conceptSearching

The ROI of Intelligent Metadata Enabled Solutions

Information Security

Intelligent metadata enabled solutions are implemented based on Concept Searching's Smart Content Framework™. This enterprise infrastructure is based on a metadata repository where semantic metadata is automatically generated and auto-classified to one or more taxonomies.

The taxonomy component provides organizations with the ability to test, validate, and manage one or more taxonomies resulting in an intelligent metadata infrastructure that address search, compliance, information lifecycle management, sensitive information protection, migration, text analytics, and Enterprise/Web 2.0 challenges.

Enterprise Metadata Management | Search | Records Management | Compliance | Policy Enforcement | Migration
Information Governance | Data Privacy | Text Analytics | Social Networking | Cloud Computing | eDiscovery

Intelligent Metadata Enabled Solutions

The Typical Information Security Approach

Organizations are well aware of security challenges and many have very sophisticated applications to protect the organization from information security exposures. Surprisingly, many global organizations actually do not have a comprehensive documented information security strategy. With cyber security issues on the rise, although organizations may feel confident their information is protected, most likely it is not.

The issue is not in the security architecture or strategy, it is the inability to identify potential sensitive information exposures that are unknown. Sensitive information exists in documents, scanned items, faxed items, emails, and could be in any unstructured or semi-structured content. Although some security applications provide the ability to recognize industry standard descriptors such as a social security number, other sensitive and confidential information can exist that contains information the organization does not wish to share, such as financial information, new product information, pre-published stockholder information. Most exposures are caused either intentionally or unintentionally by the organization's own staff. They can prove costly, damage brand, and increase organizational risk.

The Costs
70% of all breaches were due to a mistake or malicious intent by an organization's own staff *(Ponemon Institute)*
88% of security breaches are attributed to negligence. *(Wharton Information Security Best Practices)*
Average loss of brand for a data exposure ranges from $184 million to $330+ million representing a 17% to 31% decline in market share *(Ponemon Institute)*
86% of IT security professionals said that their job would be at risk if a security incident were to occur, 24% reported that the CEOs' or other executives' confidential data had been breached. 34% reported losing data needed for compliance, while 34% stated that confidential information has been posted on a social networking site. Nearly 37% said that data has been lost by employees. *(WebSense Survey)*
Malicious insiders account for 10% of the costs associated with a cybercrime and represent 38% of the types of attacks. *(Ponemon Institute)*

The Hidden Costs of Information Security

Symantec asserted that cybercrime was costing us about $110 billion per year. McAfee stated that cybercrime was instead costing us approximately $1 trillion per year.

The Global Cost of Cyber Security

conceptSearching

The Intelligent Information Security Approach

The Concept Searching approach is fully customizable and identifies unique or industry standard descriptors. Content is automatically meta-tagged and classified to the appropriate node(s) in the taxonomy, based upon the presence of the descriptors, phrases, or keywords from within the content. Once tagged and classified, the content can be managed in accordance with regulatory or government guidelines. The identification of potential information security exposures includes the proactive identification and protection of unknown privacy exposures before they occur, as well as monitor in real time organizationally defined vocabulary and descriptors in content as it is created or ingested.

Regardless of the size of the organization or the industry, data privacy should be a high priority to ensure that content is proactively identified and protected. Whether it is an internal or external breach of confidential information, the stakes are too high not to address this issue.

The Benefits

- Reduces organizational costs associated with data exposures, remediation, litigation, and fines and sanctions
- Eliminates the risk associated with end user non-compliance issues
- Eliminates manual metadata tagging and human inconsistencies that prohibit accurate identification and protection of unknown privacy/confidential data assets
- Protects an organization by identifying and securing unknown data privacy/confidential information and preventing the portability and electronic transmission of secured assets

Intelligent Platform Components

The Concept Searching technology platform is comprised of a Service Oriented architecture (SOA) based search and classification technology, a browser based taxonomy management technology, and a tightly integrated feature set that operates with any platform. Industry unique compound term processing technology enables the rapid creation of semantic metadata, which can be classified to organizationally defined taxonomies.

The tagging and auto-classification of content can be aligned to business goals and the semantic metadata generated can be easily integrated with any third party application or platform that can interface via web services.

The Concept Searching suite of products is platform agnostic and includes conceptSearch, conceptClassifier and conceptTaxonomyManager. The Microsoft suite of products includes conceptClassifier for SharePoint and conceptClassifier for Office 365. The products use a single code base, able to be deployed in SharePoint 2007, 2010, 2013, and Office 365, providing clients with the choice of on-premise, cloud based, or hybrid environments.

conceptTaxonomyWorkflow is an add-on product, workflow product that serves as a strategic tool managing migration activities and content type application across multiple SharePoint and non-SharePoint farms and is platform agnostic. This component delivers value specifically in migration, information security, records management or any application or business process that requires workflow capabilities.

The technologies also support a variety of search solutions including Solr, Autonomy, SharePoint, Google Search Appliance, and IBM Vivisimo.

About Concept Searching

Concept Searching specializes in semantic metadata generation, auto-classification, and taxonomy management and is a Microsoft Gold ISV and Managed Partner. Concept Searching has a current Enterprise Authority to Operate (ATO) US Air Force, a current Enterprise Certificate of Networthiness (CoN) US Army, and has been deployed on the SIPR, NIPR, and DISA networks.

The technologies encompass the entire portfolio of unstructured information in on-premise, cloud, or hybrid environments. Clients are using the technologies to improve search, records management, data privacy, migration, and text analytics.

Americas
+1 703 531 8567
info-usa@conceptsearching.com

Europe
+44 (0)1438 213545
info-uk@conceptsearching.com

Canada
+1 703 531 8567
info-canada@conceptsearching.com

Australia
+61 (0)2 8006 2611
info-australia@conceptsearching.com

New Zealand
+64 (0)4 889 2867
info-nz@conceptsearching.com

Africa
+27 (0)21 712 5179
info-sa@conceptsearching.com

Marketing and PR
International: +1 703 531 8564
Europe: +44 (0)1438 213545
marketing@conceptsearching.com

Follow us on Twitter
@conceptsearch

www.conceptsearching.com