LiveWebinar

SECURITY AND PRIVACY

INTRODUCTION

LiveWebinar enables employees located globally and virtual teams to meet and collaborate in real time by placing them in the same room together allowing seamless interaction. Real Time Online Communication can improve on traditional face-to-face collaboration by making travel time and costs, and even conference room space, a non-issue.

Businesses, institutions and government agencies worldwide rely on the solutions of LiveWebinar to simplify business processes and improve results for sales, marketing, training, project management and support teams.

For every business or organisation privacy is key to maintaining control over your ideas and information- naturally your environment for online collaboration must also protect you. LiveWebinar security technology protects you right from the point of scheduling a meeting all the way up to authenticating participants and content sharing.

RTC^{Lab} places security as a top priority in the design, deployment and maintenance of its network, platform and application allowing LIveWebinar to be incorporated into the most rigorous business security processes with confidence. Understanding the security features of LiveWebinar online solutions and the communication structure of the LiveWebinar Cloud is a vital aspect of your investment decision.

THE LIVEWEBINAR CLOUD INFRASTRUCTURE

LiveWebinar platform is a solution delivered through the LiveWebinar Cloud - a dynamic and highly secure service-delivery platform designed with only industry leading performance, integration, flexibility, scalability and availability. The LiveWebinar Cloud offers ease of deployment and application delivery to lower your total cost of ownership while making it possible to achieve the highest grade of enterprise security.

SWITCHED ARCHITECTURE

RTC^{Lab} has deployed a globally distributed and dedicated network of high-speed meeting switches meaning all meeting session data originating from the presenter's computer and arriving at the attendees end destination is put through a process of switching and never permanently stored through the LiveWebinar Cloud.

DATA CENTERS

The LiveWebinar Cloud is a communications infrastructure which has been purpose-built for real time web communication. LiveWebinar sessions use switching equipment located in multiple data centres around the world. Data centres are strategically placed in major internet access points and employ dedicated high-bandwidth fibre connections to route traffic globally. RTC^{Lab} operates the infrastructure within the LiveWebinar Cloud allowing data to remain isolated by region, for example all data shared in the U.S. remains local to the U.S.

In addition RTC^{Lab} operates network point-of-presence (PoP) locations that facilitate backbone connections, internet peering, global site backup and caching technologies used to enhance end-user performance and availability. RTC^{Lab} security personnel are available to assist 24 hours a day, seven days a week.

OVERVIEW OF THE HIGHLY SECURE LIVEWEBINAR EXPERIENCE

The LiveWebinar experience encompasses:

- Various options for starting and joining a LiveWebinar session
- Multiple Encryption Technologies
- Transport-layer Security
- Firewall Compatibility Assessment
- Meeting Data Privacy Assured
- Additional In-Meeting Security
- Single Sign-on Option
- Third-Part Accreditations (Independent audits are conducted to validate security).

The terms “LiveWebinar (s)” and “LiveWebinar sessions” refer to integrated audio conferencing, internet voice conferencing and single/multi-point video-conferencing used in all LiveWebinar online products.

LIVEWEBINAR ROLES

Three role types can be used during a LiveWebinar: Host, Presenter and Attendee.
The following sections describe the security privileges of each role:

HOST
The host is the meeting administrator and is the person who created the meeting session- the host is able to view and change all details as the owner of the room.

PRESENTER
A presenter is an attendee given extra permissions by the host- a presenter unlike normal attendees is able to share certain applications, invite new attendees and has additional security privileges.

ATTENDEE
An attendee has no security responsibilities or privileges.

LIVEWEBINAR SITE ADMINISTRATION MODULE

LiveWebinar employs a site administration module which allows certain authorized administrators to manage and implement security policies for both Host and Presenter privileges on a meeting-by-meeting basis. We allow the option to customize sessions configurations to disable a Presenter's ability to share certain applications or transfer files on a specific site or user.

LiveWebinar can recommend the security features below:

Specific User Account Actions

Change of password at next log-in a requirement
Lock or unlock a user account
Activate or deactivate a user account

Account Creation

- Require security text on new account requests
- Require email/mobile confirmation of new accounts
- Allow self-registration (sign-up) for new accounts

Account Passwords
Enforce strong account password criteria, including:

- Mixed case

- Minimum length
- Minimum number of numeric characters
- Minimum number of alphabetic characters
- Minimum number of special characters
- No character to be repeated three times or more
- No reuse of a specified number of previous passwords
- No dynamic text (site name, Host's name, username)
- No passwords from a configurable list (for example, "password")
- Minimum time interval before password change
- Change of account password by Host at a configurable time interval
- Change of account password by all users at next login

PERSONAL MEETING ROOMS

Personal Meeting Rooms can be accessed via a personalized URL - this allows the host to list all scheduled and in-progress meetings as well as start or join a meeting.

OTHER SECURITY-RELATED FEATURES ENABLED THROUGH LIVEWEBINAR SITE ADMINISTRATION

- The Host or Attendee have the option to save names and email addresses making organizing or joining new meetings easier.
- Site access can be restricted through authentication for all Host and Attendee access. Authentication can be required to gain access to meetings or any site information including listed meetings.
- Strong password rules can be applied to LiveWebinar.
- Approval required for all 'Forgot Password?' emails can be activated.
- Required reset for account passwords can be activated rather than re-entered on behalf of the user.

SECURITY OPTIONS FOR SCHEDULING LIVEWEBINAR SESSION

- Individual hosts can be enabled to specify meeting access security- this can be configured at a site administration level and cannot be overridden.

- Attendees can be given access to join a meeting before the host arrives.
- Attendees can access audio prior to the Host joining the meeting.
- Attendees can be required to provide their email address before joining a meeting.

INTERNAL OR EXTERNAL MEETINGS

The Host can restrict access to attendees who not possess a LiveWebinar account - this is verified by their ability to log-in to LiveWebinar before joining a meeting.

MEETING PASSWORDS

A Host can set a meeting password and then choose to include or exclude the password in the meeting invitation email.

ENROLLMENT

- The 'Access Control List' allows the host to restrict access to invitees meaning only those who have enrolled and have been explicitly approved are able to join.
- Meetings can be further secured by blocking the re-use of registration IDs - any attendee attempting to re-use a registration ID that is already in use will be prevented from joining the meeting to prevent the sharing of IDs among multiple attendees.
- Additionally a Host can maintain meeting security by restricting access and being able to remove participants.

We are able to customize any combination of these scheduling options to further support your security policies.

STARTING AND JOINING A LIVEWEBINAR SESSION

The Host is able to maintain control over the meeting room by having the ability to grant or revoke permissions of Attendees, expel certain members from the session or terminate the session at any time. Meetings are then more secure by eliminating the chance a Host will be assigned to an unexpected or unauthorized attendee.

LiveWebinar can be configured and customized to allow Attendees to join a meeting with audio before the host or by limiting the features to early joiners to just chat and audio.

ENCRYPTION TECHNOLOGIES

Meetings with LiveWebinar are designed to deliver real time rich-media content securely to each Attendee- everything shared by a Presenter is directly encoded with TLS. LiveWebinar provides the following encryption mechanisms:

- LiveWebinar system was built on the most current security methods to provide a fully encrypted and data isolated service.
- Transit Layer Security (TLS) ,
- Secure Socket Layering (SSL).
- Compliant with: Health Insurance Portability and Accountability Act (HIPAA).
- All data protected both in Transit and at Rest,
- Fully safeguards PHI allowing HIPAA compliance.
- Automated Infrastructure: Access to production is fully restricted.
- User Data Isolation- Dedicated and isolated infrastructure options.
- Double Encryption- SSL in addition to stream encryption.

MEETING DATA PRIVACY

All LiveWebinar session content including chat text, audio, video and desktop sharing are entirely transient meaning by default no data is stored locally on the attendees computer or through the cloud. RTC^{Lab} retains only two types of meeting data which include:

- **Event Detail Records (EDRs):** RTC^{Lab} uses EDRs for billing and reporting- you may review event detail information on your customized LiveWebinar site by logging in using your Host ID. Once authenticated you can also download this data from your LiveWebinar site or access it through LiveWebinar APIs. EDRs contain very basic meeting attendance information including who joined (user name SECURITY 7 and email), what meeting (meeting ID) and when (joining and leaving times).

- **Network Based Recording Files (NBR):** If a Host chooses to record a LiveWebinar session the recording will be stored within the LiveWebinar Cloud and can be accessed through the MyRecordings area of your customized LiveWebinar site. The file is only created if a Host enables NBR during a meeting or chooses a sitewide option to record all meetings. NBRs can be accessed through a URL which contains a non-predictable token- the Host has full control over access to an NBR file including the ability to delete, share or add password protection. The NBR function is optional and can be disabled by the administrator.