



KAZEON

Classify, Secure & Search Unstructured Documents

Discover and Classify Data

- Periodically scan and index all network file shares
- Identify all files with privacy data such as CC#, SS#, License, DoB, Customer id...
- Identify all files to be retained for compliance
- Tag files with additional metadata

Search and Report

- Generate compliance reports showing all privacy and retention exposures
- Tag files for future legal discovery
- Mine semi-structured file formats

Automated Policy Enforcement

- Copy compliance records to WORM volumes and set retention date
- Move all privacy files and metadata to encrypted storage
- Perform regular data integrity checks to detect corruptions or modifications

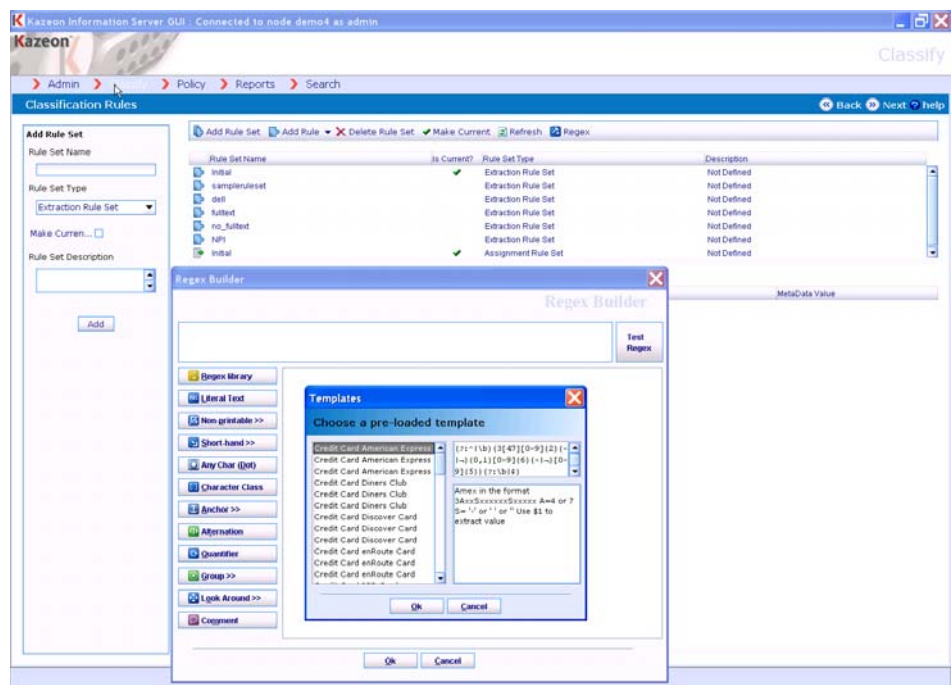
Networks today store radically more and more information (hundreds of terabytes for some large businesses) in hundreds of file types (from text to video, from spreadsheets to MP3s). This information is growing at 50 to 75% per year and is increasingly distributed across the network.

Over 80% of what's on the network is stored in individual documents, outside of databases and email - it is unstructured and unmanaged. It is essentially invisible. The sheer volume of information hampers finding the things you need. The hundreds of file formats obscure your content. It is also increasingly regulated (e.g., PCI, SOX, HIPAA, SEC).

Kazeon introduces the ability to find, classify and manage this unstructured information - building file content and metadata against existing files across your network to create an abstract for each of your unstructured documents. This enables consistent classification of documents based upon content as well as accurate application of governance policies. It is the basis for indexed searching and reporting that will help you quickly find information during e-discovery requests as well as auditing the use of your storage infrastructure by individuals and departments.

Classify & Secure Sensitive Information

When first connected to the network and thereafter on a regular basis, Kazeon takes an inventory of all enterprise file assets in a two-step process. First, Kazeon searches the network for every file and then creates a unique fingerprint for each file. This fingerprint can identify duplicate files or detect corruption of a file.



Use Kazeon to identify documents on the network containing Credit Card Numbers

Kazeon can open files and extract content, such as dates, telephone numbers, or customer IDs and will identify if users are violating data storage policies, for instance storing documents containing credit card information on an unencrypted server.

More Information:
www.re-soft.com/discovery

Kazeon also collects metadata from the file system, such as size, name, owner, path, and format. Kazeon recognizes hundreds of standard file formats, including PDF, media files, and Microsoft Office, based on the file's content, not the file extensions. The fingerprint, content, and metadata are gathered together into a single abstract that is stored in a metadata repository. "Tags" can be added to a file abstract automatically using predefined rules.

Kazeon supports a full range of archiving services required to manage corporate governance policies, optimize storage and respond to litigation. Compliance policies can be configured using the Kazeon policy engine. Policies can be set for almost any action, such as moving a file to a specific storage device based on age or file content, for example policies might state that Excel spreadsheets from the Finance department should be saved for 3 years and Word files from Legal should be stored for 10 years on a specific WORM device. When a file is archived, Kazeon tracks it with an audit trail, saving information on the file's movement over the network or within an archive.

Kazeon's search technology is fine-tuned to work with very large numbers of files. The search feature uses a familiar user interface making it possible to offer search to individual users.

The screenshot shows the Kazeon Information Server web interface. The main content area displays a report titled "Summary Coalescence Report Grouped By Document Type". The report includes a table with the following data:

File Type	Coalesced Size (MB)	Number of Duplicates	Savings	Number of Files	Total Size (MB)
	5150.52	13665	12.34 %	26485	5875.58
Microsoft Outlook PST/OST 2003	2371.31	10	2.94 %	28	2443.17
UNIX GZip	471.44	1	0.05 %	4	471.66
VVOL File	460.09	0	0.00 %	2	460.09
Unknown (ANSI 8)	293.02	254	31.41 %	2031	427.22
DLIS File	168.78	1	49.89 %	3	336.79
EBCDIC encoded Text	154.63	1	45.06 %	7	281.47
Text - 7-Bit File	125.07	583	34.87 %	1742	192.03
DVVOL File	190.54	0	0.00 %	1	190.54
MPEG Layer3 ID3 Ver 2.x	61.62	11	47.26 %	24	116.83
RAW File	92.36	0	0.00 %	3	92.36
JPG File	90.45	0	0.00 %	5	90.45
UNIX Compress	82.40	0	0.00 %	1	82.40
SD5 File	79.26	0	0.00 %	1	79.26
BAT File	62.16	9	14.63 %	67	72.81

For example, lawyers can run their own discovery searches or compliance officers can keep track of file and file content use. It can also be easily tailored to extract the unique information types created by every enterprise, for example, invoices, trade records, or contracts.

The Kazeon Information Server is remarkably easy to deploy. It comes in a plug-and-play appliance package and as a Virtual Machine server. It integrates seamlessly with the surrounding environment without changing user behavior or inserting itself into the production environment. A single Kazeon Information Server can manage millions of files. Several servers can be clustered together into a single system capable of managing hundreds of millions of files.

© Kazeon Inc.