Lookout

Lookout Cloud Security Platform Data Loss Prevention

Mit cloudbasierter DLP Daten analysieren und schützen

Ein integrierter Ansatz für DLP

Die Anforderungen an die Sicherheit von Daten in der Cloud entwickeln sich weiterhin rasant, was unter anderem auf die operativen Vorteile der Cloud-Infrastruktur und die drastische Ausweitung von Remote-Mitarbeitern zurückzuführen ist. Während die meisten Cloud- und SaaS-Apps integrierte Sicherheitskontrollen bieten, benötigen Unternehmen dedizierte und zentralisierte Data Loss Prevention (DLP)-Funktionen, die fortschrittlichen Schutz bieten, um komplexe Anwendungsfälle über mehrere Plattformen hinweg zu unterstützen. Einfach ausgedrückt: Sie benötigen eine DLP-Plattform, die sich in verschiedene Lösungen integrieren lässt, um Daten in privaten, Internet- und Cloud-Apps zu schützen.

Daten immer und überall schützen

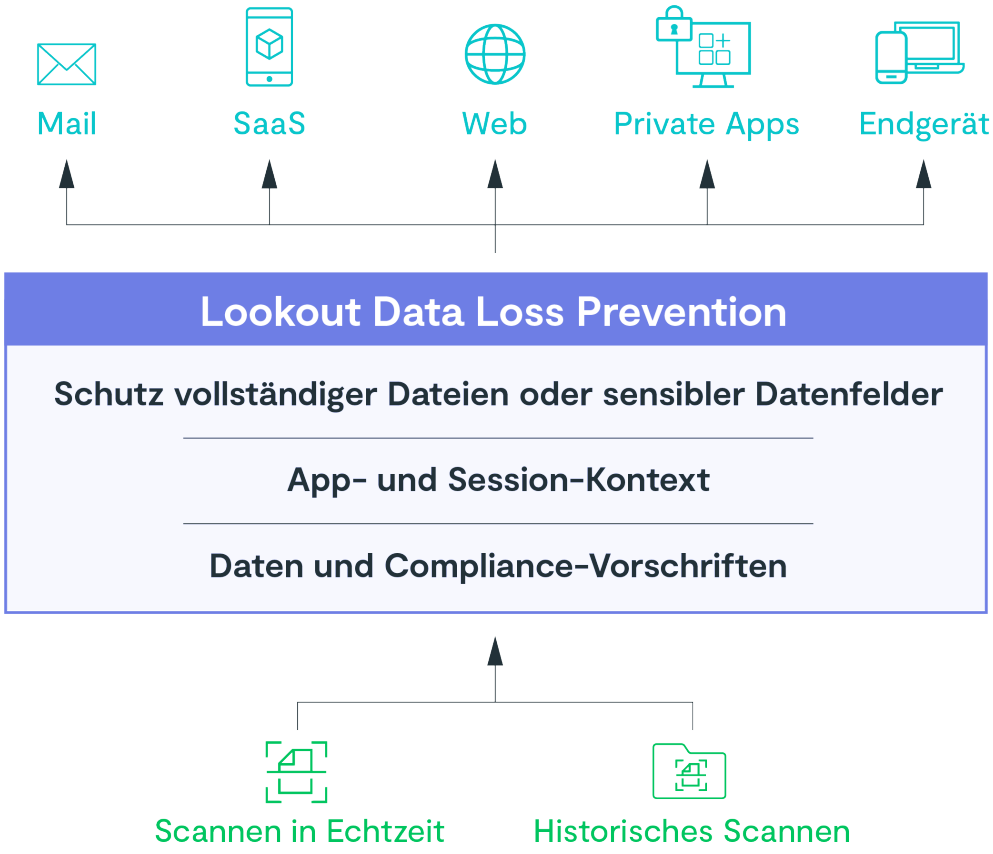
Die Lookout Cloud Security Platform bietet robuste DLP-Funktionen zum Schutz sensibler Daten über Cloud- und SaaS-Apps, private Apps, Internet und E-Mail. Lookout bietet eine moderne und Cloud-native DLP, die es Unternehmen ermöglicht, konsistente Richtlinien und Kontrollen für die Sicherheit von Daten in allen Unternehmensanwendungen umzusetzen und so die Integrität und Zugänglichkeit von Unternehmensdaten zu gewährleisten, unabhängig davon, wo sie übertragen werden - ob vor Ort, in der Cloud oder über verwaltete oder nicht verwaltete Geräte.

Lookout DLP im Überblick

- Agentenlos und nativ in die Plattform integriert
- Abdeckung von historischen als auch von Datensätzen in Echtzeit
- Mehr als 1100 vordefinierte und anpassbare Richtlinienvorlagen für viele Datentypen
- Unterstützt viele strukturierte und unstrukturierte Datentypen und Dokumentenformate
- Erweiterte Datenerkennung einschließlich OCR, API-, Proxy- und E-Mail-Prüfung
- Kontextabhängige Richtliniendurchsetzung mit Schutz für Upload-, Download-, Freigabe- und Kollaborationsaktionen

Wichtige Anwendungsfälle von Lookout DLP

- Anleitungen in Echtzeit für Nutzer zum sicheren Umgang mit Apps und Daten
- Erkennen und Blockieren von Datendiebstahl durch böswillige Insider
- Schutz vor unbeabsichtigten Datenlecks durch Mitarbeiter
- Schutz vor Datenverlusten durch KI und soziale Netzwerke
- Schutz sensibler Daten, die mit Partnern und Auftragnehmern ausgetauscht werden



Lookout's DLP ermöglicht es Unternehmen, kritische Komponenten zentral zu verwalten:

Klassifizierung

Aufspüren und Katalogisieren sensibler Informationen, wo immer sie sich befinden

Integration

Ausweitung lokaler DLP-Maßnahmen und -Richtlinien auf die Cloud

Scannen von Daten

Abdeckung aller strukturierten und unstrukturierten Datensätze

Verwaltung von Richtlinien

Einheitlicher app-übergreifender Schutz und Compliance

Visualisierung

Jede Art des Datenzugriffs, einschließlich Benutzer- und Gerätekontext, und die Verarbeitung

Zentrale Funtionen

Erkennung: Verschaffen Sie sich einen klaren Überblick darüber, wo sich Ihre Daten befinden

Erkennung von Daten in der Cloud
Cloud Data Discovery scannt sowohl Echtzeit- als auch historische Datensätze, um sensible Informationen zu identifizieren, die in Cloud-Apps gespeichert sind. Auf diese Weise erhalten Unternehmen Einblick in die in ihren Cloud-Umgebungen gespeicherten Daten, um sensible Daten zu klassifizieren und zu schützen, DLP-Richtlinien durchzusetzen und die Einhaltung von gesetzlichen Vorschriften zu gewährleisten. Unternehmen können proaktiv ungeschützte Informationen und offene Dateifreigaben identifizieren, um Korrekturmaßnahmen zu ergreifen.

Bewertung: Identifizieren Sie Daten, den Kontext in dem sie existieren und ihre Zusammenhänge.

Integrierte Datenklassifizierung
Erweitern Sie die Datenklassifizierung und -verwaltung auf jedes Dokument in jeder Cloud und integrieren Sie diese mit Klassifizierungssystemen wie Microsoft Azure's Information Protection (AIP), TITUS von Fortra und Google Classification Labels. Mithilfe der einheitlichen Richtlinien-Engine werden sensible Informationen konsistent erkannt und geschützt, einschließlich strukturierter und unstrukturierter Daten, um Inhalte in allen Formaten zu identifizieren. Unternehmen erhalten vollständige Transparenz und Schutz über Apps, Benutzer und Geräte hinweg und schützen so geistiges Eigentum und andere geschützte Informationen vor unbeabsichtigten Datenverlusten.

Kontextabhängige Durchsetzung von Richtlinien
Die kontextabhängige Durchsetzung von Richtlinien ermöglicht es Unternehmen, anhand von Informationen über den Inhalt und den Kontext des Datenaustauschs intelligente Zugriffsentscheidungen zu treffen. Da immer mehr Benutzer und Daten außerhalb der traditionellen Grenzen liegen, ist es entscheidend, das Risikoniveau zu überprüfen, bevor der Zugriff gewährt wird. Lookout nutzt UEBA-Technologie (User Entity Behavior Analytics) und bietet den vollständigen Kontext, der für das Management von Benutzerrisiken und die Erkennung von Anomalien erforderlich ist, mit Echtzeit-Einblicken in das Benutzerverhalten.

Daten in jedem Modus prüfen
Prüfen Sie Daten in jedem Modus - API, Proxy oder E-Mail -, um vollständige Transparenz in jedem anwendbaren Datensatz und Anwendungsfall zu gewährleisten, von der Erkennung ungesehener historischer Daten bis zum Schutz fortgeschrittener Szenarien wie Zusammenarbeit in der Cloud oder Interaktion mit externen Partnern. Überwachen Sie die Handhabung in jedem Anwendungsfall, einschließlich des Zugriffs auf und der Nutzung von sensiblen Informationen von verwalteten und nicht verwalteten Geräten, um Remote-Mitarbeiter zu berücksichtigen.

Einheitliche Policy Engine
Lookout DLP bietet eine zentrale Plattform zur Definition und Durchsetzung konsistenter Datensicherheitsrichtlinien, unabhängig davon, wo sich Daten befinden oder wie auf sie zugegriffen wird. Dies trägt zur Rationalisierung von Sicherheitsabläufen bei und gewährleistet, dass sensible Informationen geräte- und standortübergreifend geschützt sind.

Adaptive DLP-Richtlinien
Die zentralisierte DLP-Richtlinienverwaltung und -durchsetzung gilt für alle Plattformen und Apps. Standardrichtlinien können zur Identifizierung und Klassifizierung von Daten in vielen Apps wie Office365, Slack, G Suite, Box, Salesforce und AWS angewendet werden. Es stehen anpassbare Richtlinienvorlagen für kommerzielle und private Apps zur Verfügung, mit speziellen Richtlinien zur Einhaltung von Standards wie DSGVO, PCI, SOX, HIPAA und anderen.

Schutz: Einfaches Maskieren, Zensieren oder Entfernen von Daten - egal, wo sie sich befinden.

Umfangreiche Palette an DLP-Maßnahmen
Eine breite Palette von Optionen hilft dabei, Daten in der Cloud zu schützen, die über die grundlegenden Genehmigungs- und Ablehnungsfunktionen anderer DLP-Lösungen hinausgehen. Mit Lookout können Benutzer Zusammenarbeit in Echtzeit kontrollieren, offene Freigaben entfernen, Step-up-Authentifizierung aktivieren, Datenklassifizierungsetiketten anwenden, Dateien maskieren, redigieren oder verschlüsseln, um Daten während des Downloads zu schützen, oder sogar Benutzer-Coaching einrichten, um Benutzer über riskante Aktionen aufzuklären.

Datenabgleich und OCR
Identifizieren, klassifizieren und schützen Sie sensible Daten in jedem Format und jeder App mit Exact Data Matching (EDM) und Fingerprinting. Die OCR (Optical Character Recognition) erkennt Bilddateien, um die Weitergabe sensibler Daten über Bilddateien zu verhindern. Diese fortschrittlichen Datenschutztechniken schützen die Weitergabe von personenbezogenen Daten, geistigem Eigentum, Finanzdaten und anderen sensiblen Daten und gewährleisten so den Schutz während des gesamten Lebenszyklus der Daten.

Natives Digital Rights Management (DRM)
Verschlüsseln, maskieren oder löschen Sie sensible Daten per Fernzugriff auf der Grundlage einer fortschrittlichen Richtliniendurchsetzung, während sich die Daten über Workflows, Apps und sogar nicht verwaltete Geräte hinweg verbreiten - so stellen Sie sicher, dass die Informationen nicht außerhalb der autorisierten Parameter gelangen. Verhindern Sie unangemessene Downloads, übermäßige Freigaben für externe Partner und Fehler von Mitarbeitern im Umgang mit sensiblen Unternehmensdaten.

Integration: Nahtlose Integration in die bestehende Infrastruktur

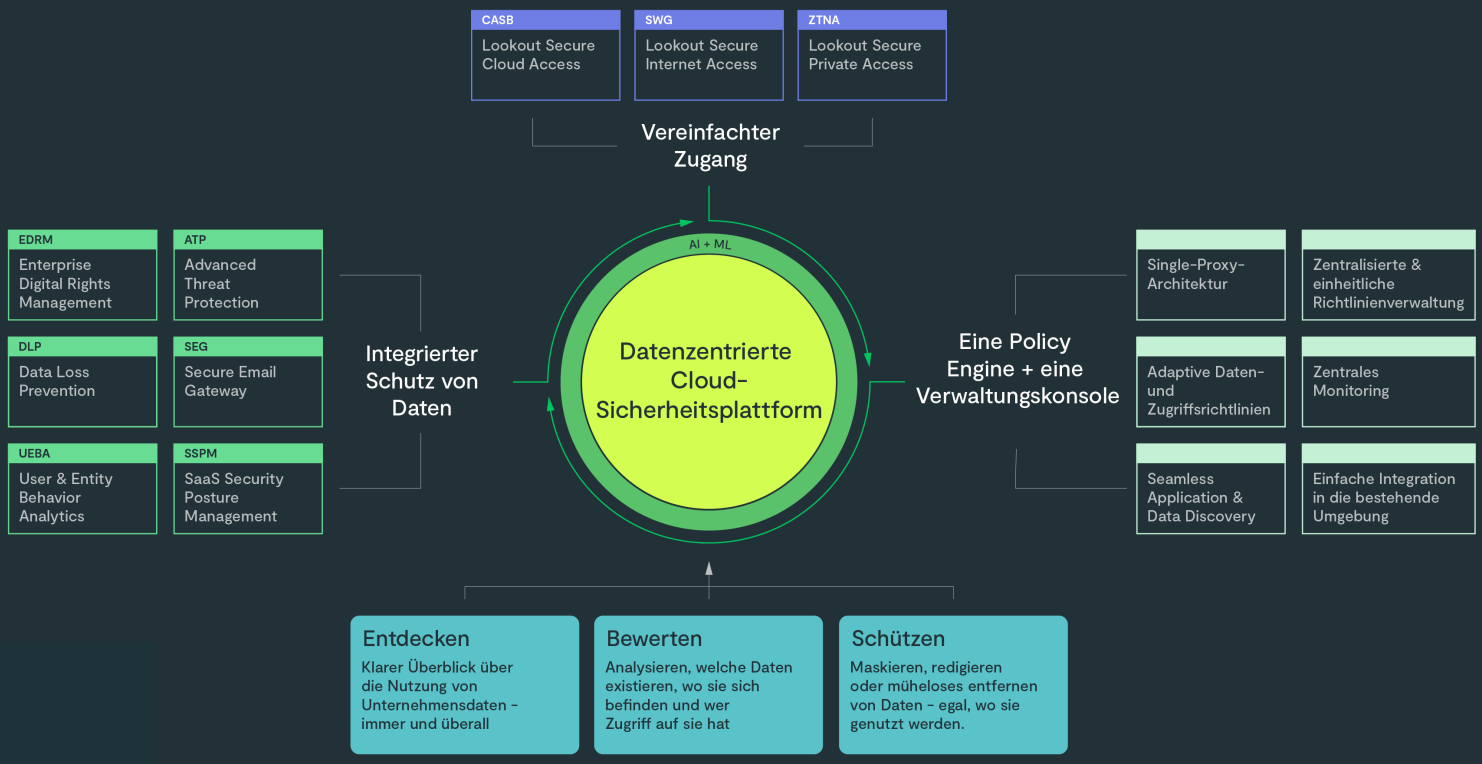
Erweiterung bestehender DLP-Lösungen
Erweitern Sie Ihr lokales DLP über Speicher-, E-Mail- und andere Plattformen mit vollständig unterstützter API-Integration. Spiegeln Sie Richtlinien in der Cloud-Umgebung, um eine DLP-Strategie mit einheitlicher Richtlinienanalyse und -durchsetzung zu ermöglichen. Lookout lässt sich mit externen DLP-Engines integrieren und bietet so die Flexibilität, Daten über native DLP, externe DLP oder einen mehrstufigen Scan zu prüfen. Lookout DLP lässt sich nahtlos in bestehende Sicherheitslösungen von Unternehmen integrieren, darunter VMware, Juniper, CloudFlare, Akamai, Okta und andere, um Arbeitsabläufe zu optimieren und die allgemeine Sicherheitslage zu verbessern.

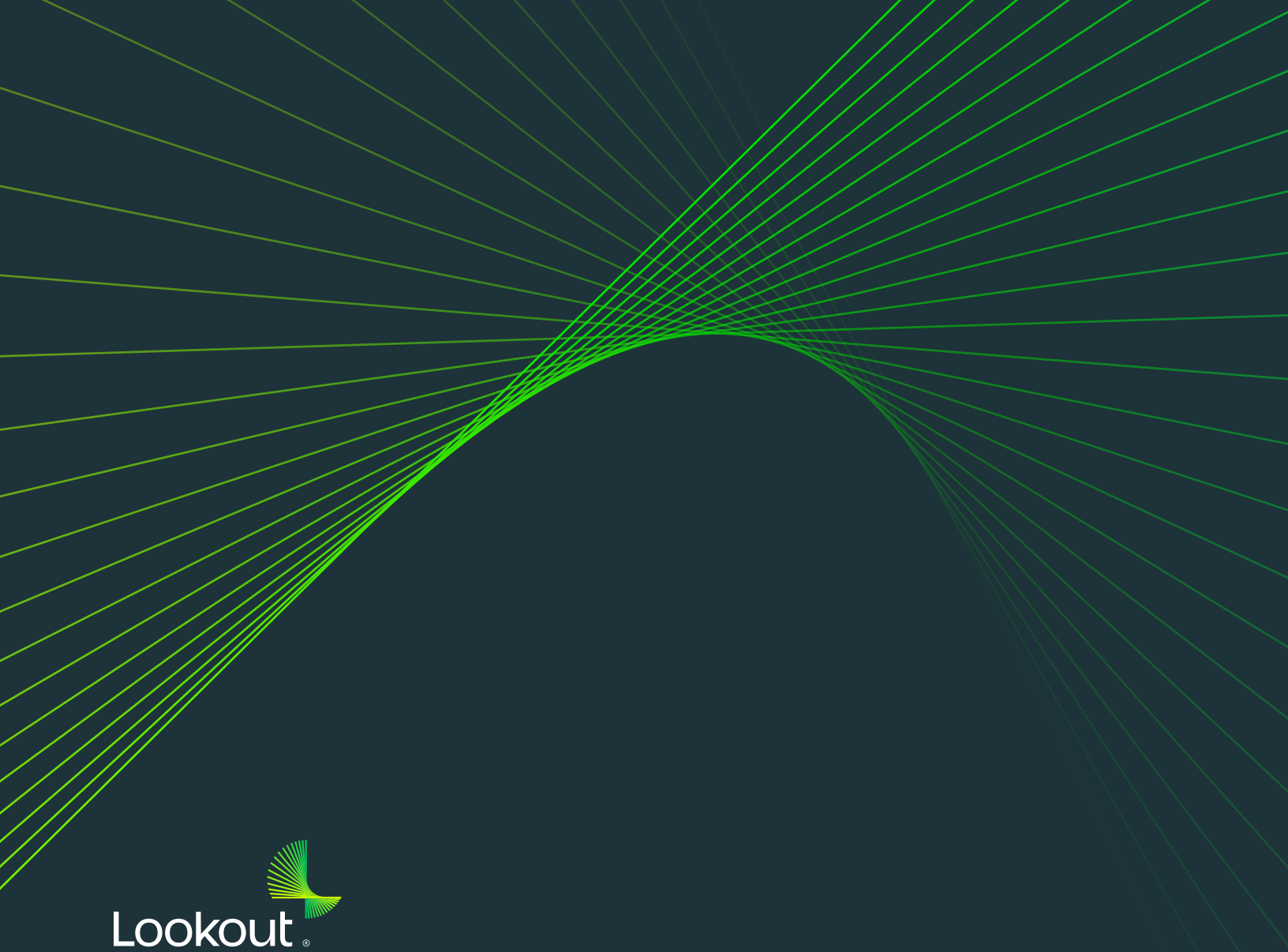
Warum Lookout DLP

- Agentenloses Design für schnelle Bereitstellung und effiziente Nutzung
- Abdeckung aller gängigen Web-, Cloud- und privaten Apps
- Zentralisierte Analyse in verschiedenen Multi-Cloud-Umgebungen
- EDM- und OCR-Funktionen
- SaaS-native Datenmaskierungs- und Verschlüsselungsfunktionen

Die Lookout Cloud Security Platform reduziert die Komplexität Ihrer Sicherheitsstrategie

Dank der in die Lookout Cloud Security Platform integrierten DLP-Funktionen können Unternehmen Cloud-Technologien bedenkenlos nutzen und gleichzeitig Daten schützen. Den Zugriff auf Dateien, Ordner oder Apps aus Sicherheitsgründen komplett einzuschränken, ist weder umsetzbar noch produktiv. Die zentrale Lookout Cloud Security Platform ist so konzipiert, dass Sie die Kontrolle behalten und sich gleichzeitig an betriebliche Anforderungen und die sich verändernden Arbeitsweisen von Mitarbeitern anpassen können.





Über Lookout

Lookout, Inc. bietet datenzentrierte Cloud-Sicherheit, die verschiedene Phasen eines modernen Cybersecurity-Angriffs bewältigt. Daten sind das Herzstück eines jeden Unternehmens, und unsere Sicherheitsstrategie ist so konzipiert, das Daten in der sich ständig weiterentwickelnden Bedrohungslandschaft geschützt werden. Die Lookout Cloud Security Platform orientiert sich am Verhalten von Menschen, hilft, Bedrohungen in Echtzeit zu erkennen und Angriffe von den ersten Phishing-Versuchen bis zur Datenexfiltration schnell zu stoppen. Um mehr zu erfahren, besuchen Sie de.lookout.com, folgen Sie Lookout auf unserem Blog, LinkedIn und X.

Weitere Informationen finden Sie unter
de.lookout.com

Holen Sie sich Ihre Demo-Version unter
de.lookout.com/contact/request-a-demo