Lookout®

Slack
Cloud Solution Brief

CASB for slack

Slack today has emerged as one of the most popular apps for cloud-based collaboration in workplaces, reaching 10 million active users in 2019. Slack allows organizations to effectively communicate and share information, boosting productivity and teamwork. Lookout CASB for Slack provides deep visibility into the application, along with real-time data protection and threat prevention for secure collaboration and sharing.

Overview

Lookout and Slack have teamed up to combine industry leading messaging application with industry leading cloud security access broker (CASB), enabling secure collaboration and messaging across Slack users and groups. Lookout CASB provides complete visibility, protection and control of all activity on Slack, with continuous risk assessment against external or internal threats. Furthermore, CASB Zero-day Threat Protection secures against malware and prevents data loss in real-time, either accidentally or due to malicious intent, addressing some of the primary cloud security concerns of organizations. Combining Lookout CASB security alongside Slack delivers a complete and safe platform for secure cross-app communication and data sharing.

Extend Slack security with Lookout CASB Cloud Security Controls

- Provides peace of mind to freely and safely use all company messaging, including Slack, without the fear of malware infections or data loss.
- Achieve full visibility and security for users, devies, links and data usage in Slack and other messaging applications.
- Identify sensitive data such as intellectual propety, GDPR, CCPA, or any PII such as medical, social security or credit card information.
- Powerful user behavior analytics to detect bad behavior by users, devices or applications and immediately remediate, mitigate or isolate the threat.

Features

Powerful Data Privacy and Protection

Lookout CASB provides industry-leading Data Loss Prevention (DLP), end-to-end Zero Trust encryption, and comprehensive key management with the flexibility to address any mix of security requirements. Our state-of-the-art data protection support that includes, native device management, secure offline data access, data classification and key management are made available through a single, scalable platform, simplifying new cloud onboarding and streamlining the workflow for creating data protection policies.

- CASB DLPs perform deep content scanning and protect sensitive content through data classification, encryption, masking, watermarking, quarantining or deleting. CASB prevents the upload of sensitive and regulated content defined as containing PII, PCI, PHI or other sensitive or confidential material. This content can also be encrypted on the fly during the upload to ensure that it is compliant and protected. CASB expands DLP monitoring with additional standard DLP templates, including driver's licenses, passport num-bers, IP and MAC addresses, email, EIN, and VIN.
- CASB native Digital Rights Management (DRM) applies protection controls on sensitive data even when it's shared externally. Based on the level of data sensitivity, policies can be defined to protect the data downloaded from Slack app to a user's device, including defining what devices are allowed to access the data (for example, the users cannot use personal devices to access sensitive content).

If downloaded data needs to be protected from mis-use (for example, former employees taking customer data to new companies), administrators can retract access to the data, even if it was downloaded and copied to another device. Real-time key revocation can protect data on lost and stolen devices.

- Optical Character Recognition (OCR) enables CASB to detect sensitive information in image files that have been uploaded to Slack. OCR protection can also be applied to files that include images; for example, a PDF or a Microsoft Word file.

Deep Visibility and Adaptive Controls

CASB provides deep visibility into every activity within the Slack application, enabling better understanding of data access and shares by the Slack users. This combines with CASB Adaptive Access Control (AAC) support to enable context-based data access, detect user access anomalies with advanced machine learning and identify sensitive data to pre-vent unintended exposure.

- CASB provides deep visibility into every activity within the Slack application, enabling better under-standing of data access and shares by the Slack users, enabling collaborative governance and sharing be-tween various internal and external groups. CASB further provides controls to limit the uploading of sensitive content to an external folder, automatically removing any links to folders contain-ing sensitive data, and to precisely define the scope of sharing. The visibility is captured in activity logs to support compliance reporting, audit, and forensic investigation.

- CASB Adaptive Access Control (AAC) can block ac-cess, even to what appear to be authorized users, based upon access context that includes, platforms used, time of day, originating location, and more that might suggest the theft, compromise of authentica-tion credentials, or a sophisticated cyber-attack.

  For example, if someone attempts to login using your credentials from Shanghai, China, one hour after you have logged in from Detroit, Michigan, AAC would immediately identify and stop this activity.

- CASB User and Entity Behavior Analytics (UEBA) capability uses machine learning to monitor user ac-tivity, including time of day of activity, attempts at bulk file download, and other anomalous behavior. UEBA can make real-time decisions to flag unusual activity or block it based upon variation from normal patterns. For example, if an employee starts down-loading unusually large amounts of documents at 1 am, this would be flagged as anomalous behavior and stopped.

- CASB enables secure collaboration within Slack application with granular file sharing controls and stateful inspection of data and application. In-depth visibility into the content, data classification and con-text-sensitive controls allows users to collaborate freely. Ethical firewalling prevents data exfiltration due to accidental shares with external collaborators or domains.

Centralized Compliance

CASB enables your Slack application to be compliant with a broad mix of current and pending global privacy and compliance regulations. This includes the controls necessary to support cloud-based applications under PCI, PII, HIPAA, General Data Protection Regulation (GDPR), Califor-nia Data Privacy Act (CCPA), and many more.

- Each country may have different compliance con-trols for data privacy, data protection, data sover-eignty, and data residency. Our Hybrid Deployment allows any multinational enterprise to manage one integrated secure deployment for key cloud applica-tions across multiple countries with controls and key management configurable to address a broad variety of differing regulatory requirements.

» CASB supports processing of personal data of res-idents within that country or region, complying with the data residency laws of the host nation. This al-lows global organizations to adopt cloud applications, without worrying about additional security controls for data protection.

Leveraging Existing Investments

The Lookout platform allows integration with existing enterprise security solutions to optimize existing investments including EDLP, SSO, and Antivirus/ Antimalware solutions, to name a few. Customers can also integrate with existing SIEM solutions as well as consume data from enterprise fire-walls and proxies to provide additional visibility on all clouds in use, including non-approved SaaS applications (Shadow IT). CASB Enterprise Integration includes support for external DLPs such as Symantec, Single Sign-On solutions such as Okta and Ping, Sandbox engines such as Juniper SkyATP, and more. CASB also includes a first class integration with Azure information Protection to leverage your other cloud data protection capabilities. Integration with Antivirus/ Antimalware (AVAM) solution provides additional detail for detection of many types of malware such as zero-day threats, viruses, spy-ware, ransomware, worms, and bots, and ensures that any additional files uploaded to Slack are protected from carrying malicious content that can affect the rest of the collaborators.

The Largest Multinationals in the World Use Lookout

5 of the Top U.S. Banks

6 of the Top Banks Worldwide

3 of the Top 10 Insurance Firms

3 of the Top 10 U.S. Health Care Firms

3 of the Top 10 Pharmaceutical Firms

2 of the Largest Telecommunication Firms

Government agencies in the United States, United Kingdom, Canada, Australia and beyond

Lookout®

Lookout is a 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.