

# Advanced Data Loss Prevention (DLP)

## pour Acronis Cyber Protect Cloud

### Protégez facilement et rapidement les données sensibles de vos clients

Depuis des années, les entreprises peinent à protéger leurs données sensibles contre les accès non autorisés et l'exfiltration via des attaques externes ou des risques internes (problèmes de configuration informatique, erreurs humaines, menaces, etc.). Ceux-ci peuvent avoir des conséquences fâcheuses : médiatisation embarrassante, perte de confiance des clients et des partenaires, chute du cours des actions, problèmes au niveau des RH et sanctions réglementaires.

Malheureusement, de nombreux obstacles continuent d'empêcher la plupart des entreprises (à l'exception

des plus grandes) d'adopter une solution DLP : complexité, coûts de déploiement, long retour sur investissement (dû au fait que les stratégies DLP ne sont pas universelles mais propres à chaque entreprise), etc.

En alliant provisionnement, configuration et gestion aisés, Acronis Advanced DLP vous permet de protéger les ressources de vos clients contre les fuites de données et de renforcer leur conformité réglementaire. Une technologie exclusive, axée sur les comportements, crée automatiquement et ajuste en continu les stratégies propres à chaque entreprise. Elle peut être déployée rapidement et ne nécessite aucune équipe pour sa maintenance, ni un doctorat en droit sur la protection de la vie privée.

### Étoffez vos offres de services avec une solution DLP rationalisée

Contrôles DLP sensibles au contenu sur plus de 70 canaux	Création et renforcement automatiques de stratégies DLP axées sur les comportements	Amélioration de la réactivité face aux événements DLP		
Protégez les données sensibles des ressources de vos clients en prévenant leur fuite via les périphériques et communications réseau grâce à l'analyse du contenu et du contexte des transferts de données et à l'application de contrôles préventifs axés sur les stratégies.	Épargnez-vous l'examen approfondi des processus des clients et la configuration manuelle de stratégies. Les flux de données sensibles sont automatiquement surveillés et analysés pour créer et ajuster en continu les stratégies DLP en fonction de l'évolution des besoins des clients. Ces derniers sont ainsi protégés contre les causes les plus fréquentes de fuite de données.	Réduisez le délai de résolution, accélérez les investigations numériques et simplifiez la maintenance des stratégies DLP grâce à la centralisation des journaux d'audit et des alertes de sécurité en temps réel. Simplifiez le reporting grâce à des widgets riches en informations.		
Création de nouvelles opportunités d'accroissement de la rentabilité	Réduction des efforts	Limitation des risques de fuite de données et renforcement de la conformité	Application de stratégies propres à chaque client	Amélioration de la réactivité face aux événements DLP
Améliorez vos revenus par client et attirez une plus large clientèle grâce à des services DLP managés (ou une solution DLP pour les RVA) accessibles aux petites et moyennes entreprises.	Étoffez vos offres avec un service DLP pour optimiser vos efforts sans accroître la complexité de gestion, les coûts ni les effectifs.	Détectez et prévenez les fuites d'informations sensibles sur un large éventail de canaux locaux et réseau.	Analysez les flux de données sensibles pour déployer des stratégies propres à chaque client.	Intervenez rapidement en cas d'événement DLP et profitez de puissantes fonctionnalités d'audit avec alertes et journalisation axées sur les stratégies dans un journal d'audit centralisé.

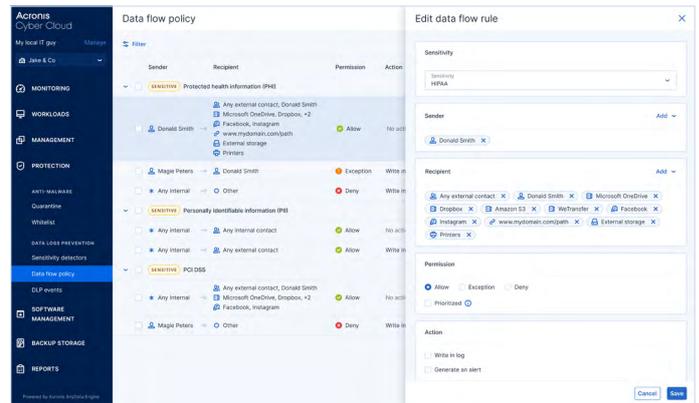
## Chronologie de provisionnement des services avec Advanced DLP

10 minutes ●	~ 2 à 6 semaines ●	~ 1 à 2 jours ●	Automatique ●	~ 1 à 3 heures par mois et par client ●
Déploiement de l'agent Acronis Cyber Protect Cloud	Création initiale de stratégies DLP	Validation des stratégies avec les clients	Renforcement automatique des stratégies	Reporting et optimisation

### Avantages du pack Advanced DLP

Protection complète qui répond aux exigences des clients avec une simplicité inégalée :

- Advanced DLP protège les données sensibles transférées via différentes communications utilisateur et système, y compris les communications réseau telles que les messageries instantanées et les périphériques comme les clés USB.
- Il propose des classificateurs de données sensibles prêts à l'emploi pour la conformité réglementaire (RGPD, HIPAA, PCI DSS, etc.).
- Il analyse les flux de données sensibles sortants pour créer et ajuster en continu les stratégies. Les clients sont ainsi protégés contre les causes les plus fréquentes de transfert de données à des parties non autorisées.
- Advanced DLP garantit une surveillance permanente des incidents DLP grâce à diverses options d'application des stratégies.
- Il permet un ajustement automatisé et continu des stratégies en fonction des besoins.
- Il réduit le délai de résolution et accélère les investigations numériques après une compromission grâce à de puissantes fonctionnalités d'audit et de journalisation.
- Il utilise la console et l'agent Acronis Cyber Protect Cloud unifiés pour garantir une bonne visibilité et classification des données.



### Canaux contrôlés

- Supports de stockage amovibles
- Imprimantes
- Lecteurs mappés redirigés
- Presse-papiers redirigés
- E-mails SMTP, Microsoft Outlook (MAPI), IBM Notes (NRPC)
- 7 messageries instantanées
- 16 services de messagerie Web
- 28 services de partage de fichiers
- 12 réseaux sociaux
- Partages de fichiers locaux, accès Web et transferts de fichiers FTP

### Principales caractéristiques

- Règles DLP personnalisables par type de fichier
- Contrôles DLP sensibles au contexte et au contenu
- Création et renforcement automatiques des stratégies DLP
- Classificateurs de données prédéfinis pour les informations d'identification personnelle, les données médicales protégées, les données PCI DSS et celles classées confidentielles
- Application stricte et adaptative des stratégies DLP
- Prise en charge du contournement du blocage des stratégies si des exceptions sont requises
- Contrôle des transferts de données indépendant du navigateur Web
- Moteur de reconnaissance optique des caractères (OCR) intégré à l'agent
- Alertes en temps réel
- Journalisation et génération d'alertes axées sur les stratégies
- Journal d'audit centralisé natif au cloud
- Visionneuse d'événements DLP avec fonctionnalités de filtrage et de recherche simplifiées
- Reporting riche en informations
- Notifications à l'écran pour les utilisateurs finaux