Which Zoom Security Features Are Best for Your Industry?

by sakar | Apr 20, 2023 | Zoom | 0 comments

Security is a crucial aspect regardless of your job or workplace, and that's why Zoom has integrated it seamlessly into its user experience. This enables organizations from different industries to collaborate securely and effortlessly.

Zoom has developed specific features and addressed indu
to help organizations enhance their efficiency and cater t
requirements, whether they are using Zoom for telehealth
meetings, or hybrid learning.

Got any questions? We're happy to help.

Although most of the security features are suitable for all industries, a few are essential for addressing specific pain points in certain sectors.

But before we discuss those, here are some tips to help all users secure their meetings:

General in-meeting controls

Every industry utilizes Zoom in a manner that caters to its distinct requirements. However, Zoom Meetings provides a security icon and a range of in-meeting controls that enable users from all industries to protect their meetings from uninvited attendees. These controls allow hosts to:

1. Manage screen sharing
2. Lock the meeting
3. Set up two-factor authentication
4. Remove disruptive participants
5. Disable video, mute participants
6. Suspend participant activities
7. Turn off file transfer
8. Disable private chat
9. Report a user

It's crucial for all organizations to prioritize these controls and educate their users on how to utilize them effectively, ensuring a secure and well-managed meeting experience.

Education

With the increasing adoption of the hybrid learning model by schools and campuses, it is important for teachers to have access to appropriate security tools to ensure that their virtual classroom is not disrupted by unwanted individuals or unexpected events. The features and commitments listed below have been created to assist teachers and administrators in simplifying the virtual learning process.

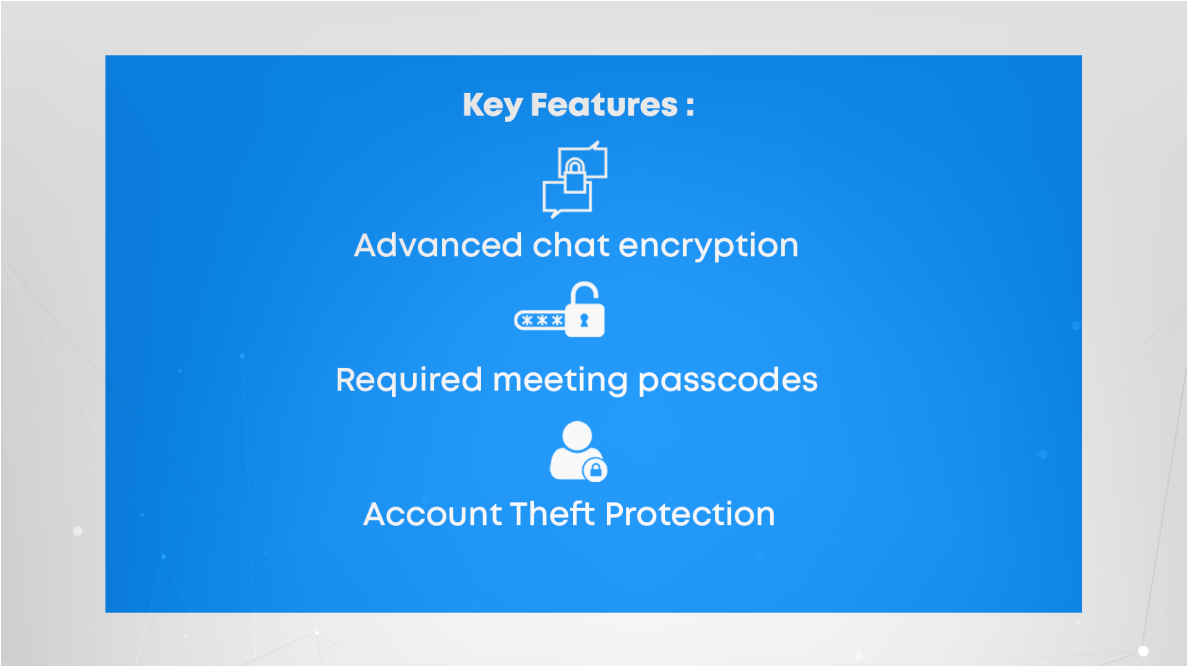
Key features

- **At-Risk Meeting Notifier:** The At-Risk Meeting Notifier is a tool that is designed to be proactive in identifying issues related to meeting privacy. It scans publicly available social media sites and other online resources for Zoom Meeting links. If the tool finds that your class link is publicly available, you will receive an email notification.
- **Chat Etiquette Tool:** The Chat Etiquette Tool automatically detects specific keywords and text patterns in both Zoom Team Chat and in-meeting chat. It helps prevent users from sharing unwanted messages that include inappropriate language. It is important to note that the Chat Etiquette Policies are set by account admins and not by Zoom. The tool does not send reports or flags to account admins or anyone else. Those interested in this feature should contact their customer success manager to enable it.
- **Waiting Room:** You can activate the Waiting Room feature in your meeting settings under "Security." This feature sends everyone to a virtual waiting area where you can admit them individually or all at once. K-12/primary and secondary education users have this feature by default. You can customize your Waiting Room by adding a personalized description or video to set expectations for the upcoming lesson.
- **Single sign-on (SSO):** To authenticate users in schools and business environments, Zoom offers a single sign-on feature. This feature creates a safe and quick process for logging in to the Zoom client. If SSO is not an option, using two-factor authentication (2FA) is recommended to add an extra layer of security to the login process.

Healthcare

Healthcare organizations always prioritize patient privacy and well-being. Whether it's telehealth appointments or virtual connections among medical communities, there are certain standards and features that can help safeguard patient privacy.

Key features



- **Advanced chat encryption:** This feature encrypts chat messages between users, making communication more secure and helping to safeguard patient data.
- **Required meeting passcodes:** By creating and sharing a passcode with patients via email, healthcare providers can ensure that only authorized individuals can join a telehealth session.
- **Account Theft Protection:** This feature helps identify users whose login credentials may have been stolen or compromised in a data breach elsewhere on the internet. Zoom sends a notification to affected users, prompting them to reset their password within one day. If the password is not reset in 24 hours, Zoom forces a logout for the user to proactively prevent account takeovers. This provides additional security to telehealth sessions, reducing the risk of cybercriminals using compromised credentials to access Zoom accounts.

Financial services

Ensuring the security of client information is of utmost importance for financial services organizations. The trust of customers, and consequently the viability of the business, depends on it. Therefore, any financial services organization that uses Zoom should make use of the following data management and encryption features to safeguard client information:

Key features

- **Data routing control:** Zoom users can choose which data centers process their data during transit, which is data that is actively moving from one location to another across the internet. You have the option to opt in or out of each specific data center region, except your default region where your account was set up. This helps to maintain control over where information travels.
- **End-to-end encryption:** This feature uses 256-bit AES GCM encryption to encrypt communication between all meeting participants when enabled. The cryptographic keys are only known to the devices of the meeting participants, meaning that no third party, including Zoom, has access to the meeting's private keys.
- **Meeting and Webinar Archiving:** Account administrators can establish an automated mechanism to collect and archive meeting data to a third-party platform of their choice. Unlike Cloud Recording, which saves video, audio, and chat/transcription files to the Zoom Cloud, the Archiving API collects necessary webinar and meeting data/metadata for specific compliance guidelines, as well as the audio, video, and chat files if set in the API call.
- **Information barriers:** This feature is intended to help control user communication policies and meet regulatory requirements at scale. You can use information barriers to prevent certain groups of users with confidential information from communicating with others who are not authorized to access this information.
- **Data loss prevention (DLP) integrations:** These integrations connect with Zoom to allow customers to apply policies designed to detect and block potential data breaches or exfiltration.

Government

As with other modern organizations, government institutions require real-time collaboration while safeguarding critical data exchange. For this reason, Zoom has created Zoom for Government, which is tailored to meet the specific requirements and needs of the government. Let's take a look at some essential security features that are relevant to government workers:

Key features

- **Cross-platform privacy features:** Zoom has introduced a number of privacy features that provide Zoom and Zoom for Government customers with greater insight and control over the privacy of their meetings. These features aid in the protection of critical government information exchanged via our platform. They include the ability to prevent participants from joining meetings using multiple devices at the same time or from a different device after being removed from a meeting, as well as the ability to only allow authenticated users to join meetings.
- **Watermarking:** Meeting hosts can enable two types of Zoom watermarks to help protect the privacy of confidential information shared during a meeting and prevent leaks:

Image watermarks superimpose an image on a shared screen that contains a portion of the email address of a meeting participant. This image is splashed across a person's presentation content as well as their video.

Audio watermarks embed a user's information as an inaudible mark in any offline meeting recording. Zoom can assist in determining which participant recorded the meeting if the audio file is shared without permission.

Securing the hybrid workforce

Secure collaboration is essential for success regardless of industry. As organizations navigate the next phase of work and learn to operationalize the hybrid workforce, security is more important than ever.

Organizations will create a realistic and scalable approach to security by supporting the hybrid workforce with technology that deploys easy-to-use security features.