IBM Guardium S-GATE

Simplified Data-Level Access Control for Heterogeneous DBMS Environments

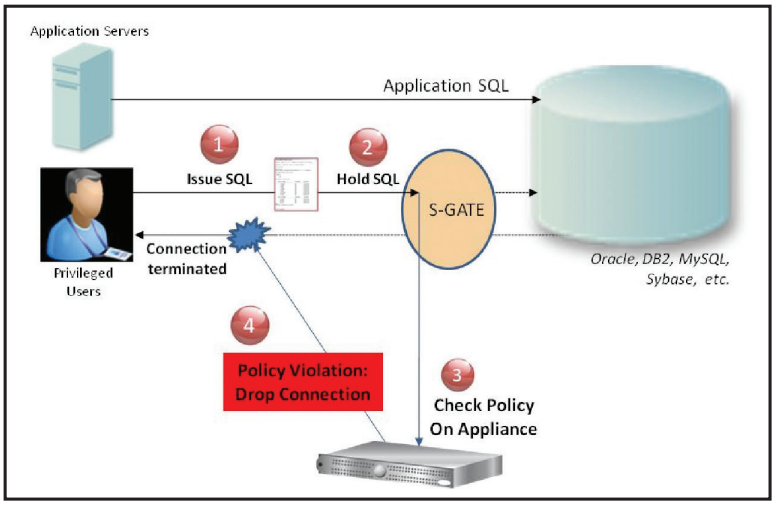
Highlights:

- Blocks privileged users from viewing or changing sensitive data, creating new user accounts or elevating privileges.
- Zero impact on application-level traffic.
- Supports IT outsourcing and associated cost savings – without increasing risk.
- Enforces separation of duties for SOX, PCI, Basel II, data privacy regulations.
- Simplifies security and compliance via single set of granular access policies for heterogeneous[2] DBMS infrastructures.
- Enhances operational efficiency by replacing manual processes with centralized and automated controls.

Background

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

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



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

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

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).

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

Real-Time Preventive Controls; Zero Disruption to IT Infrastructures

Implemented as a lightweight, host-based software agent with fine-grained security policies, Guardium S-GATE™ provides automated, real-time controls that prevent privileged users from performing unauthorized actions such as:

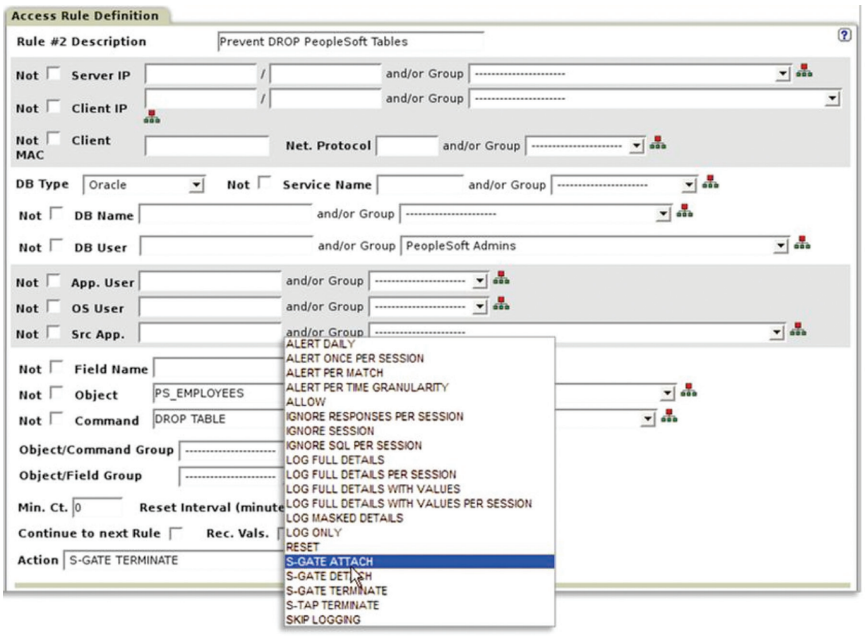
- Executing queries on sensitive tables
- Changing sensitive data values
- Adding or deleting critical tables (schema changes) outside change windows
- Creating new user accounts and modifying privileges

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

Advantages Over Database-Resident Controls

S-GATE provides strong advantages over database-resident controls, including:

- **Cross-Platform Support:** S-GATE allows organizations to define a single set of access policies for their entire application and database infrastructure, rather than controlling access for only a specific DBMS platform or version. Because it is implemented outside of the database, S-GATE supports all major DBMS platforms: Oracle, Microsoft SQL Server, IBM DB2, IBM Informix, Sybase and MySQL.
- **Ease-of-Use for Non-DBAs:** Database-resident controls require DBAs to administer them – raising issues around separation of duties. S-GATE can be managed by IT security, compliance or risk teams because it uses simple, English-language policies that can be customized via drop-down menus, without requiring knowledge of database commands and structures. In addition, S-GATE 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.




```
[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
```

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

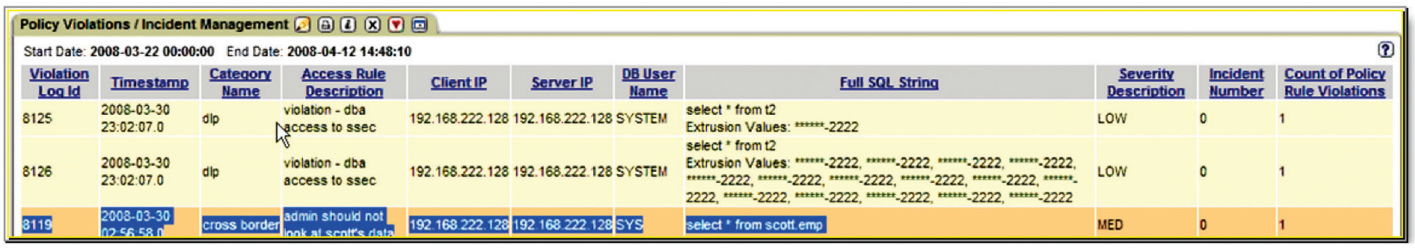
- **Single Solution for Policy Enforcement and Auditing:** Compliance regulations require storing a complete audit trail of all privileged user actions, in order to document compliance and aid in forensic investigations. DBMS vendors typically offer fine-grained auditing and audit repositories as separate add-ons. Guardium 7 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. S-GATE goes one step further by also examining query results. For example, a connection from an anomalous script or application that is suddenly seen to be extracting PII from the database can be terminated, while a valid application that extracts the same PII data will be allowed.
- **Non-Stop Enforcement:** Some database-resident controls must be turned off for routine maintenance operations such as backups and patching. During these maintenance windows, privileged users can take advantage of disabled controls to perform unauthorized actions. S-GATE provides continuous enforcement of access policies because it does not require disabling certain privileged accounts inside the database.

Extension to Guardium's Host-Based Monitoring Agent

S-GATE, available with Guardium 7, is an extension to S-TAP™ ("software tap"), Guardium's lightweight, host-based agent. Unique in the industry, S-TAPs are non-intrusive software probes that monitor network streams at the OS level of database servers, including both network access and local access by privileged users (via shared memory, named pipes, Oracle Bequeath, etc.).

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

Customers already using S-TAP can easily upgrade to S-GATE to start enforcing access at a very granular level – without disrupting their application environments.

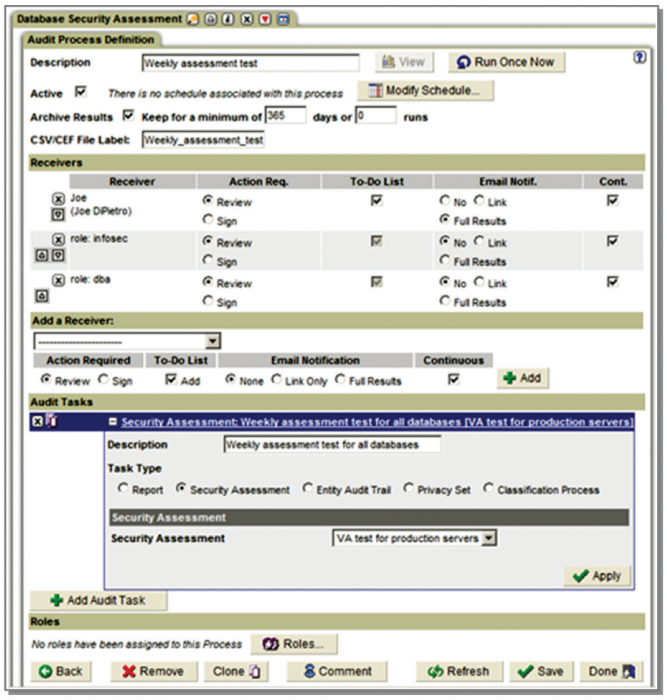


Policy Violations / Incident Management

Start Date: 2008-03-22 00:00:00 End Date: 2008-04-12 14:48:10

Violation Log Id	Timestamp	Category Name	Access Rule Description	Client IP	Server IP	DB User Name	Full SQL String	Severity Description	Incident Number	Count of Policy Rule Violations
8125	2008-03-30 23:02:07.0	dlp	violation - dba access to ssec	192.168.222.128	192.168.222.128	SYSTEM	select * from t2 Extrusion Values: ******-2222	LOW	0	1
8126	2008-03-30 23:02:07.0	dlp	violation - dba access to ssec	192.168.222.128	192.168.222.128	SYSTEM	select * from t2 Extrusion Values: ******-2222, ******-2222, ******-2222, ******-2222, ******-2222, ******-2222, ******-2222, ******-2222, ******-2222, ******-2222, ******-2222, ******-2222, ******-2222, ******-2222	LOW	0	1
8119	2008-03-30 02:56:58.0	cross border	admin should not look at scott's data	192.168.222.128	192.168.222.128	SYS	select * from scott.emp	MED	0	1

Examining Query Results to Prevent Data Leakage: 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 Guardium appliance as part of the audit trail (shown above with asterisks). You can define policy actions (called "S-TAP TERMINATE") that terminate connections after sensitive data has been detected in query results, thereby limiting data leakage (typically to tens of records). In comparison, "S-GATE TERMINATE" will terminate connections even before SQL commands have been executed on specific database objects by the DBMS..



Workflow Automation: Auditors look for evidence that organizations have well-defined processes in place to safeguard their critical data. With Guardium's workflow automation module, you can define customized Audit Tasks that automatically distribute exception reports to oversight teams, collect electronic sign-offs, automate escalations and manage incidents.

About the Guardium Platform

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

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

About Guardium, an IBM Company

Guardium, an IBM Company, safeguards critical enterprise information by continuously monitoring access and changes to high-value databases. Guardium's scalable platform simplifies governance with unified policies for heterogeneous infrastructures while reducing operational costs by automating compliance processes, enabling orgaanizations to safely use trusted information to drive smarter business outcomes.

Guardium's enterprise platform is now installed in more than 450 data centers worldwide, including 5 of the top 5 global banks; 4 of the top 6 insurers; top government agencies; 2 of the top 3 retailers; 20 of the world's top telcos; 2 of the world's favorite beverage brands; the most recognized name in PCs; a top 3 auto maker; a top 3 aerospace company; and a leading supplier of business intelligence software.

Guardium was the first company 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.

Endnote

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

[2] S-GATE currently available for UNIX/Linux. S-TAP TERMINATE currently available for Windows with similar functionality (contact Guardium for details).

Please Recycle

Guardium®
SAFEGUARDING DATABASES™ | AN IBM® COMPANY