Lookout

Lookout Cloud Security Platform Data Loss Prevention

Découvrez, évaluez et protégez vos données avec un DLP natif dans le cloud

Une approche intégrée du DLP

Les exigences de sécurité des données dans le cloud continuent de mûrir rapidement, sous l'impulsion de facteurs tels que les avantages opérationnels inhérents de l'infrastructure cloud et l'expansion spectaculaire de la main-d'œuvre à distance. Alors que la plupart des applications cloud et SaaS offrent des contrôles de sécurité embarqués, les praticiens ont besoin de capacités de prévention des pertes de données (DLP) dédiées et centralisées qui offrent une protection avancée pour prendre en charge des cas d'utilisation complexes sur plusieurs plates-formes. En d'autres termes, les organisations ont besoin d'une plateforme DLP qui s'intègre à l'ensemble des solutions pour protéger les données sur les applications privées, Internet et cloud.

Protégez les données lors de leur déplacement

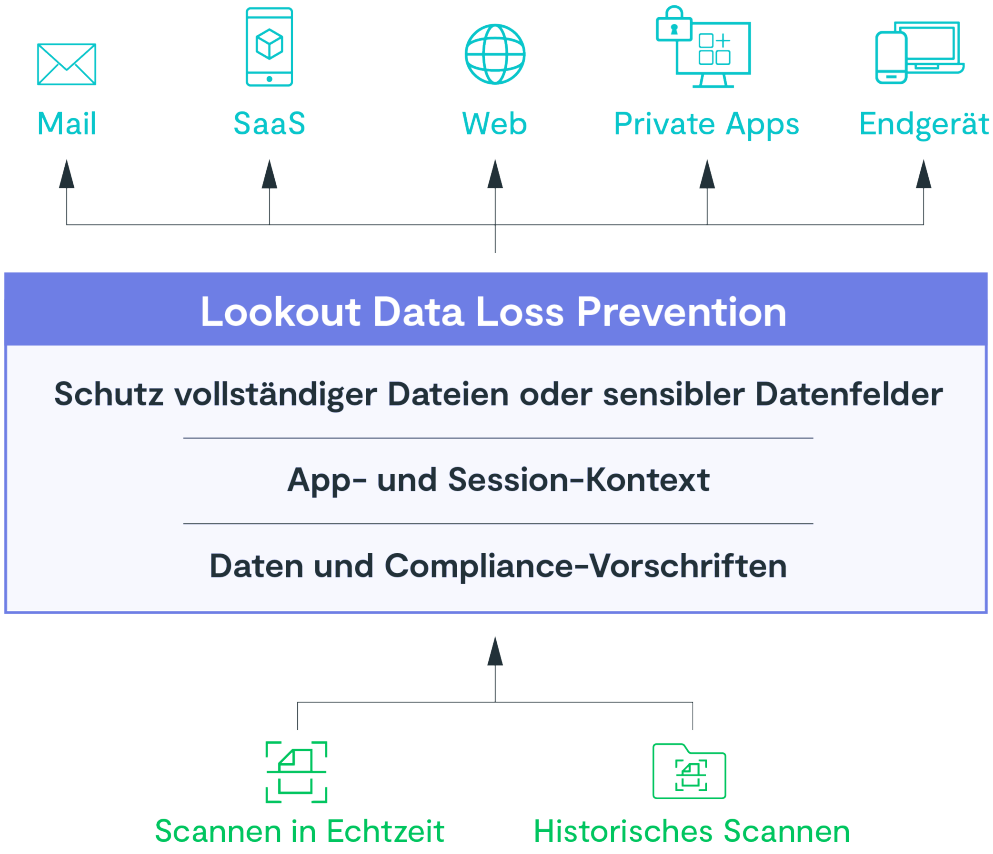
La plateforme de sécurité cloud de Lookout offre des capacités DLP robustes conçues pour protéger les données sensibles sur les applications cloud et SaaS, les applications privées, Internet et les e-mails. Lookout propose un DLP moderne et natif dans le cloud qui permet aux organisations d'appliquer des politiques de sécurité des données cohérentes et des contrôles sur l'ensemble de leurs applications d'entreprise, garantissant l'intégrité et l'accessibilité des données d'entreprise où qu'elles circulent - que ce soit sur site, dans le cloud ou consultées par des appareils gérés ou non gérés.

Aperçu du DLP de Lookout

- Sans agent et intégré nativement dans la plateforme
- Couverture des ensembles de données historiques et en temps réel
- Plus de 1100 modèles de politiques prédéfinis et personnalisables pour de nombreux types de données
- Prise en charge de nombreux types de données structurées et non structurées et de formats de document
- Détection avancée des données incluant les modes OCR, API, proxy et d'inspection des e-mails
- Application de politiques contextuelles qui incluent la protection pour les actions de téléchargement, de partage et de collaboration

Cas d'utilisation critiques du DLP de Lookout

- Guidage en temps réel pour les utilisateurs pour des pratiques d'application et de données plus sûres
- Détection et blocage du vol de données par des personnes malveillantes en interne
- Prévention des fuites de données accidentelles par les employés
- Prévention des fuites de données vers l'IA générative et les sites Web sociaux
- Protection des données sensibles partagées avec des partenaires et des sous-traitants



Le DLP de Lookout permet aux organisations de gérer de manière centralisée des exigences critiques, notamment :

Classification

Pour détecter et cataloguer les informations sensibles où qu'elles se trouvent

Intégration

Extension des pratiques et politiques de DLP sur site vers le cloud

Analyse des données

Couvrant toutes les compositions de données structurées et non structurées

Gestion des politiques

Fourniture d'une protection et d'une conformité transversales et cohérentes entre les applications

Visualisation

Dans tous les types d'accès aux données, y compris le contexte utilisateur et l'appareil, ainsi que la manipulation

Principales fonctionnalités

Découverte : Obtenez une visibilité claire sur l'emplacement de vos données - au repos et en mouvement

Découverte des données dans le cloud
La découverte des données dans le cloud analyse à la fois les ensembles de données en temps réel et historiques pour identifier les informations sensibles stockées dans les applications cloud. Cela aide les organisations à obtenir une visibilité sur les données résidant dans leurs environnements cloud afin de classer et de protéger les données sensibles, d'appliquer des politiques de DLP et de garantir la conformité. Les organisations peuvent identifier de manière proactive les informations non protégées et les partages de fichiers ouverts afin de prendre des mesures correctives.

Évaluation : Identifier vos données, le contexte où elles se trouvent et leurs interactions

Classification intégrée des données
Étendez la classification et la gouvernance des données à tout document dans n'importe quel cloud, en intégrant des systèmes de classification tels que la Protection des informations (AIP) de Microsoft Azure, TITUS de Fortra et les Étiquettes de classification de Google. En utilisant le moteur de politique unifié, les informations sensibles sont identifiées et protégées de manière cohérente, y compris les données structurées et non structurées, pour identifier le contenu dans tous les formats. Les organisations obtiennent une visibilité et une protection complètes sur plusieurs applications, utilisateurs et appareils, sécurisant ainsi la propriété intellectuelle et d'autres informations protégées contre une exposition non intentionnelle aux données.

Application de politiques contextuelles
L'application de politiques contextuelles permet aux organisations de prendre des décisions d'accès intelligentes en comprenant le contenu et le contexte des échanges de données. Avec plus d'utilisateurs et de données en dehors des périmètres traditionnels, il est crucial de vérifier les niveaux de risque avant d'accorder l'accès. En utilisant la technologie d'analyse du comportement des entités utilisateur (UEBA), Lookout fournit le contexte complet nécessaire pour gérer les risques liés aux utilisateurs et détecter les anomalies avec des informations en temps réel sur le comportement des utilisateurs.

Inspection multi-mode des données
Inspectez les données dans n'importe quel mode - API, proxy ou e-mail - pour garantir une visibilité complète sur chaque ensemble de données et cas d'utilisation applicables, de la détection de données historiques invisibles à la protection de scénarios avancés tels que la collaboration dans le cloud ou l'interaction avec des partenaires externes. Surveillez le traitement dans chaque cas d'utilisation, y compris l'accès et l'utilisation d'informations sensibles à partir d'appareils gérés et non gérés pour prendre en compte la main-d'œuvre à distance.

Moteur de politique unifié
La solution DLP de Lookout offre une plateforme centralisée pour définir et appliquer des politiques de sécurité des données cohérentes, indépendamment de l'emplacement des données ou de la manière dont elles sont accessibles. Cela aide à rationaliser les flux de travail de sécurité et garantit que les informations sensibles sont protégées sur tous les appareils et emplacements.

Politiques de DLP adaptatives
La gestion et l'application centralisées des politiques de DLP sont appliquées sur chaque plateforme et application. Des politiques prédéfinies peuvent être appliquées pour aider à identifier et à classer les données sur de nombreuses applications, y compris Office365, Slack, G Suite, Box, Salesforce et AWS. Des modèles de politiques personnalisables sont disponibles pour les applications commerciales et privées, avec des politiques de conformité dédiées incluses pour couvrir le GDPR, PCI, SOX, HIPAA et autres.

Protéger : Masquer, redacter ou supprimer facilement vos données, peu importe où elles se trouvent

Large éventail d'actions de DLP
Une large gamme d'options aide à sécuriser les données dans le cloud au-delà des capacités de base d'autorisation-refus offertes par d'autres solutions de DLP. Avec Lookout, les utilisateurs peuvent contrôler la collaboration en temps réel, supprimer les partages ouverts, activer l'authentification renforcée, appliquer des étiquettes de classification des données, masquer, redacter ou chiffrer les fichiers pour protéger les données lors du téléchargement, voire mettre en place un coaching utilisateur pour sensibiliser les utilisateurs aux actions risquées.

Correspondance de données et OCR
Identifier, classer et protéger les données sensibles dans tous les formats et applications avec la Correspondance exacte des données (EDM) et le marquage. La Reconnaissance optique de caractères (OCR) détecte les fichiers image pour éviter le partage de données sensibles dans les fichiers image. Ces techniques avancées de protection des données protègent également le partage d'informations personnellement identifiables (PII), de propriété intellectuelle, financières et d'autres données sensibles, garantissant leur protection tout au long de leur cycle de vie.

Gstion des droits numériques (DRM) native
Chiffrer, masquer ou supprimer à distance les données sensibles en fonction de l'application de politiques avancées lorsque les données circulent à travers les flux de travail, les applications et même les appareils non gérés - garantissant que les informations ne sortent pas des paramètres autorisés. Empêcher les téléchargements inappropriés, le partage excessivement permissif avec des partenaires externes, et même les erreurs des employés dans la manipulation des informations les plus sensibles de votre organisation.

Intégration : Intégration transparente avec l'infrastructure existante

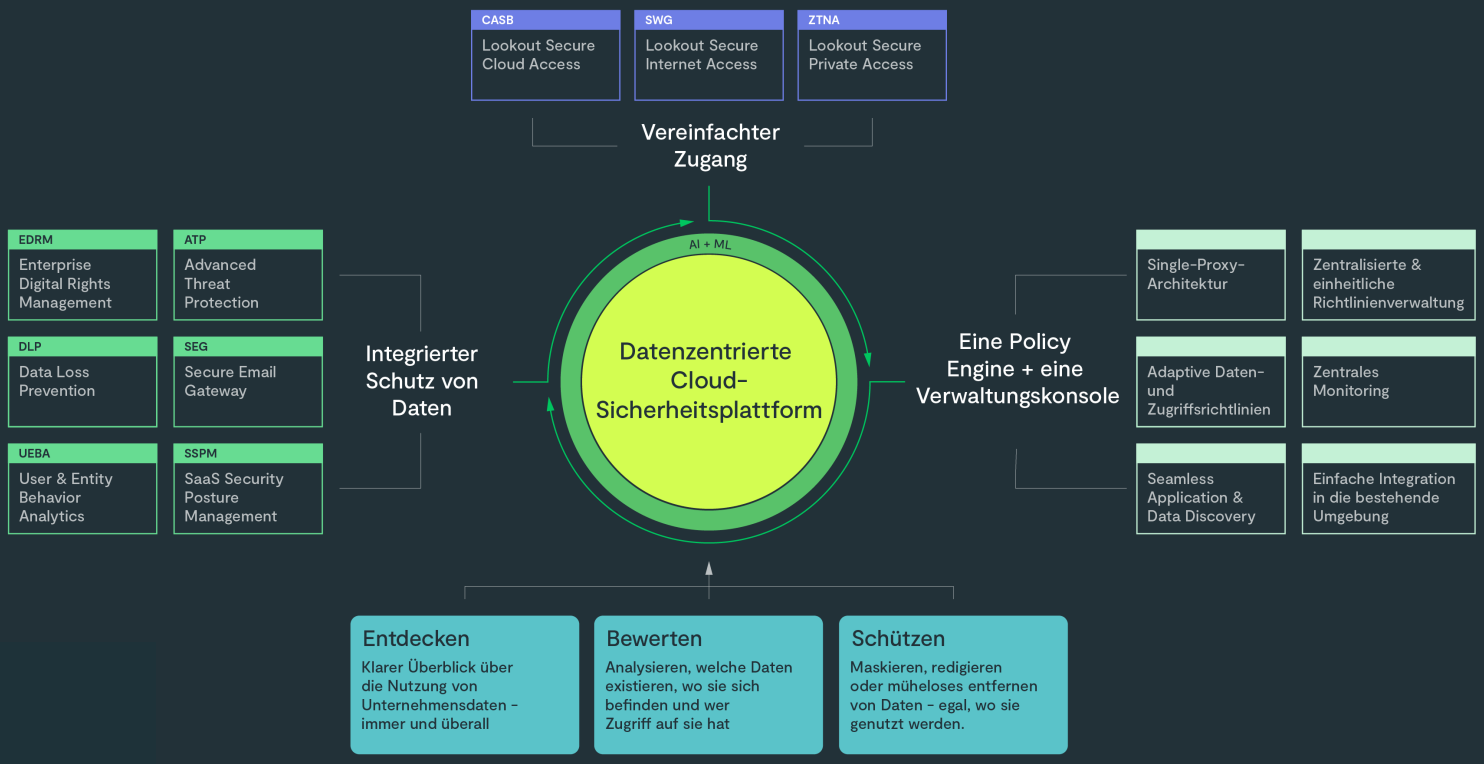
Amélioration des solutions de DLP existantes
Étendez votre solution DLP traditionnelle sur site à travers le stockage, le courrier électronique et d'autres plates-formes avec une intégration API entièrement prise en charge. Répliquez les politiques dans votre environnement cloud pour orchestrer une stratégie de DLP avec une analyse et une application de politique unifiées. Lookout s'intègre aux moteurs de DLP externes, offrant la flexibilité de scanner les données via un DLP natif, un DLP externe ou une analyse multi-niveaux. La solution DLP de Lookout s'intègre de manière transparente aux solutions de sécurité d'entreprise existantes, y compris VMware, Juniper, CloudFlare, Akamai, Okta, et plus encore, pour rationaliser les flux de travail et la posture de sécurité globale.

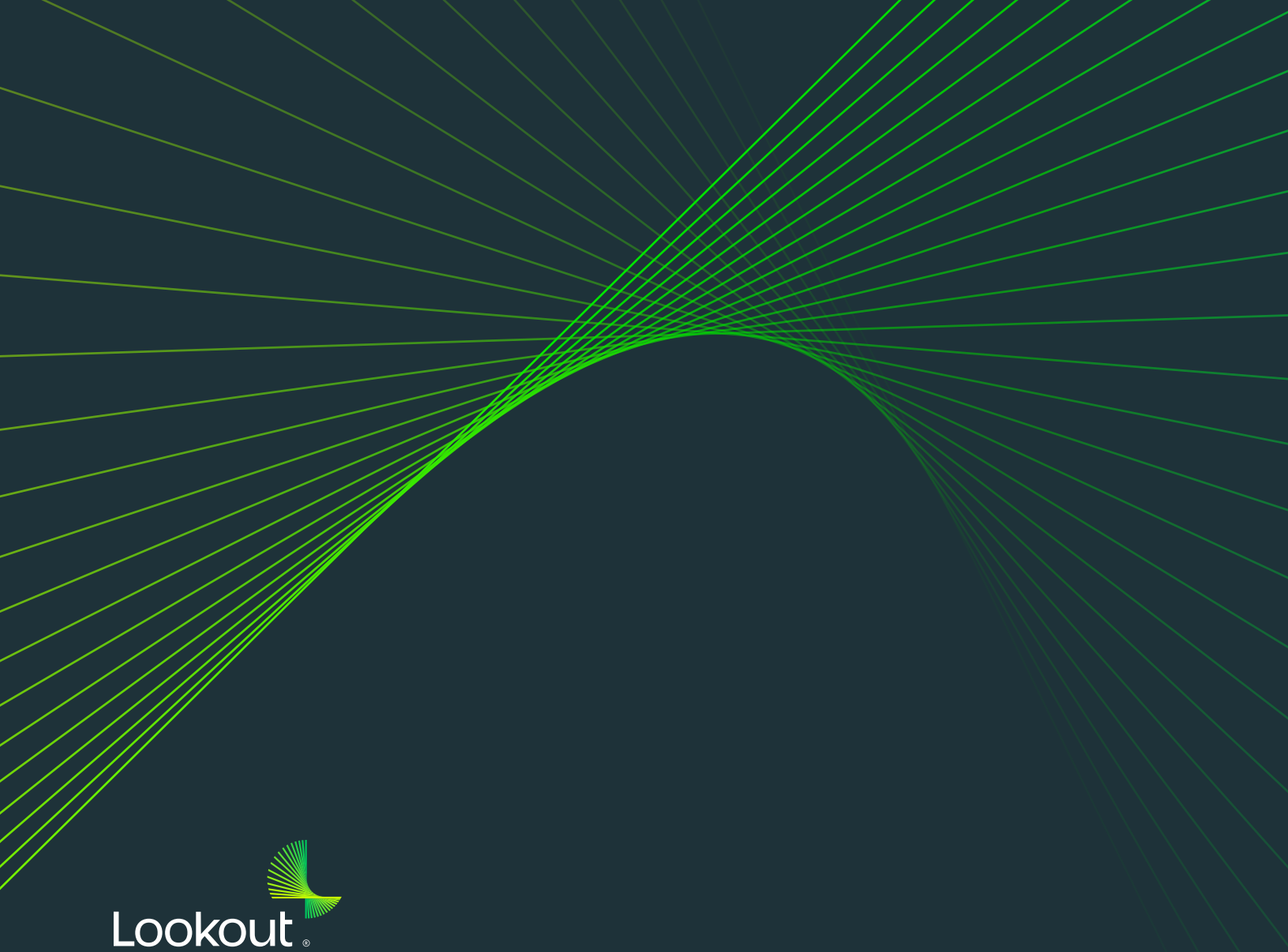
Pourquoi choisir Lookout DLP

- Conception sans agent pour un déploiement rapide et un fonctionnement efficace
- Couverture dédiée pour chaque application web, cloud et privée populaire
- Analyse centralisée à travers des environnements multi-cloud diversifiés
- Fonctionnalités EDM et OCR
- Capacités de masquage et de chiffrement des données natives SaaS Simplifiez la sécurité avec la plateforme de sécurité cloud de Lookout

En tirant parti de la technologie DLP intégrée à la plateforme de sécurité cloud de Lookout.

les organisations peuvent adopter en toute confiance les technologies cloud tout en protégeant leur actif le plus précieux - les données. Restreindre complètement l'accès aux fichiers, dossiers ou applications au nom de la sécurité n'est ni réalisable ni productif. La plateforme de sécurité cloud centrée sur les données de Lookout est conçue pour vous maintenir en contrôle tout en s'adaptant à vos besoins commerciaux et aux évolutions de votre force de travail.





À propos de Lookout

Lookout, Inc. est une entreprise de sécurité centrée sur les données qui utilise une stratégie de défense en profondeur pour traiter les différentes étapes d'une attaque de cybersécurité. Les données sont au cœur de chaque organisation, et notre approche de la cybersécurité est conçue pour protéger ces données dans le paysage moderne des menaces. En mettant l'accent sur les personnes et leur comportement, la plateforme Lookout Cloud Security Platform assure une visibilité en temps réel des menaces, et stoppe rapidement les brèches depuis les premières tentatives de phishing jusqu'à l'extraction des données. Pour en savoir plus, visitez fr.lookout.com et suivez Lookout sur notre blog, LinkedIn et X.

Pour plus d'informations, rendez-vous sur **fr.lookout.com**

Demandez une démo sur **lookout.com/request-a-demo**