

## Dataguise DgDiscover™ for Microsoft SharePoint

Sound corporate governance and compliance practices require that companies know when sensitive information is posted to corporate SharePoint sites. DgDiscover for SharePoint helps organizations quickly identify, locate and prioritize the files and data in SharePoint sites that pose the greatest potential risk allowing them to take appropriate actions.

### Solution Benefits

- **Fast time-to-value**  
Deploys quickly into existing SharePoint installations and requires no additional hardware or software
- **Low overhead**  
Searches may be scheduled for off-peak times so they are transparent to user communities. Incremental scanning of new files reduces process overhead
- **Reduces sensitive data privacy risks without burdening administrators**  
Reports support easy prioritization of search results, allowing administrators to focus on the specific files and sensitive data types representing the greatest potential for risk
- **Part of a comprehensive data privacy protection solution**  
Works with Dataguise DgDiscover and DgMasker to provide a comprehensive solution for managing sensitive data risk in the enterprise

### The Problem of SharePoint Discovery

Microsoft SharePoint improves organizational productivity by providing an easy to use platform for sharing documents and information among workgroups. These same productivity benefits, however, can greatly increase an organization's sensitive data privacy risks. SharePoint administrators and Information Security managers worry about the potential for sensitive information such as PII, credit card numbers, or proprietary information being posted (intentionally or unintentionally) to SharePoint sites. Timely knowledge of where sensitive data may have been posted to SharePoint sites is needed to allow managers and administrators to identify and remediate their sensitive data risks.

### Sensitive Data Discovery with DgDiscover

Dataguise DgDiscover automatically identifies and locates sensitive data in databases and shared file systems. DgDiscover users begin by specifying what sensitive data types they want to locate. These include pre-defined sensitive data types such as credit card numbers, social security numbers, birth dates and telephone numbers. Users can also add their own custom, user-defined sensitive data types for searching. Next, users specify the targets for their searches. These can include databases such as Oracle, SQL Server, My SQL, Sybase, Access and Teradata, as well as shared file systems to identify sensitive data in Word, Excel, PowerPoint, Adobe Acrobat and other documents. DgDiscover's multi-threaded implementation combined with its highly refined data classification logic provides highly accurate search results quickly.

### DgDiscover for SharePoint

Dataguise DgDiscover for SharePoint extends this functionality with ability to search SharePoint sites for sensitive data. It locates sensitive data in posted documents, Wiki entries, blogs, lists and other content, empowering administrators to quickly identify and remediate the files and data presenting the greatest risk for breaches and policy violations. The result is proactive risk management and compliance without overwhelming administrators with alerts and notifications.

**DATAGUISE**

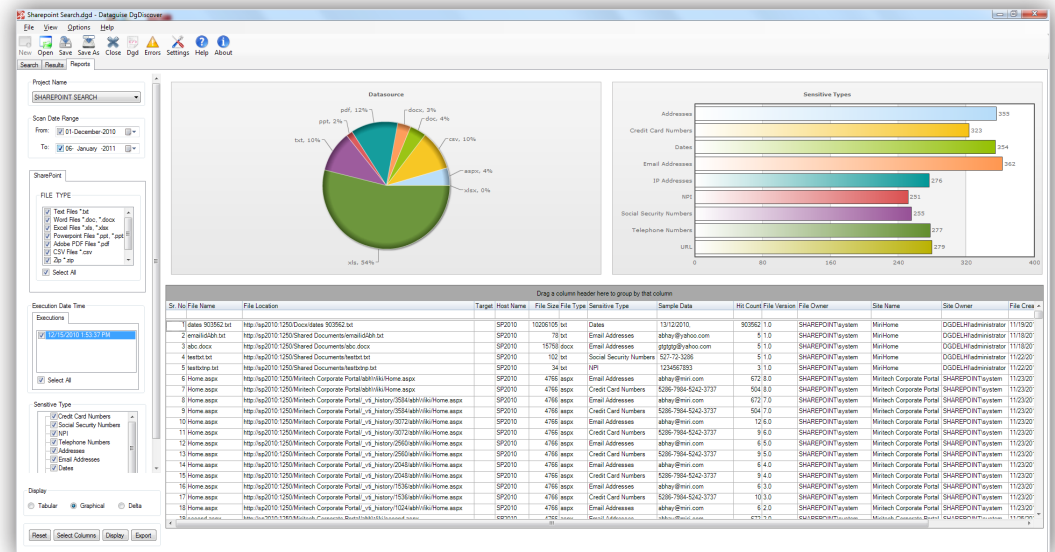
Dataguise Inc.  
2201 Walnut, Ave., Ste. 260  
Fremont, CA 94538  
P: 510.824.1036  
F: 866.384.8082  
E: sales@dataguise.com  
[www.dataguise.com](http://www.dataguise.com)

## Incremental Search and File Version Support

In SharePoint, multiple versions of a given document may be hosted on a site. Sensitive data may only reside in a subset of the versions however, since all of these versions are retrievable by users, all versions of every file must be scanned for sensitive data. DgDiscover for SharePoint addresses this challenge with an agent which periodically searches only the document versions updated since prior searches, greatly reducing the amount of processing required. The solution provides the ability to schedule these searches for off-peak times so the server load will be invisible to the user community.

### Key Features

- Searches Word, Excel, PowerPoint, Adobe PDF, CSV and text files as well as Wikis and blogs
- Searches within zip format files
- Searches for credit card numbers, social security numbers, national personal identifiers, telephone numbers, addresses, e-mail addresses, dates, IP addresses, URLs and user-defined expressions
- Can search multiple SharePoint sites on multiple servers in the enterprise
- Built-in scheduler for off-peak searching
- E-mail notification and optional lock-down of files exceeding a specified threshold of sensitive data occurrences
- Supports white listing of known safe files
- Informative, graphical reporting of search results showing file names, owners, locations and type of sensitive data found



**DgDiscover for SharePoint produces actionable reports including information such as the file name and version, the SharePoint site and location of the file, the file owner, and the type and quantity of sensitive data found in the file.**

## About Dataguise

Dataguise solutions help organizations more effectively manage their sensitive data risks while improving the efficacy of software development, test, data analysis and compliance operations. These solutions make administrators more efficient by allowing them to respond rapidly to requests for new production data sets. They improve auditor productivity by enabling them to generate reports detailing where sensitive information is maintained in the organization. Dataguise solutions provide Information Security management with actionable reports they need to understand and manage organizational data risk.



**Dataguise Inc.**  
 2201 Walnut, Ave., Ste. 260  
 Fremont, CA 94538  
 P: 510.824.1036  
 F: 866.384.8082  
 E: sales@dataguise.com  
[www.dataguise.com](http://www.dataguise.com)

Learn more about how Dataguise sensitive data protection solutions can help your organization manage sensitive data risk and address regulatory compliance requirements. Contact your Dataguise sales representative or visit our website at [www.dataguise.com](http://www.dataguise.com).