



---

# AI Companion Security and Privacy

---

This whitepaper describes Zoom AI Companion’s security and privacy features as of the date of publication and not other AI products or services offered by Zoom. In our continuing commitment to empowering productivity – while keeping security and privacy at the core of our products – the features described in this paper may evolve. AI Companion features for Zoom Contact Center are not included in the whitepaper at this time.

WHITEPAPER



## Table of Contents

03	<b>Zoom AI Companion</b>
03	<b>Our Commitment to Responsible AI</b>
04	<b>Data Flow and Transmission to Third Parties</b>
05	<b>Data Processing, Storage, and Retention</b>
06	<b>AI Companion Features</b>
14	<b>Putting You In Control of AI Companion Capabilities</b>
17	<b>Data Protection</b>
18	<b>Secure Development of Generative AI Features</b>
19	<b>Generative AI Model Security</b>
19	<b>Security Assessments</b>
19	<b>Vulnerability Disclosure Program</b>
19	<b>AI Companion Compliance</b>
20	<b>Changelog</b>

## Zoom AI Companion

Zoom AI Companion, Zoom's generative AI assistant, empowers individuals by helping them be more productive, connect and collaborate with teammates, and improve their skills. Zoom AI Companion is a set of generative AI features that can be enabled across the Zoom platform.

Zoom's unique federated approach to generative AI is designed to deliver high-quality results by dynamically incorporating Zoom's artificial intelligence models as well as third-party artificial intelligence models provided by subprocessors, such as OpenAI and Anthropic. With this approach, AI Companion can incorporate innovations in artificial intelligence models while providing users with the benefits of improved quality and performance.

---

## Our Commitment to Responsible AI

Zoom is committed to developing AI responsibly, with security and privacy at the core of the generative AI capabilities it provides to its customers, just as they are across the Zoom platform. Zoom recognizes that generative AI presents an evolving set of risk considerations for its customers, and the company is committed to prioritizing transparency and customer choice as it brings generative AI features to market.

In line with these commitments, Zoom has announced that it does not use any customer audio, video, chat, screen sharing, attachments, or other communications-like customer content (such as poll results, whiteboard, and reactions) to train Zoom's or its third-party artificial intelligence models.

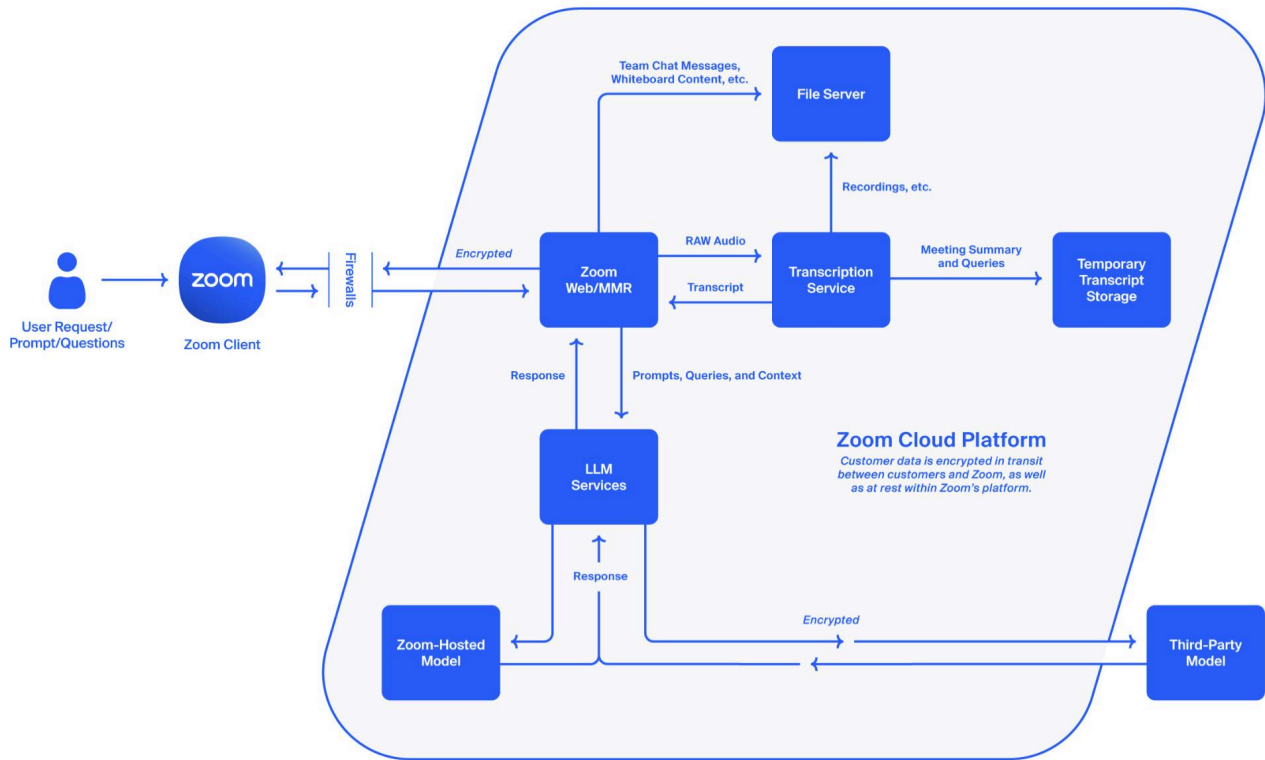
Zoom provides controls at the account, group, and user levels, allowing administrators to select which AI Companion features or capabilities they wish to enable for specific Zoom product offerings and which users have access. For example, for Zoom Meetings, administrators can enable the AI Companion features at the account level and meeting hosts can choose whether to activate them for specific meetings. To provide transparency, meeting participants will see an in-product notification describing the generative AI Companion capabilities that are activated for that meeting.

## Data Flow and Transmission to Third Parties

### Data Flow

Data used by AI Companion is sent from the user to Zoom-hosted and/or third-party generative artificial intelligence models. Customer data in transit is encrypted between customers and Zoom, between Zoom services, and any third-party models. Customer data is also encrypted at rest within Zoom’s platform.

The following diagram is an example of the general flow through Zoom systems and, where relevant, to third-party models:



### Third-Party Subprocessors

As part of Zoom’s federated approach to AI, artificial intelligence models from third parties, such as Anthropic and OpenAI, may be used for certain AI Companion features alongside Zoom’s artificial intelligence models to provide high-quality results.

Zoom requires its subprocessors to satisfy obligations equivalent to those outlined in [Zoom’s Data Processing Agreement](#). Zoom’s subprocessors are subject to security assessments on at least an annual basis as part of Zoom’s third-party risk management program. Zoom’s third-party risk management controls are assessed by independent audit firms in many of its security certifications and attestations, which are available to customers on [Zoom’s Trust Center](#).

## Data Processing, Storage, and Retention

### Data Usage

Zoom does not use any customer audio, video, chat, screen sharing, attachments, or other communications-like customer content (such as poll results, whiteboard, and reactions) to train Zoom's or its third-party artificial intelligence models.

Zoom AI Companion features must use certain content to provide the service.

### Data Access

Consistent with Zoom's [Privacy Statement](#), Zoom employees may not access or use customer content, including meeting, webinar, messaging, or email content (specifically, audio, video, files, in-meeting whiteboards, messaging, or email content), any content generated or shared as part of other collaborative features (such as out-of-meeting whiteboards), or content generated by AI Companion, unless authorized by the account owner or administrator of the account hosting the Zoom product or service where the customer content was generated, or as required for legal, safety, or security reasons.

### Model Usage and Processing

Zoom's federated approach to AI utilizes multiple models to provide its AI Companion features. Below is a summary of the models used for AI Companion. AI Companion strategically leverages these models to provide high-quality results in response to users' interactions with Zoom's product.

- Zoom-hosted models\*
- Anthropic models (e.g., Claude Instant, Claude 3)
- OpenAI models (e.g., GPT-4, DALL-E 3)

### Model Provider Data Storage and Retention

In general, Zoom stores and retains customer content and personal data for as long as required to engage in the uses described in its [Privacy Statement](#), unless a longer retention period is required by applicable law.

**After providing the AI Companion service, Zoom may retain the customer content (see tables below) for up to 30 days for support and debugging purposes\*** unless a longer retention period is required by applicable law, including for trust and safety purposes. In the context of data retention and processing, "trust and safety purposes" refers to measures taken to protect the safety and integrity of a service and its users. This involves retaining certain data for a period of time to help prevent abuse and misuse. Additional information on Zoom's Trust and Safety processes may be found in [Zoom's Safety Center](#). In addition, certain outputs may be stored in accordance with the customer's retention settings or policies, as described under "Customer Data Storage and Retention" and in the tables below.

If the AI Companion feature relies on a third-party artificial intelligence model, pursuant to Zoom's contracts, **the third-party model provider may retain the content used to provide the service for trust and safety purposes, within the U.S., for up to 30 days**, unless a longer retention period is required by applicable law.

#### \* IMPORTANT NOTE

Zoom offers a **Zoom-hosted Models Only (ZMO)** option, which means that data will **not be sent to third-party models for processing**.

To enable this feature please reach out to your account team or log a support ticket.

#### \* IMPORTANT NOTE

Zoom offers a **Zero Data Retention (ZDR)** option for the **temporary transcript used to provide a Meeting Summary**. When enabled, this temporary transcript **will be deleted immediately** after the summary is created. If a summary fails to be created it will be retained for up to 24 hours to allow for retries.

To enable this feature please reach out to your account team or log a support ticket.

## Customer Data Storage and Retention

Customers may choose Zoom’s storage location for some of the AI Companion outputs for their account. These settings differ based on the feature in use, and many align with existing retention policies of the related Zoom product.

## AI Companion Features

Below is a summary of each AI Companion feature as of the date of this whitepaper. This includes the content used or generated by the feature, where the model provider processes and stores the content, and if applicable, the customer storage location and relevant retention settings and policies that apply in addition to the model provider’s 30-day retention period.

### Meetings

AI Companion Feature	Content Used or Generated	Model Provider - Data Processing/Storage Location	Customer Storage Location (if applicable)	Customer Retention Controls and Additional Information (if applicable)
<b>Smart Recordings</b> Review cloud recordings faster through highlights, smart chapters, summaries, next steps, and more.  <div style="background-color: #663399; color: white; padding: 5px; border-radius: 5px; display: inline-block;">Zoom-hosted Models Only (ZMO) Eligible</div>  Minimum Recommended Client Version: 5.16.5	Cloud recording (input)	Zoom - Meeting host’s <a href="#">content storage location</a>  OpenAI - US Anthropic - US	Meeting host’s <a href="#">content storage location</a> .	Follows meeting host’s configured <a href="#">cloud recording retention settings</a> .
	Audio transcript (input)			
	Recording highlights, smart chapters, next steps, meeting coach metrics (output)			

## Meetings - Continued

AI Companion Feature	Content Used or Generated	Model Provider - Data Processing/Storage Location	Customer Storage Location (if applicable)	Customer Retention Controls and Additional Information (if applicable)
<p><b>Meeting summary</b></p> <p>Generate a summary and next steps of what was discussed in your meeting and share through email and Team Chat.</p> <p>Transcription begins once the meeting summary feature is activated by the meeting host.</p> <p><b>Zoom-hosted Models Only (ZMO) Eligible</b></p> <p><b>Minimum Recommended Client Version: 5.14.2</b></p>	<p><b>Audio transcript (input)</b></p> <p><b>Zero Data Retention (ZDR) Eligible</b></p>	<p>Zoom - Meeting host's <a href="#">"live transcript" location</a></p> <p>OpenAI - US Anthropic - US</p>		
	<p><b>Meeting summary (output)</b></p>	<p>Zoom - Meeting host's <a href="#">content storage location</a></p> <p>OpenAI - US Anthropic - US</p>	<p>Meeting host's <a href="#">content storage location</a></p>	<p>Summaries are stored in the web portal in accordance with the account, group, and/or user retention settings.</p> <p>Summaries shared within the continuous meeting chat are stored in accordance with the customer's <a href="#">Zoom Team Chat retention settings</a>.</p> <p>Admins and users can choose whether the full text of a meeting summary or just a link to the summary is shared via email. This can be managed at the account, group, and user level.</p> <p>Emails are stored in accordance with the customer's retention settings with the email provider.*</p>
<p><b>Meeting questions</b></p> <p>Quickly catch up and get clarity on what you missed before you joined a meeting without interrupting it.</p> <p>Transcription begins once the meeting questions feature is activated by the meeting host.</p> <p><b>Minimum Recommended Client Version: 5.15.12</b></p>	<p><b>Audio transcript (input)</b></p>	<p>Zoom - Meeting host's <a href="#">"live transcript" location</a></p> <p>OpenAI - US Anthropic - US</p>		
	<p><b>Question (input)</b></p>	<p>Zoom - Meeting host's <a href="#">content storage location</a></p> <p>OpenAI - US Anthropic - US</p>		
	<p><b>Answer (output)</b></p>			

\*Zoom uses Twilio Sendgrid as its email provider to deliver the **meeting summary** or link to the meeting summary (depending on the customer's settings). Twilio Sendgrid uses a process that takes random content samples of emails and retains the information for 7 days for anti-fraud purposes and troubleshooting.

## Email and Calendar

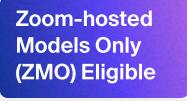
AI Companion Feature	Content Used or Generated	Model Provider - Data Processing/Storage Location	Customer Storage Location (if applicable)	Customer Retention Controls and Additional Information (if applicable)
<b>Email compose</b> Compose and reply to emails faster using AI to draft your message based on user prompts.  <b>Minimum Recommended Client Version: 5.15.0</b>	<b>User prompt (input)</b>	Zoom - Customer's <a href="#">provisioned data center</a>  OpenAI - US Anthropic - US		
	<b>Email draft (output)</b>		Customer Email Provider	Emails are stored in accordance with the customer's retention settings with the email provider.

## Team Chat

AI Companion Feature	Content Used or Generated	Model Provider - Data Processing/Storage Location	Customer Storage Location (if applicable)	Customer Retention Controls and Additional Information (if applicable)
<b>Chat compose</b> Draft Team Chat messages based on conversational context and user prompts, and customize tone and length of drafted chat messages.  <b>Minimum Recommended Client Version: 5.14.10</b>	<b>Chat message text for the selected chat thread (input)</b>	Zoom - Customer's <a href="#">provisioned data center</a>  OpenAI - US Anthropic - US		
	<b>Chat participant names (input)</b>			
	<b>User prompt (input)</b>			
	<b>Message draft (output)</b>		Customer's <a href="#">provisioned data center</a>	If the output is posted to the chat, the chat message is stored in accordance with the customer's <a href="#">Zoom Team Chat retention settings</a> .



## Team Chat - Continued

AI Companion Feature	Content Used or Generated	Model Provider - Data Processing/Storage Location	Customer Storage Location (if applicable)	Customer Retention Controls and Additional Information (if applicable)
<b>Thread Summary</b> Quickly summarize the content of long Team Chat threads.    <b>Minimum Recommended Client Version: 5.16.0</b>	<b>Chat message text for the selected chat thread (input)</b>	Zoom - Customer's <a href="#">provisioned data center</a>  OpenAI - US Anthropic - US		
	<b>Chat participant names (input)</b>			
	<b>Thread summary (output)</b>			
<b>Quick Scheduling</b> Automated recommendations to schedule meetings based on conversational context.  <b>Minimum Recommended Client Version: 5.16.10</b>	<b>Chat message text, participant names and emails (input)</b>	Zoom - Customer's <a href="#">provisioned data center</a>  OpenAI - US Anthropic - US		
	<b>Schedule suggestion (output)</b>			
<b>Sentence Completion</b> Automated recommendations to quickly complete messages in real time as you type.  <b>Minimum Recommended Client Version: 5.17.0</b>	<b>Chat message text (input)</b>	Zoom - Customer's <a href="#">provisioned data center</a>  OpenAI - US Anthropic - US		
	<b>Message draft (output)</b>			



## Whiteboard

AI Companion Feature	Content Used or Generated	Model Provider - Data Processing/Storage Location	Customer Storage Location (if applicable)	Customer Retention Controls and Additional Information (if applicable)
<b>Content generation</b> Generate ideas and mind maps, refine and extend existing content, and add objects to a canvas.	<b>Whiteboard content (input)</b>	Zoom - User's <a href="#">content storage location</a>  OpenAI - US Anthropic - US		
	<b>User prompt (input)</b>			
<b>Minimum Recommended Client Version: 5.16.0</b>	<b>Whiteboard content (output)</b>		User's <a href="#">content storage location</a>	If the output is posted to the whiteboard, the whiteboard content is stored in accordance with the customer's <a href="#">Whiteboard retention settings</a> .

## Phone

AI Companion Feature	Content Used or Generated	Model Provider - Data Processing/Storage Location	Customer Storage Location (if applicable)	Customer Retention Controls and Additional Information (if applicable)
<b>Post call summary and next steps</b>  Ability to request a post call summary when using AI Companion with a recorded phone conversation.	<b>Audio transcript (input)</b>	Zoom - US OpenAI - US Anthropic - US		
	<b>Call summary (output)</b>			
<b>Minimum Recommended Client Version: 5.17.0</b>	<div style="background-color: #6666ff; color: white; padding: 2px; display: inline-block;">Zoom-hosted Models Only (ZMO) Eligible</div>		US	Summaries are stored until deleted by the user or account administrator, or until the user or customer account is terminated.

Phone - Continued

AI Companion Feature	Content Used or Generated	Model Provider - Data Processing/Storage Location	Customer Storage Location (if applicable)	Customer Retention Controls and Additional Information (if applicable)
<b>Voicemail tasks</b> Ability to extract key action items and tasks from voicemails without listening to the voicemail recording.    <b>Minimum Recommended Client Version: 5.17.0</b>	<b>Audio transcript (input)</b>	Zoom - US OpenAI - US Anthropic - US		
	<b>Voicemail task (output)</b>		US	Follows the site's configured <a href="#">voicemail retention policy</a> .
<b>Voicemail prioritization</b> Get a list of the highest priority voicemails based on the content of the recording.  <b>Minimum Recommended Client Version: 5.17.5</b>	<b>Audio transcript (input)</b>	Zoom - US OpenAI - US Anthropic - US		
	<b>User priority labels (input)</b>			
	<b>Voicemail priority (output)</b>		US	Follows the site's configured <a href="#">voicemail retention policy</a> .
<b>Team SMS thread summary</b> Receive a summary of a team SMS chat thread.    <b>Minimum Recommended Client Version: 5.16.5</b>	<b>SMS message content (input)</b>	Zoom - US OpenAI - US Anthropic - US		
	<b>SMS participant names (input)</b>			
	<b>Thread summary (output)</b>			

## Events

AI Companion Feature	Content Used or Generated	Model Provider - Data Processing/Storage Location	Customer Storage Location (if applicable)	Customer Retention Controls and Additional Information (if applicable)
<b>Chat compose</b>  Draft chat messages based on conversational context and user prompts, and customize tone and length of drafted chat messages.  <b>Minimum Recommended Client Version:</b> N/A	<b>Chat message text for the selected chat thread (input)</b>	Zoom - Customer's <a href="#">provisioned data center</a>  OpenAI - US Anthropic - US		
	<b>Chat participant names (input)</b>			
	<b>User prompt (input)</b>			
	<b>Message draft (output)</b>		Customer's <a href="#">provisioned data center</a>	Messages posted during an event are only accessible while the event is live.
<b>Email compose</b>  Compose emails faster using AI to draft your message based on user prompts.  <b>Minimum Recommended Client Version:</b> N/A	<b>User prompt (input)</b>	Zoom - Customer's <a href="#">provisioned data center</a>  OpenAI - US Anthropic - US		
	<b>Email draft (output)</b>			
<b>Smart compose</b>  Create compelling event content when setting up an event, including event and session descriptions, speaker bios, lobby announcements, and more.  <b>Minimum Recommended Client Version:</b> N/A	<b>User prompt (input)</b>	Zoom - Customer's <a href="#">provisioned data center</a>  OpenAI - US Anthropic - US		
	<b>Event content (output)</b>			

**Events - Continued**

AI Companion Feature	Content Used or Generated	Model Provider - Data Processing/Storage Location	Customer Storage Location (if applicable)	Customer Retention Controls and Additional Information (if applicable)
<p><b>Image Generation</b></p> <p>Event hosts can save on resources by using AI Companion to generate images for emails, the event page, or in-event content.</p> <p><b>Minimum Recommended Client Version:</b> N/A</p>	<p><b>User prompt (input)</b></p>	<p>Zoom - Customer's <a href="#">provisioned data center</a></p> <p>OpenAI - US Anthropic - US</p>		
	<p><b>Image (output)</b></p>		<p>Customer's <a href="#">provisioned data center</a></p>	<p>Event content will be publicly available in accordance with the customer's configuration of Zoom Events settings, for up to two years.</p>

# Putting You In Control of AI Companion Capabilities

Zoom is committed to providing transparency and choice when it comes to enabling and using AI Companion features. Account administrators and users are provided with controls for AI Companion features. Zoom is continually working to enhance its platform and educate users on new features. Currently, users will see certain in-product notifications, which may be updated over time.

## Account Administrator Controls

Zoom AI Companion is off by default for all accounts. Account owners and administrators control whether to enable the AI Companion features for their accounts.

Administrators may enable or disable features for their entire account within the account settings page in the Admin Portal. For some features that are managed outside of the AI Companion tab, links are provided to the relevant settings.

The screenshot shows the Zoom Admin Portal interface. At the top, there is a navigation bar with the Zoom logo, links for Products, Solutions, Resources, and Plans & Pricing, and utility links for Search, Support, 1.888.799.0125, Contact Sales, and Request a Demo. Below this is a secondary navigation bar with links for Schedule, Join, Host, and Web App. The main content area is titled 'AI Companion' and contains the following sections:

- Meeting Summary with AI Companion:** A toggle switch is turned on. A lock icon is present. Below it, a checkbox is checked for 'Automatically start Meeting Summary for all meetings I host'. A description states: 'Allow hosts to generate a summary. Summaries are sent to participants after the meeting has ended.'
- Automatically share summary with:** A radio button is selected for 'Only meeting host and meeting invitees in our organization'. Other options are 'Only meeting host' and 'All meeting invitees including those outside of our organization'. A lock icon is present.
- AI Companion Questions:** A toggle switch is turned on. A lock icon is present. Below it, a checkbox is checked for 'Automatically start AI Companion questions for all meetings I host'. A description states: 'Allow hosts and invited participants to ask questions to the AI Companion during a meeting. Questions are answered based on the conversation transcript.'
- Who can ask questions to AI Companion?:** A radio button is selected for 'Only hosts'. Other options are 'All participants' and 'All participants only from when they join'. A lock icon is present.
- Recording:** A section header for 'Smart Recording with AI Companion'. A toggle switch is turned on. A lock icon is present. A description states: 'By enabling it, your cloud recording can have recording highlights, summary and smart chapters, next steps, and meeting coach, technology, which may include third-party models.'

A sidebar on the left lists various account management options, with 'Account Settings' highlighted. A user profile icon is visible in the bottom right corner of the interface.

## Group Controls

Account owners and admins can control which groups receive certain AI Companion features. Select features may be enabled or disabled, and the ability to turn features on or off may be locked. Users belonging to the group will have their feature access dictated by account administrator selections. If enabled by the account administrator at the group level, users may enable or disable features for themselves at the individual user level.

Note: Group-level controls are available for Zoom Meetings, Team Chat, Whiteboard, and Mail and Calendar features.

The screenshot shows the Zoom Admin console interface. At the top, there is a navigation bar with the Zoom logo, links for Products, Solutions, Resources, and Plans & Pricing, and utility links for Search, Support, 1.888.799.0125, Contact Sales, and Request a Demo. Below this is a secondary navigation bar with links for Schedule, Join, Host, and Web App. The left sidebar contains a menu with categories like Recordings, AI Companion, Clips, Scheduler, Settings, Data & Privacy, Reports, and ADMIN. Under ADMIN, there are sub-sections for Plans and Billing, Dashboard, User Management (Users, Groups, Roles, Contacts), Device Management, Node Management, Room Management, Workspaces Management, Phone System Management, Account Management, and Advanced. The main content area is titled 'AI Companion' and shows settings for a group. It includes a notice that Zoom does not use user data for training AI models and a link to support. The settings are organized into sections: Meeting, AI Companion Questions, and Recording. Each section has a toggle switch, a lock icon, and 'Modified' and 'Reset' links. The 'Meeting' section includes 'Meeting Summary with AI Companion' (enabled), 'Automatically start Meeting Summary for all meetings I host' (checked), and radio buttons for 'Only meeting host', 'Only meeting host and meeting invitees in our organization', and 'All meeting invitees including those outside of our organization'. The 'AI Companion Questions' section includes 'AI Companion Questions' (enabled), 'Automatically start AI Companion questions for all meetings I host' (checked), and radio buttons for 'All participants', 'All participants only from when they join', and 'Only hosts'. The 'Recording' section includes 'Smart Recording with AI Companion' (enabled) and a note that it uses account settings.

## User and In-Meeting Controls

Account owners and administrators control whether to enable Zoom AI Companion for their accounts. For features with user-level controls, Zoom provides users with control and visibility into their AI Companion features' settings. Users may see if their administrators have enabled or disabled AI Companion features. If allowed by the account administrator for features with user-level controls, users can enable or disable AI Companion features for their own use. If the administrator has locked the setting at the account or group level, the user cannot change the setting.

Note: User-level controls are available for Zoom Meetings and Whiteboard features.

The screenshot shows the Zoom Admin Center interface. The top navigation bar includes the Zoom logo, links for Products, Solutions, Resources, and Plans & Pricing, and utility links for Search, Support, 1.888.799.0125, Contact Sales, and Request a Demo. The left sidebar contains a menu with categories like Recordings, AI Companion, Clips, Scheduler, Settings, Data & Privacy, Reports, and ADMIN. The main content area is titled 'Settings' and is divided into sections for Meeting, Recording, and Whiteboard. The 'Meeting' section includes 'Meeting Summary with AI Companion' (enabled), 'Automatically start Meeting Summary for all meetings I host' (checked), and 'Automatically share summary with' (set to 'Only myself (meeting host) and meeting invitees in our organization'). The 'AI Companion Questions' section is also enabled, with 'Automatically start AI Companion questions for all meetings I host' checked and 'Who can ask questions to AI Companion?' set to 'Only hosts'. The 'Recording' section shows 'Smart Recording with AI Companion' enabled and 'Recording highlights' checked. A blue circular icon with a white question mark is visible in the bottom right corner of the settings area.

Meeting hosts may enable or disable AI Companion features in meetings. Participants may also request that the host enable these features in-meeting by clicking the respective AI Companion icon if the admin has enabled the option for the icon to be visible in the Meetings toolbar. Currently, when meeting participants join a meeting using Zoom Client version 5.15.12 or later, they will receive a notification if AI Companion features are activated for that meeting.



Starting with Zoom Client version 6.0.0, meeting hosts have a one-click option to turn off all AI Companion features in a meeting. This includes an option to delete the AI Companion meeting assets, for example, if the feature was enabled in error or where the host no longer requires the summary. Participants will also be able to send a request to the host to disable AI Companion during the meeting.

### **Site level Settings (Zoom Phone Only)**

Account owners and administrators can manage which sites have access to AI Companion features for Zoom Phone. Zoom Phone features may be enabled or disabled, and the ability to turn features on or off may be locked within the Policy section of the site. Site policies sit between Group and User level settings within the setting hierarchy. Site level phone policies are not applied to users that are members of one or more User Groups with activated Zoom Phone policies. Additional information on how to manage Sites for your account can be found in the [“Changing Zoom Phone policy settings”](#) support article.

---

## **Data Protection**

Customer data, including customer content, is encrypted in transit between customers and Zoom, where supported by the user’s connection method and as stated in Zoom’s support articles, between Zoom services, and between Zoom and its third-party subprocessors, including its third-party AI model providers (e.g., OpenAI and Anthropic), using Transport Layer Security (TLS) 1.2 or AES 256-bit GCM. Customer data, including customer content, that is either generated by or used to provide the AI Companion features, is encrypted at rest using a minimum Advanced Encryption Standard (AES) 256-bit encryption. Customers may supply their own encryption key for content stored by Zoom if they use Zoom Customer Managed Key (CMK).

Zoom’s access to customer data and content used to provide the AI Companion features is role-based and restricted based on least privilege, in accordance with Zoom’s access control policies and standards. Controls are in place to prevent Zoom employees from accessing customer content, including meeting, webinar, chat, or email content (specifically, audio, video, files, in-meeting whiteboards, messaging, or email content), or any content generated or shared as part of other collaborative features (such as out-of-meeting whiteboards), unless authorized by the account owner or administrator of the account hosting the Zoom product or service where the customer content was generated, or as required for legal, safety, or security reasons. Zoom’s access to customer data and content is logged and monitored for suspicious activity or unauthorized access. Zoom’s data access controls are assessed by independent audit firms where indicated in our security certifications and attestations, which are available to our customers on [Zoom’s Trust Center](#).

## Secure Development of Generative AI Features

Zoom's secure software development lifecycle (SDLC) is a set of practices and processes designed to integrate security into each phase of the software development lifecycle. Zoom's secure software development controls are assessed by independent audit firms as indicated in Zoom's security certifications and attestations, which are available to customers on [Zoom's Trust Center](#). Zoom AI Companion features follow Zoom's standard secure SDLC process, which includes the following:

### Design Review

Zoom's Engineering Security team is engaged during the design phase when a feature is being conceptualized so that key security controls can be built into the requirements. Security design reviews, which include threat analysis, are performed to identify potential threats and mitigations. Zoom maintains vulnerability remediation standards governing the remediation or mitigation of security vulnerabilities identified during the security design review.

### Code Review

Peer code reviews are a key element of Zoom's secure software development lifecycle and are enforced in Zoom's software development platform. In addition to peer code reviews, high-risk areas identified during the security design review require secure code reviews.

### Static Analysis Testing

Zoom utilizes static analysis security testing (SAST) tools to scan its source code for coding errors and common security vulnerabilities, including Open Web Application Security Project's (OWASP) Top 10 and National Vulnerability Database (NVD). Zoom maintains vulnerability remediation standards governing the remediation or mitigation of security vulnerabilities identified through static analysis testing.

### Dynamic Analysis Testing

Zoom utilizes dynamic analysis security testing (DAST) tools to identify common security vulnerabilities, including OWASP's Top 10 and NVD. Zoom maintains vulnerability remediation standards governing the remediation or mitigation of security vulnerabilities identified through dynamic analysis testing.

### Third-Party Code Reviews

Where open source software (OSS) is used, the OSS package must undergo Zoom's third-party code review process, which includes a set of OSS evaluation criteria and scanning for common security vulnerabilities. Zoom maintains vulnerability remediation standards governing the remediation or mitigation of security vulnerabilities identified through third-party OSS scanning tools.

## Deployment

Security approval is required for the deployment of new products and features, including AI Companion features. Zoom has a dedicated Release Security Assurance function responsible for scanning Zoom client builds prior to release. The final Zoom client build scans are designed to identify potential vulnerabilities or malicious content, and the build is digitally signed to maintain its integrity and authenticity.

---

## Generative AI Model Security

In addition to the steps outlined in Zoom's secure SDLC above, models hosted by Zoom are subject to security reviews to assess security threats specific to generative AI models. The generative AI model review includes commonly known LLM model vulnerabilities, in line with OWASP's Top 10 for LLMs and other secure AI frameworks. Vulnerabilities identified in the generative AI security reviews must be remediated in accordance with Zoom's vulnerability remediation standards.

Zoom's third-party subprocessors are subject to security assessments on at least an annual basis as part of Zoom's third-party risk management program. Zoom's third-party risk management controls are assessed by independent audit firms as indicated in Zoom's security certifications and attestations, which are available to customers on [Zoom's Trust Center](#).

---

## Security Assessments

Zoom has a dedicated offensive security team that performs ongoing vulnerability research and red team exercises across Zoom's platform, including for Zoom AI Companion features. In addition to Zoom's dedicated offensive security team, penetration tests are performed by an independent third party on at least an annual basis.

---

## Vulnerability Disclosure Program

Zoom believes that the independent security research community can provide key contributions to the security of Zoom's products. Zoom maintains a [vulnerability disclosure program](#) as well as a Bug Bounty program through HackerOne that incentivizes security researchers to responsibly report potential security vulnerabilities so Zoom can fix them and keep its users safe.

---

## AI Companion Compliance

Zoom's AI Companion features adhere to the same security and compliance requirements as the primary Zoom products within which they are incorporated. AI Companion is ISO 27001, ISO 27701, and ISO 27017/18 certified and is also included within the scope of Zoom's SOC 2 report, available on [Zoom's Trust Center](#).

---

## Changelog

Version	Published on	Change Type	Change
v. 4.0	April/17/2024	Add	Added Sections: Zoom Phone AI Companion Features. Site level Settings (Zoom Phone Only)
v. 4.0	April/17/2024	Updated	<p>AI Companion Features Table: Added information around minimum versions, ZMO and ZDR, Meeting summary retention settings, Twilio SendGrid information, and added Zoom Team Chat Sentence completion.</p> <p>User and In-Meeting Controls: Added information on the new shut off capabilities.</p> <p>AI Companion Compliance: Added information around certifications.</p>
v. 3.0	Mar/13/2024	Add	Added Sections: Model Usage and Processing, Model Provider Data Storage and Retention, Customer Data Storage and Retention
v. 3.0	Mar/13/2024	Updated	<p>AI Companion Features Table: Updated column headings and format, added Team Chat Quick Scheduling, added Zoom Events Smart Compose, and added Mindmaps to Whiteboard Content Generation.</p> <p>Putting You In Control of AI Companion Capabilities: Updated Images</p> <p>Data Protection: Added reference to Customer Manager Keys</p> <p>Global: General typographical and clarification updates.</p>