Lookout Cloud Security Platform Data Loss Prevention

Identifica, valuta e proteggi i dati con DLP cloud native.

Un approccio integrato alla DLP

I requisiti di sicurezza dei dati in cloud continuano a maturare rapidamente, guidati da fattori che includono vantaggi operativi dell'infrastruttura in cloud e la drammatica espansione della forza lavoro remota. Sebbene la maggior parte delle applicazioni cloud e SaaS offre controlli di sicurezza integrati, i professionisti della security richiedono funzionalità dedicate e centralizzate per la prevenzione dalla perdita di dati (DLP) che offrano maggiori garanzie supportando casi d'uso complessi in piattaforme multiple. Le organizzazioni richiedono una piattaforma che integri il DLP che integri soluzioni di protezione dei dati attraverso app private, internet e cloud.

Proteggi i dati durante il loro spostamento

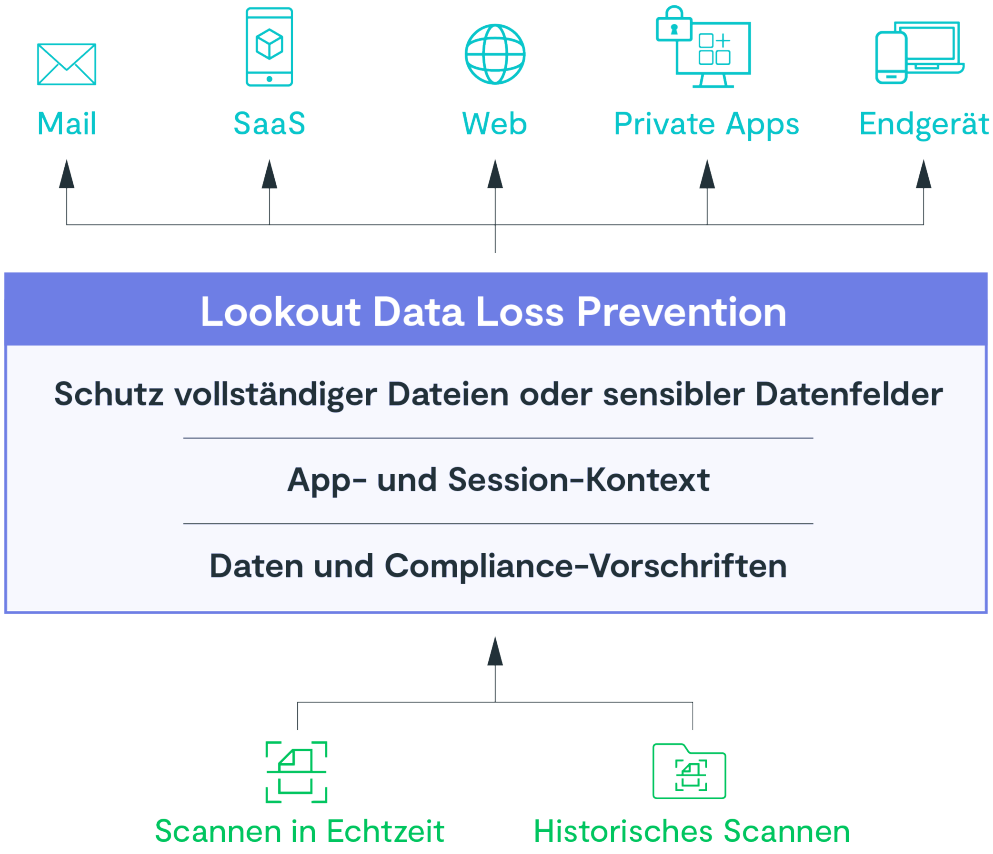
La piattaforma di sicurezza cloud Lookout offre robuste capacità di DLP progettate per proteggere dati sensibili attraverso app cloud e SaaS, app private, internet ed email. Lookout propone un DLP nativo per il cloud che consente alle organizzazioni di applicare politiche di sicurezza dei dati coerenti e controlli su tutte le app aziendali, garantendo l'integrità e l'accessibilità dei dati aziendali ovunque essi fluiscano, che si tratti di dati locali, in cloud od accessibili tramite dispositivi gestiti e non gestiti.

Panoramica sulla DLP di Lookout

- Con agente e Agentless, integrata nativamente nella piattaforma di sicurezza
- Copertura dei set di dati storici, sia in tempo reale
- 1100+ modelli predefiniti e personalizzabili per le varie tipologie di dati e contesti
- Supporta dati strutturati e non, oltre ai vari formati di documento
- Rilevamento evoluto dei dati, inclusi OCR, API, modalità di ispezione del proxy e dell'email
- Applicazione di politiche consapevoli del contesto che includono protezione per azioni di caricamento, download, condivisione e collaborazione

Alcuni esempi di Casi d'uso applicando la DLP di Lookout

- Poter indirizzare gli utenti in tempo reale durante la manipolazione dei dati.
- Rilevare e bloccare in tempo reale furti di dati da parte di insider malintenzionati.
- Prevenire perdite di dati accidentali.
- Prevenire la perdita di dati tramite IA generativa e siti web.
- Proteggere dati sensibili condivisi con partner e contractor esterni all'organizzazione



La DLP di Lookout consente alle organizzazioni di gestire centralmente requisiti critici quali:

Classificazione

Per rilevare e catalogare le informazioni sensibili ovunque si trovino.

Integrazione

Estensione delle pratiche e delle politiche DLP on prem ed in cloud.

Scansione dei dati

Copertura di tutti i formati, strutturati e non strutturati, dei dati.

Gestione delle policy

Fornire protezione e conformità consistenti tra le applicazioni.

Visualizzazione

Qualsiasi sia la modalità di accesso ai dati, incluso il contesto di uno specifico utente, tipo di dispositivo.

Principali capacità

Rilevamento: Ottenere una chiara visibilità su dove si trovino i dati - sia a riposo che in movimento

Rilevazione dei dati in cloud
La rilevazione dei dati in cloud analizza sia il tempo reale che lo storico, per identificare informazioni sensibili memorizzate nelle app cloud. Ciò aiuta le organizzazioni ad ottenere visibilità sui dati presenti nei loro ambienti cloud per classificare e proteggere i quelli sensibili, far rispettare le politiche DLP e garantire la conformità. Le organizzazioni possono identificare proattivamente informazioninon protette e condivisioni di file aperte per adottare provvedimenti correttivi.

Valutazione: Identificare dati e contesto in cui interagiscono

Valutazione: Identificare dati e contesto in cui interagiscono
Estendere la classificazione e la governance dei dati a qualsiasi documento in qualsiasi cloud, integrandosi con sistemi di classificazione terzi come Microsoft Azure Information Protection (AIP), TITUS di Fortra e Google Classification Labels. Utilizzando il motore di politiche unificate, le informazioni sensibili vengono identificate e protette in modo coerente, inclusi dati strutturati e non per rilevare contenuti in tutti i formati. Le organizzazioni ottengono così visibilità completa e protezione attraverso le molteplici app, utenti e dispositivi, proteggendo la proprietà intellettuale e altre informazioni protette da esposizioni non intenzionali dei dati.

Applicazione di politiche basate sul contesto
L'applicazione di politiche basate sul contesto consente alle organizzazioni di prendere decisioni di accesso studiate, comprendendo il contenuto ed il contesto degli scambi di dati. Con più utenti e dati al di fuori dei perimetri tradizionali, è cruciale verificare i livelli di rischio prima di concedere l'accesso. Utilizzando la tecnologia di analytics del comportamento e delle entità (UEBA), Lookout fornisce il contesto completo necessario per gestire il rischio degli utenti e rilevare anomalie con informazioni in tempo reale sui loro comportamenti.

Ispezione multi-modalità dei dati
Ispeziona i dati in qualsiasi modalità - API, proxy o email - per garantire visibilità completa su ogni set di dati e caso d'uso applicabile, dal rilevamento di dati storici non individuati, alla protezione di scenari complessi come la collaborazione in cloud o l'interazione con partner esterni. Monitora la gestione in ogni caso d'uso, inclusi l'accesso e l'utilizzo di informazioni sensibili sia da dispositivi gestiti che non gestiti per far fronte ad ogni tipologia di forza lavoro remota.

Motore di politiche unificate
Il DLP di Lookout fornisce una piattaforma centralizzata per definire e far rispettare politiche di sicurezza dei dati coerenti, indipendentemente da dove si trovino i dati o da come vengono acceduti. Ciò aiuta a razionalizzare i flussi di lavoro di sicurezza e garantisce che le informazioni sensibili siano protette su dispositivi e postazioni.

Politiche DLP adattive
La gestione e l'applicazione centralizzata delle politiche DLP vengono applicate su ogni piattaforma ed applicazione. Le politiche predefinite possono essere applicate per aiutare ad identificare e classificare i dati nelle molteplici applicazioni quali Office365, Slack, G Suite, Box, Salesforce, AWS e molto altro. Sono disponibili modelli di policy personalizzabili per applicazioni commerciali e private, con regole di conformità agli standard come GDPR, PCI, SOX, HIPAA eccetera.

Proteggere: Nascondi, rettifica o rimuovi facilmente i tuoi dati, ovunque si trovino

Ampia gamma di azioni DLP
Una vasta gamma di opzioni aiuta a proteggere i dati nel cloud con inoltre la capacità di consentire-rifiutare azioni in base alle regole di DLP impostate, supportando gli utenti nella loro produttivita'. Con Lookout, gli utenti possono monitorare la collaborazione in tempo reale, rimuovendo condivisioni aperte, abilitare l'autenticazione a piu' passaggi, applicare etichette di classificazione, nascondere, rettificare o crittografare i file per proteggere i dati durante il download ed addirittura fornire coaching agli utenti per guidarli quando si compiono azioni rischiose.

Corrispondenza dei dati e OCR
Identifica, classifica e proteggi i dati sensibili in ogni formato ed applicazione con Corrispondenza Esatta dei Dati (EDM) e fingerprinting. Il riconoscimento ottico dei caratteri (OCR) rileva file immagine per impedire la condivisione di dati sensibili all'interno di file immagine. Queste tecniche sofisticate di protezione permettono maggiore protezione delle informazioni personali identificabili (PII), proprietà intellettuale, finanziaria ed altri dati sensibili, garantendo sicurezza durante tutto il ciclo di vita.

Gestione nativa dei diritti digitali (DRM
Crittografare, mascherare o cancellare remotamente i dati sensibili in base all'applicazione di politiche qualora i dati si spostino attraverso flussi di lavoro, app e persino dispositivi non gestiti, garantendo che le informazioni non escano dai parametri autorizzati. Impedire il download inappropriato, condivisioni troppo permissive con partner esterni e persino errori dei dipendenti nella gestione delle informazioni sensibili.

Integrazione: Integrarsi senza soluzione di continuità con l'infrastruttura esistente

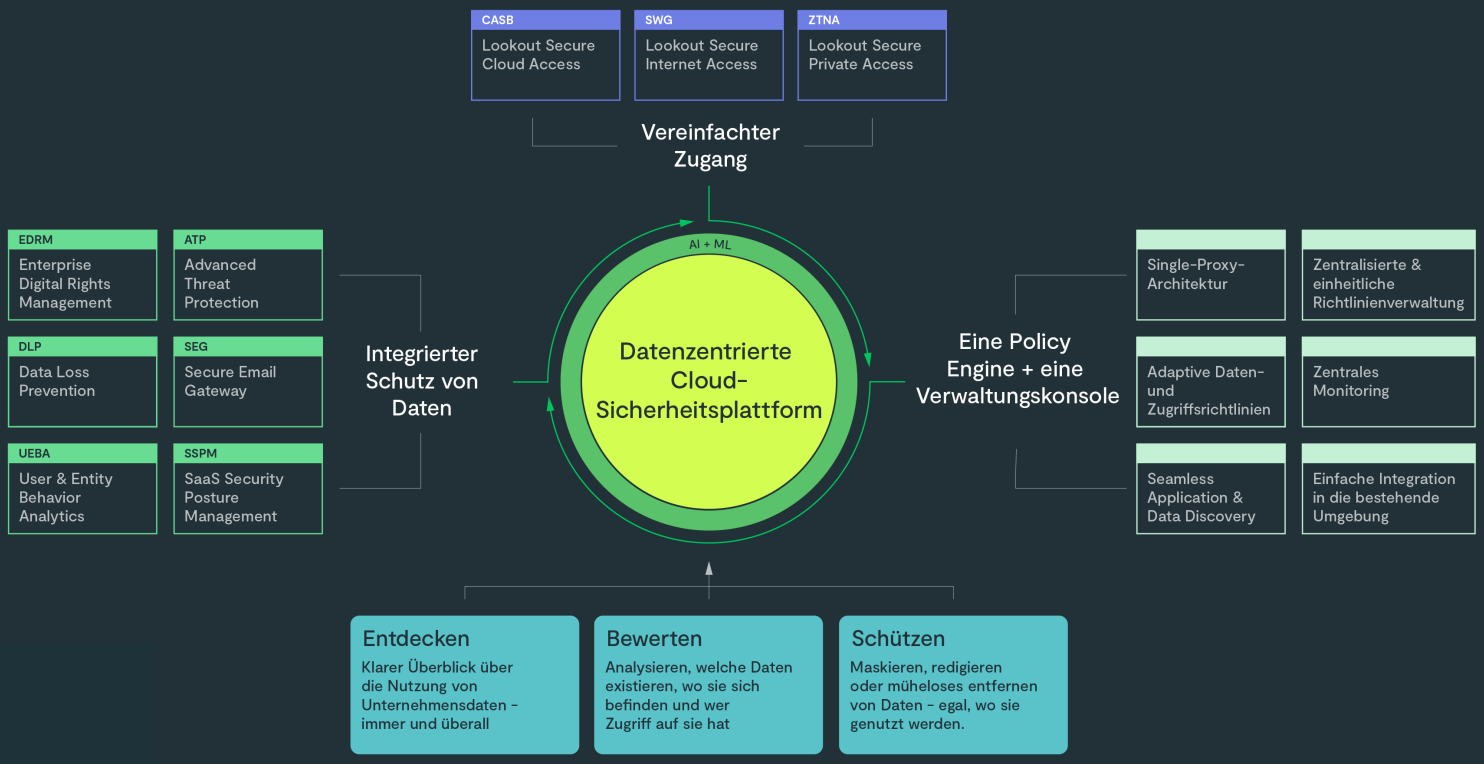
Ampliare le soluzioni DLP esistenti
Estendi la soluzione DLP on premise esistente alla posta elettronica e alle altre piattaforme grazie all'integrazione API completamente supportata. Rifletti le politiche nel tuo ambiente cloud per orchestrare una strategia DLP applicando politiche unificate. Lookout si integra con motori DLP esterni, fornendo la flessibilità di eseguire la scansione dei dati tramite DLP nativo, DLP esterno o una scansione multi-livello. Il DLP di Lookout si integra con le soluzioni di sicurezza esistenti, quali VMware, Juniper, CloudFlare, Akamai, Okta e altro ancora, per razionalizzare i flussi di lavoro e la postura complessiva della sicurezza.

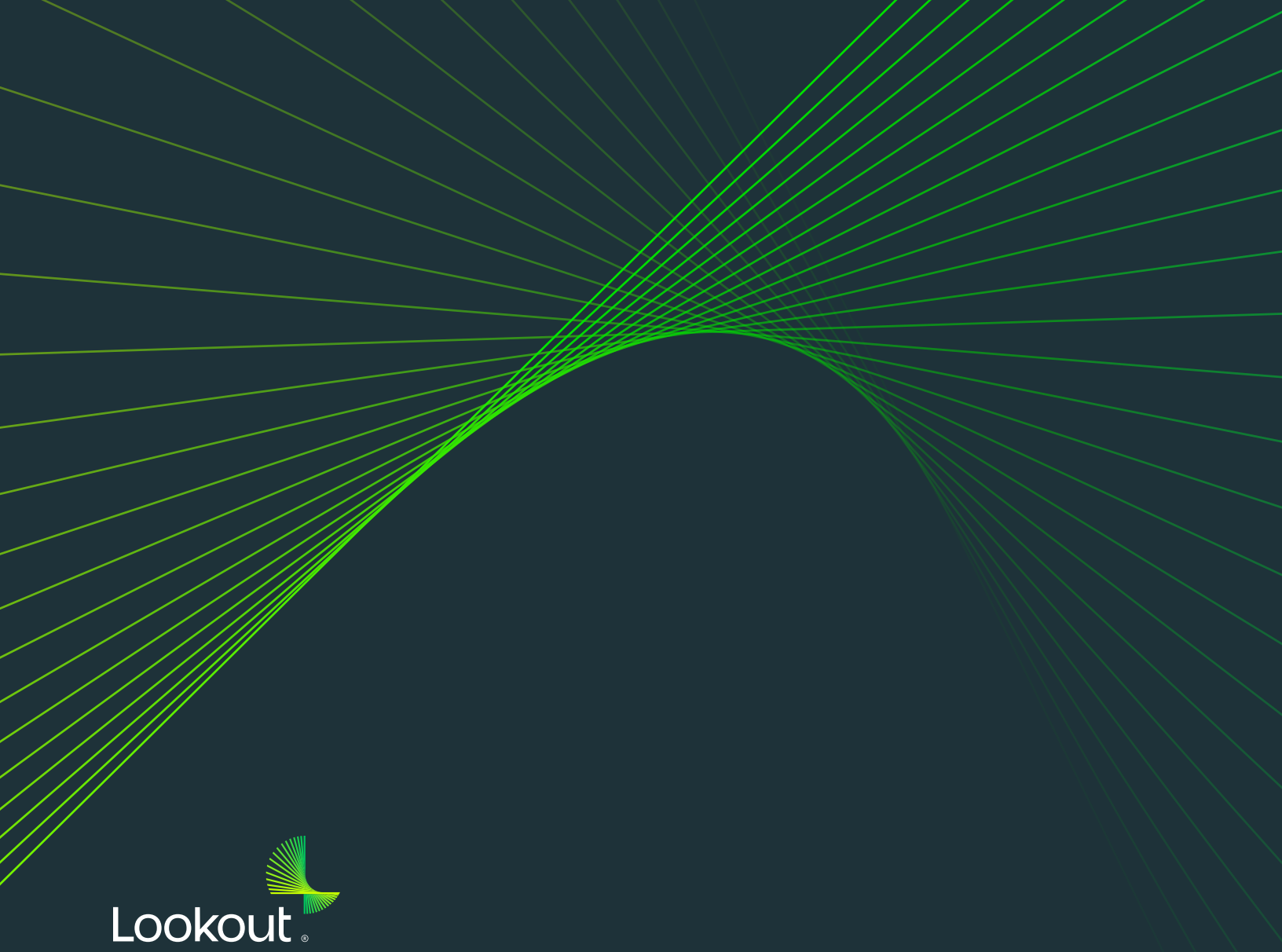
Perché Lookout DLP

- Se agentless, per una rapida distribuzio ne specie nel byod
- Copertura dedicata per ogni applicazione web, cloud e privata (popolari)
- Analisi centralizzata in ambienti multi-cloud diversificati
- Capacità EDM e OCR
- Capacità di mascheramento e crittografia dati native del SaaS
- Agente per maggiore capillarita

Rimuovi la complessità dalla sicurezza con la piattaforma di sicurezza cloud di Lookout

Sfruttando la tecnologia DLP integrata nella piattaforma di sicurezza cloud di Lookout, le organizzazioni possono abbracciare con fiducia le tecnologie cloud proteggendo il loro asset più prezioso, i dati. Limitare completamente l'accesso a file, cartelle o applicazioni per motivi di sicurezza non è né praticabile né produttivo. La piattaforma di sicurezza cloud di Lookout, incentrata sui dati, è progettata per tenere tutto sotto controllo adattandosi alle esigenze della tua azienda e ai modi in continua evoluzione in cui il tuo personale opera.





À propos de Lookout

Lookout, Inc. è un'azienda di sicurezza incentrata sulla protezione dei dati che utilizza una strategia di difesa capillare per affrontare le diverse fasi di un attacco informatico. I dati sono il cuore di ogni organizzazione e il nostro approccio alla sicurezza informatica è progettato per proteggerli in un panorama di rischio in continua evoluzione. Concentrandosi su persone e comportamenti, la Lookout Cloud Security Platform individua minacce in tempo reale e blocca le violazioni sin dai primi tentativi di phishing all'estrazione di dati. Per saperne di più, visitate il sito it.lookout.com e seguite Lookout nel blog, su LinkedIn e su X.

Maggiori informazioni sono disponibili su **it.lookout.com**

È possibile richiedere una demo su it.lookout.com/contact/request-a-demo