

DataSniff Solutions for Discovering Sensitive Information

Locating Personally Identifiable Information (PII) on mainframe systems

Overview: In an age of identity theft, protecting sensitive data is a top priority within many enterprise organizations. Stiff fines or high litigation costs are often a consequence of losing unprotected personal data. Losing this information to identity theft, may cause unrecoverable damage.

Social security numbers or credit card numbers are often located in multiple locations within an enterprise organization, which presents a difficult task when outlining and deploying a protection strategy. PII could be located in legacy mainframe data, customer service notes, documents, files, datasets, spreadsheets, or even emails. To create a strategy for protecting PII data, it is critical to “MAP” the data and determine where it resides.

Finding PII information in unstructured or structured data can be a challenge. *This is especially true within mainframe data sources, where structured data often lacks standardized mechanisms for determining the data structure outside of the application in use.*

The Solution: DataSniff blends mainframe access technologies with a well-known search technology. This powerful combination locates sensitive information of many different varieties and easily allows organizations to control that data.

Benefits: Discover Sensitive Mainframe Data

- Accurate Data Inventory
- Quick Implementation
- Reasonable Cost
- Scalable

Ensuring your sensitive mainframe data is located for protection or control.

Use Cases:

- Payment Card Industry (PCI DSS) Audits
- Privacy
 - HIPPA, EU DPD, PIPED-A, etc.
- Risk Management & Compliance
 - NIST, DIACAP, FISMA, etc

- COBIT, SOX, etc.

- Other PII Initiatives

Features:

DataSniff - Accessing Mainframe Data

- Supports unstructured data in VSAM, QSAM, ISAM data sets and partitioned data sets. Can access all datasets on the mainframe or can use a data set name mask to limit which data sets are accessed.
- Supports structured data stored in VSAM, QSAM and ISAM data sets as well as IMS and DB2 databases. Supports automatic extraction of meta data from system tables for DB2 databases. Supports assisted extraction of meta data from copy books and other existing sources for VSAM, QSAM, ISAM, and IMS data stores. Supports common mainframe practices for storing data including Packed Decimal, Occurs, and Redefines field and record types.
- Supported IMS databases:
 - HDAM - Hierarchic Direct Access Method
 - HIDAM - Hierarchic Indexed Direct Access Method
 - HISAM - Hierarchic Indexed Sequential Access Method
 - HSAM - Hierarchic Sequential Access Method
 - SHISAM - Simple Hierarchic Indexed Sequential Access Method
 - SHSAM - Simple Hierarchic Sequential Access Method
 - INDEX - Secondary Indexes Supported for: HDAM, HIDAM, & HISAM.
- Supports creating and persisting all of the meta data that describes the structured and unstructured raw data sources on a mainframe as Host Source definitions. These definitions include all the information necessary to access the data and can include credentials.
- Supports the creation and persistence of DataViews. DataViews define a subset of columns, filters and row limit restrictions that can be used to limit what data is to be

DataSniff Solutions for Discovering Sensitive Information

Locating Personally Identifiable Information (PII) on mainframe systems

analyzed. In most use cases, DataViews will be used to limit the analysis to suspect fields like text fields. In addition, DataViews can be used to include unique identifying information about the record.

- Supports other structured data sources including SQL Server, iSeries DB2, ORACLE and most other databases accessible via ODBC.
- Supports the inclusion of an Analytical Engine Module which can be used feed any data defined in a DataView to the search engine for analysis. The module can also be programmed to systematically create DataViews for unstructured data sets (typically limited by a name mask.) It can be programmed to systematically feed all or some of the DataViews defined in the system to the search engine for analysis. The module can also be programmed to accommodate transformations of the data for such things as adding a record number field to DataViews of unstructured data.

The Search Engine - Analyzing Mainframe Data

- Supports the analysis of unstructured data to identify the presence of PII.
 - Using pre-defined PII analysis rules/policies.
 - Using ad-hoc PII analysis search terms.
 - Using both exact and fuzzy logic algorithms.
- Supports a flexible reporting mechanism via a PII inventory file/report, web report or a client application interface.
- Can construct index of suspect PII data in non-human readable format or in an encrypted format.
 - Footprint is a fraction of original data.
 - The index could be used to dynamically find PII in suspect PII data on demand.

Deployment

The DataSniff team will deploy this solution with the following options:

- Installation and configuration on an organization's server,
- As an appliance, or
- As a virtual machine.

Additionally, we will install a DataSniff sub-system component on the targeted mainframe.

For one-time projects, the DataSniff team rapidly implements this solution, which is provided on a limited professional services engagement, using the software described herein.

We may configure or customize the software, based on customer preferences and requirements.

For more information contact:

Email: sales@datasniff.com

Call: (650) 564-9800.