

Comparaison des fonctionnalités DSPM

[Planifier une DRA](#)

PRINCIPALES FONCTIONNALITÉS DE DSPM	FORCEPOINT	VARONIS	CYERA	BIGID	RUBRIK	MICROSOFT
Moteurs de classification d'IA et de ML	●	●	●	●	●	●
Données structurées	●	●	●	●	●	●
Données non structurées	●	●	●	●	●	●
Apprentissage personnalisé de modèles d'IA pour des besoins uniques en matière de données	●	○	○	○		○
Capacité d'installation et de gestion sur site	●	●		●	●	
Basé sur SaaS (natif du cloud)	●	●	●	●	●	●
Tableau de bord interactif détaillé avec le niveau de risque, les autorisations, les lieux, etc.	●	●	●	●	●	○
Rapports OOTB pour l'état de préparation général et les règles de conformité spécifiques	●	●	●	●	●	●
Visualisation des autorisations et des accès des utilisateurs pour chaque fichier de données non structurées classifié	●	●	●	●	●	○
Analyse des fichiers non structurés redondants, obsolètes et inutiles (ROT)	●	●	●	●	●	○
Intègre des fonctions de remédiation et de gestion de workflows ne dépendant pas d'outils tiers	●	●	●	●	●	●
Suite analytique avancée pour la sécurité et la classification avec des tableaux de bord personnalisés	●	○	●	●	●	○
Connecteurs de sources de données étendus pour les sources de données dans le cloud et sur site	●	●	●	●	●	●
Analyse des données surexposées pour les données partagées internes et externes	●	●	●	●	●	●

PRINCIPALES FONCTIONNALITÉS DE DSPM	FORCEPOINT	VARONIS	CYERA	BIGID	RUBRIK	MICROSOFT
Identification et rapport sur les doublons de données critiques à risque	●	●	●	●	●	○
Personnalisation des rapports et création d'analyses pour l'utilisateur final, sans code	●	○	●	●	○	○
Identification des utilisateurs présentant des profils à risque élevé et ayant accès à des informations cruciales	●	●	●	●	○	●
Visibilité sur les accès et les autorisations via les intégrations Active Directory et IRM	●	●	●	●	●	●
Possibilité d'associer des tags à MPIP pour ajouter une couche supplémentaire de granularité de la classification	●	●	●	●	●	●
Étiquetage des données de tous les fichiers scannés et classifiés avec des étiquettes lisibles DLP	●	●	●	●	●	●
S'intègre à DLP pour fournir des empreintes digitales en ligne pour les données non structurées (IDM)	●	○	○	○		●
Un système d'alerte avancé détecte et signale toute anomalie ou violation potentielle	●	●	●	●	●	●
Déduplication des données pour archiver ou supprimer les fichiers à risque	●	●	○		●	●
Fonctions de gestion des tâches pour les dépositaires et les propriétaires de données	●	●	●	●		●
Analyse d'exposition aux données des ransomwares	●	●	○	●	●	●
Accès simplifié aux données pour les personnes concernées Recherche de demandes d'accès aux données (DSAR) pour une conformité plus rapide aux exigences de confidentialité	●	●	●	●	○	●
Déploiement sans agent	●	●	●	●	●	○
Compatible avec les environnements isolés (air gap)	●	●		●	●	○

AVERTISSEMENT : cette comparaison des produits est basée sur les fonctionnalités natives et les intégrations entre solutions du même fournisseur, disponibles en août 2025. Les comparaisons n'incluent pas les intégrations avec des fournisseurs tiers. Cette comparaison des fonctionnalités s'appuie sur les versions les plus récentes des solutions de chaque fournisseur, disponibles en août 2025. Les informations sont basées sur des données collectées sur des sites Web et des forums publics, des articles d'analyses et des fiches techniques de produits en date d'août 2025.