Zoom Contact Center security and privacy overview

WHITEPAPER

Zoom Contact Center is a contact center-as-a-service solution that helps businesses deliver prompt, accurate, and highly personalized experiences to their customers. The solution combines unified communications and contact center capabilities into one experience with the ease and simplicity of the Zoom platform. Intelligent routing improves agent productivity and guides your customers to faster resolution 24/7.

Below you'll find a brief overview of Zoom Contact Center's security and privacy features:

Encryption

For Zoom customer connections with their Contact Center hub, Zoom encrypts audio and video data-in-transit between the Zoom clients and the Zoom Cloud using secure real-time transport protocol (SRTP) leveraging TLS 1.2 with AES-GCM 256 bit encryption. Web and chat messages for these connections are encrypted in transit between Zoom clients and the Zoom Cloud using TLS 1.2 with AES-GCM 256 bit encryption.

Calls into a Zoom customer's Contact Center via mobile or landline phones are sent over the Public Switched Telephone Network (PSTN) and are not encrypted until reaching a Zoom gateway. Calls via Zoom Phone support standards-based encryption using SIP over TLS 1.2 AES 256 bit for calls and during phone provisioning sessions. In addition, call media is transported and protected by SRTP with AES-256 bit encryption for Zoom desktop and mobile clients, and with AES-128 or AES-256 bit algorithm for other supported devices.

Login and authentication

Zoom Contact Center users authenticate in the same way as a standard Zoom account. Zoom offers a range of authentication methods, such as SAML, OAuth, and/or password-based, which can be individually enabled or disabled for an account. Users authenticating with a username and password can also enable two-factor authentication (2FA) as an additional layer of security to sign in. These authentication mechanisms may not be available when logging into third-party integrations via Contact Center.

Security controls

- Customers can choose the region in which they'd like to store certain content, including cloud recordings, transcripts, and voicemails.
- Role management enables admins to control access to features and settings in the Zoom web portal. For example, admins can assign certain agents as supervisors and give them access to view the queue analytics dashboards so that they can track queue KPIs.
- Admins can set recording privileges to define whether users can access, download, or delete recordings. Supervisors and agents can only view voicemail inboxes for queues to which they belong.
- Operation logs for Zoom Contact Center allow account owners and admins to view changes made by admins to contact center settings and features.
- Similar to Zoom Meetings and Zoom Phone, Zoom Contact Center agents and supervisors can remove video and voice call participants.
- Zoom provides customers with the ability to inform users when their voice and video calls are recorded (through configurable options to play audio and/or display text prompts). It is up to customers to determine whether notifications are required and where to apply the appropriate notifications.
- Two-factor authentication, single sign-on, and one-time password (OTP) for suspicious logins are all features available to Zoom Contact Center customers.

Data management and access

- Zoom employees do not access Contact Center customer content unless directed by an account owner or as required for legal, safety, or security reasons.
- Zoom processes Contact Center data to provide its service, including licensed user information, billing information, engagement participant information, call logs, event and session logs, customer media assets (such as voice prompts, voicemail greetings, and hold music), voicemails, recordings, images, audio, video, chat and SMS messages, and usage metadata.
- Zoom implements and uses appropriate technical and organizational measures to protect personal data from loss, misuse, unauthorized access, disclosure, alteration, and destruction, taking into account the risks involved in the processing and the nature of the personal data.