90-Day Security Plan Progress Report: April 22

Zoom Surpasses 300M Daily Users, Announces Zoom 5.0 with AES 256-Bit GCM Encryption

In today's "Ask Eric Anything" webinar, Zoom CEO Eric S. Yuan provided progress updates on our 90-day security plan, including announcements about Zoom 5.0 and surpassing 300 million daily Zoom meeting participants.

Eric was joined by Zoom CPO Oded Gal, Zoom CTO Brendan Ittelson, Alex Stamos, who is a security adviser to Zoom, and Lea Kissner, the former Global Lead of Privacy Technology at Google, who is consulting with Zoom on privacy and encryption.

Key takeaways from this week's session

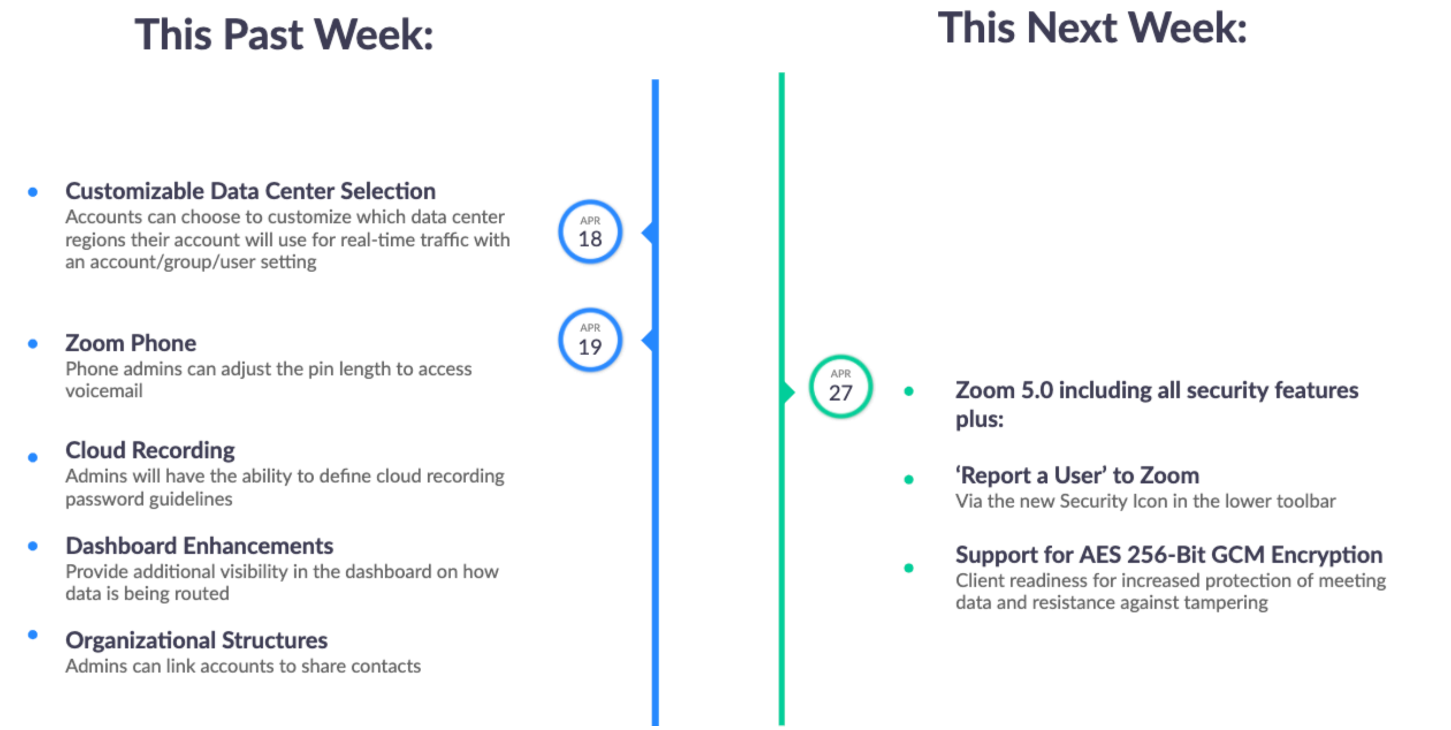
Data routing control

Zoom admins and owners of paid accounts can opt in or out of any data center region (apart from their home region) at the account, group, or user level. Read our blog for more details: **https://blog.zoom.us/wordpress/2020/04/20/data-routing-control-is-here/**

Zoom 5.0 announcement

Set to release this weekend, Zoom 5.0 includes two new features to help Zoom users protect their meetings:

- **Support for AES 256-bit GCM:** Zoom 5.0 supports AES 256-bit GCM encryption, which provides more protection for meeting data and greater resistance to tampering. Organizations will have access to GCM encryption with the release of Zoom 5.0, and a system-wide account enablement will occur May 30, when all Zoom customers will switch to the new cryptographic mode.
- **Report a User:** Hosts and co-hosts can report users to Zoom's Trust & Safety team, who will review any potential misuse of the platform and take appropriate action. This feature will be found within the Security icon in the meeting controls.



This Past Week:

- **Customizable Data Center Selection**
  Accounts can choose to customize which data center regions their account will use for real-time traffic with an account/group/user setting
- **Zoom Phone**
  Phone admins can adjust the pin length to access voicemail
- **Cloud Recording**
  Admins will have the ability to define cloud recording password guidelines
- **Dashboard Enhancements**
  Provide additional visibility in the dashboard on how data is being routed
- **Organizational Structures**
  Admins can link accounts to share contacts

This Next Week:

- **Zoom 5.0 including all security features plus:**
- **'Report a User' to Zoom**
  Via the new Security Icon in the lower toolbar
- **Support for AES 256-Bit GCM Encryption**
  Client readiness for increased protection of meeting data and resistance against tampering

90-Day Security Plan Progress Report: April 22

Introducing Lea Kissner

Eric introduced Lea Kissner, the former Global Lead of Privacy Technology at Google and Chief Privacy Officer of Humu, who has joined Zoom as a security consultant. With her expertise in privacy, protecting users, and encryption, Lea will play an instrumental role in helping Zoom create a more secure platform.

Q&A

Here are some of the topics that were addressed live from webinar attendees this week:

How does Zoom's new encryption compare to other technology providers'?

Lea explained that Zoom's new 256-bit GCM encryption will be comparable to encryption used by many leading technology companies.

Will data centers get overloaded if everyone opts into the same ones?

Even with data center customization available, Zoom is designed to scale to meet heavy usage demands. We've been adding capacity in our data centers and working with our public cloud partners to scale as needed to ensure reliability, even with more than 300 million daily users.

Can Waiting Rooms, meeting registration, and meeting passwords be used together?

Meeting registration, passwords, and the Waiting Room feature can all be used for the same Zoom Meeting, and users who are hosting sensitive meetings should use them all for the most secure environment.

How can users secure their Personal Meeting ID (PMI)?

Securing a Personal Meeting ID is similar to a professor holding office hours; you can keep your PMI open for trusted parties to join, but you must "keep the office door closed" by enabling the Waiting Room and meeting password.

How can hosts prevent users from joining with another person's name?

Hosts can require all participants to register for the meeting, where they enter their first name, last name, email address, and other information, which the host can then confirm. Hosts can also use the Security icon to disable the ability for participants to rename themselves.

Thanks for your support

We continue to be very appreciative of all of our customers' support in our journey to a more secure Zoom platform. It makes us very proud to know that more than 300 million people around the world are using Zoom during this challenging time.

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

https://youtu.be/OGQpawfDRcA

To give your feedback or to ask Eric a question, send an email to answers@zoom.us. And be sure to sign up for next week's webinar: **https://zoom.us/events**.