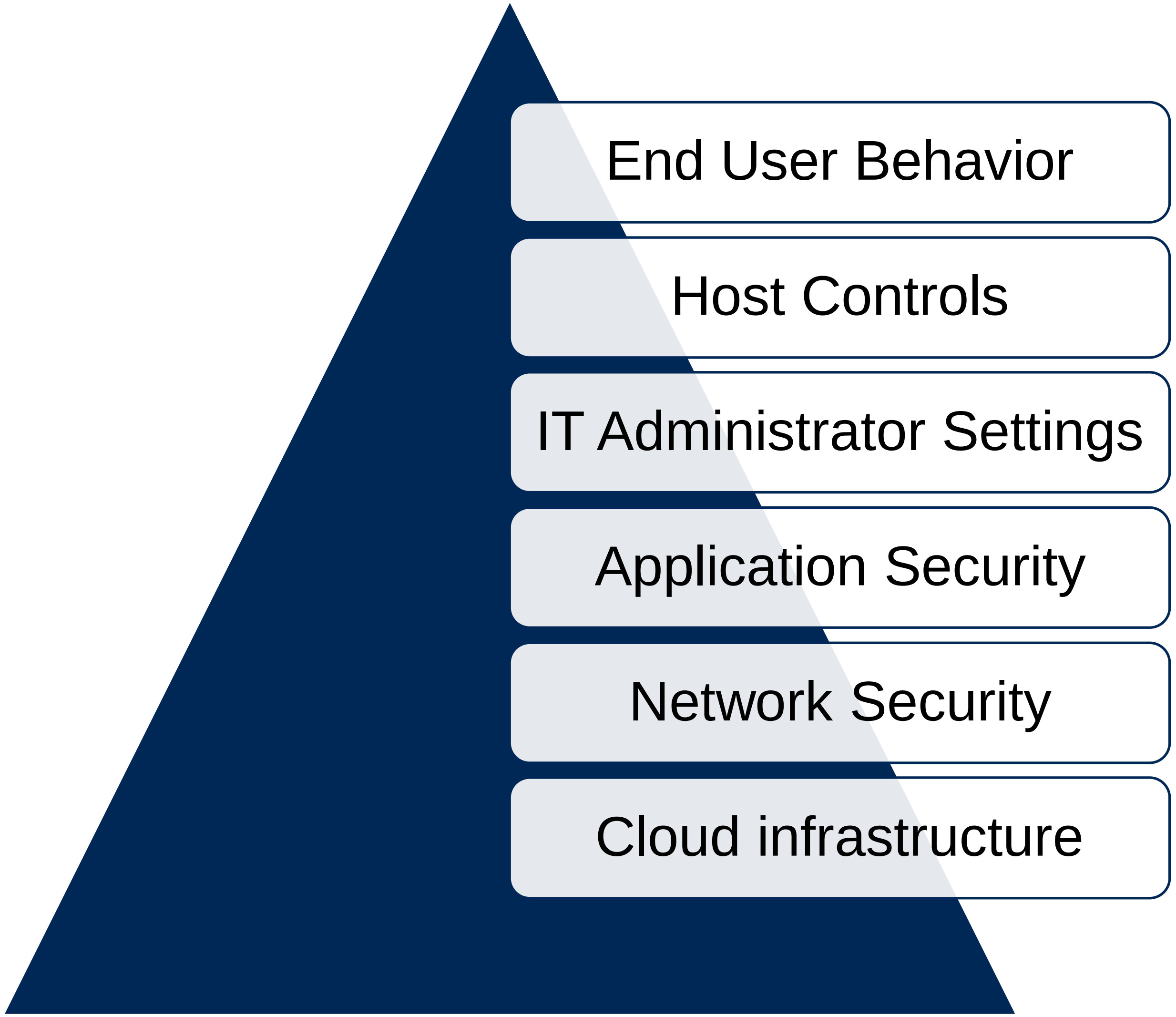
Online Meetings Security Best Practices

Mike Fasciani
Brian Doherty

Gartner®

Security Taxonomy for Meeting Solutions



End User Behavior

Host Controls

IT Administrator Settings

Application Security

Network Security

Cloud infrastructure

Online Meeting Security – Best Practices

Application/Network/Infrastructure Recommendations

- VPN is recommended but many organizations choose SSO instead
- IT provided laptops and mobile devices should be used.
- TLS/SRTP – Key Exchange managed by end user organization (preferably)
- Network vulnerability scanning, DDOS mitigation
- Cloud infrastructure meets stringent ISO27001 / Fedramp

Online Meeting Security – Best Practices

IT Administrator Settings Recommendations

Use Strong Meeting Passcodes

- For applications, six character alphanumeric or higher is recommended

Only authenticated users can join a meeting

- Each meeting participant must sign in to the online meeting account when joining.

Ensure all online meetings are set with a Host passcode

- Different than the attendee passcodes
- Prevents end users from using the online meeting space fraudulently

Meeting ID's should be randomized rather than fixed

- Do not use personal meeting spaces – uninvited guests can join

Turn on encryption

- Online meeting services support end-to end encryption on its native endpoints
- Cloud-based recording/transcription will not work with end-to-end encryption
  - Archiving requirements for regulatory purposes will impact this decision

Online Meeting Security – Best Practices

Meeting Host Control Recommendations

Send the meeting passcode using a separate email for sensitive meetings

Do not share files or links via the app chat box

- Use the corporate approved secure content collaboration platform (e.g. Sharepoint, Dropbox)

The online meeting starts only when the host arrives

- Attendees are parked in a waiting room until the host joins

Once started, a meeting can be locked and additional participants cannot join

The host should control who can present when a more structured conversation is desired

Online Meeting Security – Best Practices

Meeting Participant Recommendations

Do not forward meeting invite

Join meeting from secure location

Join meeting from IT issued device

Join meeting by signing into the meeting solutions account

Use the link in the meeting invite and do not dial directly into conference bridge

- Attendees are authenticated
- Each attendee's name is shown on the control panel
- Reduces the chance of uninvited people joining the meeting

Use VoIP / PC Audio whenever possible

- Telephone calls over the PSTN are not encrypted
- Keeps audio and video in sync

Zoom's Privacy/Security Concerns

Category	Vulnerability	Fixed	Recommendation
Privacy	Leaked iOS device data to Facebook	Yes	Do not use 3rd parties like Facebook or Google to register for Zoom's service
Privacy	User's email addresses were exposed to other users from same ISP	Ongoing	Do not use personal email addresses when registering for Zoom's service
Privacy	Zoom's Windows client allows clicking of UNC links sent via chat without any screening	Yes	Do not share files or web links within a Zoom chat window. Use secure corporate approved content collaboration platforms or email
Privacy	MacOS client allows hijacking of camera and mic, recording of screen, etc – requires local device access	Ongoing	Ensure the MacOS machines have strong password protections and locked down when not in use.

Zoom's Privacy/Security Concerns

Category	Vulnerability	Fixed	Recommendation
End to End Encryption	Zoom's End-to-End encryption only applies to audio and video that originates and terminates on Zoom native clients	No, not likely to be fixed in the near term	The vulnerability lies within the Zoom cloud itself – allowing Zoom employees to snoop the call. This vulnerability is typical for service providers that require calls to traverse a media gateway. If E2E encryption is critical for your organization, then Cisco Webex is best at this function in complex environments.
			E2E encryption breaks functions like Cloud recording and transcription which needs to be understood by regulations (eg. HIPAA)

Zoom’s Privacy/Security Concerns

Category	Vulnerability	Fixed	Recommendations
“Zoom Bombing”	Zoom Bombing is caused by the lack of awareness of consumers and organizations new to online meeting services on the necessity to set appropriate administrative and meeting host control settings	N – though Zoom is now imposing passcodes	1. Use Password protected meetings 2. Use randomized Meetings ID’s 3. Meeting Host controls screen sharing 4. In-meeting chat can be limited to host interactions as well. 5. Only guests from approved IP domains 6. Attendees must register with Zoom service before joining meeting 7. All users must join by clicking on meeting invite rather than dialing around and avoiding authentication 8. Users must not forward meeting invites to others – only the Host can invite.