

NetIQ Change Guardian™ pour Windows

Superviser les activités et changements des utilisateurs en environnement Windows avec un impact minimal sur les serveurs

Présentation générale

NetIQ Change Guardian for Windows fournit des informations précises sur les activités et modifications opérées par les utilisateurs habilités sur l'ensemble des systèmes Windows d'entreprise et procure une visibilité incomparable pour réduire l'exposition aux risques majeurs de sécurité.

Des solutions pour les systèmes d'information modernes

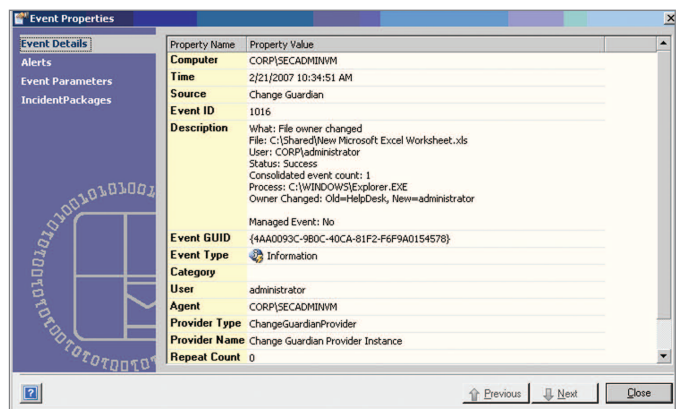
Le contrôle du changement, une des « bonnes pratiques » emblématiques des technologies de l'information, est un impératif pour certaines industries – notamment pour les standards de sécurisation des données de cartes de paiement. Malheureusement, les approches actuelles ont encore tendance à échouer lorsqu'il s'agit de les mettre en pratique sur les systèmes de production pour les raisons suivantes :

- Les audits natifs de niveau objet dégradent considérablement les performances serveur et génèrent des pistes d'audit complexes et démesurées.
- Les outils de vérification d'intégrité des fichiers causent des pics d'utilisation système inacceptables – et restent incapables d'identifier l'heure et l'auteur d'un changement sans s'appuyer sur des pistes d'audit de niveau objet.
- Les extensions du noyau (« Kernel shims ») peuvent générer des problèmes de fiabilité système et sont complexes à déployer à grande échelle.

NetIQ Change Guardian for Windows résout ces différents challenges grâce à une approche exclusive de l'audit du changement et des activités. Son pilote de filtrage du système de fichiers – pris en charge par Microsoft – capture et traite les activités souhaitées et transforme ensuite les données pour produire des alertes et pistes d'audit exploitables, cohérentes et simples – sans compromis de performance. En tant que module de NetIQ Security Manager™, il est couplé à une technologie leader de gestion des événements et informations de sécurité et à des outils avancés de gestion des logs.

Avantages clés

Monitoring performant du changement en temps réel – Contrôle des changements affectant les fichiers, répertoires, ressources partagées, entrées de registre et processus système – avec alertes rapides en cas de changements potentiellement dangereux pour l'environnement.



Grâce à une lecture intuitive des événements les plus significatifs produits par NetIQ Change Guardian for Windows, il est inutile d'être un expert pour comprendre la situation... Le système indique les valeurs avant/après et réduit le nombre d'enregistrements nécessaires pour décrire une activité donnée (changement d'habilitation, modification fichier, ajout d'une clé de registre, etc.).

Suppression des audits natifs de niveau objet et réduction drastique de l'utilisation serveur – Mise en œuvre d'un mécanisme de supervision approuvé par Microsoft évitant les dégradations de performance générées par les audits natifs – tout en fournissant des informations à haute fiabilité sur les changements.

Validation et mise en application de processus de contrôle du changement – Identification des changements « contrôlés » (à travers l'interface autorisée ou une procédure prédéfinie) par opposition aux changements « incontrôlés », pouvant révéler une tentative de contournement des contrôles.

Enregistrement et audit centralisés du changement – Compilation des données critiques pour toute l'entreprise à des fins d'analyse – éliminant les complexités d'agrégation des événements de changement et simplifiant la mise en conformité légale et les investigations.

Reporting complet des changements – Capture des valeurs « avant/après » des objets permettant de générer des rapports de changement détaillés (pour un ou plusieurs utilisateurs ou postes de travail), d'identifier au plus vite toute anomalie et de « zoomer » rapidement sur les informations détaillées à des fins d'investigation.

Intégration à une solution étendue de contrôle du changement en environnement Windows – Extension des fonctionnalités de NetIQ Security Manager et NetIQ Change Administrator™ pour fournir une solution complète de délégation de droits, de contrôle des utilisateurs privilégiés et de sécurisation des serveurs.

NetIQ Change Guardian™ pour Windows

Fonctionnalités techniques

Monitoring et notification en temps réel des changements affectant l'environnement Windows avec fourniture d'informations détaillées sur les éléments suivants :

- **Fichiers et répertoires** – Détails sur les utilisateurs ayant réalisé des opérations de création, accès, déplacement, modification ou effacement de fichiers ou répertoires (avec informations avant/après : taille du fichier, autorisations d'accès, etc.)
- **Partages de fichiers** – Identification des opérations de modification des permissions d'accès aux fichiers/répertoires.
- **Registre Windows** – Informations sur l'auteur des changements (avec fourniture des valeurs avant/après).
- **Processus système** – Contrôle de la création et de la clôture des processus, identification de l'utilisateur ou de l'application à l'origine de l'action et journalisation de tous les lancements de modules MMC (Microsoft Management Console).

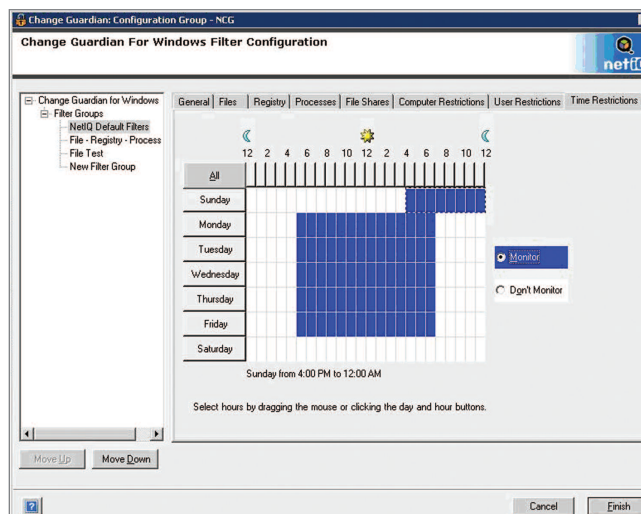
Informations d'audit avancées – Meilleure fidélité et clarté des informations que les événements natifs, résolution des SID/GUID sur la base de leurs descripteurs réels et enregistrement des informations avant/après changement pour une meilleure analyse d'incident.

- **Moteur de règles extensible et évolutif** – Création et personnalisation simplifiées des règles via des assistants intuitifs pour inclure/exclure des utilisateurs, ordinateurs, fichiers, répertoires, clés de registre et processus pendant des périodes paramétrables.
- **Système d'alertes contrôlable** Définition des changements déclenchant une alerte et de leurs modalités d'envoi (heure, destination, mode).
- **Reporting complet des changements** – Afin de démontrer la conformité avec les politiques internes et les exigences réglementaires et faciliter l'analyse de la cause source et les dépannages.

Contacts

Siège mondial de NetIQ, division d'Attachmate

1233 West Loop South
Suite 1800
Houston, TX 77027
+1 713.548.1700
info@netiq.com
www.netiq.com



NetIQ Change Guardian for Windows offre des fonctionnalités flexibles de monitoring permettant de définir des paramètres tels que les éléments à contrôler (ou à exclure) ainsi que les systèmes, utilisateurs et périodes concernés.

Collecte et audit centralisés des données de changement –

Bénéficiant des fonctionnalités de la plate-forme primée par la profession NetIQ Security Manager, cette solution propose une robuste infrastructure de contrôle librement adaptable et extensible en fonction des besoins.

Système requis

Système de monitoring :

- NetIQ Security Manager 5.6 SP1 ou supérieur

Plates-formes Windows prises en charge :

- Windows Server 2003 SP1

Pour des informations sur nos autres implantations, partenaires et revendeurs, consultez www.netiq.com/contacts.

NetIQ Change Guardian for Windows, NetIQ Change Guardian for Active Directory, NetIQ Security Manager, NetIQ et le logo NetIQ sont des marques ou marques déposées de NetIQ Corporation ou ses filiales aux États-Unis et dans d'autres pays. Tous les autres noms d'entreprises et de produits sont des marques ou marques déposées de leurs titulaires respectifs.