

RAXA™

SENSITIVE DATA MANAGEMENT PLATFORM



PROTECTING SENSITIVE INFORMATION AT THE SOURCE

With data exposure costs on the rise, security professionals, compliance personnel, and information technology departments are scrambling to find better ways to secure their most sensitive data, understand exposure, and calculate associated risk. Many security products focus on data intrusion – the outer layer of protection, such as perimeter, network, host, and application. This approach does not take into consideration the data itself – data extrusion. Kinetic Networks developed RAXA™ to fill this void by working from the inside out – at the data level.

“Damage from insiders and privileged users represents the most-significant threat, while data encryption and network segmentation remain the top technical challenges”
– Gartner Research

RAXA™ SENSITIVE DATA MANAGEMENT PLATFORM

The RAXA™ SENSITIVE DATA MANAGEMENT PLATFORM is the first integrated security solution that discovers, protects and monitors sensitive data at rest and in motion throughout the enterprise without negatively impacting productivity.

KEY DIFFERENTIATORS

- Database independent
- Value-level and cell-level inspection of data structures
 - RAXA™ DISCOVER inspects the database at the cell-level to identify sensitive information
- Fully-integrated platform
 - RAXA™ DISCOVER identifies sensitive fields for encryption and desensitization
 - Rule sets and classifications flow from RAXA™ DISCOVER to RAXA™ PROTECT and RAXA™ MONITOR
- Unique approach based on proprietary algorithm
 - Risk assessment based on weighted volume, visibility, and sensitivity
- User access/field categorization mapping
 - RAXA™ DISCOVER reconciles DB security models against the actual data values to provide a detailed access matrix as roles and privileges change
- Metadata driven encryption technology
 - Allows for protected data to be returned to original values
 - Maintains referential integrity across multiple tables and datasets
 - Incremental obfuscation provides update capabilities for protected datasets



RAXA™

SENSITIVE DATA MANAGEMENT PLATFORM



RAXA™ DISCOVER: IDENTIFY THE RISK

Before an organization can address its sensitive data management issues, it must first identify and evaluate its risk. Many IT and security professionals are surprised to discover not only where sensitive data is located, but who has access to it, and with whom they are sharing it.

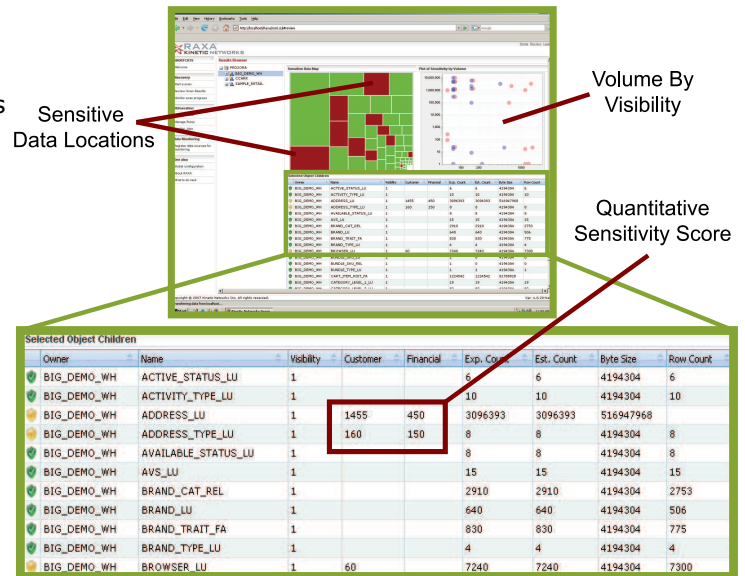
The RAXA™ DISCOVER component helps organizations identify and evaluate their sensitive data risk, automating what has traditionally been a manual, repetitive and error prone task. RAXA™ uses a data classification engine that includes identifying user access rights and scoring data sensitivity in relation to risk. It works on a variety of data elements including those involved in compliance initiatives. RAXA™ highlights potential compliance violations and data classification issues while exposing sensitive data proliferation that can often be overlooked.

FEATURES

- Risk score based on proprietary algorithm
- Standard and configurable data classifications and rule sets for customization
- Column, field, and table level data classification
- User classification

BENEFITS

- Quantitative risk analysis
- Realistic risk assessment based on specific business requirements
- Available modules support compliance standards
- Automates existing manual, repetitive and error prone reconciliations
- Single, unified view of your enterprise data access



RAXA™ documents potential areas of risks and highlights those areas identified as having the greatest risk. The most critical factor is to provide management the insight to make informed decisions about potential risk exposure.

RAXA™

SENSITIVE DATA MANAGEMENT PLATFORM



RAXA™ PROTECT: MITIGATE THE RISK

Traditional approaches, such as encryption, often reduce the intrinsic business value of the data. RAXA™ PROTECT can mask, encrypt or obfuscate the data depending on the level of security required. Unlike data masking, hashing and scrambling, obfuscation removes the sensitive nature of the data while retaining its intrinsic business value. For example, an obfuscated social security number (SSN) will still look and feel like an SSN to the data consumer. An obfuscated street address will still look like a real mailing address. Reports will still reveal actual values for business applications and provide real analytic capabilities, but the sensitive elements within the data are disguised.

FEATURES

- Maintains data relationships across multiple data sources, retaining underlying business value
- Supports all major cryptographic standards
- Supports compliance standards such as PCI and HIPAA
- Metadata driven, reversible obfuscation
- Incremental obfuscation provides update capabilities for protected datasets

BENEFITS

- Generates desensitized data that looks and acts like real data
- Allows use of desensitized production data for testing
- Maintains referential integrity between multiple source systems over time
- Reduces reliance on endpoint security needs when data is lost via a stolen laptop, USB key, CDs, emailed files, etc.
- Produces consistent, repeatable obfuscation across multiple data extracts and multiple source systems
- Provides ability to access original source data
- Provides audit trail to demonstrate data validity

Example

Production Data

Name	Surname	SSN	DOB
George	Richards	625-34-5643	11-Nov-1973
Peter	Walker	345-22-2322	02-Dec-1969
Susan	Smith	544-42-3432	06-May-1945
Mary	Jones	454-34-4354	04-Mar-1980



Protected Data

Name	Surname	SSN	DOB
George	Smith	425-32-5643	11-Nov-1973
Peter	Jones	235-12-2322	02-Dec-1969
Susan	Richards	343-12-3432	06-May-1945
Mary	Walker	843-12-4354	04-Mar-1980

RAXA™

SENSITIVE DATA MANAGEMENT PLATFORM



RAXA™ MONITOR: TRACK CHANGES AND ALERT

Data is not static: business models change, employees come and go, and data volumes expand and contract. Kinetic Networks understands this and actively monitors both changes to data patterns and to user behavior. Changes could indicate a security problem.

FEATURES

RAXA™ MONITOR actively monitors data visibility, sensitivity, volume and activity to evaluate potential changes to risk factor:

- Volume
 - Monitors the amount of data a user has access to or has acquired and flags anomalies
- Visibility
 - Tracks users and data access (copying, creating, accessing, sending and granting access)
 - Determines if roles and access levels map to the data being accessed
 - Alerts the user and supervisor(s) and generates actionable events
- Sensitivity
 - Monitors changes to the data schema including new sensitive fields, new tables, new procedures that might expose sensitive information, etc.
 - Alerts the creator and the supervisor(s) of possible security risk, and generates actionable events
- Activity
 - Monitors user activity for potential security violations (passwords, account creation and modification)

BENEFITS

- Continuous monitoring means immediate notification of security violations
- Reduces presence of unmanaged sensitive data
- Allows managers to close the loop with data stewards to ensure timely resolution of security breaches
- Provides continuous alerting until security issues are acknowledged and resolved
- Single, unified monitoring view of your enterprise data access

There will always be individuals who need access to sensitive data, and data characteristics will continue to evolve as well. The key is monitoring the user and the data to better understand and prepare for risks. Kinetic Networks designed RAXA™ MONITOR to address these issues.

RAXA™

SENSITIVE DATA MANAGEMENT PLATFORM



USING RAXA™

Sensitive data is tied to information needed and used by nearly every business user in an organization. RAXA™ can help identify and evaluate the relative risk, protect the data while still allowing analysis, and obfuscate that which should not be accessed.

RAXA™ can add value to companies in many areas including:

- Managing sensitive data proliferation
- Understanding inherited or legacy data sources
- Reducing the need for excessive security measures due to unknown data
- Automating database documentation projects
- Sharing syndicated or shared data outside the organization
- Combining data sets with sensitive fields
- Using realistic data for outsourced, offshore projects
- Using realistic data for development or testing environments
- Increasing analyst productivity and effectiveness
- Using production data for demonstrations or presentations

PROJECT OVERVIEWS

DISCOVERY

A market-leading financial institution worried about data proliferation and who had access to sensitive information. While the organization had undergone business process reengineering to reduce the transparency of sensitive data, they needed to verify the processes were working. Kinetic Networks used RAXA to provide data discovery audit. Reports included charts that outlined the highest areas of risk. This audit showed that the new processes were insufficient and paved the way for more improved processes to be developed.

DE-IDENTIFICATION

A major financial services firm uses a data mart to analyze customer interaction with its online system. The data feeds contain confidential information, which causes risk of exposure. Kinetic Networks implemented the sensitive data solution to dynamically find and obfuscate the sensitive data fields. The solution converts data such as sensitive social security numbers to alternate values, yet maintains the contextual relationships of the data and retains its integrity. This allows data from different sources to align when brought together for analysis.

RAXA™

SENSITIVE DATA MANAGEMENT PLATFORM



TECHNICAL SPECIFICATIONS

MEMORY	CPU
<p>Recommended</p> <ul style="list-style-type: none">2 GB RAMSeparate dedicated server <p>Minimum</p> <ul style="list-style-type: none">512 MB RAM1 GB Free disk space	<p>Recommended</p> <ul style="list-style-type: none">Dual CPU at 2GHz64 Bit <p>Minimum</p> <ul style="list-style-type: none">Dual CPU at 2 GHz32 Bit
APPLICATION SERVER	ENCRYPTION/CRYPTOGRAPHY
<ul style="list-style-type: none">Tomcat 6.0.16 or greaterWebSphere 6.1Most major J2EE-compliant	<ul style="list-style-type: none">Support for a wide range of standard algorithms including RSA, DSA, AES, Triple DES, SHA, PKCS#5, RC2 and RC4
OPERATING SYSTEM	METADATA REPOSITORY
<ul style="list-style-type: none">MS Windows Server 2000-2003Red Hat Enterprise 4Solaris 10	<ul style="list-style-type: none">Supports all major database platformsPKCS#11 cryptographic token support
CLIENT BROWSER	DATABASE SUPPORT
<ul style="list-style-type: none">Supports all major browsers	<ul style="list-style-type: none">Supports all major databases