

CONTROLER,

LE GARDIEN DE VOTRE System i



CONTROLER protège vos données, quel que soit le moyen d'y accéder : il surveille et contrôle les accès externes à votre System i, mais aussi toutes les commandes OS/400 et les instructions SQL.

■ CONFORMITÉ

La réglementation internationale (SOX, HIPAA, BALE II, PCI, 21-CFR) impose aux sociétés de garantir la sécurité et l'intégrité de leurs données.

■ FRAUDE, SABOTAGE & DIVULGATION

Plus de 60% des actes de malveillance sont perpétrés par des éléments internes à l'entreprise. Ils restent inexplicables dans la plupart des cas.

■ AUDIT INTERNE

Pour valider les procédures de contrôle interne réglementaires, les auditeurs demandent aujourd'hui la mise en place d'outils pour automatiser un processus d'audit continu.

■ SÉCURITÉ

Le contrôle de l'utilisation des profils « Officier de Sécurité » est une question récurrente à chaque audit. Pouvoir limiter et auditer leurs interventions en production sans perturber les règles de sécurité existantes est un facteur important de réduction des risques.

La législation en matière de contrôle interne (Loi de Sécurité Financière, Sarbanes-Oxley, HIPAA, Bâle II, C-198, PCI, 21-CFR, ...) se durcit et rend pénalement responsables les dirigeants et administrateurs des sociétés cotées et des organismes financiers, s'ils ne mettent pas en œuvre les moyens de sécuriser et d'auditer leur système d'informations. La responsabilité de la Direction Informatique peut également être mise en cause par délégation.

La suite QJRN/400 et CONTROLER met à votre disposition les solutions pour répondre à ces obligations.

CONTROLER vous aide à répondre aux objectifs de contrôle de COBIT en matière de sécurité des accès au système et aux données.

CONTEXTE

Les serveurs System i sont réputés pour leur fiabilité et leur sécurité.

Si la sécurité de l'OS est et doit rester le rempart contre les accès non autorisés, il vous faudra aussi :

- protéger votre serveur contre l'utilisation de commandes dangereuses
- bloquer certains accès laissés ouverts par la sécurité System i
- auditer et contrôler l'ensemble des flux traversant vos serveurs
- Contrôler les profils génériques
- ...

De plus, si vous souhaitez gérer un niveau de confidentialité élevé pour vos données stratégiques ou sensibles (HIPAA), la sécurité de l'OS ne vous permettra pas :

- de vous assurer que les utilisateurs n'accèdent aux données que par des programmes répertoriés et sécurisés
- de contrôler l'usage des profils ayant des droits étendus.

PRINCIPALES

CONTROLER se compose de 3 modules pilotés au travers d'une interface unique :

► Contrôle des accès réseau (Exit Points)

Grâce à la technique des Exit Points d'IBM, CONTROLER permet de contrôler les accès externes à votre serveur System i : TELNET, IFS, ODBC, FTP, DDM... .

Les accès par d'autres Middleware non IBM sont également contrôlés dans la même interface.

► Contrôle des commandes

CONTROLER surveille toute commande de l'OS et peut interdire son exécution selon son contexte d'utilisation (utilisateur, adresse IP, call stack, ...), mais aussi la valeur des paramètres, que ce soit en mode 5250 ou en Remote.

► Audit des moteurs SQL & QRY

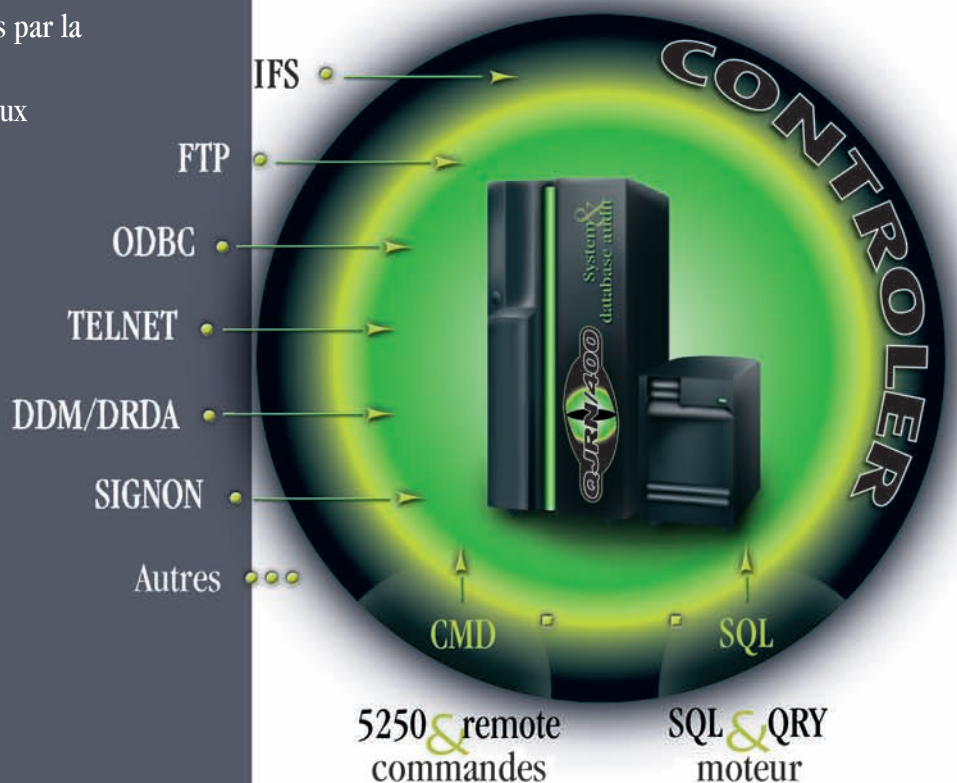
En matière de confidentialité, il est important de connaître le détail des informations qui ont pu être lues au travers d'instructions SQL et par QUERY.

Le moteur de **CONTROLER** est composé de règles de contrôle : il offre des possibilités de filtres portant sur un vocabulaire très riche dans les axes Utilisateur, Bibliothèque/Fichier, Type d'accès, Adresse IP, Travail, lien IFS, IASP,...

Un ensemble de listes contenant les combinaisons de valeurs constitue le centre de décision : il est alimenté facilement par ajout depuis la log.

L'exploitation quotidienne du produit se limite généralement au traitement de la log.

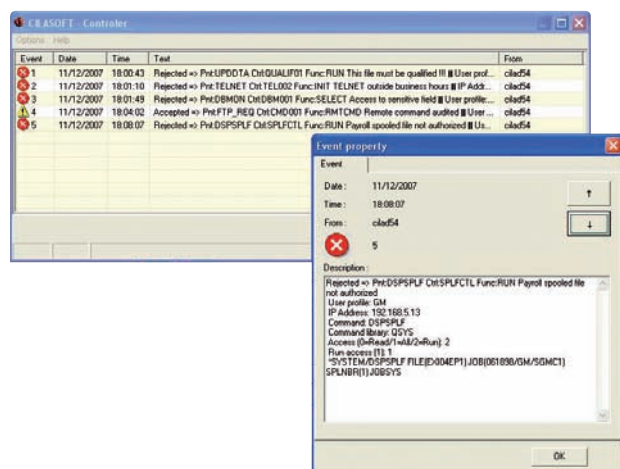
CONTROLER intervient dans le processus de contrôle avant la sécurité de l'OS. Cela permet de limiter les accès autorisés à des profils sensibles disposant de droits étendus, de protéger des objets sécurisés en mode traditionnel (listes d'autorisation, droits publics et privés...) ou en mode adoption de droits.



AVANTAGES TECHNIQUES

De conception récente, CONTROLLER évite les faiblesses de certaines solutions concurrentes et bénéficie d'avantages majeurs en termes de :

- ▶ **Faible impact sur les performances**
- ▶ Hébergement de programmes d'exit tiers
- ▶ **Prise en compte en temps réel des modifications du paramétrage**
- ▶ Suspension d'urgence
- ▶ Qualification de tous les objets
- ▶ Adresse IP disponible pour tous les contrôles
- ▶ Indépendance entre règles et valeurs
- ▶ **Non redondance des règles**
- ▶ Richesse et évolutivité du vocabulaire utilisable dans les règles
- ▶ **Mode apprentissage à partir des événements logués et mode simulation**
- ▶ **Action à exécuter que l'événement soit accepté ou refusé** (messages, swap de profil, écriture dans un journal ou un fichier, exécution d'une commande, alertes Popup ou Syslog)
- ▶ **Inversion des règles : travail en Black ou White Lists**
- ▶ Consolidation des événements issus de plusieurs serveurs System i sur une même console Syslog



Deux composants clients permettent de centraliser les alertes dans l'environnement Windows : sous forme de fenêtres Popup ou au travers de l'EventLog. Cette dernière possibilité ouvre CONTROLLER vers les consoles de sécurité du monde réseau.

MODELE LIVRE EN STANDARD

CONTROLLER est livré avec un ensemble de règles standard permettant de répondre à 95% des besoins. Le plus souvent de simples adaptations suffisent.

Si nécessaire, le paramétrage du moteur peut être entièrement réécrit pour l'adapter à votre politique de sécurité.

Des modèles complémentaires sont disponibles pour les principaux ERP du marché.

Le modèle livré en standard est basé sur le principe des White Lists pour les accès réseau. Les règles peuvent être basées sur l'utilisateur, le profil de groupe, les groupes complémentaires, ou les trois en même temps. Par défaut, tout accès est rejeté et logué. Il propose entre autres :

- ▶ **CONTRÔLES GÉNÉRAUX :**
 - Log de toute connexion en dehors des heures ouvrables.
 - Log des profils génériques, des profils avec droits étendus.
- ▶ **TELNET :**
 - Accepter les connexions pour des combinaisons Plage d'Adresse IP / Nom de Device.
- ▶ **FTP et ODBC :**
 - Détection automatique de la codification DB2 ou IFS.
 - Accepter les combinaisons Utilisateur / Bibliothèque / Nom d'objet / Type d'accès.

Deux options sont proposées : accepter sans garder de trace, ou accepter en gardant une trace dans la log pour les événements que vous jugez sensibles.
- ▶ **Remote command (FTP, ODBC, DDM) :**
 - Accepter les combinaisons Utilisateur / Commande / Valeur paramètre (avec ou sans log).
- ▶ **IFS :**
 - Accepter les accès externes selon l'utilisateur, le type d'accès et le chemin.
 - Contrôler les accès 5250 (WRKLNK) selon les mêmes règles.
- ▶ **DFU :**
 - Obligation de qualifier la bibliothèque du fichier.
 - Autoriser DFU sur les bibliothèques de tests.
 - N'autoriser DFU sur les bibliothèques de production qu'à certains profils, avec inscription dans la log et envoi d'un email au RSSI.
- ▶ **SQL :**
 - Pour tous les jobs exécutant une requête SQL sur des fichiers définis comme sensibles, toutes les instructions exécutées sont loguées. Un email est envoyé au RSSI pour les requêtes de mise à jour (UPDATE, DELETE).
- ▶ **DRDA :**
 - Toutes les requêtes SQL peuvent être loguées.



AVANTAGES

- Mise en œuvre rapide
- Adapté pour petites et grandes structures : de 100 à plus de 8 000 utilisateurs. Plus de 50 partitions, IASP supportés.
- Modèle de contrôles personnalisables livré en standard
- Interface unique pour tous les contrôles
- Maintenance simplifiée des règles
- Mise à jour en temps réel des contrôles sans redémarrage des serveurs associés
- Impact très faible sur les performances
- Mode apprentissage et simulateur intégrés



VALEUR AJOUTÉE

- Effet dissuasif, donc diminution du risque de malveillance
- Haut niveau d'automatisation
- Retour sur investissement rapide



CONTROLLER et **QJRN/400**
sont des produits



ZI Les Iles • 190 route des Sarves
74370 METZ-TESSY
FRANCE
Téléphone : +33 4 50 69 45 98
Télécopie : +33 4 50 69 45 99
Email : contact@cilasoft.com
Web : <http://www.cilasoft.fr>

AUDIT SYSTÈME ET BASE DE DONNÉES

CONTROLLER peut être associé à notre solution **QJRN/400** pour constituer **une suite d'audit et de sécurité complète** : le contrôle d'accès et le suivi détaillé de tous les événements au travers de la même interface.



**LA MAÎTRISE DE CE
QUI SE PASSE CHEZ SOI !**

VOTRE CONTACT