IRI DarkShield

Unstructured Data Search & Security

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

Discover, De-Identify, and Deliver PII in Dark Data Sources

Product Summary

The Dark Data Conundrum

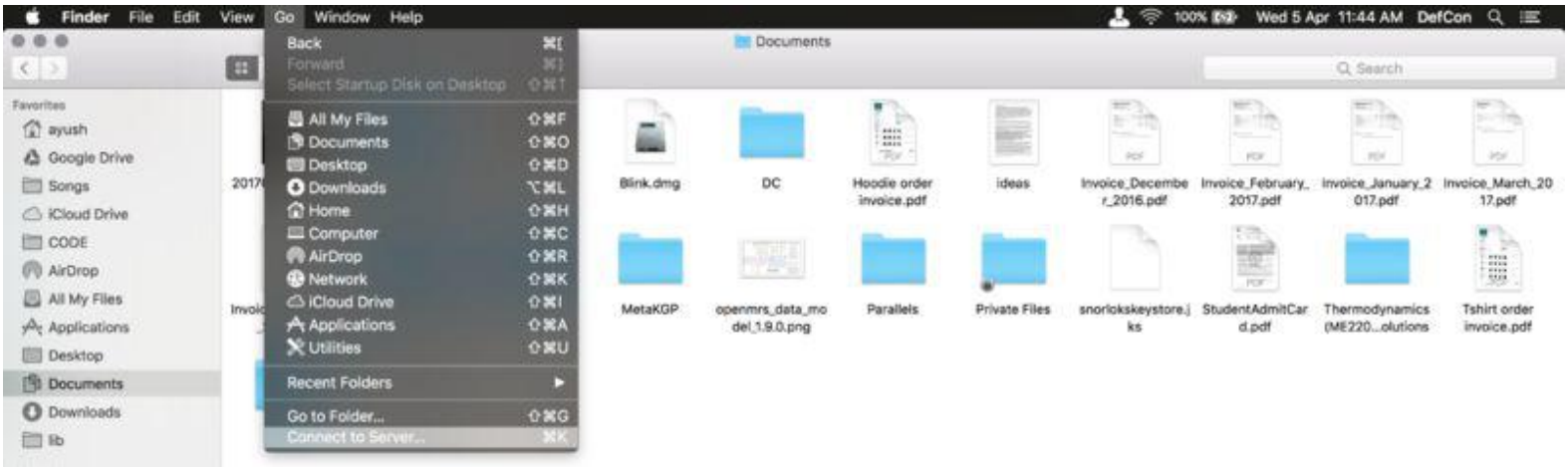
Gartner defines **dark data** as the "*information assets organizations collect, process and store during regular business activities, but generally fail to use for other purposes*" like analytics or digital business … *Organizations often retain dark data for compliance or archive retrieval. Its storage 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 which 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.



What Does IRI DarkShield Do?

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 all the supported file formats for dark data in one or more network-connected drives or folders. It searches every file in them for strings in PII classes that match:

1) stored or new Java Regex patterns;
2) values stored in a lookup table; or,
3) machine-learned named entities in a Natural Language Processing (NLP) model.

Whenever DarkShield finds a match, it applies the masking function you assigned to the “rule matcher” that you previously defined to map your search criteria to data masking rules.

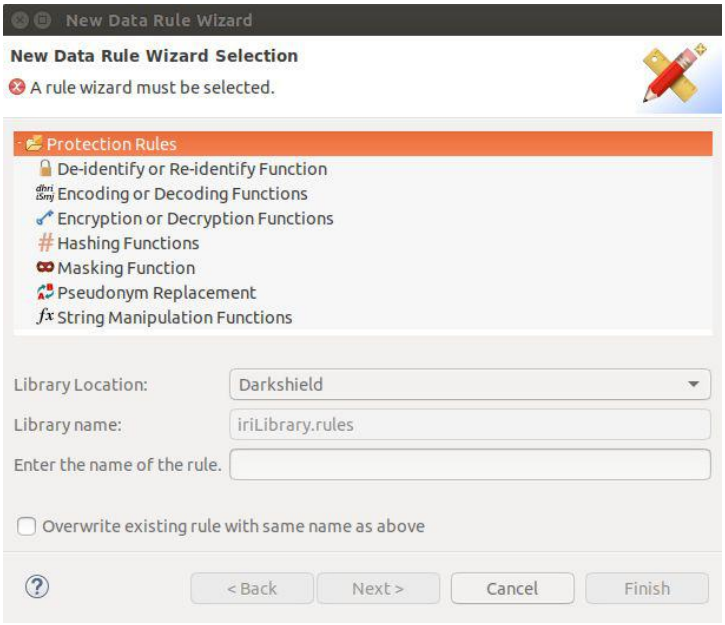
Searching and masking operations can be combined or performed separately, either in a wizard or serialized (automated, batch) job. DarkShield can also extract the search results and attendant metadata to a delimited log file ready for audit queries, data delivery (per GDPR portability provisions), and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

DarkShield Masking Functions

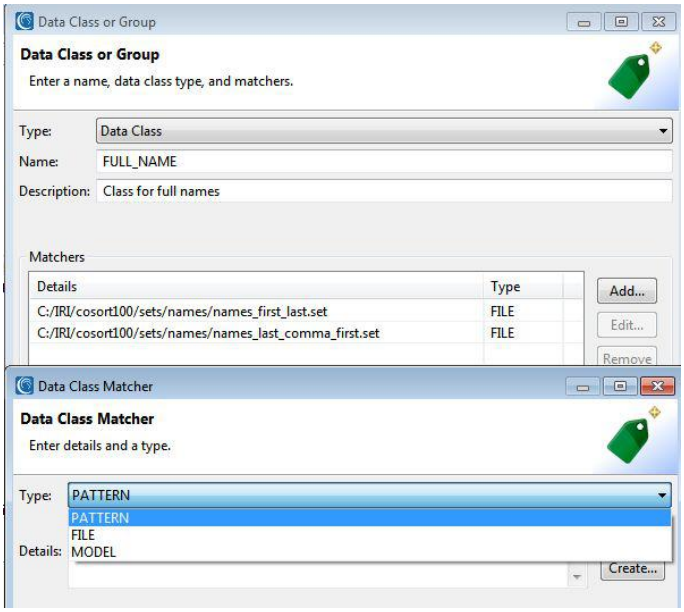
DarkShield users can use many of the same static data masking functions that IRI FieldShield uses to secure PII in DB and flat file columns.

Commonly used DarkShield functions include:

- Format-preserving (or not) encryption
- Lookup pseudonymization
- Redaction / obfuscation
- String manipulation
- 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

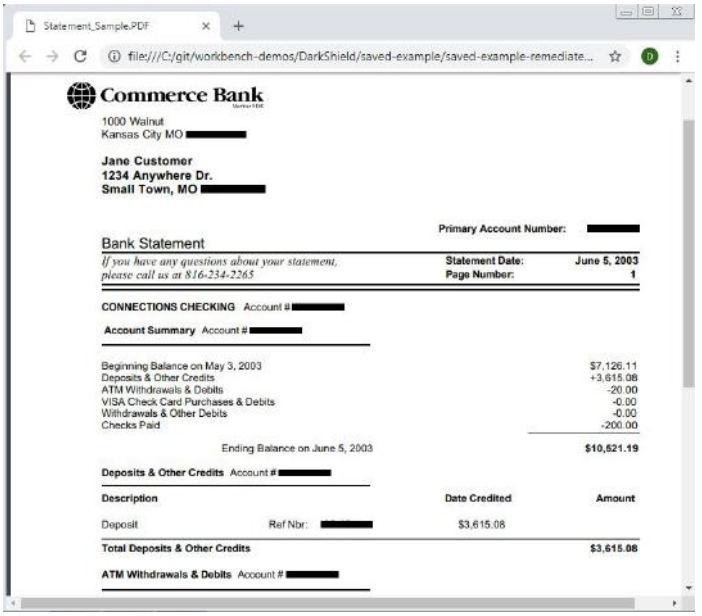
Only DarkShield supports the combination and automation of the difficult but necessary processes of data discovery, extraction, redaction, and audit reporting across multiple file formats and locations. Multiple search methods and threads are deployed in conjunction with multiple masking functions.

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

DarkShield also supports compliance with GDPR data portability and right-to-be-forgotten provisions.

DarkShield operates in the same Eclipse™ job design and metadata environment, IRI Workbench, with many other data governance and management functions. The product is also affordable and can be licensed standalone, in a bundle with other IRI Data Protector suite products, or for free within a subscription to the IRI total data management platform, Voracity.

Supported Data Sources


Statement_Sample.PDF

Commerce Bank

1000 Walnut
Kansas City MO [redacted]

Jane Customer
1234 Anywhere Dr.
Small Town, MO [redacted]

Primary Account Number: [redacted]

Bank Statement

If you have any questions about your statement, please call us at 816-234-2265

Statement Date: June 5, 2003
Page Number: 1

CONNECTIONS CHECKING Account # [redacted]

Account Summary Account # [redacted]

Beginning Balance on May 3, 2003	$7,126.11
Deposits & Other Credits	+3,615.08
ATM Withdrawals & Debits	-20.00
VISA Check Card Purchases & Debits	-0.00
Withdrawals & Other Debits	-0.00
Checks Paid	-200.00
Ending Balance on June 5, 2003	$10,521.19

Deposits & Other Credits Account # [redacted]

Description		Date Credited	Amount
Deposit	Ref Nbr: [redacted]	$3,615.08	
Total Deposits & Other Credits			$3,615.08

ATM Withdrawals & Debits Account # [redacted]

*Excel data is masked with IRI CellShield

In Development

DarkShield can find PII in .DOC/X, .PPT/X, .OST, and .PST files. It will soon be able to automatically mask this data, too. DarkShield v3 will find and mask PII in image and A/V files.

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 engines as:

- IRI FieldShield - DB and Flat File Masking
- IRI CellShield - Excel Spreadsheet Masking
- IRI Voracity - Big Data Management, ETL, etc.
- IRI CoSort - Data Transformation and Reporting

IRI DarkShield
Unstructured Data Search & Security

IRI
Total Data Management

CELEBRATING 40 YEARS 2018
The CoSort Company

2194 Highway A1A, 3rd Floor
Melbourne, FL 32937 USA
1.321.777.8889 * 1.800.333.SORT

WWW.IRI.COM