Quest InTrust

AUDIT ET CONTROLE DE CONFORMITE POUR UN SYSTEME D'INFORMATION SECURISE

«InTrust nous a séduit par sa capacité à réunir dans une même interface les fonctions de supervision de la conformité à notre stratégie de sécurité, et des capacités d'alerte en temps réel sur les événements de sécurité critiques pour notre activité.»

— Colin Harrison
Chef de projet, architectures du SI
Experian, UK, Ltd

- Réduit les coûts de gestion en automatisant la collecte et la compression des données d'événements
- Répond aux obligations réglementaires de traçabilité des événements de sécurité les plus importants aux fins d'audit
- Améliore la sécurité du système d'information en identifiant les comptes utilisateurs utilisés à mauvais escient ou en violation des règles établies par l'entreprise

De plus en plus, les entreprises doivent se soumettre non seulement aux directives internes en matière de sécurité informatique mais aussi à des obligations réglementaires toujours plus rigoureuses. Une fois que ces règles ont été mises en œuvre, il est nécessaire de s'assurer qu'elles sont effectivement respectées au quotidien. Quest® InTrust™ apporte aux administrateurs les moyens d'effectuer ces contrôles en collectant de façon automatisée des données d'événement à partir de sources hétérogènes, y compris les pares-feu, les systèmes d'exploitation et les applications, l'activité des comptes utilisateurs. Consolidée dans un référentiel unique capable d'évoluer avec la taille de l'entreprise, cette information est disponible pour le reporting ou l'audit. Par ses fonctions avancées de génération de rapports, InTrust participe activement à l'effort de contrôle de conformité des directions informatiques, autorisant au passage une exploitation optimale des données d'événement.

Collecte sécurisée des données d'événement

InTrust™ permet de planifier la collecte automatique des données d'événement aux heures les plus favorables. Ses fonctions avancées de planification économisent la bande passante tout en réduisant le risque d'erreur humaine. De plus, InTrust™ garantit la sécurité des journaux d'événements en assurant le chiffrement et la compression des données avant la transmission via le réseau.

Accessibilité optimisée de l'information

InTrust™ optimise au meilleur coût l'accès rapide aux journaux d'événements sur une longue période. Le référentiel InTrust™ est spécialement conçu pour l'archivage à long terme d'importants volumes de données, répondant ainsi aux exigences d'audit et aux obligations réglementaires. La technologie de compression utilisée permet de stocker beaucoup plus de données que des solutions s'appuyant sur des bases de données traditionnelles, ou la simple copie des fichiers natifs de journaux d'événements.

Flexibilité du reporting

InTrust™ facilite la génération et la distribution de rapports pour les besoins d'audit interne ou externe. Construits sur des modèles préparamétrés et personnalisables, les rapports peuvent être exportés dans la plupart des formats courants. InTrust™ garantit ainsi en toute simplicité la disponibilité de l'information au moment et dans le format demandé.

Amélioration de la sécurité et des performances

InTrust™ améliore la sécurité globale du système d'information en notifiant en temps réel les administrateurs d'une activité anormale d'un compte utilisateur, tel que la tentative d'accès à des fichiers en dehors des heures normales de bureau, la succession de tentatives infructueuses d'authentification suivie d'une tentative réussie, et bien d'autres événements de sécurité. InTrust™ alerte également les administrateurs en cas d'activité anormale des serveurs, afin d'anticiper tout risque de rupture de la continuité d'activité. Flexible, InTrust™ notifie les personnes concernées par email, ou via des consoles d'administration du marché.

QUEST SOFTWARE®

Quest InTrust

AUDIT ET CONTROLE DE CONFORMITE POUR UN SYSTEME D'INFORMATION SECURISE

«Les solutions Quest sont devenus l'une de nos principales sources d'information pour la notification et l'analyse des événements de sécurité. Ils constituent aujourd'hui l'un des piliers de notre infrastructure de sécurité.»

— David Bryant
Chef de projet sécurité du SI
Raymond James Financial

Configurations requises

Système d'exploitation:

- Microsoft Windows 2000 SP3 ou supérieur
- Microsoft Windows XP SP1
- Microsoft Windows Server 2003
- Sun Solaris 8.0 (installation standard) avec correctif 112439-01
- Sun Solaris 9.0 (installation standard)
- Red Hat Enterprise Linux AS 3.x
- Red Hat Enterprise Linux ES 3.x

Serveur:

- Intel x86
- SUN SPARC

Mémoire vive:

- 512 Mo et plus (recommandé)

Espace disque:

- Minimum 400 Mo

Garantie de conformité réglementaire: InTrust™ aide les entreprises à s'assurer de la conformité d'exploitation de leur système d'information en surveillant au quotidien les accès aux systèmes sensibles. InTrust™ peut ainsi détecter les accès non autorisés ou les événements suspects. En plus de la collecte automatisée, de la consolidation et de l'analyse des données d'événements, InTrust™ notifie en temps réel les administrateurs, et ce, quelque soit le niveau d'hétérogénéité du système d'information.

Automatisation de bout en bout: Basé sur la technologie SecureCollect de Quest Software, InTrust™ automatise de bout en bout et sécurise la collecte des journaux d'événements. La planification des collectes permet aussi de réduire la charge de travail des équipes d'administration.

Surveillance de l'activité des utilisateurs: Intégrée à InTrust™, la technologie UserTrack consolide en temps réel les informations relatives à l'activité des utilisateurs et des administrateurs, ainsi que d'autres événements critiques pour la sécurité du système d'information. Grâce à de puissantes fonctions de corrélation, InTrust™ peut ainsi alerter en temps réel le responsable de la sécurité de toute activité inhabituelle et de toute violation des protocoles de sécurité.

Intégrité des journaux d'événements: InTrust™ permet de définir une zone invisible sur les serveurs où seront dupliqués les journaux d'événements dès leur création. Cette fonction élimine le risque qu'un utilisateur malveillant ou un administrateur indélicat ne tente de masquer ses traces en détruisant les journaux d'événements.

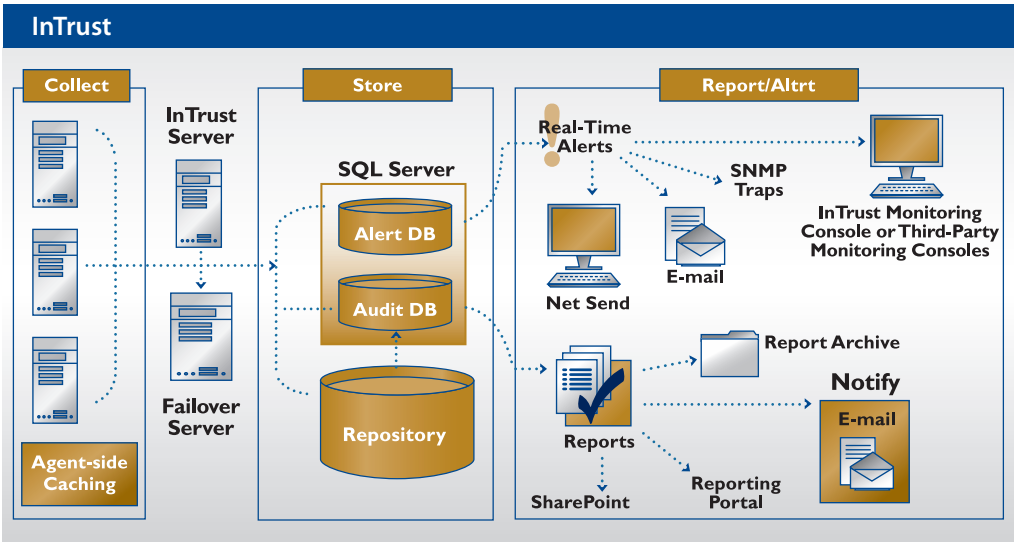
Compression des données et consolidation dans un référentiel: InTrust™ repose sur une architecture unifiée de stockage: StoreMore. StoreMore est un référentiel conçu pour permettre un stockage à long terme des données grâce à un mécanisme de compression des données particulièrement performant.

Détection et analyse des anomalies: Cette fonction d'InTrust™ automatise la découverte des incidents de sécurité et l'analyse des tendances d'évolution de l'activité réseau, par la comparaison de l'activité actuelle du réseau avec un modèle dynamique, fondé sur une activité considérée comme normale.

Notification en temps réel: Avec la technologie InTrust™ NotifyNow, l'administrateur est averti en temps réel des alertes UserTrack. Les alertes peuvent être transmises directement par email ou via une console d'administration du marché, telle que Microsoft Operations Manager (MOM).

Flexibilité du reporting: FlexReport est une technologie intégrée à InTrust™ facilitant la génération de rapports personnalisés et offrant un vaste choix de modèles de rapports préparamétrés. InTrust™ permet aussi d'exporter les rapports dans la plupart des formats de fichiers exploités en entreprise dont HTML, XML, PDF, CSV, TXT, ainsi que Microsoft Word, Visio et Excel.

Disponibilité: InTrust™ intègre un mécanisme de redondance afin de garantir la disponibilité de l'architecture de contrôle. Les capacités intégrées de reprise sur incident permettent de transférer sur un serveur de secours l'ensemble des paramètres de configuration et des tâches en cours, réduisant ainsi le risque de perte des données de journaux d'événements.



QUEST SOFTWARE

Pour de plus amples informations, rendez vous sur notre site:
www.quest.com

Microsoft GOLD CERTIFIED Partner

IMG_INT_DS_02142006