Guardium Consulting Services
Data Discovery & Classification Service.

Highlights
- Scans group of database systems
- Discovers where sensitive information is stored
- Automatically tags information with meta-data classifications such as “Privacy-Restricted” or “Regulated Record”
- Quickly identifies faulty business or IT processes that store confidential data such as magnetic stripe or PIN block information
- Ensures that security access policies are always up-to-date and protecting sensitive data
- Supports broad range of DBMS platforms including:
  - Oracle
  - SQL Server
  - IBM DB2
  - Informix
  - Sybase
  - MySQL

Deliverables
- Data discovery on up to 50 data sources per engagement

Pre-Requisites
- An IP which is defined within DNS needs to be set up before consultants arrive on-site. This IP will be assigned to the consultant’s laptop from which the assessment is run. The laptop must be able to reach and connect to all instances.
- The client must provide an employee to define characteristics of sensitive information (e.g., 16-digit credit card numbers) and desired classification labels.

Guardium's Data Discovery and Classification Service automatically locates and classifies sensitive data in your database environment, based on customizable patterns such as 16-digit credit card numbers and 9-digit social security numbers.

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

This is especially challenging for organizations that have experienced mergers and acquisitions, or environments where legacy systems have outlasted their original developers. Even in the best of cases, ongoing changes to application and database structures—needed to support new business requirements—can easily invalidate static security policies and leave sensitive data unknown and unprotected.

Organizations find it particularly difficult to:
- Map out all database servers containing sensitive information and understand how data is being accessed from all sources (line-of-business applications, batch processes, ad hoc queries, application developers, administrators, etc.)
- Secure information and manage risk when the sensitivity of stored information is unknown
- Ensure compliance when it isn’t clear which information is subject to the terms of particular regulations

Guardium’s data discovery services uses database auto-discovery and information classification to identify where confidential data is stored, and then uses customizable classification labels to automate the application of security policies that apply to particular classes of sensitive objects. These policies ensure that sensitive information is only viewed and/or changed by authorized users.

Auto-discovery and mapping of database servers
Guardium’s auto-discovery capability performs a network discovery of the database environment and creates a visual access map showing all interactions among database servers, tables, clients, and applications. This helps quickly identify authorized and unauthorized users, applications, database servers, etc.
Database auto-discovery can also be scheduled to execute on a regular basis, in order to prevent the introduction of rogue servers and ensure that no critical information is “forgotten.”

**Database content classification and policy**

Using a list of databases mapped out by the auto-discovery process, Guardium’s Classifier module automatically discovers and classifies sensitive data inside databases. The Classifier uses an intelligent database crawler to efficiently search for customizable patterns such as 16-digit credit card numbers and 9-digit Social Security numbers (based on regular expressions).

Once sensitive objects have been located, they are automatically tagged with meta-data classifications such as “Privacy-Restricted” or “Regulated Record” and added to groups of items with similar properties. This ensures that appropriate policies are automatically applied to groups of objects with similar properties. In addition, executing the classifier process on a scheduled basis ensures that your policies are always up-to-date, even as developers change locations of sensitive objects.

When a sensitive object is located, the Classifier can generate immediate security alerts to help you quickly identify and resolve faulty business or IT processes that store confidential data such as magnetic stripe or PIN block information. Guardium’s Compliance Workflow Automation module can track the resolution of these incidents with electronic sign-offs and escalations.

**About the Guardium Platform**

Guardium’s real-time database security and monitoring solution monitors all 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 Oracle EBS, PeopleSoft, Siebel, JD Edwards, SAP, Business Intelligence and in-house systems. Additional modules are available for performing database vulnerability and configuration assessments, and automating the discovery and classification of sensitive data in corporate databases.


**About Guardium**

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

The company’s enterprise security platform is now installed in more than 450 data centers worldwide, including 3 of the top 4 global banks; 2 of the top 3 global retailers; one of the world’s largest PC manufacturers; a global soft drink brand; and a leading supplier of business intelligence software.

Founded in 2002, 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.

For more information, please contact your Guardium partner, Regional Sales Manager or visit [www.guardium.com](http://www.guardium.com).

Guardium, Safeguarding Databases, and S-TAP are trademarks of Guardium, Inc. 10-08