Technical Review

Zoom: Providing Confident Security

Date: April, 2021 **Author:** Tony Palmer, Senior Validation Analyst

Abstract

This ESG Technical Review documents hands-on evaluation of the Zoom Unified Communications Platform. We evaluated how the Zoom collaboration solution achieves high levels of security, ease of use, and flexibility via its desktop and mobile application. ESG's goal was to examine how Zoom provides confident security for the strictest environments, including government, education, healthcare, financial services, and more.

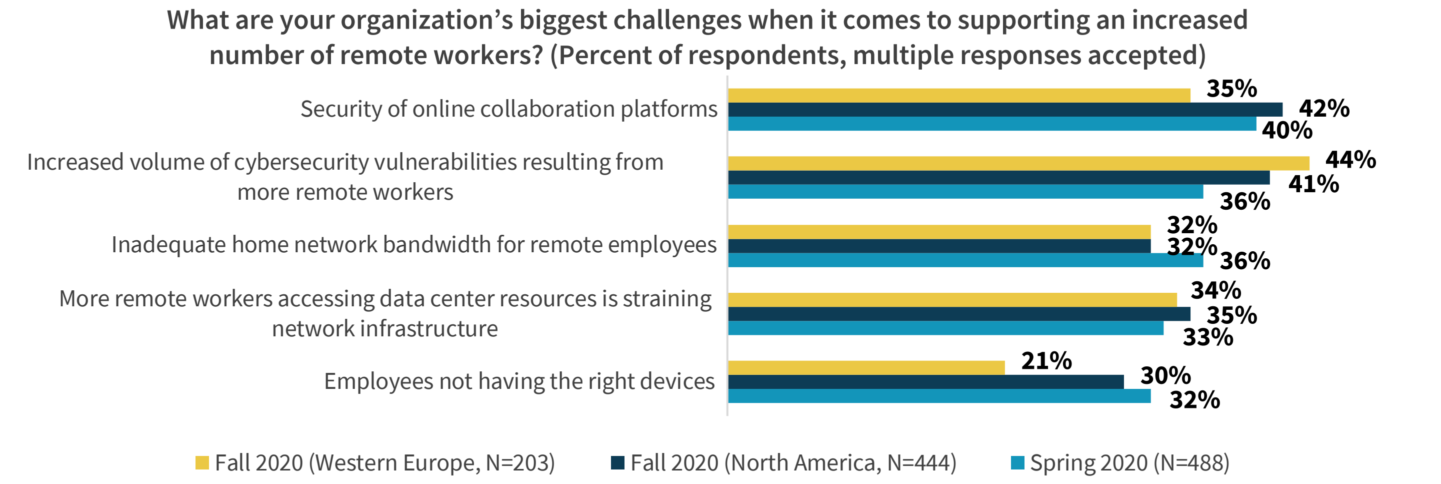
The Challenges

A recent ESG research survey showed that cybersecurity continues to be the top pain point, especially when it comes to supporting an increased number of work-from-home (WFH) or remote workers. Specifically, 42% of organizations surveyed in the fall of 2020 in North America (up from 40% in the spring of 2020) stated that security of online collaboration platforms was one of the top pain points when supporting an increased number of remote workers. In addition, 41% stated in the fall of 2020 that they saw an increase in the volume of cybersecurity vulnerabilities resulting from more remote workers, up from 36% in the spring of 2020 (Figure 1).[1]

When asked what would be most important in justifying IT investments to their organization's business management team in 2021, improved cybersecurity (47%), increased employee productivity (35%), and improved digital collaboration capabilities (30%) were the most-cited responses.

In addition, 25% stated that the broader use of online collaboration tools as part of daily work patterns would be the most significant lasting impact of the current COVID-19 business disruption on their organization's longer-term IT strategy. The lasting tech legacy of COVID-19 will be the widespread adoption of digital collaboration tools.

Figure 1. Security of Online Collaboration Platforms Continues to Be the Most Common Pain Point for WFH



Source: Enterprise Strategy Group

[1] Source: ESG Research Report, *2021 Technology Spending Intentions Survey*, January 2020. All ESG research references and charts in this technical review have been taken from this report, unless otherwise noted.

The Solution: Zoom

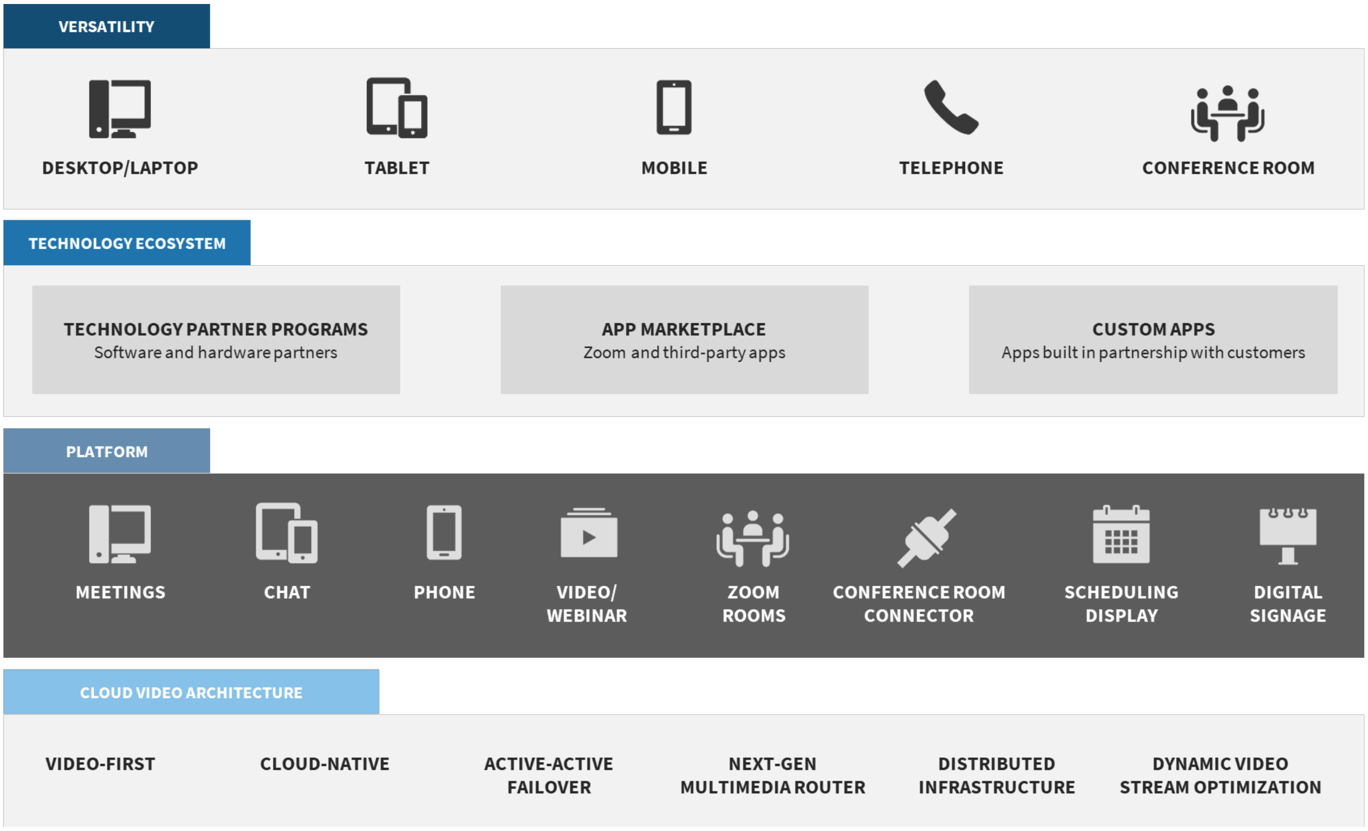
Zoom was initially founded to build a video-first communications platform for enterprises. Over time, its user base has diversified significantly to support a wide range of collaboration clients, including schools and universities; governments; and organizations of all sizes, industries, and geographies.

Collaboration has become essential over the course of the pandemic. The sharp increase in remote workers has created numerous challenges. Chief among those challenges is security.

Zoom has been offering an online collaboration solution since 2012 that provides speed, scale, and ease of use. In early 2020, millions of new users—many with little or no IT expertise—flocked to the platform, drawn by its well-known ease of use. This influx of new users created new security challenges. Zoom quickly moved to address these new challenges with architectural, administrative, and user interface adjustments. Zoom is designed to deliver a safe and secure virtual meeting environment when used with the appropriate settings and safeguards to protect meetings. IT administrators can configure the Zoom solution with specific default security settings, which can be locked so meeting hosts and users cannot modify them. Zoom enables secure meetings via multiple methods and technologies, including optional two-factor authentication; optional end-to-end AES-256 GCM meeting encryption; passcode authentication; the ability to deny, block, or remove attendees; and the ability to lock meeting/webinar access.

Zoom is also designed to be easy and flexible to use via its intuitive user interface and HD screen sharing. In addition, users can join from any device and save webinar settings as a template.

Figure 2. Zoom



Source: Enterprise Strategy Group

Zoom's Security Program

During the first few months of 2020, the Zoom team worked around the clock to support the tremendous influx of new and different types of users. The sudden and increased demand was unlike anything most companies have ever experienced. As March 2020 ended, Zoom quickly realized that it needed to expand its work on security and privacy—so it began making a number of enhancements to deepen security and privacy in Zoom's DNA.

Despite this ongoing work, Zoom has been experiencing a "trust gap" with potential users across industries. This is not because of a lack of new security or privacy features; Zoom has continued to enhance and expand its security feature set. This is more due to a lack of understanding of/hesitancy to accept Zoom's assertions of its commitment to security and privacy.

In April 2020, Zoom began with a 90-day plan, freezing features, conducting reviews with third-party experts, launching its CISO council to dialogue on security and privacy best practices, enhancing its bug bounty program, ramping up penetration testing to identify and address issues, and kicking off a weekly webinar to provide privacy and security updates to its community.

That work has driven feature enhancements like a new end-to-end encryption offering, numerous UI and feature enhancements, and a number of key hires of heavy hitters in the security and privacy space.

Zoom's security program is a testament to Zoom's alignment with customers' needs across industries and verticals. Zoom's security program includes numerous third-party certifications and attestations: to support customer needs across industries and verticals:

- SOC 2 Type II
- CSA STAR Level 2 Attestation
- FedRAMP Moderate
- HIPAA/HITECH Attestation

In short, Zoom has experienced a level of growth that few other companies have experienced. It's clear that Zoom has adapted quickly and decisively to the needs of its user community, from adding and enhancing security and privacy features to educating its user community on best practices.

ESG Technical Review

ESG evaluated Zoom, with a focus on security, ease of use, and flexibility across all client platforms.

Zoom Security

In this section, we cover a number of Zoom security capabilities that address various security and privacy needs: encryption, passcode protection, identity-based security, and in-meeting controls. While our evaluation focused on these key areas, it's important to note that Zoom offers a wide variety of additional security capabilities.

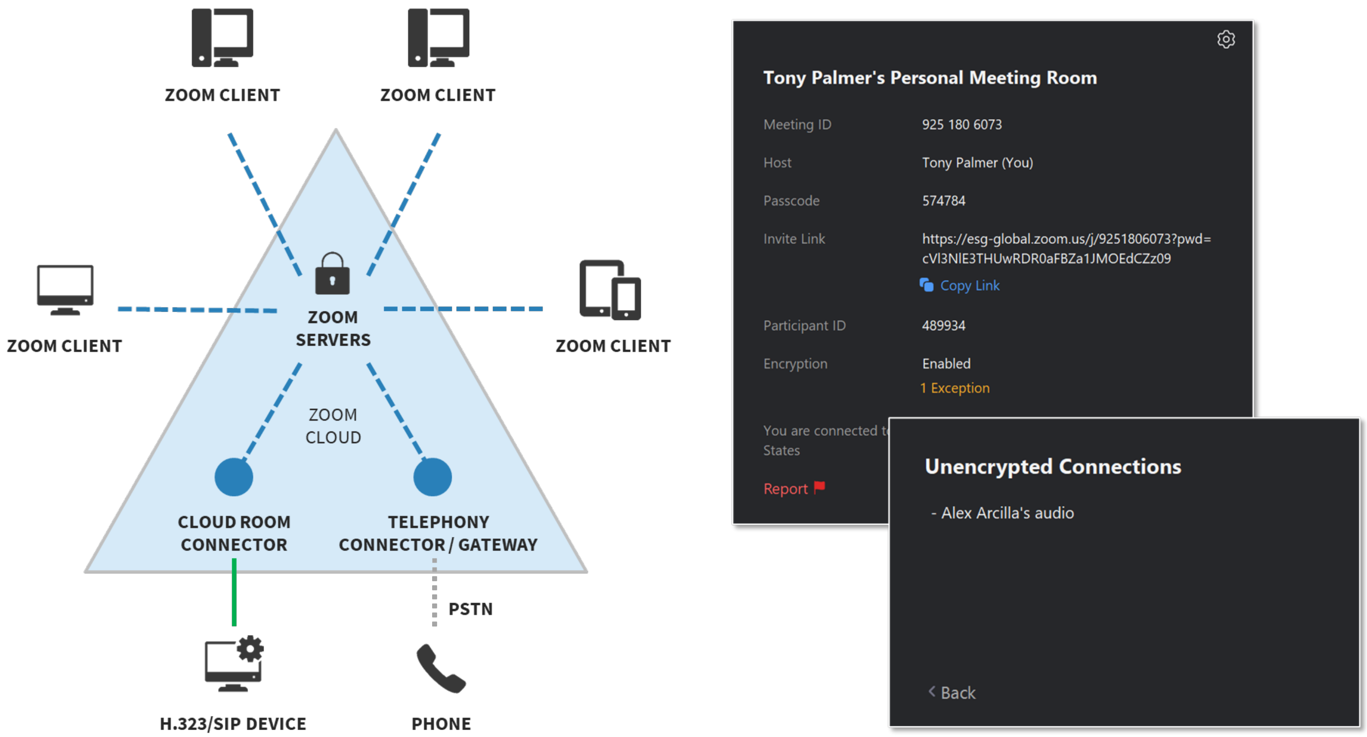
Encryption

Zoom offers client software packages for MacOS, Windows, iOS, Android, and Linux that leverage a range of encryption technologies to assist with user privacy and security. By default, all data transmitted from a Zoom client to the Zoom cloud is encrypted in transit. "End-to-end encryption" is an additional option for all Zoom users—free and paid—and is not enabled by default. Zoom's optional end-to-end encryption, when enabled, ensures that communication between all meeting participants is encrypted using cryptographic keys known only to the devices of those participants. This ensures that third parties, including Zoom, do not have access to the meeting's private keys.

Zoom lets users know when someone connected is not fully encrypted and identifies them so they can remedy it. The in-meeting shield icon, which appears in the top-left corner of meetings, is intended to give users a clearer sense of their meeting's security similar to how web browsers provide an indication in the navigation bar like a lock icon. When a meeting is encrypted, users will see a green shield icon.

Zoom offers methods for a range of third-party services and devices to connect with the system, leveraging communication protocols native to the specific third-party device or server. Encryption methods are limited to what's possible on each device. Customer data transmitted via certain devices and services may not be encrypted in transit to and from Zoom's cloud connectors. For example, if a user calls into a meeting over a telephone (Figure 3), then their audio would not be encrypted until that data reaches Zoom's telephony gateway. Link-level encryption for third-party H.323/SIP devices is supported and can be enforced as a mandatory control if the device has appropriate encryption support.

Figure 3. Zoom Encryption



Tony Palmer's Personal Meeting Room

Meeting ID 925 180 6073
Host Tony Palmer (You)
Passcode 574784
Invite Link https://esg-global.zoom.us/j/9251806073?pwd=cVl3NlE3THUwRDR0aFBZa1JMOEdCZz09
Copy Link
Participant ID 489934
Encryption Enabled
1 Exception

You are connected t
States

Report

Unencrypted Connections

- Alex Arcilla's audio

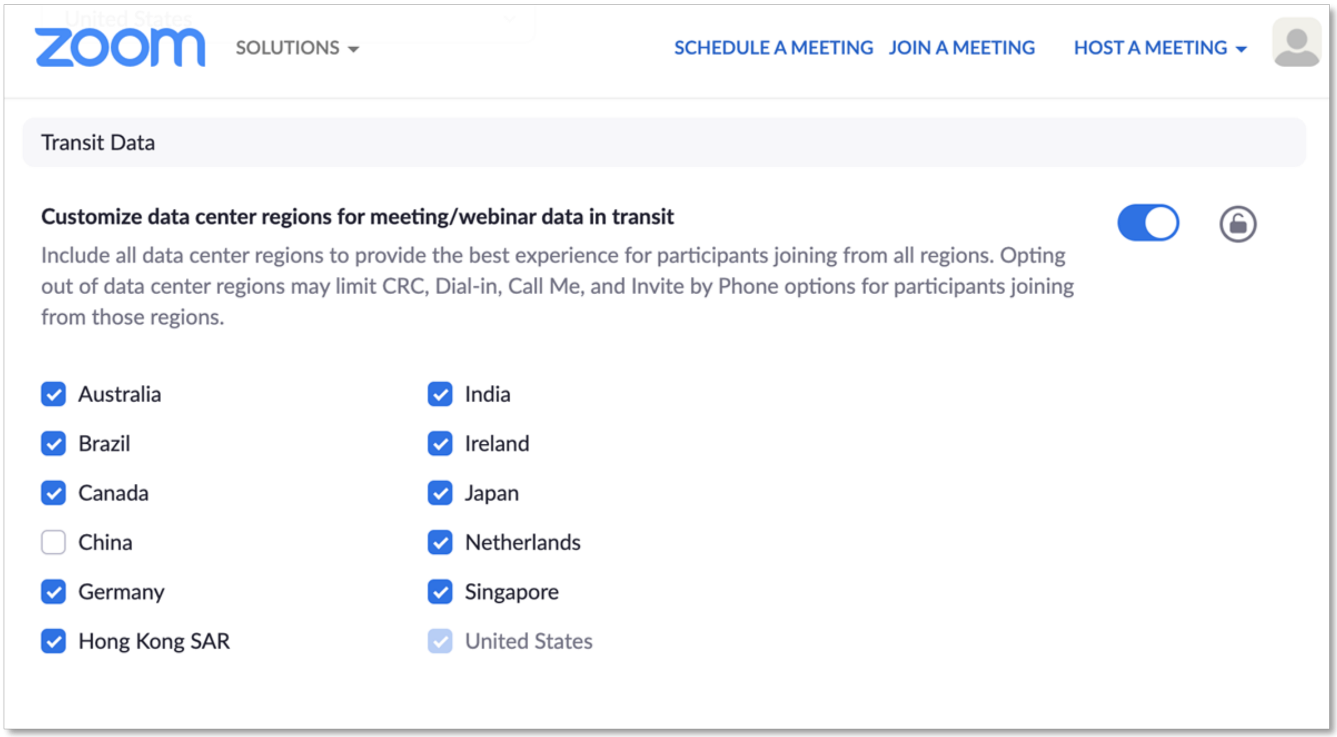
‹ Back

Source: Enterprise Strategy Group

Data Routing Control

Customers on paid accounts can customize their data center settings with respect to data in transit for Zoom meetings and Zoom video webinars at the account, group, or user level. Organizations can opt in to, or out of, specific data center regions with respect to meeting and/or webinar data in transit (see Figure 4). If someone needs to join a meeting from an opted-out region, they can, but the meeting data will still not pass through the opted-out data center.

Figure 4. Zoom Data Routing Control



Transit Data

Customize data center regions for meeting/webinar data in transit

Include all data center regions to provide the best experience for participants joining from all regions. Opting out of data center regions may limit CRC, Dial-in, Call Me, and Invite by Phone options for participants joining from those regions.

☑ Australia
☑ Brazil
☑ Canada
☐ China
☑ Germany
☑ Hong Kong SAR
☑ India
☑ Ireland
☑ Japan
☑ Netherlands
☑ Singapore
☑ United States

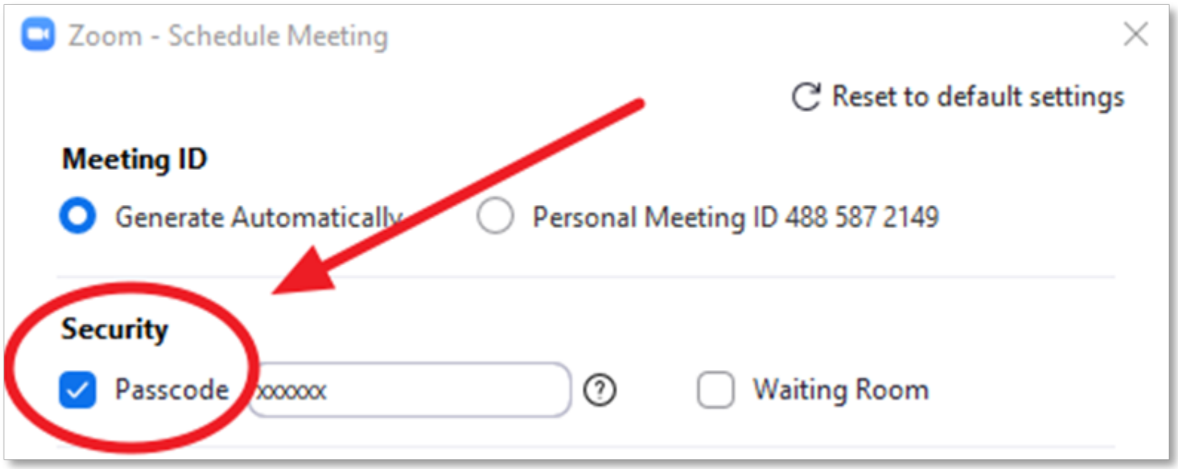
Source: Enterprise Strategy Group

This data center option feature gives organizations more control over their data and its interaction with Zoom's global network and doesn't affect data-at-rest locations. By default, long-term file storage is in an organization's home data center region.

Passcode Protection

Zoom offers pre-meeting security capabilities that are available to the account administrator and, if authorized by the account administrator, individual users on the account, including secure log-in using standard username and password or single sign-on using Security Assertion Markup Language (SAML) (see Figure 5). By default, meetings using Personal ID and scheduled meetings are secured with passcodes.

Figure 5. Zoom Passcode Protection



Meeting ID

● Generate Automatically ○ Personal Meeting ID 488 587 2149

Security

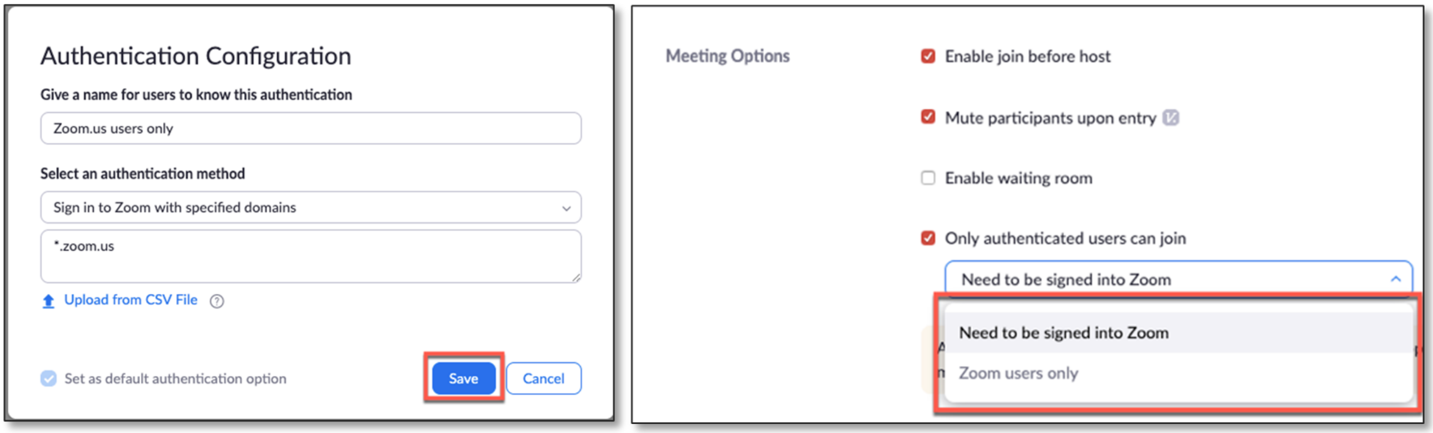
☑ Passcode xxxxxx ☐ Waiting Room

Source: Enterprise Strategy Group

Authentication and Domain Restrictions

The meeting host can selectively invite participants via email, instant message (IM), or text message (SMS), which provides greater control over the distribution of meeting access information. The host can also allow members from a certain domain to join a meeting and/or wait in a meeting's waiting room. Meeting hosts can also customize the registration page with a banner and logo. Zoom enables meeting hosts to restrict participants to just those who are logged into Zoom (see Figure 6). Any of these features can be selectively locked by the administrator.

Figure 6. Zoom Participants Domain



Authentication Configuration

Give a name for users to know this authentication: Zoom.us users only

Select an authentication method: Sign in to Zoom with specified domains

*.zoom.us

☑ Set as default authentication option

Meeting Options

☑ Enable join before host

☑ Mute participants upon entry

□ Enable waiting room

☑ Only authenticated users can join

Need to be signed into Zoom

Need to be signed into Zoom

Zoom users only

Source: Enterprise Strategy Group

In-meeting Controls

Zoom provides multiple methods for a host to secure and protect a meeting in progress, including the At-Risk Meeting Notifier, muting participants, stopping video, disabling chat, removing a user, reporting meeting offenders, locking meetings, and an option for reporting inappropriate conduct.

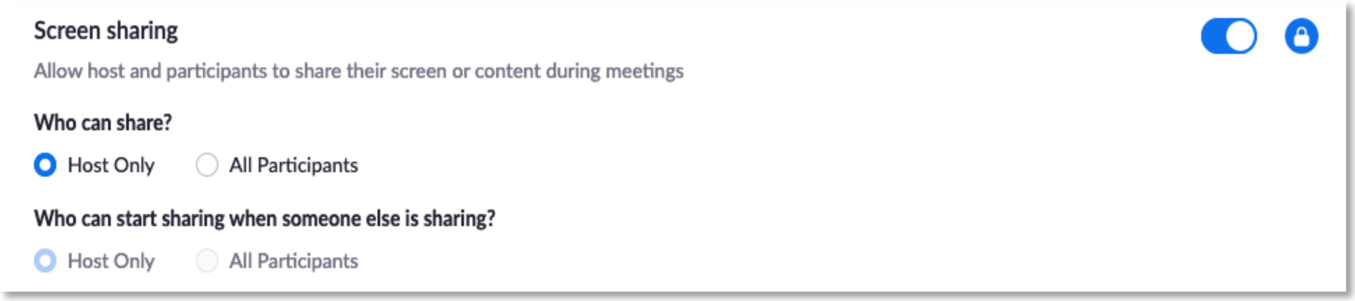
The At-Risk Meeting Notifier scans public social media and other websites for publicly shared Zoom meeting links. When the tool detects a meeting that looks to be at high risk of being disrupted, it automatically alerts the account owner by email and provides remediation advice like deleting the vulnerable meeting and creating a new one with a new meeting ID, enabling security settings, or using another Zoom solution, like Zoom Video Webinars or OnZoom.

If a meeting participant forgets to mute or they are otherwise disruptive or behaving inappropriately during the meeting, Zoom allows the meeting host to solve this problem by muting any or all participants.

For an added layer of security, Zoom allows the meeting host to disable a participant's ability to unmute themselves. When the meeting host is ready to make the meeting interactive, they can simply hit the "Unmute All" button or allow participants to unmute themselves, which asks participants for unmute consent.

The ease of screen sharing is one of Zoom's advantages, but that can also leave the meeting open to unwanted disruptions. Zoom gives the meeting host the ability to restrict screen sharing to only the meeting host or limit users' ability to start sharing if someone else is presenting. The meeting host can easily toggle these features on and off from the screen sharing menu, as well as the security menu (see Figure 7).

Figure 7. Zoom Screen Sharing



Screen sharing

Allow host and participants to share their screen or content during meetings

Who can share?

● Host Only ○ All Participants

Who can start sharing when someone else is sharing?

● Host Only ○ All Participants

Source: Enterprise Strategy Group

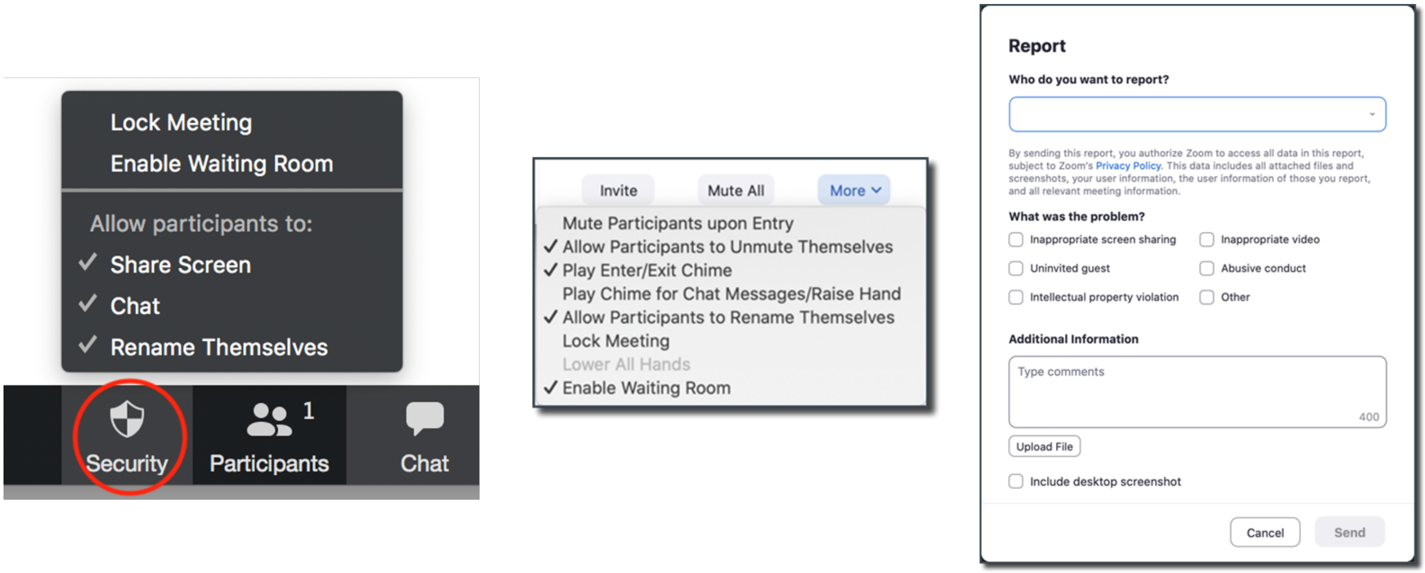
The in-meeting chat adds another dimension of collaboration to meetings, creating a place for questions to be asked and fielded later or for supplemental resources to be posted. But unrestricted chat can become distracting or unproductive at times. Zoom provides the ability to disable and enable chat when scheduling the meeting or at any time during the meeting.

The meeting host also has the ability to remove an attendee from the meeting at any point. For additional security, Zoom allows the host the ability to not allow participants to rejoin the meeting once they have been removed.

Once all attendees have arrived, the meeting host can easily lock the meeting from the security menu, preventing any additional attendees from joining.

Zoom is designed to enable meeting hosts to know exactly who will be attending the meeting. When scheduling, meeting hosts can require attendees to register with their email, name, and custom questions and then restrict users from changing their display name (see Figure 8).

Figure 8. Zoom Host Options



Lock Meeting
Enable Waiting Room
Allow participants to:
✓ Share Screen
✓ Chat
✓ Rename Themselves

Mute Participants upon Entry
✓ Allow Participants to Unmute Themselves
✓ Play Enter/Exit Chime
Play Chime for Chat Messages/Raise Hand
✓ Allow Participants to Rename Themselves
Lock Meeting
Lower All Hands
✓ Enable Waiting Room

Report

Who do you want to report?

By sending this report, you authorize Zoom to access all data in this report, subject to Zoom's Privacy Policy. This data includes all attached files and screenshots, your user information, the user information of those you report, and all relevant meeting information.

What was the problem?

□ Inappropriate screen sharing □ Inappropriate video
□ Uninvited guest □ Abusive conduct
□ Intellectual property violation □ Other

Additional Information

Type comments 400

Upload File

□ Include desktop screenshot

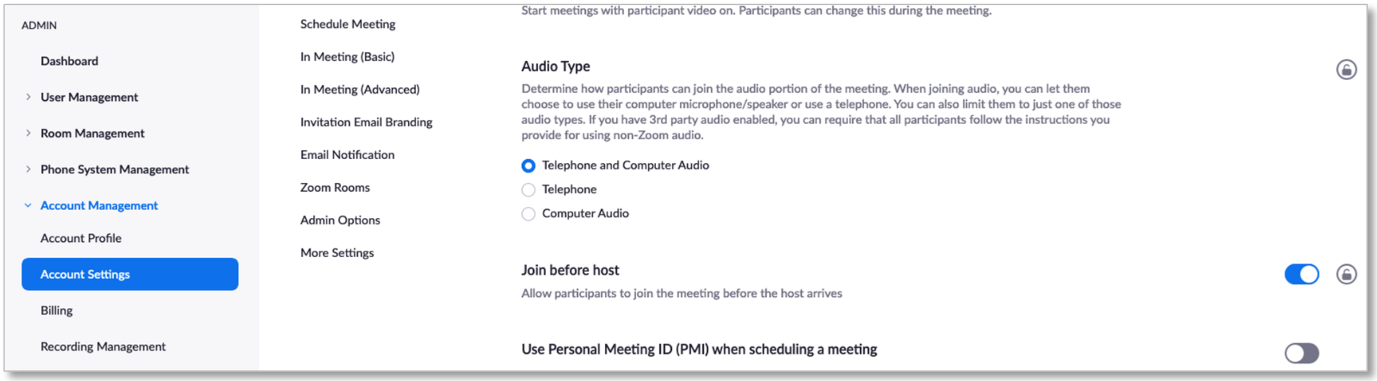
Cancel Send

Source: Enterprise Strategy Group

Ease of Use

With Zoom, administrators can make it easy for meeting hosts and attendees to start, join, and collaborate securely across any device. Zoom syncs with multiple calendar systems and delivers streamlined video conferencing from desktop and mobile devices. Zoom offers centralized IT management and remote assistance to simplify deployment and support, including the ability to track utilization and usage trends; view version distribution; and assign granular permission settings, including account, group, and user levels (see Figure 9).

Figure 9. Zoom Administrator Options



ADMIN

- Dashboard
- User Management
- Room Management
- Phone System Management
- Account Management
  - Account Profile
  - Account Settings
  - Billing
  - Recording Management

- Schedule Meeting
- In Meeting (Basic)
- In Meeting (Advanced)
- Invitation Email Branding
- Email Notification
- Zoom Rooms
- Admin Options
- More Settings

Start meetings with participant video on. Participants can change this during the meeting.

Audio Type

Determine how participants can join the audio portion of the meeting. When joining audio, you can let them choose to use their computer microphone/speaker or use a telephone. You can also limit them to just one of those audio types. If you have 3rd party audio enabled, you can require that all participants follow the instructions you provide for using non-Zoom audio.

● Telephone and Computer Audio
○ Telephone
○ Computer Audio

Join before host (on)

Allow participants to join the meeting before the host arrives

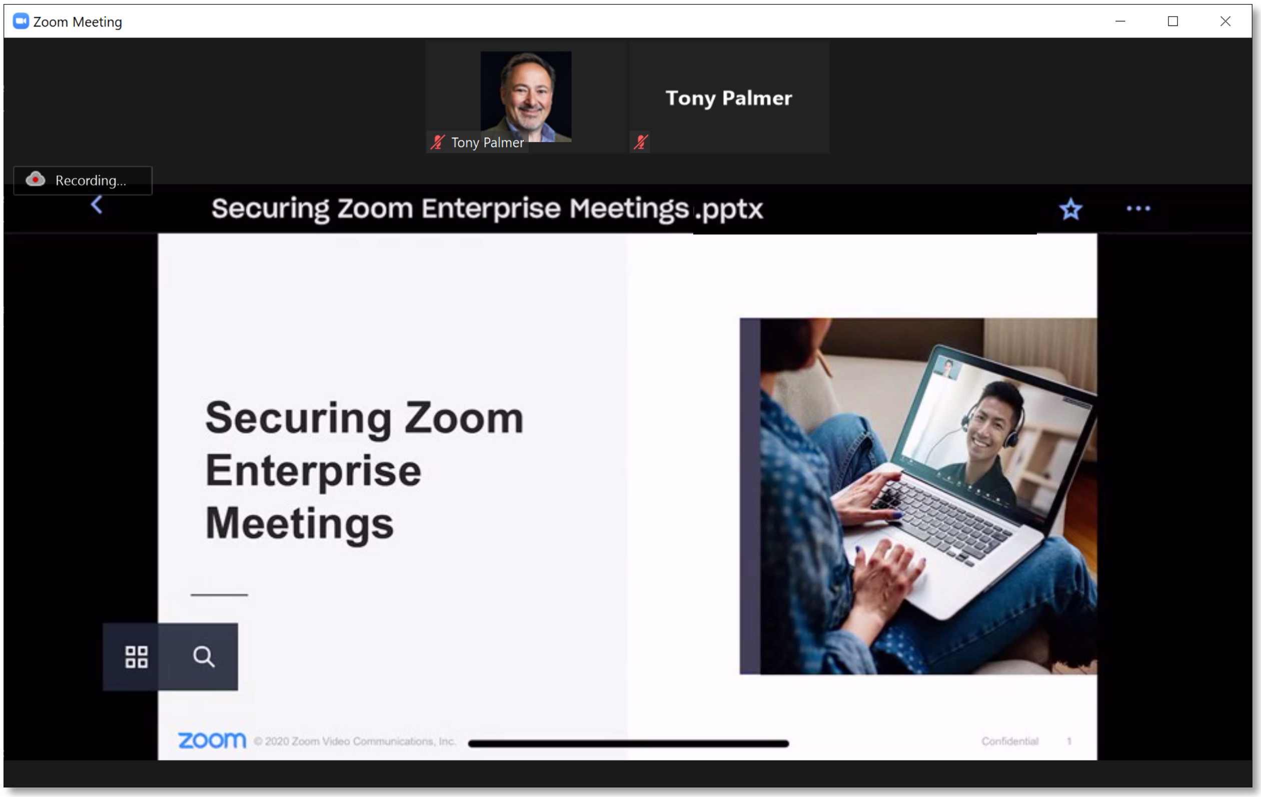
Use Personal Meeting ID (PMI) when scheduling a meeting (off)

Source: Enterprise Strategy Group

Flexibility

Users can join Zoom meetings using a desktop client, mobile app, or web client via the Zoom web portal. The Zoom web portal is primarily used for editing profiles, adjusting meeting and Zoom Phone settings, and accessing meeting recordings in the cloud. While Zoom supports connecting via web clients—Firefox, Chrome, Edge, and Safari—the desktop client or mobile app are recommended, as they offer a more feature-rich experience. Figure 10 shows a meeting with a participant using a smartphone while sharing a PowerPoint presentation.

Figure 10. Zoom Flexibility


Zoom Meeting
Tony Palmer
Tony Palmer
Recording...
Securing Zoom Enterprise Meetings.pptx
Securing Zoom Enterprise Meetings
zoom © 2020 Zoom Video Communications, Inc.
Confidential 1

Source: Enterprise Strategy Group

Connecting to the meeting, sharing, and other features and functionality are available across desktop and mobile clients, which makes joining and actively participating in meetings from anywhere easy.

Why This Matters

When asked what would be most important in justifying IT investments to their organization's business management team over the next 12 months, improved cybersecurity was the most-cited response (47% of respondents), followed by increased employee productivity (35%), and improved digital collaboration capabilities (30%).

ESG believes that Zoom effectively addresses these demands. Collaboration is essential, and the global pandemic has made it more essential. WFH mandates created new challenges for organizations, with security and ease of use at the top of the list. Zoom helps organizations securely connect teams, people, and organizations with strong features and best practices confirmed through hands-on evaluation to make it easy for administrators to manage and even easier for participants to use.

Secure collaboration solutions that don't impede productivity continue to be a high IT priority. ESG believes that Zoom is a secure collaboration platform that delivers on what organizations with the toughest security and privacy requirements—government, education, financial services, and healthcare, for example—and their users need.

The Bigger Truth

Many more organizations are managing remote workforces than ever before. Collaboration platforms are a popular choice, but based on ESG research, organizations and their users expect collaboration technology to be easy to use *and* secure.

Zoom's unified communications platform provides a highly secure, easy-to-use, and flexible solution that helps organizations increase and maintain employee productivity in a remote, in-office, or hybrid workforce environment.

ESG's evaluation confirmed that Zoom delivers a highly secure collaboration solution, with features including strong authentication, optional end-to-end encryption, passcode protection, pre-meeting security options, numerous flexible in-meeting controls, and an option to report inappropriate conduct. Zoom makes its platform quick to adopt, with meeting capabilities that make it easy to start, join, and collaborate across any device. It's clear to ESG that Zoom is a secure platform that can be confidently used in environments with diverse and stringent security and privacy requirements: government, education, healthcare, financial services, and more.

The analysis presented in this report is based on ESG's evaluation, which is conducted in a controlled environment. Due to the many variables in each production environment, following Zoom best practices and aligning policies to your organization's business requirements is strongly recommended.

For organizations that recognize the importance of secure remote collaboration to the success of their endeavors, ESG recommends serious consideration of Zoom. Zoom's strong security protections, combined with its ability to maintain high levels of meeting quality and usability, while allowing hosts to act upon potentially disruptive issues quickly, can help any company or organization to maintain and enhance productivity and collaboration confidently and securely.

The goal of ESG Validation reports is to educate IT professionals about information technology solutions for companies of all types and sizes. ESG Validation reports are not meant to replace the evaluation process that should be conducted before making purchasing decisions, but rather to provide insight into these emerging technologies. Our objectives are to explore some of the more valuable features and functions of IT solutions, show how they can be used to solve real customer problems, and identify any areas needing improvement. The ESG Validation Team's expert third-party perspective is based on our own hands-on testing as well as on interviews with customers who use these products in production environments.