Symantec by Broadcom

CloudSOC® CASB Security for Slack

SOLUTION BRIEF

SAFELY USE SLACK AND PROTECT YOUR ORGANIZATION AND DATA FROM THREATS AND LOSS

- Are you sure your Slack accounts are secure?
- How do you prevent confidential data from being broadly shared?
- Do you have protections in place to prevent the spread of malware via messages?

INTEGRATED CYBER DEFENSE

CloudSOC is an integral part of Symantec Integrated Cyber Defense, which delivers multichannel protection across cloud, web, email, and endpoints—backed by the Symantec Global Intelligence Network, aggregated and distilled from Broadcom® products and technologies.

Data Loss Prevention (DLP) Industry-leading DLP helps protect sensitive data from loss with comprehensive detection and unified policies for cloud, web, endpoint, and data center.

MALWARE PROTECTION

Advanced malware defense using reputation, machine learning, behavior analysis, and virtual machine-aware sandboxing.

Overview

With Symantec® CloudSOC®, you gain visibility and control over the messages, content, and actions performed by Slack channels, teams, and users with an industry-leading cloud access security broker (CASB) solution. In CloudSOC, you can automate policies to prevent data loss and stop the proliferation of malware by monitoring and controlling message content and file sharing by your employees, contractors, vendors, and systems. CloudSOC is optimized to efficiently leverage Slack API integration and inline controls to provide extensive and integrated security enabling your organization to take full advantage of the Slack platform.

Detect security issues: Detect and analyze risky activity and content exposures to quickly investigate security incidents and monitor the security status of your users, teams, and channels.

Protect against threats: Scan messages and content for malware, ransomware, and advanced persistent threats (APTs). Dynamically identify suspicious user behavior to alert, quarantine, or block high risk actions and accounts.

Govern sensitive data: Enforce DLP on data at rest in Slack and data in motion between users to protect confidential content from exposure, loss, and breach in both private messages and team messages.

Automate policy controls: Automatically enforce security controls to quarantine or block high risk user actions, coach users, or alert admins with content-based and context-based policies.

Figure 1: Multiple Deployment Options

Quickly Investigate and Respond to Security Incidents

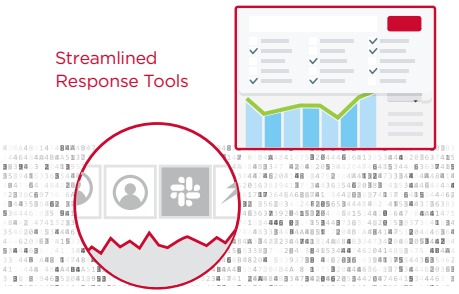
Track granular user, team, and channel activities and events within Slack, and provide critical insights to your compliance, audit, and other internal stakeholder teams when you have a security incident. Quickly investigate a specific user or activity, correlate events across apps and accounts, and discover what really happened with powerful search and data visualization tools and dashboards or export detailed incident log files to your SIEM system for analysis.

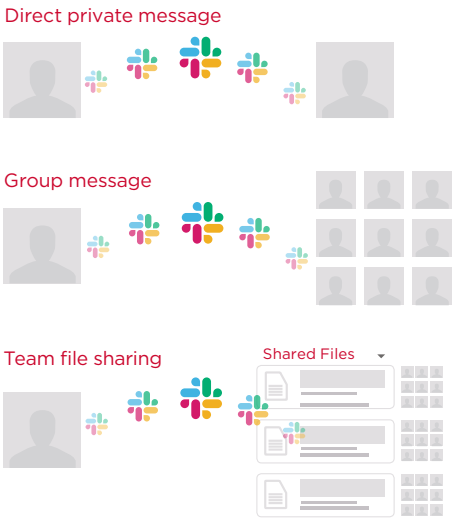
Protect Your Confidential Data in Slack Messages and Attachments

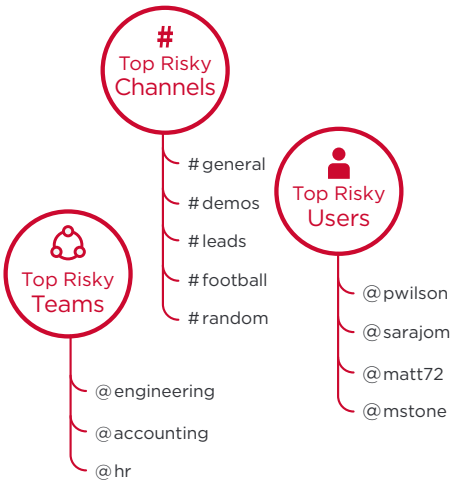
Quickly identify and mitigate risky data exposures in Slack with highly accurate DLP in the cloud that scans and automatically classifies message content and attachments. Use the data-science-powered Cloud Detection Service to prevent data exposures with content-aware and context-aware cloud DLP. Use event-driven policies to automate data security enforcement activities such as quarantining content for inspection, notifying users, and enforcing actions that control how sensitive data can be uploaded, shared, and accessed. Extend your enterprise DLP to Slack by using CloudSOC integration with Symantec DLP to enforce your centralized DLP policies and workflows.

Safeguard Your Organization Against High-Risk Users, Teams, and Channels

Automatically identify high-risk Users, Teams, and Channels; compromised accounts; and insider threats with CloudSOC unique data-science-driven User Behavior Analytics (UBA). Alert, quarantine, or block users from sharing corporate content based on their dynamic ThreatScore. Enforce granular policies that target specific Teams or Channels. Detect elaborate data exfiltration sequences, such as a pattern of downloading content from a corporate Slack channel and then uploading that content to a personal collaboration app, or anomalous and repetitive messages followed by deletes of sensitive files.







Automate User Coaching for Safer Behavior

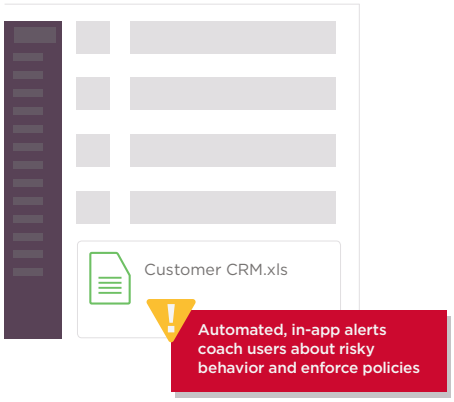
Automatically alert admins and educate users on safe practices directly in Slack with policy-driven CloudSOC notifications. A prompt response with coaching appearing directly in the app after a user takes a risky action can be more effective at modifying user behavior than traditional email-based notifications. CloudSOC can automatically notify users if content is quarantined for review by DLP and the result of that DLP scan. The same automated in-app notification capability can be used as a policy response to alert admins of policy violations.

Secure Your Slack Accounts Against Attacks and Malware

Continuously scan Slack message content and attachments to remediate and prevent the proliferation of ransomware, macros, APTs, and other malware threats. CloudSOC finds threats by inspecting content and analyzing user behavior with machine learning, UBA, and industry-leading Symantec threat protection that includes advanced anti-malware and file insight reputation technologies. Effectively protect your organization from emerging threats with dynamic analysis of files using integrated Symantec cloud sandboxing.

Always Know the State of Your Security with Intuitive Dashboards and Reports

Easily keep track of your Slack security status through an intuitive user interface providing default and fully customizable dashboards that show content risks and exposures in messages aggregated at team, channel, and user levels. Gain deep insights into Slack activity through detailed pivot tables, charts, and graphs to visualize risks over time. Role-based access controls provide admins just the right level of visibility and control. Management, compliance officers, and other stakeholders can be kept informed with regularly scheduled, customizable reports.



BROADCOM
connecting everything®

For more information, visit our website at: www.broadcom.com

CloudSOC-CASN-SB101 January 24, 2025