InTrust®

Outil de gestion des journaux d'événements intelligent et extensible

Les ressources les plus précieuses de votre entreprise sont ses données et les utilisateurs qui peuvent y accéder. Pour l'équipe informatique et le département chargé de la sécurité, il est crucial de garder une trace de l'activité des utilisateurs et des comptes à privilèges, en particulier sur les postes de travail et les appareils des utilisateurs finaux, afin d'assurer la sécurité de l'environnement ainsi que la conformité aux diverses réglementations du secteur. Mais cette tâche s'avère difficile en raison des énormes volumes de données répartis sur différents systèmes, appareils et applications. La collecte, le stockage et l'analyse de toutes ces données nécessitent généralement d'importantes capacités de stockage, un processus chronophage de collecte des données d'événements et une expertise en interne sur les données collectées.

Avec Quest® InTrust®, vous pouvez surveiller toute l'activité des administrateurs et des postes de travail des utilisateurs, de la connexion à la déconnexion, en passant par tous les événements intermédiaires. Réduisez les coûts de stockage avec une compression des données de 20:1 et stockez des années de journaux d'événements provenant des serveurs Windows, UNIX/Linux, des bases de données, des applications et des appareils réseau. Les alertes en temps réel de la solution InTrust vous permettent de répondre immédiatement aux menaces à l'aide de réponses automatisées pour les activités suspectes.

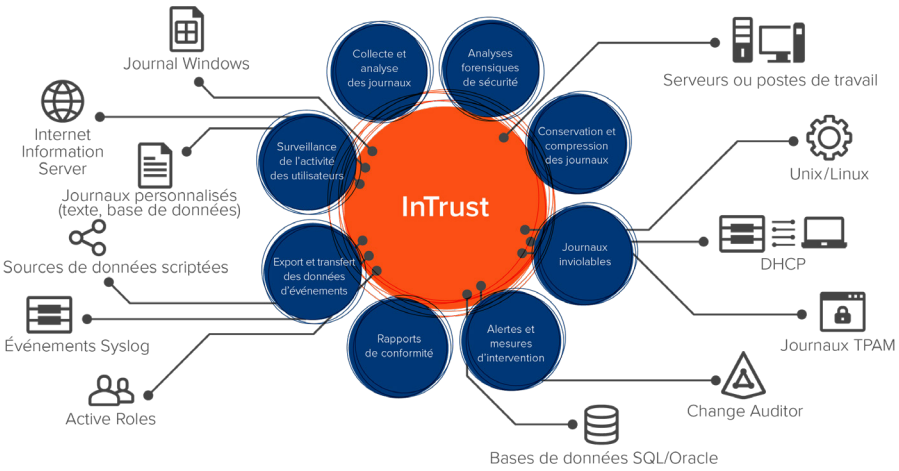
FONCTIONNALITÉS

Écran unique

Centralisez la collecte et le stockage de tous les journaux des postes de travail natifs ou tiers provenant de différents systèmes, appareils et applications, et profitez de fonctions de recherche et de rapports immédiats sur la sécurité et la conformité. InTrust fournit une vue unifiée des journaux d'événements Windows, d'UNIX/Linux, des journaux d'applications Web et IIS, des pistes d'audit PowerShell des systèmes de protection des terminaux, des proxy et pare-feu, des plateformes de virtualisation, des appareils réseau, des journaux texte personnalisés et des événements Quest Change Auditor.

Surveillance des journaux des postes de travail des utilisateurs

Protégez vos postes de travail des cyberattaques modernes telles que « pass-the-hash », le phishing ou les rançongiciels, en surveillant l'activité des administrateurs et des utilisateurs, de la connexion à la déconnexion, en passant par tous les événements intermédiaires. Collectez et stockez les données principales de l'accès utilisateur telles que l'identité de l'individu à l'origine d'une action, en quoi celle-ci



Surveillez efficacement toute l'activité des administrateurs et des postes de travail des utilisateurs pour assurer la sécurité de vos ressources les plus précieuses : vos données.

« Nous utilisons InTrust pour collecter des journaux sur les contrôleurs de domaine et les événements de surveillance en vue des audits de conformité SOX. Repository Viewer est parfait pour rechercher des verrouillages de compte et d'autres événements liés à la connexion à des fins de sécurité. »

Ingénieur, entreprise de services professionnels S&P 500

TVID : 726-084-5E5

AVANTAGES :

- Réduisez les coûts du stockage et assurez une conformité continue avec un espace de sauvegarde des journaux indexé et hautement compressé
- Recherchez facilement l'activité de tous les utilisateurs finaux et comptes à privilèges à partir d'une console centrale
- Signalez, résolvez et examinez rapidement les événements de sécurité
- Comprenez vos données à l'aide de journaux d'événements natifs et standardisés
- Profitez d'une intégration simple avec votre solution de gestion des événements et des informations de sécurité (SIEM) existante
- Réagissez immédiatement aux menaces avec les alertes en temps réel et les réponses automatisées
- Protégez les données des journaux d'événements des falsifications ou destructions en dupliquant les événements dès leur création

« Je pense que le produit offre de précieuses fonctionnalités d'alerte et de création de rapports relatifs à la sécurité. D'autres produits proposent des fonctionnalités similaires, mais InTrust semble offrir une implémentation rapide et des avantages immédiats dans les domaines des audits et de la conformité. »

Responsable informatique senior, entreprise automobile et de transport du classement Fortune 500

TVID : D2B-CDB-505

CONFIGURATION REQUISE

PLATEFORMES PRISES EN CHARGE
Événements Microsoft Windows
Événements Microsoft IIS
Événements Microsoft Forefront Threat Management Gateway et ISA Server
Événements de serveur DHCP Microsoft
Événements Solaris
Événements Red Hat Enterprise Linux
Événements Oracle Linux
Événements SUSE Linux
Événements Debian GNU/Linux
Événements Ubuntu Linux
Événements IBM AIX
Événements HP-UX
Événements VMware vCenter
Événements VMware ESX et ESXi
Pour en savoir plus, consultez le document relatif à la configuration requise.

consistait, sur quel serveur elle s'est produite et à partir de quel poste de travail.

Analyse simplifiée des journaux

Consolidez les journaux d'événements obscurs et provenant de sources différentes en un format simple et normalisé qui indique les éléments suivants pour mieux comprendre les données : qui, quoi, quand, où, à partir de quel emplacement et vers qui. Les données syslog diffèrent particulièrement d'une application à une autre. Avec InTrust®, vous pouvez détecter les données structurées au sein des événements syslog et les analyser correctement. Une indexation unique en texte intégral permet d'effectuer facilement des recherches sur des données d'événements anciennes pour créer rapidement des rapports, résoudre des problèmes et mener une enquête de sécurité.

Compression intelligente et extensible des journaux d'événements

Collectez et stockez d'importants volumes de données dans un espace de stockage hautement compressé, jusqu'à 20 fois avec un index et 40 fois sans index, et économisez jusqu'à 60 % sur les coûts liés au stockage, tout en respectant la conformité aux réglementations HIPAA, SOX, PCI, FISMA, etc. En outre, un serveur InTrust peut traiter jusqu'à 60 000 événements par seconde avec 10 000 agents écrivant des journaux d'événements simultanément, optimisant ainsi l'efficacité, l'extensibilité et les coûts liés au matériel. Si vous avez besoin d'un volume plus élevé, vous pouvez simplement ajouter un serveur InTrust supplémentaire et partager la charge de travail : l'extensibilité de la solution est presque sans limites.

Alertes en temps réel et mesures d'intervention

Surveillez les activités des utilisateurs non autorisées ou suspectes, telles que la création de fichiers en dehors des limites définies, à l'aide d'extensions de fichiers propres à des attaques connues par rançongiciel ou de commandes PowerShell suspectes. Répondez immédiatement aux menaces avec les alertes en temps réel. InTrust vous permet de déclencher facilement des réponses automatisées pour les activités suspectes, comme le blocage de l'activité, la suspension de l'utilisateur incriminé, l'annulation des modifications effectuées et/ou l'activation d'un audit d'urgence.

Journaux inviolables

Protégez les données des journaux d'événements pour empêcher leur manipulation ou leur destruction. Pour ce faire, créez un emplacement cache sur chaque serveur distant où les journaux peuvent être dupliqués lors de leur création.

Intégration avec des solutions de gestion des événements et des informations de sécurité (SIEM)

Réduisez vos frais de licence SIEM annuels avec les connecteurs InTrust pour Splunk et IBM QRadar. Avec InTrust, stockez les données des journaux d'événements à long terme, et filtrez et transmettez uniquement les données appropriées à votre solution SIEM existante en vue de réaliser des analyses de sécurité en temps réel.

Informations enrichies avec IT Security Search

Exploitez dans un seul emplacement les informations utiles provenant de toutes vos solutions Quest® de sécurité et de conformité. Avec IT Security Search, vous pouvez corréler des données issues des outils InTrust, Change Auditor, Enterprise Reporter, Recovery Manager for AD et Active Roles dans un moteur de recherche informatique semblable à Google afin d'accélérer la réponse aux incidents de sécurité et les analyses forensiques. Analysez facilement les autorisations et l'activité des utilisateurs, les tendances d'événements, les activités suspectes et plus encore avec des visualisations enrichies et la chronologie des événements.

Création automatisée de rapports de bonnes pratiques

Convertissez facilement des analyses dans différents formats de rapport, notamment HTML, XML, PDF, CSV et TXT, ainsi que Microsoft Word, Visio et Excel. Planifiez des rapports et automatisez la distribution dans les équipes ou choisissez un des nombreux rapports de bonnes pratiques prédéfinis de la bibliothèque avec une expertise intégrée en matière de journaux des événements. Avec des workflows de consolidation et d'importation des données, vous pouvez même transmettre automatiquement un sous-ensemble de données à SQL Server pour une analyse approfondie.

PROFIL DE QUEST

L'objectif de Quest est de résoudre des problèmes complexes à l'aide de solutions simples. Nous y parvenons en appliquant une philosophie qui repose sur l'excellence de nos produits, un service de qualité et un objectif global de simplicité dans nos interactions. Notre vision est de proposer une technologie qui apporte à la fois efficacité et résultats concrets, afin que votre entreprise consacre moins de temps à la gestion informatique et plus de temps à l'innovation.

Quest
quest.com/fr
Rendez-vous sur (quest.com/fr-fr/locations) pour obtenir les coordonnées de notre bureau local.

DataSheet-InTrust-US-KS-FR-WL36670