Lookout

Lookout Cloud Security Platform Data Loss Prevention

Discover, assess, and protect your data with cloud-native DLP

An integrated approach to DLP

Cloud data security requirements continue to mature rapidly, driven by factors including the inherent operational benefits of cloud infrastructure and dramatic remote workforce expansion. While most cloud and SaaS applications offer onboard security controls, practitioners require dedicated and centralized data loss prevention (DLP) capabilities that deliver advanced protection to support complex use cases across multiple platforms. Simply put, organizations need a DLP platform that integrates across solutions to protect data across private, internet, and cloud apps.

Protect data as it moves

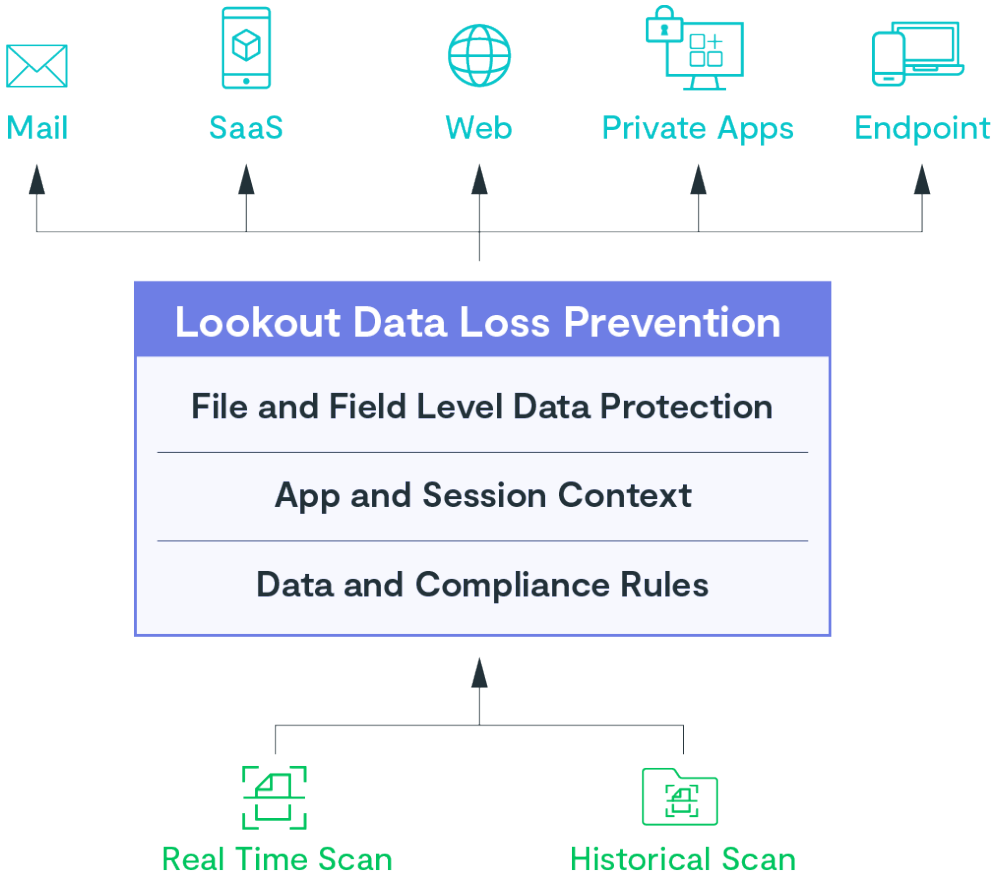
The Lookout Cloud Security Platform offers robust DLP capabilities designed to protect sensitive data across cloud and SaaS apps, private apps, internet, and email. Lookout delivers a modern and a cloud-native DLP that enables organizations to apply consistent data security policies and controls across all of their corporate apps, ensuring the integrity and accessibility of corporate data no matter where it flows — whether on premises, in the cloud, or accessed by managed or unmanaged devices.

Lookout DLP at a glance

- Agentless and natively built into the platform
- Coverage of both historical and real-time data sets
- Over 1100+ pre-defined and customizable policy templates across many data types
- Supports many structured and unstructured data types and document formats
- Advanced data detection including OCR, API, proxy, and email inspection modes
- Context-aware policy enforcement that include protection for upload, download, share, and collaborate actions

Lookout DLP critical use cases

- Real-time guidance for users for safer app and data practices
- Detect and block data theft by malicious insiders
- Prevent accidental data leaks by employees
- Prevent data leakage to Generative AI and social websites
- Protect sensitive data shared with partners and contractors



Lookout's DLP enables organizations to centrally manage critical requirements including:

Classification

To detect and catalog sensitive information wherever it lives

Integration

Extending on-premises DLP practices and policies to the cloud

Data Scanning

Covering all structured and unstructured data compositions

Policy Management

Providing consistent cross-apps protection and compliance

Visualization

Into every manner of data access, including user and device context, and handling

Key capabilities

Discover: Get clear visibility into where your data is – at rest and in motion

Cloud data discovery
Cloud data discovery scans both real-time and historical data sets to identify sensitive information stored in cloud apps. This helps organizations gain visibility into the data residing in their cloud environments to help classify and protect sensitive data, enforce DLP policies, and ensure compliance. Organizations can proactively identify unprotected information and open file shares in order to take corrective action.

Assess: Identify your data, the context where it exists, and its interactions

Integrated data classification
Extend data classification and governance to any document in any cloud, integrating with classification systems like Microsoft Azure's Information Protection (AIP), TITUS by Fortra, and Google Classification Labels. Using the unified policy engine, sensitive information is consistently identified and protected, including both structured and unstructured data to identify content across all formats. Organizations get full visibility and protection across multiple apps, users and devices — securing intellectual property and other protected information from unintended data exposure.

Context-aware policy enforcement
Context-aware policy enforcement enables organizations to make smart access decisions by understanding the content and context of data exchanges. With more users and data outside of traditional perimeters, it's crucial to verify risk levels before granting access. Utilizing user entity behavior analytics (UEBA) technology, Lookout provides the full context needed to manage user risk and detect anomalies with real-time insights into user behavior.

Multi-mode data inspection
Inspect data in any mode — API, proxy or email — to ensure full visibility into every applicable data set and use case, from detecting unseen historical data to protecting advanced scenarios such as cloud collaboration or interaction with external partners. Monitor handling across every use case including access and utilization of sensitive information from both managed and unmanaged devices to account for the remote workforce.

Unified policy engine
Lookout's DLP provides a centralized platform to define and enforce consistent data security policies, regardless of where data is located or how it is accessed. This helps streamline security workflows and ensures that sensitive information is protected across devices and locations.

Adaptive DLP policies
Centralized DLP policy management and enforcement is applied across every platform and application. Out-of-box policies can be applied to help identify and classify data across many applications including Office365, Slack, G Suite, Box, Salesforce, and AWS. Customizable policy templates are available for commercial and private applications, with dedicated standards compliance policies included to cover GDPR, PCI, SOX, HIPAA, and others.

Protect: Easily mask, redact, or remove your data– no matter where it is

Extensive range of DLP actions
A wide range of options help to secure data in the cloud beyond the basic allow-deny capabilities offered by other DLP solutions. With Lookout, users can control real-time collaboration, remove open shares, enable step-up authentication, apply data classification labels, mask, redact or encrypt files to protect data during download, or even set up user coaching to educate users on risky actions.

Data matching and OCR
Identify, classify and protect sensitive data in every format and application with Exact Data Matching (EDM) and fingerprinting. Optical Character Recognition (OCR) detects image files to prevent sharing of sensitive data within image files. These advanced data protection techniques further protect sharing of personally identifiable information (PII), intellectual property, financial and other sensitive data, ensuring its protection throughout its lifecycle.

Native digital rights management (DRM)
Encrypt, mask, or remote wipe sensitive data based on advanced policy enforcement as data moves across workflows, apps and even unmanaged devices — ensuring that information does not move outside authorized parameters. Prevent inappropriate downloads, overly permissive sharing with external partners, and even employees mistakes in handling your organization's most sensitive information.

Integrate: Seamlessly integrate with existing infrastructure

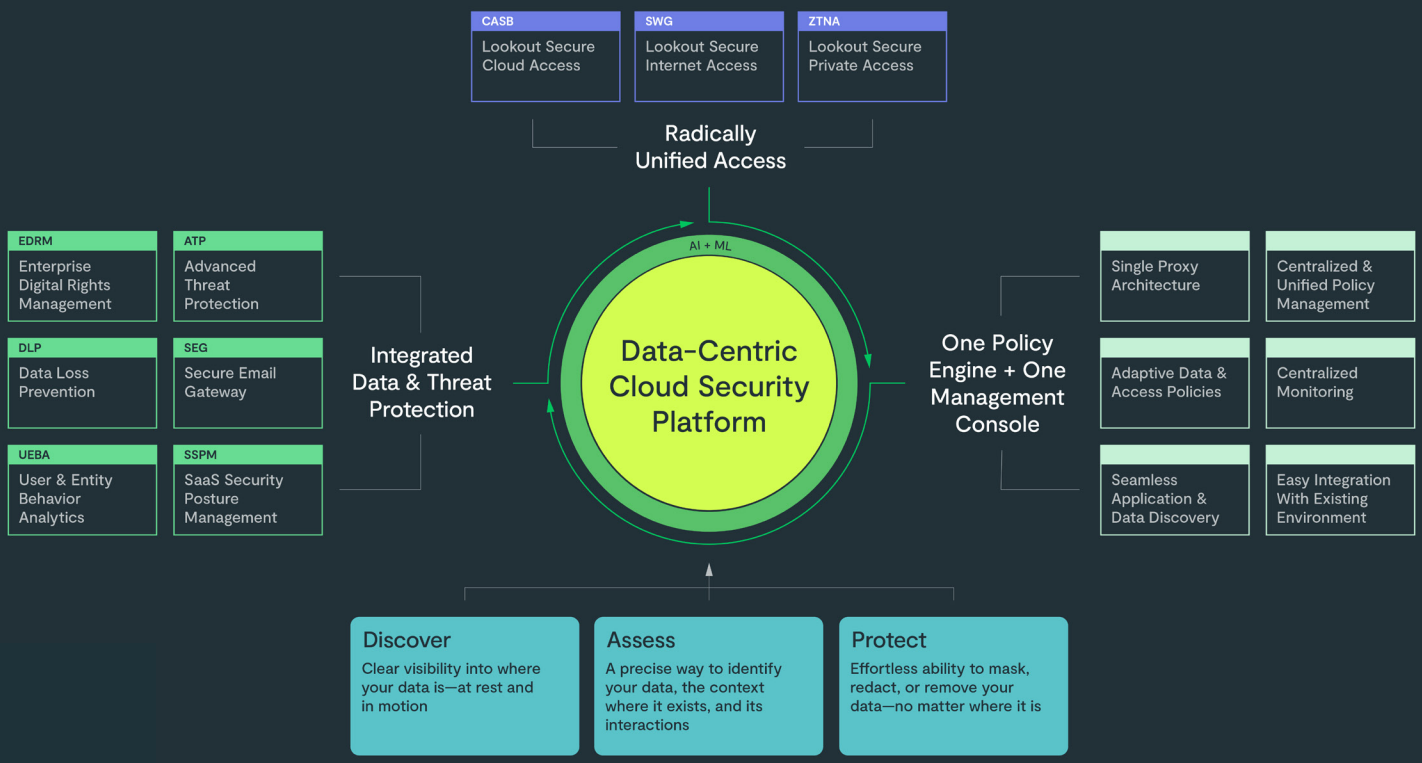
Enhance existing DLP solutions
Extend your traditional on-premises DLP across storage, email, and other platforms with fully-supported API integration. Mirror policies in your cloud environment to orchestrate a DLP strategy with unified policy analysis and enforcement. Lookout integrates with external DLP engines, providing the flexibility to scan data through native DLP, external DLP, or a multi-level scan. Lookout's DLP seamlessly integrates with existing enterprise security solutions, including VMware, Juniper, CloudFlare, Akamai, Okta, and more, to streamline workflows and overall security posture.

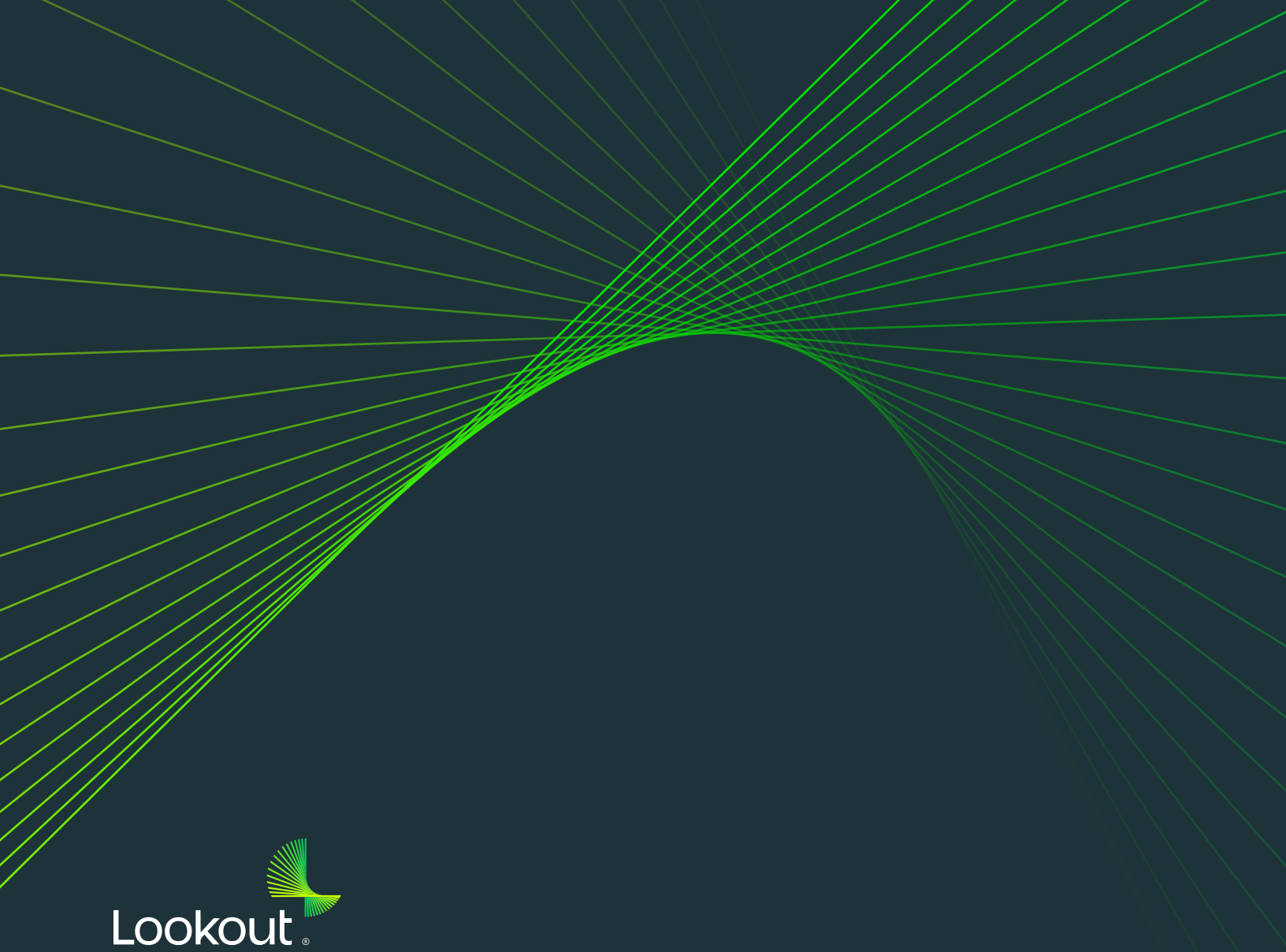
Why Lookout DLP

- Agentless design for rapid deployment and efficient operation
- Dedicated coverage for every popular web, cloud, and private app
- Centralized analysis across diverse, multi-cloud environments
- EDM and OCR capabilities
- SaaS-native data masking and encryption capabilities

Take the complexity out of security with The Lookout Cloud Security Platform

By leveraging DLP technology built into the Lookout Cloud Security Platform, organizations can confidently embrace cloud technologies while safeguarding their most valuable asset — data. Completely restricting access to files, folders, or applications for the sake of security is neither feasible nor productive. The data-centric Lookout Cloud Security Platform platform is designed to keep you in control while adapting to your business needs and the evolving ways your workforce operates.





Lookout

About Lookout

Lookout, Inc. is the data-centric cloud security company that delivers zero trust security by reducing risk and protecting data wherever it goes, without boundaries or limits. Our unified, cloud-native platform safeguards digital information across devices, apps, networks and clouds and is as fluid and flexible as the modern digital world. Lookout is trusted by enterprises and government agencies of all sizes to protect the sensitive data they care about most, enabling them to work and connect freely and safely. To learn more about the Lookout Cloud Security Platform, visit www.lookout.com and follow Lookout on our blog, LinkedIn, and X (previously 'Twiiter').

For more information visit
lookout.com

Request a demo at
lookout.com/request-a-demo

© 2023 Lookout, Inc. LOOKOUT®, the Lookout Shield Design®, LOOKOUT with Shield Design® and the Lookout multi-color/multi-shaded Wingspan Design® are registered trademarks of Lookout, Inc. in the United States and other countries. DAY OF SHECURITY®, LOOKOUT MOBILE SECURITY®, and POWERED BY LOOKOUT® are registered trademarks of Lookout, Inc. in the United States. Lookout, Inc. maintains common law trademark rights in EVERYTHING IS OK, PROTECTED BY LOOKOUT, CIPHERCLOUD, and the 4 Bar Shield Design.