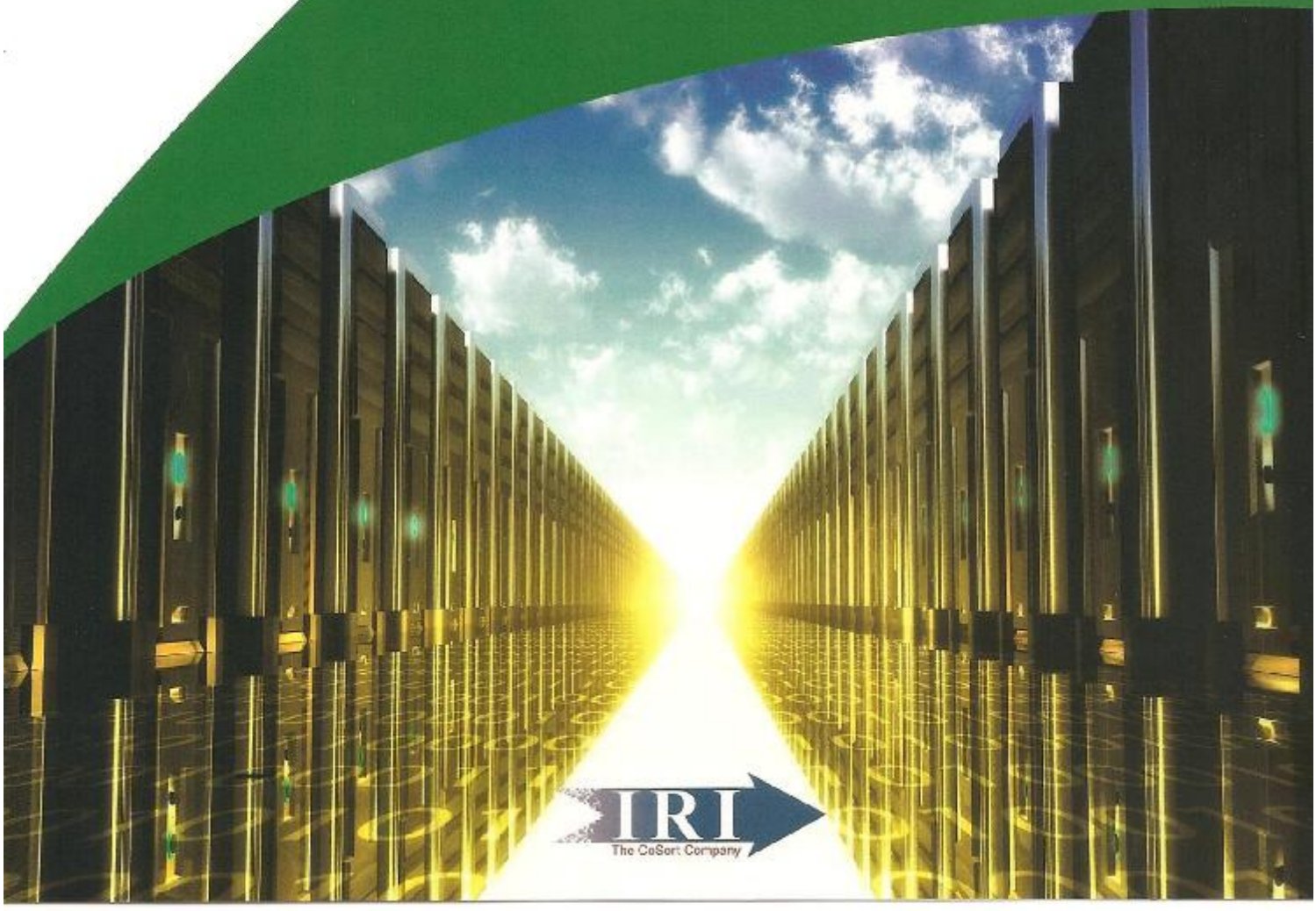
FieldShield

Targeted Data Security Functions

Product Summary

Protection Functions for Sensitive Data

- Field-Level Encryption
- De-ID and Pseudonymization
- Data Masking & Redaction
- Compliance Audit Logging



What Does FieldShield Do?

Data loss prevention and the protection of sensitive information are critical elements of modern data governance. Protecting data at risk is a multifaceted problem that requires: 1) knowledge of business and regulatory requirements, 2) identification of sensitive data and its authorized recipients, and 3) implementation of policies and techniques that support these requirements.

FieldShield® is designed to support the risk and controls framework in corporate and government IT environments with sensitive data in flat files and relational database tables. FieldShield quickly and effectively protects sensitive data in these repositories - down to the field level - before that data leave the firewall. FieldShield can safeguard:

- **Personally Identifiable Information (PII)** which can be used to uniquely identify, contact, or locate a single person, or can be used with other sources to identify an individual.
- **Protected Health Information (PHI)** which is any information in a medical record or a designated record set that can be used to identify an individual, and was created, used, or disclosed in the course of providing a health care service.
- **Payment Card Industry Data (PCI)** which is used to process credit card payments, and is thus subject to fraud, hacking and other threats.

FieldShield makes sensitive fields private by encrypting, masking, or removing them based on business rules.

How Does FieldShield Work?

FieldShield allows you to define a specific protection method for each field, or group of fields, within sequential files and relational database tables. With FieldShield, you can:

- Encrypt with built-in AES-256 libraries
- Filter input fields or redact records
- Mask via anonymization or obfuscation
- Mask via pseudonymization or de-identification
- Invoke custom protection methods

FieldShield uses the same data definition and manipulation language as CoSort's widely used SortCL program to define protections and output formats. Each field name and its attributes can be coupled with an encryption routine, masking method, de-identification code, pseudonymous lookup value, or custom security function that you write. The protection can even be conditioned upon specific attributes or ranges within the data.

FieldShield job scripts can be run on the command line, and from within batch and application programs. An XML audit log with all job parameters and runtime details is provided to show the data protections applied, helping to verify compliance with data privacy regulations. A Graphical User Interface (GUI) is in development.

Encryption and Decryption Options

Among the many data-centric privacy protections that FieldShield offers is a choice of different encryption and decryption routines:

- **Standard AES-256 -** Expanded ciphertext fields are displayed as printable ASCII characters
- **GPG/PGP -** Compatible with GPG key ring management, the input format is not retained
- **Width-Preserving -** The original field width, but not the original data format, is retained
- **Format-Preserving -** The original width and alpha-numeric field (column) format is retained
- **Custom Algorithms -** OpenSSL or any function you write or link to is supported at the field level

Symmetric encryption keys can be held within job scripts as passphrases or environment variables, embedded in secured files (on secured servers), or remain invisible (by default). Assymetric (public) encryption and (private) decryption keys can be stored in central key ring servers. HSM support is in development.

What are the Advantages of FieldShield?

Though many physical and broad-brush logical security solutions are available, the wrong design or execution choice reduces efficiency and leaves data vulnerable to privacy breaches. By contrast, FieldShield delivers:

- **Specificity** - secures sensitive data by applying discrete protection functions to individual fields.
- **Efficiency** - field-only encryption is fast, and leaves remaining data open for further processing.
- **Flexibility** - supports the selective application of data protection functions on a conditional basis.
- **Safety** - supports different security functions or encryption keys for each field.
- **Simplicity** - one job script for multiple protections; one output for multiple recipients.
- **Clarity** - uses self-documenting 4GL to define file layouts and field protections.
- **Particularity** - targets unique field disclosures for differently-authorized recipients in the same pass.

What are the Business Benefits of FieldShield?

FieldShield helps CISOs and compliance officers follow both business rules and privacy laws in a data-centric context. With FieldShield, data are protected at the field level. Some fields will remain clear while others will be secured with one or more user-specified functions. There are several benefits to this approach:

- Data are protected at sources and endpoints across multiple flat-file formats and database platforms.
- Protected data can retain realism (for testing and sharing).
- Appropriate protections can be assigned to each data element and each recipient.
- Data stays safe even if stolen, or if a laptop or network is decrypted.
- A query-ready XML audit log helps to verify compliance with data privacy regulations.
- Simple job scripts save development and maintenance time.
- 4GL job scripts are simpler to implement than DB-specific column encryption methods.
- Single job scripts and executions produce single targets that can be safely distributed to multiple recipients with different authorizations. Similarly, multiple instances of the same field - each protected with a different function or encryption key - can be created. These features save additional passes across the data, and prevent data synchronization errors.

Which Applications are Compatible?

FieldShield runs on Unix, Linux, and Windows platforms, and operates on file formats common to all of them, as well as on some mainframe file formats. FieldShield uses the same metadata as:

- CoSort for data transformation and reporting
- RowGen for realistic test data generation
- NextForm for file and data type conversion
- Fast Extract (FACT) for Oracle, DB2, et al.

FieldShield's data definition file (.ddf) format is interchangeable with all IRI products, and is also supported in Meta Integration Technology (MITI)'s Meta Integration Model Bridge (MIMB) suite. MIMB support for IRI's .ddf format facilitates the conversion of third-party ETL, BI, and modeling tool metadata into FieldShield metadata. This allows FieldShield to re-use those data layouts, and protect the sensitive data in those applications sooner.

Data & File Sources

- ASCII, EBCDIC, COBOL and C (binary) forms
- European, ISO, Japanese & U.S. Timestamps
- IP Addresses, Whole Numbers
- Bulk RDBMS Unloads - via Fast Extract (FACT)
- ODBC-connected Database Tables
- ACUCOBOL-GT (Vision) Indexed Files
- IBM Unblocked Variable Record Format
- LDIF (LDAP), Microsoft CSV, Flat XML
- Micro Focus Variable Length & I-SAM Files
- Sequential Flat Files (Line, Record, Variable)
- Fixed Block File Format
- VSAM - via Clerity Mainframe Re-hosting
- W3C Common & Extended Log (Web)
- Unicode and Native Multi-Byte Character Sets

Compatible Products

- CoSort - Data Transformation & Reporting
- FACT - Fast Extract for Oracle and DB2
- MIMB - Meta Integration Model Bridge
- NextForm - File and Data Type Conversion
- RapidACE - 3D Data Model Integration
- RowGen - Referentially Correct Test Data

Supported Platforms

- UNIX (AIX, HP-UX, Solaris, Tru64 & more)
- Linux on x86, Itanium, IBM x/p/i/z; FreeBSD
- Windows® (XP, 2000/2003/2008, Vista, 7)

IRI, The CoSort Company
2194 Highway A1A, Suite 303
Melbourne, FL 32937 USA

1.321.777.8889
1.800.333.SORT

info@iri.com
www.iri.com