



Agency Contact:

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

dataguise ANNOUNCES DATA MASKING TEMPLATES, EXPANDING dgmasker SUPPORT ACROSS POPULAR ENTERPRISE APPLICATIONS

Template-based Solutions Enable Organizations Using Oracle® E-Business Suite, PeopleSoft Enterprise, SAP ERP and NextGen Healthcare Software To Reduce Time Spent Masking Large Sensitive Data Sets from Weeks to Days

Fremont, Calif., January 13, 2010 – dataguise™ (<http://www.dataguise.com>), a leading innovator of security solutions for protecting sensitive data across the enterprise, today announced the availability of its dgmasker™ enterprise application templates. Developed with leading application experts, the dataguise dgmasker templates provide enterprise organizations that have deployed Oracle® E-Business Suite, PeopleSoft Enterprise, SAP ERP and NextGen Healthcare Software with the ability to quickly secure Personally Identifiable Information (PII) for use in non-production application development, testing, QA & training environments.

Enterprise package applications are extremely complex, often requiring customizable deployments based on a particular organization or industry. The dataguise dgmasker application templates eliminate the complexities of protecting sensitive data within these applications, allowing organizations to implement secure data masking procedures in just a few days versus weeks – an industry first.

dgmasker is a highly automated and advanced security solution that helps enterprises meet the multitude of compliance requirements, including PCI-DSS, PII, HIPAA, GLBA and SOX. Unlike alternatives on the market, dgmasker is an easy-to-use data masking solution that has been built from the ground up with security and compliance in mind. By developing the dgmasker application templates, dataguise has further simplified the data masking process across industry-leading applications, offering its unique Masking On-Demand™ technology to

organizations spanning several vertical markets including education, healthcare, financial services and human resources.

The [University of California, Berkeley](#) recently leveraged **dgm**masker application templates for [NextGen Software](#) in order to enforce data privacy requirements in the university's software testing and application development environments. Prior to **dat**aguisse, UC Berkeley was challenged with providing quality test data to its application development group which works on the University's internally developed Web-based software solutions for SQL Server and includes the housing and assignment system.

UC Berkeley's use of **dat**aguisse technology has allowed large volumes of student information, critical for effective software development, to be randomized so that student social security numbers, record numbers, home addresses, names and dates of birth look like original data but are related in format only. The de-identification process takes place entirely within the production network, preventing the exposure of sensitive data before it enters the less secure non-production environment.

"Our internal application development processes require production quality data - which in our case means student data," said Steve McCabe, Associate Director of Information Technology in UC Berkeley's Residential and Student Service Program. "With the original data preserved in the production database, our software developers perform development and testing with data that have been processed using **dgm**masker to desensitize the information, essentially rendering it inert. This significantly reduces our risk exposure and allows us to readily share test data with our end users during QA and training."

In order to effectively implement packaged applications, enterprises need to have the ability to support these systems in production environments as well as during the development, QA, testing and pilot deployment process. These methods can expose highly-sensitive data to employees at various levels within an organization – developers, QA personnel, etc. – as well as offshore and outsourced personnel, increasing the risk of a data breach. **dgm**masker supports non-production use of enterprise applications while eliminating the risk of sensitive data exposure.

“Developing a masking strategy for packaged enterprise applications is a particularly difficult and time-consuming issue for organizations, as a typical application may contain tens of thousands of tables with hundreds of potentially sensitive data types,” said Allan Thompson, Executive Vice President, Operations for **dataguise**. “By using our **dgmasker** application templates, organizations can implement a comprehensive data masking solution within a matter of days, ensuring they are protected against exposure resulting from an internal or external breach, reducing their risk profile.”

Pricing and Availability

The **dataguise dgmasker** application templates will be available in the first quarter of 2010 with pricing based on environment and configuration. Organizations with security concerns reviewed in this announcement can learn more about **dataguise** by visiting www.dataguise.com.

Tweet this: dataguise Announces Data Masking Application Templates, Expanding dgmasker Support Across Industry-Leading Applications

Follow dataguise on Twitter at: <http://twitter.com/dataguise>

About dataguise

dataguise offers automated and advanced data security solutions to help ensure regulatory compliance, protect against data theft, discover sensitive data and maintain data quality.

dgdiscover enables organizations **to find** structured database repositories across the network, **search** and discover sensitive data in structured databases. **dgmasker** is then able to **mask** or de-identify to protect sensitive data. **dgmasker** 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

###