Agency Contact:
Joe Austin
Ventana PR
(818) 591-2646
Joe.austin@ventanapr.com

DATAGUISE EXPANDS SENSITIVE DATA DISCOVERY AND MASKING SOLUTION WITH VERSION 3.0 TO HELP ORGANIZATIONS *FIND IT*, *SEARCH IT* AND *MASK IT*

Company announces innovative security solutions for discovering where sensitive data resides within production and non-production environments, and protecting from theft, loss or external breach

Fremont, CA, Via Oracle OpenWorld San Francisco, CA & SC World Congress New York City, NY., October 12, 2009 – **data**guise (http://www.dataguise.com), a leading innovator of security solutions for protecting sensitive data across the enterprise, today announced the next generation of the company's popular **data**guise security solution - **dg**discover™ 3.0 and **dg**masker™ 3.0. Version 3.0 is the industry's first integrated solution for comprehensive sensitive data discovery and masking. It is designed ***to find*** structured database repositories across the network, ***search*** and discover sensitive data in structured databases, and then ***mask*** or de-identify to protect sensitive data.

With **data**guise, organizations now have access to a single product that finds, searches and masks sensitive data across all databases throughout the enterprise. This allows organizations to create corporate masking policies for faster adherence to compliance regulations, lower risk of a data breach, and reduced reliance on cumbersome single database masking solutions.

"Sensitive data stored in non-production databases are exposed to abuse or negligence from outsiders but mostly from enterprise employees. Potential abusers, whom data masking aims to deter, are mainly users of test databases (programmers, testers and database administrators)," says Dr. Joseph Feiman, Research Vice President and Gartner Fellow. "Adopting data masking will help enterprises raise the level of security and privacy assurance against insiders' and outsiders' abuses. At the same time, data masking will make enterprises compliant with the security and privacy standards recommended by regulating/auditing organizations."

Find IT, Search IT, and Mask IT.

In many organizations, sensitive information is scattered in unprotected databases and file servers across corporate infrastructure.

Although most enterprises have taken measures to control access to critical data in their production environments this protection does not always extend to non-production data. Enterprises are continuously cloning production data to support development, testing, QA and pre-production deployment. As a result, sensitive data can be inadvertently propagated throughout the extended enterprise. This can include employee data such as Taxpayer IDs, employee names/addresses, and dependent information, customer information such as credit cards and card expiration dates, and intellectual property or classified information. The need to satisfy requirements for regulations such as, HIPAA, PCI and PII as well as data theft prevention and sound governance make it imperative that organizations implement the necessary processes to block exposure of this sensitive information. The first step is finding the databases containing the sensitive data.

Leading organizations, including Amgen (Nasdaq: AMGN), Facebook, John Muir Hospital, and the University of California Berkeley have turned to **data**guise as their partner in the protection against sensitive information loss or theft. **data**guise offers the first integrated product offering of its kind to combine both discovery of databases containing sensitive data, identification of the data at risk in the database and Masking In Place (MIP) of the information for seamless security. **dg**discover 3.0 empowers these organizations by quickly determining where sensitive information resides throughout the enterprise and **dg**masker 3.0 then de-identifies information targeted for use outside of the production network.

dataguise provides a high level of automation to deliver fast and reliable discovery without extensive management overhead. Unlike alternative offerings, the solution was developed to be simple and user friendly, resulting in a relatively low dependency on professional services for implementation and support. Both **dg**discover and **dg**masker scale for use in small and medium size enterprises to the largest multi-national corporations for unlimited enterprise-wide discovery and masking.

Additional benefits of **dg**discover and **dg**masker:

- Rapidly determines where databases are running;

- Quickly analyzes what tables/columns contain sensitive data for masking recommendation;
- Easy to deploy enterprise class software without network hardware installation requirements;
- Searches structured data repositories: Oracle, DB2, SQL Server, MySQL, Teradata, Sybase, MS Access;
- Searches unstructured data repositories for file formats that include Text, MS Office, PDF, XML, CSV and LOG;
- Pre-defined templates for PCI, HIPAA, and PII compliance regulations
- Ability to easily create and add custom policies;
- Provides an easy-to-interpret graphical summary of search results
- Secures data in *non-production* environments;
- Preserves business data rules so as not to break applications.

"The identification and protection of sensitive information across enterprise networks is a top priority to ensure more complete data protection," said Jim Krantz, President and CEO of Krantz Security Associates, New York City, New York, a leading **data**guise reseller. "**data**guise mitigates the risk of unauthorized use of information because with masking the data is usable for testing, but is not associated with sensitive information in any way other than format. In addition to critical protection of information assets, **data**guise automation significantly lowers total cost of ownership compared to alternatives for unmatched ease-of-use, value and security."

"Prevention of unauthorized use of privileged corporate information is a mandatory business directive in industries covered under rigid compliance mandates. This is especially true in the healthcare, biotech, government, and insurance industries," said Allan Thompson, SVP, BD, Marketing & Product Strategy for **data**guise. "No other solution combines the DNA of structured and unstructured database knowledge with security, and provides the breadth and depth of **data**guise in finding, searching and removing sensitive data from unauthorized access. For organizations under strict regulatory guidelines, **data**guise brings a critical security layer that ensures conformity."

Pricing and Availability

The **data**guise security solution, featuring **dg**discover 3.0 and **dg**masker 3.0, is available immediately with pricing based on environment and configuration. Organizations with security concerns reviewed in this announcement can learn more about **data**guise by visiting www.dataguise.com.

About dataguise

dataguise offers automated and advanced database security solutions to help ensure regulatory compliance and protect against data theft. **data**guise **dg**discover focuses on sensitive data discovery and classification across the enterprise and the company's **dg**masker product solution provides secure masking of database content with unprecedented flexibility and functionality across heterogeneous environments. For more information, call 510-824-1036 or visit www.dataguise.com