

October 28, 2020



Dear Client:

We founded Zoom nearly 10 years ago to build the best video-first communications platform for the enterprise segment. Now, our user base has diversified significantly, and we are humbled to have the opportunity to support such a wide range of clients from schools (over 100,000 in 25 countries), to universities (many of the major US institutions), to governments (e.g., major functions of the US Government, the British Parliament, and many other governments around the world), to enterprises of all sizes, industries, and geographies, including full deployments in many Fortune 500 companies. We have grown from 10M daily meeting participants as of December 2019, to over 300M a day in April 2020. We are very proud of the rapid adoption of the Zoom platform, as well as our ability to support this remarkable growth – with strong uptime throughout.

We have always been a leader in innovating at speed and scale, and are equally committed to doing that with respect to privacy and security. We actively and quickly addressed specific security concerns as they were raised over the past few weeks. Zoom absolutely delivers a safe and secure virtual meeting environment when used with the appropriate safeguards to protect meetings, like enabling passwords and waiting rooms. Zoom has been – and continues to be – the platform of choice for many sophisticated organizations all over the world. The attached data sheet includes additional information regarding our security features, both old and new, that help keep your data safe. Our hope is that this information will allow you to take comfort in the fact that Zoom is secure.

If you have additional questions regarding Zoom, we are more than happy to join a call with you and/or your clients to talk through the privacy and security of our platform and company. Zoom remains committed to developing the best, most secure video-first communications platform in the industry, and to keep you, our valued-client, happy. On behalf of the entire Zoom team, thank you for your trust, your support, and your partnership. We hope you, your family, friends, and colleagues are healthy and stay that way as we work our way through this global health crisis.

Please feel free to share this letter with your employees, your management teams, your board, your clients, or any other organization you feel appropriate,

Eric S. Yuan
CEO & Founder

Ryan Azus
Chief Revenue Officer

Aparna Bawa
Chief Legal Officer

Nick Chong
Global Support Services

Richard Farley
CISO

Oded Gal
Chief Product Officer

Brendan Ittelson
Chief Technology Officer

Harry Moseley
Chief Information Officer

Lynne Oldham
Chief People Officer

Janine Pelosi
Chief Marketing Officer

Kelly Steckelberg
Chief Financial Officer

Key Zoom Features for Secure Meetings

Zoom is committed to providing a safe and secure communications platform that allows users and administrators to customize their security and experience via easy-to-use settings. We have engaged some of the industry's top security professionals and our clients to advise us as we continue to develop our products and services given that we are now supporting so many different use cases. Some of our most notable security features include:

- AES 256 GCM encryption for real-time content (Refer to [Encryption Whitepaper](#) for more details).
- Optional end-to-end encryption
- Controlled data routing that allows paying customers to opt-in or opt-out of any of our data centers (excluding their home region) and, for enterprise clients, the ability to customize and manage geographic regions for specific meetings
- **Transparency on data routing** via the account administration dashboard
- Safeguards and controls to **prohibit unauthorized participants** such as:
 - Eleven (11) digit unique meeting IDs
 - Complex passwords
 - Waiting Rooms with the ability to automatically admit participants from your domain or another selected domain
 - Meeting lock feature that can prevent anyone from joining the meeting
 - Ability to remove participants
 - Authentication profiles that only allow entry to registered users, or restrict to specific email domains
- **Meeting host controls** can enable/disable participants to:
 - Content share
 - Chat
 - Rename themselves
- **Admin Controls** to manage virtual backgrounds from the web portal
- **Report** a user
- **Security controls** at the fingertips of the host/co-host with a dedicated Security icon on the main interface
- All cloud **recordings are encrypted** with complex passwords on by default
- Prevent robocalling with **rate limiting and reCAPTCHA** (requires human intervention) enabled across all platforms
- Audio recordings with a user's electronic fingerprint embedded into the audio as an **inaudible watermark** so if the recording is shared without permission, we can help identify the source
- **Content watermarking** superimposes the image of a meeting participant's email address onto shared content they screenshot

We meet the following industry and security organization standards:

- SOC 2 (Type II)
- FedRAMP (Moderate)
- GDPR, CCPA, COPPA, FERPA, and HIPAA Compliant (with BAA)

The above are just some of the key features available in our platform and there will be more as we engineer new defaults and controls over the weeks to come. In addition to these features, we have revamped our vulnerability management and bug bounty programs, acquired Keybase to build our end-to-end encryption offering, engaged advisors such as Alex

Stamos, a widely respected expert on cybersecurity, and formed the Zoom client CISO Council and Advisory Board to collaborate with us in an ongoing dialogue around privacy and security. Please subscribe to our ongoing “Ask Eric” webinar (zoom.com/events) and our blog (blog.zoom.us) to keep updated and informed on our progress in this important area. For more details on Zoom’s privacy and security policies, please visit our [Privacy and Security](#) webpage