Camouflage Data Discovery is a full-featured sensitive data discovery and analysis tool that automates the process of finding and analyzing the information within your organization that is subject to legislative or industry compliance, corporate governance, and risk management policy. Compliance legislation and information security standards such as HIPAA, PCI-DSS, SOX, GLBA and FERPA require organizations to restrict access to sensitive information. But how can you prevent unwanted disclosure of sensitive data if you don’t know where it is? The challenge often lies in the complex mix of legacy, homegrown and third-party applications that run your organization. Sometimes the original developers of legacy applications have moved on and adequate documentation is non-existent. Many times commercial software is a proprietary “black-box” requiring expensive experts and time-consuming manual effort to uncover the sensitive data contained within. Regardless of whether you need to secure in-house or commercial off-the-shelf applications, Camouflage Data Discovery makes it easy to identify data at risk. Organizations that understand the nature of their sensitive data and the context in which it resides can then take measures to put appropriate data privacy and security controls in place.

HOW DATA DISCOVERY WORKS

Intelligent discovery algorithms and a high performance architecture allow Discovery to efficiently scan billions of data points for sensitive data and data relationships throughout an enterprise, greatly reducing the need for manual effort and enabling a more agile and efficient process. To find sensitive information, such as credit card numbers, bank card numbers, social security numbers, birth dates, names, addresses, phone numbers, and a wide variety of other sensitive and personally identifiable information, Data Discovery intelligently profiles database content and metadata for sensitive data matching predefined search patterns and uses heuristics and statistical analysis to identify sensitive data relationships. Results are persistently stored in a centralized Data Discovery repository and can be compared with historical results to detect and audit changes to the sensitive data landscape. Browser-based data analysis tools and reports enable risk managers and other business stakeholders to accurately and thoroughly assess sensitive data risk and derive actionable insights for improving the organization’s data security posture.

Benefits of Camouflage / Data Discovery

- Assess data risk by discovering where sensitive information resides and who has access
- Classify and categorize sensitive information
- Ensure compliance with legislative authorities including HIPAA, PCI-DSS, SOX, GLBA and FERPA
- Reduce the threat of internal data breaches
- Utilize pre-packaged search templates to fast track data security projects, reduce costs and eliminate inefficient manual search processes
- Derive actionable insights with customizable report templates
- Visualize data risk with extended browser-based data analysis tools, data export capabilities (such as CSV and MS Excel formats) and integration capabilities for third party reporting tools
- Supports a wide variety of platforms and databases

Intelligently identify, classify & analyze sensitive data with data relationship discovery and data analytics

Camouflage Data Discovery is a full-featured sensitive data discovery and analysis tool that automates the process of finding and analyzing the information within your organization that is subject to legislative or industry compliance, corporate governance, and risk management policy. Compliance legislation and information security standards such as HIPAA, PCI-DSS, SOX, GLBA and FERPA require organizations to restrict access to sensitive information. But how can you prevent unwanted disclosure of sensitive data if you don’t know where it is? The challenge often lies in the complex mix of legacy, homegrown and third-party applications that run your organization. Sometimes the original developers of legacy applications have moved on and adequate documentation is non-existent. Many times commercial software is a proprietary “black-box” requiring expensive experts and time-consuming manual effort to uncover the sensitive data contained within. Regardless of whether you need to secure in-house or commercial off-the-shelf applications, Camouflage Data Discovery makes it easy to identify data at risk. Organizations that understand the nature of their sensitive data and the context in which it resides can then take measures to put appropriate data privacy and security controls in place.

HOW DATA DISCOVERY WORKS

Intelligent discovery algorithms and a high performance architecture allow Discovery to efficiently scan billions of data points for sensitive data and data relationships throughout an enterprise, greatly reducing the need for manual effort and enabling a more agile and efficient process. To find sensitive information, such as credit card numbers, bank card numbers, social security numbers, birth dates, names, addresses, phone numbers, and a wide variety of other sensitive and personally identifiable information, Data Discovery intelligently profiles database content and metadata for sensitive data matching predefined search patterns and uses heuristics and statistical analysis to identify sensitive data relationships. Results are persistently stored in a centralized Data Discovery repository and can be compared with historical results to detect and audit changes to the sensitive data landscape. Browser-based data analysis tools and reports enable risk managers and other business stakeholders to accurately and thoroughly assess sensitive data risk and derive actionable insights for improving the organization’s data security posture.
**BENEFITS**

**VISUALLY ASSESS RISK**

With surging data volumes and proliferating content repositories, accessing, analyzing and securing data has become increasingly difficult for IT users and data managers alike. The first step towards assessing data at risk is knowing where sensitive information is located within your organization.

Sensitive information associated with Data Discovery and Data Profiling is securely stored within a centralized repository to facilitate collaboration among authorized users. Data Discovery elements such as search rules and data connectors can be shared among users for consistency and accuracy, and the search results associated with Data Discovery run configurations and Data Profiles are also stored and leveraged via pre-packaged reports and design tools to facilitate communication within IT, Risk Management, and other stakeholder groups to accelerate remediation and guide the selection of data security controls. Camouflage Data Discovery provides a variety of reporting options, from an in-depth data filtering and export tool to more specific informational reports.

**LOW COST, RAPID RESULTS**

By replacing error-prone manual data analysis with automated search processes, Camouflage Data Discovery dramatically improves the speed and accuracy at which sensitive data is identified, classified and earmarked for protection.

**INTUITIVE AND EASY TO USE**

You don’t need to be a database expert to quickly and easily identify information that should only be accessed on a need-to-know basis. Simply point and click to start the search based on templates and be presented with a clean listing of relevant, actionable results and sensitive data analysis reports.

**REPEATABLE, FLEXIBLE, WITH Expert GUIDANCE**

Kick-start compliance with search templates and refine as you go to produce reliable, repeatable search processes tailored to the unique requirements of your organization. Best practice guidance from our data security experts maximizes the benefits to your organization.
FEATURES

BROAD PLATFORM SUPPORT
Leveraging open standards such as Java, JDBC and XML, Data Discovery supports a wide variety of operating systems and data sources from Windows, UNIX and Linux to Mainframe and AS/400. Text files and databases including Oracle, SQL Server, DB2, SAP ASE, Teradata, MySQL, HSQL, Netezza, PostgresSQL, IMS, and more are supported.

CENTRALIZED REPOSITORY
The repository database securely stores, organizes and processes sensitive information associated with search. Proven search rules can be reused, rather than reinvented, to yield persistent results, and connectors to data sources can be created and maintained by administrators at an organizational level for improved consistency and accuracy.

INTEGRATED PRODUCT SUPPORT
Discover, subset and mask sensitive data within a single, integrated suite of products. Camouflage offers best of breed functionality in support of your data security initiatives. Automatically export Data Discovery results from the centralized repository database into a Functional Masking Document (FMD). The generated FMD is downloaded to your local environment as an Excel document, which can then be used to build data masking projects that prevent disclosure of sensitive data in support of development, testing, training and outsourcing activities.

UNDERSTAND YOUR SENSITIVE DATA LANDSCAPE
By automating the identification of data relationships via metadata heuristics, data profiling and statistical analysis, Camouflage Data Discovery greatly reduces the need for manual effort, enabling a more agile and efficient process in analyzing the sensitive data landscape of an enterprise. Data profiling provides snapshots of database information at a particular point in time, then syncs to scan those databases to retrieve metadata information. That data is then stored in a centralized repository where it is used to generate a Functional Masking Document (FMD) or design a Subsetting Configuration. Data analysis reports provide a comprehensive overview of the Discovery Run results in an in-depth and easy to understand manner. The graphs, tables and recommendations in the reports are ideal for sharing with business stakeholders.

DATABASES SUPPORTED
- Oracle
- SQL Server
- DB2
- Sybase ASE
- Teradata
- MySQL
- HSQL
- Netezza
- PostgresSQL
- IMS via export to VSAM (KSDS, ESDS) or QSAM data files
ENTERPRISE-CLASS SCALABILITY AND COLLABORATION

Fast and highly scalable, Camouflage Data Discovery is engineered to meet the demands of today’s data-driven enterprise. Search multiple data sources in parallel to rapidly locate sensitive data wherever it resides within your organization. Data Discovery elements such as search rules and data connectors can be configured globally for consistent and synchronized organization-wide execution, scaling and management of data security projects. Users with defined permission access can easily see what data security projects they and others have been working on and the browser-based user interface provides complete access to create, maintain, share and execute discovery run configurations and manage search results and associated reports.

SENSITIVE DATA ANALYTICS

With extended browser-based data analysis tools, data export capabilities (such as CSV and MS Excel formats) and integration capabilities for third party reporting tools, visualizing data at risk and taking action to mitigate those risks has never been easier. View, sort and filter discovered data via executed data profiles and Discovery Run Configurations and define settings by category, heat map and data analysis reports. Defined filters and proven search rules can be reused, rather than reinvented, and connectors to data sources can be created and maintained by administrators, minimizing the level of manual effort and time in managing the sensitive data landscape of an enterprise.

For more information on Camouflage Data Discovery or to obtain a quote, contact a Camouflage sales representative today at info@datamasking.com or call 1.866.345.8888

As pioneers in data masking, Camouflage offers an end-to-end intelligent data masking solution featuring discovery, classification, subsetting and data masking technologies designed to ensure that sensitive information is properly protected for use in application development, testing, outsourcing and training. Combining its team of data masking experts and best practice guidance, Camouflage offers a proven and comprehensive approach to securing sensitive data and facilitating compliance with legislation like US-EU Safe Harbor, EU Data Protection Directive, HIPAA/HITECH, PCI-DSS, GLBA, PIPEDA and more. For additional information please visit us at www.datamasking.com

Learn more about how Camouflage’s integrated solutions help ensure information security and regulatory compliance. Visit us at www.datamasking.com, or contact a Camouflage sales representative at info@datamasking.com or call 1.866.345.8888.

©2015 Camouflage Software Inc. All rights reserved. Camouflage and related designs are the property of Camouflage Software Inc. All other trademarks are the property of their respective owners. There are no warranties, express or implied, with respect to the contents of this documentation.