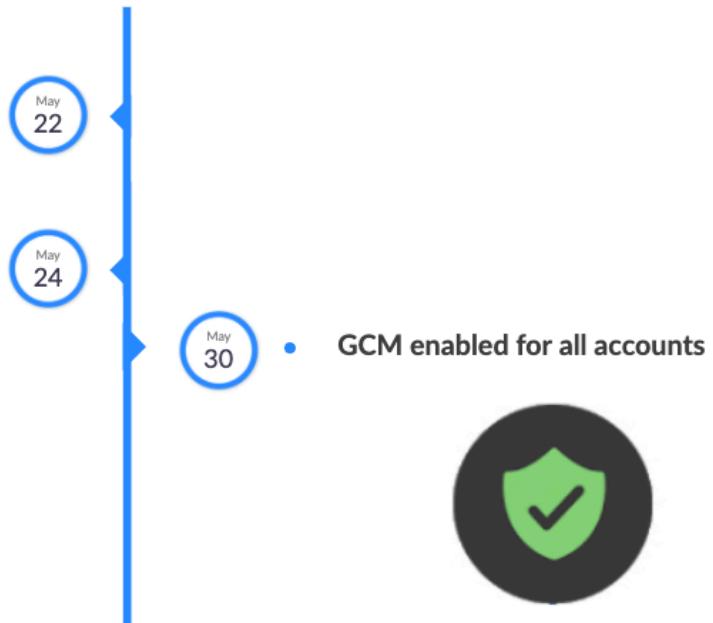


90-Day Security Plan Progress Report: May 27

This Past Week:

- Published Draft Design of End-to-End Encryption
- Report a user for hosts on Web client and from Zoom Rooms
- Support for 3rd-party virtual camera re-enabled for MacOS
- Zoom Rooms Security Updates
 - Security Icon controls
 - Assign new host when leaving meeting
 - Get dialogue to consent to unmute and an option to always let host unmute

This Week:



As we continue on our 90-day plan to improve the security and privacy of our platform, this week's "Ask Eric Anything" webinar focused on the draft design of our end-to-end encryption offering, Zoom's new president of engineering and product, security updates for Zoom Rooms, and this week's Zoom 5.0 update deadline for GCM encryption.

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

Zoom CTO Brendan Iltelson; Lea Kissner, former Global Lead of Privacy Technology at Google who is consulting with Zoom on privacy and encryption; Alex Stamos, security and privacy adviser to Zoom; and Lynn Haaland, Zoom Deputy General Counsel, Chief Compliance and Ethics Officer, joined for the Q&A session.

Key takeaways from this week's session

End-to-end encryption update

We published a draft cryptographic design for our end-to-end encryption offering on GitHub (https://github.com/zoom/zoom-e2e-whitepaper/blob/master/zoom_e2e.pdf) last Friday for users and the tech community to review and leave feedback. Zoom's engineering team has been working diligently to build our vision for end-to-end encryption for Zoom Meetings, and Max gave an overview of the logic and goals driving the design and the different phases of the project.

New head of engineering and product

Velchamy Sankarlingam, a cloud and collaboration veteran who has spent the last nine years at VMware, will join Zoom on June 12 as our President of Engineering and Product. With deep expertise in R&D, IT, and cloud design and management, Velchamy will play a crucial role in

90-Day Security Plan Progress Report: May 27

helping us continue innovating the meeting experience for our users.

Zoom 5.0 reminder – update your clients before May 30

Zoom 5.0 became generally available on April 27, and a system-wide account enablement to AES 256-bit GCM encryption will occur on May 30, 2020. Only Zoom clients on version 5.0 or later, including Zoom Rooms, will be able to join Zoom Meetings starting that day. We encourage users to update to 5.0 today: <https://zoom.us/download>. Zoom admins should visit our IT administrators page to manage this update in their environment: <https://zoom.us/docs/en-us/zoom-v5-admin.html>. Users can preview the GCM experience at <https://zoom.us/testgcm>.

Q&A

Here are some of the webinar attendee questions (and summarized answers) that were addressed live this week:

Why aren't Zoom Phone and webinars in the initial scope for end-to-end encryption, and will Zoom Chat receive end-to-end encryption?

Our top priority is to focus on building effective end-to-end encryption for our meeting product first, where it will be most useful. We are considering end-to-end encryption options for Zoom Chat, Zoom Phone, and Zoom Video Webinars down the road.

When do you expect end-to-end encryption to be implemented, and why is it being done in different phases?

The implementation scope and timeline of end-to-end encryption will depend on the feedback we receive on the draft of our cryptographic report. The initial review period is two weeks, and we'll revise our design accordingly. And we've chosen to implement our end-to-end encryption in phases so our teams can implement the feedback

we receive from users, security researchers, and the community to help us build the best offering for our users.

Will end-to-end encryption affect the quality of meetings?

End-to-end encryption won't have any impact on meeting quality.

Will there be a different version of encryption for different license types?

Only our paid users will have access to end-to-end encryption for their meetings. However, all users will use the 256-bit GCM encryption on May 30 regardless of their license type.

Will participants and hosts need a Zoom account after 5.0 goes live on May 30?

There will be no changes to how you join meetings after the May 30 update; you just need to update to the newest client (Zoom 5.0+). A meeting host needs a Zoom account, but anyone can join a meeting using the Zoom mobile apps or desktop applications. This means you can hold meetings with students, co-workers, or other people without them having to create an account.

Did Zoom make changes to the screen sharing feature?

We changed the default setting for Basic and Single Pro user accounts so that only the host can share the screen. However, you can enable screen sharing for participants during a meeting, or you can change it in your settings.

Can a user set up a meeting but not attend the meeting?

Yes, a meeting host can select another licensed user on the same account as an alternative host to host in their place. Please read our support article – <https://support.zoom.us/hc/en-us/articles/208220166-Alternative-host> – for more on setting an alternative host.

90-Day Security Plan Progress Report: May 27

Can a host or admin prevent attendees from inviting other users during a meeting?

Participants have the ability to invite other users once they are in a meeting. This feature cannot be disabled.

To prevent participants from inviting other users during a meeting, the host can turn on the Waiting Room or lock the meeting to prevent anyone else from joining.

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://youtu.be/deu07TL8mhc>

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.