



Dataguise DgSuite – Sensitive Data Privacy Protection for the Enterprise

PRODUCT SUMMARY

The pressure for enterprises to take proactive measures to protect PII and other sensitive information under their care has never been greater. Technology managers, line-of-business owners, and information security and compliance professionals need solutions to help them locate, identify, protect and manage the sensitive data in their organizations. Dataguise addresses this challenge with DgSuite, an integrated set of enterprise applications for managing sensitive data privacy. DgSuite enables managers to locate and identify sensitive data on systems in use throughout the enterprise, transparently protect sensitive data in non-production use with next-generation masking technology, and leverage dashboard reporting to help them understand and manage sensitive data risks.

MANAGING SENSITIVE DATA IN THE ENTERPRISE

Enterprise applications generate and maintain large volumes of sensitive and proprietary information. These may include personally identifiable information (PII) about customers and employees, customer financial information such as account numbers and balances, employee health information, proprietary data such as supplier names and pricing, and company financial information. This data proliferates throughout the extended enterprise as it is shared with other departments, divisions and business partners to support critical activities such as testing, development, QA, support and business analysis. Organizations need to be able to leverage enterprise data to improve business processes and make better decisions while addressing compliance requirements and protecting sensitive data from disclosure.

INTEGRATED SOLUTION FOR PROTECTING DATA PRIVACY

Dataguise DgSuite meets this need with an enterprise solution for risk-based sensitive data privacy. DgSuite helps organizations by automating the identifica-

tion, categorization and periodic review of sensitive data holdings with DgDiscover. High performance Masking on-Demand™ with DgMasker transparently protects data in non-production and business analysis use. DgDashboard delivers actionable intelligence enabling executives, information security, compliance and infrastructure managers to better understand shared responsibilities for protecting data.

FASTEST TIME-TO-VALUE

Dataguise DgSuite delivers the fastest time-to-value for organizations seeking to meet their objectives for protecting sensitive data in the enterprise and address compliance initiatives. With DgSuite, auditors can monitor compliance and identify exposed sensitive data. DBAs can quickly and efficiently protect data that they distribute to support development, test, and analysis. CIOs and CISOs can visualize and monitor their organization's sensitive data risks. The results are better risk management, improved operational efficiencies and reduced regulatory compliance costs.

DgDiscover 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

DGDISCOVER – IDENTIFY AND LOCATE SENSITIVE DATA

DO YOU KNOW WHERE YOUR SENSITIVE DATA IS?

Knowing what sensitive information exists in the enterprise, and where it is located, are essential requirements for any organization's information security program. 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. As a result, information spreads throughout the organization to make tracking sensitive data difficult. Dataguard addresses the challenge of identifying and locating sensitive data with DgDiscover, a component of DgSuite. By finding data repositories deployed in enterprise networks and searching repositories for sensitive data, DgDiscover provides analysts the information they need to implement effective privacy risk remediation and provides managers the timely intelligence they require to manage their risk.

DGDISCOVER LOCATES AND IDENTIFIES SENSITIVE DATA

DgDiscover streamlines and automates the

process of identifying and locating the sensitive data in the enterprise. DgDiscover rapidly identifies where databases are running in the network. It then determines what sensitive data is contained in databases and shared file systems. DgDiscover searches databases and returns information such as the types of sensitive data identified, their table and column locations within a database, and whether or not the data has been protected with DgMasker. 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 locations, sensitive data types and sensitivity levels.

IMPROVED COMPLIANCE AND BREACH PREVENTION

Information security professionals use DgDiscover to perform regular scans of their environments to help them manage risks associated with sensitive data. Compliance auditors use DgDiscover to catalog the sensitive data maintained by production applications and produce audit-ready reports. Application analysts use

DgDiscover to analyze application data sets and more efficiently implement data risk mitigation strategies such as deleting obsolete data, encrypting sensitive data in production, setting policies for monitoring access to sensitive data, or masking data to transparently protect it from disclosure in non-production environments with DgMasker.

DgMasker Key Features

- Built-in and custom data transformations for masking sensitive information for non-production use in Oracle, IBM and Microsoft databases
- Automatically determines and maintains data relationships and preserves application integrity
- High performance masking-in-place architecture scales to support large enterprise data sets
- Exclusive CUPS (Consistent, Unique, Persistent, Synchronous) data transformation capability supports the most complex application requirements
- Integrates with DgDiscover for rapid analysis of applications and specification of masking policies

DGMASKER – PROTECT DATA PRIVACY WITH MASKING ON-DEMAND™

DATA IN NON-PRODUCTION ENVIRONMENTS

Enterprise applications and data warehouses are repositories for the “crown jewels” of any organization’s intellectual property. Leading enterprises today have improved the way they secure their production databases and enterprise applications. Many of these same enterprises, however, are not paying enough attention to how this data is being used for activities such as development, test, QA, support and business analysis. Once data is duplicated from a production source, multiple copies of that data can proliferate throughout the enterprise. Personally Identifiable Information (PII) and other sensitive or proprietary information can be exposed to external users such as outsourced development partners, or viewed by internal users who don’t have a “need to know,” making this data an attractive target for data compromising malware attacks.

DGMASKER DELIVERS SCALABLE, EFFICIENT DATA MASKING

Data masking is a state-of-the-art technique for protecting sensitive application data in non-production environments.

Masking works by transforming the sensitive data in an application data set so that it can be safely used to support test, development and business intelligence. Unlike encryption techniques, masking does not require complex key generation and management and masked data does not need to be decrypted before use. As a result, sensitive data protected by masking is completely secure from accidental or intentional disclosure even when being used by a downstream application. DgMasker, a component of DgSuite, masks sensitive application data sets with a highly scalable, masking-in-place technology that leverages the computing power and features of the database platform. With DgMasker, data administrators quickly define customized masking policies from an extensive library of pre-defined data masking options. DgMasker’s exclusive CUPS (Consistent, Unique, Persistent, Synchronous) options allow users to place additional constraints on how the data is masked, enabling them to meet virtually any downstream application requirements. DgMasker supports heterogeneous databases through a single user interface so administrators can define masking policies for applications across

databases from Oracle, IBM and Microsoft.

IMPROVED PROCESS EFFICIENCIES WITH GREATEST TIME-TO-VALUE

DgMasker generates custom masked data sets more quickly and reliably than manual subsetting or DBA-written scripts. With DgMasker, masking policies can be quickly implemented for any downstream application requirement and data is transformed using reliable and proven algorithms. Users can create and manage multiple policies for masking the same set of production data and then mask their data with the click of a button. This Masking on-Demand™ capability empowers administrators to create customized data sets to meet the needs of every downstream information consumer. DgMasker deploys quickly into any environment and features an intuitive, easy-to-use interface providing enterprises with the fastest time-to-value for protecting sensitive data privacy.

DgDashboard Key Features

- Provides on-demand reporting and analysis of DgDiscover and DgMasker results throughout the enterprise
- Summarizes database discovery, sensitive data discovery and masking operations
- Historical reporting shows results of past operations and trends over time
- Intuitive, web-based interface for quick deployment and fast time-to-value
- Interactive graphics and customized report generation capabilities
- Integrates with enterprise directory services and provides departmental, divisional or enterprise views according to users' roles

DGDASHBOARD – ENTERPRISE SECURITY INTELLIGENCE FOR SENSITIVE DATA

MANAGING SENSITIVE DATA IN THE ENTERPRISE

Information security best practices require that enterprises adopt a life cycle approach to how they generate, distribute and use sensitive data in their production and non-production systems. PII such as driver's license numbers and social security numbers, financial information such as salaries and credit card numbers, and proprietary information all represent a liability to the organization in the event of a breach or compromise. An effective, risk-based approach to managing sensitive data requires identifying systems which may contain sensitive data, inventorying and classifying data by sensitivity level, applying the appropriate controls for protecting data from disclosure, and engaging the various parties responsible for protecting

sensitive information in the enterprise. By far the biggest challenge is fostering the close coordination required between the information security analysts, application administrators, line-of-business owners, internal auditors, and executives in the organization responsible for understanding and managing sensitive data risks.

MANAGING SENSITIVE DATA RISK WITH DGDASHBOARD

DgSuite's DgDiscover and DgMasker products provide the foundation for an effective sensitive data protection program. DgDashboard, the third component of DgSuite, leverages DgMasker and DgDiscover to provide an enterprise view of the sensitive data life cycle. DgDashboard helps managers understand where sensitive data resides in the various systems in their

enterprise and see how the data is being protected when it is copied to non-production environments. These views help them monitor successful implementation of corporate policies and compliance efforts.

ACTIONABLE SECURITY INTELLIGENCE FOR THE ENTERPRISE

DgDashboard helps line-of-business managers, information security analysts, internal auditors, and C-level managers coordinate to effectively implement sensitive data protection policies. DgDashboard's role-based access controls provide customized views delivering users the information they need to make informed risk management decisions for their areas of responsibility. DgDashboard also includes sophisticated analytic capabilities so users can measure and quantify the impact of their sensitive data privacy programs.



DataguiSe™ Inc.
2201 Walnut Ave. #260
Fremont, CA 94538
Phone: 510-824-1036
Email: info@dataguiSe.com

Learn more about how DataguiSe sensitive data privacy 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.