AI Companion
Security and Privacy

This Whitepaper relates to Zoom's AI Companion, not to other AI products or services offered by Zoom. It describes AI Companion's security and privacy features as of the date of publication. In our continuing commitment to empowering productivity - while keeping security and privacy at the core of our products - the features described herein may evolve.

WHITEPAPER

NOVEMBER 30, 2023 | VERSION 02

Table of Contents

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 model 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 getting the benefits of improved quality and performance.

Our Commitment to Responsible AI

Zoom is committed to responsible AI, with security and privacy at the core of the generative AI capabilities we provide to our customers. Zoom AI Companion is built on top of our current commitments to security and privacy across the Zoom platform. We recognize that generative AI brings an evolving set of risks for our customers and we are committed to prioritizing transparency and customer choice as we bring 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.

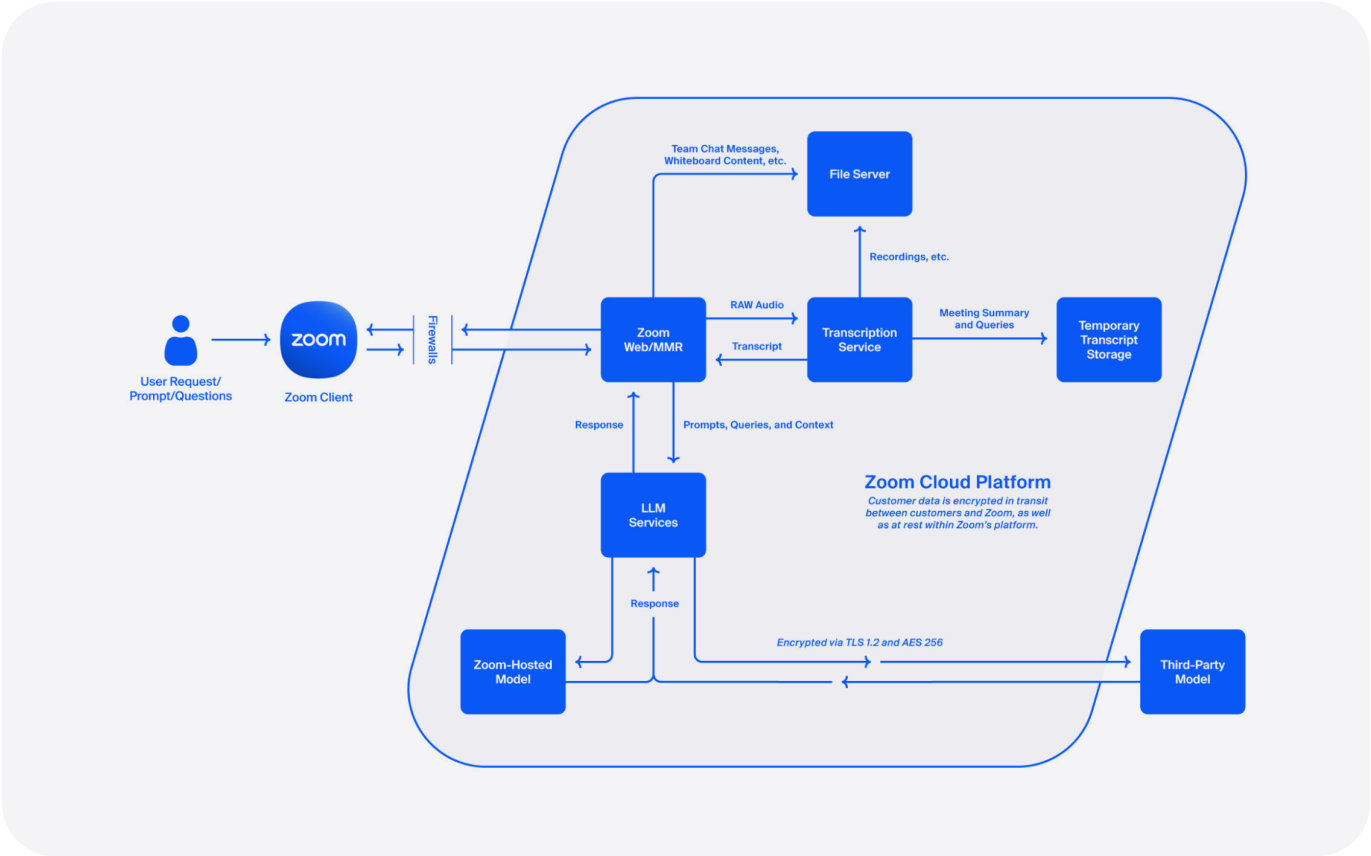
We provide layers of controls at account, group, and user levels, allowing administrators to select which AI Companion features or capabilities they wish to enable for specific Zoom product offerings. For example, for Zoom meetings, administrators can enable the AI Companion features at the account level and meeting hosts can choose whether to enable them for specific meetings. To provide transparency, meeting participants will see an in-product notification for the generative AI Companion capabilities that are in use 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 artificial intelligence models. Customer data is encrypted in-transit between customers and Zoom, as well as at-rest within Zoom's platform.

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



Third-Party Subprocessors

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

Zoom requires its subprocessors to satisfy equivalent obligations as those outlined in Zoom's Data Processing Agreement. Zoom's sub-processors 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 our security certifications and attestations, available to our 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 in order to provide the services.

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 contents), 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 hosting the Zoom product or service where the Customer Content was generated, or as required for legal, safety, or security reasons.

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. Zoom retains the content used to provide the service - as described herein - for up to 30 days to provide the service and for debugging purposes, and Zoom may also retain for a longer period content that is flagged for trust and safety purposes.

If the AI Companion feature relies on a third-party artificial intelligence model, pursuant to Zoom's contracts, third-parties may retain 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.

Below is a summary of the models used for each AI Companion feature as of the publish date of this whitepaper, and the specific storage and retention settings for the content used to provide each feature.

Smart Recordings
The cloud recordings and audio transcripts can only be used to provide the Smart Recordings feature if cloud recordings are enabled by the account administrator and meeting recording is enabled by the meeting host.

AI Companion Feature	Generative AI Models Used	Content Used	Storage / Processing Location	Retention Period
Smart Recordings Review cloud recordings faster through highlights, smart chapters, summaries, next steps, and more.	Zoom OpenAI Anthropic	Cloud Recording	Zoom - Meeting host's provisioned data center OpenAI - US Anthropic - US	Zoom: Up to 30 days to provide the service and for debugging purposes. Third-party: Up to 30 days to provide the service and for trust and safety purposes. Follows meeting host's configured cloud recording retention settings.
		Audio Transcript	Zoom - Meeting host's provisioned data center OpenAI - US Anthropic - US	Zoom: Up to 30 days to provide the service and for debugging purposes. Third-party: Up to 30 days to provide the service and for trust and safety purposes. Follows meeting host's configured cloud recording retention settings.

Meeting Summary
For Meeting Summary, transcription only begins once the Meeting Summary feature is enabled by the meeting host.

AI Companion Feature	Generative AI Models Used	Content Used	Storage / Processing Location	Retention Period
Meeting Summary Generate a summary and next steps of what was discussed in your meetings and share through email and Team Chat.	Zoom OpenAI Anthropic	Audio Transcript	Zoom - Meeting host's provisioned data center OpenAI - US Anthropic - US	Zoom: Up to 30 days to provide the service and for debugging purposes. Third-party: Up to 30 days to provide the service and for trust and safety purposes.
		Meeting Summary	Zoom - Meeting host's provisioned data center OpenAI - US Anthropic - US	Until the meeting summary is deleted by the user or account administrator or until the user or customer account is terminated. Zoom: Up to 30 days to provide the service and for debugging purposes. Third-party: Up to 30 days to provide the service and for trust and safety purposes.

Meeting Questions

For Meeting Questions, transcription only begins once the Meeting Questions feature is enabled by the meeting host.

AI Companion Feature	Generative AI Models Used	Content Used	Storage / Processing Location	Retention Period
Meeting Questions Quickly catch up and get clarity on what you missed during a meeting without interrupting it.	Zoom OpenAI Anthropic	Audio Transcript	Zoom - Meeting host's provisioned data center OpenAI - US Anthropic - US	Zoom: Up to 30 days to provide the service and for debugging purposes. Third-party: Up to 30 days to provide the service and for trust and safety purposes.
		Question (Input)	Zoom - Meeting host's provisioned data center OpenAI - US Anthropic - US	Zoom: Up to 30 days to provide the service and for debugging purposes. Third-party: Up to 30 days to provide the service and for trust and safety purposes.
		Answer (Output)	Zoom - Meeting host's provisioned data center OpenAI - US Anthropic - US	Zoom: Up to 30 days to provide the service and for debugging purposes. Third-party: Up to 30 days to provide the service and for trust and safety purposes.

Email Compose

AI Companion Feature	Generative AI Models Used	Content Used	Storage / Processing Location	Retention Period
Email Compose Compose and reply to emails faster with suggested content based on the email thread and what you want to say.	Zoom OpenAI Anthropic	Email text	Zoom - Customer's provisioned data center OpenAI - US Anthropic - US	Zoom: Up to 30 days to provide the service and for debugging purposes. Third-party: Up to 30 days to provide the service and for trust and safety purposes.
		Sender and recipient names	Zoom - Customer's provisioned data center OpenAI - US Anthropic - US	Zoom: Up to 30 days to provide the service and for debugging purposes. Third-party: Up to 30 days to provide the service and for trust and safety purposes.
		User inputs and prompts	Zoom - Customer's provisioned data center OpenAI - US Anthropic - US	Zoom: Up to 30 days to provide the service and for debugging purposes. Third-party: Up to 30 days to provide the service and for trust and safety purposes.
		Output	Zoom - Customer's provisioned data center OpenAI - US Anthropic - US	Zoom: Up to 30 days to provide the service and for debugging purposes. Third-party: Up to 30 days to provide the service and for trust and safety purposes. Emails are stored in accordance with the customer's retention settings with the email provider.

Team Chat Compose

AI Companion Feature	Generative AI Models Used	Content Used	Storage / Processing Location	Retention Period
Chat Compose Draft chat messages based on conversational context and what you want to say, as well as customize its tone and length.	Zoom OpenAI Anthropic	Chat message text for the selected chat thread	Zoom - Customer's provisioned data center OpenAI - US Anthropic - US	Zoom: Up to 30 days to provide the service and for debugging purposes. Third-party: Up to 30 days to provide the service and for trust and safety purposes.
		Chat participant names	Zoom - Customer's provisioned data center OpenAI - US Anthropic - US	Zoom: Up to 30 days to provide the service and for debugging purposes. Third-party: Up to 30 days to provide the service and for trust and safety purposes.
		User inputs and prompts	Zoom - Customer's provisioned data center OpenAI - US Anthropic - US	Zoom: Up to 30 days to provide the service and for debugging purposes. Third-party: Up to 30 days to provide the service and for trust and safety purposes.
		Output	Zoom - Customer's provisioned data center OpenAI - US Anthropic - US	Zoom: Up to 30 days to provide the service and for debugging purposes. Third-party: Up to 30 days to provide the service and for trust and safety purposes. If the output is posted to the chat, the chat message is stored in accordance with the customer's Zoom Team Chat retention settings.

Team Chat Thread Summary

AI Companion Feature	Generative AI Models Used	Content Used	Storage / Processing Location	Retention Period
Thread Summary Quickly summarize the content of long Team Chat threads.	Zoom OpenAI Anthropic	Chat message text for the selected chat thread	Zoom - Customer's provisioned data center OpenAI - US Anthropic - US	Zoom: Up to 30 days to provide the service and for debugging purposes. Third-party: Up to 30 days to provide the service and for trust and safety purposes.
		Chat participant names	Zoom - Customer's provisioned data center OpenAI - US Anthropic - US	Zoom: Up to 30 days to provide the service and for debugging purposes. Third-party: Up to 30 days to provide the service and for trust and safety purposes.
		Output	Zoom - Customer's provisioned data center OpenAI - US Anthropic - US	Zoom: Up to 30 days to provide the service and for debugging purposes. Third-party: Up to 30 days to provide the service and for trust and safety purposes.

Whiteboard Content Generation

AI Companion Feature	Generative AI Models Used	Content Used	Storage / Processing Location	Retention Period
Whiteboard Content Generation Generate ideas for your whiteboard and refine / categorize existing content.	Zoom OpenAI Anthropic	Whiteboard content	Zoom - Customer's provisioned data center OpenAI - US Anthropic - US	Zoom: Up to 30 days to provide the service and for debugging purposes. Third-party: Up to 30 days to provide the service and for trust and safety purposes.
		User inputs and prompts	Zoom - Customer's provisioned data center OpenAI - US Anthropic - US	Zoom: Up to 30 days to provide the service and for debugging purposes. Third-party: Up to 30 days to provide the service and for trust and safety purposes.
		Output	Zoom - Customer's provisioned data center OpenAI - US Anthropic - US	Zoom: Up to 30 days to provide the service and for debugging purposes. Third-party: Up to 30 days to provide the service and for trust and safety purposes. If the output is posted to the whiteboard, the whiteboard content is stored in accordance with the customer's Whiteboard retention settings.

Events Chat Compose

AI Companion Feature	Generative AI Models Used	Content Used	Storage / Processing Location	Retention Period
Chat Compose Draft chat messages based on conversational context and what you want to say, as well as customize its tone and length.	Zoom OpenAI Anthropic	Chat message text for the selected chat thread	Zoom - Customer's provisioned data center OpenAI - US Anthropic - US	Zoom: Up to 30 days to provide the service and for debugging purposes. Third-party: Up to 30 days to provide the service and for trust and safety purposes.
		Chat participant names	Zoom - Customer's provisioned data center OpenAI - US Anthropic - US	Zoom: Up to 30 days to provide the service and for debugging purposes. Third-party: Up to 30 days to provide the service and for trust and safety purposes.
		User inputs and prompts	Zoom - Customer's provisioned data center OpenAI - US Anthropic - US	Zoom: Up to 30 days to provide the service and for debugging purposes. Third-party: Up to 30 days to provide the service and for trust and safety purposes.
		Output	Zoom - Customer's provisioned data center OpenAI - US Anthropic - US	Zoom: Up to 30 days to provide the service and for debugging purposes. Third-party: Up to 30 days to provide the service and for trust and safety purposes.

Events Email Compose

AI Companion Feature	Generative AI Models Used	Content Used	Storage / Processing Location	Retention Period
Email Compose Compose and reply to emails faster with suggested content based on the email thread and what you want to say.	Zoom OpenAI Anthropic	Email text	Zoom - Customer's provisioned data center OpenAI - US Anthropic - US	Zoom: Up to 30 days to provide the service and for debugging purposes. Third-party: Up to 30 days to provide the service and for trust and safety purposes.
		Sender and recipient names	Zoom - Customer's provisioned data center OpenAI - US Anthropic - US	Zoom: Up to 30 days to provide the service and for debugging purposes. Third-party: Up to 30 days to provide the service and for trust and safety purposes.
		User inputs and prompts	Zoom - Customer's provisioned data center OpenAI - US Anthropic - US	Zoom: Up to 30 days to provide the service and for debugging purposes. Third-party: Up to 30 days to provide the service and for trust and safety purposes.
		Output	Zoom - Customer's provisioned data center OpenAI - US Anthropic - US	Zoom: Up to 30 days to provide the service and for debugging purposes. Third-party: Up to 30 days to provide the service and for trust and safety purposes. Emails are stored in accordance with the customer's retention settings with the email provider.

Putting You In Control of AI Companion Capabilities

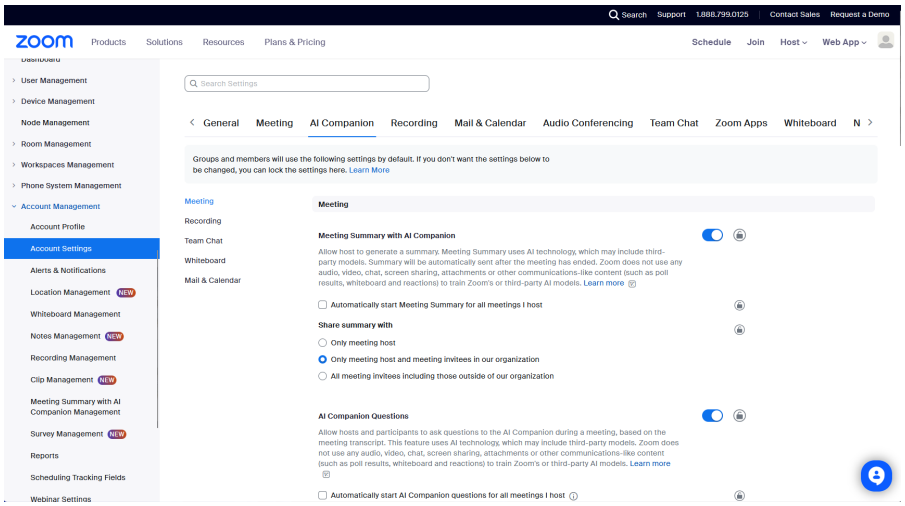
Zoom is committed to providing transparency and choice when it comes to enabling and using AI Companion features. Account administrators and users are provided with controls for AI Companion features. We are continually working to enhance our platform and educate users on our new features. Currently,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

Account Administrator Controls

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

Administrators can enable or disable features for their entire account within the account settings page in the Admin Portal.

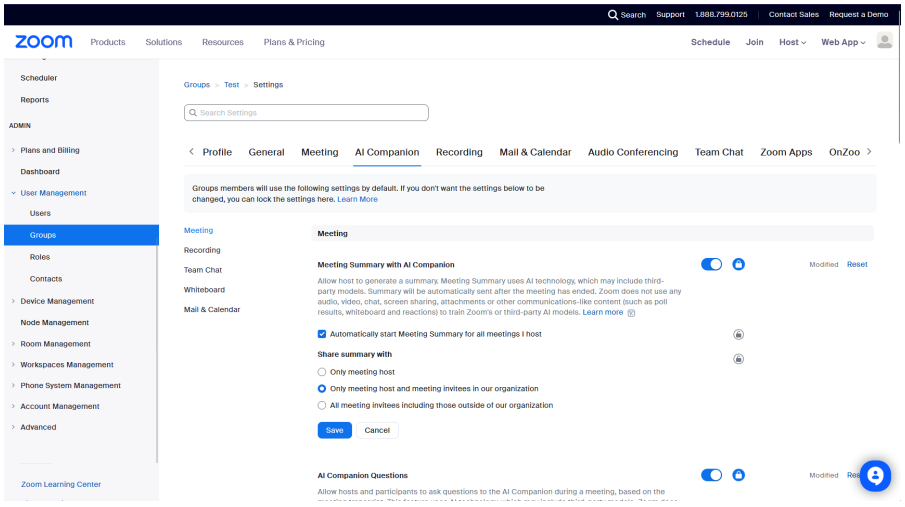
Putting You In Control of AI Companion Capabilities (cont.)



Group Controls

Account owners and admins can control which groups receive certain AI Companion features. Select features can be enabled or disabled, and set to locked for these features. Users belonging to this group will have their feature access dictated by these selections. If allowed at the group level, users can still enable or disable features for themselves at the individual user level.

Note: Group level control is only available for select features.



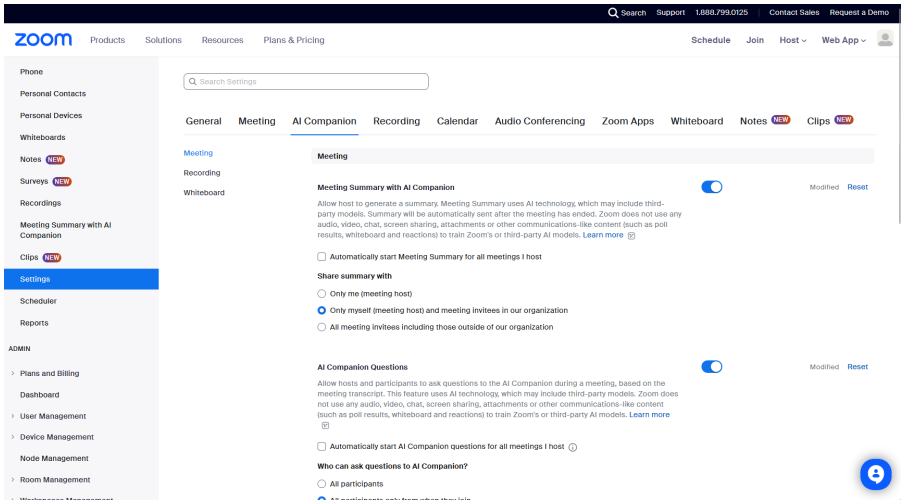
User and In-Meeting Controls

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 can see if their administrators have enabled or disabled AI Companion features. If allowed by the account administrator, for features with

Putting You In Control of AI Companion Capabilities (cont.)

user-level controls, users can enable or disable AI Companion features. If the administrator has locked the setting at the account or group level, the user cannot change the setting.

Note: User level control is only available for select features.



Meeting hosts can enable or disable AI Companion features in-meeting. Participants can also request to the host that these features be enabled in-meeting, if the option for the icon to show in the toolbar is enabled. Currently, meeting participants connecting to a meeting using Zoom Client 5.15.12 or later will receive a message stating that AI Companion is on.

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, 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 higher. Customer data, including customer content, that is used for providing the AI Companion features is encrypted at rest using a minimum Advanced Encryption Standard (AES) 256-bit encryption.

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, messaging, or email content (specifically, audio, video, files, in-meeting whiteboards, messaging, or email contents), or any content generated or shared

Data Protection (cont.)

as part of other collaborative features (such as out-of-meeting whiteboards), unless authorized by the account owner hosting the Zoom product or service where the customer content was generated, or as required for legal, safety, or security reasons. 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 in many of our security certifications and attestations, 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 in many of our security certifications and attestations, available to our 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 the 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.

Secure Development of Generative AI Features (cont.)

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.

Deployment

Security approval is required for 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 to verify that the build contains only the content intended for release. Flagged files are investigated and identified issues are remediated prior to release.

Generative AI Model Security

In addition to the steps outlined in Zoom's secure SDLC above, Zoom AI Companion models are subject to security reviews to assess security threats specific to generative AI models. The generative AI model assessments include 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 assessments must be remediated in accordance with Zoom's vulnerability remediation standards.

Security Assessments

Zoom has a dedicated offensive security team that performs ongoing vulnerability research and red team exercises across Zoom's platform, including 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 we can fix them and keep our 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. These products are covered in Zoom's existing third-party certifications and attestations available on Zoom's Trust Center. Zoom plans to include the AI Companion features into the renewal certifications and attestations for these products.