



Validation, classification et protection des données (DVCP)



Sécurisation Des Contenus Sensibles

Détectez les « données sombres » où qu'elles se trouvent dans vos référentiels actuels grâce aux API évolutives de Compliance Guardian.

Parcourez SharePoint, Exchange, les partages de fichiers, les bases de données, les sites Web, les plateformes cloud (notamment Office 365, Salesforce, ServiceNow, G-Suite, Box, Dropbox et Slack) ainsi que les plateformes sociales telles que Skype Entreprise, Microsoft Teams et Yammer.



Prévention Des Fuites De Données

Surveillez de manière centralisée le statut de n'importe quel incident ainsi que les niveaux de risque associés afin de garantir que les atteintes à la sécurité sont traitées en fonction de leur gravité et du moment auquel elles se sont produites.

Suivez et gérez le niveau de risque tout au long du cycle de vie de vos données grâce à des rapports sur les tendances et des analyses historiques détaillées.



Assignment Des Incidents Aux Rôles Sur La Base Des Données

Faites correspondre les contenus à des rôles (auteurs, propriétaires, équipes juridiques, groupes d'utilisateurs, etc.) propres à votre organisation afin que les utilisateurs appropriés puissent rapidement analyser les violations et y remédier.

L'affectation des contenus et l'envoi des violations à des rôles ou groupes d'utilisateurs déterminés garantit que des actions peuvent être initiées sur la base des rapports de risque.



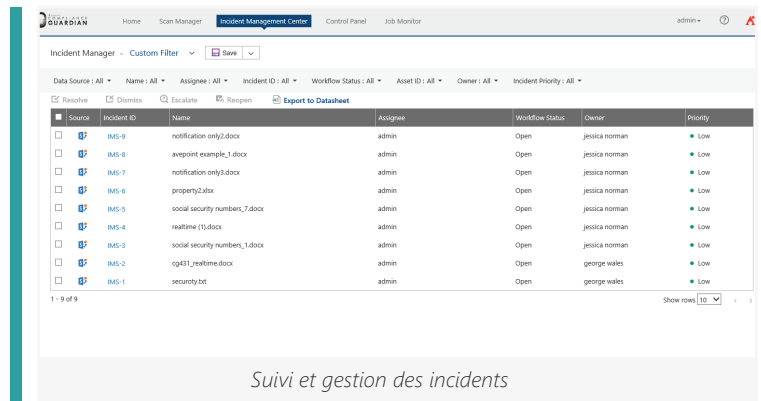
Processus De Révision Exhaustif

Bloquez, placez en quarantaine, expurgez, cryptez, supprimez, exportez de façon automatique les fichiers contenant des informations sensibles ou acheminez-les vers un emplacement approprié dès leur téléchargement, ou à l'occasion d'une analyse effectuée régulièrement ou à la demande.

Créez des alertes notifiant des utilisateurs ou groupes d'utilisateurs précis afin qu'ils contrôlent et valident les mesures à prendre à l'occasion d'incidents.

Surveillez Et Sécurisez Vos Données De Façon Proactive

Identifier les risques potentiels menaçant vos informations n'est que la première étape. Remédiez aux problèmes de façon rapide et efficace par l'expurgation, la pseudonymisation, le cryptage, la gestion des autorisations, la mise en quarantaine et le blocage grâce à des rapports hautement sécurisés et préalablement priorisés qui guident vos propriétaires d'informations et équipes de conformité dans la résolution des violations les plus graves. En intégrant aux analyses des contenus des actions automatisées visant à sécuriser les documents sensibles, à mettre à jour les autorisations et à appliquer les règles définies, nous donnons aux utilisateurs finaux les moyens de collaborer tout en protégeant vos ressources les plus précieuses.



PRÉVENTION DES PERTES DE DONNÉES

- Grâce à des analyses en temps réel planifiées identifiant et examinant les fichiers et leurs contenus, vous pouvez facilement cartographier les données sur la base de vos requêtes à l'aide de nombreuses conditions de filtrage (type de fichier, âge, taille, appartenance, emplacement, niveau de sensibilité, etc.).
- Détectez les cryptovirus et les attaques de ransomwares dans les sources de données et consultez les informations correspondantes dans un tableau de bord affichant les menaces potentielles afin d'assurer la sécurité des données.
- Faites appliquer les stratégies de sécurité relatives à la gestion de l'information afin d'assurer le stockage, la conservation, la déduplication et la sécurisation des contenus.
- La fonction intégrée « Aperçu en direct » de Perimeter permet aux utilisateurs d'ouvrir des fichiers en toute sécurité depuis l'intérieur d'un rapport IMS en suivant le lien URL indiqué.
- Supprimez, placez en quarantaine, cryptez, expurgez, anonymisez, exportez ou acheminez des contenus vers les emplacements appropriés en fonction de leur classification afin de respecter les stratégies de gouvernance des informations mises en place.

VALIDATION, CLASSIFICATION ET PROTECTION DES DONNÉES (DVCP)

- DVCP offre toutes les capacités de recensement, d'analyse et d'étiquetage de Compliance Guardian DVC, et bien plus !

GESTION DES INCIDENTS

- Repérez les atteintes à la vie privée et à la sécurité des informations et affectez-les en fonction des rôles et de l'appartenance afin que les problèmes puissent être résolus par les bonnes personnes.
- le suivi et la gestion des incidents grâce à un système de gestion des incidents automatisé incluant des révisions humaines et contrôlant les statuts, les résultats de classification et le contenu des documents afin d'assurer une résolution souple et de réduire les faux positifs.
- Générez des rapports sur les niveaux d'accès pour garantir que les bonnes personnes peuvent voir, modifier, télécharger et partager des informations et types de fichiers donnés.
- En cas d'intégration à Office 365 DLP, les incidents sont regroupés à l'échelle des systèmes et des workflows de gestion des incidents automatisés permettent de remédier aux violations.

Pour la liste complète des nouvelles fonctionnalités de cette version, veuillez consulter les notes de versions sur le [portail clients d'AvePoint](#).

Comment acheter des produits AvePoint

+33 (1) 70 61 02 17 | SalesFR@avepoint.com | N'attendez plus pour démarrer votre essai gratuit: www.avepointonlineservices.com
AvePoint France | 235 Avenue Le Jour Se Lève | 92100 Boulogne Billancourt