

Zoho Meeting Cloud Infrastructure

Zoho Meeting is a cloud-based, SaaS (Software-as-a-service) solution which helps you launch and join meetings and webinars directly from your computer using your web browser. We follow a highly secure **WebRTC Multipoint conferencing unit (MCUs)** based architecture. The MCU architecture assumes that each meeting/webinar participant sends their clubbed stream to the MCU. The MCU decodes each received stream, rescales it, composes a new stream from all received streams, encodes it, and sends a single stream to all other participants.

Zoho Identity and Account Management

Zoho Meeting ensures that only authorized administrators are allowed to manage and enforce Host - based privileges.

Our account administration module includes:

Account Management:

- Lock out an account after a considerable amount of failed

log-in attempts

- Account revival
- Account deactivation based on inactivity

Account Creation:

- Email verification of new accounts
- Single sign-on (SSO)
- Self-registration (sign-up) for new accounts

Account Passwords:

We enforce strong account password criteria, including:

- Mixed case
- Minimum length
- Minimum number of numeric characters
- Minimum number of alphabetic characters
- Minimum number of special characters
- No character to be repeated three times or more
- No reuse of a specified number of previous passwords
- No dynamic text (site name, Host's name, username)
- No passwords from a configurable list (for example, 'password')
- Minimum time interval before password change

- Change of account password by the Host at a configurable time interval
- Change of account password by all users at next log in

Organizational management

Zoho Meeting comes packed with several organizational management capabilities using which you can add team members to your Zoho Meeting account.

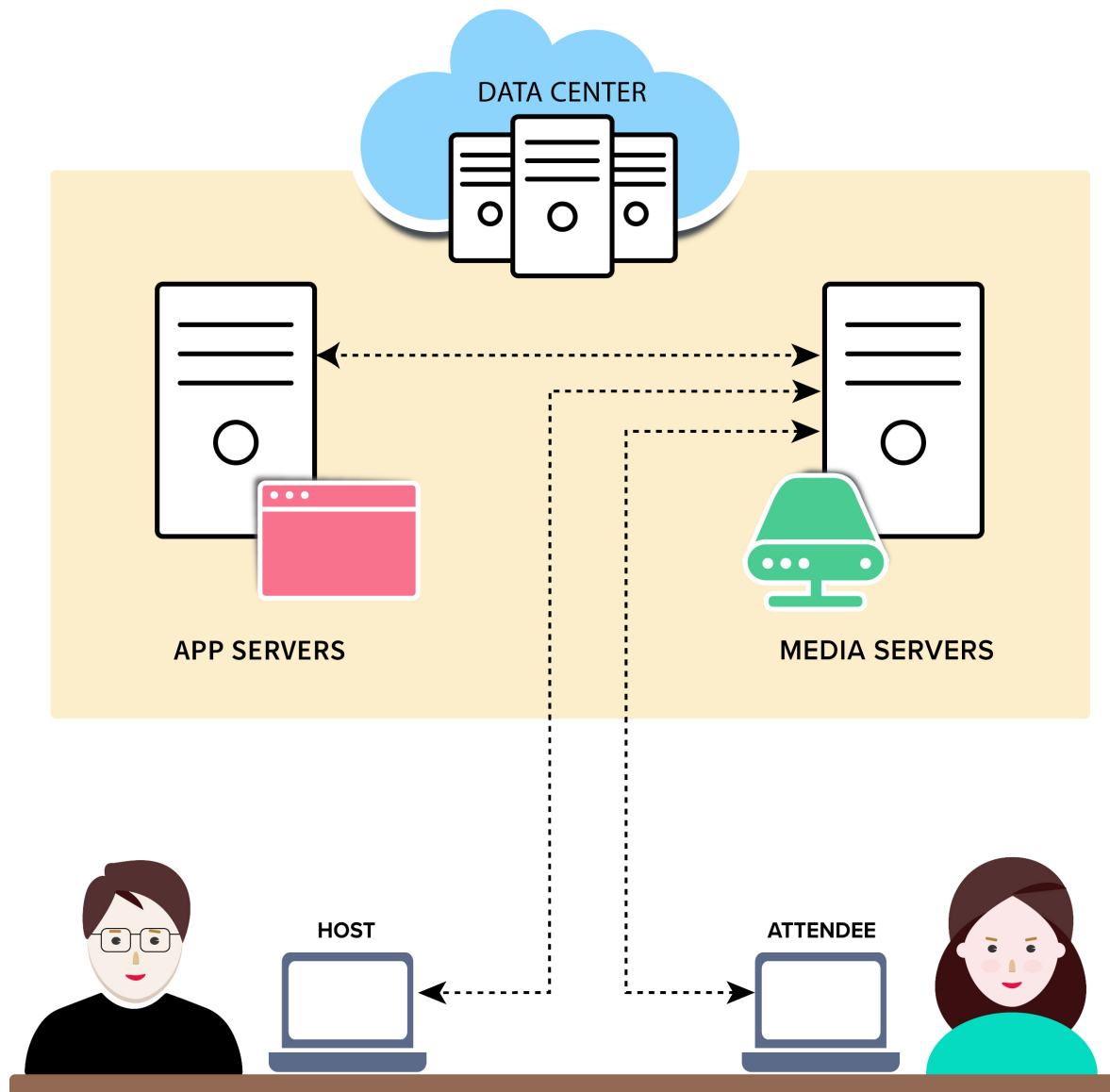
- Schedule team meetings and add members as presenters.
- Keep track of your events by automatically adding them to your email calendar as you receive meeting invitations and webinar registration notifications in your inbox.
- Manage team settings and notifications, and enable co-branding for meetings and webinars.

Industrial standard security and privacy

Zoho Meeting is entirely cloud-based; all data exchanged during a webinar or an online meeting takes place through **TLS 1.2 encrypted communication.**

What happens to your data?

To break it down into simple terms, all data collected from a user to create their Zoho Account, such as name and email address, is highly confidential and can only be shared as identification with other participants present in your online meeting or webinar based on your prior consent. Other data such as your chat transcripts, information regarding attendee performance, webinar registrant information, poll results, and Q&A information is only stored for the duration of the meeting or webinar to generate detailed session reports with the user's consent. This data is wiped from data servers immediately when the user deletes the respective session report.



Encryption at transit:

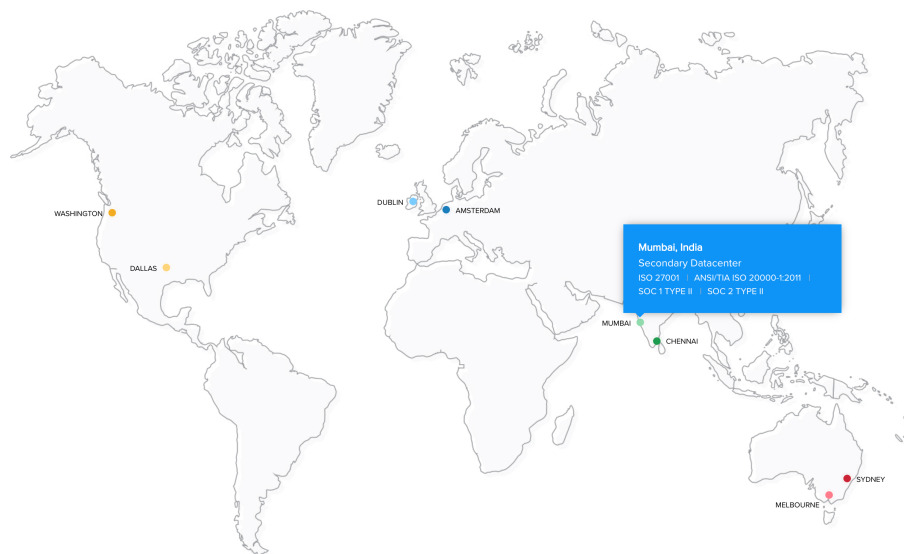
Customer data transmitted to our servers is protected by strong encryption protocols. We have enabled **HTTP Strict Transport Security header (HSTS)** to all our web connections to ensure

data protection while initiating a webinar or an online meeting session using our web-portal.

Data Center:

Access to our data centers, which stores sensitive information, is limited. The activity at our data centers is monitored round the clock by security personnel with the help of the state-of-the-art CCTV surveillance. Moreover, our data centers are protected by Multi-factor authentication, which includes biometric scanning to ensure maximum security.

Location of Datacenters



App Servers:

Application servers are responsible for all user authentication and organizational management activities inside Zoho Meeting.

Media Servers:

Media servers are responsible for the initiation of an online meeting or a webinar session between the Host/Presenter and the Attendees.

Where do we store your data?

Customer data is stored in our data centers based on the default domain location of the customer.

- <https://meeting.zoho.in> users' data will be stored in India.

If you integrate with other third-party applications, the data will be stored in their respective storage locations. This statement also holds true when Zoho Meeting uses third party sub processors.

Note:

- We have our own Live Chat (Zoho SalesIQ) which empowers our Live chat in product and website pages.
- All user tickets and feedback are processed by **Zoho Desk**, our in-house Customer Support Tool.
- All customer data is stored in **Zoho CRM**, our own Customer Management software.

Recorded sessions are safely encrypted at rest and stored on our media servers and sent via email to the hosts of the respective online meeting or webinar. The recorded session can also be accessed through the host's verified Zoho Meeting account as well.

How long is your data stored?

In our media servers (a server that handles audio, video, and screen sharing related information), the recorded sessions **will be deleted after 24 hours**. In case of a Data File Storage upload failure, the targeted data file **will be deleted in 48 hours, and the user will be notified and kept updated proactively**.

Traditionally, when you host a webinar or a meeting using

Zoho, the connection will be established using the nearest gateway i.e., data will be transmitted to the nearest server (geographically speaking) in your location. For example, if you're in the US, you'll connect with one of our servers based in the US. If you're in Europe, you'll connect with one of our servers based in Europe.

In order to ensure maximal security for the Government of India, Zoho has added several distinct servers located in Mumbai for data storage and transmission. Every meeting/webinar hosted from your account will be mapped through these new servers irrespective of the geographic location. Thus, we can guarantee that the data collected, processed, and stored inside India, stays inside India at all times and does not leave India.

Encryption at rest:

Customer data at rest is encrypted using a **256-bit Advanced Encryption Standard (AES)**. We own and maintain the keys using our in-house **Key Management Service (KMS)**.

[Learn more.](#)

Security features in Zoho Meeting

Maintain complete control of your online meetings

If you feel apprehensive about having confidential discussions online, **locking meetings** will help you keep your information private. Locking meetings gives the meeting host complete control over who enters a meeting. The meeting host gets a notification every time someone requests to enter their meeting and can accept or decline the request; **ergo nobody can enter a locked meeting without the permission of the meeting host.** This will help you secure your meetings from online intruders like hackers or abusers.

Remove participants and use recording privileges

If someone shares your meeting link with an outsider and they enter your meeting, you can easily remove them and lock your meeting to prevent further intrusion. Only the meeting host can record a meeting and get access to the recording after the meeting session. The host can also decide not to share the recording link with others if there are safety concerns.

Ring notifications for entry and exit

Your organization's admin can enable sound notifications for entry and exit of participants during online meetings. This helps the meeting host keep an eye on who joins their meeting and remove participants who should not be part of the discussion.

Consent for sharing audio and video

Zoho Meeting protects your privacy by giving you complete control over sharing your audio and video during a meeting. You can enable or disable your audio and video before entering a meeting or any time you want during a meeting. Admins can disable video meetings altogether in their organization, if required. Zoho Meeting also asks your permission before enabling remote access for another participant to your computer during screen sharing. To ensure user-privacy and security, session recording will be switched off by default. Users are recommended to enable session recording only when it is required.

Respecting Users' Browser sandboxing protocol

At Zoho, we respect our users' operating system privacy and

browser sandboxing techniques. Thus all features including but not limited to **Audio/Video/Screen sharing** are enabled by **strict adherence to the rules set by the users' browser/Operating System of their choice.**

Zoho Meeting does not tamper with the installers or bypass any of the Operating System security mechanisms by installing Web browsers etc.

Risks and Controls

We have made sincere efforts to secure our processing environment. As a user, depending on your organizational policies, you may need to configure some of the system settings in order to comply with your organizational policies and applicable data protection laws.

S.NO	Risks	Risk Mitigation and Controls	Residual Risks
------	-------	------------------------------	----------------

1.	Being a web-based application, Zoho Meeting is vulnerable to online data theft.	<p>The security framework is designed to mitigate the Open Web Application Security Project (OWASP) vulnerabilities.</p> <p>Furthermore, we run a static code analysis tool to ensure maximum security.</p>	-
2.	Increase in number of customers/ Usage by customers	<p>Multiple application servers and load balance support are there to handle an increase in the number of requests to a server caused by the rise in customers/usage.</p> <p>Horizontal scaling can be used to solve this. Data clusters with master-slave configurations are there as well. Server Monitoring events are being sent to</p>	-

		the Zoho Meeting server team for events like connection exhaust, MySQL down, etc.	
3.	Data interception by hackers during data transit	All data transmissions during backup and in flight are encrypted using Transport Layer Security (TLS) 1.2 protocols.	Users should avoid sharing invitation links to anyone other than the intended participants.
6.	Application is not accessible.	Customer data is stored and continuously synchronized between Zoho's primary and secondary data centers. In case of any disaster that may occur at the primary data center, the secondary data center will serve, ensuring data availability.	-

7.	DDoS attack.	At the application level, proper thresholds and lock periods are configured for the request URLs. At the network level we have centralized DDoS protection.	Users can check the service availability status at status.zoho.com
8.	SPAM	We provide disclaimer information to the end user in all invitations and mailing options.	Users should send invites only to those with whom they want to collaborate remotely.
11.	Interruption of meeting due to ISP or downtime of a server.	Zoho has a geographical distribution of gateways. If one gateway goes down or is unreachable, the other gateway will work as its replacement.	Users can get in touch with our dedicated technical support team who are available 24x7.

13.	Application blocking due to anti-virus	On regular release basis, we send our application to be whitelisted by anti-virus vendors.	Try whitelisting the Zoho Meeting app in your anti-virus software
15.	Reusing the key	Session key expiration is based on proper session termination/completion, or after 15 mins of session termination.	Close/Exit the meeting properly after the session ends.
17.	Mishandling / accidental deletion of data.	As long as the domain is valid and the deleted device is not the only device or the master agent, the deleted device can be reinstalled.	Users can get in touch with our dedicated technical support team who are available 24x7.

Privacy Data sheet:

Zoho Meeting allows users to connect with one another via virtual meetings with face-to-face video communication, screen sharing and instant messaging. If your organization uses Zoho Meeting, the account Administrator serves as the “data controller ” for user generated content.

These settings allow the account administrator to enable or disable features for your meetings such as camera and microphone usage, along with various co-branding options.

The host can admit attendees to a meeting, mute participants, remove participants and also record meetings. The host will receive the recording via email after the meeting and will also be access it from their Zoho Meeting account.

Personal Data	Data Type	Purpose for processing
Registration Information	<ul style="list-style-type: none">● Name● Email Address● Password● Public IP Address● Browser● Phone Number	<p>We use Registration Information to:</p> <ul style="list-style-type: none">● Provide and enlist you in our service● Provide technical support● Notify you about product

	<p>(Optional)</p> <ul style="list-style-type: none">● Mailing Address (Optional)● Geographic region● Billing Information● User information included in the Zoho User ID (ZUID)	<p>updates</p> <ul style="list-style-type: none">● Process payment and billing details
Host and Usage Information	<ul style="list-style-type: none">● IP Address● User Agent Identifier● Hardware Type● Operating System Type and versions● Client Version● IP Addresses along with the Network Path● MAC address of Your Client (As	<p>We use Host and Usage Information to:</p> <ul style="list-style-type: none">● Understand how the service is used● Respond to customer support queries● Improve product quality● Generate product usage stats

Applicable)

- Service Version
- Actions Taken
- Geographic Region
- Meeting Session Information (title, date and time, frequency, average and actual duration, quantity, quality, network activity, and network connectivity)
- Number of meetings
- Number of screen-sharing and Non screen-sharing sessions
- Number of participants

- Meeting Host Information*
 - Host Name
 - Meeting Site URL
 - Meeting Start/End Time
- Screen Resolution
- Join Method
- Performance, Troubleshooting,

Call attendee information including email addresses, IP address, username, phone numbers, room device information

* Used for billing purposes.

Personal Data Security

Zoho Meeting has taken necessary technical and organizational security measures which are designed to protect your personal data from unauthorized use or disclosure. Here is how your data is encrypted.

Type of Data	Type of Encryption
Registration Information	Encrypted at both transit and rest
Passwords	Encrypted and hashed at both transit and at rest
Host and Usage information	Encrypted at both transit and rest

Third Party Service Providers (Sub-processors)

Zoho evaluates the security and privacy practices of sub-processors whom we wish to contract to ensure that they are

in line with Zoho's information security and privacy standards. We then execute appropriate data protection agreements with them. Sub-processors used by Zoho Meeting are as follows:

Entity name	Purpose	Location of processing
Tata communications	To provide in-bound dialling services	USA- LA, NY ,Canada- Montreal, Toronto, Europe- London, Frankfurt and Madrid,Asia- Singapore, HK and Australia
Voxbone	To provide in-bound dialling services	Belgium, Germany,Hong Kong, USA

Usage of Third party Software Development Kit

Zoho doesn't use any third party Software Development Kit (SDKs) or code belonging to other companies. We develop and maintain our own **Two Factor Authentication mechanism, Captcha mechanism** to ensure that the highest level of user privacy and security is offered to our esteemed users.

For third party federated logins, we develop a separate code

(with our Gadgets team) to ensure that personal user data stays within our servers.

Third party Advertisements

Zoho has never put users at risk by selling or disclosing their information to unauthorized third parties, and we never will. This has been our approach for almost 20 years, and we remain committed to it. We do not have any third party trackers on our website and within the application. At any point of time, Zoho does not serve any third party advertisement to users.

Certification and Compliance

What is an ISMS?

An ISMS is a systematic approach to managing sensitive company information so that it remains secure. It includes people, processes, and IT systems by applying a risk management process.

It can help small, medium, and large businesses in any sector keep information assets secure.

ISO 27001, 27017, and 27018

International Organization for standardization is widely known for its development of globally acknowledged standards such as the ISO/IEC 27001 series, which provides the requirement for an information security management system ([ISMS](#)). Zoho has achieved its certification for ISO 27001 in 2016 and is renewed every three years with an annual external audit.

GDPR

Zoho has always demonstrated its commitment to its user's data privacy by consistently exceeding industry standards. Zoho welcomes GDPR as a strengthening force of the privacy-consciousness that already exists in it.

Zoho's offerings have privacy features that comply with GDPR, and Zoho's processing of its customer's data adheres to the data protection principles of the GDPR. To know more about how Zoho complies with GDPR, [click here](#).

SOC 2

Zoho is SOC 2 Type II compliant. SOC 2 is an evaluation of the design and operating effectiveness of controls that meet the AICPA's Trust Services Principles criteria.



Reach us at support@zohomeeting.com / sales@zohocorp.com for any clarifications. If you would like a live demo, please raise your request [here](#).

Zoho Meeting is a product of Zoho Corporation Pvt Ltd. Zoho offers a comprehensive suite of award-winning online business, productivity and collaboration applications. With headquarters in Chennai, India and offices in Austin, Pleasanton, London, Tokyo and Beijing, ZOHOO Corporation serves the technology needs of more than 50 million users worldwide.

For more information about Zoho, please visit:
<https://www.zoho.com/aboutus.html>