This document is for CIOs who are subscribing to Zoom and need some resources to help answer questions of their colleagues and employees related to recent press and news about Zoom.

COVID RESOURCES:  
[https://zoom.us/docs/en-us/covid19.html#resources](https://zoom.us/docs/en-us/covid19.html#resources)  
Includes links to best blogs/whitepapers for securing your meetings, how to work remotely, tips for education, tips for telehealth, and how to run virtual events.

Outline of our security and privacy features and resources

FAQS:

1) **Do you really send personal data to Facebook?**
   
   No, Zoom does not share personal data with Facebook.

   Zoom originally implemented the popular “Login with Facebook” feature using the standard Facebook Login SDK for iOS in order to provide users with an easy way to access the platform. Zoom was made aware on March 25th that the Facebook SDK was collecting device information that was unnecessary for Zoom to provide its services, such as the mobile OS type and version, the device time zone, device OS, device model and carrier, screen size, processor cores, and disk space.

   On March 27th, Zoom removed the Facebook SDK in the iOS client and reconfigured the feature so that users will still be able to log in with Facebook via their browser. At no time has Zoom ever shared meeting data (e.g. names, notes, attendees, etc.) with Facebook or any other 3rd party without the explicit permission from the user. Visit [this blog](https://zoom.us/) for more information.

2) **Can the Chinese Government listen to my meetings and access my data?**

   No, Zoom uses geo-fencing to keep users outside of China from connecting to systems within mainland China, and Zoom’s policies regarding compliance with valid legal process preclude cooperation where a government does not have jurisdiction.

   Zoom has over 17 data centers around the world to optimize the meeting experience for the 200M+ daily meeting participants -- only one of which is in China -- and the Zoom platform is built to work in a way that any information and/or data transiting the system is routed through the data center nearest to the user who initiated the call. So, data from U.S. calls is routed to datacenters in the U.S., etc. Additional server capacity was added to meet increased demand and two servers from a data center in China were mistakenly added to a backup whitelist. Zoom immediately removed these Chinese servers from the whitelist on April 2, after learning of the error. To be clear, non-Chinese users being connected to the Chinese data center only ever happened in extremely limited circumstances, and the issue has been fixed such that it will not happen again.

   This situation did not and could not impact Government customers.
Additionally, beginning April 18, every paid Zoom customer can opt in or out of a specific data center region. This will determine the meeting servers and Zoom connectors that can be used to connect to Zoom meetings or webinars you are hosting and ensure the best-quality service. Read more on this blog post.

3) If Zoom is not end-to-end encrypted, is that a concern?
   The security community generally considers "end-to-end encryption" as that in which the provider of the service has absolutely no access to the decryption keys. There was a discrepancy between this commonly accepted definition of end-to-end encryption and how Zoom used it in a few marketing materials. Zoom uses AES-256 ECB (moving to GCM); this level of encryption is equal to, or better than, the method used by Zoom's competitors in market. To be clear, in a meeting where all of the participants are using the Zoom app (on a computer or smartphone) or a Zoom room, and the meeting is not being recorded, Zoom encrypts all video, audio, screen sharing, and chat content at the sending client, and does not decrypt it at any point before it reaches the receiving clients.

4) Are my meetings secure?
   Yes, your meetings are secure. We have enabled default meeting security settings to help keep uninvited guests out, including randomly generated meeting IDs, meeting passwords, and participant waiting rooms. Even when all of the settings for security are used, it's important for hosts and attendees to use best practices for securely sharing meeting IDs and passwords to help keep unwanted people from entering the meeting.

   If someone who's not meant to be there somehow manages to join a meeting, Zoom has simplified the steps needed for hosts to remove them through a new "Security" icon that was added to the Toolbar. Additionally, hosts can use the new Security Toolbar to review and customize all security settings at any time during the meeting.

   Hosts can take extra steps to safeguard their meetings by restricting access by domain, by specific invitees, etc as outlined in the Securing Your Zoom Meetings Guide.

5) Who is on your CISO advisory board?
   We formed a CISO Council with CISOs from companies including, Ellie Mae, NTT Data, Procore, HSBC, Sanofi, SentinelOne, and Arizona State University. Within our CISO Council, we are establishing an Advisory Board that will include a subset of CISOs who will act as advisors to Eric personally, including, EA, Netflix, Uber, VMWare. For more information, check out this blog that discusses the progress we have made on our 90-day plan to bolster key privacy and security initiatives, which was announced in full in this blog post by Eric on April 1.

6) How is Zoom handling the increased demand?
   We feel incredibly privileged to be in a position to help you stay connected with business, classes, healthcare and with friends and family. Zoom went from 10 million daily active participants in December 2019 as a business-to-business video communications platform to over 200 million users in March 2020 -- a massive growth in users, and a significant change in the type of users, that occurred virtually overnight.
Zoom’s unique architecture allowed us to scale to meet the demands that this pandemic raised. We’ve always maintained 50% excess capacity in all aspects of our infrastructure to accommodate growing business needs and to meet peak usage requirements. Zoom is the most reliable solution on the market and the only one that can support up to 1000 people all on video.

7) How does Zoom compare on security to the competition?

As an industry, we all must focus on ensuring the security and privacy for customers -- particularly in this time of isolation as millions of people are relying on video conferencing platforms both personally and professionally. With the help of researchers and bug bounty programs, we all improve our software and services. A few differences on the Zoom platform to highlight:

- New Security control menu in toolbar - brings essential features to your fingertips
- Passwords for Personal Meeting IDs (aka PMI) - now on by default
- Waiting rooms - a virtual staging area that prevents people from joining a meeting until the host is ready. You can customize your waiting room logo and message. You can turn on this feature as a default, or during your meeting for added visibility into who’s trying to join.

For a feature comparison - please view this doc.

Balanced Press/Articles/Videos:

- 4/12/20 - Oracle Chairman and CTO Larry Ellison video on YouTube
- 4/12/20 - Equinix CEO Charles Meyers video on LinkedIn
- 4/10/20 - PagerDuty CEO Jennifer Tejada video on Twitter
- 4/10/20 - Security & Privacy: Beyond the noise — 7 reasons it’s safe to run Zoom
- 4/9/20 - Meeting Tips: The complete Zoom guide: From basic help to advanced tricks
- 4/8/20 - Meeting Tips: How to look your best on a video call
- 4/8/20 - Security & Privacy: Here’s how to make sure your Zoom meetings are secure during the coronavirus pandemic
- 4/8/20 - Entertainment: How Thao & The Get Down Stay Down made a music video on Zoom
- 4/7/20 - Zoom Bashing: How Low Can We Go?
- 4/7/20 - Privacy & Security: A Partial Defense of Zoom
- 4/6/20 - Privacy & Security: ZOMG It’s ZOOM! - Don't worry, it's safe. As long as you follow some rules. - SANS Webcast
- 4/6/20 - Privacy & Security: Get off Zoom's Case, I Trust Them, and so Should You
- 4/6/20 - Zoom Bashing: It’s time to stop bashing Zoom
- 4/5/20 - Privacy & Security: Zoom founder responds to safety and privacy concerns
- 4/5/20 - Privacy & Security: Zooming to Conclusions
- 4/2/20 - Privacy & Security: Security tips every teacher and professor needs to know about Zoom, right now
- 3/29/20 - Privacy & Security: Do These 4 Things To Keep Hackers Out Of Your Zoom Call
- 3/27/20 - Privacy & Security: Zoom Security: Everything That Home Users And IT Teams Need To Know
- 3/20/20 - Meeting Tips: 13 Zoom video chat tips, tricks and hidden features