



SafeVchat WhitePaper

Introduction

In our last whitepaper, we examined some of the catalysts that have led to the revolution of the massive uptick in demand for Video Conferencing Platforms. The two primary reasons have been the COVID19 pandemic and the near 99% Remote Workforce explosion. Because of this, the Cyberattacker of today has honed-in their crosshairs to targeting the likes of Zoom, WebEx, Skype, Microsoft Teams, etc.

Although the vendors of these various packages have come out with their updates and patches in order to fix the vulnerabilities and weaknesses that have been exposed, it is simply not enough.

- Lack of secure authentication channels
- In-band authentication is easily bypassed
- Unencrypted data entry fields
- Audio and video streams can be eavesdropped

What is needed is a robust Video Conferencing Platform that not only addresses the Cyber Threat Landscape now but also well into the future, thus greatly eradicating the need to apply those upgrades and patches for each new variant that comes out.

The research team at StrikeForce Technologies has designed such a solution, known as the SafeVchat.

The Features of the SafeVchat

1) It utilizes a multi-tiered approach:

In the world of Cybersecurity, we very often hear of the buzzwords of "2FA" and "MFA." This means that a business should use just two or even three protection layers to authenticate an individual trying to access shared resources. But the StrikeForce team quickly realized that even this is not enough; the chances that a perpetrator could break through all of these lines of defenses is still significantly high. Therefore, in SafeVchat, there are at least five distinct layers that are currently available. If the need arises, even more layers can be added, depending upon how private you want your meeting to be. Here is what is currently offered:

- Passwords: A unique OTMP (One-Time-Meeting Passcode) is required for each meeting participant and is auto created by the platform;
- Authentication: Each meeting participant is authenticated with 2FA/MFA "Out-of-Band" Authentication

- Authorization: Only meeting participants who are provisioned or “pre-registered” in advance of the meeting are granted access – he or she cannot simply enter the meeting while it is going on;
- Endpoint Security: The Host meeting endpoint can be secured from spyware and malware (Premium Version with PrivacyLok)
- Encrypted Audio & Video: Both the audio and video in the meeting are fully encrypted. This simply means that in the off chance a Cyberattacker can break through these lines of defenses, there is not much that they hijack that is worth value because what is being spoken and seen is entirely encrypted.

2) A robust suite of User Authentication tools:

In this regard, there are numerous tools in which a meeting participant can use various means to authenticate themselves (proving whom they are claiming to be). Examples of this include the following:

- Out-of-Band Phone Call to the user’s mobile device
- Mobile App Tokens;
- Various forms of Push Notifications;
- Email OTMP (One-Time-Meeting Password)
- Biometrics – This is where a unique physiological or behavioral trait is captured to confirm the individual's identity i.e. Fingerprint & Facial Recognition

3) Further levels of Endpoint Security:

As previously mentioned, not only are the device endpoints protected but the following as well, thus affording your team of the highest levels of security that is offered:

- All passwords that are used and all chats (that are happening both in real-time and which are also archived) are fully encrypted;
- The features that are available in the Privacy Lok can also be deployed here as well, which are as follows:

*Anti-Keylogger Keystroke Protection: Stops keylogger malware from stealing login credentials and other confidential corporate & customer data, meets or exceeds compliance requirements for 2FA;

*Anti Screen Capture: Prevents malware from secretly taking screenshots or your personal information or the content displayed on your computer monitor;

*Anti-Clickjack: Detects and highlights hidden clickjacking attacks. Warns you against clicking on malicious invisible objects embedded in legitimate web pages

*Video Lock-Down: Locks down access to the computer's video camera (Only pre-authorized applications can be seen and gain access);

*Clipboard Protection: Encrypts the data saved when you use the copy/paste feature and prevents malicious applications from accessing sensitive data;

*Audio (In/Out) Lock Down: Locks down access to your computers microphone, speakers, and all audio input/output devices. Prevents unwanted applications from accessing the audio stream or tampering with your systems.

4) 100% web-based; No Client Agent to install:

This is probably one of the best features of the SafeVchat. This simply means that your team participants do not have to have a dedicated device on hand; they can use whatever device they already have. Once connected, all of the security features described thus far will become instantaneously available. This is a complete win-win situation for the road warrior when either their iPhone or Android device becomes the primary vehicle for communications.

One of the other features of the SafeVchat, which far outpaces the other Video Conferencing Platforms, is real-time Audit Reports and Analytics that can be quickly accessed by the meeting managers and other levels upper management that need to see what has transpired. With this particular functionality, one can:

- Get a birds-eye view of the meetings that have been created, occurred, currently in progress, or those that have pre-planned to take place at some future point in time;
- Obtain access to the logs, which shows all of the granular details of the meetings that have transpired, which includes the following:

- *The creators and the participants;

- *The various authentication methods that have been used to confirm without a doubt the identity of all of the meeting attendees;

- *What time each authorized participant logged into the meeting and how long they stayed in;

- *Failed attempts to login, and those meetings that were terminated for no immediate reason;

- *Various filters and queries can also be deployed based on other permutations that you have established.

5) System Features:

- Unlimited Meetings
- Unlimited Meeting Participants
- Unlimited Meeting Duration

6) Flexible Deployment:

- 100% Cloud-based:
- Hybrid- Installation is available for organizations that want to manage the entire platform from their own data center or virtual private network.

- Active Directory Sync/LDAP
- API Interface
- Users provisioned via portal, File Import or Active Directory

7) Meeting Management:

- Shared Corporate Database- Toggle between personal and corporate database
- Mobile Applications- iOS and Android
- User Self Administration Portal
- Multi-level Admin Portal – User Management and Audit Reports
- Add meeting agenda
- Add meeting minutes, notes and related links
- Desktop sharing
- Raised hand functionality
- Instant chat
- Mute participants
- Video Recording
- Live Stream

Conclusions

The best of all is that SafeVchat is very affordable, even to the Small and Medium-Sized Business (SMBs). There is a three-tiered pricing platform, which is:

- The SafeVchat Standard version: \$12.95 per month per user;
- The SafeVchat Premium version: \$15.95 per month per user (includes PrivacyLok);
- SafeVchat On-Premise version: Pricing is based on your configuration.

If you would like to have a free demo of the SafeVchat or have any other questions, please contact us at www.SafeVchat.com.