

LOOKOUT CASB DATA LOSS PREVENTION

GET FULL VISIBILITY AND PROTECTION FOR EMAIL, SAAS AND IAAS APPLICATIONS

DLP Overview

Lookout delivers Data Loss Prevention (DLP) that enables organizations to apply consistent data security policies and controls across all of their cloud applications – ensuring the protection of sensitive information across every key requirement.

As organizations seek to utilize the broadest range of cloud capabilities to increase business agility – from email and collaboration, to applications infrastructure, and beyond – the necessity for dedicated cloud DLP has intensified. With the need to enforce stringent data protection, without preventing important business operations, practitioners are challenged to enlist centralized, efficient multi-SaaS capabilities. Lookout CASB DLP allows today's organizations to remain confident that every information security and compliance consideration is being met while allowing for open, optimized cloud data interaction.

Framing the CASB 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.

CASB+ DLP AT A GLANCE

- Agentless deployment for optimized performance
- Covers both historical and real-time data sets
- Pre-defined and customizable policy templates
- Advanced data detection including OCR API, Proxy, and Email inspection modes
- Context-aware policy enforcement: upload, download, share, collaborate

While most cloud applications offer onboard security controls, practitioners require dedicated DLP capabilities that deliver advanced protection in an orchestrated fashion – supporting complex use cases across multiple platforms. Put simply, organizations require an integrated CASB and DLP platform that mirrors the sophistication of traditional on-premise tooling.

To address every data security requirement for both commercial and private cloud applications, CASB delivers integrated Data Loss Prevention that enables organizations to centrally manage critical requirements including:

Classification

To detect and catalogue sensitive information wherever it lives

Visualization

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

Policy Management

Providing consistent cross-apps protection and compliance

Data Scanning

Covering all structured and unstructured data compositions

Integration

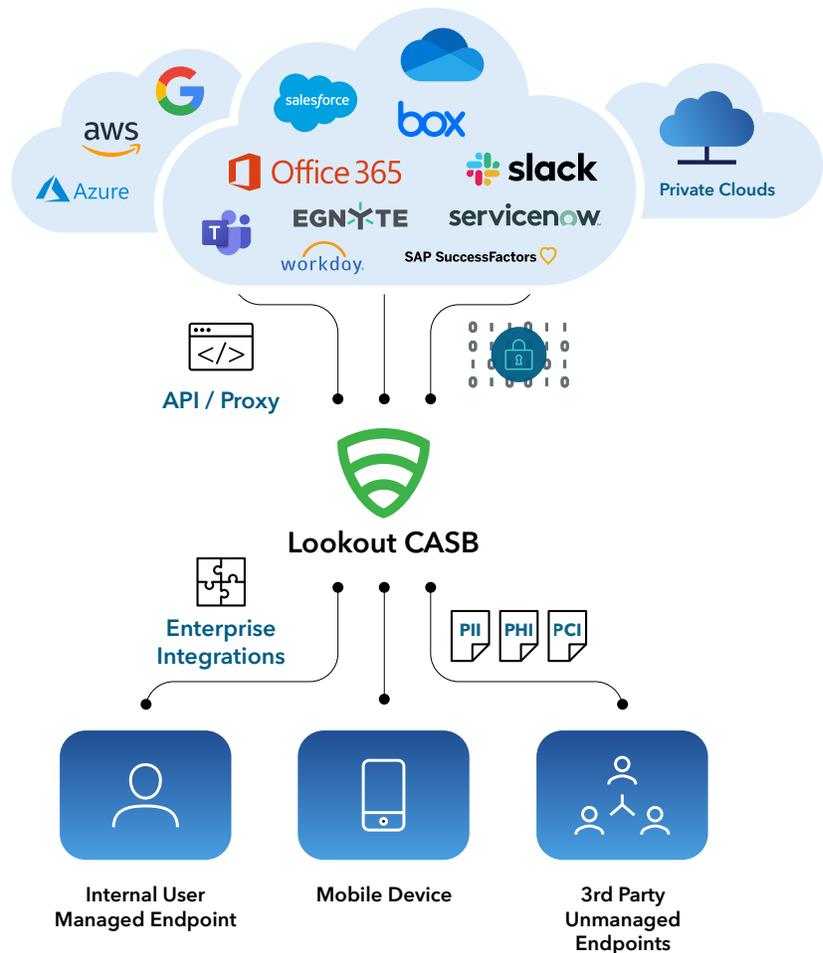
Extending on-prem DLP practices and policies to the cloud

By seamlessly translating enterprise data protection requirements to the cloud, Lookout CASB optimizes DLP implementation – reducing management costs while ensuring that business requirements are achieved securely and efficiently.

Lookout CASB DLP (formerly CipherCloud CASB) is recognized by experts including Gartner as an industry-leading set of capabilities, based on its unique ability to provide advanced data matching, document fingerprinting and analysis of both structured and unstructured data. Purpose-built to detect both historical information and real-time data in motion, CASB DLP offers practitioners the full breadth of integrated features needed to address every critical challenge.

CASB DLP differentiators include:

1. Agentless design for rapid deployment and efficient operation
2. Dedicated coverage for every popular cloud app and private app
3. Centralized analysis across diverse, multi-cloud environments
4. Exact data matching and optical character recognition (OCR)
5. SaaS-native data masking and encryption capabilities



CASB DLP Solution Features

Adaptive DLP Policies

CipherCloud CASB offers centralized DLP policy management and enforcement across every platform and application. Apply out-of-box policies to identify and classify data across most applications on Office365, Slack, G Suite, Box, Salesforce, AWS and many more, along with customizable policy templates for both commercial and private applications. Dedicated standards compliance policies cover GDPR, PCI, SOX, HIPAA, and many more.

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, including 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 expanded remote workforce.

Extensive Range of DLP Actions

CASB+ DLP offers a wide range of options to secure data in the cloud that goes beyond the basic allow/deny capabilities offered by other DLP solutions. With CASB DLP, users can control real-time collaboration, remove open shares, enable step-up authentication, apply data classification labels, encrypt files to protect data during download, and set up user coaching, among other capabilities.

Data Matching and OCR

Identify, classify and protect sensitive data in every format and application, across email, collaboration and every other scenario via exact data matching and fingerprinting. CASB DLP Optical Character Recognition (OCR) enables the detection of image files to prevent screen capture sharing and other unsanctioned handling, delivering the industry's most inclusive approach to cloud DLP enforcement.

Integrated Data Classification

CASB DLP extends data classification and governance to any document in any cloud, integrating with Microsoft Azure's Information Protection (AIP) and TITUS classification. Using the CASB policy engine, sensitive information is consistently identified and protected, including both structured and unstructured data. CASB provides full visibility into and protection across multiple apps, users and devices – securing intellectual property and other protected information from unintended data exposure.

Native Rights Management

Encrypt, mask or remote wipe sensitive data based on advanced policy enforcement as it is moved across workflows, applications and even unmanaged devices – ensuring that information does not move outside authorized parameters. Prevent inappropriate downloads, overly permissive sharing with external partners, and employee mistakes in handling your organization's most sensitive information.

Centralized DLP Management

Integrate and extend every form of traditional on-premise DLP across storage, email and other platforms via fully supported API integration with every other popular solution and vendor. Mirror and advance policies into the cloud environment to enable a consistent, orchestrated DLP strategy with unified policy analysis and enforcement. CASB seamlessly integrates with external DLP engines, offering organizations the flexibility to scan data through native DLP, external DLP, or augment data protection using a multi-level scan, where the data is pre-scanned through native DLP and a final scan is performed by an external DLP engine.

Awards



About Lookout

Lookout is an integrated endpoint-to-cloud security company. Our mission is to secure and empower our digital future in a privacy-focused world where mobility and cloud are essential to all we do for work and play. We enable consumers and employees to protect their data, and to securely stay connected without violating their privacy and trust. Lookout is trusted by millions of consumers, the largest enterprises and government agencies, and partners such as AT&T, Verizon, Vodafone, Microsoft, Google, and Apple. Headquartered in San Francisco, Lookout has offices in Amsterdam, Boston, London, Sydney, Tokyo, Toronto and Washington, D.C. To learn more, visit www.lookout.com and follow Lookout on its [blog](#), [LinkedIn](#), and [Twitter](#).

For more information visit
lookout.com

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

Integrated endpoint-to-cloud security



Learn more at lookout.com

© 2021 Lookout, Inc. LOOKOUT®, the Lookout Shield Design®, LOOKOUT with Shield Design®, SCREAM®, and SIGNAL FLARE® are registered trademarks of Lookout, Inc. in the United States and other countries. EVERYTHING IS OK®, LOOKOUT MOBILE SECURITY®, POWERED BY LOOKOUT®, and PROTECTED BY LOOKOUT®, are registered trademarks of Lookout, Inc. in the United States; and POST PERIMETER SECURITY ALLIANCE™ is a trademark of Lookout, Inc. All other brand and product names are trademarks or registered trademarks of their respective holders. 20210402-Lookout-USv1.0