Yealink

Entrust Video Conferencing Security

with Industry-leading Yealink Meeting Solution

Contents

Preface

Yealink Meeting is a proprietary global network service developed by Yealink to deliver a quality communication experience. The web services providing meeting setup, user management, meeting management, meeting recording, and other features are hosted in the cloud, while the real-time meeting media is processed in globally distributed first-level hosting and commercial cloud data centers with GDPR, Trusted Cloud, and Information Security Level Protection (Level 3) three certifications.

Infrastructure Security

Computing Environment Security

The computing environment security adopts the security mechanism service between client, application server, and database to secure the processing of application business. System terminals and servers form a tight security protection environment by setting system security mechanisms, mainly mandatory access control, at the core and system layers of the operating system. By controlling user behaviors and permissions, we prevent unauthorized access, ensure the confidentiality and integrity of information and information systems, guarantee the regular operation of business systems, and protect the system from malicious damage.

Zone Boundary Security

The zone boundary is the boundary of the system's secure computing environment and the components that realize the connection between the secure computing environment and the secure communication network for security protection. It includes:

- **Zone boundary access control**: The cloud host configures an appropriate access control policy for the security group to control the data information entering and exiting the zone boundary and prevent unauthorized access.
- **Zone boundary pack filtering**: The cloud host determines whether to allow the packet in or out by configuring the security group to check the source address,

destination address, transport layer protocol, requested service, and so on.

- **Zone boundary security audit**: With the firewall, anti-virus, and IPS intrusion prevention at the zone boundary, timely defense and alarm alerts are given to confirmed risk behaviors.
- **Anti-virus capability**: The anti-virus feature checks the network data flow in real-time at the exit to prevent malicious and unnecessary applications and web content from entering and exiting the network so as to maximize the protection, control and, use of the office area network. Using ASIC-accelerated data inspection engine can quickly and accurately inspect and classify HTTP, HTTPS, FTP, SMTP, and POP3 data without affecting the network traffic speed. URL filtering engine and application control based on users and user groups can assist administrators in implementing web application policies. Malicious content such as spyware, viruses, rootkit attacks, adware, and Trojans can be identified and blocked at the gateway. Moreover, we keep our anti-virus database up-to-date, which could form protection and greatly reduce attacks such as viruses and Trojan.
- **Application security protection**: The exits of the data center network deploy high-performance intrusion prevention systems to prevent attacks on the data center network. The Distributed Denial of Service (DDoS) attack protection system at the exits can clean the application layer attacks of the server and ensure the regular operation of the system.

Virtual Hosting Security

We have security protection, detection, and auditing to protect the virtual hosting. Besides, virtualized security services provided by Network Functions Virtualization (NFV) can improve the security capacity of the virtual hosting.

The virtualized security services provided by NFV include:

- Intrusion prevention (virtual patch)
- Anti-virus (AV)

Configure security groups on the cloud platform to address inter-VM access security.

Isolate and protect the invisible east-west traffic on the network to solve the virtualized network security problems from the network layer and VM multi-layers.

In addition, the cloud security service platform manages and monitors the security components deployed in the host and provides security reports and visual analysis based on the host security events and network behaviors.

System Operating Security

- The system ensures the stable operation and timely disposal of the overall distributed public opinion system and deploys a network monitoring management platform to monitor the running status of servers across the network.
- Yealink Meeting clients strictly check the running environment, including root detection, jailbreak detection, debugging detection, injection monitoring, etc., to ensure that the client runs in a trusted environment and prevents the program from being cracked or exploited by malware.
- Yealink Meeting has a full-time team that conducts security assessment and vulnerability detection on Android, iOS, Windows, and macOS clients, as well as used third-party components (libraries, SDKs), to find vulnerabilities in applications as much as possible to ensure client security.
- Yealink Meeting provides users with network access through Content Distribution Network (CDN) and dynamic acceleration and flexible-stable access through corporate load balancing. When encountering a DDoS attack on the computer room, we defend it through the cleaning services provided by network access service providers.
- Yealink Meeting regularly scans server assets to reduce security risks. Security personnel conduct regular weak password detection and urge server operation and maintenance personnel to increase password strength to prevent brute force attacks.
- Yealink Meeting uses automated vulnerability scanning tools to regularly detect server vulnerabilities. The security personnel will notify relevant personnel to handle and repair them as soon as they confirm problems. In addition, operation and maintenance

personnel will regularly update the system patch to ensure the stable operation of the server.

- Yealink Meeting server has fully deployed with an intrusion detection system, which can monitor the baseline changes of server files in real-time, find abnormal processes, backdoor Trojan and other abnormal behaviors, and respond in time. In addition, all traffic from the Yealink Meeting clients is detected and verified by Web Application Firewall (WAF) to ensure its security and legitimacy and block malicious requests in real-time. The security team closely follows the security posture and the latest attack methods and regularly upgrades the defense strategy.
- Yealink Meeting monitors internal and external security vulnerabilities and threat through multiple methods. We have a perfect vulnerability life cycle management strategy, and a professional security team follows up with all security problems. The security team uses automated security scanning tools to scan services and operating systems and conducts security checks on applications through regular penetration tests. After the security team confirms the vulnerability and threats, the team will determine the risk level according to the hazard situation and push the issue to the relevant departments for repair and processing at the first time.
- Yealink Meeting has a full-time security team to provide remote server monitoring 24 hours a day, 7 days a week. When a security incident occurs, the security team will quickly classify the incident according to the security contingency plan and start the emergency response process to prevent the security from expanding. After handling the security incident, the security team will review the incident and record the review results and follow-up measures to ensure the closed-loop of the incident.

Data Security

Data Storage

Yealink Meeting provides a global service and the information of users around the world is stored according to the following rules:

- The user information generated from using Yealink Meeting products and/or services

within the EU and Americas is stored on servers in Frankfurt, Germany.

- The user information generated from using the Yealink Meeting products and/or services by users outside the regions mentioned above will be transmitted and stored on the servers in Germany.

Recording Storage: Yealink Meeting allows users to record video meetings, live streaming and webinars. Users can choose the Local Recording option to save the recording files to the local device or the Automatic Cloud Recording option (available to paying users) to save the recording files to Yealink Meeting. For automatic cloud recording, the recording files are processed and stored in the cloud storage of Yealink Meeting when the meeting is finished.

- The recording files can be password-protected or only available to the registered users.
- Users can save the recording as video and(or) audio files or audio-only files.
- Users can manage their recording files via the secure web user interface.
- Users can download, share or delete the recording files.

Data Isolation

Yealink Meeting secures the data of each registered user. Each individually registered user/enterprise user has data security group isolation and encryption, including:

- **User data management:**

  Yealink Meeting assigns a unique account for each individual user/enterprise user. The enterprise and user accounts cannot be duplicated or mixed, thus ensuring data invisibility between different users of the same resource pool.

- **Users' basic data**:

  User's basic data includes employee information, enterprise information, employee's operation records in Yealink Meeting and other data. These data may be viewed by the operation and maintenance personnel of Yealink Meeting when authorized by the user, but the operation will be recorded.

- **Encrypted user data**:

  We will use encryption and security group isolation to ensure that the user data in the

same resource pool is invisible to each other. The security group realizes the isolation of different user resources through a series of access control at the data link and the network layers.

Data Transmission

The data transmission between the inter-application, and Yealink Meeting server and the applications are all encrypted. In addition to the HTTPS/TLS encryption method, we also have specially customized private encryption methods. These encryption methods can well protect the transmission security of the user's audio, video and other application data, avoiding theft or tampering.

Data Destruction

The data of each registered user is destructible, and the destroyed data cannot be recovered. In order to cooperate with the relevant judicial authorities and to enable users to use the service normally, Yealink Meeting has made the following distinctions regarding the destruction of data in different cases:

- **The data deleted by the user include:**
  - The enterprise administrator deletes user data from the Yealink Meeting web portal.
  - The user closes his Yealink Meeting account
  - The user deletes his recording files

Yealink Meeting will continue to retain the above data for 3 months in accordance with legal requirements. During the retention period, the user-related data will be anonymized and be completely deleted after 3 months.

- **Keep the data of users who have not renewed their subscriptions in time.**

If some paying users are unavailable to renew their subscription in time for some reasons, Yealink Meeting will downgrade these paying users to free users to prevent their important data from being deleted.

Meeting Security

Permission Control

The following in-meeting security capabilities are available to the meeting host:

- Waiting Room
- Remove a participant or all participants
- Lock the meeting
- End the meeting
- Chat with a participant or all participants
- Mute/unmute a participant or all participants
- Screen share permission control for meeting participants
- Call statistics
- Chat permission control for all meeting participants
- Annotation permission control for all meeting participants
- Screen share with watermark
- Set a password before starting a meeting
- Set a password before scheduling a meeting

In-Meeting Security

All content shared with the participants in a meeting is only a representation of the original data. This content is encoded and optimized for sharing using a secured implementation as follows:

- Support H.323 and SIP
- Support dual video stream (H.239 and BFCP)
- Support TLS encryption standard
- Support SRTP (AES-256 bit) encryption standard for encrypting all real-time media (video, audio, and shared content)
- Support SSH for remote connections
- Meeting password and wrong-password detection mechanism
- Support HTTPS encryption standard

- Support not-reversible MD5 hashing function

Identity Authentication

A host is required to authenticate to the Yealink Meeting site with their user credentials (ID and password) to start a meeting. The client or WeChat Mini-program authentication process uses a unique per-client, per-session token to confirm the identity of each participant attempting to join a meeting. Each session has a unique set of session parameters that Yealink Meeting generates. Each authenticated participant must have access to these session parameters in conjunction with the unique session token to join the meeting successfully.

Open or Password-Protected Meetings

The meeting host can require the participants to enter the correct password before joining the meeting. This provides greater access control and prevents uninvited guests from joining a meeting.

Meeting Access Control

To well protect the meeting and release the meeting resource, you can set Yealink Meeting to automatically end a meeting without a host after a specific time.

Login Authentication

Authentication methods include password, captcha, WeChat quick login, or single sign-on (SSO) with SAML. Users authenticating with email and password, phone number and password, or phone number and captcha can also enable two-factor authentication (2FA) as an additional security layer to sign in.

With SSO, a user signs in once and gains access to multiple applications without being prompted to sign in again at each of them. Yealink Meeting supports SAML 2.0 which enables web-based authentication and authorization including SSO. SAML 2.0 is an XML-based protocol that uses security tokens containing assertions to pass information about

a user between a SAML authority (an identity provider) and a web service (such as Yealink Meeting).

Yealink Meeting also offers an API call to pre-provision users from any database backend. Additionally, your organization or enterprise can associate users to your account with domains. Once your associated domain application is approved, all existing and new users with your email address domain will be given the choice to be added to your account.

Administrative Controls

The following security capabilities are available to the enterprise administrator:

- Add users and sub-administrators to the enterprise account
- Delete users and sub-administrators from the enterprise account
- Set permission for the sub-administrators
- Manage the enterprise subscriptions and recording files
- Control the ongoing meetings
- Manage the enterprise Virtual Meeting Room (VMR)
- Manage the security and recording settings for the enterprise meetings.
- Manage the enterprise reports and billings

Chat Security

Yealink Meeting chat encryption allows for a secured communication where only the intended recipient can read the secured message.

Meeting Details Security

Yealink Meeting retains event details pertaining to a meeting for billing and reporting purposes. The event details are stored at the Yealink Meeting secured database and are available to the customer enterprise administrator for review on the web portal interface once they have securely signed in.

Security and Privacy Certifications

GDPR

Picture 4-1 GDPR

Yealink Meeting is authorized to operate under the European Union General Data Protection Regulation (GDPR), a government wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services used by European Union agencies.

Information Security Level Protection (Level 3)

Yealink Meeting has passed the evaluation and filing of Information Security Level Protection (Level 3), established data security system specifications, and implemented technical security measures, which prevent users' personal information from being accessed and modified without authorization and avoid data damage or loss.

Trusted Cloud

Picture 4-2 Trusted Cloud

Yealink Meeting has obtained "Enterprise SaaS Service Certification" from Trusted Cloud, and met the requirements of Trusted Cloud Enterprise SaaS Service in terms of data storage persistence, data portability, data privacy, data confidentiality, user security, service functions, service availability, service resource provisioning capability, fault recovery capability, network access performance, service measurement accuracy, user experience performance and other index items.

Yealink

YMinfo@yealink.com | www.yealinkmeeting.com