

ManageEngine

DataSecurity Plus

Une plateforme unifiée de visibilité et de sécurité des données

- **Audit de fichier**
- **Analyse des fichiers**
- **Évaluation des risques des données**
- **Prévention des fuites de données**
- **Protection du Cloud**



Programme

- À propos de DataSecurity Plus
- Solutions proposées
- Points forts et capacités
- Modèle de licence
- Plateformes prises en charge
- Assistance à l'évaluation
- Nos clients
- Contactez nous

DataSecurity Plus

ManageEngine DataSecurity Plus est une plateforme unifiée de visibilité et de sécurité des données. Elle offre les fonctionnalités suivantes :

- Audit des serveurs de fichiers
- Supervision de l'intégrité des fichiers
- Détection et réponse aux ransomwares
- Réponse aux incidents de sécurité
- Analyse des fichiers et des autorisations de sécurité
- Découverte et classification des données
- Protection contre la duplication de fichiers
- Prévention des fuites de données au niveau des terminaux
- Protection des applications en nuage, et plus encore.

Solutions offertes

DataSecurity Plus comprend les modules suivants :



Audit de fichiers

Rapport, analyse et alerte sur les accès et les modifications de fichiers en temps réel.



Analyse des fichiers

Analyser le stockage des fichiers, superviser l'utilisation de l'espace disque et examiner les autorisations de sécurité pour localiser les données inutiles et les failles de sécurité.



Évaluation des risques liés aux données

Découvrir et classer les fichiers contenant des données sensibles (PII, PCI et ePHI).



Prévention des fuites de données

Détecter et interrompre les fuites de données sensibles via les terminaux (USB, courrier électronique, etc.).



Protection du cloud

Auditer le trafic Web de votre entreprise pour suivre et contrôler l'utilisation des applications Web à haut risque.



Points forts:

Audit des fichiers

Points forts: Audit des fichiers

- **Auditer l'accès aux fichiers et aux dossiers:** Suivez la lecture, la création, la modification, le déplacement, la suppression, le copier-coller, etc. des fichiers pour savoir qui a fait quoi, quand et à partir de quel endroit.
- **Contrôler l'intégrité des fichiers:** Détectez les événements critiques tels que les modifications de fichiers après les heures de bureau, l'activité des utilisateurs dans les fichiers sensibles et les multiples tentatives d'accès infructueuses.
- **Recevoir des alertes de modification en temps réel:** Alertez les administrateurs en cas de modifications de fichiers non autorisées ou inhabituelles, et exécutez automatiquement des scripts personnalisés pour mettre fin aux attaques.
- **Arrêter les attaques de ransomware:** Détectez et répondez aux attaques de ransomware grâce à un mécanisme automatisé de réponse aux menaces.
- **Respecter les obligations réglementaires:** Répondez aux exigences de plusieurs réglementations informatiques telles que PCI DSS, HIPAA, GDPR, FISMA, GLBA, etc.



Points forts:

Analyse des fichiers

Points forts: Analyse des fichiers

- **Gérer les données ROT:** Trouvez et supprimez les fichiers redondants, obsolètes et insignifiants pour réduire les dépenses de stockage.
- **Supprimer les fichiers en double:** Localisez les fichiers en double en comparant leur nom, leur taille et leur date de dernière modification, et supprimez les copies inutiles pour libérer de l'espace de stockage primaire.
- **Analyser l'utilisation de l'espace disque:** Suivez la consommation d'espace disque et recevez des alertes en cas de manque critique d'espace disque pour assurer la continuité de l'activité.
- **Examiner les autorisations de fichiers:** Analysez les permissions NTFS et détectez les failles de sécurité telles que les héritages brisés et les fichiers appartenant à des utilisateurs inactifs.
- **Détecter les fichiers surexposés :** Détectez les fichiers dont les permissions sont excessives, par exemple ceux qui sont accessibles à tous les utilisateurs ou qui permettent un accès illimité.



Points forts:

Évaluation des risques liés aux données

Points forts: Évaluation des risques liés aux données

- **Identifier les données sensibles:** Recherchez dans le stockage de l'entreprise les numéros de passeport, les adresses électroniques, les numéros de carte de crédit et plus de cinquante autres types de données personnelles.
- **Analyser les tendances en matière de stockage des IIP :** Recevez des rapports sur le volume, le type et les tendances du stockage des données sensibles.
- **Détecter les violations des politiques de stockage :** Détectez instantanément les données qui violent les politiques de stockage de l'entreprise et réagissez en exécutant un script personnalisé.
- **Analyser la sensibilité et la vulnérabilité des fichiers :** Analysez le risque associé aux fichiers en affichant des détails sur la quantité et le type de données personnelles qu'ils contiennent et sur les personnes qui peuvent y accéder.
- **Classifier les fichiers sensibles :** Classez les fichiers contenant des informations PII, PCI ou ePHI pour mieux comprendre quels sont les fichiers qui nécessitent des mesures de sécurité élevées.

- **Éviter la non-conformité** : Évitez le risque de pénalités de non-conformité en générant des rapports périodiques sur l'emplacement et la quantité de données sensibles stockées dans votre environnement.
- **Exploiter l'analyse incrémentielle** : N'analysez que les fichiers nouveaux et récemment modifiés pour réduire le temps de recherche des données.
- **Examiner la sécurité des fichiers** : Identifiez les employés qui peuvent accéder aux fichiers contenant des informations personnelles
- **Analyser les scores de risque** : Évaluez la vulnérabilité des données personnelles à l'aide d'un score de risque évolutif, attribué en fonction de leur contenu, de leur propriétaire, etc.



Points forts:

Prévention des fuites de données

Points forts: Prévention des fuites de données

- **Auditer l'activité des fichiers sur les terminaux:** Auditez les accès aux fichiers sur vos postes de travail Windows en temps réel.
- **Classifier les données des terminaux:** Classez les fichiers en fonction de leur sensibilité (public, interne, confidentiel ou restreint).
- **Activer la protection en fonction du contenu:** Surveillez de près qui possède et accède aux données sensibles. Exécutez des réponses instantanées lorsque des menaces sur ces données sont détectées.
- **Surveiller les périphériques amovibles:** Auditez et contrôlez l'utilisation des supports de stockage amovibles et toutes les activités de transfert de données sensibles vers ces supports.
- **Prévenir les fuites de données via les USB:** Verrouillez les ports périphériques en réponse aux comportements malveillants des utilisateurs afin d'éviter les fuites de données potentielles.

- **Bloquer l'exfiltration de données par courrier électronique:** Empêchez le transfert de fichiers contenant des données très sensibles, telles que des informations confidentielles ou des informations personnelles électroniques, par courrier électronique (Outlook).
- **Automatiser la réponse aux incidents:** Supprimez ou mettez en quarantaine les fichiers, bloquez les ports USB ou choisissez parmi d'autres options de remédiation prédéfinies pour éviter les fuites de données.
- **Auditer l'utilisation des imprimantes:** Suivez et analysez qui a imprimé quels fichiers et quand
- **Contrôler l'utilisation des applications :** Créez des listes d'autorisation et de blocage pour exercer un contrôle granulaire sur les applications qui peuvent être utilisées par les employés.
- **Empêcher les actions de duplication de fichiers :** Suivez les tentatives de duplication de fichiers critiques sur les partages locaux et réseau et bloquez les transferts de fichiers injustifiés.



Highlights of

Protection du cloud

Points forts: Protection du cloud

- Suivre l'utilisation des applications en cloud : Surveillez le trafic Web de votre entreprise pour analyser l'utilisation d'applications autorisées ou non.
- Évaluer la menace du Shadow IT: Repérez les employés qui font courir un risque à votre organisation en utilisant des applications fantômes dans le cloud.
- Surveiller les requêtes web : Capturez toutes les requêtes HTTP avec des détails sur le moment où une application en cloud a été accédée, par qui, les détails de la réputation de l'application, etc.
- Bloquer les applications non approuvées : Empêchez vos employés d'accéder à des données d'entreprise ou de les télécharger via des applications à haut risque en bloquant leurs actions en temps réel.

Détails des licences



Audit de fichiers

La licence est basée sur le nombre de serveurs de fichiers. Les utilisateurs bénéficient également de 1 To de capacités d'analyse de fichiers gratuites pour chaque serveur sous licence.



Analyse de fichiers

La licence est basée sur la taille des données en téraoctets.



Évaluation des risques liés aux données

La licence est basée sur la taille des données en téraoctets.



Prévention des fuites de données

Licence basée sur le nombre de terminaux.



Protection du Cloud

Add-on gratuit du module de Prévention des Fuites de Données.

Plateformes prises en charge



Audit des fichiers

Windows File Server 2003 R2 et plus



Analyse des fichiers

Windows File Server 2003 R2 et plus



Évaluation des risques liés aux données

Windows File Server 2003 et plus



Prévention des fuites de données

Windows Vista et plus



Protection du Cloud

Windows XP et plus, Windows Server 2003 et plus,
Linux, et Mac

Comment nous contribuons à votre évaluation

- Un essai gratuit de [30 jours entièrement fonctionnel](#)
- Prolongation de la licence d'évaluation, si nécessaire
- Assistance technique 24x5
- Une [base de connaissances](#) détaillée

Nos clients

“DataSecurity Plus est une solution de grande importance qui garantit l'intégrité des systèmes de fichiers et la prévention des pertes de données, et qui nous aide à nous conformer aux normes réglementaires.”

-Phurich Leemakanot, Mubadala Petroleum



Contactez-nous

- **Téléphone:** 02 51 60 26 75
- **Chat en direct:** Pour des réponses instantanées
- **Envoyez un courriel à l'équipe d'assistance:** helpdesk@pgsoftware.support
- **Visitez notre site web:** <https://www.pgsoftware.fr/iam/datasecurity-plus>