ManageEngine
DataSecurity Plus

Prenez en charge vos données sensibles avec DataSecurity Plus.

Découvrez, surveillez et protégez les données sensibles contre l'exposition ou le vol.

www.manageengine.fr/data-security-plus

Solutions proposées

par **DataSecurity Plus**

Audit des serveurs de fichiers

Auditez et signalez en temps réel tous les accès aux fichiers et toutes les modifications apportées à vos serveurs de fichiers, clusters de basculement et environnements de groupes de travail.

Prévention des fuites de données

Détectez, interrompez et répondez aux fuites de données sensibles via les endpoints, c'est-à-dire les clés USB, les e-mails et autres grâce à la surveillance de la sécurité.

Evaluation des risques liés aux données

Exploitez l'inspection approfondie du contenu et le marquage manuel pour découvrir les données sensibles et classer les fichiers en fonction de leur vulnérabilité.

Analyse des fichiers

Obtenez une visibilité approfondie des data stores pour localiser les données à risque et gérer les données inactives pour réduire les coûts de stockage des données grâce à des rapports détaillés sur les métadonnées des fichiers, les fichiers indésirables et le stockage sur le serveur.

Télécharger

Essai gratuit de 30 jours

ManageEngine DataSecurity Plus

Audit des serveurs de fichiers avec DataSecurity Plus

Télécharger

Essai gratuit de 30 jours

Auditez l'accès aux fichiers et aux dossiers et obtenez des informations détaillées sur les quatre W's - qui a accédé à quoi, quand et d'où - pour tous les accès et modifications de fichiers.

Détectez et arrêtez les attaques potentielles de ransomware dès leur début grâce à un mécanisme automatisé de réponse aux menaces.

Déclenchez des alertes instantanées en cas de pics soudains d'accès aux fichiers ou aux dossiers, de modifications ou de changements d'autorisation.

Signalez et alertez sur les événements de copier-coller de fichiers en temps réel à l'aide de stratégies prédéfinies.

Suivez et analysez les tentatives d'accès effectuées par des utilisateurs suspects avant qu'elles ne se transforment en problèmes de sécurité critiques

Effectuez une analyse approfondie en utilisant des données d'audit précises et exploitables pour tous les événements anormaux.

Environnements pris en charge : Serveurs de fichiers Windows, clusters de basculement groupes de travail.

ManageEngine
DataSecurity Plus

Prévention des fuites de données

avec DataSecurity Plus

Télécharger

Essai gratuit de 30 jours

Surveillez, suivez et analysez le moment où des données sensibles (PII/ePHI) sont modifiées par des utilisateurs, copiées vers ou depuis des postes de travail, et plus encore.

Envoyez des alertes instantanées aux propriétaires des données, aux administrateurs système ou à votre équipe de sécurité informatique en cas de violation des règles.

Sensibilisez les utilisateurs à l'aide de messages contextuels personnalisés en cas de violation des règles, notamment en cas de déplacement injustifié de fichiers par e-mail.

Surveillance de la sécurité en temps réel pour un large éventail d'événements de fichiers afin de garantir l'intégrité des fichiers locaux.

Bloquez, supprimez et mettez en quarantaine les fichiers ou choisissez toute autre mesure corrective active prédéfinie pour éviter les fuites de données.

Applications: Outlook

Stockage amovible : USB, cartes SD, appareils photo, téléphones portables...

Bureaux virtuels : Citrix, VMware (à condition que le système d'exploitation installé soit Windows 2003 et supérieur).

Machines distribuées : Ordinateurs portables, ordinateurs de bureaux

Autres : Impression, presse-papiers, fax, partages réseau.

ManageEngine
DataSecurity Plus

Evaluation des risques liées aux données

avec DataSecurity Plus

Télécharger

Essai gratuit de 30 jours

Trouvez, analysez et suivez les données personnelles sensibles également appelées PII/ePHI - stockées dans des environnements de serveurs de fichiers et de clusters de basculement.

Détectez les données à haut risques à l'aide de mots-clés spécifiques et d'expressions régulières, ou utilisez une combinaison prédéfinie des deux pour réduire les faux positifs.

Automatisez la réponse aux incidents grâce à des options de remédiation prédéfinies notamment le blocage, la suppression et la mise en quarantaine.

Console web-unique pour créer et définir vos propres stratégies et règles, répondre aux incidents critiques, signaler les événements liés aux fichiers, et bien plus encore.

Simplifiez la classification des données grâce à des fonctions de marquage automatique et manuel des fichiers afin de réduire la charge de travail de l'administrateur.

Utilisez des analyses incrémentielles pour réduire le temps d'exécution en analysant uniquement les fichiers nouveaux ou modifiés.

Analysez le contenu sensible de plus de 50 types de fichiers y compris les e-mails, les textes, les fichiers compressés, etc.

Optimisez la conformité à l'aide de stratégies prédéfinies pour divers mandats externes notamment les RGPD, PCI DSS, HIPAA et SOX, grâce à plus de 50 modèles de règles.

ManageEngine
DataSecurity Plus

Analyse des fichiers avec DataSecurity Plus

L'analyse des fichiers permet d'analyser, d'identifier et de supprimer les données inutiles afin de réduire l'espace de stockage.

Télécharger

Essai gratuit de 30 jours

Gérez les données ROT en trouvant et en purgeant les données obsolètes et triviales (ROT), les fichiers en double, etc.

Optimisez l'utilisation de l'espace disque en analysant les tendances de croissance et les modèles d'utilisation du disque, et générez des alertes lorsque l'espace libre passe sous une limite préconfigurée.

Examinez les permissions de sécurité pour identifier les fichiers surexposés, qui a accès à vos fichiers sensibles, et plus encore.

Vérifiez les autorisations de fichiers pour capturer les fichiers dont les autorisations sont incohérentes et les fichiers accessibles à tous afin de renforcer les privilèges des utilisateurs en fonction de leur rôle.

Localisez et gérez les fichiers non professionnels tels que les vidéos, les images et autres fichiers personnels appartenant aux employés, ainsi que les fichiers cachés qui doivent être filtrés hors de vos serveurs de fichiers.

Analysez le volume des données l'état de l'espace disque et les fichiers indésirables au niveau du domaine, du serveur ou du lecteur, le tout dans un tableau de bord central.

Suivez les fichiers dangereux infectés par des ransomwares à l'aide de notre bibliothèque prédéfinie de plus de 50 types de fichiers ransomwares afin de les éliminer de vos serveurs de fichiers.

Suivez tous les partages de votre serveur de fichiers avec des détails sur la taille et l'emplacement des chemins de partage afin d'optimiser les ressources de partage de fichiers.

Configuration requise pour DataSecurity Plus

Navigateurs pris en charge : Firefox, Google Chrome, Microsoft Edge

OS serveur pris en charge : 2003 R2, 2008, 2008R2, 2012, 2012 R2, 2016

OS client pris en charge : Windows XP, Vista, 7, 8, 8.1, 10

Processeur : 2.0 GHz

RAM : 8 GO

Espace disque : 20 GO

Pour connaître la configuration complète requise pour DataSecurity Plus, consultez notre page d'assistance.

ManageEngine DataSecurity Plus

ManageEngine

DataSecurity Plus

Visibilité et sécurité des données en un seul produit.

Une solution à deux volets pour lutter contre les menaces internes, prévenir la perte de données et répondre aux exigences de conformité

Télécharger

Information de contact

PG Software EUROPE

Website
www.manageengine.fr/data-security-plus

Support technique
manageengine@pgsoftware.support

Contact commercial
commercial@pgsoftware.fr

Téléphone
0 805 296 540 Service & appel gratuits