90-Day Security Plan Progress Report: June 17

"Ask Eric Anything" webinar focused on recent product security updates, including an end-to-end encryption update and additional security controls for account owners and admins.

Zoom CEO Eric S. Yuan was joined by Zoom CPO Oded Gal, Zoom Head of Security Engineering Max Krohn, and Zoom Global Deputy CIO Gary Sorrentino for this week's session.

Zoom CTO Brendan Ittelson and Lynn Haaland, Zoom Deputy General Counsel, Chief Compliance and Ethics Officer joined for the Q&A session.

End-to-end encryption update

Following our conversations with our users and a number of advocacy organizations, we are pleased to announce that we will be offering end-to-end encryption for all of users - free and paid - as an advanced feature at no additional charge. Free users seeking access to end-to-end encryption will participate in a one-time process to verify their account, such as verifying a phone number via text message.

We are confident that this risk-based authentication process, combined with our current arsenal of tools, will enable us to continue to prevent and fight abuse on our platform. More information on this announcement.

CISO council update

Our CISO council, which includes 36 members representing a variety of industries and enterprise businesses, has met 3 times since its inception in late April. The members of the CISO council serve as the voice of our customers, offer candid guidance and advice on security and privacy, and provide recommendations in regards to best security and privacy practices as well as feature prioritization.

Starting in July, the CISO council will host CISO Roundtables to give existing and prospective customers the opportunity to meet with a few members from Zoom's CISO council and security team leaders to get an in-depth review of the security measures Zoom has taken and our 90-day security plan. Up to 40 participants at each roundtable will have the chance to ask our CISO council members and Zoom's security team their questions, provide their insights, and join in on the conversation surrounding privacy and security. We encourage any CISOs interested in attending one of our CISO Roundtables to reach out to their Zoom account executive to reserve their spot.

Product update

Option to disable email/password for login: Account administrators can now disable the ability to log in to Zoom with an email address and password, requiring users to sign in through SSO or other third party logins that Zoom offers.

Additional whitelist domain options for Waiting Room: Account administrators can whitelist domains beyond their own so participants can bypass the Waiting Room and directly join a meeting.

Option to disable participant annotation: Account admins can now disable the ability for participants to annotate on a shared screen. This setting is available at the account, group, and user level.

Ability to Unmute All: The ability to Unmute All is now available again in meetings with fewer than 200 participants.

Webinar Q&A management: Hosts and panelists can delete questions and comments submitted through the Q&A and chat during a webinar, allowing them to remove

questions that are inappropriate or have already been answered.

Data retention policy: Account owners and admins can set the amount of time that Zoom Phone user data — call logs, ad hoc / automatic call recordings, voicemail recordings, and transcriptions — is retained.

Q&A

Will there be fees to use Zoom's end-to-end encryption?
No, Zoom's end-to-end encryption will be free for both paid and free users.

Are you still accepting feedback on Zoom's cryptography design?
Yes. The best place to leave your feedback on our cryptography design is on Github.

What does end-to-end encryption do, and how is it different from Zoom's AES 256 bit GCM encryption?
With Zoom's current Enhanced Encryption offering, encryption keys are created on Zoom's servers and distributed to the meeting participants. Each key is randomly generated and only used for one meeting, then thrown away. In end-to-end encryption, one meeting participant generates the encryption key and uses public key cryptography to distribute this key to the other participants; Zoom's servers never see the key. Both offerings behave similarly after the key exchange: the meeting data is encrypted with the meeting key using AES GCM encryption.

If a meeting host enables end-to-end encryption, do other participants need to have end-to-end encryption to join the meeting?
End-to-end encryption won't be compatible with an older version of the Zoom client, and all participants must have an E2EE-enabled client to join the meeting.

Will users with free accounts be forced to use end-to-end encryption for their meetings?
No, we will not be forcing users with free accounts to use end-to-end encryption. Both free and paid users will have the option to enable end-to-end encryption for their meetings.

How do I enable end-to-end encryption for my meetings?
You will be able to turn end-to-end encryption on or off in the settings panel where you configure your specific meeting settings, while account owners and admins will be able to enable and disable end-to-end encryption at the account and group level. Once the meeting has started, you won't be able to change the end-to-end encryption setting.

Will end-to-end encryption be available for Zoom Video Webinars?
End-to-end encryption will not be available for Zoom Video Webinars during the initial release; however, plan to include that feature in future releases.

When will we receive more information on the Waiting Room and Passcode change happening on June 19th?
We will begin sending out emails this week to our customers to prepare them for the change and we will also be posting a FAQ document to our support site next week. As a reminder, after June 19th, users and admins must enable Waiting Room, Passcode, or both for their meetings.

90-Day Security Plan Progress Report: June 17

What is the status of accessibility compliance for the Zoom client?

Accessibility compliance is very important to us as we strive to provide a platform that anyone can use with ease. Users can get more information about our accessibility compliance at zoom.com/accessibility.

Is there a limit to how many people can participate in a webinar?

Up to 50,000 participants can join a webinar, and webinar hosts can accommodate even more viewers by streaming their webinar over Youtube, Facebook, or other streaming platforms.

Thank you for your support

Thanks for attending this week's session, and thank you to everyone who submitted questions! We truly appreciate your support on our journey to make Zoom the world's most secure enterprise communications platform.

If you missed this week's session, you can watch the recording here:

https://www.youtube.com/watch?v=R4cn4qb_FoE

To give your feedback or to ask Zoom a question, send an email to answers@zoom.us. And be sure to sign up for next week's "Ask Eric Anything" webinar.