IRI
Total Data Management

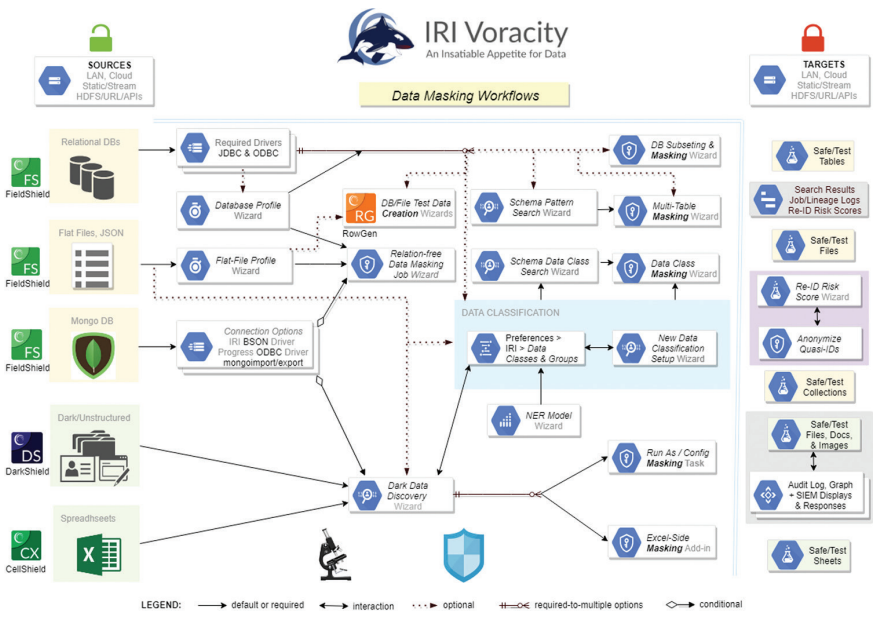
Discover, Classify and Mask PII in Structured and Unstructured Sources

In the last issue of *CyberSecurity Sourcebook*, IRI defined the term 'Startpoint Security' to encompass nine data-centric security concepts:

1. Permission & Disclosure—authorizing you to store submitted PII via user agreement
2. Discovery & Classification—finding and cataloging PII to find and mask it consistently
3. Data Masking—de-identifying PII via encryption, redaction, pseudonymization, etc.
4. IAM & RBAC—managing access to sources, (un)masking jobs, programs, and logs
5. Data & Metadata Lineage—saving and analyzing changes to data and masking jobs
6. Latency—architecting, configuring and running static or dynamic data masking jobs
7. Risk Scoring—measuring the statistical likelihood of re-identification (e.g., for HIPAA & FERPA)
8. Audit Logs—seeing or querying who did what, and who saw what, when, and where
9. Assessment & Insurance—conducting expert procedural, statistical, and legal reviews

These activities can complement and be used in conjunction with end-point security approaches to harden vulnerable data targets against hackers, insider threats or breaches, and to comply with both U.S. and international data privacy laws.

IRI currently offers three interrelated data masking products that satisfy the bulk of these requirements based on the data sources involved:



- **FieldShield**—RDB tables and flat files/streams, plus MongoDB and JSON sources
- **CellShield EE**—MS Excel spreadsheets 2010 and later, in local/LAN/cloud folders
- **DarkShield**—unstructured text files, documents and image files in several formats and locations

All, plus RowGen for test data creation, are front-ended in the same Eclipse IDE called IRI Workbench, and all their search results and masking logs can be exported to SIEM tools like Splunk Enterprise Security.

The schematic above diagrams the typical flow of activity through these products and serves as a how-to template for solution design and implementation.

These products also belong to the IRI Data Protector suite, and are included components of the IRI Voracity data management platform. You can find Voracity in recent DBTA special reports and buyers' guides covering big data, data integration and governance, data lakes, and cybersecurity, or at iri.com/voracity.

If you would like a white paper on the case for data masking, or require information on the IRI technology or services that drive these results, see iri.com/solutions/data-masking or contact info@iri.com. ■

IRI, THE COSORT COMPANY
www.iri.com
+1.321.777.8889
info@iri.com