Lookout®

EBOOK

Remote collaboration requires endpoint-to-cloud data security

Highlights

- Protect users, mobile devices, apps, connections, and data usage for collaboration and messaging app platforms.
- Collaborate and communicate securely from any managed or unmanaged device on any network from any location..
- Data loss prevention (DLP) and early detection of malware and exploit kits.
- Identify malicious behaviors associated with users, mobile devices, and apps.
- Prevent sharing of medical records, social security numbers, credit card data and other personally identifiable information (PII).
- Enforce compliance with GDPR, HIPAA, CCPA and other data privacy regulations.

Introduction

The epic migration to a remote workforce has prompted enterprises to populate the cloud with collaboration and messaging apps so employees can stay virtually connected to business. Slack, Microsoft Teams and other tools augment real-time communication and information sharing to keep employees productive and well informed.

With everything going everywhere, how do you protect corporate data, apps and privacy on these collaboration and messaging platforms?

The cloud access security broker (CASB) from Lookout® protects Slack, Teams and other business communication platforms by providing granular file-sharing controls and stateful inspection of data and apps.

In-depth visibility into content, data classification and context-aware controls allow users to collaborate securely – even from unmanaged mobile devices.

From endpoints to the cloud, Lookout CASB protects data, identifies cyberthreats, and enforces compliance rules to safeguard sensitive corporate information at every location. Lookout CASB gives you complete protection and control, making it safer to deploy any apps in your business cloud.

The agentless design of Lookout CASB ensures quick, frictionless deployment without the expense and administrative burden of manually installing and managing agents on every mobile device.

Deep visibility into users and SaaS apps

The State of Cloud Monitoring report from Keysight

Lookout CASB provides deep visibility into the security of collaboration and messaging apps in your cloud, giving you a better understanding of how data is being shared by Slack and Teams users. This visibility prevents accidental disclosure and exposure of sensitiveand privacy-regulated data.

- A single pane-of-glass view lets you view and monitor system and user activity across email, collaboration, messaging, and infrastructure.
- Shadow IT discovery automatically calculates your cloud risk score by scanning more than 20,000 cloud apps and analyzing over 60 attributes.
- Deep app intelligence secures all activities, not just data uploads and downloads. CASB discovers and differentiates between app instances to manage in real-time external collaboration and prevent open shares to secure files and folders.
- Insights allows you to narrow down incident and entity investigations by building queries that define scenarios of interest. Entity investigations can include users, devices, locations, and apps.
- Detailed 30+-page CIO/CISO reports about your organization's cloud security posture for audits and risk analysis.

"87% of cloud professionals feel that a lack of cloud visibility is obscuring security threats to their organization."

- The State of Cloud Monitoring report from Keysight

Secure access for unmanaged mobile devices

Lookout CASB identifies and protects SaaS apps from unauthorized account access with zero-trust cloud security controls. This gives you end-to-end user and data security from any mobile device, app, user, and location.

- Classifies mobile endpoint devices as managed or unmanaged through digital certificates for the duration of a connection to cloud apps.
- Integrates with Okta and other identity-as-a-service (IDaaS) solutions to verify user integrity and control access at the door with single sign-on (SSO) and multifactor authentication (MFA).
- Nonstop risk assessments of verified users with Adaptive Access Control (AAC). This blocks access to authorized users based on platforms, time of day, and other context that point to theft, compromise of authentication credentials or a cyberattack. For example, if someone tries to log in using your credentials from Shanghai an hour after you logged in from Detroit, AAC immediately identifies and stops this activity.
- Policies control access to cloud resources based on types of managed and unmanaged devices. For example, unmanaged devices are only given browser-based access to SaaS apps and access through thick apps are denied. Similarly, access control policies can deny data synching on unmanaged devices.

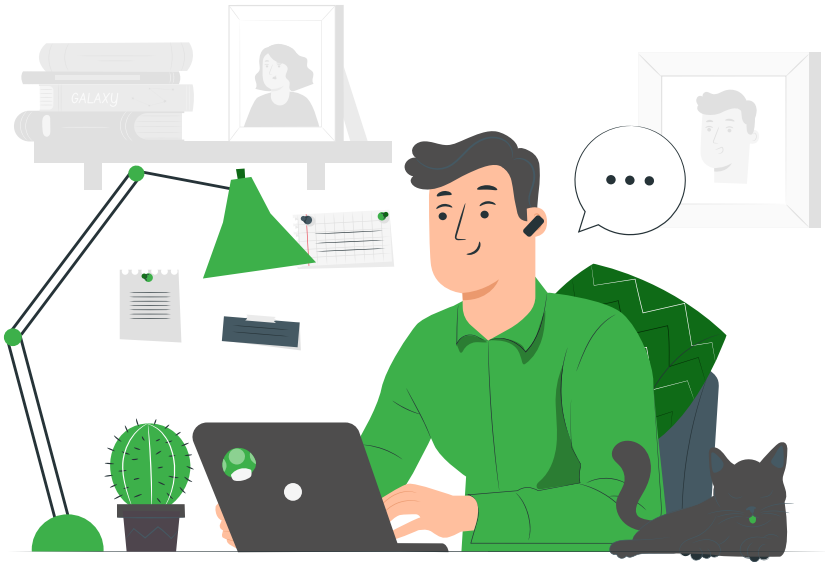
"Half of all organizations take about 120 days – or four months – to discover a credential breach. And even then, it is only after a third party has informed them."

- Dark Reading, 2021

Powerful data privacy and protection

Top cloud security concerns

- Network security (58%)
- Lack of cloud expertise (47%)
- Migrating workloads to the cloud (44%)
- Insufficient staff to manage cloud environments (32%)



Cloud Security Alliance "State of Cloud Security Concerns, Challenges, and Incidents," March 2021

It's notable that a total of 79 percent of respondents reported staff-related issues, highlighting that organizations are struggling with handling cloud deployments and a largely remote workforce.

Lookout CASB provides industry-leading DLP policies, end-to-end encryption, and comprehensive encryption-key management to restrict access to sensitive content in the cloud and prevent data leaks, theft of intellectual property and compliance failure.

The scalable, centrally managed security platform from Lookout, simplifies new cloud on-boarding processes and streamlines workflows for the creation of data protection policies.

- Deep content scanning with DLP policies protects PII, PCI, PHI, and other sensitive content through data classification, encryption, masking, watermarking, quarantining, and deleting. CASB includes built-in DLP templates to scan driver's licenses, passport numbers, IP and MAC addresses, email, EIN, and VIN.
- Zero-trust encryption protects data no matter where it is – at rest, in transit, in cloud app layers (API, middleware, memory), and in use. FIPS 140-2 compliance meets global regulatory mandates and ensures the highest levels of cyberthreat protection, including API attacks that target encrypted data. Data encryption keys are always secure and never shared with cloud providers.
- Optical character recognition (OCR) enables CASB to detect sensitive information in image files that have been uploaded to the cloud. OCR protection is also applied to PDFs and Microsoft Word files.

Protect data downloaded on personally owned devices

Information rights management (IRM) in Lookout CASB applies data protection controls, encryption and centralized management to sensitive data, even when it's shared externally. Based on data sensitivity levels, IRM automatically envelopes data with advanced encryption to ensure data and human-centric protection.

- Native IRM secures offline data access, protecting data that is downloaded from cloud apps to user devices. Only authorized users with an IRM mobile app and valid keys are authenticated to decrypt and view sensitive content in downloaded files.
- To protect downloaded data from misuse, you can retract access to the data, even if it was downloaded and copied to another device. Lookout CASB integrates with Microsoft and other major third-party IRM packages.
- Remote control data with ActiveSync proxy integration lets users block connected devices or remote wipe Teams content from a personal mobile device based on a device's posture.
- Restrict file- and folder-sharing with external groups and personal devices on Slack, Teams and other collaboration and messaging apps

"Personal mobile devices are much more susceptible to phishing attacks than enterprise mobile devices. Our data shows that personal devices were exposed to phishing threats at a rate of 19.4% in the first quarter of 2021. Compared to 13.5% for enterprise devices."

- Lookout Threat Report, 2021

Zero-day threat prevention in SaaS environments

In partnership with FireEye, Lookout provides the industry's first real-time protection of zero-day threats from mobile to SaaS environments. You can now aggregate and correlate threats across the endpoint-to-cloud spectrum to stop the incoming wave of cybersecurity threats that target today's mobile workforce.

- Antivirus and antimalware (AV/AM) protection against ransomware and other threats to keep data in file-sharing and cloud content management services safe. URL link protection and on-premises sandbox integration discover and remediate elusive zero-day threats. This enables AV/AM to detect and isolate infected cloud documents before malware spreads.
- User and entity behavior analytics (UEBA) use advanced machine learning to monitor user activity, including the time of day of activity, bulk file download attempts, and other anomalous behaviors. In real time, UEBA flags or blocks unusual activity based on variations from normal behaviors, such as preventing downloads of unusually large volumes of documents at odd hours of the day.
- Cloud security posture management (CSPM) automatically assesses SaaS and IaaS security posture of the Microsoft Office 365 suite, Microsoft Azure, Amazon Web Services, and the Google Cloud Platform. Centralized security management for all cloud services and infrastructure dramatically reduces operational complexity.

"The average cost to recover from a cyberattack for organizations with more than $1 billion in revenue is $4.6 million."

- TechBeacon

Centralized governance and compliance

Lookout CASB ensures that collaboration and messaging apps like Slack and Teams support a wide range of current and pending data privacy rules. This includes compliance with PCI, PII, HIPAA, General Data Protection Regulation (GDPR), California Consumer Privacy Act (CCPA), and others.

- Cloud data discovery (CDD) scans historical cloud data, discovers and classifies sensitive content, and defines data protection policies to comply with data residency laws. Lookout CASB includes predefined DLP templates that address GDPR, HIPAA, CCPA, GLBA, and other data regulations.
- Every country has different compliance rules for data privacy, data protection, data sovereignty, and data residency. Lookout enables multinational enterprises to manage one integrated secure deployment for key cloud apps with controls and key management that are configurable to address a variety of regulatory requirements.
- Lookout CASB augments the protection of personal information about residents in countries and regions and complies with the data residency laws of host nations. This allows enterprises worldwide to adopt cloud apps without worrying about additional security controls for data protection.

"By 2023, 65% of the world's population will have its personal information covered under modern privacy regulations, up from 10% today."

- Gartner

Lookout®

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

To learn more about Lookout CASB, visit
lookout.com/products/cloud-access-security-broker