



Agency Contact:

Joe Austin

Ventana PR

(818) 332-6166

Joe.austin@ventanapr.com

**DATAGUISE PROVIDES GUIDANCE IN MEETING PCI DSS 2.0 REQUIREMENTS
WITH ADVANCED SECURITY SOLUTIONS**

New Guide Shows how Sensitive Data Discovery and Masking Aid in PCI DSS 2.0 Compliance

Fremont, Calif., December 15, 2010 – Dataguise™ (<http://www.dataguise.com>), a leading provider of security solutions for protecting sensitive data across the enterprise, has developed a guide, "Key Steps to Meeting PCI DSS 2.0 Requirements Using Sensitive Data Discovery and Masking," that shows organizations how integrated sensitive data discovery and masking solutions can be used to efficiently and cost effectively address the latest security requirements spelled out in PCI DSS 2.0.

All organizations with payment card data - including merchants who are authorized acceptors of cards and service providers who store, process or transmit cardholder data - must meet this latest iteration of the standard, released in October 2010, by January 1, 2011. Dataguise solutions help organizations comply with sections 3.1, 3.1.1, 7, and 11 of PCI DSS 2.0 by enabling them to quickly identify cardholder data in networks and systems, facilitate safe testing of applications with masked production data and manage risks to sensitive data.

"Dataguise solutions are organized around four critical data protection functionalities: finding databases deployed on the network; searching databases and shared file systems for sensitive data; remediating sensitive data risk in application data sets with next-generation, high-speed data masking; and reporting on the existence of sensitive data risks in the enterprise," said Allan Thompson, EVP, Operations for Dataguise. "These are exactly the functionalities companies must have in place to meet the requirements of PCI DSS 2.0. Our new guide maps the

standard's requirements and testing procedures against our products' capabilities to illustrate how DgDiscover and DgMasker can help organizations fulfill those requirements."

These highlights from Dataguise summarize some PCI DSS 2.0 requirements and the corresponding Dataguise capabilities.

1. **Do not store the full contents of any track from a magnetic strip or equivalent data.** DgDiscover automatically locates sensitive data in unstructured sources such as files, documents and log files, as well as in structured database schemas and contents.
2. **Do not store the card verification code or value used to verify card-not present transactions.** DgDiscover can leverage the user-defined-expression features to automatically locate card verification codes in log files, documents, and database schemas and contents.
3. **Do not store the personal identification number (PIN) or the encrypted PIN block.** DgDiscover can leverage its user-defined expression feature to automatically locate likely PIN numbers in log files, documents, and database schemas and contents.
4. **Mask the primary account number (PAN) when displayed (the first six and last four digits are the maximum to be displayed).** DgMasker provides a number of options for masking PAN information. For example, it can use character masking to selectively display PAN digits in a customer support database. More sophisticated options include "intellimasking," which masks only selected characters within a string with random values; masked values can be consumed by downstream applications.
5. **Render PAN unreadable anywhere it is stored using one-way hashing based on strong cryptography, truncation, index tokens and pads, or strong cryptography with associated key-management processes and procedures.** DgMasker protects translation tables with strong hashing algorithms to prevent potential exposure of PANs while providing consistency and repeatability in masking operations. DgDiscover searches databases and files, removable media, and audit log files to verify that PAN data is adequately protected.
6. **Do not use production data (live PANs) for testing or development.** DgMasker masks sensitive information so PANs may be safely leveraged for non-production applications, including testing and development. DgDiscover finds database instances on the network and searches databases to identify and locate PANs, enabling managers and auditors to verify sensitive data is not used in non-production environments.

7. **Restrict access rights to privileged user IDs to the fewest privileges needed to perform job responsibilities.** With DgMasker, data custodians can create realistic-looking data sets that protect sensitive information from being viewed. Test, development and support personnel can work from application instances running on these masked data sets, thus reducing the number of IDs required for production application instances.

Organizations that use Dataguide solutions have a better knowledge of where sensitive information such as cardholder data resides, can support key business processes such as application development, test and deployment without exposing cardholder data, and have a more complete view of the organizations' activities in protecting cardholder data.

About DgDiscover and DgMasker

DgDiscover is a software solution that scans networks to locate deployed data repositories stored throughout the enterprise and identifies instances of sensitive data. To support key business processes, enterprises need to be able to leverage their sensitive production data for activities such as development, testing, QA, support and business analysis. Dataguide helps organizations do this safely with DgMasker, a risk-based data protection solution that transparently masks sensitive information in production data sets for use in non-production environments.

To receive a free copy of "Key Steps to Meeting PCI DSS 2.0 Requirements Using Sensitive Data Discovery and Masking" visit <http://www.dataguide.com/resources/index.html>

Tweet this: Dataguide Provides Key Steps to Meeting PCI DSS 2.0 Requirements with its Security Solutions

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

About Dataguide

Dataguide offers automated and advanced database security solutions to help ensure regulatory compliance and protect against data theft. Dataguide DgDiscover focuses on sensitive data discovery and classification across the enterprise and the company's DgMasker 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.dataquise.com