Assure Encryption

Protect IBM i data privacy and achieve compliance

Customers, business partners and employees trust you to protect their confidential information from unauthorized access and theft. Any breach of that data would negatively impact relationships and your business' reputation.

In addition to preventing theft of data by criminal intruders, internal staff, contractors and business partners should only be allowed to see the specific data to which they are authorized.

In fact, industry and state regulations such as PCI-DSS, HIPAA, GDPR and more mandate encryption of personally identifiable information (PII), payment card information (PCI) and personal health information (PHI).

In addition to data encryption, tokenization may also be used to replace sensitive data with replacement (token) values. Tokenization removes sensitive data from the production server, removing that server from the scope of compliance.

Assure Encryption, a feature of Assure Security and part of the Assure Data Privacy feature bundle, is trusted by organizations worldwide to protect their private data. It encrypts data anywhere it resides on the IBM i, including database fields, backup tapes, Save files, IFS files and more. The solution is optimized for performance and is the only NIST-validated AES database encryption solution for IBM i. Built-in masking, logging, and tokenization capabilities make Assure Encryption the clear choice for privacy of IBM i data at rest.

Benefits

- Encrypts data such as credit card numbers, bank account information, salary data, birth dates and other personally identifiable information instantly without impacting applications
- Greatly reduces compliance exposure by replacing sensitive data with tokens that have similar characteristics but no value
- Protects your organization's intellectual property and the data of customers, partners and employees from theft
- Meets or exceeds the data privacy requirements of GDPR, PCI-DSS, HIPAA, GLBA/FFIEC and other regulations for protecting data at rest
- Ensures sensitive data in databases, spool files, IFS and backup tapes is encrypted using best practice
- Ensures encryption keys will be properly managed and secured to avoid encryption breaches

Strong, Automatic Encryption

Version 7.1 of the IBM i OS introduced a column-level API called FIELDPROC. This Db2 feature calls an exit program for each database insert, read or update, allowing for those programs to perform encryption, decryption, tokenization, masking and more.

Assure Encryption uses FIELDPROC to automatically encrypt data in Db2 columns without requiring application changes. Its high-performance encryption libraries are validated by the National Institute of Standards and Technology (NIST) to meet the 256-bit AES encryption standard. Assure Encryption is the only NIST-certified AES encryption solution for IBM i.

Commands are also available to encrypt backup tapes, Save files, IFS files and more.

Supported Fields and Applications - Assure Encryption supports a variety of data types including character, zoned, packed, binary, hex and more. Double-byte character sets may also be used.

Legacy RPG and COBOL applications as well as SQL applications are supported by Assure Encryption. ILE and OPM applications will work well with FIELDPROC encryption.

Command and API Integration - Assure Encryption provides a complete set of APIs for securing data in individual fields in your database, or you can use SQL views and triggers for encryption tasks. Assure Encryption APIs integrate with IBM i OPM and ILE applications built with RPG, Cobol, and other languages.

Assure Encryption also provides a command level interface for starting and stopping FIELDPROC control and for performing FIELDPROC key change operations.

Key Management

While encryption algorithms are public information, encryption keys are secret and must be protected from loss and theft. Robust key management is a critical part of any data protection strategy and is required by industry and state regulations. Storing encryption keys locally on the same IBM i partition with the data will not meet compliance requirements.

Assure Encryption integrates seamlessly with Townsend Security's Alliance Key Manager, a FIPS 140-2 compliant key management solution. Other OASIS KMIP-compliant key managers are also supported to enable use of a common key manager across multiple platforms and encryption solutions.

Access Control and Masking

Because automatic decryption works for all users and applications, Assure Security enables administrators to define which users can view unencrypted data, which users can only view masked data (first 6, last 4, etc.), and which users are not allowed to view the information. User controls are based on user and group profiles. A default user and masking policy can also be defined.

Assure Encryption administrators can also define which applications can access data using context sensitive controls. For example, Bill in HR may be allowed to view social security numbers using JD Edwards but not to transfer the file to his PC using FTP.

Tokenization

Assure Security also provides tokenization to replace sensitive data with tokens that have similar characteristics but no value. Tokenization maintains the data relationships in applications while eliminating sensitive data from production, test, or QA environments. The result is a much smaller target for data thieves.

Over 20 different field types such as credit card, driver's license, zip code and more are supported for tokenization. Tokens can be either recoverable, where the original data is stored in an independent and encrypted repository for retrieval, or non-recoverable for permanent anonymization.

Compliance Logging

Comprehensive logging of encryption and tokenization activities is performed to ensure full auditability of data access.