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. CipherCloud CASB+ for Slack provides deep visibility into the application, along with real-time data protection and threat prevention for secure collaboration and sharing.

Overview

CipherCloud 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. CipherCloud 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 malwares 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 CipherCloud CASB+ security alongside Slack delivers a complete and safe platform for secure cross-app communication and data sharing.

Extend Slack security with CipherCloud 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

CipherCloud 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 numbers, 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 misuse (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 prevent unintended exposure.

>> CASB+ provides deep visibility into every activity within the Slack application, enabling better understanding of data access and shares by the Slack users, enabling collaborative governance and sharing between various internal and external groups. CipherCloud CASB+ further provides controls to limit the uploading of sensitive content to an external folder, automatically removing any links to folders containing 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 access, 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 authentication credentials, or a sophisticated cyberattack.

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 activity, 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 downloading 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 context-sensitive controls allows users to collaborate freely. Ethical firewalling prevents data exfiltration due to accidental shares with external collaborators or domains.

Centralized Compliance

CipherCloud 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), California Data Privacy Act (CCPA), and many more.

>> Each country may have different compliance controls for data privacy, data protection, data sovereignty, and data residency. Our Hybrid Deployment allows any multinational enterprise to manage one integrated secure deployment for key cloud applications 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 residents within that country or region, complying with the data residency laws of the host nation. This allows global organizations to adopt cloud applications, without worrying about additional security controls for data protection.

Leveraging Existing Investments

The CipherCloud 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 firewalls 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, mobile device management (MDM) systems such as Airwatch, 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, spyware, 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 CipherCloud

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

CipherCloud®

CipherCloud introduced the first CASB solution to the market in 2011 and continues to reshap the cloud security market. CipherCloud's recognized data protection expertise forms the foundation for the industry's only zero-trust CASB solution, providing seamless zero-trust security across all clouds with unified policies, trusted data protection, and automated compliance for the cloud-mobile era. CipherCloud is a winner of the Best Cloud Security Product of teh Year by SC Magazine, the Leading Visionary in Gartner's 2018 CASB Magic Quadrant, and the Overall Leader in the KuppingCole CASB Leadership Compass two years in a row. The world's largest global enterprises and government institutions in over 25 countries protect and secure their cloud information with CipherCloud. CipherCloud is backed by Andreessen Horowitz, Transamerica Ventures, Delta Partners and T-Venture, the venture capital arm of Deutsche Telekom. For more information, visit www.ciphercloud.com and follow us on Twitter @ciphercloud.