ZTEdge™
By Ericom Software

ZTEdge Virtual Meeting Isolation

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

Virtual Meetings: A Significant Threat Vector

Virtual meeting solutions are crucial enablers of collaborative work. However, legitimate security concerns regarding Zoom, Microsoft Teams, Google Meet, BlueJeans by Verizon and similar apps' web portal software have led many organizations to impose strict policies that prevent users from benefitting from these tools. Alternative client-based virtual meeting apps do not address the need, since many security-conscious organizations do not allow agents to be deployed on user devices.

Concerns regarding the web portals of these virtual meeting solutions are similar to those about any web page. Recent headlines confirm that vulnerabilities of these web portals can be exploited by cybercriminals to penetrate endpoints and networks. Additionally, web portals expose IP addresses of meeting participants, creating an attack surface that could potentially be exploited by attackers. Finally, links and files are frequently exchanged in virtual meetings, sometimes with outsiders, creating additional risks.

ZTEdge Virtual Meeting Isolation

- Supports Zoom, Microsoft Teams, BlueJeans by Verizon, and Google Meet
- Cloud service--requires no endpoint agents
- Meetings may include both isolated and non-isolated participants
- Policies can be applied to control data sharing
- Protects against advanced web-base malware
- Users enjoy standard virtual meeting experience in an isolated environment
- Delivered on the high performance Ericom Global Cloud

ZTEdge Virtual Meeting Isolation: Complete Protection from Cyber-Threats

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

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

Cloaks endpoint IP addresses to prevent them from providing an attack surface for hackers seeking entry.

Restricts content sharing from virtual meeting portals.

Prevents unauthorized, malware-enabled recording of virtual meetings.

ZTEdge™
By Ericom Software

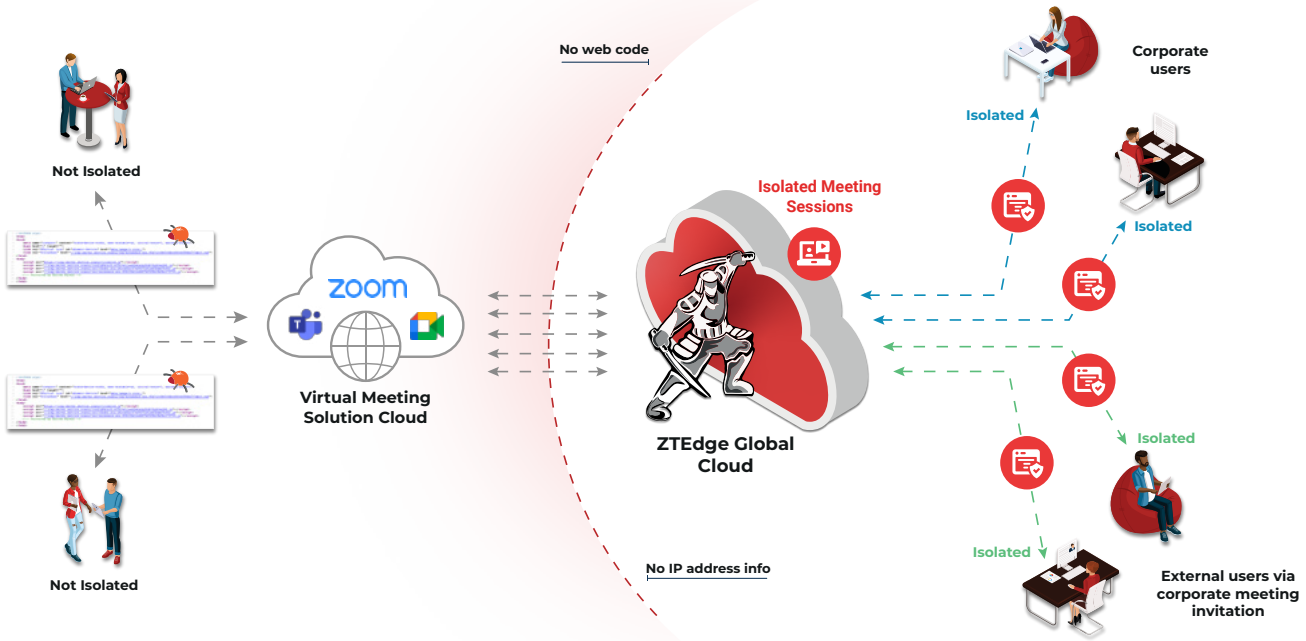
How Virtual Meeting Isolation Works

- User connects to their virtual meeting solution web portal, which opens in a container in the ZTEdge RBI cloud
- Virtual devices--microphone, webcam, desktop--are created within the container
- Virtual device status is synchronized with endpoint (enabled/disabled)
- If enabled - media content flows between the endpoint device (e.g., webcam) and corresponding virtual device within the container
- 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

Leveraging ZTEdge Remote Browser Isolation Cloud Service

ZTEdge Web Isolation renders websites in remote, isolated containers in the cloud, delivering only safe rendering information to endpoint browsers. No active content from the web ever reaches the endpoint, so all threats hidden on websites, even advanced browser-based exploits, are completely neutralized.

ZTEdge Virtual Meeting Isolation is an optional “add-on” module that organizations using ZTEdge Web Isolation can license to extend the benefits of remote browser isolation to the use of virtual meeting solutions.



www.zerotrustedge.com

info@zerotrustedge.com

Americas:
T +1 (201)767-2210

UK & Western Europe:
T +44 (0)1905 777970

Worldwide:
T +972-2-591-1700

Follow us