cilasoft

PREVENT FRAUD
& COMPLY WITH
INDUSTRY REGULATIONS

CONTROLER

THE SOLUTION FOR GLOBAL ACCESS CONTROL ON THE IBM i

Introduced in 2003, CONTROLER was created to meet the access-control needs of IBM i clients who could not find a satisfactory solution with other products. CONTROLER was developed as a global-access control product to secure any type of accesses to the IBM i and ensure data is highly secured.

Today, companies all over the world have chosen CONTROLER thanks to its technological superiority and its unique approach to security, especially as a means for companies to comply with regulations such as Sarbanes-Oxley (SOX), Basel II, PCI-DSS, HIPAA and other compliance laws.

DESCRIPTION

CONTROLER is a global access control product that complements IBM i OS security, either in classic mode or by using adopted authorities.

CONTROLER not only covers exit points using all the traditional access methods, such as FTP, ODBC, DDM, DRDA, Netserver, etc. but also all system or user commands (whether issued remotely or directly from a 5250 interface), jobs, SQL instructions from the SQE engine, and files invoked by the CQE engine and file opening.

The product includes two modules, which can be used separately or concurrently: Access Protocol Control module and Command Control module.

Examples of access controls you can implement with the **Access Protocol Control** module:

* Block all authentication protocols using one powerful, easy-to-maintain rule
* Block «open session request» (not TELNET) according to specific criteria
* Install generic controls on remote commands issued from users who do not normally have command-line access
* Strengthen security for generic users

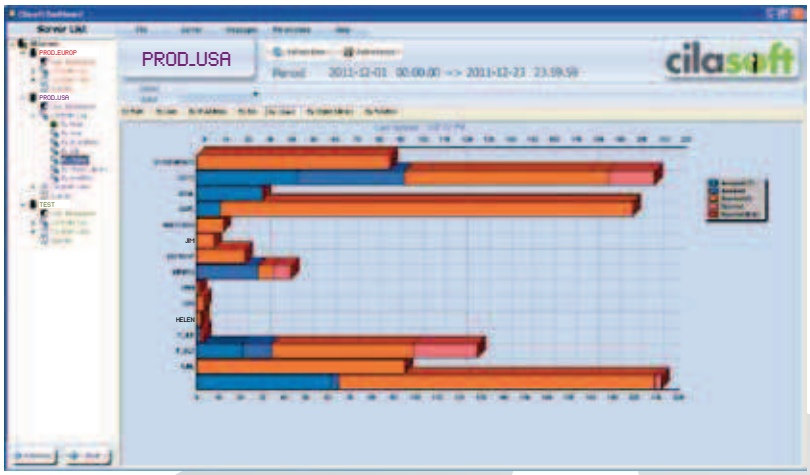
POWERFUL AND LOW IMPACT

Examples of access controls you can implement with the **Command Control** module:

* Block access and/or send alerts when users try to open a spooled file they do not own and that is part of a sensitive element list based on file name and/or author (even if users have *SPLCTL authority)
* Restrict authority of *SECADM users to only allow changing specific system values
* Force users to qualify files while using specific commands; i.e.: UPDDTA or CRTDUPOBJ from the command line
* Block copying or saving of sensitive save files outside of normal operating procedures

Advanced Business Partner IBM

CONTROLER



“Manage access control rules through a single interface with powerful and flexible settings. It’s easy to use for day-to-day operations.”

KEY FEATURES

* Controls all traditional access points (**FTP, ODBC, DDM, DRDA, TELNET, NetServer**, etc)
* Controls all user or system **commands**
* Identifies and blocks the **opening of critical files** outside of applications
* Manages the **SQL engine** (CQE & SQE) in different ways, including a blocking mode for the SQE engine
* Identifies **CPU consumption for SQL queries** and then adjusts job priority if usage exceeds preset limits
* Manages any starting or ending **job**, and any job in JOBQ status
* Ensures **very low impact** on system performance
* Provides an **extensive vocabulary** for rule definitions
* Includes **simulation and learning modes** allowing you to test your rules before putting into your live environment
* **Secures your data** (not the access route) by using powerful, easy-to-understand rules
* Allows for setting **actions** and **alerts** via e-mail, popup, syslog, command, program, journal, file, swap, etc.
* Produces reports in many different **formats (XLS, CSV, PDF,** etc)
* Includes a standard off-the-shelf **access-control model**
* And many other useful features

BENEFITS

* Reduce significantly the time and associated costs required to achieve regulatory compliance
* Record as well as act rapidly and effectively on security incidents
* Deter fraudulent activity while encouraging security best practices

cilasoft

www.cilasoft.com

ZI Les Iles, 190 route des Sarves
74370 Metz-Tessy (Annecy) - France
Tel: +33 4 50 69 45 98 - Fax: +33 4 50 69 45 99
E-mail: contact@cilasoft.com

GLOBAL AUDIT
& SECURITY SUITE FOR IBM i

QJRN/400
System
& Database
Auditing

DVM
Audit
Read Access

EAM
Authority
Management