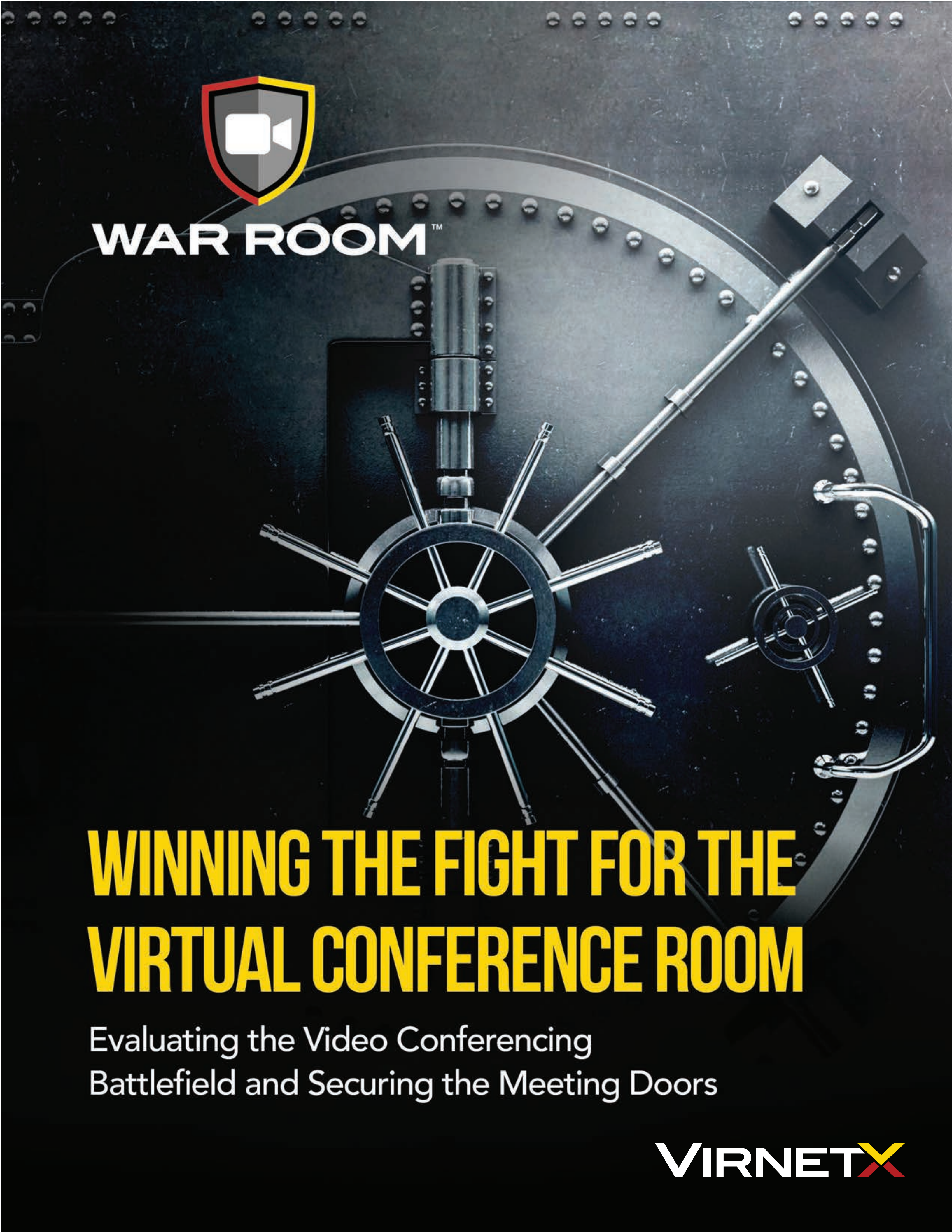


WAR ROOM™

WINNING THE FIGHT FOR THE VIRTUAL CONFERENCE ROOM

Evaluating the Video Conferencing
Battlefield and Securing the Meeting Doors

VIRNETX

Reevaluating video conferencing tools

Accelerated by Covid-19, video conferencing is rapidly becoming a business requirement today for companies with growing remote workforces. According to a recent Omdia Future of Work Survey, 58 percent of respondents indicated they will be working from home, relying on video conferencing to do their jobs.

Initially, the pandemic resulted in big increases in video conferencing tools that were often reactionary and based on business survival. But no more. Businesses are now taking a step back and reevaluating video conferencing tools with an eye on data privacy to better understand the impact of having a predominantly remote workforce regularly using these platforms.

Reevaluation is a smart strategy considering the rise in cyber-attacks on businesses involving remote workers. Since the pandemic, there have been countless attacks on employees using video conferencing including zoom bombing, stolen information, leaked communications, and other costly breaches.

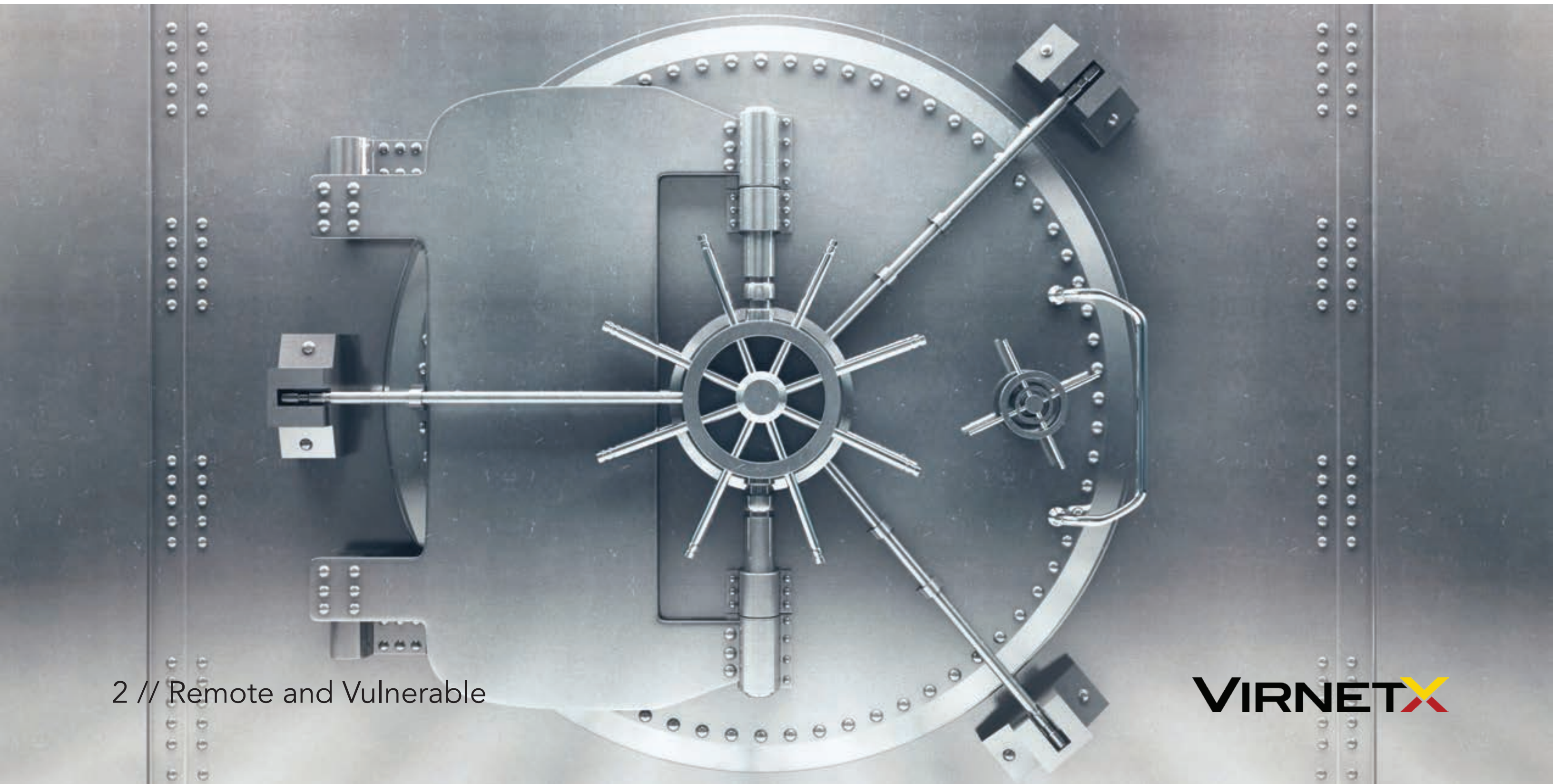
With these attacks continuing, businesses need to protect their workers as well as its sensitive, and valuable information and data.
Most video conferencing companies are good at what they do but none specialize in cyber security. These companies do not fully understand the threat vectors and how they can infiltrate a system.

In this VirnetX white paper, we will introduce a new solution that goes to war against relentless attackers and nefarious bad actors to thwart video conferencing cyber-attacks.

Enter War Room

War Room delivers a closed and private video conferencing and meeting solution that secures the exchange and privacy of information between trusted parties without fear of eavesdropping or data breaches.

Easy to use and secure, War Room works on all devices so employees can seamlessly participate in meetings while working remotely or in the office. Secured by the VirnetX One platform, War Room is built on VirnetX Secure Domain Names and patented technology, giving businesses protection, control, and visibility to secure its communications.



Choose War Room

Customers choose War Room for their meetings to protect sensitive and confidential discussions. All communication is encrypted and removed from any public access, protecting the information that is exchanged. War Room ensures data privacy and compliance requirements can be achieved to protect your communications.

War Room Capabilities

Designed to make it easy to create, join and schedule meetings, War Room offers a full suite of video conferencing capabilities that includes:

- **Video and Audio Conferencing** - High-definition video and clear audio that offers clear and reliable communication regardless of your device or location.
- **Screen Sharing** – Collaborate by easily sharing documents and presentations while receiving feedback and making changes in real time.
- **Group and Private Chat** – Share links and feedback directly with the group or privately with individual participants without impacting the meeting discussion.
- **Moderator Controls** – Manage meeting participants based on the topic with controls to a moderator, ensuring all voices are heard.

Zero-Trust Philosophy, Many Solutions

Built on technology originally developed for the U.S. intelligence community, War Room provides a variety of other features, benefits, and solutions. Here's what War Room can do for your business:

Prevent Zoom Bombing

Meeting links are only accessible by authorized and authenticated participants given access by the meeting host. Zoom bombing is eliminated, because just knowing the meeting link does not give an individual access to the meeting.

For unauthorized participants, the meeting does not exist. They will be automatically blocked from joining and will not have access to the meeting topic or participants through the meeting link itself. War Room's alternative approach is to eliminate all public access.

Unfortunately, other third-party video conferencing solutions create features like waiting rooms to give a false sense of meeting security. Instead of enforcing all participant authentication and creating a truly secure meeting, they instead force the host to filter out unwanted participants at the start of every meeting.

Encrypted Communications

All communications are encrypted (AES 256), protecting the information that is exchanged during the meeting. This extends to video, audio, chat, and screen sharing.

All information about the meeting including the meeting topic, date and time and participants is only accessible by authorized participants and stored encrypted-at-rest.

War Room offers meeting services infrastructure in both the United States and Japan, which means a business has full control over where meeting metadata is stored, and where business communications is routed across all their employee meetings.

Instantly Start Meetings

In one click, you can instantly start a meeting with your contacts and co-workers. You can even create a meeting on-demand to have a private discussion with a select group of participants. Meetings can be started anytime and will run until the host ends the meeting.

In addition, you can easily add or remove participants from the meeting, based on the meeting discussion topics. Instant meetings allow on-demand, private and secure discussions without the need to schedule or coordinate availability.

Instant meetings are ideal for secure, ad hoc, one-on-one conversations that can grow into a group conversation with just a select group of participants.

Schedule Meetings with Ease

War Room allows you to schedule meetings around a topic for a specific date and time with a select group of participants.

Easily change the meeting participants or adjust the date and time as plans or discussion topics change. Quickly view your upcoming meetings schedule and securely join a scheduled meeting with a single click.

Use War Room invite templates to share meeting information in other calendar tools such as Microsoft Outlook.

24/7 Closed and Secure Meeting Rooms

War Room meeting rooms are the new conference rooms, where only select participants have a key to enter. Meeting rooms are reserved, virtual meeting spaces for participants to have on-going discussions.

All the authorized participants or just a subset can join the meeting room at any time to have ad hoc discussions. The host controls which participants can join the meeting room and those participants can be changed over time based on the topics of the discussions. Meeting rooms offer flexibility for businesses

to setup pre-defined team meetings or create rooms for specific clients or discussion topics. All authorized participants can see which participants are active in the meeting room prior to joining the discussion.

Private meeting rooms are ideal for situations like board meetings, team meetings and confidential client discussions where the same group of trusted participants need to meet for on-going discussions.

Share Private Meeting Links

Every meeting has a unique link that can be shared outside of War Room through email, calendar invite or through another communication channel. Meeting links are only accessible by authorized and authenticated participants given access by the meeting host. Zoom bombing is eliminated, the meeting link only has value to those invited.

Collaborate with External Stakeholders

With War Room, you can invite trusted partners, contractors, clients, and customers to participate in meetings. These external individuals can only join meetings or meeting rooms when they are added as a participant. They have limited visibility into employees within your organization. War Room enables collaboration with these external stakeholders while offering security and protection over the meeting discussions.

Control Entry to War Room

Each business or organization can manage employees that are licensed to create, join and participant in War Room meetings and can set organization specific meeting policies. Without a license, employees cannot participate in business related War Room meetings. This offers an additional layer of security and control for managing War Room.

By the Numbers – The Case for War Room

As we emerge from the pandemic, it is important to remember how COVID-19 opened the door for cybercriminals who were able to strike vulnerable remote workers. Many of those threats continue today. The following are some remote work-specific data breach statistics from the pandemic from IBM's Annual Data Breach Report:

- The average total cost of a data breach was more than $1 million higher when working remotely, compared to breaches in which working remotely was not a factor.
- Businesses with more than 60 percent of its workforce working remotely had a higher average data breach cost than those without remote employees.
- When organizations in the United States did not adjust and adapt its IT to handle work changes during the pandemic, the average cost of a breach was more than $5 million, compared to the global overall average of $4.24 million.

Other Alarming Numbers

Not only were video conferencing incidents and attacks on the rise last year, so were other cyber-crimes and attacks including ransomware and crypto jacking. Here are 34 Cybersecurity Statistics to Lose Sleep Over in 2022, courtesy of WhatIs.com, a reference and self-education tool about technology information.

Securing Key Industries with War Room

The following are critical sectors that require absolute stealth video conferencing, and how War Room brings solutions to the fight.

Healthcare

Before COVID-19, many healthcare providers were hesitant to swap their in-person medical appointments in favor of telemedicine. When the pandemic hit, everything changed, and healthcare providers had to step up their telemedicine services.

In the telemedicine world, personal health information and other patient data may be transmitted over devices that are not subject to security protocols set in place by a medical practice. This increases the security risks of telemedicine. Unsecured transmissions are not conducive to privacy and telehealth security.

If a patient's medication data is not secured, it could be intercepted by hackers. According to an Arlington Research report, 52 percent of remote telehealth providers have experienced cases where patients, not trusting the technology, have refused to have a video call, citing concerns about privacy and data security.

War Room Healthcare Use Cases :

- Improve patient outcomes with virtual care, well checks and preoperative visits.
- Real-time communication, training, and career development.
- Bridging the gap to allow collaboration between healthcare providers and teams.

Legal

Since the pandemic, more law firms and private practice attorneys have been utilizing video conferencing for a variety of legal matters including client discovery meetings and official court actions.

Bad actors and other scammers are typically not targeting the firm or the lawyer, but the sensitive information of clients. The legal profession has many rules that require attorneys to preserve client confidentiality and privileged conversations.

Attorneys have a full range of legal duties, and a video conferencing breach can do big reputational damage as well as cost them millions of dollars if existing or new clients leave.

In the American Bar Association's 2021 Cybersecurity Report, 25 percent of the overall respondents reported their law firm had experienced a data breach at some point.

[1] Separate HIPAA business associate agreement (BAA) is required for using War Room to handle protected health information.

The main challenge for the legal industry is to build trust while reducing risk and helping attorney teams securely communicate while working remotely.

War Room Legal Use Cases:

- Mergers and acquisitions (M&A) discussions.
- Confidential attorney-client communications and depositions.
- Company board meetings and discussions.

Financial

The pandemic greatly increased the number of video banking interactions among financial institutions with the technology in place. Before Covid-19, a handful of banks and credit unions were using a video banking platform. But after the pandemic closed branches and limited in-person visits, financial institutions worldwide were desperate to replace in-person interactions.

In general, cyber risks for banks and other financial institutions have grown in recent years as this Carnegie Endowment for International Peace timeline shows. While video banking has its advantages, existing challenges remain such as security, compliance, cost, and customer preparedness. The bottom line: Sensitive information needs to stay private.

War Room Financial Use Cases:

- Comprehensive planning, advice, and financial management for remote members.
- Personalized planning with 1-on-1 coaching for members.
- Differentiate their financial service offerings with an emphasis on security and privacy.

Government

From insiders to criminal organizations, penetrating U.S. national decision-making processes is the primary goal of many foreign intelligence services and bad cyber actors. Adversaries are attempting to steal Federal government data on research and development, personally identifiable information and data on development and research.

In addition, many are looking to disrupt the operations of American institutions and upend systems for politically motivated purposes. One of the first of several Zoom-bombing attacks occurred in 2020 when a House Oversight Committee meeting was disrupted.

Since then, similar attacks have happened at the state and local government levels. The challenge is for governments to adapt to the new realities of remote and hybrid work.

Hackers have become more adept at infiltrating video conferencing platforms and federal, state, and local government organizations must find secure alternatives.

War Room Government Use Cases:

- Collaboration and information sharing between government and the public.
- State and local government internal collaboration.
- Protecting sensitive research and development collaborations.

Enlist in War Room

Diffusing Zoom bombing and other destructive cyber dynamite have never been more critical for businesses. Half measures and insufficient video conferencing technology give cyber thieves and hackers an open portal to listen in on confidential meetings, gain information on insider trading, and conduct corporate espionage and other criminal activities.

Without secure video conferencing, the consequences can be dire. Zoom bombing and other cyber-attacks can do irrefutable damage to your good name, company reputation, and financial bottom line.

War Room elevates today's remote workforce by prioritizing user safety with a private and secure virtual environment – all while maintaining business continuity.

War Room is also transcending the virtual and remote meeting space for government agencies and all professional sectors including healthcare, legal and financial.

Isn't it time you went to war against Zoom bombers and other bad actors with a private, virtual meeting space weapon that above all secures the room? Why not learn more and enlist in the War Room today.

Available On All Your Devices

War Room is available on Windows, macOS, iOS and Android to secure your virtual meetings regardless of participants location or their device. Participants can seamlessly transition meetings between devices as they go from the office to working remotely.

Supported Operating Systems
Windows 10 or later macOS 10.15 or later iOS 14.3 or later Android 9 or later

For more information, visit https://virnetx.com/matrix/.

About VirnetX

VirnetX Holding Corporation (NYSE: VHC) is an Internet security software and technology company with industry-leading, patented technology for Zero Trust Network Access ("ZTNA") based secure network communications. VirnetX's patented Secure Domain Name Registry and GABRIEL Connection Technology™, are the foundation for its VirnetX One™, software-as-a-services (SaaS) platform. VirnetX's technology generates secure connections on a "zero-click" or "single-click" basis, significantly simplifying the deployment of network security solutions by eliminating the need for end-users to enter any encryption information. VirnetX's products, including War Room™, VirnetX Matrix™, and Gabriel Connection Technology™, are designed to be device and location independent, and enable a secure real-time communication environment for all types of applications, services, and critical infrastructures. For more information, please visit: https://virnetx.com/.

WAR ROOM™

VIRNETX