IBM InfoSphere Guardium

Database Activity Monitoring and Vulnerability Assessment Suites

IBM

Contents

InfoSphere Guardium overview

The IBM® InfoSphere® Guardium® solution provides a simple, robust means of 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, IBM Cognos® and others).
- Database leak prevention for locating sensitive data and thwarting data center breaches.

The solution is now installed in more than 500 client sites worldwide, including all of the top five global banks; top global insurance agencies; top government agencies; two of the top global retailers; 25 of the world's leading telecommunications companies; four of the top four managed healthcare organizations; one of the most recognized names in personal computers; a top three auto maker; and leading energy suppliers. 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 paper provides an overview of a variety of optional capabilities available for the InfoSphere Guardium solution. For a more complete overview of the core InfoSphere Guardium solution, please see the InfoSphere Guardium data sheet.

Real-time database security and monitoring

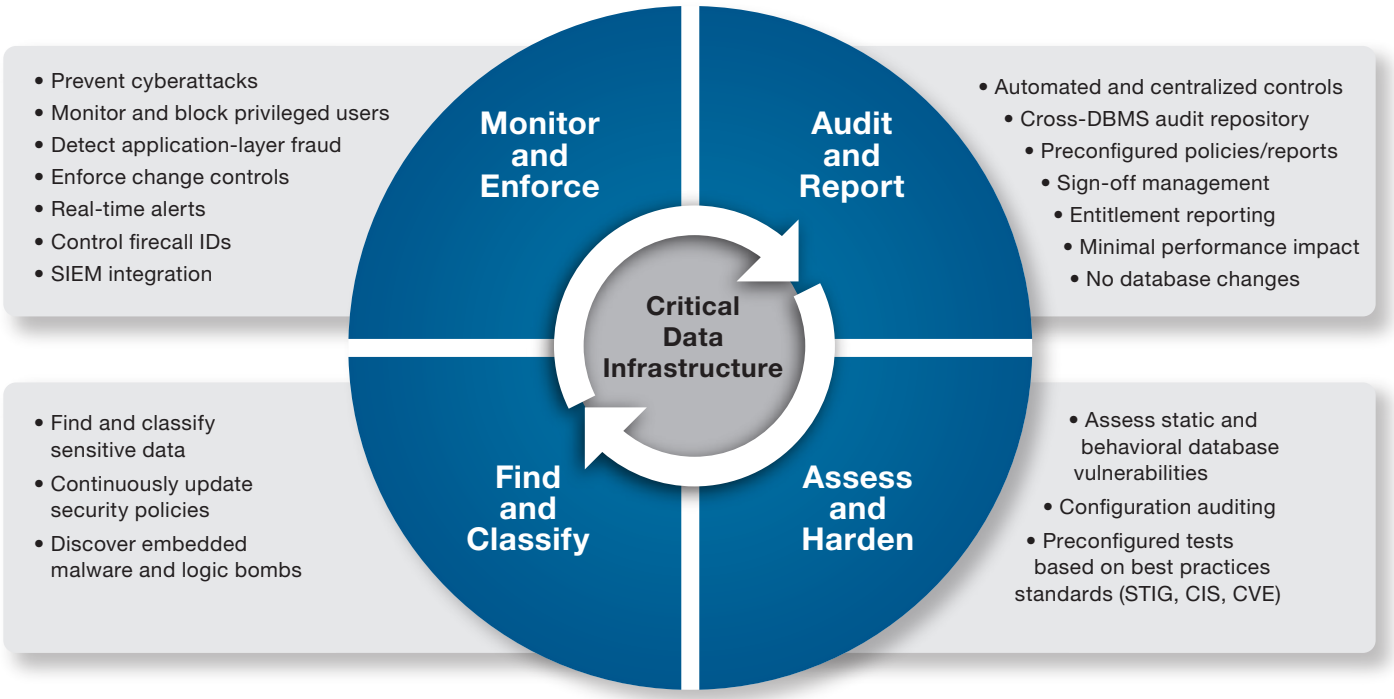


Figure 1: Built upon a single unified console and back-end data store, the InfoSphere Guardium solution offers a family of integrated modules for managing the entire database security and compliance life cycle.

Guardium is part of IBM InfoSphere, an integrated platform for defining, integrating, protecting and managing trusted information throughout 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, enabling you to start anywhere and mix and match InfoSphere software building blocks with components from other vendors, or 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.

Application End-User Identifier

Detects fraud in real time by monitoring application-user activities

Highlights

- 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.

The InfoSphere Guardium Application End-User Identifier module 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.

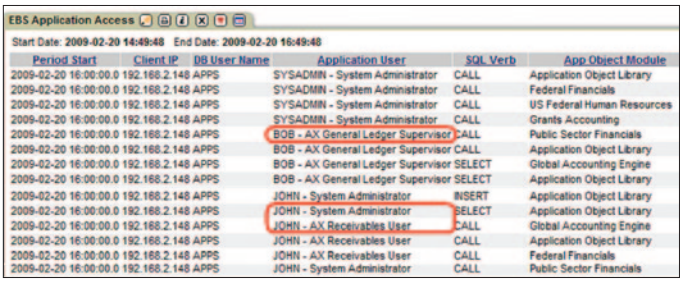
The primary purpose of application-layer monitoring is to detect fraud that occurs by way of enterprise applications. This level of monitoring is often required for data-governance requirements, such as SOX, ISO 270001, SAS 70 and NIST 800-53 controls.

Securing multitier enterprise applications

Multitier 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, multitier 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 are relying on traditional database logging tools that can monitor and identify users based on their database login accounts only.

Because enterprise-application data resides in relational databases, it can also be accessed through direct database connections (for example, by way of 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 2, 6 and 7), and identifies direct access by privileged users to unauthorized objects. For example, in Figure 4 a policy specifying that 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.



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 2: The InfoSphere Guardium Application End-User Identifier module 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 use 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.

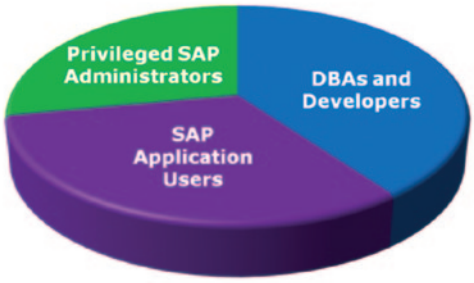


Figure 3: The InfoSphere Guardium solution protects enterprise-application environments from all major sources of risk.

Scalable enterprise-security platform

The Application End-User Identifier module is architected on industry leading InfoSphere Guardium 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, the InfoSphere Guardium solution's multitier 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.

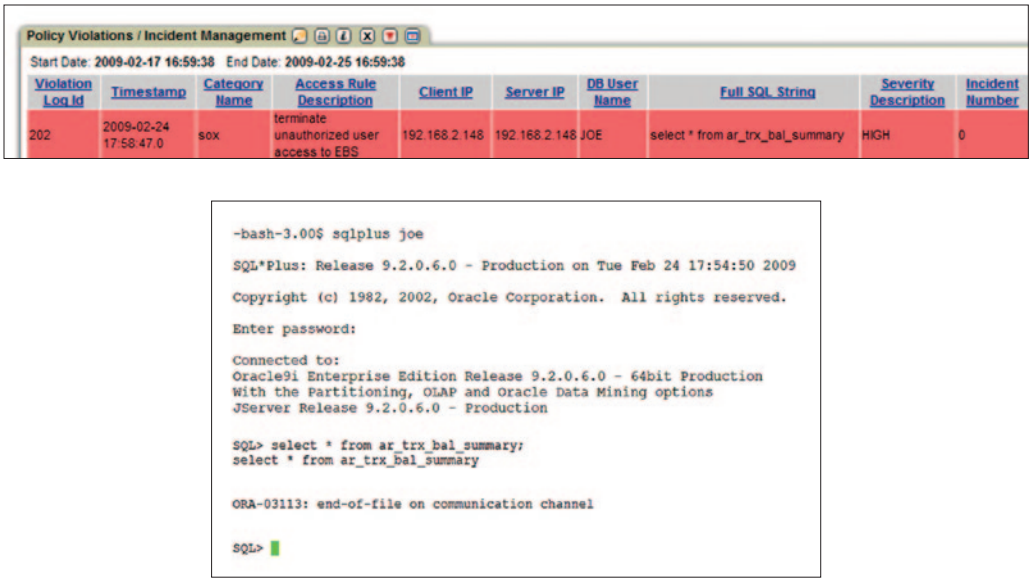


Figure 4: Policy violations, such as circumventing EBS using tools like SQL *Plus to access data directly, can be detected and optionally blocked (see lower portion of figure). Supporting detail can be logged (see upper portion of figure) and automatically dispatched for investigation through workflow automation.

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

The InfoSphere Guardium solution also offers a Database 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 Knowledgebase 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

The InfoSphere Guardium solution 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 5).
- 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 2, 6 and 7). Audit records show user IDs and the client host from which access was performed.

Broad heterogeneous-application support

The InfoSphere Guardium solution 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
- IBM Cognos
- Siebel
- Business Objects Web Intelligence

The InfoSphere Guardium solution 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

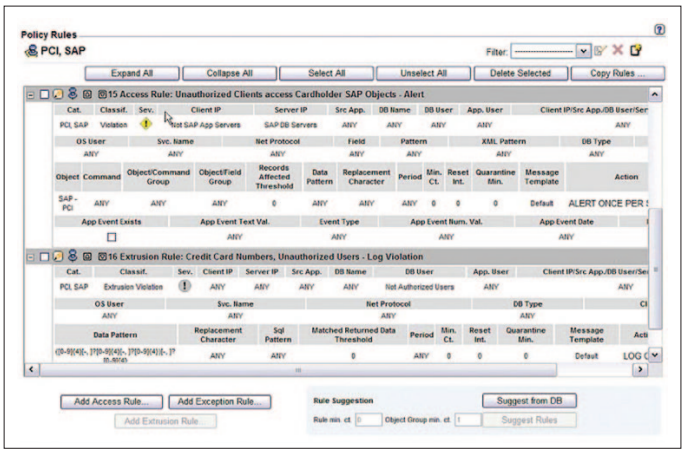


Figure 5: The InfoSphere Guardium solution provides granular, preconfigured policies for SAP and Oracle EBS applications to rapidly identify suspicious or unauthorized activities, such as changes to sensitive objects or multiple failed logins. Sensitive objects, which can require significant research to locate, are identified through the Knowledgebase 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.

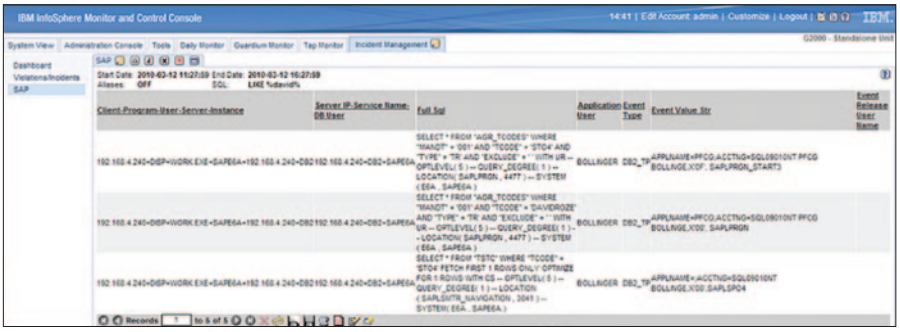


Figure 6: The InfoSphere Guardium Application End-User Identifier module is able to monitor all transactions between SAP and rich database environments like DB2 and Oracle.

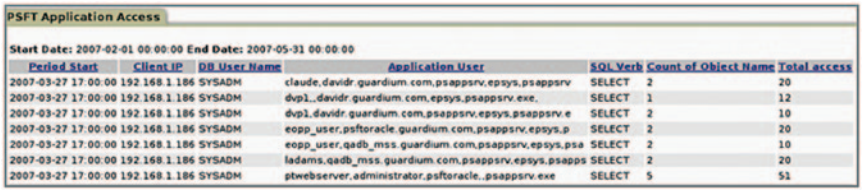


Figure 7: The Application End-User Identifier module identifies the user associated with specific transactions (Application User) in PeopleSoft pooled-connection environments where traditional tools that relying on native database auditing information will show only the generic identifier (SYSADM).

Sensitive Data Finder

Places controls on all sensitive data

Highlights

- Automates the process of finding and classifying sensitive data, using intelligent search technology
- Supports a wide range of responsive actions, ranging from real-time alert generation to automated application of appropriate policies
- Maximizes the identification of sensitive data by providing four complementary search techniques
- Integrated with other InfoSphere Guardium applications, including Compliance Workflow Automation, Incident Management and Reporting to maximize security and minimize operational costs

The importance of unknowns

The task of securing sensitive data begins with identifying it. This can be challenging, because database environments are highly dynamic: the content of known instances is constantly changing and most organizations lack an effective means of identifying and understanding the content of unknown instances. In mature organizations, legacy databases deployed before change control mechanisms had been implemented are not uncommon. Larger organizations growing through acquisition often struggle to gauge with certainty sensitive data risk in acquired infrastructures. Even in stable environments, where cataloging processes have historically existed, uncontrolled instances can inadvertently be introduced through mechanisms, including developers that create "temporary" test environments; business units seeking to rapidly implement local applications; and purchases of new applications with embedded databases.

Data compiled from hundreds of actual data breaches over the past several years consistently shows victims' lack of comprehensive understanding of their environment is a contributing factor in losses. In roughly 20 percent of incidents, unknown data played a role in the compromise. To minimize this risk, organizations need a systemic way to identify all database instances in their environment and determine on an ongoing basis which instances contain sensitive data, so that appropriate controls can be implemented.

Automate identification of sensitive data to maximize security and minimize compliance costs

The InfoSphere Guardium solution provides a complete means for addressing the entire database security and compliance life cycle. This includes applications to automate the discovery and classification of sensitive data, as well as ensuring appropriate action is taken upon discovery. The Auto-Discovery application can be configured to probe specified network segments on a scheduled or on-demand basis, and can report on all databases discovered—solving the problem of identifying both legacy and newly introduced databases.

Once instances of interest are identified, the Sensitive Data Finder application can be used to examine the content of each to determine whether sensitive data is included, then take appropriate action. The examination process is defined using the Classification Policy Builder function, which provides an easy-to-use graphical interface to define a series of search rules (see Figure 8) which are applied to identify one or more categories of sensitive data. When a match is found, the rule can specify a wide variety of responsive actions, including:

- Logging the match.
- Sending a real-time alert detailing the match to an oversight team.
- Automatically adding the object to an existing privacy set or group (objects with similar properties, such as those containing payment card data), ensuring related security policies are automatically applied to the newly discovered object.
- Inserting a new-access rule into an existing security-policy definition.

Classification policies can be run against any specified database group on a scheduled or on-demand basis, using limited read-only credentials.

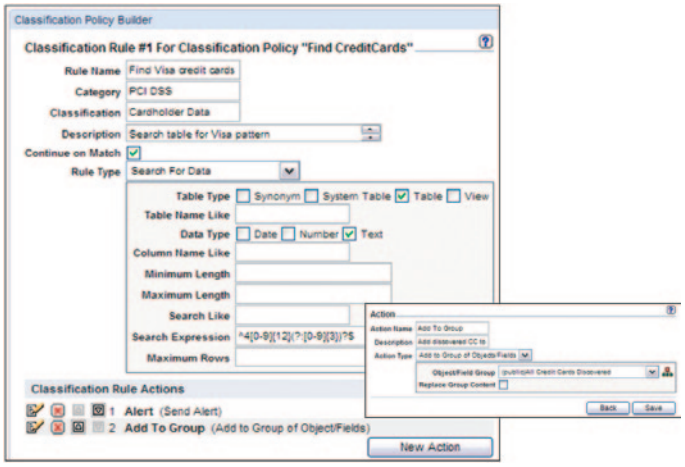


Figure 8: The InfoSphere Guardium Sensitive Data Finder application automates the process of identifying sensitive data and taking appropriate responsive action. Search rules and actions are defined through an easy-to-use graphical interface, then applied on a scheduled or on-demand basis. In this example a simple regular expression to search for the payment card pattern used by VISA was built using the pop-up regex editor. When a match is found, the oversight team will be alerted and the object will be added to the Credit Cards Discovered group.

This capability simplifies compliance validation, reduces operational costs and improves security. For example, databases considered out-of-scope for a particular compliance policy can be regularly scanned to prove to auditors that no data has been introduced which brings them in-scope. Should sensitive data be discovered, the appropriate policy can be applied automatically, enhancing security and demonstrating the proactive controls sought by auditors. Similarly, the Auto-Discovery application can be used to demonstrate that a process exists to identify all new instances. Using the Sensitive Data Finder application, those with sensitive data can be classified, with appropriate controls implemented, and proof that the remainder are out-of-scope can be more easily provided to auditors.

Powerful search techniques maximize results

Classification rules can be built using the following four different search techniques, which are easily selected from a pull-down menu in the policy builder (see "Rule Type" in Figure 9):

1. **Search for data.** This technique searches for a particular data value or a particular pattern, using a custom algorithm provided by the user or a regular expression built using the InfoSphere Guardium solution's POSIX 1003.2-compliant regex builder. Custom algorithms are uploaded as a Java class conforming to an IBM-provided interface. Templates for common expressions like credit cards, phone numbers and national identity numbers are provided for those using regular expressions. Luhn algorithm support is also provided. The Luhn algorithm was invented by an IBM scientist, and is widely used to validate identification number matches, such as credit cards.
2. **Catalog search.** This technique searches the database catalog for tables or column names matching specified patterns.
3. **Search by permissions.** This option searches the database catalog for tables based on permissions granted to users or roles, or both.
4. **Search for unstructured data.** This technique searches a non-database file for a particular value or pattern.

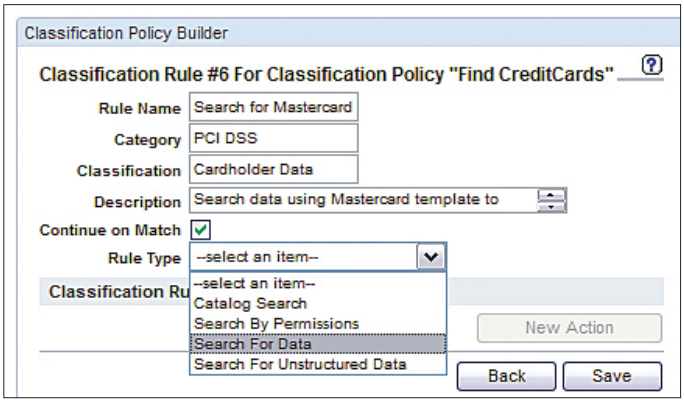


Figure 9: The Sensitive Data Finder application supports four different search techniques, which are selected from a pull-down menu.

The breadth of techniques available in the InfoSphere Guardium solution provides organizations with the flexibility to use the technique, or combination of techniques, most appropriate for a particular application. Irrespective of the approach selected, a variety of tuning and throttling techniques are provided to help users optimize the application for their production environment. These include resource throttles, query optimizations and sampling techniques that can be configured for lightweight scans or more comprehensive scans, depending upon requirements. Match thresholds are also supported to filter out false-positives.

An essential application for database infrastructures

The Sensitive Data Finder application is important for improving security and reducing operational costs. By automating the process of discovering sensitive data, as well as validating the absence of sensitive data, the application eliminates time-consuming, error-prone manual processes. It also adds credibility to data provided to auditors, because many prefer results generated by proven commercial tools.

The Sensitive Data Finder application is integrated with a variety of other InfoSphere Guardium applications to further automate operations and reduce costs. These include:

- **Reporting.** This application ensures summary results of scans are readily available to oversight teams, auditors and other stakeholders.
- **Compliance Workflow Automation.** This application enables matches to be automatically routed to appropriate oversight personnel, with electronic sign-offs, comments and escalations captured as part of the audit trail.
- **Incident Management.** This application provides enterprise-wide management of all incidents, including sensitive data discovery, to ensure timely follow-up.

Data-Level Access Control

Simplifies preventive control for heterogeneous DBMS environments

Highlights

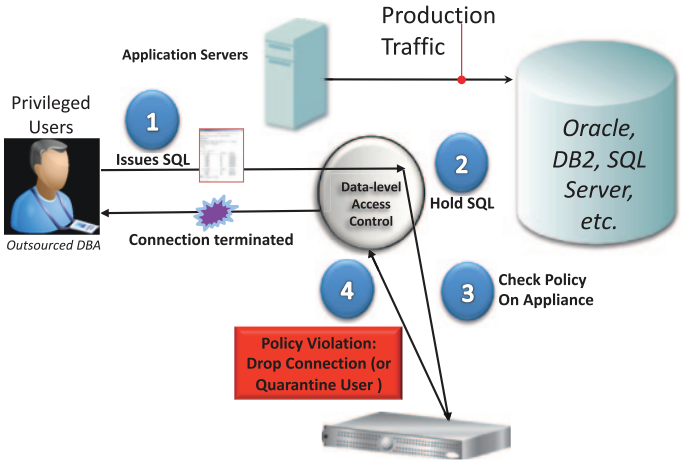
- Blocks privileged users from viewing or changing sensitive data, creating new user accounts or elevating privileges
- Has no impact on application-level traffic
- Supports IT outsourcing and associated cost savings—without increasing risk
- Enforces separation of duties for SOX, PCI DSS, Basel II and data privacy regulations
- Simplifies security and compliance by way of a 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

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 10: The InfoSphere Guardium Data-Level Access Control module simplifies enterprise security with a single set of granular policies for enforcing separation of duties spanning 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. The InfoSphere Guardium Data-Level Access Control module monitors all database connections, including local access by privileged users, by way of non-TCP connections, such as Oracle BEQ, SHM, TLI, IPC and others.

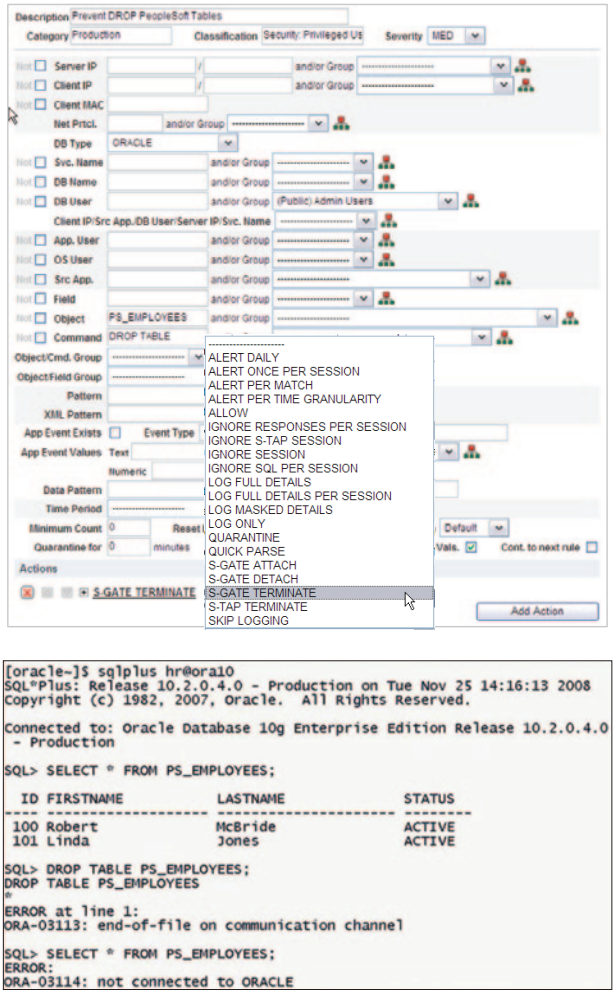
While DAM is an important element of a defense-in-depth strategy, it has traditionally been limited to providing detective controls rather than preventive controls, because monitoring alone cannot enforce security policies and prevent unauthorized actions from occurring.

Real-time preventive controls; no disruption to IT infrastructures

Implemented as a lightweight, host-based software agent (see Figure 10) with fine-grained security policies (see Figure 11), the InfoSphere Guardium Data-Level Access Control module 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

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




```
[oracle~]$ sqlplus hr@ora10
SQL*Plus: Release 10.2.0.4.0 - Production on Tue Nov 25 14:16:13 2008
Copyright (c) 1982, 2007, Oracle.  All Rights Reserved.

Connected to: Oracle Database 10g Enterprise Edition Release 10.2.0.4.0
 - Production

SQL> SELECT * FROM PS_EMPLOYEES;

  ID FIRSTNAME            LASTNAME             STATUS
---- -------------------- -------------------- --------
 100 Robert               McBride              ACTIVE
 101 Linda                Jones                ACTIVE

SQL> DROP TABLE PS_EMPLOYEES;
DROP TABLE PS_EMPLOYEES
*
ERROR at line 1:
ORA-03113: end-of-file on communication channel

SQL> SELECT * FROM PS_EMPLOYEES;
ERROR:
ORA-03114: not connected to ORACLE
```

Figure 11: 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 by way of 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 in the figure).

Advantages over database-resident controls

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

- **Cross-platform support.** The InfoSphere Guardium Data-Level Access Control module enables organizations to define a single set of access policies for their entire application and database infrastructure, rather than controlling access for a specific DBMS platform or version only. Because it is implemented outside of the database, the InfoSphere Guardium Data-Level Access Control module supports all major DBMS platforms: Oracle, Microsoft SQL Server, IBM DB2, IBM Informix, Sybase, Oracle MySQL, Teradata, IBM Netezza and PostgreSQL.
- **Ease-of-use for non-DBAs.** Database-resident controls require DBAs to administer them—raising issues around separation of duties. The InfoSphere Guardium Data-Level Access Control module can be managed by IT security, compliance or risk teams, because it uses simple English-language policies that can be customized through drop-down menus, without requiring knowledge of database commands and structures. In addition, the InfoSphere Guardium Data-Level Access Control module 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.
- **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. The InfoSphere Guardium solution 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. The InfoSphere Guardium Data-Level Access Control module goes one step further by also examining query results (see Figure 12). For example, a connection from an anomalous script or application that is suddenly seen to be extracting Personally Identifiable Information (PII) from the database can be terminated or quarantined while being investigated, although 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. The InfoSphere Guardium Data-Level Access Control module provides continuous enforcement of access policies, because it does not require disabling certain privileged accounts inside the database.

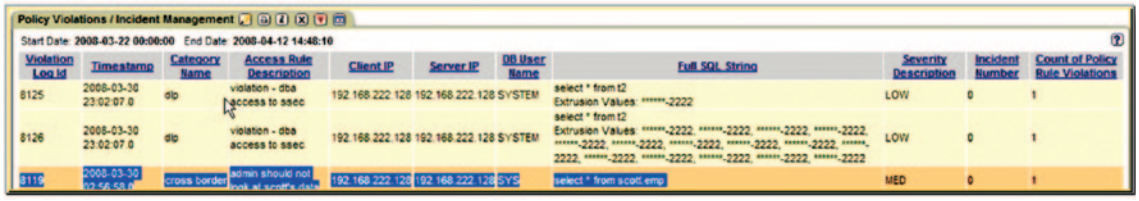


Figure 12: Extrusion rules examine returned data (rather than inbound SQL commands), looking for numeric patterns such as 16-digit credit card numbers or 9-digit social security numbers. Extruded data is typically masked before being stored in the InfoSphere Guardium appliance as part of the audit trail (shown in the figure 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 the InfoSphere Guardium host-based software probe

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

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 the InfoSphere Guardium Data-Level Access Control module to start enforcing access at a very granular level—without disrupting their application environments.

Enterprise Integrator

Data integration for enhanced operational and security effectiveness

Highlights

- Easily connects to multiple relational databases or text files to retrieve and integrate data into the InfoSphere Guardium repository for audit completeness
- Creates unified audit reports, including external information that enhances security and improves operational efficiency
- Imports descriptive information, such as full names and phone numbers corresponding to user names, to streamline investigation of exceptions
- Integrates information, such as roles and departments, to enable deployment of finer-grained security policies
- Creates a single management point for all database security and compliance data by integrating journal information from environments, such as IBM iSeries® and Progress databases
- Leverages existing IBM Tivoli® and EMS 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 cyber attacks 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 over geographical and organizational boundaries, administrative and entitlement information is fragmented among a variety of systems and personnel and system data is constantly changing, even as 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

The InfoSphere Guardium solution's Enterprise Integrator module can simplify and automate the integration of data from external databases or text files into the InfoSphere Guardium repository and enables 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.

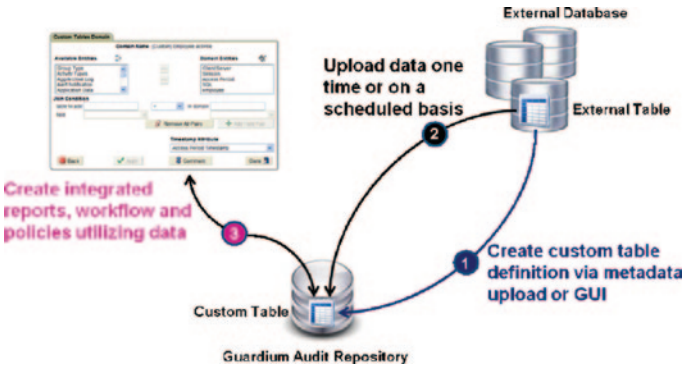


Figure 13: The Enterprise Integrator module provides a simple means to integrate important security-related information from external sources. Tools are provided to automatically or manually: 1) create a custom table definition for the imported data in the InfoSphere Guardium Audit Repository, 2) upload the data from the external source and 3) create data links so the full array of InfoSphere Guardium tools can easily and completely use the imported data.

External information can be integrated with a few simple steps (see Figure 13). First, a custom table is created to house the data. The table definition can be created by providing the InfoSphere Guardium solution 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 the InfoSphere Guardium solution providing tools to check schema compatibility and execute any post-upload Data Manipulation Language (DML) desired. Uploads can be one-time events or regularly scheduled, allowing the repository to be kept in sync 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 iSeries can be imported so that 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 14), 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.

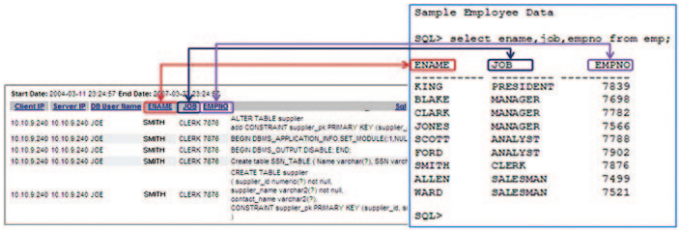


Figure 14: The Enterprise Integrator module enables users to create unified audit reports, including external information, which can enhance security and improve operational efficiency. For example, real employee names (ENAME) and numbers (EMPNO) stored in a remote employee database can be integrated so exception reports can be investigated without having to manually research the employee corresponding to a particular DB User Name. Importing an employee's job classification (JOB) enables potentially inappropriate activity to be identified, such as a CLERK modifying database tables.

By using the Enterprise Integrator module in conjunction with the core InfoSphere Guardium solution, change-control policies can be easily enforced without significant labor. The Enterprise Integrator module enables approved change requests from the change-management system to be retrieved and brought into the InfoSphere Guardium solution. 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 the InfoSphere Guardium solution through the ticket ID enables automation of the reconciliation process (see Figure 15). Reviewers are more easily able to compare the Summary description to the executed SQL commands to ensure the change made is appropriate. Workflow automation ensures all changes are reviewed and approved, and that 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 of 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.

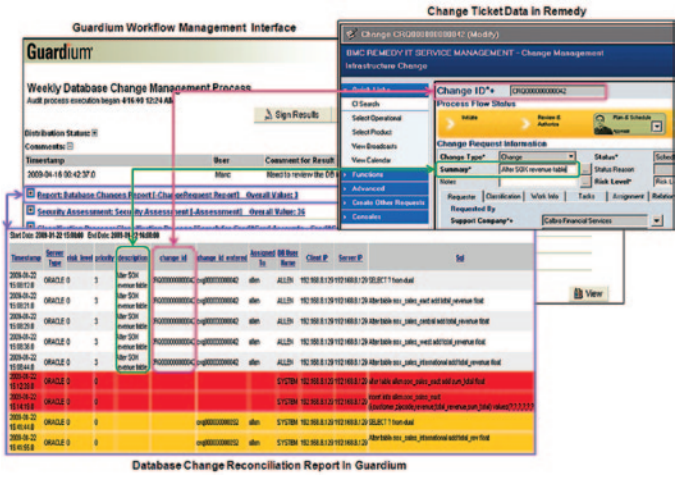


Figure 15: The Enterprise Integrator module can be used to import change-management information from custom or commercial systems like BMC's Remedy or HP's Peregrine. In this example the Change ID and Summary description are included in a weekly Database Change Report, which is distributed and managed using the InfoSphere Guardium solution's workflow capabilities. The report has been structured so that 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.

Eliminate security gaps by automating policy information updates

Although the InfoSphere Guardium solution may initially be deployed to protect a particular high-value asset, over time the use of the solution is typically expanded to encompass all of the enterprise's sensitive databases. As the solution scales, the use of groups becomes important. A group is a 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.

Enterprise Integrator support

Data sources	Built-in, ready-to-use support for Oracle, DB2, Sybase, Microsoft SQL Server, Informix, mySQL, Teradata, Netezza and PostgreSQL data sources
Connections	Built-in, ready-to-use support for HTTP, HTTPS, FTP, SAMBA and iSeries connections to CSV text file data sources

Table 1: InfoSphere Guardium Enterprise Integrator module supported environments.

Groups are used to simplify management of a wide variety of other objects, such as classes of servers (for example, those containing SOX, PCI and PII data) and users (for example, privileged users, users 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 the Enterprise Integrator module to retrieve this data and populate the group, both labor and errors can be eliminated. More important, as objects change (because of changes in responsibility, infrastructure changes and more), group membership can automatically be updated, without making any changes to the InfoSphere Guardium solution's groups or policies, by scheduling regular Enterprise Integrator module 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 module includes built-in, ready-to-use connectors for both Tivoli Storage Manager and EMC Centera, allowing these major enterprise-archiving solutions to be used more easily with the InfoSphere Guardium solution's archiving capabilities.

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

Entitlement Reports

Simplifies management of user rights across heterogeneous database environments

Highlights

- Provides a simple means of aggregating and understanding entitlement information from your entire database infrastructure
- Offers built-in, ready to use support for database platforms from all major vendors on all major operating systems
- Provides predefined reports for commonly required views
- Comes fully integrated with other InfoSphere Guardium modules, including the Advanced Compliance Workflow Automation module, 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, 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 changing roles and responsibilities more frequently than ever. Mergers and acquisitions are creating distributed, multivendor database infrastructures in which DBAs must cope with varying vendor entitlement models and numerous distinct systems. As a result, it has become extremely difficult to ensure that database privileges are restricted so that 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
IBM Netezza

Table 2: The InfoSphere Guardium Entitlement Reports module provides a simple means of collecting and understanding user-rights information that span heterogeneous database infrastructures.

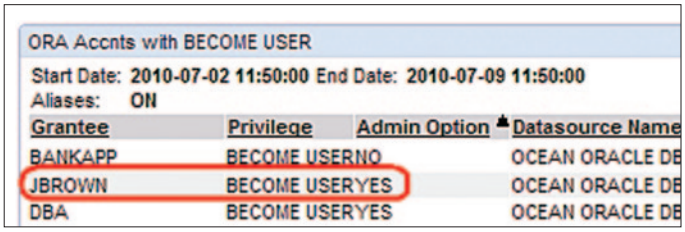
Automating and centralizing collection of entitlement information

The InfoSphere Guardium Entitlement Reports module provides a simple means of aggregating and understanding database entitlements throughout 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 database 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 preconfigured reports

The Entitlement Reports option is designed to work with the authorization systems of a wide variety of popular DBMSs (see Table 2), enabling it to retrieve, understand and present information gathered from any and all heterogeneous environments, using limited credentialed read-only access.[1] A variety of predefined reports (see Figures 16 and 17) 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 predefined reports include:

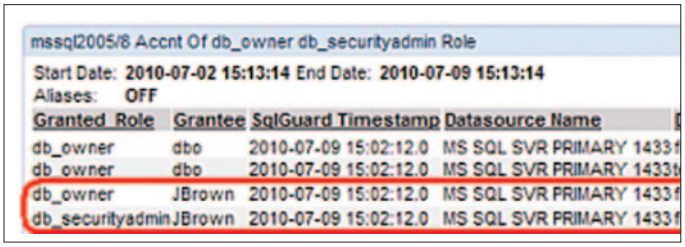
- Accounts with system privileges
- All system and administrator privileges, shown by user and role
- Object privileges by user
- All objects with PUBLIC access
- User privileges by object
- Roles granted to users and roles
- Grants and revocations of privileges
- Execute privileges by procedure


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 16: Users with inappropriate rights can be identified more easily with the InfoSphere Guardium Entitlement Reports option. 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_owner	dbo	2010-07-09 15:02:12.0	MS SQL SVR PRIMARY 1433
db_owner	dbo	2010-07-09 15:02:12.0	MS SQL SVR PRIMARY 1433
db_owner	JBrown	2010-07-09 15:02:12.0	MS SQL SVR PRIMARY 1433
db_securityadmin	JBrown	2010-07-09 15:02:12.0	MS SQL SVR PRIMARY 1433

Figure 17: The InfoSphere Guardium solution aggregates and presents entitlement information among eight DBMS platforms, including SQL Server, Oracle and DB2. This simplifies the process of identifying inappropriately granted roles, such as JBrown being granted both the db_owner and db_security admin role for the financial database.

Automating validation activities for security and compliance

All entitlement information gathered from throughout your database infrastructure is stored in the InfoSphere Guardium solution'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 be built easily by way of an intuitive drag-and-drop interface, to show specific views not provided by the predefined reports. The Compliance Workflow Automation module enables the reports required for these periodic reviews to be generated and distributed to the appropriate oversight team automatically. It also captures comments, escalations and approvals electronically, and stores them in the repository for use in audits.

The InfoSphere Guardium solution'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—for example, to automatically populate 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 be reflected automatically 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

The InfoSphere Guardium Entitlement Reports module provides 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, and 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.

Advanced Compliance Workflow Automation

Automates oversight processes to reduce operational costs

Highlights

- Centralizes and automates oversight processes enterprise-wide, including report generation, distribution, electronic sign-offs and escalations
- Easily creates custom processes by specifying your unique combination of workflow steps, actions and users
- Enables automated execution of oversight processes on a report line-item basis, maximizing process efficiency without sacrificing security
- Ensures that oversight team members see only data and tasks related to their own roles
- Improves process efficiency with real-time tools for centralized process management
- Stores 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 and 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 breakdowns 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 InfoSphere Guardium 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 composed of individual event states and actions (see Figure 18).
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 database management systems (DBMSs) 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 19).
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.

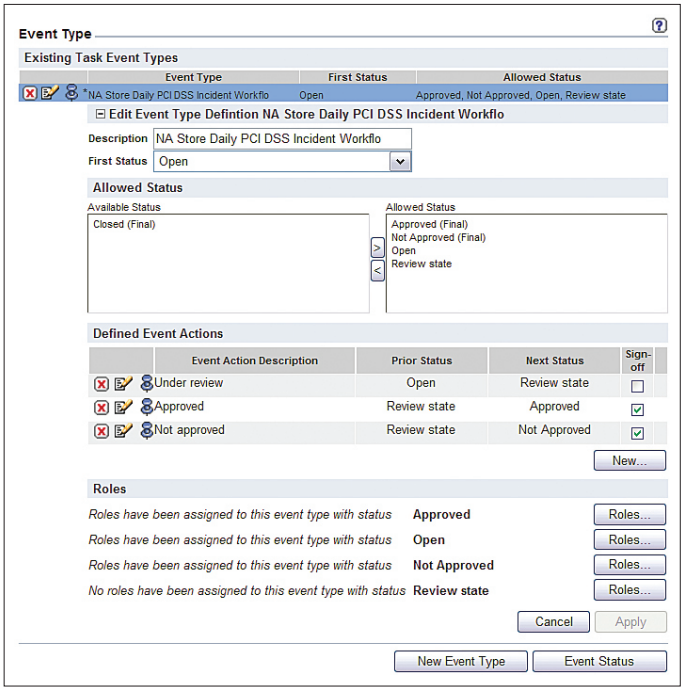


Figure 18: The InfoSphere Guardium Advanced Compliance Workflow Automation module enables users to easily create workflows that are customized to each of their own unique processes by specifying the appropriate combination of actions, event states and roles through a simple graphical user interface.

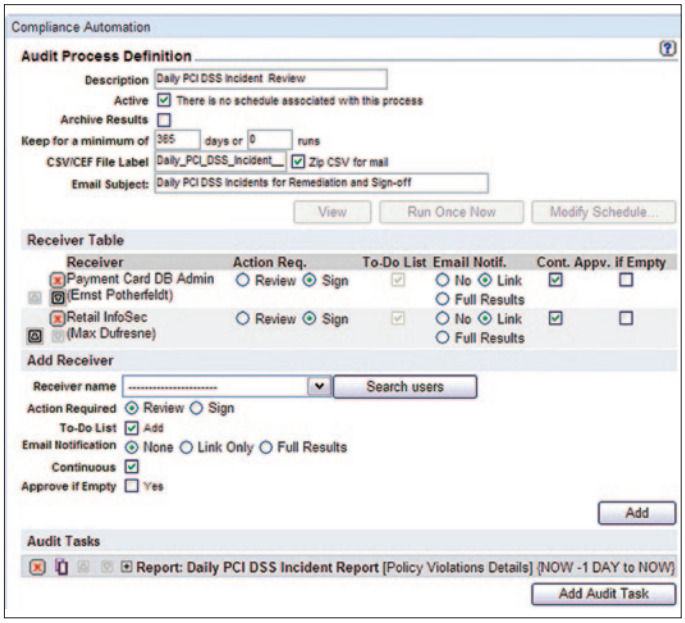


Figure 19: Workflow can be automatically initiated on a scheduled basis, ensuring that recurring tasks, such as daily incident reviews and vulnerability assessments, are consistently executed and tracked.

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 and 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 the workflow process are able to see only information related to their specific responsibilities. Responsibilities are assigned on two levels. The first relates to workflow responsibilities, as discussed above. Individuals see only information related to actions assigned to them through the workflow definition.

The second relates to access control mechanisms built into the core InfoSphere Guardium solution, 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 "Database Administrators (DBAs)" review test results. Martha, a member of the DBA group who was granted InfoSphere Guardium rights for all the financial databases, will see only test results related to financial databases, while Patrick, who was granted rights to the payment card databases, will see only those results. The InfoSphere Guardium solution 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 among heterogeneous database infrastructures and widely distributed teams, increasing accountability and minimizing audit exceptions.

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

The InfoSphere Guardium Advanced Compliance Workflow Automation module 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.

Configuration Audit System for Database Servers

Detects configuration changes impacting database security

Highlights

- Tracks all changes that can affect the security of database environments outside the scope of the database engine
- Complements the InfoSphere Guardium Database Activity Monitor 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 and registry variables
  - Configuration files (for example, SQLNET.ORA, NAMES.ORA)
  - Shell scripts
  - OS files
  - Executables, such as Java programs
- Is 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 database security administrators.

These activities are secured more easily, using the InfoSphere Guardium Database Activity Monitor module, which enables 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, the InfoSphere Guardium Database 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.

The InfoSphere Guardium Configuration Audit System for Database Servers (CAS) module tracks all changes made to the database at various levels, and reports on these changes to a centralized web-based console. Using the CAS module, database 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 the InfoSphere Guardium Database Activity Monitoring functionality, the CAS module provides the only comprehensive monitoring, auditing and control solution for databases in the industry.

What the CAS module does

The CAS module uses a lightweight 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.

The module then polls these constructs based on a set of periods defined by the user and, if there are any changes, notifies the InfoSphere Guardium server precisely which element was changed, what the new value is (versus the old value) and such.

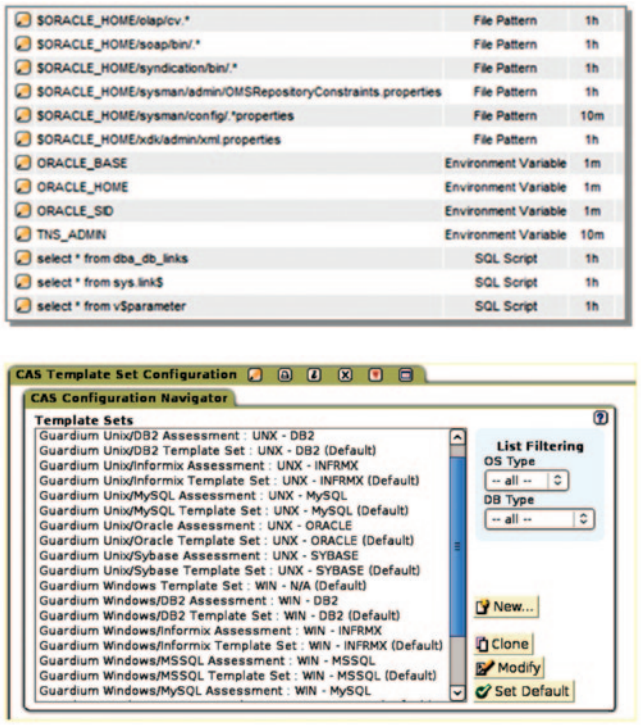


Figure 20: The InfoSphere Guardium Configuration Audit System for Database Servers (CAS) module tracks all changes to external database objects—such as configuration files, environment and registry variables, scripts and executables—that can affect your database security posture. To accelerate deployment, CAS includes a best-practices library with hundreds of preconfigured knowledge templates for all major OS and DBMS combinations.

The CAS module works from a template that defines what to monitor. The InfoSphere Guardium solution 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 environment (see Figure 20). A user deploys these templates to the server by selecting the template and the host—the CAS module does the rest.

When deployed, the CAS module expands this template to the actual instance elements. 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. For 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.

The CAS module also tracks other values. For example, SQL Server enables encrypting of the database communication using Secure Sockets Layer (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 21). A Windows administrator can easily turn off encryption of data-in-transit with a simple modification and no one would be the wiser. The CAS module templates monitor these values to further ensure the robustness of your database security.

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

- Changes to environment variables.
- Changes to file permissions; the CAS module can also validate that file permissions are not set to exceed a certain limit.
- Changes to file ownership; the CAS module 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.

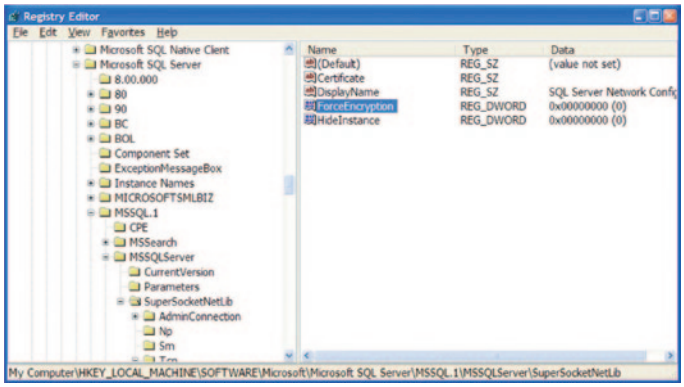


Figure 21: The CAS module simplifies the process of tracking critical registry values, such as the "Force protocol encryption" registry value for SQL Server.

The CAS module 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 22). An administrator can specify how the CAS module 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.

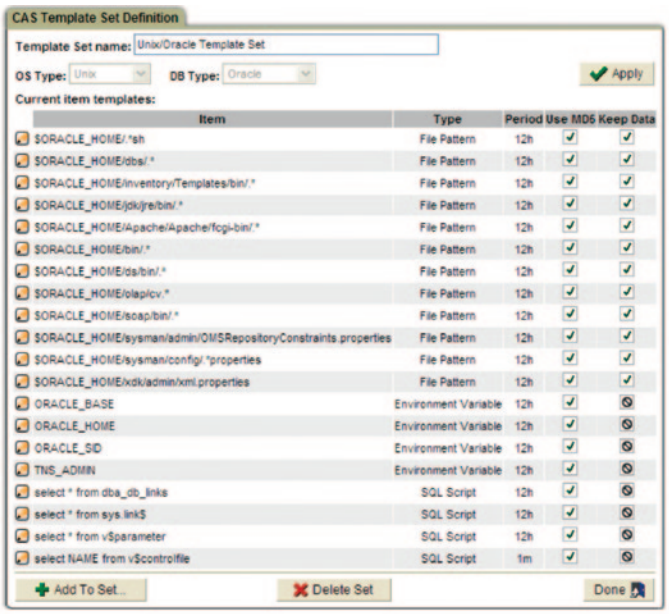


Figure 22: The CAS module enables you to define the polling period for tracking changes, whether MD5 checksums are used to track changes (rather than timestamps) and whether the CAS module should also "keep data" to track "before" values.

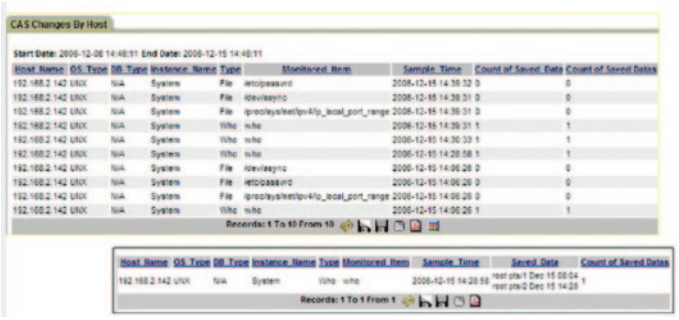


Figure 23: The CAS module provides the option of retaining "before" and "after" values, if desired ("Saved Data" in the figure).

Additionally, each element specifies whether or not the CAS module should just report on the change or whether it should also bring back the "before" and "after" values. In the latter case, reports are provided, which show the difference between the old and the new values (see Figure 23).

Installing and operating the CAS module

The CAS module can be installed as part of an S-TAP installation or as a separate installation. The CAS agent runs as a Java program and thus needs Java 1.4 or above installed on the host. Java is a prerequisite and the CAS agent installer asks for the location of the Java installation. Table 3 summarizes the storage requirements for the CAS module.

Customizing the CAS module

In addition to the prebuilt templates and tracked elements, the CAS module enables 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 the CAS module and that can also be used to supplement the extensive built-in functionality that the module provides.

Operating system	Required disk space
AIX	350 MB
HP-UX	650 MB
Linux	450 MB
Solaris	400 MB
Tru64	350 MB
Windows	300 MB

Table 3: CAS storage requirements.

Documenting compliance with automated sign-offs and escalations

Auditors want to know that incidents are being tracked and resolved in a timely manner. With the InfoSphere Guardium solution's incident management and Advanced Compliance Workflow Automation functionality (see Figure 24), you can automate report distribution, electronic sign-offs, comments and escalations, while tracking progress on the remediation of change incidents.

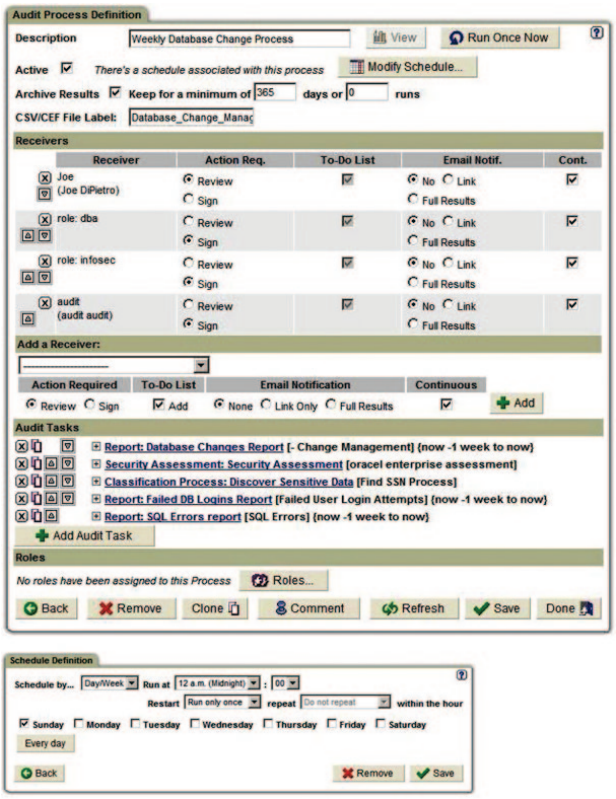


Figure 24: Auditors look for evidence that organizations have well-defined processes in place to safeguard their critical data. The InfoSphere Guardium Advanced Compliance Workflow Automation module enables you to define customized audit tasks that automatically perform scheduled change-audit reporting, report distribution, sign-offs and escalations.

Database Vulnerability Assessment

Comprehensive automated tests based on best practices

Highlights

- 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 US Department of Defense (DoD)
- Generates security health report card and recommends concrete action plans to strengthen database security
- Simplifies deployment in large-scale environments, as multiple data sources (DB name, type, server IP, ports, roles) can be loaded and linked to assessments automatically by way of a script interface

Improving database security and compliance

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

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 internal and external threats.

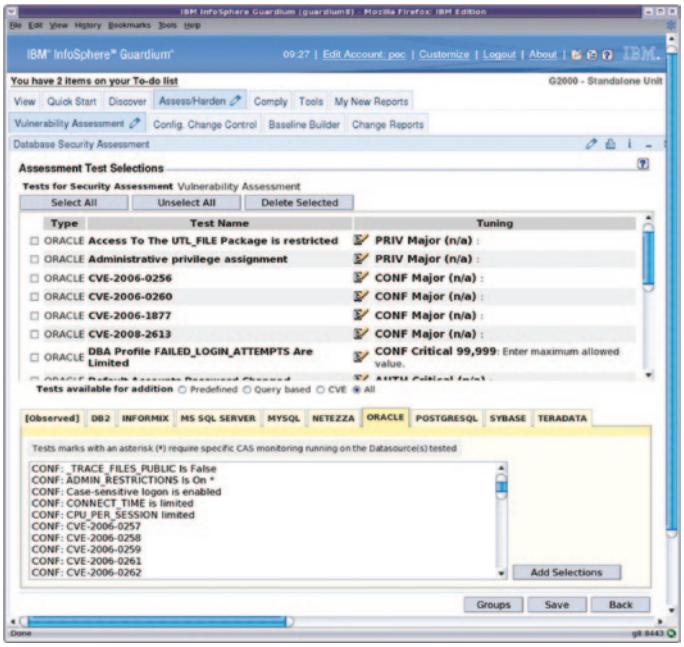


Figure 25: The InfoSphere Guardium Database Vulnerability Assessment module scans your database infrastructure for missing patches, misconfigured privileges and other vulnerabilities. It incorporates a best-practices library with hundreds of preconfigured tests, and provides recommendations on how to remediate vulnerabilities, including identifiers (for example, CVE) associated with external resources. You can also create custom tests and oversight processes.

Preconfigured tests based on CIS and DoD best practices

The InfoSphere Guardium 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.

The InfoSphere Guardium Database VA module includes a comprehensive library of preconfigured tests (see Figure 25) based on industry best practices such as the Computer Internet Security (CIS) benchmarks and the Database Security Technical Implementation Guide (STIG) created by the DoD. 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 by way of the InfoSphere Guardium Knowledgebase service. You can also define custom tests (see Figure 26) and schedule automated audit tasks incorporating scans, distribution of reports, electronic sign-offs and escalations.

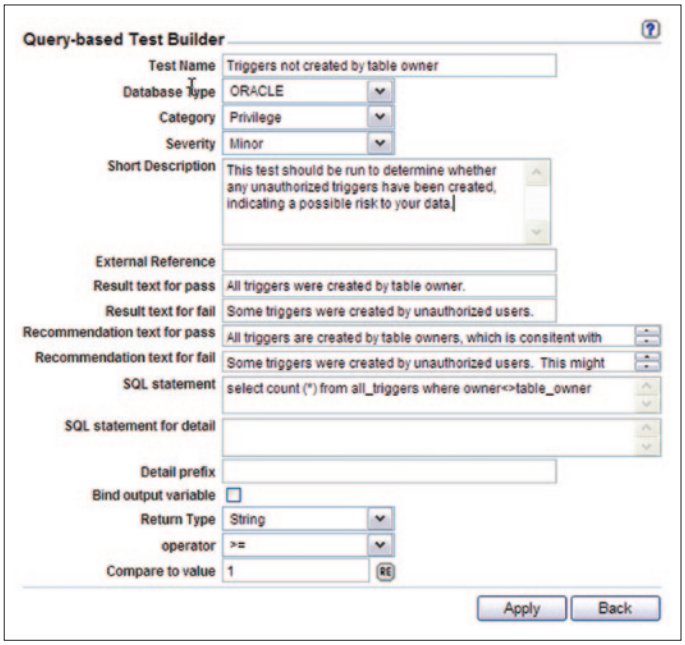


Figure 26: Custom tests using SQL queries can be created easily with the form-based test builder. Custom tests can also be created by way of OS scripts and Java classes.

In addition to producing detailed reports with drill-down capabilities (see Figure 27), the assessment module recommends concrete action plans for each vulnerability to help you strengthen security. For example, if there are privilege-related 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 to related external resources, such as Common Vulnerabilities and Exposures (CVE) identifiers.

Figure 27: The InfoSphere Guardium Database Vulnerability Assessment (VA) module produces summary results that can provide an understanding of your overall security posture, along with detailed drill-downs containing concrete recommendations for improvement.

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

Broad range of granular tests

Assessments are grouped into multiple categories, including:

- **Privileges.** The InfoSphere Guardium solution checks for object creation and usage rights, privilege grants to DBAs and users and system level rights.
- **Authentication.** The system verifies password policies, default vendor accounts, no empty passwords, remote login parameters and more.
- **Configuration.** The system 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.** The system verifies appropriate version numbers and patch levels.
- **Behavior.** These tests leverage the InfoSphere Guardium system's real-time activity monitoring capability 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.** The system checks permissions on key objects, such as database home directories, configuration files, such as sqlnet.ora, and registry and environment variables.

Multiple assessment technologies, without impacting uptime or performance

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

- **Scanning.** The system assesses database vulnerabilities by way of 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, the InfoSphere Guardium Database VA module provides complete platform coverage (see Table 4), without impacting the performance or stability of critical systems. The system does not run intrusive exploits that can result in system failures 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® (Linux, UNIX and Windows [LUW] and IBM z/OS®)
IBM Informix®
Sybase
Oracle MySQL
Teradata
PostgreSQL
IBM Netezza®

Table 4: The InfoSphere Guardium solution can provide a simple means of hardening your entire database infrastructure, providing vulnerability assessment capabilities for all major DBMS platforms.

Beyond simple reporting: Addressing the entire vulnerability management lifecycle

The InfoSphere Guardium Database VA module is tightly integrated with other modules in the platform, enabling you to manage the entire database security and compliance life cycle 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, the InfoSphere Guardium solution enables you to rapidly:

- **Pinpoint database vulnerabilities.** Unpatched and misconfigured databases create enormous risk. The InfoSphere Guardium Database VA module incorporates an extensive library of assessment tests, based on industry best practices, to flag vulnerabilities. A quarterly Knowledgebase 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. The InfoSphere Guardium solution helps protect databases until they can be patched, through activity monitoring, signature-based policies and preventive controls. Policies and baselining can also help protect against application vulnerabilities, such as SQL Injection and buffer overflow. For example, you can alert or block, or alert and block, on any calls by non-line-of-business applications to unpatched procedures, indicating a possible attack.
- **Prioritize remediation activities based on business risk.** The InfoSphere Guardium Sensitive Data Finder 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, because most organizations do not 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, the InfoSphere Guardium CAS module "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 the InfoSphere Guardium incident management and Compliance Workflow Automation (see Figure 28) capabilities, you can automate report distribution, electronic sign-offs and escalations, while tracking progress on the remediation of vulnerable systems.

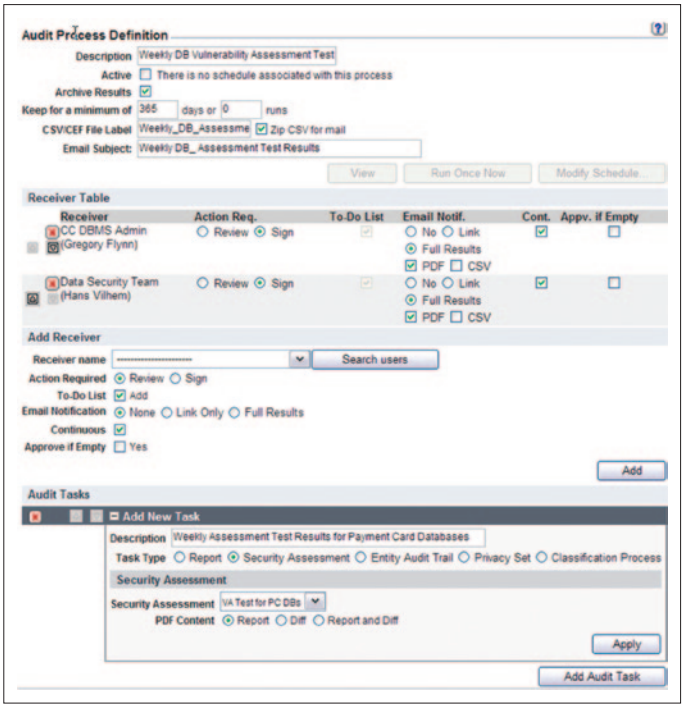


Figure 28: Auditors look for evidence that organizations have well-defined processes in place to safeguard their critical data. The InfoSphere Guardium Advanced Compliance Workflow Automation module enables you to define customized audit tasks that perform scheduled vulnerability assessments automatically, along with report distribution, sign-offs and escalations.

Database Protection Knowledgebase

Maximizes protection and compliance with recurring content updates

Highlights

- Proactively updates your InfoSphere Guardium solution 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 up-front and ongoing labor by identifying sensitive tables in common enterprise applications (for example, SAP, Oracle EBS and PeopleSoft) requiring protection, such as those containing PCI DSS or financial (SOX) information
- Updates the InfoSphere Guardium solution'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 that identify database and application objects with security and compliance requirements

The challenge of protecting sensitive data in rapidly changing environments

Organizations spanning every industry 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 the InfoSphere Guardium solution, are common.

To maximize the protection afforded by the InfoSphere Guardium solution, 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 the configurable parameters of the InfoSphere Guardium solution to account for such changes, many 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, integrate and exploit information from throughout 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 InfoSphere Guardium Database Protection Knowledgebase is an annual service which provides clients with updated content, in InfoSphere 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 like CVE. Information is assembled, packaged for integration into appropriate InfoSphere Guardium elements (for example, vulnerability tests, groups and more), tested and delivered to InfoSphere Guardium clients.

Simple to administer

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

Updates are applied easily with the click of a mouse (see Figure 29). The intelligent update process built into the InfoSphere Guardium solution 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 is reflected. At the next update, the InfoSphere Guardium solution will recognize that object was added and preserve it during the update process.

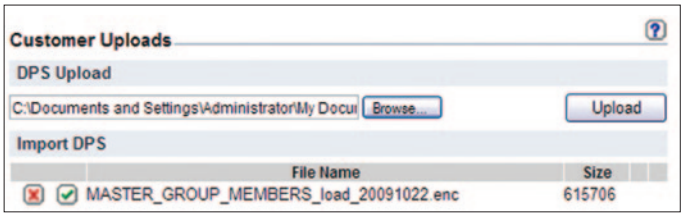


Figure 29: Current vulnerability, auditing and best-practices libraries regularly provided by the Database Protection Knowledgebase service are integrated into the InfoSphere Guardium solution with the click of a mouse.

By delivering current content packaged for immediate integration into the InfoSphere Guardium solution, IBM has 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 threat landscape.

Comprehensive protection for heterogeneous environments

The InfoSphere Guardium Database Protection Knowledgebase service updates deliver content for all major platforms (see Table 5), 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 earlier) is delivered, enabling a wide range of applications, including:

- **Testing to avert exposure to the most recent database vulnerabilities.**[2] Updated InfoSphere Guardium Database VA tests ensure that regularly scheduled database 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, Oracle EBS and PeopleSoft ensure controls can be implemented more easily, using the InfoSphere Guardium solution, without the need to spend hours researching those applications on an ongoing basis to identify sensitive tables.
- **Vulnerable object protection (virtual patching).** In most organizations 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 more easily implement rules that alert or block unexpected access to the vulnerable objects until the patch until can be installed.

A wide variety of other applications become feasible with the InfoSphere Guardium Database Protection Knowledgebase service, 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, the InfoSphere Guardium solution 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
IBM Netezza

Table 5: The InfoSphere Guardium Database Protection Knowledgebase service delivers a wide range of updated content, including vulnerability tests, sensitive objects, vulnerable objects and current patch information spanning all major database platforms.

IBM InfoSphere Guardium for z/OS

Comprehensive auditing visibility for DB2, IMS and VSAM, using proven z/OS technology

Highlights

- Monitors and audits IMS, VSAM and DB2 on IBM z/OS® activity by privileged users, mainframe-resident applications and network clients
- Provides visibility at a granular level into critical operations, including reads, data and structural changes
- Performs all analysis, reporting and storage of audit data off-mainframe in a secure environment
- Can be used for mainframe environments only, or deployed enterprise-wide to provide a unified security and compliance solution for both mainframe and distributed database environments
- Uses 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 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, IBM IMS™ and VSAM 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.

The IBM InfoSphere Guardium solution offers a simple yet powerful means of securing critical data throughout 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; and automated reporting capabilities, which simplify validation of compliance for mandates, such as SOX, PCI DSS and data privacy regulations.

The InfoSphere Guardium for z/OS solution provides these capabilities for DB2, IMS and VSAM on z/OS. The solution can be used independently for the mainframe environment only, or integrated with other InfoSphere Guardium database security and monitoring components throughout the enterprise (see Figure 30), to provide a secure, centralized audit repository and management point.

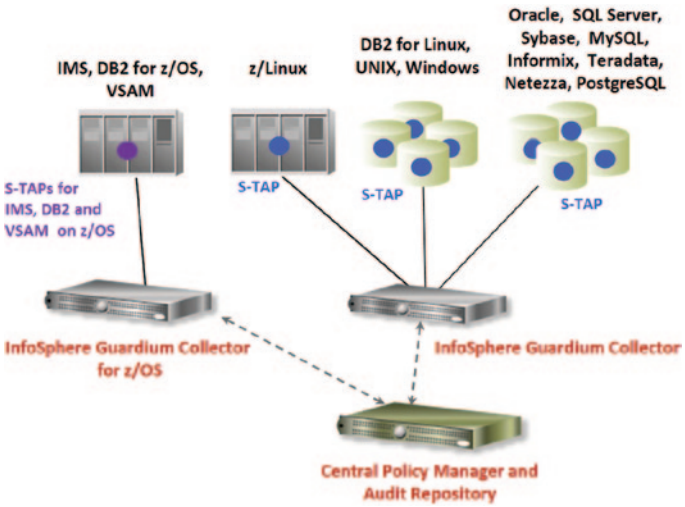


Figure 30: The InfoSphere Guardium solution uses lightweight software probes to capture key DB2, IMS and VSAM activities executed by privileged users, mainframe-resident applications and network clients on z/OS. Both mainframe and distributed environments can be monitored from a single console; in addition, all audit data is automatically aggregated and normalized into a single centralized repository for enterprise-wide compliance reporting, analytics and forensics.

Avoid the security and cost issues associated with traditional solutions

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

- Reliance on mainframe DBAs for administration, thus 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.

The InfoSphere Guardium for z/OS solution 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.

Scalable enterprise-wide database security and compliance platform

The InfoSphere Guardium for z/OS solution uses lightweight software probes, called S-TAPs, to capture DB2, IMS and VSAM activities by privileged users, mainframe-resident applications and network clients, including those connecting through services such as JDBC, DB2 or IMS Connect. Proven IBM event-capture technologies are used for each environment to ensure all critical operations are captured, without the use of Class 4 and Class 5 audit traces.

Each S-TAP on z/OS is designed for the unique monitoring requirements of a particular data environment. The IBM InfoSphere Guardium S-TAP for DB2 on z/OS module monitors all DB2 activities, including SELECTs, DML, data definition language (DDL) and changes in access privileges. To enhance performance, the underlying DB2 event-capture technology can be shared with IBM Query Monitor in systems utilizing both offerings. The IBM InfoSphere Guardium S-TAP for VSAM on z/OS module supports a comprehensive range of VSAM file types, including entry-sequenced data set (ESDS), key-sequenced data set (KSDS), relative record data set (RRDS), virtual relative record data set (VRRDS) and linear data set (LDS), monitoring OPENs, READs, UPDATEs, DELETEs, CREATEs and ALTERs. The IBM InfoSphere Guardium S-TAP for IMS on z/OS module monitors both online and batch tasks, providing auditing and policy management related to READs, INSERTs, UPDATEs, DELETEs.

Each S-TAP sends information specified by user-defined audit policies to an InfoSphere Guardium Collector for z/OS appliance. This ensures that the mainframe is not burdened with incremental storage or processing requirements, network traffic is limited and a full audit trail is stored securely.

Unique in the industry, the InfoSphere Guardium solution's multitier architecture (see Figure 30) aggregates and normalizes audit information—spanning 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 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.

Automated, policy-based monitoring and auditing streamline compliance validation

The InfoSphere Guardium solution's web console provides centralized management of alerts, report definitions, compliance workflow processes, and settings (such as archiving schedules) without the involvement of DBAs, thus 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 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 and incident responses, including steps such as sign-offs, commenting and escalation.
- Running hundreds of ready-to-use reports, including those required for SOX, PCI DSS and data privacy laws, in addition to creating customized reports.

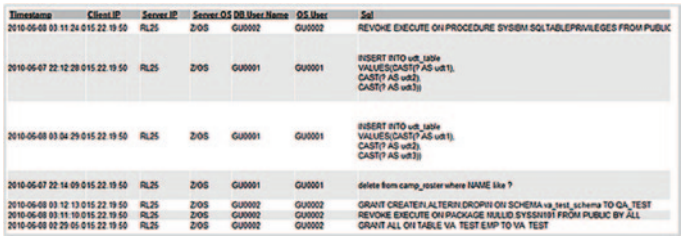


Figure 31: The InfoSphere Guardium solution provides comprehensive visibility into DB2, IMS and VSAM data usage on z/OS, capturing both mainframe and network access with key details such as OS user name, client IP, database user name and data access statements executed.

With the InfoSphere Guardium solution, you gain full visibility into your z/OS data environment, enabling unauthorized activities like data tampering or hacking to be identified and addressed in real time. Automation of the entire security and compliance life cycle reduces labor costs, facilitates communication throughout 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 (LUW)
- 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 and others) running in the IBM z/VM hypervisor
- Cognos, for which the InfoSphere Guardium solution identifies fraud and other unauthorized activities through application-layer monitoring. The InfoSphere Guardium solution also supports other enterprise applications, such as SAP, PeopleSoft and service-oriented architecture (SOA) applications developed for IBM WebSphere Application Server and other middleware platforms

IBM InfoSphere Guardium solution support for z/OS	
DB2 versions	DB2 for z/OS V8.1, V9.1, V10.1
IMS versions	V9, V10, V11, V12[3]
z/OS versions	z/OS V1.10 (5694-A01) or later

Table 6: The InfoSphere Guardium solution provides comprehensive z/OS support.

References

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.

2 Requires the IBM InfoSphere Guardium Database Vulnerability Assessment module.

3 Announced support corresponding to IMS 12 general availability.

For more information

To learn more about the IBM InfoSphere Guardium database security solution, please contact your IBM marketing representative or IBM Business Partner, or visit the following website: **ibm.com**/software/data/guardium

IBM Corporation
Route 100
Somers, NY 10589

Produced in the United States of America
September 2011

IMW14585-USEN-00