

CONTROLLER

YOUR System i PROTECTOR



CONTROLLER offers
a complete solution to protecting
Corporate Data
that includes controlling
external access to the System i,
OS/400 commands
as well as SQL statements.

■ COMPLIANCE

International regulations including SOX, HIPAA, BASEL II, PCI, 21-CFR increasingly demand that firms maintain the security and integrity of Corporate Data.

■ FRAUD, SABOTAGE AND DISCLOSURE

60% of malicious acts are perpetrated by internal elements in a company.
In most cases these acts go undetected.

■ INTERNAL AUDIT

ISO 17799 establishes strict guidelines in terms of legal conformity, control audits, and internal controls.
Auditors today, are requiring companies to demonstrate and validate their level of conformity.

■ AUTOMATING THE PROCESS OF COMPLIANCY

Maintaining compliance is a costly endeavour for companies.
CONTROLLER can significantly reduce the number of man-days required for supporting the compliance program by automating the process of monitoring and reporting on all critical events.

Legislations concerning internal control (Sarbanes-Oxley, HIPAA, Basel II, C-198, PCI, 21-CFR, laws against money laundering, ...) are getting tougher and hold directors and administrators of financial organizations and quoted companies directly and criminally responsible if they have not set up a structure for securing and auditing their information system.

The QJRN/400 and CONTROLER Security Suite offers you a comprehensive solution to fulfil these audit requirements.

CONTROLER helps you meet the Control Objectives of COBIT in terms of system and data access security.

CONTEXT

System i servers are well-known for being reliable and secure.

If OS security is the principal method used to protect the server against non authorized access, you will also have to:

- Protect against the use of dangerous commands
- Block additional server access paths left open by standard System i security
- Audit and control the overall traffic across the server
- Control of generic profiles
- ...

Moreover, if you want to manage a high level of confidentiality for strategic and sensitive data (HIPAA), OS security is not enough in these cases, additional protection to System i security is required:

- To be confident users can only access data by authorized and secured programs
- To control the use of profiles with extensive authority.

MAIN FEATURES

CONTROLER is made up of 3 modules included in a single platform:

► **Network Access Control (Exit Points)**

By using IBM Exit Points, CONTROLER has the ability to control external access to the System i: TELNET, IFS, ODBC, FTP, DDM...

Access via other non IBM Middleware can also be controlled by this platform.

► **Command Control**

Any OS command can be monitored depending on the using context (User, IP Address, Call Stack,...), and also the parameters, in both 5250 or Remote mode.

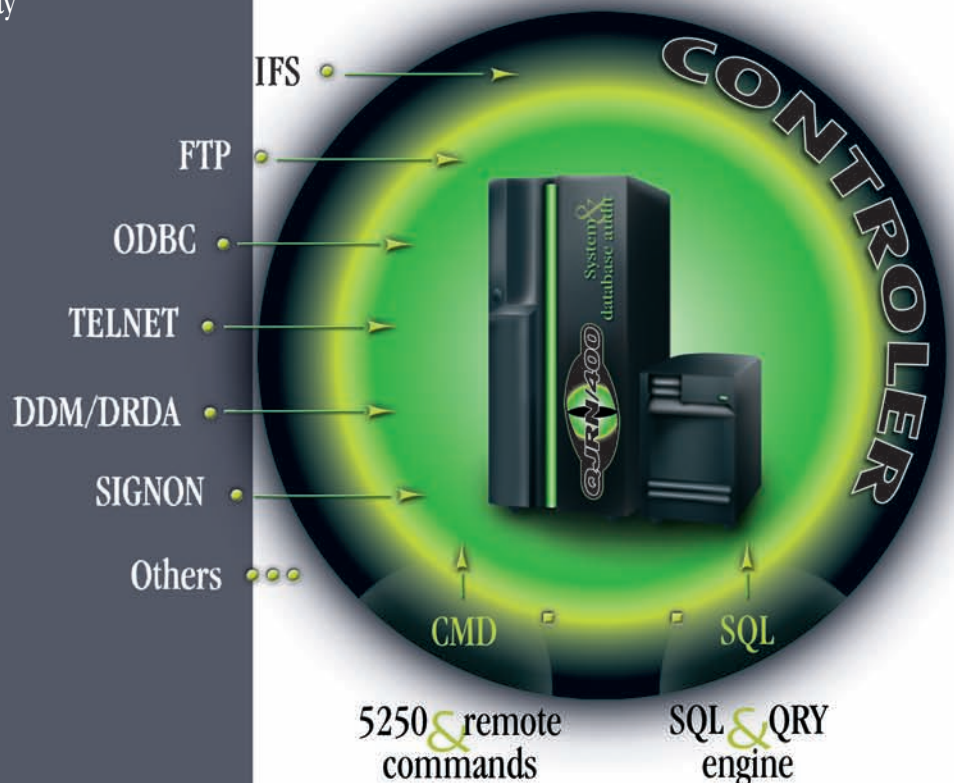
► **Audit of SQL & QRY Engine**

In terms of confidentiality, it is important to be informed about the information details read while running SQL and QUERY statements.

The **CONTROLER** engine is based on control rules: The rules provide (variable) filter options using a very rich vocabulary for each property: User, Library/File, Access Type, IP Address, Job, IFS link, IASP etc.

A group of lists containing value combinations is the decision centre: lists can be easily modified automatically by log analysis. Daily use of the software allows the processing of the log.

In the control process, **CONTROLER** is used as an extension to the OS security. It has the ability to limit access to profiles with extensive authority, protect secured objects by classic methods (Authorization Lists, Public and Private Authority, ...) or by using adopted authority.

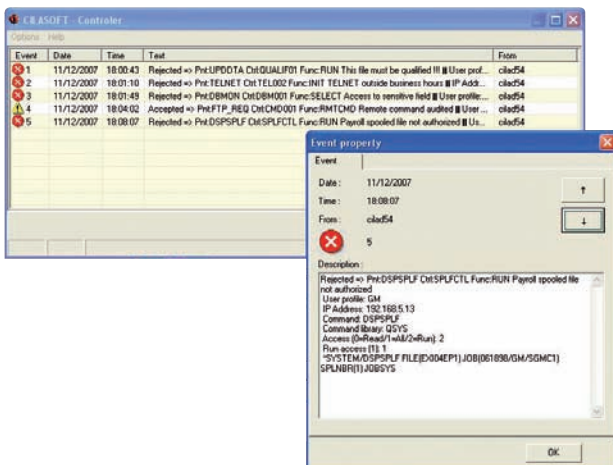


TECHNICAL BENEFITS

The initial design of CONTROLER focused on developing a universal solution to managing an increasing number of exit points. The latest release of the technology offers a tightly integrated solution for companies whilst offering much better performance compared to other third party products.

Primary Benefits:

- ▶ **Virtually No Impact on Performance**
- ▶ Third Party Exit Program Hosting
- ▶ **Real Time Update of Parameter Modifications**
- ▶ Emergency Suspension
- ▶ Qualification of All Objects
- ▶ IP Address Available For All Controls
- ▶ Independence Between Rules and Values
- ▶ **Rules are not Redundant**
- ▶ Rich and Adaptable Vocabulary Used in Rules
- ▶ **Learning Mode from logged events and Simulation Mode**
- ▶ **Generates an action whether the event is authorized or denied** (messages, profile swap, record in a journal or file, run a command, Popup alerts or Syslog)
- ▶ **Rules Inversion: Works in Black or White Lists**
- ▶ Consolidation of events from several System i servers on a single Syslog console



Two client components provide the ability to centralise alerts in the Windows environment: Popup messages or via the Event Log. Event logging gives CONTROLER the ability to interface with network security consoles.

STANDARD CONFIGURATION TEMPLATES

The Cilasoft CONTROLER is delivered with an extensive Rules Library which allows companies to develop a complete access control policy with only minor adjustments.

If necessary however, it is possible to rewrite the settings of the control engine entirely to adapt it to your security policy. Additional models are available for the main ERPs on the market.

The standard model delivered is based on the White List principle for network access. The rules can be set according to user profile, group profile, supplemental groups, or all three simultaneously. By default, any access is refused and logged. It provides for example:

▶ STANDARD CONTROLS:

- Log of any connection outside business hours.
- Log of standard profiles and profiles with extensive authority.

▶ TELNET:

- Authorise connections according to combinations of IP Address Range/ Device Name.

▶ FTP and ODBC:

- Automatic detection of DB2 or IFS codification.
- Authorise combinations User / Library / Object Name / Type of Access.

There are two types of authorization: without leaving a trace in the log, or by leaving a trace in the log for the events you consider sensitive.

▶ Remote command (FTP, ODBC, DDM):

- Authorise combinations User / Command / Parameter Value (with or without log).

▶ IFS:

- Authorise external access depending on the user, access type and path.
- Control 5250 access (WRKLNK) according to the same rules.

▶ DFU:

- Obligation to qualify the file library.
- Authorise DFU on test libraries.
- Authorise only some profiles to production libraries, it is recorded in the log and an email is sent to the ISSM.

▶ SQL:

- For all jobs running a SQL query on sensitive files, all the statements run are logged. An email is sent to the ISSM for updating queries (UPDATE, DELETE).

▶ DRDA:

- All SQL queries can be logged.



STANDARD FEATURES

- Standard Delivery of Customizable Models of Controls
- Complete Deployment in Days, not weeks!
- Real time updates of controls without restarting associated servers
- Minimal Impact on Performance
- Includes Learning and Simulator Modes
- Adapts from small-sized to large companies: from 100 to over 8,000 users. More than 50 partitions. Manages IASP.
- Unique platform for all controls
- Easy Management of Rules



ADDED VALUE

- Additional level of security lowering the risk of fraudulent activity
- Highly automated, CONTROLER secures your system 24 hours a day, 7 days a week
- Rapid return on investment by reducing the on-going cost of compliancy



CONTROLER and **QJRN/400** are products designed and developed by



Z.I. des Iles • 190, route des Sarves
74370 METZ TESSY
FRANCE
Tel.: +33 4 50 69 45 98
Fax: +33 4 50 69 45 99
Email: contact@cilasoft.com
Web: <http://www.cilasoft.com>

■ DATABASE and SYSTEM AUDITING

CONTROLER can be integrated with our **QJRN/400** software to build **a complete audit and security solution:** a single platform for managing user access and detailed monitoring of all events.



CONTROL WHAT'S GOING ON INSIDE!

YOUR CONTACT