90-Day Security Plan Progress Report: July 1

As we come to the close of our 90-day security plan, this week's "Ask Eric Anything" focused on the progress we've made since the start of our security plan and our path forward, including they key updates we've made, the status of the commitments we made to our customers as part of our 90-day security plan, and updates regarding Zoom's CISO Council.

Zoom CEO Eric S. Yuan was joined by COO Aparna Bawa, CPO Oded Gal, Deputy CIO and Chairman of the CISO Council Gary Sorrentino, and our new CISO Jason Lee.

CTO Brendan Ittelson, Head of Security Engineering Max Krohn, and Chief Compliance and Ethics Officer Lynn Haaland joined for the Q&A session.

Product updates

Oded provided a quick summary of the key updates we have made to the platform in the last 90 days, including:

- **Zoom 5.0 release**: We released Zoom 5.0 on April 27, which supports AES 256-bit GCM encryption, one of the most secure encryption standards used today. A system-wide account enablement to AES 256-bit GCM encryption occurred on May 30.
- **New Security Icon in the user interface**: The Security Icon provides hosts and co-hosts instant access to important security controls in meetings, including the ability to lock meetings and enable waiting rooms, and the options to manage participants' ability to share their screen, participate in chat, and rename or unmute themselves.
- **"Report a User" feature**: Hosts and co-hosts can report users and incidents of meeting disruption to Zoom's Trust & Safety team, who will review any potential misuse of the platform and take appropriate action.
- **Updated default security settings for meetings**: Passcodes, Waiting Room, and screen share for host only are turned on by default for Free/Basic and Single Pro accounts. Free/Basic accounts users have Passcodes enforced for their meetings.
- **Customized data routing**: To give hosts more control over their data, we implemented data routing options on April 18 for customers on paid accounts, allowing them to customize their data center settings. Admins and account owners of paid accounts can, at the account, group, user, or meeting level, opt out of, or into, specific data center regions with respect to data in transit.

As we develop new features in the future, we have put mechanisms in place to make sure that security and privacy remain a priority in each phase of our product and feature development.

CISO Council Updates with Guests

Gary then interviewed two members of our CISO Council, James Shira, Global and US Chief Information Technology Officer at PwC, and Cy Fenton, Chief Security Officer, Chief Privacy Officer & Senior Vice President, Global Infrastructure at Ralph Lauren, to provide some color and context on the council's mandate and meetings. Here are some of the highlights from that session:

Cy, why did you choose to join Zoom's CISO Council?

"It was an easy decision. Zoom has become such a core and important piece of our toolkit for serving our end users. We moved from using Zoom as a conferencing tool, pre-COVID, to using it every day, multiple times a day, for almost every meeting we have. Zoom is a super important vendor of ours and the opportunity to provide input and

get additional knowledge about the roadmap was a really key opportunity."

James, how do you think the 90-day journey has gone?

"I've been involved in a number of large enterprise security transformations, and I think the important thing to remember is that it's a journey. What's so unique, in my view, with what happened with Zoom is to have that journey occur in the public square, in the real world, in real time. In view of that, I think it's gone extremely well."

Introducing Jason Lee, Zoom CISO

Eric introduced Jason Lee, Zoom's new CISO. Lee brings 20 years of expertise in information security and operating mission-critical services. He was recently the Senior Vice President of Security Operations at Salesforce where he was accountable for the global organization delivering critical end-to-end security operations to customers and employees including company-wide network and system security, and the offensive security team.

"I'm incredibly excited to work with this talented team at Zoom," Jason said. "The recent progress on the security front has been very impressive, and I'm excited for the future."

Reviewing our 90-Day Security Plan Commitments

Aparna Bawa, Zoom's COO, provided a recap of the commitments that we made to our customers as part of our 90-Day Security Plan, which included:

- Enacting a feature freeze, effective April 1, and shifting all our engineering resources to focus on our biggest trust, safety, and privacy issues.
- Committing to a comprehensive review with third-party experts and representative users to understand and ensure the security and privacy of all of our new use cases.
- Preparing a transparency report that details information related to requests for data, records, or content.
- Enhancing our bug bounty program.
- Launching a CISO Council.
- Engaging in a series of simultaneous white box penetration tests to further identify and address issues.
- Hosting a weekly webinar on Wednesdays to provide privacy and security updates to our community.

For more information about the status of these commitments, check out our blog detailing our journey over the course of our 90-Day Security Plan and our PDF summary of our key updates since July 1st, 2020.

Q&A

What was the hardest thing about executing Zoom's 90-Day Security Plan, and what did you learn as a leader?

Eric explained that Zoom was originally designed for use in business, and addressing the needs of first time users in regards to privacy, security, and their unique use cases was a significant challenge. He also explained that he learned that Zoom can overcome anything as long as we listen to our customers, maintain transparency, and remain dedicated to building the best platform possible.

Does the end of Zoom's 90-Day Security Plan mean Zoom will restart feature releases not related to security?

Zoom is committed to maintaining a major focus on

90-Day Security Plan Progress Report: July 1

security. We'll also resume working on non-security features that we froze for 90-days and create new features and products that align with how people are working now and in the future.

Can mandated security settings be set at the group level, as opposed to setting them at the account level?
Yes. They can be set at the account, group or user level.

As a CISO, what is the best way to educate end users on security best practices?
Guest CISO Cy Fenton explained that the best way to educate employees about security at the corporate level is to develop a robust security education program and ensure employees understand the importance of security by talking through the security risks they face, how to defend against them, and how security plays into their daily workflows.

Why did Zoom publish a Government Requests Guide?
Aparna explained that Zoom published this guide as part of an ongoing effort to remain open and transparent about how we operate. We view this as a blueprint for governments on how they interact with Zoom, including pertinent contact information and the criteria and processes Zoom uses to address various government requests.

What is Zoom's general approach to security?
Jason explained that he will frame Zoom's security standing using industry standards and public frameworks to provide clarity surrounding the functions and maturity of Zoom's security standing.

Can system admins see what client version their users have?
System admins can go to the user management section of their dashboard and click on the gear in the upper right hand corner to view an additional column that displays the client versions. Admins with business or equivalent plans can go into the Zoom dashboard where there is a graph that shows the distribution of client versions in their account. They can also go to the meetings tab and dive into any meeting metadata to see what client versions are being used by the participants.

As more companies move to cloud-based services, what's the best way to evaluate vendors and hold them accountable for cyber security?
Jason explained that he examines the innovation of the specific vendor in the present tense and historically, and the quality of the leadership team of the organization. He also looks to other CISOs and asks about their experience with the organization. Cy added that it is important that the organization is transparent about how they are handling issues and their challenges.

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=09Bb43Q6aZI