



Agency Contact:

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

DATAGUISE RELEASES WHITE PAPER ANSWERING KEY QUESTIONS ABOUT CHOOSING AND DEPLOYING DATA MASKING TO SECURE SENSITIVE DATA

*Systems Engineering Design and Management Expert Demonstrates Effectiveness of **dataguise**TM Solutions in Protecting Non-Production Data from Security Breaches*

Fremont, Calif., September 24, 2009 – dataguise (<http://www.dataguise.com>), a leading provider of next-generation security solutions for protecting enterprise sensitive data, today announced the release of an important new white paper that serves as a guide for organizations that need to employ data masking to protect data—especially non-production data—across their enterprises. And that describes a large percentage of companies doing business today. Companies with data masking requirements span all vertical markets and include corporations ranging in size from SMBs to the enterprise.

Entitled ***Why Add Data Masking to Your Best Practices For Securing Sensitive Data***, the paper maps out the route to choosing and deploying the most effective and easy-to-use protection against ever-increasing data breaches. This paper clearly summarizes when and how to employ data masking in parallel with other data security measures such as encryption, auditing, and access controls. Each of these technologies play an important part in securing data in production environments, however for *non-production* environments data masking remains the best practice for securing sensitive data. The comprehensive guide is authored by dataguise CTO Adrian Booth, whose 25 years' experience in systems engineering design and management make him an expert in enterprise-wide data protection.

Answering the Critical Questions

In his paper, Booth answers the key questions being asked by security professionals, systems engineers and database administrators as they seek to secure data and remain in compliance with growing lists of government regulations and industry standards. The paper goes on to note that data masking is THE key technology for providing strong production of private data in non-production environments. Neither encryption, auditing, access control nor vulnerability assessment and monitoring can provide the needed protection in this environment.

Data Masking Defined

Data_masking is the process of de-identifying (masking) specific data elements within data stores. It

ensures sensitive data is replaced with realistic but not real data. The result is sensitive customer information is not available outside of authorized environments. Data masking is done while provisioning non-production environments so that copies created to support test and development processes are not exposing sensitive information. Masking algorithms are designed to be repeatable so referential integrity is maintained.

Ensuring Successful Deployment

And, unless the right team drives a data masking project, the initiative could also lose direction and momentum. Booth writes, “A key question often raised by enterprises is who should drive the data masking project? Security departments are preferred if they exist. Otherwise, IT Applications groups, along with other related personnel from database and business analyst teams should be part of the data masking team.”

Asserting that “all enterprises should ensure strong protection for private data, regardless of where it is stored,” Booth explains why **dataguise** solutions, including **dgm masker**[™], are best suited to this role.

“**dataguise** offers **dgm masker** for databases, a highly automated and advanced security solution that helps enterprises meet various compliance requirements, including PCI, PII, HIPAA, GLBA and SOX. Unlike other solutions on the market, **dgm masker** has been built from-ground-up with security and compliance in-mind. **dgm masker** lets application developers and testers test applications against production data WITHOUT being exposed to sensitive information including credit card numbers, social security numbers, account numbers and other data.”

“We hope this paper gives people responsible for data security the information and confidence they need to make informed decisions about securing their non-production environments,” Booth says. “It should become clear after reading the paper that organizations can no longer afford to ignore this critical aspect of enterprise data security.”

Why Add Data Masking to Your Best Practices For Securing Sensitive Data, is available to registered users at www.dataguise.com.

About dataguise

dataguise offers automated and advanced database security solutions to help ensure regulatory compliance and protect against data theft. **dataguise dgd discover**[™] focuses on sensitive data discovery and classification across the enterprise and the company’s **dgm masker** product suite 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. ###