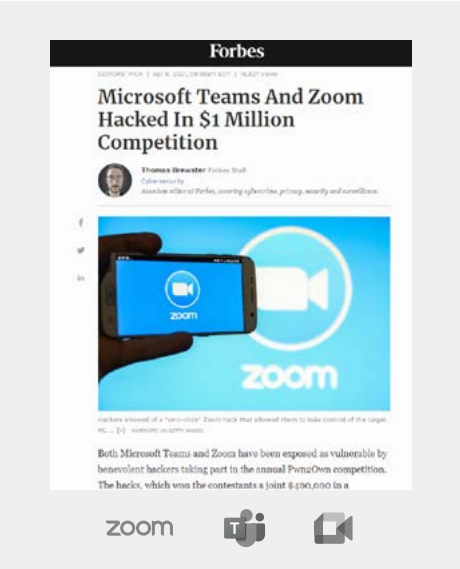
Ericom Virtual Meeting Isolation

The simple, secure way to protect your organization from risks associated with web conferencing tools

Virtual meetings are simply how work is done today. However, serious security concerns regarding data loss and IP protection when using tools like Zoom, Microsoft Teams and Google Meet have led many organizations to impose strict policies that prohibit use of these tools. Client-based virtual meeting apps are not a viable option since many security-conscious organizations do not allow agents to be deployed on user devices.



Concerns regarding virtual meetings often focus on the information sharing aspects of the solutions. Confidential data and PII that may be exposed in meeting chats, shared documents, or via screen shares is a security challenge. Additionally, reported incidents confirm that vulnerabilities can be exploited by cybercriminals to penetrate endpoints and networks. Finally, meeting applications expose IP addresses of participants to potential attackers.

ericom security by cradlepoint

Ericom Virtual Meeting Isolation Highlights

- Supports Zoom, Microsoft Teams, Google Meet and more
- Prevents exposure of sensitive information in chats and screen shares
- Cloud service--requires no endpoint agents
- Policy-based data sharing controls
- Protects against advanced web-base malware
- Meetings may include both isolated and non-isolated participants
- Users enjoy standard virtual meeting experience in a secure, isolated environment
- Delivered on the high performance Ericom Global Cloud

Ericom Virtual Meeting Isolation: Complete Protection from Cyber Threats and Data Loss

Ericom Virtual Meeting Isolation is an innovative solution that preserves all virtual meeting functionality while addressing security concerns.

Prevents exposure of data and PII in chats, screen shares or shared documents and camera images.

Isolates virtual meeting portals to protect against web-based malware that may be hidden in JavaScript and other website code.

Safeguards against unauthorized, malware-enabled recording of virtual meetings.

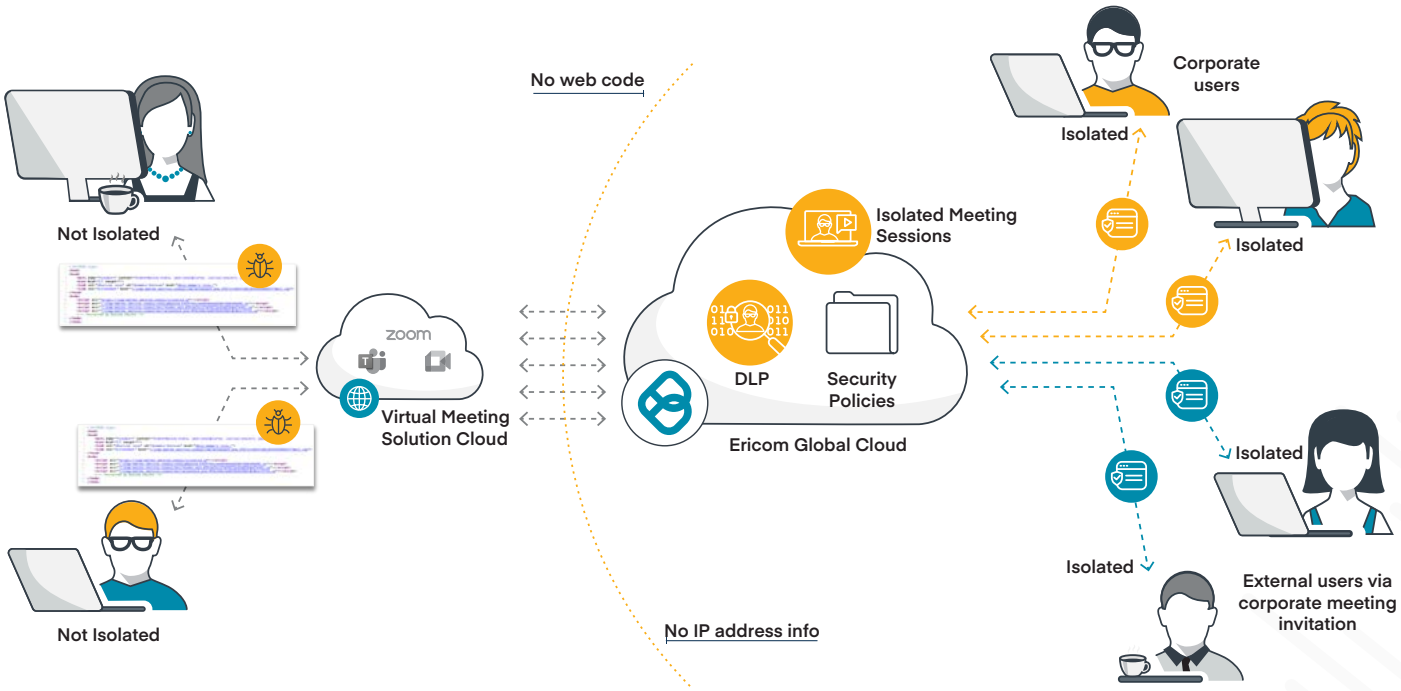
Cloaks endpoint IP addresses from hackers seeking entry.

How Ericom Virtual Meeting Isolation Works

- The user launches their meeting as usual, with a link or via the application website
- The meeting, including virtual microphones, webcams, desktops and other devices, is created within an isolated container in the Ericom Global Cloud
- Virtual devices are synchronized with respective endpoint device status (enabled/disabled)
- When permitted by policy-based controls, media content flows between the endpoint device (e.g., webcam) and corresponding virtual device within the container
- Granular policy-based controls restrict copy/pasting/sharing of documents in chats; screen shares of web and private applications; and ability to share screens.
- DLP prevents exfiltration of sensitive data via chat or document uploads
- Isolated and non-isolated users may participate in meetings, although only Virtual Meeting Isolation users and those joining via Virtual Meeting Isolation-issued invitations are fully protected

Control Each Meeting Participant's Activity

- Limit who can share screens or use cameras and microphones
- Determine who can upload and share files
- Select which users can engage in the chat box
- Specify if file uploads/downloads should be scanned with CDR for malware prevention or DLP to stop data loss



Discover how Ericom Virtual Meeting Isolation can empower your organization to securely leverage virtual meetings without risk of data loss or cyberattack.

Contact us today for a personalized demonstration or to learn more about our scalable cloud-delivered service at ericom.com/contact-us.