on a weekly basis.

Most enterprises have hundreds, if not thousands or tens of thousands of databases, managed and overseen by a variety of organizations including security and IT groups. These in turn may be organized by division, geography, system functionality and other factors. This complexity typically directly impacts oversight processes, requiring a variety of different processes, each with its own unique sequence of review steps, actions and participants.

Manual Processes Increase Operational Costs and Audit Exceptions

Traditionally, organizations have managed their oversight processes manually, relying on tools like email and spreadsheets to record events, distribute information to appropriate parties for investigation, capture remediation activities and document comments. Given the variety and complexity of processes, resultant operational costs are high, and audit exceptions resulting from process break-downs are frequent. Retrieving historical results for forensic purposes is equally challenging, since oversight information is stored in a variety of formats, sometimes in different physical locations.

Automating Oversight Processes to Improve Operational Efficiency

The Advanced Compliance Workflow Automation module automates the entire security and compliance workflow process, eliminating manual tasks and ensuring timely completion of oversight activities. 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. New processes can be created with a few simple steps:

1. Create a custom workflow comprised of individual event states and actions (see Figure 2).
2. Assign one or more individuals or roles to actions to be performed. Actions can optionally require electronic sign-off. Parallel actions are allowed, supporting processes where actions are segmented by various criteria (for instance the review of exceptions generated by different DBMS's may be signed-off by different parties).
3. Create and schedule an audit process to execute the workflow automatically on a regular basis (see Figure 3).
4. Add any combination of tasks to each audit process. For example, several reports that are to be executed and reviewed on a weekly basis using the same workflow can be assigned to the same audit task. A wide variety of audit tasks are supported, including reviewing the results of automatically generated vulnerability assessments, asset discovery, data classification, configuration auditing and database activity monitoring reports.

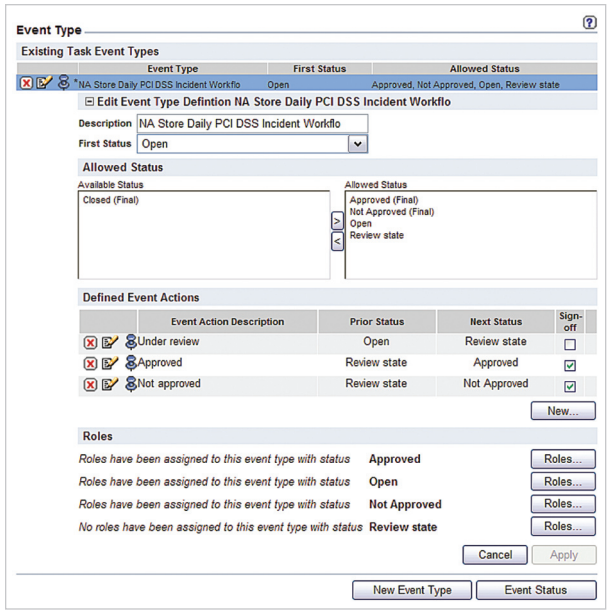


Figure 2: InfoSphere Guardium's Advanced Compliance Workflow Automation module allows users to easily create workflows that are customized to each of their own unique processes by specifying the appropriate combination of actions, event states and roles through a simple graphical user interface.

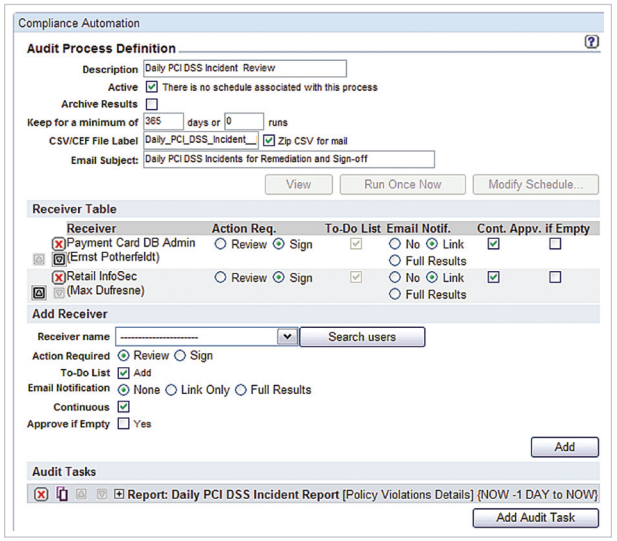


Figure 3: Workflow can be automatically initiated on a scheduled basis, ensuring recurring tasks such as daily incident reviews and vulnerability assessments are consistently executed and tracked.

Improving Security with Granular Workflow Controls

Individuals to whom actions have been assigned are notified of specific actions required on their part as the workflow process is executed, using automatic email notification as well as updates of the "To-Do" list on their InfoSphere Guardium web interface. All required actions can be securely executed through the web, including reviewing results, providing approvals, commenting and escalating an action.

Actions are executed on a line-item basis, allowing rapid but thorough review, and ensuring processes are not blocked by individual line items requiring investigation. For example an individual receiving a daily PCI DSS exception report may find it contains five incidents, four of which were caused by a known issue that has been resolved. Those four line items can quickly be marked as reviewed and approved; while the fifth item will not be approved until the incident is investigated and resolved. The four approved items will proceed to the next step in the workflow process immediately; with the fifth proceeding subsequently. Comments, such as those indicating which remediation actions have been taken, can also be added on a line item basis.

To maximize security, and support separation of duties, individuals participating in workflow process are only able to see information related to their specific responsibilities. Responsibilities are assigned on two levels. The first relates to workflow responsibilities, as discussed above. Individuals only see information related to actions assigned to them through the workflow definition.

The second relates to access control mechanisms built into the core InfoSphere Guardium system, which allow administrators to assign responsibilities for particular databases or systems to individuals (or roles) and their hierarchical management. A simple example illustrates the benefits of this capability. Consider a workflow designed for reviewing the results of regular Database Vulnerability Assessments, which includes as a first step having the group "DBAs" review test results. Martha, a member of the DBA group who was granted InfoSphere Guardium rights for all the financial databases, will only see test results related to financial databases, while Patrick, who was granted rights to the payment card databases, will only see those results. InfoSphere Guardium makes it possible to define efficient workflow processes with parallel actions, without compromising security or burdening users with information that is not relevant to their responsibilities.

Increasing Accountability with Enterprise-wide Management

A comprehensive, enterprise-wide view of the status of each of the defined audit tasks is available to the workflow manager in real-time, including viewing required actions by responsible party, current action status and comments. This powerful interface provides the information necessary to appropriately manage the oversight process across heterogeneous database infrastructures and widely distributed teams, increasing accountability and minimizing audit exceptions.

The results of audit processes are stored in InfoSphere Guardium's secure repository, along with the audit data itself, enabling organizations to easily provide auditors with an irrefutable audit trail demonstrating consistent execution of all required tasks. A sophisticated archiving capability allows the repository to be automatically and securely archived to support the most demanding record keeping requirements, and easily restored as required by audits or forensic investigations.

InfoSphere Guardium's Advanced Compliance Workflow Automation enables organizations to automate and streamline compliance processes, reducing operational costs and simplifying preparation for successful audits, even in complex environments with unique operational requirements.

Database Vulnerability Assessment

Comprehensive Automated Tests Based on Best Practices

- Scans specified groups of databases
- Checks for common vulnerabilities such as missing patches, weak passwords, misconfigured privileges and default vendor accounts
- Includes hundreds of preconfigured tests based on best practices developed by the Center for Internet Security (CIS) and U.S. Department of Defense (DoD)
- Generates security health report card and recommends concrete action plans to strengthen database security
- Simplified deployment in large-scale environments – multiple data sources (DB name, type, server IP, ports, roles) can be automatically loaded and linked to assessments via script interface

Improving Database Security and Compliance

One of the best ways to secure database infrastructures – plus comply with regulations and pass your audits – is to regularly perform security assessments of your database environment.

Security assessments evaluate the security strength of your database environment and compare it with industry best practices. These in-depth evaluations examine patch levels and database configurations to highlight vulnerabilities in your environment – so you can quickly remediate problems and safeguard your critical enterprise data from both internal and external threats.

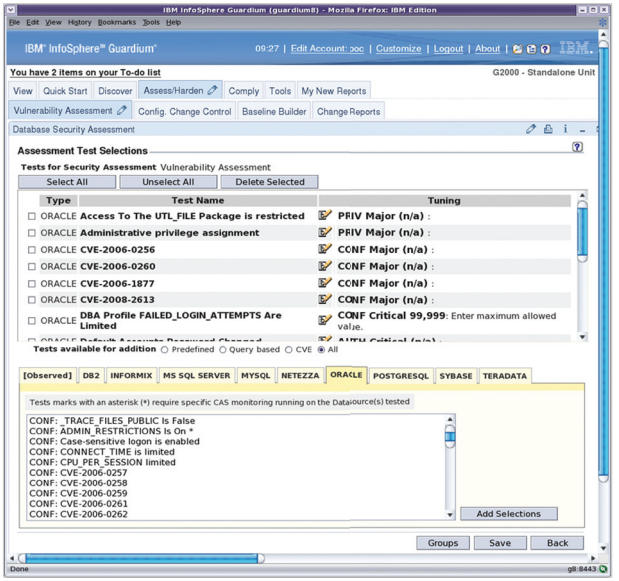


Figure 4: InfoSphere Guardium's Database Vulnerability Assessment module scans your database infrastructure for missing patches, misconfigured privileges and other vulnerabilities. It incorporates a best practices library with hundreds of preconfigured tests, and provides recommendations on how to remediate vulnerabilities, including identifiers (e.g. CVE) associated with external resources. You can also create custom tests and oversight processes.

Preconfigured Tests Based on CIS and DoD Best Practices

InfoSphere Guardium's Database Vulnerability Assessment (VA) module scans your database infrastructure for vulnerabilities and provides an ongoing evaluation of your security posture, using both real-time and historical data.

InfoSphere Guardium VA includes a comprehensive library of preconfigured tests (see Figure 4) based on industry best practices such as the Computer Internet Security (CIS) benchmarks and the Database Security Technical Implementation Guide (STIG) created by the U.S. Department of Defense. These tests check for common vulnerabilities such as missing patches, weak passwords, misconfigured privileges and default accounts, as well as unique vulnerabilities for each DBMS platform.

Tests are updated on a quarterly basis via InfoSphere Guardium's Knowledge Base Service. You can also define custom tests (see Figure 5) and schedule automated audit tasks incorporating scans, distribution of reports, electronic sign-offs and escalations.

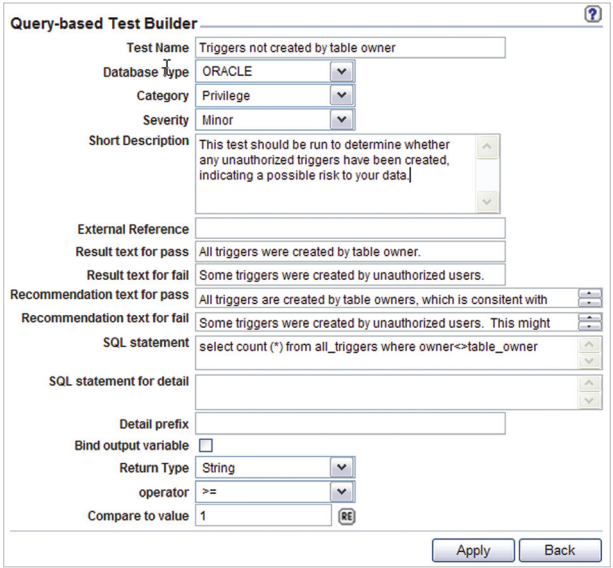


Figure 5: Custom tests using SQL queries can easily be created with the form-based test Builder. Custom tests can also be created via OS scripts and Java classes.

In addition to producing detailed reports with drill-down capabilities (see Figure 6), the assessment module recommends concrete action plans for each vulnerability to help you strengthen security. For example, if there are privilege issues the system will tell you exactly which privileges need to be revoked in order to comply with best practices. Test results also include references , such as CVE identifiers, to related external resources.

Once vulnerable systems have been remediated, organizations need to ensure that only authorized changes are made. InfoSphere Guardium's Configuration Audit System (CAS) monitors systems for any changes once a secure configuration baseline has been established.

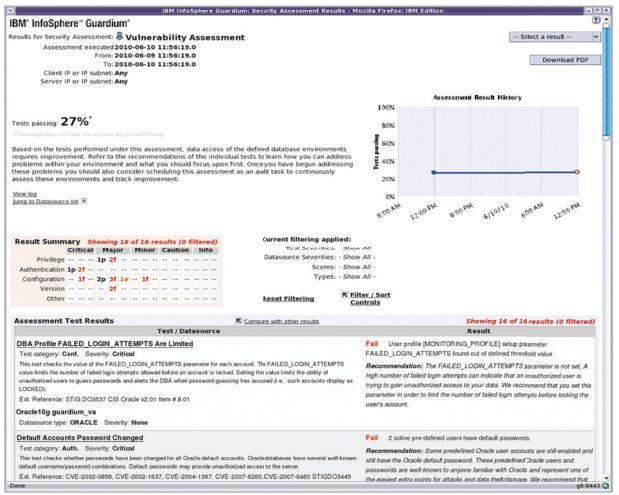


Figure 6: InfoSphere Guardium's Database Vulnerability Assessment module produces summary results that provide an understanding of your overall security posture, along with detailed drill-downs containing concrete recommendations for improvement.

Broad Range of Granular Tests

Assessments are grouped into multiple categories covering:

- **Privileges:** Checks for object creation and usage rights, privilege grants to DBAs and users, and system level rights.
- **Authentication:** Verifies password policies, default vendor accounts, no empty passwords, remote login parameters, etc.
- **Configuration:** Checks platform-specific variables such as maximum failed logins for DBA profiles (Oracle), not allowing updates to system tables (MS-SQL) and ensuring the SYSADM_GROUP has been defined (DB2).
- **Version:** Verifies appropriate version numbers and patch levels.
- **Behavioral:** These tests leverage InfoSphere Guardium's real-time activity monitoring to identify vulnerabilities in observed behavior such as excessive after-hours logins, login failures, execution of privileged commands and sharing of privileged credentials.
- **File Permissions:** Checks permissions on key objects such as database home directories, configuration files such as sqlnet.ora and registry/environment variables.

Multiple Assessment Technologies, Without Impacting Uptime or Performance

Unique in the industry, InfoSphere Guardium VA combines three essential detection methods to provide comprehensive coverage for a wide range of vulnerabilities and threats:

- **Scanning:** The system assesses database vulnerabilities via credentialed (read-only) access to the database.
- **Agent-based Scanning:** Lightweight agents installed on each database server are used to identify vulnerabilities that cannot be determined remotely, such as file permissions on key OS and database configuration files and scripts (requires CAS).
- **Passive Network Monitoring:** The system discovers vulnerabilities by observing all database transactions in real-time, such as an excessive number of database errors (indicating a possible SQL Injection attack), usage of shared administration accounts and service IDs, or usage of default vendor accounts.

Best of all, InfoSphere Guardium's vulnerability assessment provides complete platform coverage (see Figure 7) without impacting the performance or stability of critical systems. The system does not run intrusive exploits that can crash systems by imitating the behavior of an attacker, and it does not rely on traditional database logs or native auditing features that can introduce additional overhead.

Database Support
Oracle
Microsoft SQLServer 2000, 2005, 2008
IBM DB2 (LUW and z/OS)
IBM Informix
Sybase
Oracle MySQL
Teradata
PostgreSQL
Netezza

Figure 7: InfoSphere Guardium provides a simple means of hardening you entire database infrastructure, providing Vulnerability Assessment capabilities for all major DBMS platforms.

Beyond Simple Reporting: Addressing the Entire Vulnerability Management Lifecycle

InfoSphere Guardium's Database Vulnerability Assessment module is tightly-integrated with other modules in the platform, allowing you to manage the entire database security and compliance lifecycle with a single unified Web console, back-end data store and workflow automation system.

This integration enables enterprises to go beyond simply producing vulnerability reports to addressing the end-to-end vulnerability management process, including assessing and mitigating business risk, prioritizing remediation activities, and streamlining compliance reporting and oversight processes. In particular, InfoSphere Guardium allows you to rapidly:

- **Pinpoint database vulnerabilities:** Unpatched and misconfigured databases create enormous risk. InfoSphere Guardium VA incorporates an extensive library of assessment tests, based on industry best practices, to flag vulnerabilities. A quarterly Knowledge Base Service ensures that assessment tests are always up to date.
- **Protect unpatched systems with real-time controls:** Vulnerable systems can take 3-6 months to patch. InfoSphere Guardium protects databases until they can be patched, through activity monitoring, signature-based policies, and preventive controls. Policies and baselining can also protect against application vulnerabilities such as SQL injection and buffer overflow. For example, you can alert and/or block on any calls by non-line-of-business applications to unpatched procedures, indicating a possible attack.
- **Prioritize remediation activities based on business risk:** InfoSphere Guardium's Classifier module locates and classifies sensitive data in corporate databases such as credit card numbers, while its baselining function analyzes observed behavior to understand how and when line-of-business applications are accessing vulnerable databases. Risk assessment is crucial for prioritizing remediation, since most organizations don't have sufficient resources to patch all vulnerable systems at the same time.
- **Harden databases:** Once vulnerable systems have been repaired using recommendations provided by the assessment tests, InfoSphere Guardium's CAS "hardens" configurations by ensuring they are not changed in an unauthorized manner.
- **Document and streamline compliance:** Auditors want to know that incidents are being tracked and resolved in a timely manner. With InfoSphere Guardium's incident management and Compliance Workflow Automation (see Figure 8), you can automate report distribution, electronic sign-offs and escalations, while tracking progress on the remediation of vulnerable systems.

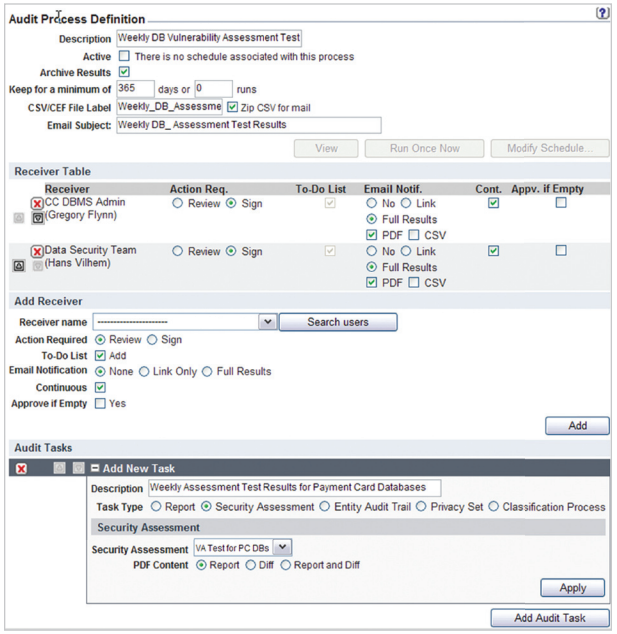


Figure 8: Auditors look for evidence that organizations have well-defined processes in place to safeguard their critical data. InfoSphere Guardium's workflow automation module allows you to define customized Audit Tasks that automatically perform scheduled vulnerability assessments along with report distribution, sign-offs and escalations.

Database Protection Knowledge Base

Maximize Protection and Compliance with Recurring Content Updates

- Proactively updates your InfoSphere Guardium system with the latest information on database vulnerabilities, best practices policies and sensitive tables in enterprise applications
- Populates Vulnerable Objects group with the most current information on database objects and packages with security risks, automatically updating associated defensive policies
- Eliminates hours of upfront and on-going labor by identifying sensitive tables in common enterprise applications (e.g. SAP, Oracle EBS) requiring protection, such as those containing PCI DSS or financial (SOX) information
- Updates InfoSphere Guardium's extensive library of predefined database vulnerability assessment tests, helping avert exposure to the latest threats
- Enables the development of sophisticated policies by maintaining scores of groups identifying database and application objects with security and compliance requirements

The Challenge of Protecting Sensitive Data in Rapidly Changing Environments

Organizations across industries rely on databases to store their most valuable information and execute mission-critical tasks in conjunction with enterprise applications. As a result, deployments of database protection and compliance solutions, such as IBM's InfoSphere Guardium, are common.

To maximize the protection afforded by InfoSphere Guardium, groups, policies, tests and other configurable parameters should be regularly updated to adapt to the constantly evolving nature of the database infrastructure and associated threats. For example, vulnerability tests should reflect the most recent exploits and patch levels, while policies should encompass current lists of sensitive and vulnerable objects.

While administrators can easily manually modify InfoSphere Guardium's configurable parameters to account for such changes, they frequently lack the expertise or time to do so. Assembling comprehensive vulnerability information requires both technical expertise in the systems to be protected, and the ability to research and integrate exploit information from across the industry. Staying abreast of changes in the variety of database systems and enterprise applications found in a typical enterprise is similarly challenging. Each has their own unique architecture, documentation and release schedules. Yet failing to make updates to reflect the most recent changes in all of these parameters can result in the creation of substantial security and compliance gaps.

Leverage IBM's Expertise and Staff to Maximize Protection and Compliance

IBM's InfoSphere Guardium Database Protection Knowledge Base is an annual service which provides clients with updated content, in Guardium consumable formats, related to supported databases and applications in order to maximize protection and compliance. Content provided includes:

- Software patch levels
- Version levels
- Vulnerable objects
- Sensitive objects (such as tables with SOX, PII or PCI data)
- Vulnerability assessment tests and identifiers
- Stored procedures
- Administrative programs
- Commands, errors and user roles.

A wide variety of sources are used to identify this information including internal IBM research, relationships with other vendors and cross-industry cooperative efforts such a CVE. Information is assembled, packaged for integration into appropriate Guardium elements (e.g. vulnerability tests, groups, etc.), tested and delivered to InfoSphere Guardium clients.

Simple to Administer

Knowledge Base updates are generally released quarterly to align with DBMS vendors' quarterly release schedule; however exceptions are made depending upon the current environment and risk profile.

Updates are easily applied with the click of a mouse (see Figure 9). The intelligent update process built into InfoSphere Guardium accommodates user specific customization. If an object has been added by the user, the system will recognize that action and preserve it during the update process. For example, if an enterprise application has been customized, an object might be added to the associated PCI group to ensure that the customization if reflected. At the next update InfoSphere Guardium will recognize that object was added and preserve it during the update process.

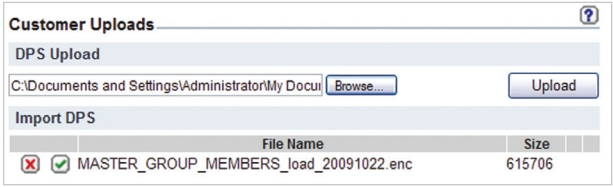


Figure 9: Current vulnerability, auditing and best practices libraries regularly provided by the Database Protection Knowledge Base service are integrated into InfoSphere Guardium with the click of a mouse.

By delivering current content packaged for immediate integration into InfoSphere Guardium, IBM has both minimized administrative costs by eliminating the need for manual updates to content, and maximized data protection and compliance benefits of the system by ensuring policies and tests reflect the most current information about your enterprise infrastructure and the threatscape.

Comprehensive Protection for Heterogeneous Environments

InfoSphere Guardium Database Protection Knowledge Base updates deliver content for all major platforms (see Figure 10), providing a simple means of ensuring protective policies are current, even in the heterogeneous environments common in most organizations. For each platform, a variety of content (outlined above) is delivered, enabling a wide range of applications, including:

- **Testing to Avert Exposure to the Most Recent Database Vulnerabilities**[1]**:** Updated Vulnerability Assessment (VA) tests ensure that regularly scheduled VA scans required by security best practices, as well as various compliance mandates, detect the most recent vulnerabilities for each platform in the database infrastructure, including missing patches.
- **Compliance Validation:** Mandates such as PCI DSS and SOX require the implementation of controls to prevent unauthorized modification and access to sensitive data. Updated best practices auditing libraries for SAP and Oracle EBS ensure controls can easily be implemented using InfoSphere Guardium, without the need to spend hours researching those applications on an on-going basis to identify sensitive tables.
- **Vulnerable Object Protection (Virtual Patching):** In most organization there is a significant delay between the time a database patch is announced and the time it is installed. Organizations interested in minimizing their exposure during this time can use updates to the Vulnerable Objects Group to easily implement rules which alert or block unexpected access to the vulnerable objects until the patch until can be installed.

1 Requires Vulnerability Assessment module

A wide variety of other applications become feasible with InfoSphere Guardium's Database Protection Knowledge Base, ranging from alerting when sensitive stored procedures are used, to tracking certain types of errors which may indicate inappropriate activity. By providing current information on groups with important security and compliance implications InfoSphere Guardium enables the development of powerful controls, without increasing operational expense.

Database Support
Oracle
Microsoft SQLServer 2000, 2005, 2008
IBM DB2 (LUW and z/OS)
IBM Informix
Sybase
Oracle MySQL
Teradata
PostgreSQL
Netezza

Figure 10: InfoSphere Guardium Database Protection Knowledge Base delivers a wide range of updated content including vulnerability tests, sensitive objects, vulnerable objects and current patch information across all major database platforms.

Data-Level Access Control

Simplified Preventive Control for Heterogeneous DBMS Environments

- Blocks privileged users from viewing or changing sensitive data, creating new user accounts or elevating privileges
- Zero impact on application-level traffic
- Supports IT outsourcing and associated cost savings – without increasing risk
- Enforces separation of duties for SOX, PCI, Basel II, data privacy regulations
- Simplifies security and compliance via single set of granular access policies for heterogeneous DBMS infrastructures
- Enhances operational efficiency by replacing manual processes with centralized and automated controls

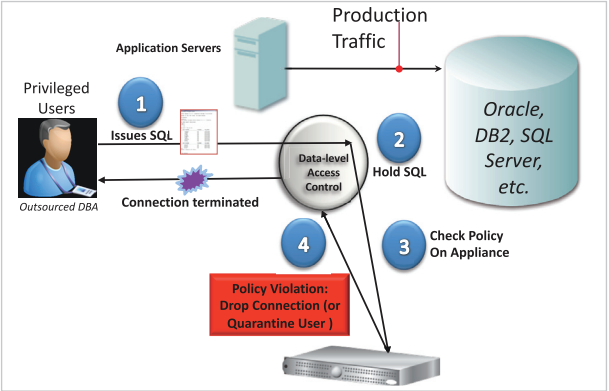
Changing Control Requirements

"Gartner predicts that there will be increasing regulations as a result of the 2008 financial crisis. Therefore, this is no time to ignore risk management and compliance."[1]

Doing more with less – while managing risk, protecting against insider threats and addressing compliance – is increasingly important for most organizations.

Role-based access and other built-in DBMS controls are designed to prevent end-users from accessing sensitive data, but can't prevent unauthorized access by privileged users who have unfettered access to all SQL commands and database objects.

Newer technologies such as database activity monitoring (DAM) provide an additional layer of protection by generating detailed audit trails and real-time security alerts whenever anomalous activity is detected or access policies are violated (including violations by privileged users).



Roles & Associated Policies	DDL	DML	SELECT	CREATE/ ALTER USER
PeopleSoft DBA	Allow	Allow	Block	Block
DBA access to other schemas	Block	Block	Block	Block
DBA working on DBA schema *(sys, v$ tables, tuning)*	Block	Allow	Allow	Allow or Block
Replication & Backups	Allow	Allow	Allow	Block
Developers	Block	Block	Block	Block

Figure 11: InfoSphere Guardium Data-Level Access Control simplifies enterprise security with a single set of granular policies for enforcing separation of duties across multiple DBMS platforms – without disrupting application access or changing database configurations. It's the only cross-DBMS technology that blocks privileged users – such as DBAs, developers, outsourced personnel and other superusers – from viewing or changing sensitive data. InfoSphere Guardium Data-Level Access Control monitors all database connections including local access by privileged users via non-TCP connections (such as Oracle BEQ, SHM, TLI, IPC, etc.).

While DAM is an important element of a defense-in-depth strategy, it has traditionally been limited to providing detective controls rather than preventive controls, because monitoring alone can't enforce security policies and prevent unauthorized actions from occurring.

Real-Time Preventive Controls; Zero Disruption to IT Infrastructures

Implemented as a lightweight, host-based software agent (see Figure 11) with fine-grained security policies (see Figure 12), InfoSphere Guardium Data-Level Access Control provides automated, real-time controls that prevent privileged users from performing unauthorized actions such as:

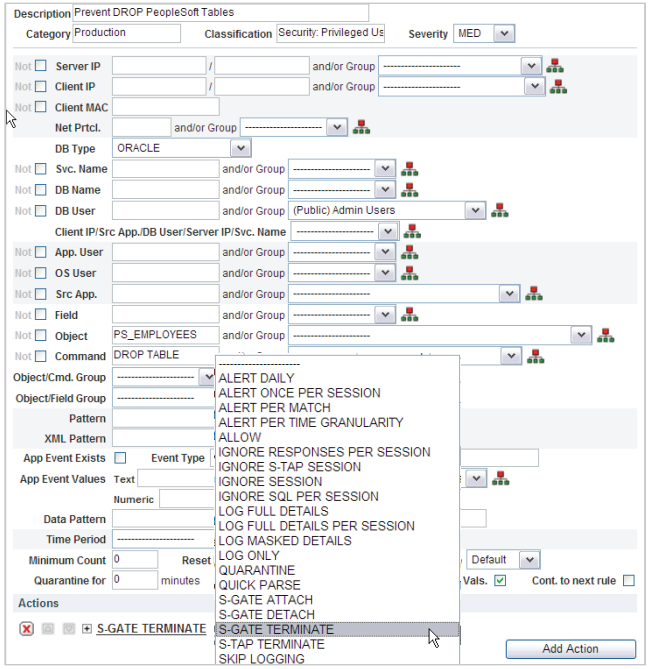
- Executing queries on sensitive tables
- Changing sensitive data values
- Adding or deleting critical tables (schema changes) outside change windows
- Creating new user accounts and modifying privileges

InfoSphere Guardium Data-Level Access Control is completely non-intrusive, and does not require add-on functionality inside the database. As a result, it's implemented quickly without disrupting business-critical applications such as Oracle E-Business Suite, PeopleSoft, Siebel, SAP, Business Objects and in-house applications.

Advantages Over Database-Resident Controls

InfoSphere Guardium Data-Level Access Control provides strong advantages over database-resident controls, including:

- **Cross-Platform Support:** InfoSphere Guardium Data-Level Access Control allows organizations to define a single set of access policies for their entire application and database infrastructure, rather than controlling access for only a specific DBMS platform or version. Because it is implemented outside of the database, InfoSphere Guardium Data-Level Access Control supports all major DBMS platforms: Oracle, Microsoft SQL Server, IBM DB2, IBM Informix, Sybase, Oracle MySQL, Teradata, Netezza and PostgreSQL.



- **Ease-of-Use for Non-DBAs:** Database-resident controls require DBAs to administer them – raising issues around separation of duties. InfoSphere Guardium Data-Level Access Control can be managed by IT security, compliance or risk teams because it uses simple, English-language policies that can be customized via drop-down menus, without requiring knowledge of database commands and structures. In addition, InfoSphere Guardium Data-Level Access Control uses a hardened, Linux-based network appliance to manage access policies, preventing privileged users from disabling or modifying policies, and further strengthening separation of duties.

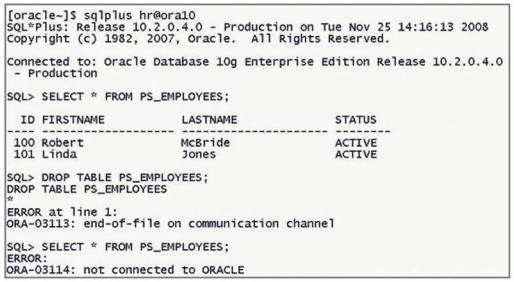


Figure 12: The InfoSphere Guardium platform supports granular, deterministic policies to positively identify violations (rather than relying on heuristics). Rules are based on specific session properties such as client IP address, MAC address, source application, DB user, OS user, application user, time-of-day, SQL command, and table names, which are typically defined via pre-defined groups to simplify ongoing management. A broad range of policy actions can be invoked for policy violations, such as real-time alerts (SMTP, SNMP, Syslog, CEF), user quarantine and terminate connection (shown above).

- **Single Solution for Policy Enforcement and Auditing:** Compliance regulations require storing a complete audit trail of all privileged user actions, in order to document compliance and aid in forensic investigations. DBMS vendors typically offer fine-grained auditing and audit repositories as separate add-ons. InfoSphere Guardium offers policy enforcement and fine-grained auditing in a single solution, further reducing cost and complexity.
- **Policies that Examine Query Results, Not Just Incoming Queries:** Database-resident controls are limited to controlling execution of specific SQL commands on specific objects. InfoSphere Guardium Data-Level Access Control goes one step further by also examining query results (see Figure 13). For example, a connection from an anomalous script or application that is suddenly seen to be extracting PII from the database can be terminated, or quarantined while being investigated, while a valid application that extracts the same PII data will be allowed.
- **Non-Stop Enforcement:** Some database-resident controls must be turned off for routine maintenance operations such as backups and patching. During these maintenance windows, privileged users can take advantage of disabled controls to perform unauthorized actions. InfoSphere Guardium Data-Level Access Control provides continuous enforcement of access policies because it does not require disabling certain privileged accounts inside the database.

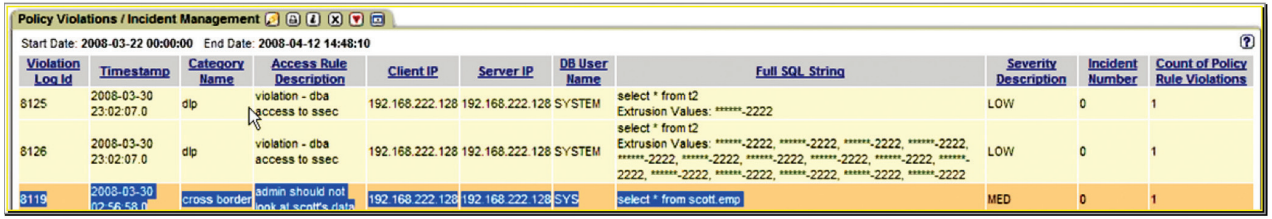


Figure 13: Extrusion rules examine returned data (rather than inbound SQL commands), looking for numeric patterns such as 16-digit credit card numbers or 9-digit social security numbers. Extruded data is typically masked before being stored in the InfoSphere Guardium appliance as part of the audit trail (shown above with asterisks). You can define policy actions (called "S-TAP TERMINATE") that terminate connections after sensitive data has been detected in query results, thereby limiting data leakage (typically to tens of records). In comparison, "S-GATE TERMINATE" will terminate connections even before SQL commands have been executed on specific database objects by the DBMS.

Extension to InfoSphere Guardium's Host-Based Software Probe

Data-Level Access Control is an extension to S-TAP™ ("software tap"), InfoSphere Guardium's lightweight, host-based probe. Unique in the industry, S-TAPs are non-intrusive software probes that monitor network streams at the OS level of database servers, including both network access and local access by privileged users (via shared memory, named pipes, Oracle Bequeath, etc.).

S-TAPs have minimal impact on server performance because they relay all traffic to separate InfoSphere Guardium appliances for policy evaluation, analysis, reporting and secure online storage of audit trails.

Customers already using S-TAP can easily upgrade to InfoSphere Guardium Data-Level Access Control to start enforcing access at a very granular level – without disrupting their application environments.

1 Gartner, "Managing IT Risks During Cost-Cutting Periods," by Mark Nicolett, Paul Proctor, French Caldwell, 22 October 2008.

Entitlement Reports

Simplify Management of User Rights Across Heterogenous Database Environments

- Provides a simple means of aggregating and understanding entitlement information across your entire database infrastructure
- Out-of-the-box support for database platforms from eight vendors on all major operating systems
- Pre-defined reports for commonly required views
- Fully integrated with other InfoSphere Guardium modules including Compliance Workflow Automation to reduce operational costs
- Eliminates manual labor, improves data security and simplifies compliance validation with major mandates such as SOX, PCI DSS and data privacy regulations

The Challenges of Managing Database User Rights

In recent years organizations have struggled to cope with rapidly escalating database information growth. Among the challenges associated with this trend is implementing effective data protection measures. Traditionally database administrators (DBAs) have relied primarily on the native authorization capabilities of the DBMS to secure data; striving to grant users minimal object and system privileges (entitlements) consistent with their job requirements. Given the broad range of privileges available, the growth in user accounts and objects, and the complexity of managing cascading roles, this has required significant labor.

However changes in the business environment are exacerbating the challenge of managing user entitlements. Increasingly dynamic organizations are changes roles and responsibilities more frequently than ever. Mergers and acquisitions are creating distributed, multi-vendor database infrastructures where DBAs must cope with both varying vendor entitlement models and numerous distinct systems. As a result, it has become extremely difficult to ensure that database privileges are restricted so sensitive objects and system rights are not inappropriately exposed. This creates not only a data protection issue, but also a compliance issue.

Auditors validating compliance with major mandates require regular reviews (sometime referred to as database user rights attestation reporting) to ensure user entitlements are regularly adjusted to align with changes in personnel status, responsibilities and actual usage.

Database Support
Oracle
Microsoft SQL Server 2000, 2005, 2008
IBM DB2
IBM Informix
Sybase
Oracle MySQL
Teradata
PostgreSQL
Netezza

Figure 14: InfoSphere Guardium Entitlement Reports provide a simple means of collecting and understanding user rights information across heterogeneous database infrastructures.

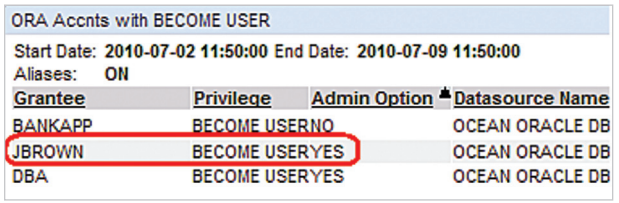
Automating and Centralizing Collection of Entitlement Information

InfoSphere Guardium Entitlement Reports provide a simple means of aggregating and understanding database entitlements across the organization. The optional software module is configured to scan all selected databases in your infrastructure on a scheduled basis, automatically collecting information on user rights, including those granted through roles and group membership. This eliminates the time consuming process of examining each database, as well as the need to step through cascading roles (roles granted to roles) in each to develop a true understanding of entitlements. It also enables collection of this information on a frequent systematic basis without the use of scarce technical resources, providing timely, accurate information that will enhance your security posture and satisfy the needs of auditors, while reducing operational costs.

Wide Range of Pre-Configured Reports

The Entitlement Reports option is designed to work with the authorization systems of a wide variety of popular DBMSs (see Figure 14), enabling it to retrieve, understand and present information gathered across heterogeneous environments using limited credentialed read-only access[1]. A variety of pre-defined reports (see Figures 15 and 16) provide different views of the 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 pre-defined reports include:

- Accounts with system privileges
- All system and admin privileges; shown both by user and role
- Object privileges by user
- All objects with PUBLIC access
- User privileges by object
- Roles granted to users and roles
- Grants and revocation of privileges
- Execute privileges by procedure

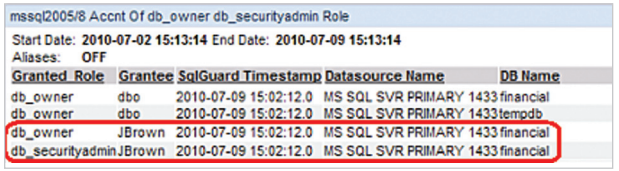


ORA Accnts with BECOME USER

Start Date: **2010-07-02 11:50:00** End Date: **2010-07-09 11:50:00**
Aliases: **ON**

Grantee	Privilege	Admin Option	Datasource Name
BANKAPP	BECOME USER	NO	OCEAN ORACLE DB
JBROWN	BECOME USER	YES	OCEAN ORACLE DB
DBA	BECOME USER	YES	OCEAN ORACLE DB

Figure 15: Users with inappropriate rights can easily be identified with InfoSphere Guardium Entitlement Reports. In this report JBROWN has the powerful Oracle "BECOME USER" system privilege which could be misused to gain access to unauthorized information or compromise an important application.



mssql2005/8 Accnt Of db_owner db_securityadmin Role

Start Date: **2010-07-02 15:13:14** End Date: **2010-07-09 15:13:14**
Aliases: **OFF**

Granted_Role	Grantee	SqlGuard Timestamp	Datasource Name	DB Name
db_owner	dbo	2010-07-09 15:02:12.0	MS SQL SVR PRIMARY 1433	financial
db_owner	dbo	2010-07-09 15:02:12.0	MS SQL SVR PRIMARY 1433	tempdb
db_owner	JBrown	2010-07-09 15:02:12.0	MS SQL SVR PRIMARY 1433	financial
db_securityadmin	JBrown	2010-07-09 15:02:12.0	MS SQL SVR PRIMARY 1433	financial

Figure 16: InfoSphere Guardium aggregates and presents entitlement information across eight DBMS platforms, including SQL Server, Oracle and DB2. This simplifies the process of identifying inappropriately granted roles, such a JBrown being granted both the db_owner and db_security admin role for the financial database.

1 Login to the database to gather entitlement information is accomplished via an IBM supplied script that requires limited (read-only) privileges; customers can examine this script to determine that privileges are consistent with their corporate policies.

Automating Validation Activities for Security and Compliance

All entitlement information gathered from across your database infrastructure is stored in InfoSphere Guardium's forensically secure and tamper-proof repository along with all database audit information, where it available for use by all system modules, including the Report Builder, Policy Builder and Compliance Workflow Automation application. Custom reports can easily be built via an intuitive drag-and-drop interface, to show specific views not provided by the pre-defined reports. Compliance Workflow Automation allows the reports required for these periodic reviews to be automatically generated and distributed to the appropriate oversight team. It also electronically captures comments, escalations and approvals, and stores them in the repository for use with auditors.

InfoSphere Guardium's policy monitoring and enforcement capabilities are also designed to leverage information captured from the Entitlement Reports module. Entitlement information can be used in applications such as automatically populating policy groups. A typical use case is automatically updating a policy written to generate an alert whenever an unauthorized user attempts to access the customer records of a Very Important Person (VIP). An employee being investigated for leaking VIP records will typically have their access rights revoked during the investigation, which will automatically be reflected in the "Authorized Users" group through the next regularly scheduled update of the associated report. If the employee attempts to access a VIP record, an alert will be generated and the incident logged for use in the investigation.

Reducing Operational Costs and Improving Data Protection

InfoSphere Guardium Entitlement Reports provide a simple means of aggregating, understanding and utilizing user rights information to maximize sensitive data protection, minimize operational costs and ensure successful audits. It eliminates the time consuming and error prone process of manually collecting and analyzing user rights information, ensures important security gaps are quickly identified, while reducing operational costs. Compliance workflow and policy management integration further reduce operational costs, while demonstrating the implementation of proactive controls required to satisfy the demands of discerning auditors.

Configuration Audit System for Database Servers

Detect Configuration Changes Impacting Database Security

- Tracks all changes that can affect the security of database environments outside the scope of the database engine
- Complements InfoSphere Guardium's Database Activity Monitoring module to provide comprehensive database monitoring
- Tracks changes to database configuration files and other external objects that can affect your database security posture, such as
  - Environment/registry variables
  - Configuration files (e.g. SQLNET.ORA, NAMES.ORA)
  - Shell scripts
  - OS files
  - Executables such as Java programs
- Required for all governance and risk management implementations
- Implements security best practices with no administrator work

Securing Database Environments

Most changes to database environments occur through the database engine. For most database types, controlling and configuring the database is done through specialized SQL commands or stored procedures performed by DBAs or security administrators (of the database).

These activities are easily secured using InfoSphere Guardium's database activity monitoring functionality, which allows you to monitor and audit all database activities – including privileged user actions – and enforce access control policies, without impacting performance or relying on DBMS-resident logs or auditing functions.

Additionally, InfoSphere Guardium's Vulnerability Assessment offering can assess the security strength of the database and highlight weaknesses that must be addressed in terms of misconfigured parameters, default accounts, vulnerabilities for which patches should be applied, and privileges that need to be revoked.

Having said all that, a database is a program that is installed at the operating system level and that makes use of operating system services. There are many configuration elements that reside within operating system constructs rather than within the database itself.

Examples include files, registry values and environment variables. Many of these files and values control some of the most important aspects of database security. A good example is the authentication method of the database. In almost all database platforms an administrator can change the way that a database authenticates users by changing such a value – either in addition to or instead of using SQL.

Clearly, a serious security breach can occur if an administrator modifies and uses a weak authentication method. Therefore, this must be monitored and alerted on.

InfoSphere Guardium's Configuration Audit System for Database Servers (CAS) tracks all changes made to the database at various levels and reports on these changes to a centralized Web-based console. Using CAS, security administrators can know that no changes that may affect security have been made in ways that bypass the database's SQL engine.

Together with InfoSphere Guardium's Database Activity Monitoring functionality, this provides the only comprehensive monitoring, auditing and control solution for databases in the industry.

What CAS Does

CAS is a light-weight agent that runs on the server where database instances are installed. CAS monitors all changes to various constructs, including changes to files, file ownership and permission definitions, registry values, environment variables, and database structures.

It will then poll these constructs based on a set of periods defined by the user and, if there are any changes, it will notify the InfoSphere Guardium server precisely which element was changed, what the new value is (versus the old value), etc.

CAS works from a template that defines what to monitor. The InfoSphere Guardium system includes a set of predefined templates that define the best practices for monitoring in an Oracle, DB2, Sybase, SQL Server, Informix, MySQL, Netezza, Teradata or PostgreSQL environments (see Figure 17). A user deploys these templates to the server by selecting the template and the host – CAS does the rest.

When deployed, CAS expands this template to the actual instance elements. For example, it is common for security best practices to require that you ensure that no changes are made to the database executables. A database installation has tens of executables and each one can be used by an attacker to compromise an environment. As an example, an attacker can replace one of these executables with a version that in addition to doing the regular work also stores user names and passwords in a file that the attacker then reads. Making sure that these files are not changed is part of any audit – external or internal.

CAS also tracks other values. For example, SQL Server allows encrypting the database communication using SSL. This value is set within various SQL Server utilities. At the end of the day this value is stored in the standard Windows registry (see Figure 18). A Windows administrator can easily turn off encryption of data-in-transit with a simple modification and no one would be the wiser. CAS templates monitor these values to further ensure the robustness of your database security.

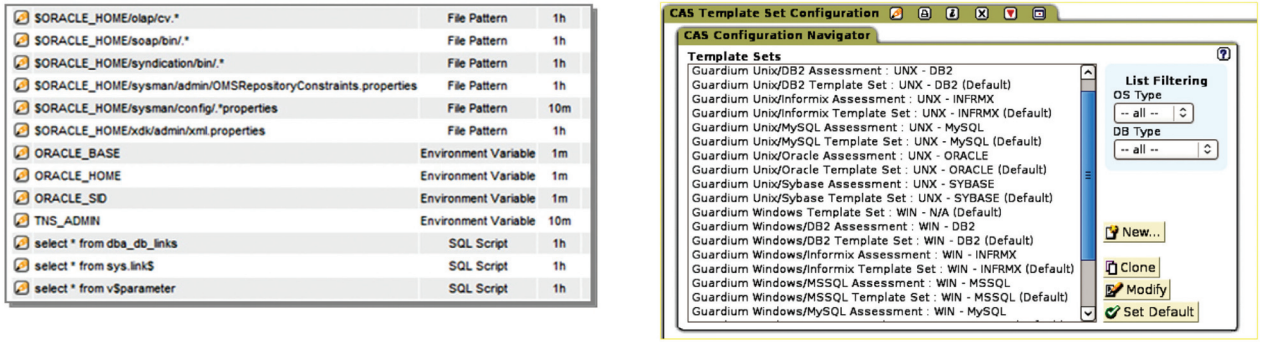


Figure 17: InfoSphere Guardium's Configuration Audit System for Database Servers (CAS) module tracks all changes to external database objects – such as configuration files, environment and registry variables, scripts and executables – that can affect your database security posture. To accelerate deployment, CAS includes a best practices library with hundreds of preconfigured knowledge templates for all major OS and DBMS combinations.

Other changes that CAS can monitor in addition to changes to file and registry values are:

- Changes to environment variables
- Changes to file permissions. CAS can also validate that file permissions are not set to exceed a certain limit
- Changes to file ownership. CAS can also validate that file ownership is set to certain values only
- Changes to any database element that can be queried
- Changes to any operating system value that can be queried.

CAS provides additional parameters that a security administrator can control. For example, while every template element has a default polling interval, an administrator can set different polling intervals (see Figure 19). An administrator can specify how CAS should determine whether or not there is a change. One option is to use a timestamp and the other is to use an MD5 checksum value. The latter is more resource-intensive to compute, but more robust.

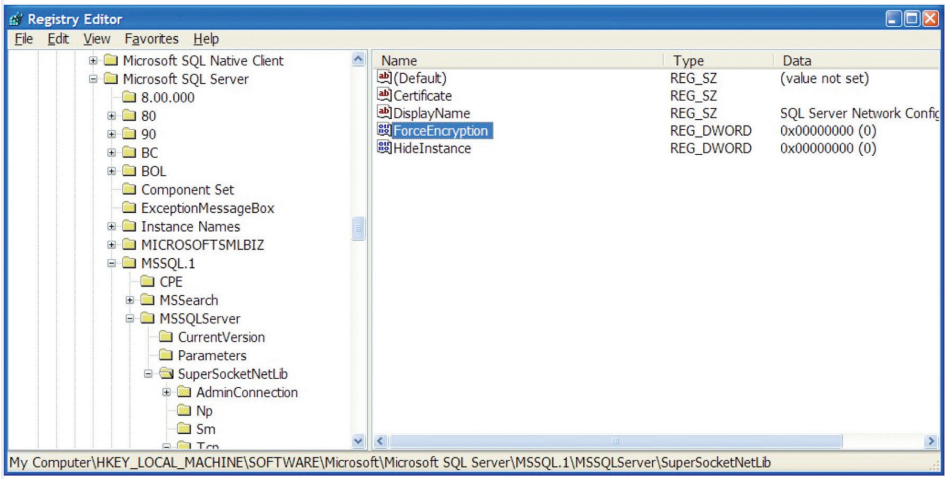


Figure 18: CAS simplifies the process of tracking critical registry values, such as the "Force protocol encryption" registry value for SQL Server.

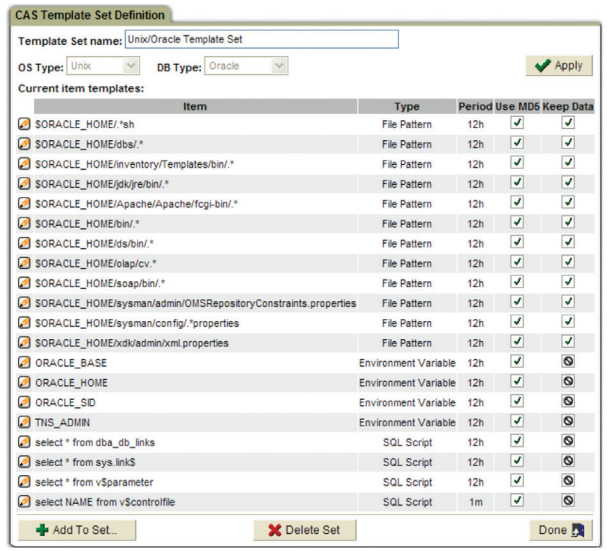


Figure 19: CAS allows you to define the polling period for tracking changes; whether MD5 checksums are used to track changes (rather than timestamps); and whether CAS should also "keep data" to track "before" values.

Additionally, each element specifies whether or not CAS should just report on the change or whether it should also bring back the before and after values. In the later case reports are provided that show the difference between the old and the new values (see Figure 20).

Installing and Operating CAS

CAS can be installed as part of an S-TAP installation or as a separate installation. CAS runs as a Java program and thus needs Java 1.4 or above installed on the host. Java is a prerequisite and the CAS installer asks for the location of the Java installation. The table to the right summarizes the storage requirements for CAS.

Customizing CAS

In addition to the pre-built templates and tracked elements, CAS allows security administrators to build new targets that should also be tracked. This includes much more than just defining new files or elements to be watched. You can define new database scripts and new operating system scripts that are managed by CAS and that can also be used to supplement the extensive built-in functionality that CAS provides.

Operating System	Required Disk Space
AIX	350MB
HP-UX	650MB
Linux	450MB
Solaris	400MB
Tru64	350MB
Windows	300MB

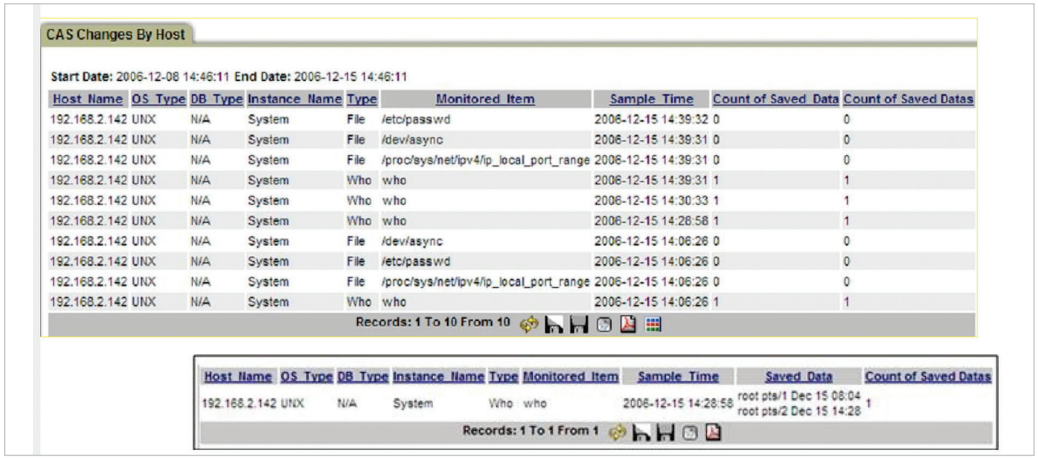


Figure 20: CAS provides the option of retaining before values, as well as after values, if desired ("Saved Data" above).

Documenting Compliance with Automated Sign-Offs and Escalations

Auditors want to know that incidents are being tracked and resolved in a timely manner. With InfoSphere Guardium's incident management and Compliance Workflow Automation (see Figure 21), you can automate report distribution, electronic sign-offs, comments and escalations, while tracking progress on the remediation of change incidents.

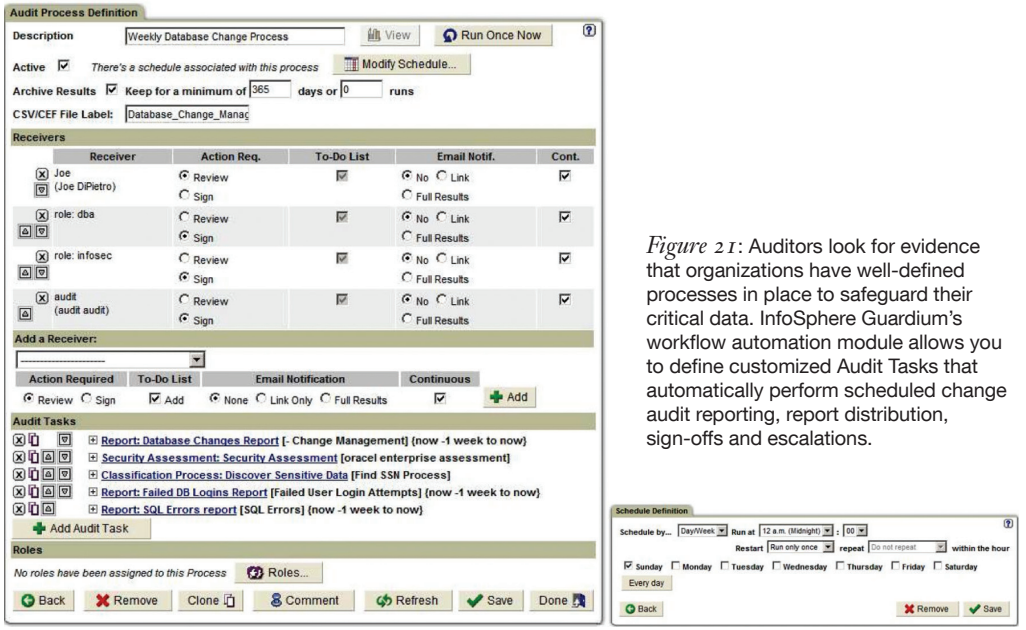


Figure 21: Auditors look for evidence that organizations have well-defined processes in place to safeguard their critical data. InfoSphere Guardium's workflow automation module allows you to define customized Audit Tasks that automatically perform scheduled change audit reporting, report distribution, sign-offs and escalations.

Application End-User Identifier

Detect Fraud in Real-Time by Monitoring Application User Activities

- Protects major enterprise applications from fraud, external or internal attack, privilege abuse and data leakage
- Reports on application user credentials from which unauthorized operations were performed, even when the application uses a generic service account to access the database
- Uses deterministic methods to positively identify application users, unlike other systems that rely on approximate methods such as statistical sampling and traffic matching, which are not valid for auditing and forensic purposes
- Meets auditor requirements to monitor access to sensitive information, regardless of origin
- Reduces operational costs and simplifies compliance with internal and external audit requirements including SOX, PCI DSS, ISO 27001, NIST 800-53 and SAS70

Security and Compliance in Enterprise Application Environments

Many organizations rely on enterprise applications to execute core business processes and manage significant amounts of data which are both mission critical and highly sensitive. Financial data, personnel data and customer data are all examples of assets managed within applications like SAP, PeopleSoft and Oracle EBS. It is therefore not surprising that many compliance requirements and audits involve data managed by enterprise applications, requiring IT security organizations to ensure this data is secure.

InfoSphere Guardium Application End-User Identifier provides a packaged solution that addresses security and compliance requirements for the data managed by major enterprise applications — without requiring changes to existing business processes or application source code.

The primary purpose of application-layer monitoring is to detect fraud that occurs via enterprise applications. This level of monitoring is often required for data governance requirements such as SOX, ISO 270001, SAS 70 and NIST 800-53 controls.

Securing Multi-Tier Enterprise Applications

Multi-tier enterprise applications are often the most difficult to secure because they are highly distributed and designed to allow Web-based access from insiders and outsiders such as customers, suppliers, and partners. In addition, multi-tier enterprise applications typically mask the identity of end-users at the database transaction level, using an optimization mechanism known as “connection pooling”.

Connection pooling identifies all transactions with a generic service account name, making it challenging to associate specific database transactions with particular application end-users. This is especially true if you’re relying on traditional database logging tools that can only monitor and identify users based on their database login accounts.

Since enterprise application data resides in relational databases, it can also be accessed through direct database connections (for example, via developer tools such as SQL *Plus) as well as through the application itself. IBM provides the only comprehensive solution that addresses both of these access paths. It positively identifies application

users associated with specific database transactions (see Figures 22, 26, and 27), as well as identifying direct access by privileged users to unauthorized objects. For example, in Figure 24 a policy specifying users can access EBS data only through the Oracle application has been violated by an attempt to SELECT data through SQL *Plus. That violation automatically triggers specified actions. In this case termination of the SQL *Plus session, logging of the details of the violation and generation of an alarm were specified.

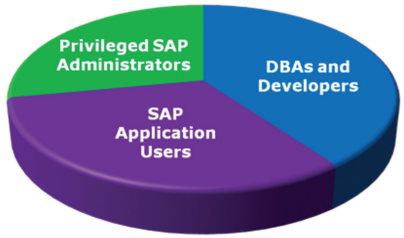
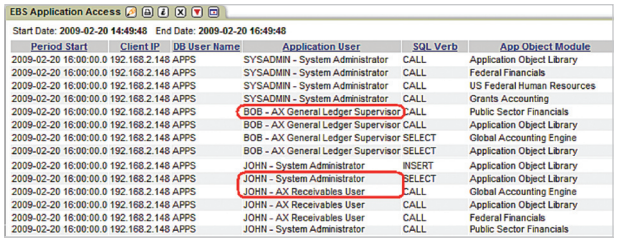


Figure 23: InfoSphere Guardium protects enterprise application environments from all major sources of risk.



EBS Application Access

Start Date: 2009-02-20 14:49:48 End Date: 2009-02-20 16:49:48

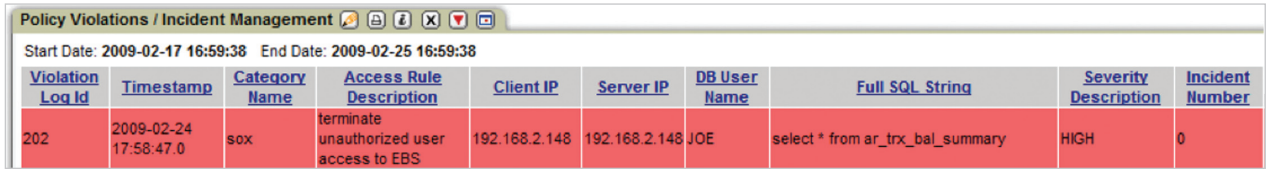
Period Start	Client IP	DB User Name	Application User	SQL Verb	App Object Module
2009-02-20 16:00:00.0	192.168.2.148	APPS	SYSADMIN - System Administrator	CALL	Application Object Library
2009-02-20 16:00:00.0	192.168.2.148	APPS	SYSADMIN - System Administrator	CALL	Federal Financials
2009-02-20 16:00:00.0	192.168.2.148	APPS	SYSADMIN - System Administrator	CALL	US Federal Human Resources
2009-02-20 16:00:00.0	192.168.2.148	APPS	SYSADMIN - System Administrator	CALL	Grants Accounting
2009-02-20 16:00:00.0	192.168.2.148	APPS	BOB - AX General Ledger Supervisor	CALL	Public Sector Financials
2009-02-20 16:00:00.0	192.168.2.148	APPS	BOB - AX General Ledger Supervisor	CALL	Application Object Library
2009-02-20 16:00:00.0	192.168.2.148	APPS	BOB - AX General Ledger Supervisor	SELECT	Global Accounting Engine
2009-02-20 16:00:00.0	192.168.2.148	APPS	BOB - AX General Ledger Supervisor	SELECT	Application Object Library
2009-02-20 16:00:00.0	192.168.2.148	APPS	JOHN - System Administrator	INSERT	Application Object Library
2009-02-20 16:00:00.0	192.168.2.148	APPS	JOHN - System Administrator	SELECT	Application Object Library
2009-02-20 16:00:00.0	192.168.2.148	APPS	JOHN - AX Receivables User	CALL	Global Accounting Engine
2009-02-20 16:00:00.0	192.168.2.148	APPS	JOHN - AX Receivables User	CALL	Application Object Library
2009-02-20 16:00:00.0	192.168.2.148	APPS	JOHN - AX Receivables User	CALL	Federal Financials
2009-02-20 16:00:00.0	192.168.2.148	APPS	JOHN - System Administrator	CALL	Public Sector Financials

Figure 22: InfoSphere Guardium Application End-User Identifier empowers IT security organizations to rapidly identify fraud and other actions that violate corporate policies, such as unauthorized changes to sensitive data, in enterprise application environments with pooled connections (note DB User Name is APPS for all transactions). For the Oracle EBS environment it is also designed to be aware of, and utilize the responsibilities assigned to users when they are defined in EBS. Above, Bob's direct responsibility as AX General Ledger Supervisor is identified as part of the activity monitoring specified by his organization's policies, simplifying review of reports. We can also see that John has two roles; one as AX Receivables User, and another as System Administrator, identifying a potentially inappropriate entitlement.

Scalable Enterprise Security Platform

The Application End-User Identifier module is architected on InfoSphere Guardium's industry-leading Database Activity Monitoring (DAM) and Vulnerability Assessment (VA) technology, augmenting these core modules with application-specific policies, audit reports and tracking groups for selected enterprise platforms.

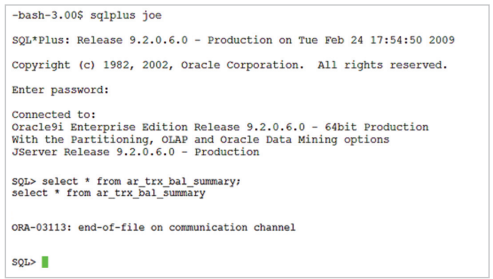
The DAM technology monitors all database access in real-time without relying on native database logs, impacting performance or requiring database changes. Unique in the industry, InfoSphere Guardium's multi-tier architecture automatically aggregates and normalizes audit information – from multiple DBMS systems and locations – into a single centralized repository. This enables enterprise-wide compliance reporting, correlation, forensics, and advanced database-focused analytics.



Policy Violations / Incident Management

Start Date: 2009-02-17 16:59:38 End Date: 2009-02-25 16:59:38

Violation Log Id	Timestamp	Category Name	Access Rule Description	Client IP	Server IP	DB User Name	Full SQL String	Severity Description	Incident Number
202	2009-02-24 17:58:47.0	sox	terminate unauthorized user access to EBS	192.168.2.148	192.168.2.148	JOE	select * from ar_trx_bal_summary	HIGH	0



```
-bash-3.00$ sqlplus joe

SQL*Plus: Release 9.2.0.6.0 - Production on Tue Feb 24 17:54:50 2009

Copyright (c) 1982, 2002, Oracle Corporation.  All rights reserved.

Enter password:

Connected to:
Oracle9i Enterprise Edition Release 9.2.0.6.0 - 64bit Production
With the Partitioning, OLAP and Oracle Data Mining options
JServer Release 9.2.0.6.0 - Production

SQL> select * from ar_trx_bal_summary;
select * from ar_trx_bal_summary


ORA-03113: end-of-file on communication channel

SQL>
```

Figure 24: Policy violations, such as circumventing EBS using tools like SQL *Plus to access data directly can be detected, and optionally blocked (left). Supporting detail can be logged (above) and automatically dispatched for investigation through workflow automation.

A graphical Web console provides centralized management of policies, report definitions, compliance workflow processes, and appliance settings (such as archiving schedules). This scalable, multi-tier architecture can easily be scaled up to meet any mix of throughput and auditing policies, simply by adding appliances which work together in a federated model.

InfoSphere Guardium also offers a Vulnerability Assessment module that provides a best practices library of automated tests for identifying vulnerabilities such as missing patches, misconfigured privileges, default accounts, and weak passwords. This module is supported by a Knowledge Base service that provides regular updates to vulnerability tests, as well as sensitive objects and preconfigured groups for SAP and Oracle EBS. By providing updated object lists and groups, IBM simplifies the task of monitoring access and changes to important tables.

Comprehensive Policy-Based Monitoring and Auditing

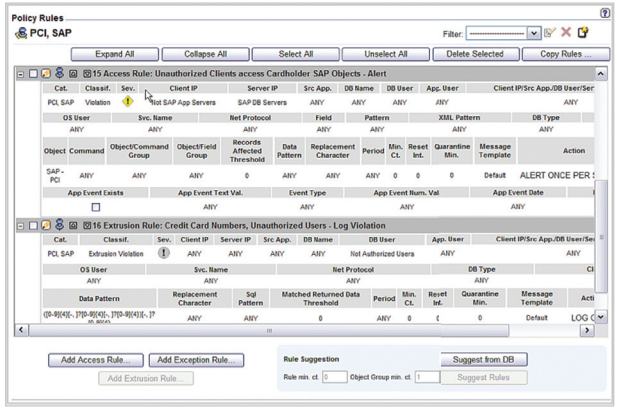


Figure 25: InfoSphere Guardium provides granular, preconfigured policies for SAP and Oracle EBS applications to rapidly identify suspicious or unauthorized activities such as changes to sensitive objects or multiple failed logins. Sensitive objects, which can require significant research to locate, are identified through the Knowledge Base service to facilitate the development of custom policies. A range of actions, such as real-time SNMP alerts, can be configured to occur when policy rules are violated.

InfoSphere Guardium provides:

- Built-in preconfigured reports developed specifically for SOX and PCI environments – environments that usually include enterprise applications within their scope.
- Built-in SOX and PCI DSS policies for Oracle EBS and SAP (see Figure 25).
- Comprehensive assessments of the underlying database engine where the application data is stored.
- Full activity and data access auditing that shows both direct and indirect activities performed and data accessed.
- Audit trails for activity performed by users, showing access at the database level with user IDs at the application level (see Figures 22, 26, and 27). Audit records show user IDs and the client host from which access was performed.

Broad Heterogeneous Application Support

InfoSphere Guardium supports application-layer monitoring for all major applications and application servers, without requiring application changes. These applications include:

- Oracle E-Business Suite
- SAP ERP and NetWeaver BW
- PeopleSoft
- Cognos
- Siebel
- Business Objects Web Intelligence

InfoSphere Guardium also identifies application user IDs for custom and packaged applications built upon standard application server platforms such as:

- IBM WebSphere
- BEA WebLogic
- Oracle Application Server
- JBoss Enterprise Application Platform.

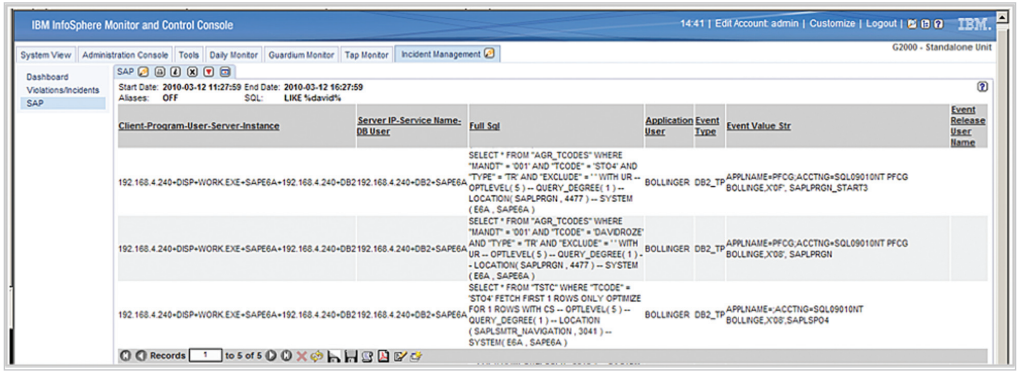
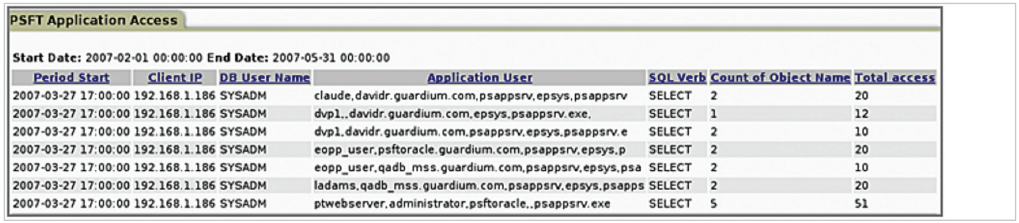


Figure 26: InfoSphere Guardium Application End-User Identifier is able to monitor all transactions between SAP and rich database environments like DB2 and Oracle.



Period Start	Client IP	DB User Name	Application User	SQL Verb	Count of Object Name	Total access
2007-03-27 17:00:00	192.168.1.186	SYSADM	claude,davidr.guardium.com,psappsrv,epsys,psappsrv	SELECT	2	20
2007-03-27 17:00:00	192.168.1.186	SYSADM	dvp1,,davidr.guardium.com,epsys,psappsrv.exe,	SELECT	1	12
2007-03-27 17:00:00	192.168.1.186	SYSADM	dvp1,davidr.guardium.com,psappsrv,epsys,psappsrv.e	SELECT	2	10
2007-03-27 17:00:00	192.168.1.186	SYSADM	eopp_user,psftoracle.guardium.com,psappsrv,epsys,p	SELECT	2	20
2007-03-27 17:00:00	192.168.1.186	SYSADM	eopp_user,qadb_mss.guardium.com,psappsrv,epsys,psa	SELECT	2	10
2007-03-27 17:00:00	192.168.1.186	SYSADM	ladams,qadb_mss.guardium.com,psappsrv,epsys,psapps	SELECT	2	20
2007-03-27 17:00:00	192.168.1.186	SYSADM	ptwebserver,administrator,psftoracle,,psappsrv.exe	SELECT	5	51

Figure 27: The End-User Identifier module identifies the user associated with specific transactions (Application User) in PeopleSoft pooled connection environments where traditional tools that relying on native database auditing information will only show the generic identifier (SYSADM).

Enterprise Integrator

Data Integration for Enhanced Operational and Security Effectiveness

- Easily connect to multiple relational databases or text files to retrieve and integrate data into the InfoSphere Guardium repository for audit completeness
- Create unified audit reports including external information that enhance security and improve operational efficiency
- Import descriptive information, such as full names and phone numbers corresponding to user names to streamline investigation of exceptions
- Integrate information such as roles and departments to enable deployment of finer grained security policies
- Create as single management point for all database security and compliance data by integrating journal information from environments such as IBM iSeries and Progress databases
- Leverage existing Tivoli and Centera infrastructures to simplify automated archiving of InfoSphere Guardium audit data and task results

Managing Complex, Rapidly Changing Environments

Managing database security and compliance has become increasingly challenging. Not only has the rate of cyberattacks continued to grow, but the complexity of the environments managed has increased dramatically.

Driven by a rapidly changing business landscape that includes mergers, outsourcing, workforce adjustments and accelerating business automation, the information needed to effectively create, manage and report on security policies is increasingly difficult to access in a timely manner. Databases continue to proliferate across geographical and organizational boundaries, administrative and entitlement information is fragmented across a variety of systems, personnel and system data is constantly changing, while audit information expectations are steadily increasing.

Traditionally enterprises have relied on manual processes to gather the information needed to ensure database security policies and reports contain accurate and meaningful data. 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.

Automate the Acquisition, Integration and Archiving of all Security Data

InfoSphere Guardium's Enterprise Integrator is an optional software module which simplifies and automates the integration of data from external databases or text files into the InfoSphere Guardium repository, as well as enabling existing enterprise storage infrastructure to be utilized for archiving. Its powerful capabilities enable a wide variety of functionality ranging from new applications like automated change control reconciliation to process and policy improvements that eliminate costly manual efforts.

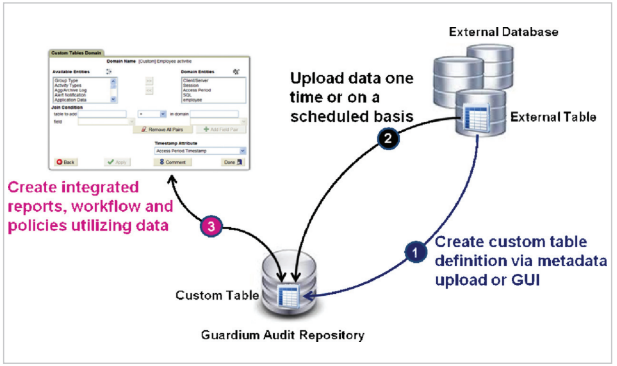


Figure 28: The Enterprise Integrator provides a simple means to integrate important security related information from external sources. Tools are provided to automatically or manually: 1) Create a custom table definition for the imported data in the InfoSphere Guardium Audit Repository 2) Upload the data from the external source 3) Create data links so the full array of InfoSphere Guardium tools can seamlessly utilize the imported data.

External information can be integrated with a few simple steps (see Figure 28). First, a custom table is created to house the data. The table definition can be created by providing InfoSphere Guardium with the information needed to retrieve metadata from the source database, or a more specific GUI can be used to manually enter the table definition. The target data is then uploaded, with InfoSphere Guardium providing tools to check schema compatibility and execute any post-upload DML desired. Uploads can be one-time events, or regularly scheduled, allowing the repository to be kept in synch with changing primary data sources without manual intervention.

With data housed in the repository, the full array of InfoSphere Guardium policy, analysis, reporting and workflow tools can be leveraged. For example, journaling information from unique environments like the IBM iSeries can be imported so automated reporting, workflow and sign-off tools are applied to the data, ensuring policy consistency and improving operational efficiency. Uploaded data may also be linked to existing data in the repository. This enables important descriptive information to be added to reports and policies (see Figure 29), eliminating manual lookup, and providing data critical to identifying certain policy violations.

Automate Change Control Reconciliation

Most organizations have formal change control policies and processes that govern how and when changes are made to production databases. However, since the change management application and the production database are different systems, in most cases unauthorized changes cannot be detected. Without enforcement mechanisms, change control policies are ineffective. Yet the only option typically available, manual reconciliation using native auditing logs, is extremely labor intensive.

By using the Enterprise Integrator in conjunction with the core InfoSphere Guardium system, change control policies can be easily enforced without significant labor. The Enterprise Integrator enables approved change requests from the change management system to be retrieved and brought into the InfoSphere Guardium system. In commercial systems such as BMC's Remedy and HP's Peregrine, requests include business level summary descriptions. Linking the change descriptions to actual changes observed by InfoSphere Guardium through the ticket ID allows automation of the reconciliation process (see Figure 30). Reviewers are able to easily compare the Summary description to

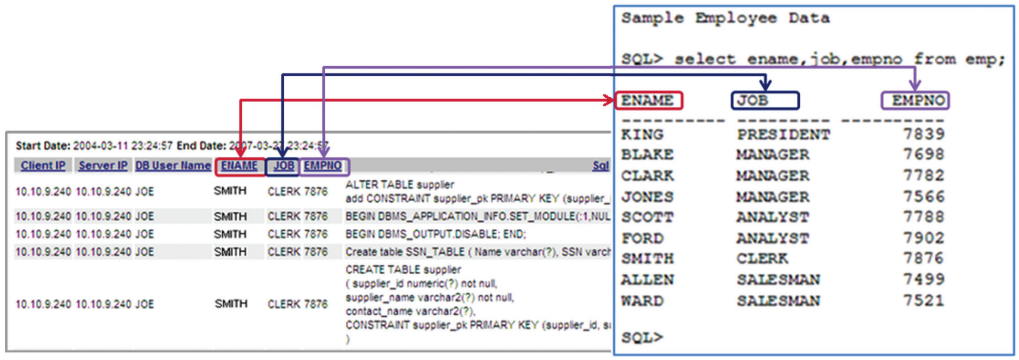


Figure 29: The Enterprise Integator enables users to create unified audit reports including external information, which can enhance security and improve operational efficiency. For example, real employee names (ENAME) and numbers (EMPNO) stored in a remote employee database can easily be integrated so exception reports can be investigated without having to manually research the employee corresponding to a particular DB User Name. Importing employee's job classification (JOB) allows potentially inappropriate activity to be identified, such as a CLERK modifying database tables.

the executed SQL commands to ensure the change made is appropriate. Workflow automation ensures all changes are reviewed and approved, and issues are flagged for follow-up and remediation. If changes are made without valid ticket IDs, outside authorized change periods or with unauthorized user IDs, they are automatically detected. A variety or responses are possible, ranging from issuing a real-time alert to blocking the action.

Automating change-control reconciliation safeguards valuable data and demonstrates the proactive controls which satisfy the requirements of discerning auditors.

Eliminate Security Gaps by Automating Policy Information Updates

Although InfoSphere Guardium may initially be deployed to protect a particular high value asset, over time the use of the system is typically expanded to encompass all of the enterprise's sensitive databases. As the system scales, the use of groups becomes important. A group is set of elements sharing a common property. Using groups simplifies the development and maintenance of policies and reports. For example, an organization may have 30 separate objects containing sensitive financial data. Rather than creating policies and reports specifying all these objects individually, a SOX group can be defined that encompasses all the members. As a result, the policies and reports designed to monitor and report on access to SOX objects become simpler.

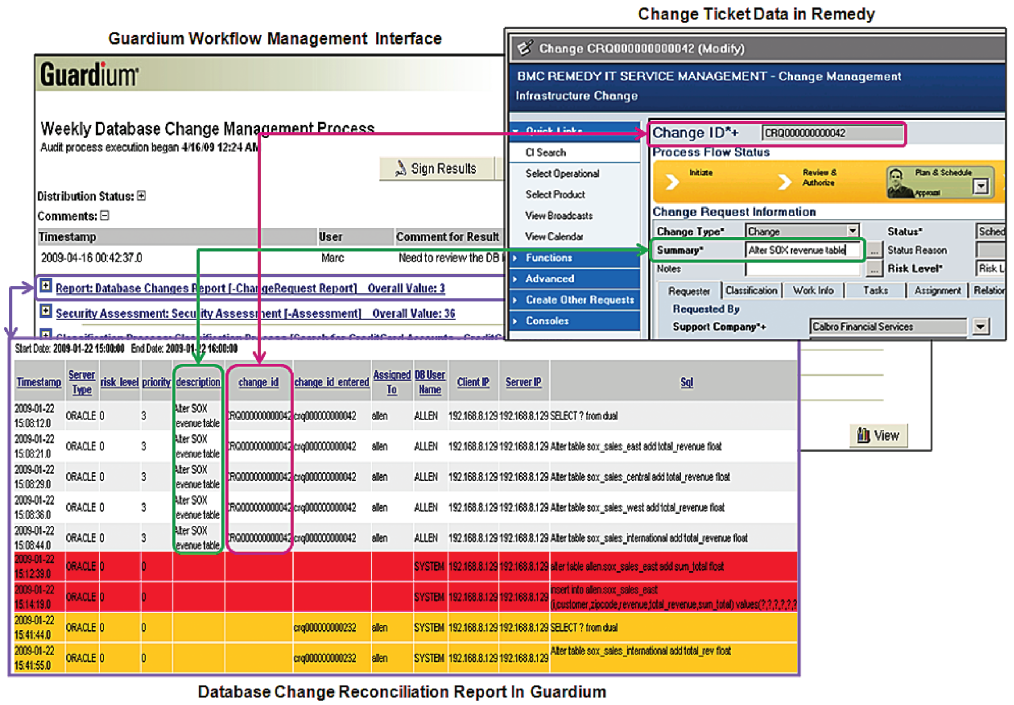


Figure 30: The Enterprise Integrator can be used to import change management information from custom or commercial systems like BMC's Remedy or HP's Peregrine. In this example the Change ID and Summary description are included in a weekly Database Change Report which is distributed and managed using InfoSphere Guardium's workflow capabilities. The report has been structured so actual changes made with no tickets are highlighted in red. Changes in yellow indicate an invalid change number was entered for the change. Displaying the Remedy Summary of the authorized change along with the actual SQL commands executed allows report recipients to verify that changes made correspond to those authorized.

Enterprise Integrator Support	
Data Sources	Out-of-the-box support for Oracle, DB2, Sybase, Microsoft SQL Server, Informix, mySQL, Teradata, Netezza and PostgreSQL data sources
Connections	Out-of-the-box support for HTTP, HTTPS, FTP, SAMBA and IBM iSeries connections to CSV text file data sources

Groups are used to simplify management of a wide variety of other objects such as classes of servers (for example those containing SOX, PCI, PII data) and users (for example privileged users, user authorized to access SOX objects or business partners responsible for reviewing exceptions for a group of servers). Often the data contained in groups originates, and is maintained, in a database on the network. By using Enterprise Integrator to retrieve this data and populate the group, both labor and errors can be eliminated. More importantly, as objects change (due to changes in responsibility, infrastructure changes, etc.), group membership can automatically be updated, without making any changes to the InfoSphere Guardium groups or policies, by scheduling regular Enterprise Integrator uploads. This too will eliminate work, and avoid the introduction of security gaps that result when group membership data is not current.

Automate Archiving to Reduce Compliance Costs

In most organizations, compliance mandates and internal policies require that all InfoSphere Guardium data, both audit data and audit tasks results, be archived for reporting and forensic purposes. To support this need, the solution includes automated archiving and restoration capabilities. The Enterprise Integrator includes out-of-the-box connectors for both Tivoli Storage Manager and EMC Centera, allowing these major enterprise archiving solutions to be easily used with InfoSphere Guardium's archiving capabilities.

Users need only enter configuration information such as the pool connection string and password to enable InfoSphere Guardium to connect to these systems. With the Enterprise Integrator users can leverage existing enterprise archiving solutions without the need to develop custom integrators.

IBM InfoSphere Guardium for z/OS

Complete Auditing Visibility for DB2 Using Proven z/OS Technology

- Monitors and audits all database activity on z/OS by privileged users, mainframe-resident applications and network clients
- Provides visibility at a granular level into critical operations including SELECTs, DDL, DML, access grants and revokes
- All analysis, reporting and storage of audit data is performed off-mainframe in a secure environment
- Integrates with the enterprise-wide Guardium architecture to provide a unified security and compliance solution for both mainframe and distributed database environments
- Utilizes proven z/OS technology from IBM to maximize reliability and efficiency

Growing DB2 Security and Compliance Requirements

Many organizations host extensive amounts of data 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, mainframe data is often within the scope of a growing range of compliance mandates. This is compelling organizations to implement new controls to ensure their DB2 data is secure from unauthorized access and tampering by both internal and external parties, and that a detailed audit trail validating the effectiveness of the controls can easily be made available to auditors.

IBM's InfoSphere Guardium solution offers a simple yet powerful means of securing critical data across the enterprise. It provides rapid policy-based detection of anomalous activities that violate corporate policies, real-time responses such as alerts, auditable workflow to ensure appropriate resolution of exceptions, along with automated reporting capabilites which simplify validation of compliance for mandates such as SOX, PCI DSS and data privacy regulations.

InfoSphere Guardium for z/OS 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 monitoring components across the enterprise (see Figure 31), to provide a secure, centralized audit repository and management point.

Avoid the Security and Cost Issues Associated With Traditional Solutions

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

- Reliance on mainframe Database Administrators (DBAs) 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 granular analysis and alerting capability, eliminating the possibility of immediately detecting and containing important categories of unauthorized activities (such as an unauthorized update to data a user is authorized to access)
- The need to apply significant amounts of skilled labor to maintain custom software or to analyze reports to detect policy violations

InfoSphere Guardium for z/OS eliminates these limitations, while providing important additional

capabilities such as compliance workflow automation, reporting and an enterprise-wide view of your database security and compliance posture.

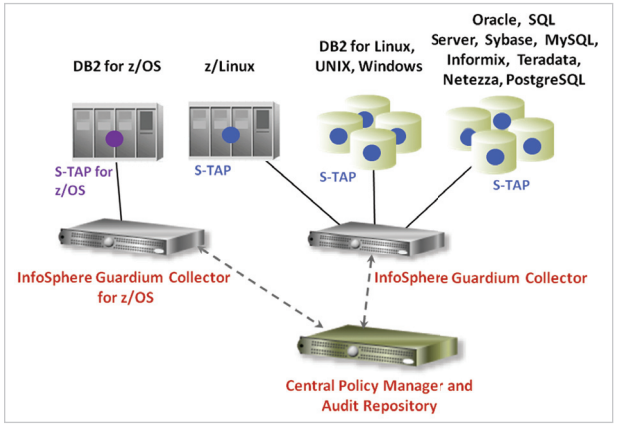


Figure 31: Guardium uses a lightweight software probe called S-TAP for z/OS to capture key database activities executed by privileged users, mainframe-resident applications and network clients on z/OS. Both mainframe and distributed environments can be monitored from a single console; in addition, all audit data is automatically aggregated and normalized into a single centralized repository for enterprise-wide compliance reporting, analytics and forensics.

Scalable Enterprise-Wide Database Security and Compliance Platform

InfoSphere Guardium for z/OS uses a lightweight software probe called S-TAP for z/OS to capture all database activities by privileged users, mainframe-resident applications and network clients, including those connecting via services such as JDBC or DB2 Connect. Proven IBM DB2/z event capture technology is used to ensure all critical operations such as SELECTs, DML, DDL and access grants are captured, without the use of DB2 Class 4 and Class 5 audit traces.

S-TAP for z/OS sends information specified by user defined audit policies (see Figure 32) to an InfoSphere Guardium Collector for z/OS appliance. This ensures the mainframe is not burdened with incremental storage or processing requirements, network traffic is limited and a full audit trail is stored securely. S-TAP event capture technology can also be shared by IBM Query Monitor, providing further performance enhancements for clients utilizing both offerings.

Unique in the industry, InfoSphere Guardium's multi-tier architecture (see Figure 31) aggregates and normalizes audit information – across database platforms, applications and locations – into a single centralized repository. This provides comprehensive enterprise-wide compliance reporting, correlation, forensics, and 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 S-TAPs, Collectors and Aggregators, which work together in a federated model.

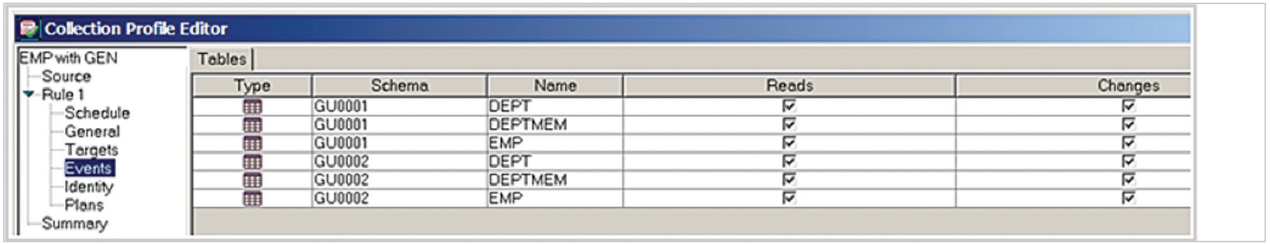
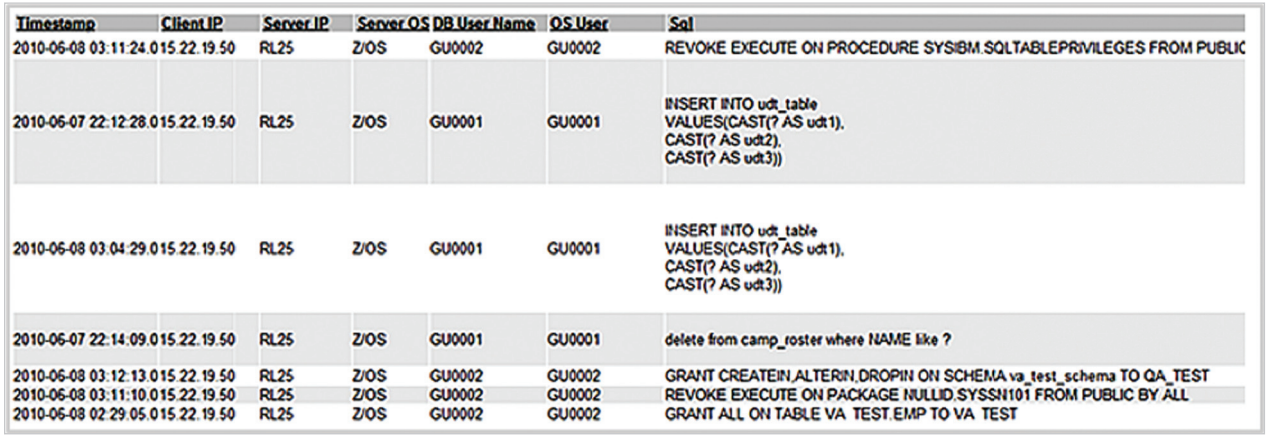


Figure 32: Audit policies which define which DB2 transactions are to be captured can be easily built using the Windows-based audit policy editor.



Timestamp	Client IP	Server IP	Server OS	DB User Name	OS User	Sql
2010-06-08 03:11:24.015	22.19.50	RL25	Z/OS	GU0002	GU0002	REVOKE EXECUTE ON PROCEDURE SYSIBM.SQLTABLEPRIVILEGES FROM PUBLIC
2010-06-07 22:12:28.015	22.19.50	RL25	Z/OS	GU0001	GU0001	INSERT INTO udt_table VALUES(CAST(? AS udt1), CAST(? AS udt2), CAST(? AS udt3))
2010-06-08 03:04:29.015	22.19.50	RL25	Z/OS	GU0001	GU0001	INSERT INTO udt_table VALUES(CAST(? AS udt1), CAST(? AS udt2), CAST(? AS udt3))
2010-06-07 22:14:09.015	22.19.50	RL25	Z/OS	GU0001	GU0001	delete from camp_roster where NAME like ?
2010-06-08 03:12:13.015	22.19.50	RL25	Z/OS	GU0002	GU0002	GRANT CREATEIN,ALTERIN,DROPIN ON SCHEMA va_test_schema TO QA_TEST
2010-06-08 03:11:10.015	22.19.50	RL25	Z/OS	GU0002	GU0002	REVOKE EXECUTE ON PACKAGE NULLID.SYSSN101 FROM PUBLIC BY ALL
2010-06-08 02:29:05.015	22.19.50	RL25	Z/OS	GU0002	GU0002	GRANT ALL ON TABLE VA_TEST.EMP TO VA_TEST

Figure 33: Guardium provides full visibility into DB2 data usage on z/OS, capturing both mainframe and network access with key details such as OS user name, client IP, database user name and SQL statements executed.

Automated, Policy-Based Monitoring and Auditing Streamline Compliance Validation

The InfoSphere Guardium Web console provides centralized management of alerts, report definitions, compliance workflow processes, and settings (such as archiving schedules) without the involvement of DBAs, providing the SOD required by auditors and streamlining compliance activities. A broad range of management functions can be executed across your entire database infrastructure, including:

- Defining 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, OS user name, source application or time-of-day
- Automatically creating a baseline of normal activities to suggest policies which will detect anomalous activities such as SQL injection attacks
- Defining actions in response to policy violations, such as generating alerts and logging full incident details
- Automating compliance workflow for routine activities as well as incident responses, including steps such as sign-offs, commenting and escalation
- Running hundreds of out-of-the box reports including those required for SOX, PCI DSS and data privacy laws, as well as creating customized reports

With InfoSphere Guardium, you gain full visibility into your DB2 environment, enabling unauthorized 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.

Comprehensive Support for IBM Environments

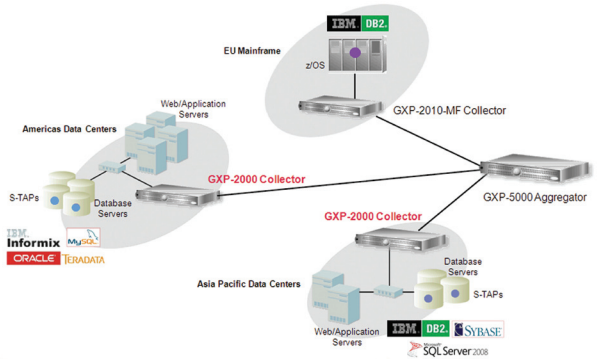
The InfoSphere Guardium solution provides support for other popular IBM platforms including:

- IBM DB2 for Linux, UNIX and Windows
- IBM Informix
- IBM DB2 for iSeries
- 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
- Cognos 8, for which InfoSphere Guardium identifies fraud and other unauthorized activities via application-layer monitoring. Guardium also supports other enterprise applications such as SAP, PeopleSoft and SOA applications developed for IBM WebSphere Application Server and other middleware platforms.

IBM InfoSphere Guardium for z/OS	
Supported DB2Versions	DB2 for z/OS V7 or V8 or V9
Supported z/OS Versions	z/OS V1.6 or later

IBM InfoSphere Guardium Collector Hardware Unit

High-Performance Hardware for Secure Audit Data Collection, Analytics and Compliance Reporting



The IBM InfoSphere Guardium Collector Hardware Unit is a hardened 1U rack-mountable hardware component built on a high-performance, industry-standard server platform. It executes licensed InfoSphere Guardium software to collect data from lightweight host-based probes (S-TAPs) that monitor all database traffic, including local access by privileged users. Data can also be collected from the SPAN ports in network switches.

Built with a hardened OS and database kernel, the InfoSphere Guardium Collector is fully locked and tamper-proof. There is no super user or root access to the appliance, preventing administrators from accessing the base OS, file system or embedded database to view or modify audit data. The InfoSphere Guardium Collector is delivered with licensed software fully loaded, tested and ready for deployment. The InfoSphere Guardium solution is also available as a preconfigured virtual appliance for VMware infrastructures.

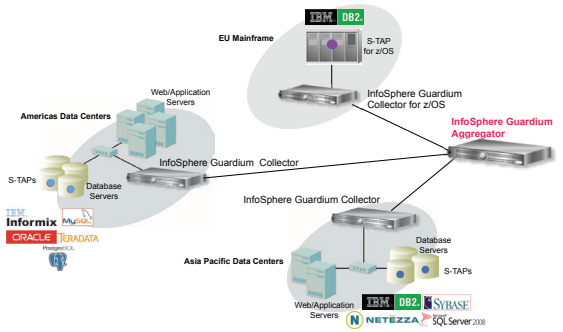
Feature	Specification
Form Factor	1U
CPU	Two Quad Core Xeon X5650 processors, 12 MB cache, 2.66 GHz
Memory	12 GB, 1033 MHz
Network Interface	4 ports, Gigabit Ethernet NIC
Network Speeds	10/100/1000 Mbps
Internal Storage	Two 600 GB, SAS, 2.5 inch, 10K RPM, RAID-1, hot-swappable
Power	Dual Energy Smart power supply, redundant, 502W, hot-plug, auto-sensing
High Availability	Multi-LAN; hot-plug RAID-1 protected internal storage; hot-plug redundant power supply
Expansion Slots	Accommodate 1 or 2 separately purchasable quad NIC options
Remote Management	DRAC function
Options	**Description**
Networking Card	Quad fiber NIC
Networking Card	Quad copper NIC

Figure 1: InfoSphere Guardium Collector Hardware Unit Specifications

Contents > IBM InfoSphere Guardium Aggregator Hardware Unit

IBM InfoSphere Guardium Aggregator Hardware Unit

High Performance Hardware for Centralized Audit Data Aggregation, Analytics and Compliance Reporting



IBM's InfoSphere Guardium Aggregator Hardware Unit is a hardened 1U rack-mountable hardware component built on a high-performance, industry-standard server platform. It executes licensed InfoSphere Guardium software to automatically aggregate audit data from multiple collector appliances. For maximum scalability and flexibility, you can configure multiple tiers of aggregators to integrate all audit information into a single centralized repository.

Built with a hardened OS and database kernel, the InfoSphere Guardium Aggregator is fully locked and tamper-proof. There is no super user or root access to the appliance, preventing administrators from accessing the base OS, file system or embedded database to view or modify audit data. The InfoSphere Guardium Aggregator is delivered with licensed software fully loaded, tested and ready for deployment. The InfoSphere Guardium solution is also available as a preconfigured virtual appliance for VMware infrastructures.

Feature	Specification
Form Factor	1U
CPU	Two Quad Core Xeon X5650 processors, 12 MB cache, 2.66 GHz
Memory	12 GB, 1033 MHz
Network Interface	4 ports, Gigabit Ethernet NIC
Network Speeds	10/100/1000 Mbps
Internal Storage	Two 600 GB, SAS, 2.5 inch, 10K RPM, RAID-1, hot-swappable
Power	Dual Energy Smart power supply, redundant, 502W, hot-plug, auto-sensing
High Availability	Multi-LAN; hot-plug RAID-1 protected internal storage; hot-plug redundant power supply
Expansion Slots	Accommodate 1 or 2 separately purchasable quad NIC options
Remote Management	DRAC function
Options	**Description**
Networking Card	Quad fiber NIC
Networking Card	Quad copper NIC

Figure 1: InfoSphere Guardium Aggregator Hardware Unit Specifications

IBM Corporation
Route 100
Somers, NY 10589

Produced in the United States of America
May 2010

Please Recycle

InfoSphere®
software

IMB14083USEN-01