IRI FieldShield
PII / PHI Classification & Masking

- Descubre, clasifica, aplica reglas especializadas en Información de Identificación Personal (PII)
- Cifra, seudomiza, redacta…
- Cumple con HIPAA, PCI, GDPR…
- Registra, Integra, comparte y asegura trabajos

Des-identificación de datos sensitivos

Resumen del producto

La prevención de pérdida de información confidencial y la protección de la misma, son elementos críticos de la administración moderna de los activos digitales. La protección de datos en riesgo es un problema multifacético que requiere: 1) conocimiento de los requisitos comerciales y regulatorios, 2) clasificación de datos sensitivos y sus destinatarios autorizados, y 3) implementación de políticas y técnicas que soporten estos requisitos.

¿Qué hace FieldShield ?

IRI FieldShield es compatible con el marco de riesgos y controles en entornos de TI corporativos y gubernamentales, al encontrar y enmascarar datos confidenciales en tablas de bases de datos relacionales, archivos planos y muchas otras fuentes de datos convencionales ("legacy") o de última generación. FieldShield camufla los datos de forma rápida y efectiva en estos repositorios, hasta el nivel de campo, antes de que sean utilizadas por grupos de pruebas, desarrolladores o compartidas con terceros. FieldShield puede asegurar:

- **Información de identificación personal (PII)** que revela a alguien directamente, o en combinación con otros datos.
- **Información de salud protegida (PHI, por sus siglas en inglés)** que identifica a una persona de un registro médico o un conjunto de registros designado que se creó, utilizó o divulgó en el curso de la prestación de un servicio de atención médica.
- **Información de la industria de tarjetas de pago (PCI),** que es generada al realizar pagos con tarjeta de crédito, dado que por su valor está sujeta a piratería, fraude, etc.

FieldShield cifra, enmascara o anonimiza estos datos de acuerdo con las normas comerciales y las leyes de privacidad.

¿Cómo trabaja FieldShield?

FieldShield localiza y clasifica PII, PHI o PCI en diferentes fuentes con herramientas integradas de clasificación y perfil de datos. Fieldshield asigna protecciones específicas para des-identificar cada elemento:

- Cifrar con bibliotecas incorporadas o propias
- Filtrar o enmascarar valores, columnas o filas de acuerdo a condiciones que se definan
- Enmascar a través de alteración o manipulación de cadenas de caracteres
- Seudomizar (Separar información original) valores "hash", intercalar o generar valores aleatorios

Los trabajos de FieldShield se ejecutan en el entorno gráfico denominado "IRI Workbench GUI" o desde la línea de comandos o desde programas de aplicaciones. Para preservar la integridad referencial, puede asegurar columnas similares en varias tablas a través de una sola acción, usando las funciones de enmascaramiento que se definen o importan desde una biblioteca de reglas. Un registro de auditoría XML con todos los detalles de trabajo y tiempo de ejecución muestra las protecciones de datos aplicadas para verificar el cumplimiento con las regulaciones de privacidad de datos.

También puede usar las funciones de cifrado, algoritmos hash o funciones diseñadas por el usuario para realizar enmascaramiento dinámico de datos, Hadoop. El componente de desarrollo de software (SDK) de FieldShield soporta y documenta las llamadas de APIs en C / C ++, Java y .NET.

Opciones de cifrado y descifrado

Entre las muchas funciones de protección centradas en los datos de FieldShield, se encuentran las poderosas rutinas de cifrado y descifrado, mencionadas a continuación:

- **AES-128 o 256**: muestra los campos de texto cifrado expandidos como caracteres ASCII imprimibles
- **3DES**: Utiliza archivos de claves públicas
- **GPG / PGP**: funciona con la administración del conjunto de claves GPG y no conserva el formato de entrada
- **OpenSSL**: se ajusta al estándar de seguridad informática FIPS 140-2
- **Conservar formato**: conserva el ancho original y el formato del campo alfanumérico (columna)
- **Conservación de ancho**: conserva el ancho del campo original, pero no el formato de datos original
- **Algoritmos personalizados**: admite cualquier función que escriba o enlace que proteja los datos en ese campo.

Las claves de cifrado simétricas pueden: 1) Mantenerse dentro de los scripts de trabajo como frases de contraseña o variables de entorno; 2) Incrustarse en archivos protegidos (en servidores seguros); o, 3) Permanecer invisibles (por defecto).

Almacene el cifrado (público) asimétrico y las claves de descifrado (privado) en los servidores centrales de conjuntos de claves. Obtenga soporte de HSM a través del desarrollo personalizado.

Ejecutar FieldShield en entornos de base de datos

FieldShield se conecta a los datos de la base de datos en reposo o en movimiento, y ejecuta:

- En la línea de comando o en procesamiento por lotes
- Desde la interfaz gráfica de usuario de Eclipse: IRI Workbench
- A través de un sistema, o una llamada a la API desde un programa C ++, Java o .NET
- In situ, a través de procedimientos SQL utilizando una biblioteca personalizada.

¿Cuáles son las ventajas técnicas de FieldShield?

Aunque existen muchas soluciones de seguridad lógica y física de amplio alcance, la elección incorrecta de diseño o ejecución reduce el rendimiento y deja los datos vulnerables a las violaciones de la privacidad. Por el contrario, FieldShield entrega:

- Eficiencia: acelera la protección apuntando solo a datos confidenciales
- Simplicidad: solo requiere un trabajo para múltiples protecciones y destinatarios
- Seguridad: Soporta diferentes funciones de seguridad o claves de cifrado para cada campo
- Flexibilidad: permite enmascarar y desenmascarar según los valores de datos o la autorización
- Claridad: utiliza una GUI de Eclipse familiar y 4GL auto-documentada para definir diseños de datos y funciones de protección.

¿Cuáles son los beneficios comerciales de FieldShield?

FieldShield ayuda a que los CDO y los CISO se adhieran tanto a las reglas comerciales como a las leyes de privacidad en un contexto centrado en los datos. Algunos campos permanecen en claro, mientras que otros son asegurados. Con FieldShield:

- La PII es encontrada automáticamente (o manualmente) y clasificada
- Los datos son protegidos en las fuentes y destinos con múltiples funciones
- Los datos se mantienen seguros incluso si son robados, o si una computadora portátil o una red es descifrada
- Los datos protegidos pueden retener realismo para las pruebas, el intercambio y el subconjunto de bases de datos
- La implementación y el mantenimiento son más fáciles que el cifrado de una columna específica de BD.
- Un log de auditoria a través de una consulta disponible XML ayuda a verificar el cumplimiento de las regulaciones de la privacidad de la información.

En una sola ejecución, FieldShield puede producir uno o más recipientes destinos con diferentes autorizaciones. A través del entorno GUI de protección de múltiples tablas se enmascaran de igual forma las columnas comunes. Esto evita realizar muchos procesos sobre los datos, previene errores de sincronización de datos y preserva la integridad referencial.

¿Cuáles son algunas fuentes de datos que protege FieldShield?

Estándard

- CVS
- Delimitado
- Formato de archivo de bloqueo fijo
- LDIF
- Línea, Registro, Variable Secuencial
- Longitud Variable de Micro Focus & ISAM
- RDBMS (Oracle, DB2, MySQL, SQL Server, PostgreSQL, Sybase, Teradata)
- Text
- XML

Legado

- Adabas
- C-ISAM Informix, D-ISAM
- Datacom
- DataFlex
- dBase
- IDMS
- IMS
- Intersystems
- PostgresSQL
- Unidata

Moderno

- Amazon EMR, RDS, etc.
- Cloudera CDH & Impala
- Hortonworks Hive
- MapR Hive
- MS SQL Azure
- NoSQL (Cassandra & MongoDB)
- Pivotal (Greenplum, Hive)
- Spark SQL
- Web-based (Eloqua, Hubspot, Marketo, SalesForce, etc.)

¿Qué aplicaciones son compatibles con FieldShield?

FieldShield se ejecuta en UNIX, Linux y Windows, y opera en las bases de datos y formatos de archivo que soportan además las plataformas de mainframe, Hadoop, NoSQL y SaaS. FieldShield usa los mismos metadatos que:

- AnalytiX DS - Gestor de mapas
- IRI CellShield - Enmascaramiento de datos para Excel
- IRI CoSort - Integración y transformación de datos
- IRI FACT- Extracto rápido para Oracle, DB2, y otros
- IRI NextForm - Conversión de datos y bases de datos
- IRI RowGen - Generación de datos de prueba realistas
- Voracidad IRI - Gestión total de datos
- MITI - Meta modelo de integración de puente

El formato del archivo de definición de datos (.ddf) de FieldShield es intercambiable con todos los productos IRI y es compatible con los centros de intercambio de metadatos más populares. Facilitan la conversión de metadatos de herramientas ETL, BI y de modelado de terceros en metadatos de FieldShield para que pueda proteger con mayor rapidez los datos confidenciales en esos entornos.

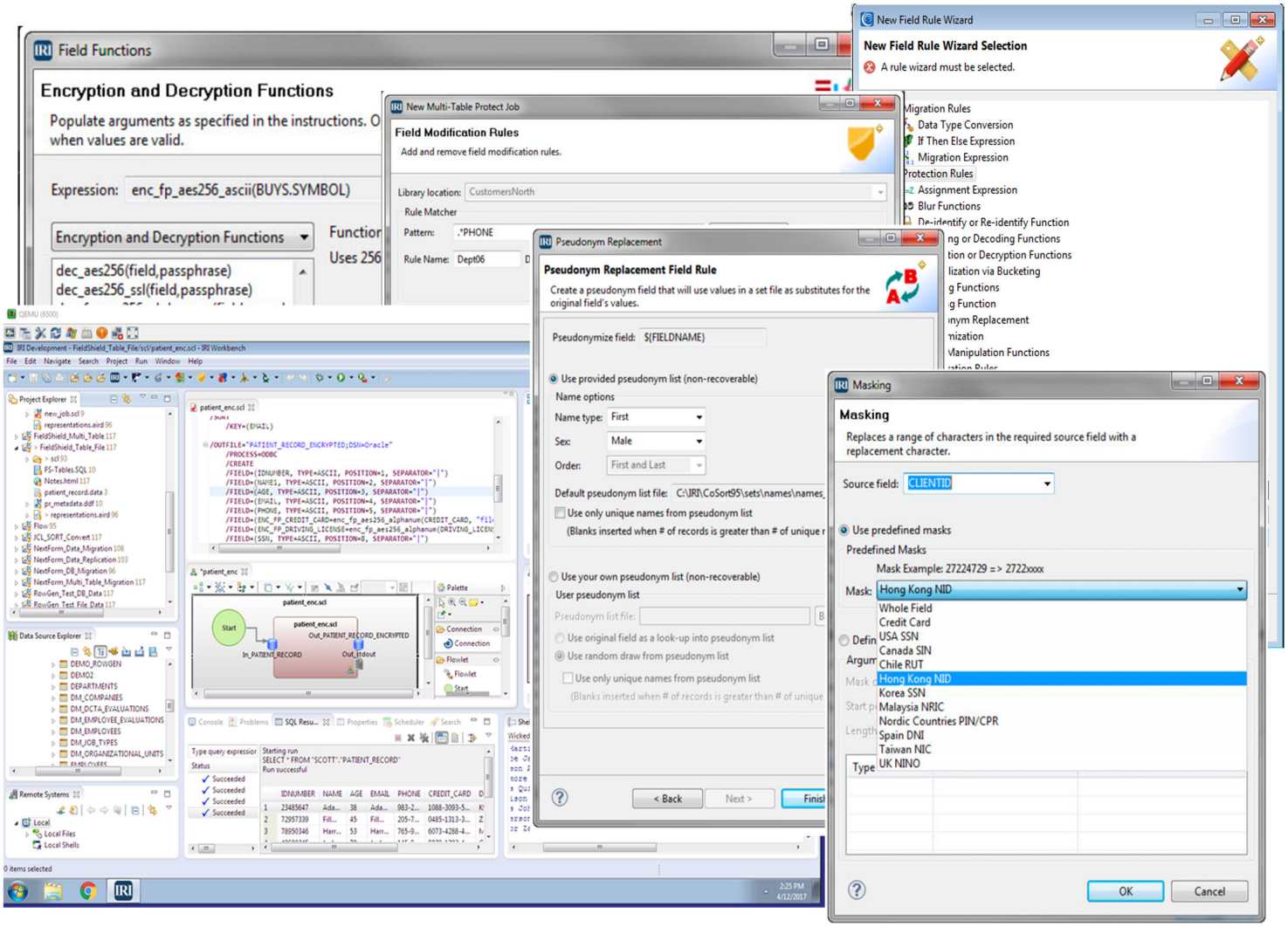
Plataformas compatibles con FieldShield

- UNIX (AIX, HP-UX, Solaris, Tru64 & mas)
- Linux on x86, Itanium, IBM s/p/i/z, FreeBSD
- Windows® (XP, 2000-2016, 7, 8, 10)
- MacOS (Sierra)

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

FieldShield en el IRI Workbench

Los usuarios de FieldShield obtienen un complemento Eclipse gratuito para crear, ejecutar y administrar trabajos de protección de datos. La GUI soporta nueve de las doce categorías de funciones de protección de FieldShield. El editor de diseño de campo de salida controla el formato de cada objetivo.



555 Winderley Place, Suite 300
Maitland, Florida 32751
(786) 206.6512
info@greenlt.com www.greenlt.com

Total Data Management

CELEBRATING 40 YEARS 2018
The CoSort Company