

DgDiscover™ – Identification and Location of Sensitive Enterprise Data

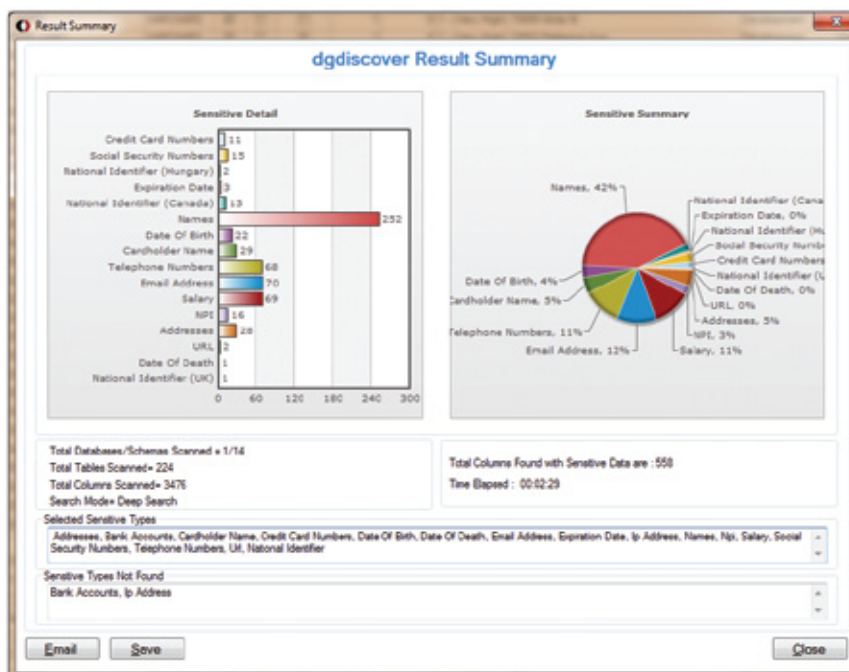
Enterprise applications serve as repositories for large quantities of sensitive data, and organizations need to be able to leverage this data to support essential processes such as application development, customer support and business analysis. These needs encourage the spread of information throughout the organization and make tracking sensitive data more difficult. Dataguise addresses the challenge of identifying and locating sensitive data with DgDiscover. By finding data repositories deployed in enterprise networks and searching repositories for sensitive data, DgDiscover provides analysts with the information they need to implement effective remediation and managers with intelligence they require to manage their risk.

Solution Benefits

- Addresses governance concerns around management of PII and other sensitive data
- Improves risk management by identifying sensitive data in application schemas
- Streamlines regulatory compliance activities with scheduled scans and automatic report generation
- Locates and identifies sensitive data in Excel spreadsheets, Word documents and text files stored on shared file systems
- Deploys rapidly with fast time-to-value and low total cost of ownership
- Enterprise class software; no network hardware required

Do You Know Where Your Sensitive Data Is?

Enterprises constantly make copies of production application data to support development, testing, QA and business analysis. While most organizations have locked down their production environments sensitive data in non-production environments is exposed to broad communities of internal and external users. Test data sets can contain sensitive information such as taxpayer IDs, employee names, addresses, and dependent(s) information, credit card numbers, and intellectual property or classified information. Data theft prevention, sound governance practices and the need to satisfy compliance requirements for PCI, HIPAA, PII, GLBA and SOX make it imperative that organizations implement the necessary processes to identify and protect this sensitive information.



DgDiscover provides actionable intelligence regarding sensitive data in the enterprise.



Discover Sensitive Data In Your Environment

DgDiscover streamlines and automates the process of identifying and locating sensitive data in the enterprise. DgDiscover rapidly determines where databases are running in the network. It then determines what sensitive data is contained in databases and fileshares. DgDiscover searches databases and returns information such as the types of sensitive data identified, their table and column locations, and sensitivity confidence levels. It also searches shared file systems to identify sensitive data contained in documents and text files. DgDiscover's integrated reporting functionality makes it easy to analyze results and sort them according to criteria such as location, sensitive data types and sensitivity levels.

Using DgDiscover Improves Security and Compliance

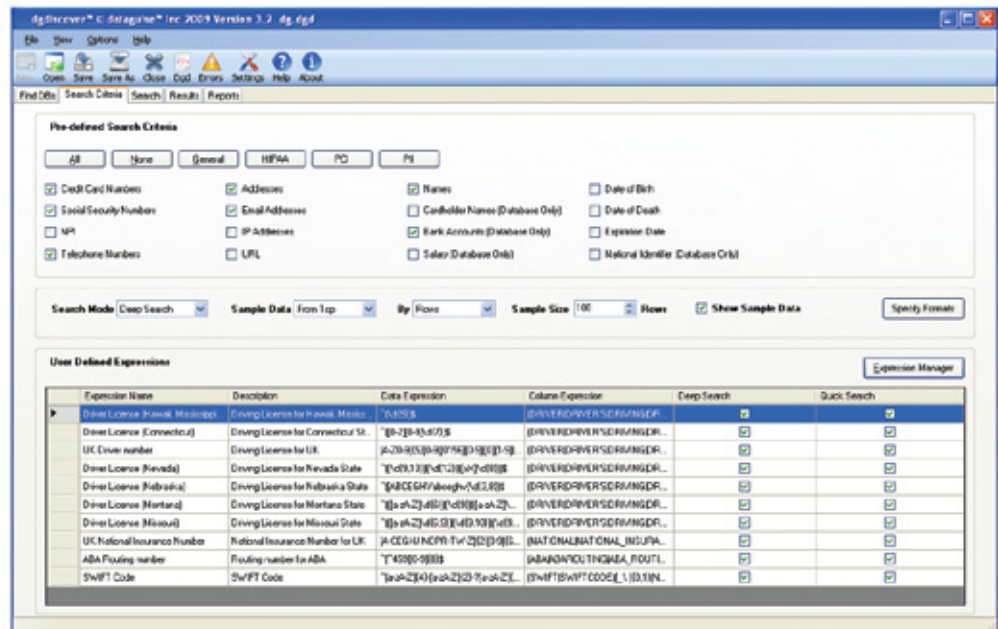
Information security professionals use DgDiscover to perform regular scans of their environments to help manage risks associated with sensitive data. Compliance teams use DgDiscover to audit the contents of production applications and produce audit-ready reports. Application analysts use DgDiscover to analyze application data sets and develop data risk mitigation strategies such as deleting obsolete data, encrypting, or masking data to transparently protect it from disclosure.

Part of An Integrated Solution

DgDiscover is part of an integrated solution which includes DgMasker for high-speed, database Masking on-Demand. Sensitive data identified by DgDiscover can be imported and leveraged by DgMasker, allowing users to go directly to specifying masking policies for columns of interest. DgDiscover enables sites to understand what sensitive data exists in the organization and implement the best mitigation strategies to effectively manage their sensitive data risk.

Key Features

- Scans networks to locate deployed database instances
- Searches across multiple heterogeneous databases and file systems for sensitive data
- Pre-defined search criteria for credit card numbers, social security numbers, national provider identifiers, bank accounts, birth dates, and several other sensitive data types
- Quick, user-friendly specification of custom search criteria to enable location of enterprise-specific or industry-specific sensitive data
- Highly efficient, two-stage database search process reliably identifies sensitive data that other data search approaches miss
- Runs interactively through an easy-to-use GUI, or on a scheduled basis, to produce audit-ready risk management reports
- Supports Oracle, IBM DB2, Microsoft SQL Server, MySQL, Teradata, Sybase, and Microsoft Access databases



DgDiscover users may search for pre-defined sensitive data types, or define their own data types using the Expression Manager.



Dataguise Inc.
 2201 Walnut Ave., Ste. 260
 Fremont, CA 94538
 P: 510.824.1036
 F: 866.384.8082
 E: info@dataguise.com
www.dataguise.com

Learn more about how **DgDiscover** and related Dataguise sensitive data protection solutions can help your organization manage sensitive data risk and address regulatory compliance requirements. Contact your Dataguise sales representative or visit our website at www.dataguise.com.