IRI DarkShield

Unstructured Data Search & Security

- Classify and Search for Hidden PII
- Extract and Report on Values and Metadata
- Mask Simultaneously, Later, or in Batch
- Combine Multiple Functions and Formats

Discover, Deliver, and Delete PII in Dark Data Sources

Product Summary

The Dark Data Conundrum

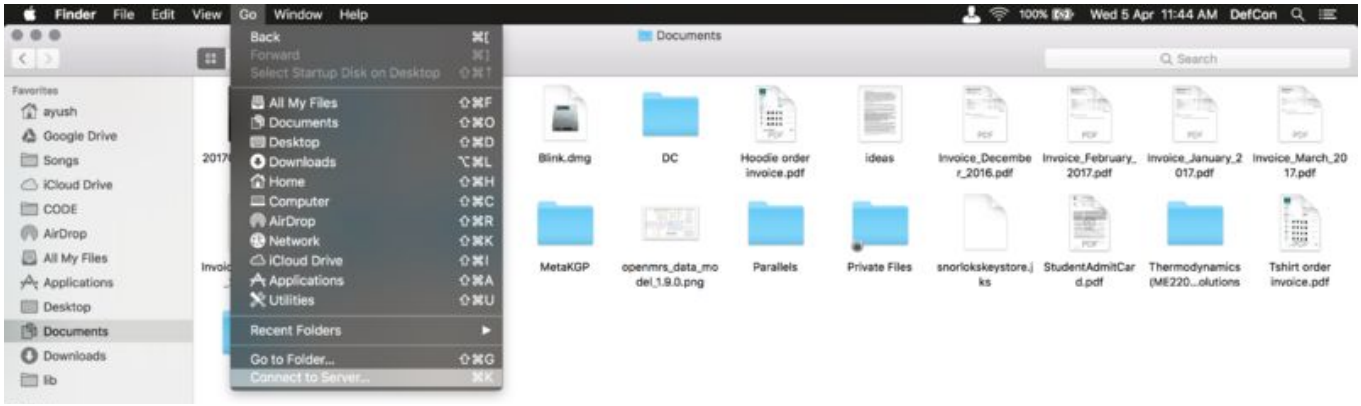
Gartner defines **dark data** as the "*information assets organizations collect, process and store during regular business activities, but generally fail to use for other purposes*" like analytics or digital business … *Organizations often retain dark data for compliance or archive retrieval. Its storage and security "typically incurs more expense (and sometimes greater risk) than value*."

Source: Gartner IT Glossary

Despite this observation, data loss prevention and the protection of personally identifiable information (PII) are critical elements of modern data governance and, in many cases, required by law. Unfortunately, safeguarding data at risk is a multifaceted problem -- especially when the data is hidden -- requires:

1) Knowledge of business and regulatory requirements,
2) Classification of sensitive data and its authorized recipients, and
3) The implementation of policies and techniques that support these requirements and protect PII.

PII search, remediation, and reporting techniques are particularly challenging to implement in dark data environments due to the volume, variety, and unstructured nature of the data sources in them.



Enter DarkShield Version 3

IRI DarkShield supports the risk and controls framework in enterprise IT environments by classifying, finding, extracting, masking, and reporting on PII and other data 'hidden' in unstructured sources.

DarkShield quickly and effectively scans supported file and NoSQL DB formats for PII in local or SMB drives or folders, plus Amazon S3. It searches everything for strings in PII data classes that match:

1) values stored in a lookup table;
2) named 'path' or column filters for JSON, XML, CSV, Excel
3) stored or new Java Regex patterns;
4) drawn (bounding box) regions in images;
5) machine-learned named entities in a trained Natural Language Processing (NLP) model; or.
6) facial recognition in images.

Whenever DarkShield finds a match, it applies the masking function you assigned to a "rule matcher" that you previously defined. In this way, you affix masking rules to data meeting specific search criteria. DarkShield can also auto-detect faces, and recognize those you train in a model, in order to mask them.

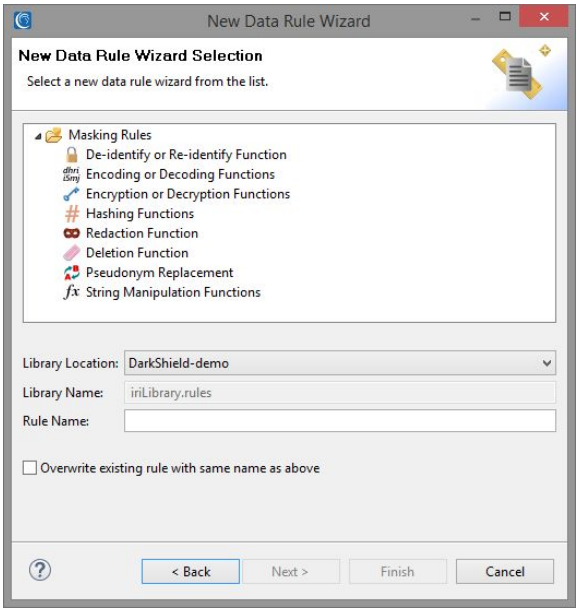
Searching and masking operations can be combined or performed separately, either in a wizard or via serialized (automated, batch) job. DarkShield can also extract the search results and attendant metadata to a delimited log file ready for audit queries, data delivery (per GDPR portability provisions), and graphs.

DarkShield Masking Functions

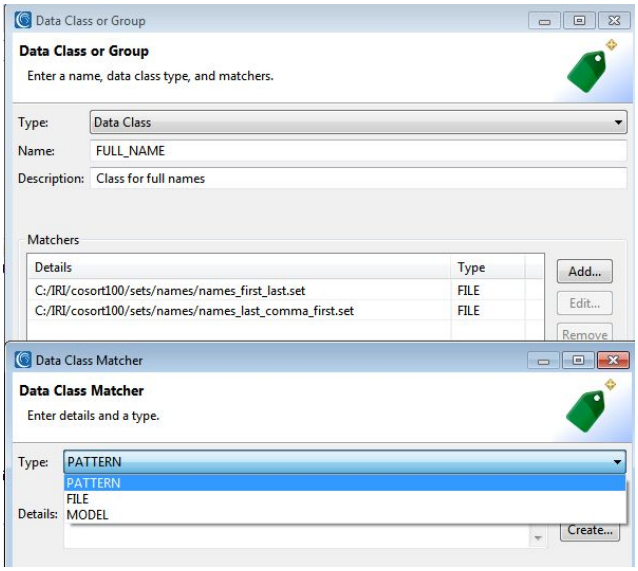
DarkShield users can employ many of the same static data masking functions that IRI FieldShield does to secure PII in DB and flat-file columns.

Commonly used DarkShield functions include:

- Format-preserving (or not) encryption
- Lookup pseudonymization
- Redaction / obfuscation
- String manipulation
- Deletion / erasure
- Bit scrambling
- Encoding
- Hashing



The masking rule you match to each data class should depend on the desired results for the ciphertext; i.e., whether they can be reversed, how they appear (conform to format constraints), and if they must be unique values. DarkShield can replace existing or create new files in current or cloned folder structures.



DarkShield Business Benefits

Only DarkShield supports the combination and automation of the difficult but necessary processes of data discovery, extraction, redaction, and audit reporting across multiple file formats and locations. Multiple search methods and threads are deployed in conjunction with multiple masking functions.

All of this optimization and consolidation speeds compliance efforts and document management systems testing.

DarkShield also:

- helps GDPR data collectors and processors comply with data portability and right-to-be-forgotten provisions.
- operates in the same free Eclipse™ job design and metadata environment, IRI Workbench, with many other data governance and management functions.
- licenses affordably licensed standalone, in a bundle with other IRI Data Protector suite products, or for free inside IRI Voracity total data management platform subscriptions.

Supported Approaches and Data Sources

IRI DarkShield
Unstructured Data Search & Security

Architecture

Front-Ends

IRI Workbench
Built on Eclipse™

Command Line
For App Calls, Requires JRE

Back-End

Search Matcher

- **Data Rule** — Masking Functions
- **Data Class** — Search Methods

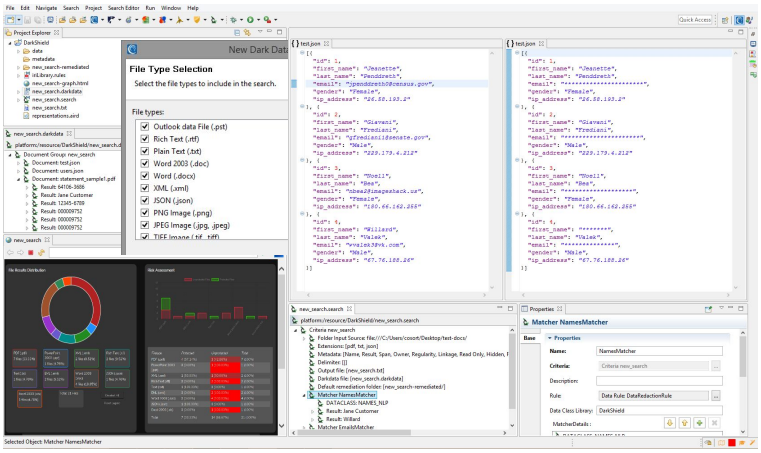
SortCL Program

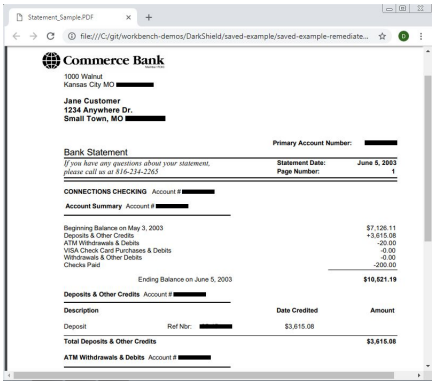
- IRI CoSort
- IRI FieldShield
- IRI DarkShield
- IRI NextForm
- IRI RowGen

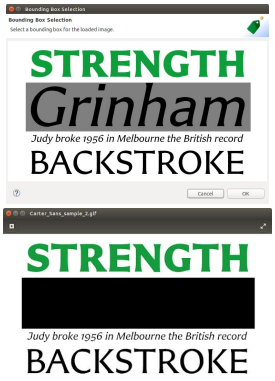
Supported File Types (V3)

Text	Documents	Images
asc	doc/x	png
txt	ppt/x	jpg/x/2
html & eml	pdf	bmp
json & xml	xls/x (CellShield)	gif
hl7 & x12	rtf (scan only)	tif/f

*Excel data can also be masked with IRI CellShield







DarkShield v4 will find and mask PII in more cloud platforms, HDFS, and industry-specific file formats

Compatible Platforms and Applications

DarkShield runs on Windows, Linux, and MacOS (Sierra) platforms, but it can also reach files in any operating system drive mounted or connected through SMB.

DarkShield uses the same IRI Workbench front-end, data classes, and masking functions as:

- IRI FieldShield - DB and flat-file masking
- IRI CellShield - Excel spreadsheet masking
- IRI CoSort - Data transformation and reporting
- IRI Voracity - Big data integration, test data, etc.

IRI DarkShield
Unstructured Data Search & Security

IRI
Total Data Management

2194 Highway A1A
Melbourne, FL 32937 USA
1.321.777.8889 * 1.800.333.SORT

iri.com/darkshield