All Your Video Conferencing Security Questions, Answered

Maintaining a strong security posture with our partners, stakeholders, employees, and customers has always been a central focus for LogMeIn. Protecting the confidential and personal data of our customers and their end-users continues to be a top priority. Our dedicated Security Team is monitoring all LogMeIn's services 24/7 and is always evaluating industry standard practices regarding technical data privacy and information security and strives to meet or exceed those standards. You can read more about our long-standing commitment to security directly from our CISO, Gerry Beuchelt, in this blog post.

As the demand for remote work increases around the globe across all industries, we'd like to address some of the most common questions our customers have been asking related to the security of our online meetings.

Q: What security measures have you put in place to handle increased traffic?

LogMeIn's collaboration products, such as GoToMeeting, have long been the leader for secure professional meetings for millions of users. With the surge in demand for remote working, we are working to make sure the experience is as secure and reliable as possible. LogMeIn's business continuity plan is designed to ensure all product and operations teams are still fully functional even while working remote. Since the disruption caused by COVID-19, we have increased capacity through extra vCPU, memory and network capacity with no single point of failure in any location and the ability to move traffic between centers without changing the regional controls over data residency.

Q: How is GoToMeeting Secured?

At LogMeIn, all of our products are developed in collaboration with our security team and are rescanned regularly for vulnerabilities. For each LogMeIn UCC solution, standards-based cryptography, a high-availability hosted service infrastructure and an intuitive user interface combine in order to maximize confidentiality, integrity and availability. With TLS encryption protecting sensitive chat, session, and control data transmitted across the network (distributed to all endpoints using up to v1.2 if supported), as well as encryption at rest using 256-bit AES for session cloud recordings, transcriptions and meeting notes, GoToMeeting ensures your company's meetings and information stay confidential.

Our products make it easy to quickly start or join a meeting by enabling GoToMeeting to be launched from a browser. This communication between our components and our user's computers is designed to ensure secure connections that are either installed with end-user consent or hosted on our secure and verified servers. We believe in providing our users with control over their experience, as well as their data (including how and when they install software, as well as use of their webcam and their microphone).

You can find a deeper dive into the security features for GoToMeeting in this whitepaper.

Q: What GoToMeeting security capabilities are available to users?

GoToMeeting product security capabilities include:

- **Secure Content Sharing**: As we continue to expand the features and functionality of GoToMeeting, including by offering cloud recording and transcription capabilities, we have increased the security capabilities for sharing these assets. Within the content sharing and security preferences of GoToMeeting, users can choose what content to share, with whom, and how long to make it available for viewing.
- **Meeting Lock and Password Protected Meetings**: As video conferencing becomes a part of our daily lives, it's more important than ever to take advantage of security features to make sure that the right people are in your meetings. With features like meeting lock, you can keep others out of a meeting. With password protected meetings, only those with the code will be able to gain entry keeping your meeting secure from others who may know your personal meeting code.
- **Security and Privacy Compliance**: All tiers of GoToMeeting include privacy and security features such as Transport Layer Security (TLS) encryption in transit, AES-256 bit encryption at rest of cloud recordings, transcriptions, and meeting notes, SOC2 Type II + BSI C5 certification, TRUSTe Verified Privacy, Rich Based Authentication and are GDPR, CCPA, and HIPAA readiness.

Q: Does GoToMeeting allow the host to track the attention of user, and what other apps they are using?
No. GoToMeeting does not offer a feature to report to its hosts on attendee's usage of other applications. If this is a required functionality for a Webinar or Training use case, this functionality is optionally available in GoToWebinar and GoToTraining, but is turned off by default.

Q: Can all GoToMeeting attendees see everyone else in the meeting, including their names?
Administrators can control the ability for meeting attendees to see each other's name and information, to protect their privacy.

Q: Can all my online meetings be recorded and transcribed?
While meeting recording and transcription is included as a feature in GoToMeeting, administrators can turn this off for an entire organization or for individual users. This feature is also default set to OFF from the start.

Q: If enabled for meeting hosts, who can access GoToMeeting cloud-based recordings and transcripts?
The meeting host can make the meeting recordings and transcripts broadly available, or restrict access to specific individuals.

Q: Can GoToMeeting chat be seen by the organizer?
While meeting chat is included as a feature in GoToMeeting, administrators can turn this off for an entire organization or for individual users.

Q: Does GoToMeeting share my camera without my knowledge or consent?
No. The first time you use our video feature you will be asked for permission – your webcam will not be enabled to share video by default. After that, you are free to remove that permission and change the default settings any time you want. When you use our applications, we will never automatically turn the camera on or share your feed without your consent. Each individual user has access to turn on/off their camera at will. Turning on the camera from outside the application or a meeting is not possible.

Q: Does GoToMeeting install a web server to my computer?
No. Our products install a URI handler which can be used to quickly launch the application, but this does not bypass the security in place by the browser. This is a standard behavior by all modern browsers to provide added security measures. Additionally, our products can be uninstalled completely without leaving any components on the user's machine.