



AvePoint

Policies & Insights

For Microsoft 365

Recherchez, hiérarchisez, corrigez et appliquez les contrôles de sécurité **Microsoft 365**.



Sécurisez la collaboration Microsoft 365



Rechercher & Hiérarchiser

Globalisez les accès, les données sensibles et l'activité dans Microsoft 365. Hiérarchisez les problèmes en fonction de la façon dont vous définissez les risques, conformément aux réglementations en vigueur et aux stratégies de sécurité.

Les aperçus exposent vos principales préoccupations, qu'ils soient le contenu sur la zone partagé, les liens anonymes ou les utilisateurs fantômes !



Surveiller & Corriger

Les tableaux de bord de sécurité soulignent les liens anonymes risqués, le contenu sensible surexposé et plus. Analysez les problèmes potentiels et connus pour un meilleur aperçu. Corrigez les problèmes lorsque vous modifiez les permissions et les paramètres de partage en bloc.

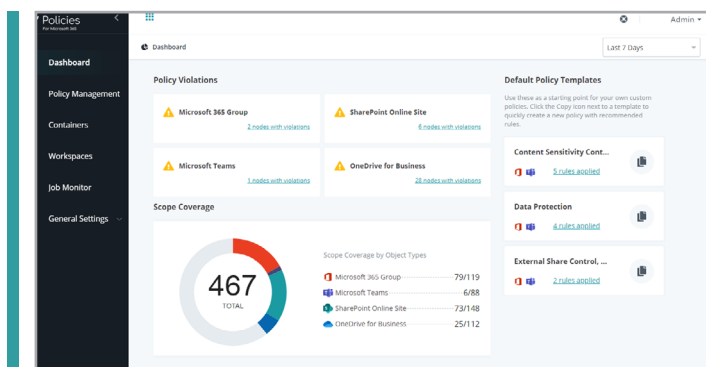


Appliquer & Empêcher

Empêchez la dérive de configuration avec les stratégies automatisées. Les stratégies déclenchent des alertes ou la restauration des modifications non autorisées et des actions risquées. Suivez les améliorations au fur et à mesure pour prouver que votre collaboration est sûre.

Les meilleures histoires mènent à des stratégies plus fortes

PI facilite l'exécution des rapports de sécurité à l'échelle de l'utilisateur. Mais comment savez-vous s'il y a un problème ? PI transforme les rapports de sécurité traditionnels en ajoutant du contexte. La globalisation des données de sensibilité et d'activité dans Microsoft Teams, groups, SharePoint et OneDrive garantit que vos problèmes les plus critiques soient hiérarchisés. Ensuite, modifiez les permissions et les paramètres en bloc et définissez les stratégies à appliquer automatiquement. Tous vos espaces de travail sont entièrement sécurisés.



INSIGHTS

- Agrégez les permissions Microsoft 365 et les données de sécurité avec les types d'activité et d'informations sensibles
- Créez des rapports sur les données de permissions dans votre « locataire » ou analysez Teams, Groups, SharePoint et OneDrive pour surveiller des services spécifiques ou des utilisateurs
- Les problèmes critiques sont hiérarchisés en fonction de la manière dont vous définissez les risques – basé sur les types d'informations sensibles et votre définition du risque
- Sélectionnez dans les modèles d'informations sensibles de Microsoft adaptée à votre industrie ou votre région, ou créez la vôtre dans les centres de conformité et de sécurité Microsoft 365
- Utilisez nos définitions d'exposition recommandées, ou ajustez les paramètres de grands groupes et des utilisateurs externes
- La hiérarchisation des risques souligne d'abord les problèmes hautement prioritaires, tel que le contenu sensible, surexposé ou les liens anonymes qui n'expirent pas
- Analysez les problèmes potentiels ou connus, et apportez des modifications directement dans des rapports à l'aide du contexte complet de l'historique des activités et de la sensibilité du contenu
- Prendre des mesures individuelles ou en bloc pour cesser, supprimer ou modifier les permissions accordées aux utilisateurs externes, aux utilisateurs fantômes ou via des liens anonymes
- Les tableaux de bord de sécurité démontrent les risques réduits et les progrès au fil du temps pour les liens anonymes, l'accès des utilisateurs externes et les utilisateurs fantômes

STRATÉGIES

- Définissez les stratégies en fonction des aperçus ou des instructions de votre société qui sont appliqués automatiquement
- Appliquez les stratégies à Microsoft Teams, groupes Microsoft 365, SharePoint et à OneDrive pour conserver les collaborations sécurisées
- Alertez ou annulez les modifications apportées aux stratégies à une période qui peut descendre à 15 minutes
- Les stratégies sont déclenchées selon les données du flux d'activité
- Plus de 20 stratégies prédéfinies peuvent être configurées en quelques clics, vous pouvez donc appliquer, sélectionner vos règles aux espaces de travail en fonction du contexte, tel que les types d'informations sensibles ou de métadonnées :
 - Application de la classification
 - Restriction de création
 - Paramètres du partage externe
 - Restriction de suppression
 - Restriction de nombre d'objets de bibliothèque/liste
 - Protection de l'héritage des permissions
- Restriction d'adhésion/de propriété
- Visibilité du groupe dans Outlook
- Restriction du nombre de propriétaires
- Membres du groupe prédéfinis (via l'intégration de la Cloud Governance)
- Analyse des utilisateurs externes
- Restriction du nombre d'administrateurs de la collection de sites
- Restriction de confidentialité
- Paramètres de la demande d'accès
- Restriction de téléchargement et de création du contenu
- Restriction de propriétaire/d'administrateur de la collection de sites
- Paramètre du partage externe du contenu du site
- Restriction de groupe/d'utilisateur

Pour obtenir une liste complète des nouvelles fonctionnalités de cette publication, veuillez consulter nos [notes de publication](#) (en anglais).

Comment acheter les produits AvePoint

+33 (1) 70 61 02 17 | Sales.FR@avepoint.com

Commencer votre essai gratuit aujourd'hui : www.avepointonlineservices.com

AvePoint France | 235 avenue le jour se lève | 92100 Boulogne-Billancourt | France