

# Proofpoint Cloud DLP

Visibilité et contrôle sur les données sensibles dans les applications cloud

## Principaux avantages

- Dotez-vous de visibilité sur les menaces cloud, les mouvements de données suspects, l'exposition des données cloud et l'utilisation à risque des applications cloud.
- Protégez les données sensibles au moyen de fonctionnalités de prévention des fuites de données (DLP) qui couvrent à la fois le contenu, le comportement et la télémétrie des menaces.
- Simplifiez les opérations DLP au niveau du cloud, de la messagerie, du Web et des endpoints grâce à un gestionnaire d'alertes unifié.
- Protégez-vous contre les prises de contrôle de comptes, les utilisations abusives d'applications OAuth, les accès persistants et les attaques basées sur des fichiers.
- Détectez les risques internes liés au cloud à l'aide de modèles d'apprentissage automatique conçus pour détecter les téléchargements, partages et exfiltrations de données inhabituels.
- Accélérez la correction avec des actions automatisées qui suppriment les partages, limitent les autorisations, verrouillent les comptes, révoquent l'accès OAuth et neutralisent les risques.

Grâce à son approche centrée sur les personnes, Proofpoint Cloud DLP protège vos données sensibles et vos utilisateurs contre les menaces cloud. Il aide les entreprises à surveiller l'exposition des données, à gouverner l'utilisation des services SaaS et à contrôler l'accès aux applications OAuth tierces.

La sécurité du cloud doit commencer par la sécurisation des applications approuvées par l'équipe informatique qui contiennent vos données les plus critiques, telles que Microsoft 365, Google Workspace, Salesforce ou Box. Proofpoint Cloud DLP vous dote d'une visibilité centrée sur les personnes sur les menaces cloud, l'exposition des données aux risques, le comportement des utilisateurs et les transferts de données. Cette visibilité contribue à établir et à préserver une sécurité cloud robuste.

Intégré à la plate-forme de sécurité des données Proofpoint, Cloud DLP corrèle les menaces et le comportement des utilisateurs, et applique des règles DLP cohérentes aux applications cloud, à la messagerie, au Web et aux endpoints.

Proofpoint Cloud DLP vous aide à prévenir le partage excessif et les fuites de données sensibles, à atténuer les risques internes et à limiter les comportements à risque des utilisateurs. Vous pouvez ainsi vous protéger contre les attaques de prise de contrôle de comptes, les fichiers malveillants et l'utilisation abusive d'OAuth.

## Extension de la visibilité centrée sur les personnes aux applications cloud

Proofpoint Cloud DLP vous dote de visibilité sur les menaces cloud et email. Son approche centrée sur les personnes vous permet d'identifier vos VAP (Very Attacked People™, ou personnes très attaquées) et de protéger leurs données et comptes cloud. Vous pouvez identifier les fichiers qui enfreignent les règles DLP, mais aussi les utilisateurs qui en sont propriétaires ainsi que tous ceux qui les téléchargent, les partagent et les modifient. En outre, ses outils d'analyse et contrôles adaptatifs performants vous aident à octroyer les niveaux d'accès appropriés aux utilisateurs et aux applications OAuth tierces en fonction des facteurs de risque les plus importants à vos yeux.

# Protection des utilisateurs, des applications et des données contre les menaces cloud

Proofpoint Cloud DLP associe le contexte utilisateur avec la threat intelligence multicanale de Proofpoint Behavior Graph. L'apprentissage automatique et la corrélation des menaces vous aident à déterminer lorsqu'un compte cloud a été compromis et est utilisé pour des activités suspectes — par exemple l'envoi ou le transfert d'emails ou l'exfiltration de données.

Le tableau de bord intuitif de Proofpoint Cloud DLP vous permet d'examiner les alertes concernant les connexions suspectes, les activités liées aux fichiers et les fonctions d'administration. Vous pouvez exporter des données d'investigation numérique vers une solution SIEM pour des analyses ultérieures, manuellement ou à l'aide d'API REST.

Grâce aux règles robustes, aux alertes en temps réel et aux réponses automatisées de Proofpoint Cloud DLP, vous pouvez :

- Protéger votre environnement contre la prise de contrôle des comptes cloud et suspendre les comptes compromis
- Implémenter une authentification basée sur les risques et des contrôles d'accès adaptatifs
- Prévenir le vol de données et l'utilisation abusive d'applications OAuth en identifiant et en révoquant les accès tiers à risque
- Détecter et mettre en quarantaine les

fichiers malveillants

- Supprimer les autorisations et partages de fichiers inappropriés
- Limiter l'accès aux contenus sensibles
- Verrouiller les comptes utilisateurs et automatiser les flux de correction
- Examiner et neutraliser les activités suspectes sur les comptes cloud

Proofpoint Cloud DLP permet également d'identifier les risques internes au niveau du cloud. Des modèles d'apprentissage automatique spécialisés détectent les comportements souvent associés aux menaces internes et aux collaborateurs quittant une entreprise. Citons par exemple des téléchargements anormaux, des partages excessifs, des tendances inhabituelles d'accès aux données ou encore l'exfiltration potentielle de données par comparaison avec les activités de référence au niveau des utilisateurs ou de l'entreprise dans son ensemble.

Le module complémentaire SaaS Isolation vous permet également de protéger les utilisateurs, d'appliquer des règles DLP aux terminaux non gérés et d'intégrer votre solution de gestion des identités via l'authentification SAML (Security Assertion Markup Language).

## Règles DLP unifiées sur tous les canaux

Proofpoint Cloud DLP partage des classificateurs DLP avec d'autres solutions de sécurité des données Proofpoint. Il s'agit notamment d'identifiants intelligents intégrés, de dictionnaires, de règles, de modèles et de classificateurs personnalisés autonomes (ACC) qui utilisent des grands modèles de langage (LLM) pour découvrir et classer automatiquement le contenu sensible propre à l'entreprise.

Ce partage vous aide à identifier et à protéger les données sensibles plus rapidement. Dans le cadre de la plate-forme de sécurité des données Proofpoint, vous pouvez déployer des règles DLP cohérentes sur les applications SaaS, la messagerie, le Web et les endpoints.

La solution combine les données d'analyse des contenus, des comportements et des menaces de ces canaux. Vous pouvez ainsi déterminer si l'utilisateur qui a déclenché

l'alerte DLP a été victime d'une compromission, a des intentions malveillantes ou est simplement négligent. De même, vous pouvez unifier la gestion des alertes DLP sur plusieurs canaux.

Plus de 240 classificateurs intégrés couvrent les données relevant de la norme PCI, du RGPD et des réglementations sur les données personnelles et les données médicales personnelles. Les technologies de détection avancées vous aident à créer des contrôles sur mesure, tels que la correspondance exacte des données et des règles contextuelles. De plus, vous pouvez restreindre l'accès aux données depuis des terminaux non gérés, empêcher les téléchargements de fichiers sensibles vers des applications cloud non approuvées et limiter les autorisations de partage excessives. Vous pouvez également identifier les fichiers sensibles largement exposés et corréler les activités de connexion suspectes avec les incidents DLP.

# Gouvernance des applications cloud et tierces

Proofpoint Cloud DLP met en évidence le Shadow IT et découvre les applications cloud au sein de votre entreprise. Notre catalogue compte 46 000 applications, chacune possédant plus de 50 attributs. Vous pouvez classer les applications cloud par type et score de risque, ce qui vous aide à évaluer les risques de sécurité, les vulnérabilités en termes de fuites de données et les lacunes de conformité. Vous pouvez bloquer les applications à risque ou accorder aux utilisateurs des accès en lecture seule à celles-ci.

La solution détecte et évalue également les autorisations OAuth pour les applications tierces qui accèdent aux services cloud de base approuvés par l'équipe informatique. Sa fonction d'analyse permet d'identifier les applications à risque et de réduire votre surface d'attaque. Vous pouvez définir ou automatiser certaines actions en fonction du score de risque et du contexte.

## Déploiement rapide

Notre architecture multimodale vous permet de rentabiliser plus rapidement votre investissement. En moins de quatre semaines, vous pouvez intégrer la solution avec des API cloud, des outils hybrides de gestion des identités et des produits d'orchestration de la sécurité (dont Proofpoint Threat Response).

Cette intégration vous permettra de détecter automatiquement les menaces, de les contenir et de sécuriser les données. L'authentification SAML basée sur les risques et la fonction SaaS Isolation contribuent à bloquer les accès non autorisés aux applications d'entreprise et prennent en charge les stratégies BYOD.

# Les atouts de Proofpoint Cloud DLP

Proofpoint Cloud DLP associe, dans une solution unique, la protection des données, la défense contre les menaces cloud, la détection des risques internes, la visibilité sur l'exposition des données cloud et des contrôles adaptatifs centrés sur les personnes. En intégrant l'activité cloud, le comportement des utilisateurs, la threat intelligence et la télémétrie DLP, les entreprises peuvent mieux protéger les informations sensibles tout en réduisant la complexité opérationnelle.

## En savoir plus

Pour plus d'informations, visitez notre site à l'adresse : [proofpoint.com/fr](https://proofpoint.com/fr)

**À propos de Proofpoint, Inc.** Proofpoint, Inc. est un leader mondial de la cybersécurité centrée sur les personnes et les agents, qui sécurise la manière dont les personnes, les données et les agents d'IA se connectent via la messagerie électronique, le cloud et les outils de collaboration. Proofpoint est un partenaire de confiance pour plus de 80 entreprises du classement Fortune 100, plus de 10 000 grandes entreprises et des millions de petites entreprises. Il les aide à bloquer les menaces, à prévenir les fuites de données et à renforcer la résilience des personnes et des workflows d'IA. La plate-forme de collaboration et de sécurité des données de Proofpoint aide les entreprises de toutes tailles à protéger et à responsabiliser leurs collaborateurs tout en adoptant l'IA en toute sécurité et en toute confiance. Pour en savoir plus, consultez le site [proofpoint.com/fr](https://proofpoint.com/fr).

Suivez-nous : [LinkedIn](#)

Proofpoint est une marque déposée ou un nom commercial de Proofpoint, Inc. aux États-Unis et/ou dans d'autres pays. Toutes les autres marques citées dans ce document sont la propriété de leurs détenteurs respectifs.

**proofpoint**<sup>®</sup>

