syncsort

PRODUCT SHEET

Assure System Access Manager

Take Control of Access to IBM i Systems and Data

The days when the IBM i was an isolated platform communicating through proprietary protocols are gone. Modern IBM i systems are highly connected through standard network and open-source protocols. This opens a wide variety of access points to the worldwide hacker community, who recognize the high value of data residing on an IBM i.

Assure System Access Manager, a feature of Assure Security and part of its Assure Access Control feature bundle, is a true global access control platform with a flexible, powerful, data-centric approach to securing access to your IBM i. Using IBM i exit point technology, Assure System Access Manager gives you control of a wide range of system and data access points, including:

- Network protocols such as FTP, ODBC, DDM, DRDA, NetServer and Telnet
- SQL statements such as STRSQL, RUNSQLSTM, RUNSQL, *EDRSQL and embedded SQL
- CQE usage such as RUNQRY, WRKQRY, QQQQry and OPNQRYF
- File opens using QSH, STRSQL, DSPPFM, UPDDTA and others
- System and user commands issued from a 5250 session or remotely
- Sockets
- Jobs
- And more

Benefits

- Supports regulatory requirements for SOX, GDPR, PCI-DSS, HIPAA, and others
- Significantly reduces the time and cost of achieving regulatory compliance
- Satisfies security officers by securing access to IBM i systems and data
- Enables implementation of security best practices
- Quickly detects security incidents so you can efficiently remediate them

How Assure System Access Manager Works

Assure System Access Manager primarily uses exit point technology to detect access attempts to your IBM i systems and data, determine whether to accept or deny them, and optionally log those decisions and trigger actions.

Assure System Access Manager's exit point programs are driven by precise and powerful rules defined for each access point. Rules contain information that allows the program to know:

- When the rule applies to an access event
- Whether to accept or deny the access
- Whether to log the event
- Whether an optional action should be launched for the event, such as executing a command, disabling a user profile, sending a message, writing a record in a log file or executing a program

With Assure System Access Manager, you can specify conditions for whether access is accepted or denied based on parameters such as date, time, user profile setting, IP address and more. If no rule is found for the access event, a default access decision, log decision and action can be defined.

With Assure System Access Manager, you can block:

- Any open session requests – not just Telnet
- Specific SQL statements based on precise selection criteria
- File accesses outside of normal application programs
- Specific commands issued after business hours
- Copying or saving files outside of normal procedures

You can also perform actions such as:

- Restricting activity of *SECADM users to certain system values
- Alerting and auditing *CMD when users receive *ALLOBJ authority
- Forcing users to qualify files on commands such as UPDDTA or CRTDUPOBJ
- Restricting users to specific files for UPDDTA

Key Features

- Secures systems and data with powerful, flexible data-centric rules that are easy to maintain
- Offers an extensive vocabulary for access rule definitions
- Includes a standard access control model
- Provides simulation and learning modes to enable non-disruptive rules testing
- Allows rules to be updated without a service outage
- Has very low impact on system performance, particularly with high-volume ODBC/JDBC applications
- Provides an easy, intuitive graphical interface for managing day-to-day operations
- Controls all traditional access points such as FTP, ODBC, DDM, DRDA, Netserver, TELNET, etc.
- Controls all user or system commands
- Initiates actions either before or after execution of user and system commands
- Monitors CPU consumption and automatically regulates job priority for SQL queries
- Offers a large choice of actions, including alerts via e-mail, popup or syslog
- Produces reports in PDF, XLS and CSV formats
- Logs data that can be forwarded to a SIEM console

syncsort