syncsort

PRODUCT SHEET

Assure Monitoring and Reporting

Powerful Auditing of IBM i System and Database Activity

In response to today's world of complex regulatory requirements and evolving security threats, you need a simple way to monitor all IBM i system and database activity, quickly identify deviations from compliance or security best practices, and maintain an audit trail to satisfy security officers and auditors.

Assure Monitoring and Reporting, a feature of Assure Security, and part of its Assure Compliance Monitoring feature bundle, comprehensively monitors system and database activity to save you time and money on achieving regulatory compliance, identifying compliance deviations and detecting unauthorized activities on IBM i systems. Assure Monitoring and Reporting produces clear, concise, easy-to-read reports based on system activity and database changes recorded in journals – the only source of audit information accepted by IBM i security and audit professionals. Best of all, no application modifications are required.

Reports can be ad hoc, or they can be scheduled and emailed automatically to the people who need them. Assure Monitoring and Reporting can optionally integrate with a SIEM console for monitoring database events, system events or system information alongside other enterprise systems.

Assure Monitoring and Reporting is comprised of two modules, the System Module and the Database Module, which can operate independently or together. Assure Monitoring and Reporting's System Module comprehensively monitors your system to report on changes to system objects, access attempts, powerful user activity, command line activity, access to sensitive data, and more. The Database Module produces reports and alerts for any database activity on the IBM i. Static system data sources are also analyzed to identify possible deviations from best practice.

No environment is too small or too large and complex to benefit from the power and flexibility that Assure Monitoring and Reporting delivers for monitoring and reporting on IBM i security and compliance.

Benefits

- Simplifies the process of analyzing complex journals
- Reduces the time and expense required to achieve regulatory compliance with GDPR, SOX, PCI DSS, HIPAA and others
- Comprehensively monitors system and database activity
- Quickly identifies security incidents and compliance deviations when they occur
- Satisfies requirements for a journal-based audit trail
- Supports segregation of duties and enforces the independence of auditors

How Assure Monitoring and Reporting Works

Assure Monitoring and Reporting's goal is to extract only pertinent data from journals so that administrators can focus on relevant information. Once journals are registered with Assure Monitoring and Reporting, a field repository is generated to allow journal entries to be analyzed and fields to be selected for auditing. Based on the repository, queries can be defined that will generate audit reports.

Both Assure Monitoring and Reporting's Database Module and System Module use queries to define and generate a report. A query specifies details such as:

- The information source (database journal, system journal or system information)
- Analysis rules and report type that define exactly what to audit and include in the report
- Report format
- Report detail level and presentation rules
- Report distribution mode (email, IFS or SIEM message)
- The destination or list of users who will receive the generated report

When a query is run, a process is launched that analyzes the journal entries or the system information, extracts the information corresponding to the analysis rules, generates an audit report with the formatted analysis results and distributes it.

Reports can be run continuously, on a schedule or on-demand. Continuous mode informs you in real time of events as they arise and is useful for quickly identifying malicious actions or harmful defects.

With Assure Monitoring and Reporting, you can easily produce reports on activities such as:

- File accesses outside business hours
- Accesses to sensitive database fields such as bank account or credit card numbers
- Changes to a field that exceed a limit, such as a change of more than 10% to a credit limit
- All accesses from a specific IP address, port, job or user
- Command line activity for powerful users (*ALLOBJ, *SECADM)
- Changes to system objects such as system values, user profiles, and authorization lists
- Attempts to sign into a specific account or access a specific object
- Actions on a sensitive spool file, such as display or deletion of the payroll spool file
- Object transfers to production libraries and IFS directories

Key Features

- Easy to install and set up
- Requires no application modifications
- Makes no impact on applications
- Compatible with high availability solutions
- Audits both system and database activity
- Analyzes any type of journal entry, including QAUDJRN, QACGJRN, QZMF, user entries, and more
- Examines static sources such as QSYS.LIB or IFS objects, profiles, system values, authorization lists, commands, jobs, spool files and more
- Provides a powerful query engine with extensive filtering
- Generates reports and alerts continuously, on a schedule or on-demand
- Provides pre-defined audit reports for common ERP applications
- Comes with an out-of-the-box model for assessing GDPR compliance
- Produces reports in PDF, XLS, CSV and PF formats
- Supports distribution of reports via SMTP, FTP or the IFS
- Allows customization of PDF reports to add logos, highlight changes, and more
- Offers event notifications or alerts via e-mail, popup or syslog
- Optionally integrates with leading SIEM consoles

syncsort