

# ADAPTIVE CONTENT INSPECTION



**VERDASYS**

## VERDASYS ADAPTIVE CONTENT INSPECTION

Verdasys' Adaptive Content Inspection extends the powerful host-based data protection capabilities of Digital Guardian through the automated discovery and classification of confidential data at rest, data in use and data in motion, providing unparalleled visibility and control over sensitive information. Through real-time policy based enforcement, organizations are able to protect private information, secure intellectual property, achieve corporate compliance and prevent data loss.

### AUTOMATED DISCOVERY

Knowing the location of sensitive data, as well as how it is used is crucial for organizations to prevent proprietary and private data loss and meet the requirements of regulations including Sarbanes-Oxley, GLBA, HIPAA, FISMA, PCI Security Standards and more. Through the established technology of Autonomy, the global leader in search engine technology, Adaptive Content Inspection applies various methods of analysis to accurately inspect the content of files, desktops, servers, emails and more, enabling flexible and customizable keyword matching, entity extraction and document similarity capabilities for more than 90 languages. By using both a full regular expression engine and query engine, Adaptive Content Inspection uses advanced custom pattern matching as well as search by keywords, word associations, soundexing, stemming and more. Adaptive Content Inspection transparently operates both background and on-demand scans across more than 300 file formats, including unstructured data such as HTML pages, word processing documents, spreadsheets and e-mail. Whether in file servers, file shares, or at the endpoint, Adaptive Content Inspection seamlessly examines the content of files finding confidential and sensitive information including:

## AUTONOMY

**"The risk posed by unauthorized distribution of data to and from an enterprise must be managed effectively. We are pleased that our products have become critical components of the Verdasys' data security solution."**

**MIKE LYNCH**  
CEO, AUTONOMY

### PERSONALLY IDENTIFIABLE INFORMATION (PII)

- Social Security Numbers
- Credit Card Numbers
- Names
- Addresses
- Phone Numbers
- Date of Birth

### INTELLECTUAL PROPERTY

- Source Code
- Product Designs
- CAD Files
- Product Roadmap
- Trade Secrets

### CONFIDENTIAL DATA

- Medical Records
- Financials
- Customer Lists
- Contracts
- Marketing Plans
- Business Plans

### ACCURATE RESULTS

Adaptive Content Inspection's world-class technology utilizes existing pre-built patterns, checksums, validated number ranges and other criteria to assure accurate results. The content is matched against both user defined content patterns and dictionaries as well as pre-built policy packs containing search criteria for common confidential and sensitive information. This secondary checking reduces the amount of false returns to less than 1%, ultimately assuring that highly sensitive data is accurately identified and protected.

## COMPREHENSIVE CLASSIFICATION

The classification of proprietary and private data is needed for accurate inventory reporting, overall data protection and performance. As Adaptive Content Inspection seamlessly scans and discovers highly sensitive information, Digital Guardian provides real-time classification of the files, tagging the documents as sensitive and creating an inventory of confidential documents and files in the organization. Pre-defined rules designate the level at which documents should be classified and ultimately the amount of protection needed. Classification rules can be as broad or specific as an organization needs, including specific classification rules based on whether documents contain intellectual property, confidential company information or personal identifying information. Once documents are classified, policies can be defined based on classification levels to control how the files are used.

## ENHANCED POLICY ENFORCEMENT

Adaptive Content Inspection works seamlessly with the powerful monitoring, control and reporting capabilities of the core Digital Guardian solution. Once sensitive data is discovered and classified, organizations can enhance corporate policies which allow the protective capabilities of Digital Guardian to focus on data most deserving of protection, resulting in finer grain controls and meeting regulatory demands for data protection while having the least impact on business processes. Based on these policies, Digital Guardian enforces sensitive data usage through a range of control options including alert, warn, prompt, encrypt, and/or block. This enables organizations to control and monitor data for accountability no matter where, how or by whom it is used.



**“We use Digital Guardian to help with IP leakage prevention, DRM, and content monitoring.”**

**GEOFF ARANOFF**  
**DIRECTOR, INFO. SECURITY**  
**BROADCOM**

### Adaptive Content Inspection

Scan Files for Sensitive Content or Existing Classification Tag

6	Lucy Kreek	5126 5194 0448 7400	Jan-09	MasterCard
7	Dwayne Kerns	5126 5194 0451 9400	Feb-09	MasterCard
8	Dante Jumper	5126 5194 0427 8810	Apr-07	VISA
9	Allen Ricardo	5126 5194 0454 9050	May-07	VISA
10	Seth Schwarz	5126 5194 0461 1230	May-08	VISA

### Classification Mechanisms

Methods for Identifying Sensitive Information

**Regular Expression Engine** identifies pre-load or custom alphanumeric entities

Technology, Inc. **Proprietary and Confidential** Information  
1

**Keyword Query Engine** identifies standard or company specific words using advanced linguistic approaches

General Procedures	
Tympanometry	92567
DDST	96110
Flex sigmoidoscopy	45330
Trigger point injection	20552

**Query Engine** uses custom dictionaries based on industry or company terminology

### Digital Guardian

User Actions Controlled Based on Content (or Context) Match

#### User Activities

Read  
 Write  
 Print  
 Move  
 Burn  
 Copy/Paste

#### Risk Appropriate Control

Log  
 Alert  
 Warn  
 Prompt  
 Encrypt  
 Mask  
 Block

## LEVERAGING CONTENT AND CONTEXT METHODOLOGY

The content monitoring capabilities of Adaptive Content Inspection act in conjunction with Digital Guardian’s proven context-based approach of protecting data at the point of use, which creates a secure virtual perimeter around all data. Certain sensitive data can be overlooked when searching for specific content alone, simply because the correct search parameters are difficult to determine. Through the classification of sensitive data based on where data comes from and/or how it is being used, sensitive data that may have been missed by content inspection will be caught and classified, resulting in ultimate data protection. By creating classification rules and policies based on both the context and content of a file, the ability to monitor and protect this data is assured. Digital Guardian has a range of options for determining context including classifying specific areas of servers, a set of user machines, a specific device or network location as sensitive.



## VERDASYS ADAPTIVE CONTENT INSPECTION

**Automated data discovery** in the content files to assure organizations know where highly sensitive data is located

**Advanced auditing** of sensitive data usage to comply with regulations such as Sarbanes-Oxley, GLBA, HIPAA, and PCI

**Unmatched multi language** support for over 90 languages including Asian character sets

**Operates transparently across more than 300 file formats** including unstructured data such as HTML pages, word processing documents, spreadsheets, and e-mail

**Enhanced query engine** support for word associations, soundexing, stemming and more

**Accurate secondary checking**, keeping returns of false positives less than 1%

**Seamlessly operates** with Digital Guardian's comprehensive monitoring, control and reporting capabilities for world-class data protection

## SYSTEM REQUIREMENTS

### Digital Guardian Server

- Windows 2003 Server
- IIS 6
- MS SQL Server 2000 - SP3a
- MS SQL Server 2005
- .Net 1.1 - SP1
- WSE 1.0 - SP1

### Digital Guardian Agent – Client Desktop

- Windows 2003
- Windows XP
- Windows 2000 Workstation - SP4

### Server Operating Systems

- Windows 2000 Server – SP4
- Windows 2003 Server

Note: Adaptive Content Inspection Requires Digital Guardian Server and Digital Guardian Agent



#### Corporate Headquarters

950 Winter Street  
Waltham, MA 02451  
info@verdasys.com  
781-788-8180

#### APAC Headquarters

Shinjuku Sky Bldg. 6F  
1-18-8 Nishi Shinjuku  
Shinjuku-ku  
Japan  
apac@verdasys.com  
+81 3 5909 1278

#### EMEA Headquarters

400 Thames Valley Park Drive  
Reading RG6 1PT  
United Kingdom  
emea@verdasys.com  
+44 118 965 3512

[www.verdasys.com](http://www.verdasys.com)