Zoom unifies cloud video conferencing, simple online meetings, group messaging, and a software-defined conference room solution into one easy-to-use platform. Zoom offers the best video, audio, and wireless screen-sharing experience across Windows, Mac, Linux, iOS, Android, Blackberry, Zoom Rooms, and H.323/SIP room systems.

Zoom places security as the highest priority in the lifecycle operations of its public and hybrid cloud networks. Zoom strives to continually provide a robust set of security features to meet the requirements of businesses for safe and secure collaboration.

The purpose of this document is to provide information on the security features and functions that are available with Zoom. The reader of this document is assumed to be familiar with Zoom functionalities related to meetings, webinars, and group messaging.

Unless otherwise noted, the security features in this document apply across the product suite of Zoom Video Conferencing, Zoom Video Webinars, and Zoom Rooms, and across supported mobile, tablet, desktop, laptop, and H.323/SIP room system endpoints.

Infrastructure

The Zoom Cloud is a proprietary global network that has been built from the ground up to provide quality communication experiences. Zoom operates in a scalable hybrid mode; web services are hosted in the cloud and real time media is hosted out of tier-1 data centers.

A distributed network of low-latency multimedia routers (software) resides on Zoom's communications infrastructure. With these low-latency multimedia routers, all session data originating from the host's device and arriving at the participants' devices is dynamically switched — never stored persistently through the Zoom communications infrastructure.

Zoom's communications infrastructure for real-time video, audio, and data communications resides on Zoom dedicated servers, which are housed in SSAE 16 SOC2 compliant datacenters on opposite sides of the US.

Zoom sessions are completely temporary and operate analogously to the popular mobile conversation over the public mobile network.

In addition to unique security benefits, Zoom's communications infrastructure also enables an extremely scalable and highly available meeting infrastructure unrestricted by the limitations of physical data centers.

Firewall Compatibility

The Zoom client communicates with the multimedia router to establish a reliable and secure connection. At the time of instantiation, the Zoom client will determine the best method for communication, attempting to connect automatically using udp and tcp port 8801, 8802 and 8804 or HTTPS (port 443/TLS).

Client Application

Role-based user security

The following pre-meeting security capabilities are available to the meeting host:

- Enable end-to-end encrypted meeting
- Secure log-in using standard username and password or SAML Single Sign On
- Start a secured meeting with password
- Schedule secured meetings with password

Selective meeting invitation: The host can selectively invite participants via email, IM or SMS. This provides greater control over the distribution of the meeting access information. The host can also create the meeting to only allow members from a certain domain email to join.

Meeting Details Security: Zoom retains event details pertaining to a session for billing and reporting purposes. The event details are stored at the Zoom secured database and are available to customers for review on the customer portal page once they have securely logged-on.

Application security: Zoom can encrypt all presentation content at the application layer using the Advanced Encryption Standard (AES) 256-bit algorithm.

E2E Chat Encryption

Zoom end-to-end (E2E) chat encryption allows for a secured communication where only the intended recipient can read the secured message. Zoom use public and private key to encrypt the chat session with Advance Encryption Standard (AES256). Session keys are generated with device unique hardware ID to avoid data being read from other devices. This ensures that the session can not be eavesdropped or tampered with.

Meeting Security

Role-based user security

The following in-meeting security capabilities are available to the meeting host:

- Secure a meeting with end-to-end encryption (E2E)
- Enable wait for host to join
- Expel a participant or all participants
- End a meeting
- Lock a meeting
- Chat with a participant or all participants
- Mute/Unmute a participant or all participants
- Enable/Disable a participant or all participants to record
- Temporary pause screen-sharing when a new window is opened

The following in-meeting security capabilities are available to the meeting participants:

- Mute/Unmute audio
- Turn On/Off video

Host and Client authenticated meeting: A host is required to authenticate (via https) to the Zoom site with their user credentials (ID and password) to start a meeting. Client authentication process uses a unique per-client, per-session token to confirm the identity of each participant attempting to join a meeting. Each session has a unique set of session parameters that are generated by Zoom. Each authenticated participant must have access to these session parameters in conjunction with the unique session token in order to successfully join the meeting.

Open or password protected meeting: The host can require the participants to enter a password before joining the meeting. This provides greater access control and prevent uninvited guests from joining a meeting.

Edit or delete meeting: The host can edit or delete an upcoming or previous meeting. This provides greater control over availability of meetings.

Host controlled joining meeting: For greater control of meeting, the host can require participants to only join the meeting after the host has started it. For greater flexibility, the host can allow participants to join before the host. When joining before host, participants are restricted to a 30-minute meeting.

In-meeting security: During the meeting, Zoom delivers real-time, rich-media content securely to each participant within a Zoom meeting. All content is shared with the participants in a meeting is only a representation of the original data. This content is encoded and optimized for sharing using a secured implementation as follows:

- Is the only means possible to join a Zoom meeting
- Is entirely dependent upon connections established on a session-by-session basis
- Performs a proprietary encoding process that encodes all shared data
- Can encrypt all screen sharing content using the AES 256 encryption standard
- Can encrypt the network connection to Zoom using 256-bit TLS encryption standard
- Provides a visual identification of every participant in the meeting

Secured Communications

Zoom can secure all session content by encrypting the communications channel between the Zoom client and the multimedia router using a 256-bit Transport Layer Security (TLS) encryption tunnel.

Host controlled joining meeting

Authentication methods include Single Sign-on (SSO) with SAML or OAuth

With SSO, a user logs-in once and gains access to multiple applications without being prompted to log-in again at each of them. Zoom supports SAML 2.0 which enables web-based authentication and authorization including single sign-on (SSO). SAML 2.0 is an XML-based protocol that uses security tokens containing assertions to pass information about a user between a SAML authority (an identity provider) and a web service (Zoom). Zoom works with Exchange ADFS 2.0 as well as Enterprise Identify Management such as PingOne, Okta, Centrify, Shibboleth, Gluu, OneLogin, Fugen, Symplified and many others. Zoom can map attributes to provision a user to different group with feature controls.

Oauth based provisioning works with Google or Facebook OAuth for instant provisioning.

Zoom also offers an API call to pre-provision user from any database backend.

Additionally, your company/university can add users to your account automatically with Managed Domains. Once your Managed Domain application is approved, all existing and new users with your email address domain will be added to your account.

Administrative Controls

The following security capabilities are available to the administrator:

- Secure login options using standard username and password or SAML Single Sign On.
- Add user and admin to account
- Upgrade or downgrade user subscription level
- Delete user from account
- Review billing and reports
- Manage account dashboard and cloud recordings

Special Security Features/Options API

A set of APIs is available for admins that are approved for use by Zoom. Each customer account managed by the admin will be given a pair of API key and passcode. The API calls are transmitted securely over secure web services and API authentication is required.

Meeting Connector

Zoom Meeting Connector is a hybrid cloud deployment method, which allows a customer to deploy Zoom multimedia router (software) within the company's internal network.

User and meeting metadata are managed in Zoom communications infrastructure, but the meeting itself is hosted in customer's internal network. All real-time meeting traffic including audio, video and data sharing go through the company's internal network. This leverages your existing network

security setup to protect your meeting traffic.

When customers choose a hybrid deployment, they have the option to segment by type of user where PRO and FREE (Basic) user type will use the cloud, and CORP user type will use the on-premise.

If on-premise is offline, the meeting will automatically revert to use the cloud. Both our cloud and on-premise solutions are designed with failover and load balancing mechanisms when deployed.

Zoom Rooms

Zoom Rooms combines video conferencing, wireless content sharing, and integrated audio into one easy to use platform designed to work with Mac and iPad devices. Communications are established over secured network using 256-bits TLS encryption standard and all shared contents are encrypted using AES256 encryption standard.

Zoom Rooms app is secured with App Lock Code. App Lock Code for Zoom Rooms is a required 1-16 digit numeric lock code that is use to secure your Zoom Room application. This prevents unauthorized changes to your Zoom Room application and settings on your iPad or Mac mini devices.

Webinar

Zoom webinar allows you to broadcast a Zoom meeting to up to 10,000 view-only attendee and invite up to 50 panelists. Panelists are full participants in the meeting. They can view and send video, screen share, annotate, etc. Panelist invitation are sent separately from the Webinar attendee. Zoom Webinar contents and screensharing are secured using AES256 and communicate over secured network using 256-bit encryption standard.

Registration Webinar

- Manually Approve Registration - The host of the Webinar will manually approve or decline whether a registrant receives the information to join the Webinar.
- Automatically Approve Registrants - All registrants to the Webinar will automatically receive information on how to join the Webinar

Registration-less Webinar

- One-Time - Attendees will join the webinar only once. After the webinar ends, attendees will not be able to use the same information to join the Webinar
- Recurring - Attendees will be able to repeatedly join the same Webinar with the information provided.

Recording Storage

Zoom offers our customers the ability to record and share their meetings. Recordings can be stored on the local device with local recording option or on Zoom's cloud with Cloud Recording option. Cloud recordings are processed and securely stored in Zoom's cloud once the meeting has ended. The recordings are stored in both video/audio format and audio only format. Recording originator can manage their recordings through the secured web interface. Recordings can be download, share or deleted. Local recordings are stored locally on the recording originator's hard drive.

Privacy

Zoom only stores basic information under user account profile information.

- Email address
- User password - salted hashed
- First Name
- Last Name
- Company Name
- Company Phone Number
- Profile Picture

For more information about our privacy policy, visit https://zoom.us/privacy

Billing Details

Zoom leverage a third-party, PCI compliant partner to process payment and handle all aspect of billing. We do not store any user credit card information or billing information in our database.

Conclusion

A growing number of businesses, small and large, use Zoom meeting services everyday. It is a high quality service for team meetings, sales interactions, marketing events, group mediation, product training, educational environments, and customer support. Zoom places privacy and security as the highest priority in the lifecycle operations of its communications infrastructure and meeting connector networks. In addition, Zoom strives to continually provide a robust set of security features to achieve its goal of providing the most efficient and secure real-time HD meeting service.