Netskope for Cisco Webex Teams

Cisco Webex Teams is a collaboration service that offers video meetings, group messaging, file sharing, and white boarding. Webex Teams offers employees flexibility in collaboration and tools to share information regardless of location and device. Netskope for Cisco Webex Teams allows for security teams to gain visibility and controls over Webex Teams to protect sensitive data, defend against cloud threats, and maintain compliance.

QUICK GLANCE

- Get detailed visibility into the activities of users accessing Webex Teams
- Apply granular policies to control risky activities and promote appropriate usage
- Protect PII, PCI, PHI, and other sensitive data shared in Webex Teams
- Defend against cloud threats and malware, like anomalous user behavior and ransomware

NETSKOPE FOR CISCO WEBEX TEAMS PRODUCT OVERVIEW

Netskope helps organizations add security to Webex Teams by helping security professionals to understand and control risky activities in Webex Teams, protect sensitive data, and stop cloud threats. Gain granular visibility into Webex Teams usage, all the way down to the actual cloud activities, user identity, device, data, and more. Place security policies to guide usage and use advanced, enterprise DLP to protect sensitive data and maintain compliance. Security professionals can also defend against cloud threats such as malware, including ransomware, as well as compromised credentials, privileged user account abuse, and more.

Netskope for Webex Teams Feature Table

FEATURE	BENEFIT
Granular visibility of Webex Teams usage	• Assess the security risk associated with your users' activities within Webex Teams
Granular control of Webex Teams user activities	• Prohibit risky activities from being performed by your users in Webex Teams and include adaptive access controls based on context
Advanced, enterprise cloud DLP	• Secure the upload, download, and sharing of sensitive or regulated data in Webex Teams
Continuous monitoring of Webex Teams	• Protect sensitive content collaborated on in Webex Teams with automated actions like alerting
Cloud threat and malware protection	• Detect malware going to or from and already resident in Webex Teams

FEATURES

Granular visibility of Webex Teams usage

Drill down into the details and activities of users accessing Webex Teams. Understand in real time the user identities and the types of devices accessing your environment. Audit the activities performed by your Webex Teams users including the creation, deletion, editing, uploading, or downloading of content. Perform ad-hoc queries or create reports of relevant access and usage information for compliance.

Granular control of Webex Teams user activities

Create granular, contextual policies based on user, activity, device, and more. Limit certain activities to only authorized users, and encourage correct user behaviors through coaching with custom user notifications—all in real time. Extend policies beyond activities by leveraging DLP and threat protection capabilities to protect your data and your organization.

Advanced, enterprise cloud DLP

Netskope lets you detect data violations in transfers to and from Webex Teams—including shadow IT instances. Govern content uploads and downloads containing sensitive data using pre-built profiles for personally identifiable information (PII), payment card industry data (PCI), protected health information (PHI), source code, profanity, and more.

Alternatively, you can custom-build DLP profiles using Netskope's robust set of advanced cloud DLP features such as 3,000+ data identifiers, 1000+ file types, support for language agnostic double-byte characters, custom regular expressions, pattern matching, proximity analysis, fingerprinting, and exact match.

FEATURES (CONT.)

Continuous monitoring of Webex Teams

Netskope API Protection capabilities for Webex Teams can provide alerts when sensitive data is shared and also when users are added. Netskope allows you to understand and govern who has access to Webex Teams at all times.

Additionally, API Protection retrieves detailed audit logs from Webex Teams in order to provide a clear and detailed picture of activities within the instance.

Cloud threat and malware protection

Detect and respond to usage anomalies using Netskope machine learning- and rules-based anomaly detection. See logins from suspicious locations, be alerted to data exfiltration, know when users' credentials have been compromised, and understand privileged user threats. Using Netskope Threat Protection capabilities, detect and block cloud malware in real-time activities or already resident in files within Webex Teams.

FLEXIBLE DEPLOYMENT OPTIONS

		API PROTECTION	REAL-TIME PROTECTION	
			Forward Proxy	Reverse Proxy
USE CASES	Out-of-band, near real-time visibility of Webex Teams including their user membership and public exposure Out-of-band retrieval of detailed audit logs from Webex Teams Automated policies and actions like alerting DLP and threat protection	X		
	Inline, real-time visibility and granular policy-based control* for users accessing Webex Teams		X	
	Inline, real-time visibility and granular policy-based control* for users accessing Webex Teams—including from unmanaged devices			X

*Real-time Webex Teams activities recognized by Netskope:
Create | Delete | Download | Edit | Invite | Login Attempt | Login Failed | Login Successful | Logout | Post | Share | Stop | Upload | View | View All

netskope

Netskope is the leader in cloud security. We help the world's largest organizations take advantage of cloud and web without sacrificing security. Our patented Cloud XD technology targets and controls activities across any cloud service or website and customers get 360-degree data and threat protection that works everywhere. We call this smart cloud security.