Yealink Meeting Security White Paper

Preface

Yealink Meeting is a proprietary global network service developed by Yealink Network Technology Co., Ltd. to provide a high-quality audio and video communication experience to bring business communication and collaboration to enterprise customers. For customers, security is a critical issue involving the data throughout the event flow of a conference.

With security as a top priority, this article provides a comprehensive overview of Yealink Meeting's infrastructure and security measures to ensure secure and controlled cloud video conferencing for our customers. You can confidently apply Yealink Meeting's solutions to your business processes.

Trust and Security

Infrastructure Security

Yealink Meeting is a Software-as-a-Service solution, a highly secure service delivery platform with industry-leading performance, integration, flexibility, scalability and availability. Specifically designed for real-time web communications, communication infrastructure security includes the construction of networks, systems, and data centers. This infrastructure can help to achieve the following:

- Securely deploy services
- Secure data storage with end-user privacy safeguards
- Securing communication between services
- Communicate securely and privately with customers over the Internet
- Safety operations for engineers

Real-Time Media Communication

Based on the distributed low-latency media router with selective forwarding architecture, media data from all terminals are sent to other legitimate terminals

on demand through this distributed media router after 1 or more forwarding. By utilizing dynamic routing calculations and employing a weak stateful service design, it enables real-time selection and adjustment of the optimal media routing link and facilitates second-level disaster-tolerant path switching. The forwarding process does not decrypt the media content, ensuring end-to-end encryption.

Data Center Security

Yealink Meeting useS Microsoft Azure data centers that are SOC2 and ISO compliant. These security vendors provide multiple layers of security measures and complete physical security protection to prevent unauthorized access to data.

These data centers host web services for meeting settings, user management, meeting management, meeting recording, and other features.

Real-time meeting media is processed in globally distributed Tier 1 hosted and commercial cloud data centers. These data centers are strategically located near major Internet access points and use dedicated high-bandwidth fiber to handle global traffic.

In addition, we implement strict access and security policies within our data centers, such as using security groups in an allowlisted manner.

- Deny all access by default and add specified port range and authorized objects to the allowlist.
- Add security groups following the principle of minimal authorization. For example, we recommend that you allow access only to specific IPs instead of all IP addresses (0.0.0.0/0) when opening port 22 of a Linux instance for remote login.
- Add instances of different applications to separate security groups and maintain security group rules independently. For example, associating instances available to public network access to the same security group, opening only ports providing external services, such as 80, 443, etc., and denying all other access by default.

Low Latency and High Availability Solutions

Yealink Meeting designs platform components with a high degree of redundancy. This redundancy applies to the design of our servers, the way we store data, our network and Internet connections, and the software services themselves. This "redundancy of everything" includes handling errors by design and the ability to create solutions that are not dependent on a single server, data center or network connection. With data centers located in different geographical locations, Yealink Meeting can minimize the impact of regional disruptions, such as natural disasters and local power outages on global products. In the event of a hardware, software or network failure, the platform services and control plane are

automatically and promptly switched between facilities, thereby avoiding disruption of platform services and ensuring continuous operations. A highly redundant infrastructure also helps customers avoid data loss. Allow customers to build flexible and highly available systems.

Development Security

The development process of the Yealink Meeting fully follows the Software Security Development Life Cycle (S-SDLC), which covers security activities in all phases of design, development, testing and maintenance. The core concept is to drive relevant personnel to bring security awareness/activities into the entire development life cycle, clarify the collaboration between various parties involved in the project development process, and continuously build enterprise-level software security development capabilities.

Requirement design: During the requirement design phase, we thoroughly assess the security aspects involved according to industry security certification standards (for example, GDPR), to avoid significant design risks. User privacy implications will be evaluated at each release so that the product design meets the product privacy policy and data processing security.

Development phase: By integrating IDE security plugins, we perform real-time security checks during the development process. We also conduct Software Composition Analysis (SCA) scans for open-source components and Static Application Security Testing (SAST) scans for static source code during code submission in Continuous Integration (CI). Any identified issues from the scans are promptly addressed and fixed. All developers are required to follow standardized security processes and coding practices, and regular manual code audits are conducted.

Test verification: The test engineers utilize DAST scanners such as AWVS and Nessus for dynamic application security testing and manual penetration testing to uncover vulnerabilities within the application. Furthermore, they conduct periodic reviews and training sessions on product vulnerabilities to establish a security knowledge base.

Online evaluation: Each version release undergoes a rigorous evaluation to ensure compliance with environment, application, and online security requirements. The criteria for formal online deployment are determined based on system-level security conditions.

Maintenance Phase: Once deployed, the image undergoes regular scanning and timely patching. In the formal environment, operations and maintenance personnel continuously monitor product security using security devices like WAF, XDR, and others. They respond promptly to any detected attacks and establish a vulnerability management system to address and fix external vulnerabilities reported promptly.

Security Precautions

Monitoring Plan

Yealink Meeting's security monitoring program focuses on collecting feedback from traffic level, system host level, and external vulnerabilities.

We conduct traffic analysis to detect suspicious behavior across multiple points in the global network. This includes identifying traffic that may indicate connections from botnets or malicious requests displaying abnormal attack behavior. We employ both open-source and commercial tools, such as Web Application Firewalls (WAF), to detect and validate these activities at the application layer. Continuous auditing and monitoring of traffic flowing through our services are performed to ensure their security and legitimacy. Any detected malicious requests are promptly blocked in real-time to mitigate potential threats.

By deploying an intrusion prevention system, the changes in server files are monitored in real-time. Once abnormal processes, backdoors Trojans and other abnormal behaviors are detected, a timely response will be provided. In addition, the security team closely monitors the security posture and the latest attack methods, regularly upgrades the defense strategy and hardens the servers.

Vulnerability Management

Yealink Meeting monitors internal and external security vulnerabilities and threats through multiple methods. We have implemented a robust vulnerability lifecycle management strategy that encompasses various measures to ensure software security. This includes the use of commercial and in-house tools specifically designed for vulnerability scanning. We conduct automated and manual penetration testing, employ quality assurance processes, perform software security reviews, and engage in external audits to assess and address any potential vulnerabilities in our software. The vulnerability management team is responsible for collecting, discovering, tracking and following up on vulnerabilities. Once the vulnerabilities that need to be fixed are identified, they are recorded through the vulnerability management tool and prioritized according to severity, urgency, and resolution version, and then assigned to developers. The vulnerability management team will track such issues and follow up frequently until it is confirmed that the issue has been fixed, forming a closed-loop tracking and analysis management of vulnerability issues.

The Yealink Vulnerability Disclosure Program encourages security researchers and the public to provide feedback, act in good faith, and participate in responsible vulnerability research and disclosure. If you are confident that you have discovered a vulnerability, data disclosure or other security issue, you are welcome to report it to us at security@yealink.com

Security Emergency Response

Security has always been a focus of Yealink. As industry security technology iterates, Yealink invests heavily in resources yearly to improve Yealink's security level. At the same time, Yealink will find multiple well-known, authoritative third-party organizations for security verification every year to ensure that the security level matches the current security technology. If you find a possible security issue while using Yealink products, you can contact us in Yealink's Security Center or submit your issue through the Ticket system. We will respond and handle the issue in a timely manner. Security emergency response is mainly divided into four stages: issue collection, vulnerability analysis, vulnerability fix, and tracking and resolution.

- Problem Collection: Collect relevant logs and information based on reported security incidents and assign dedicated personnel to track and handle them.
- Problem Analysis: Priority is given to determining vulnerability risks based on the problem. During the processing stage, temporary solutions will be provided first to avoid the problem from expanding.
- Vulnerability Fix: Analyze the root cause of the problem based on its occurrence, trace the reasons for the defects in the design and solve the vulnerability problem in a timely manner from the root cause.
- Tracking and resolution: Investigate whether all product lines have the same problem and follow up to resolve it.

Data Security

Data Privacy

Yealink Meetings places great importance on the protection of user/customer data. Our collection, use and processing principles are only described in Yealink Meeting's Privacy Policy.

User Data: User data includes user information, terminal data, log data, and user-submitted data for specific use cases. We do not share, provide, disclose, sell, rent, or trade your user information with any unrelated third parties unless we obtain your permission or the third party is providing services to you separately or jointly with us. After the service ends, the third party will be prohibited from accessing all such data, including any previously accessible information.

Meeting Data: Meeting data includes titles, times and other attributes of meetings held by users on Yealink Meeting. Meeting data is only for personal viewing by users and management by enterprise administrators.

The following controls are in place to protect the privacy of our customers:

- Encrypt all static data, data in transit, and data in process by default.
- Preventing internal access: Yealink employees do not access customer data unless initiated by the customer for technical support and with their consent to access the relevant data to resolve the encountered issues. In this case, permission requests need to be made through an internal data security specification process and audited by a dedicated person.
- Support numerous privacy regulations.

Data Transmission

All communications between the Yealink Meeting application, Yealink Meeting devices, and Yealink Meeting services registered on the cloud are encrypted. Yealink Meetings uses TLS protocol version 1.2 or higher with high-strength cipher suites to send signals. Once a session is established over TLS, all media streams (audio VoIP, video, screen sharing, and document sharing) are encrypted, as described in the table below.

Media packets are encrypted using AES 256 or SM4 SM3 based ciphers and transmitted via the UDP protocol. The app and room devices utilize AES-256-CBC to encrypt the media. The encryption keys for these media are exchanged through a secure signaling channel using TLS, ensuring the secure transmission of user's audio, video, and other application data, preventing theft or tampering. SIP and H323 devices that support SRTP media encryption can use AES-CBC-128, AES-CM-128, AES-CM-128-HMAC-SHA1 and AES-CM-256-HMAC-SHA1

For standard conferences, devices and services use SRTP hop-by-hop encrypted media, and the Yealink Media Server needs access to the media encryption key to decrypt the media for each SRTP call branch.

Cipher Kit	Bit Length
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	128
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	128
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	256

TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256	256
TLS_ECDHE_RSA_WITH_RC4_128_SHA	128
TLS_RSA_WITH_AES_128_CBC_SHA	128
TLS_RSA_WITH_AES_256_CBC_SHA	256
TLS_RSA_WITH_RC4_128_SHA	128

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 data and meeting data are stored in the following locations**

  User information collected and generated when using Yealink Meeting within the European Union and North American regions is stored on servers located in Paris, France.

  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 France. In such cases, we take steps to ensure that the data we collect is processed in accordance with our privacy policy and the requirements of applicable law.

- **Meeting data that are stored in the cloud**

  Encryption: Transmitted via the TLS protocol and stored on a secure cloud in the client's region;

  Storage method: Each enterprise account will be provided with an unused file storage address, providing logical file segregation;

  Retrieval method: Users granted access to the meeting management platform can only retrieve the recorded files they have permission to access under their own enterprises.

- **Storage, access and deletion of recorded files and transcribed files**

  Allow users to record video conferences and webinars. Users can select the Local Recording option to save the recorded files to the local device or the Cloud Recording option to save the recorded files to the cloud. For

transcribed files, the files are processed and stored in the enterprise's cloud storage when the meeting is over. File owners can perform the following operations on recording files:

- Set password protection.
- Access is restricted to members within the enterprise only.
- Access during the validity period.
- Prevent file downloads.
- Delete recording files. Once a file is deleted, it will be moved to the file recycle bin for a period of 30 days. Users have the option to delete the file directly from the recycle bin or wait for 30 days, after which the file will be permanently erased from the recycle bin.
- The owner of the recording file can manage it through Yealink Meeting Client/Yealink Meeting Management Platform.

- **Data Isolation for each registered user**

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

  User data operations are restricted based on the tamper-proof authorization credentials issued by the server, which includes the user information of the tenant. This ensures that user operations are limited to the scope of the tenant, thereby restricting any changes to the data within that specific tenant.

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.

  When a user deregisters their Yealink Meeting account, all associated user data, meeting data, and recording data will be permanently deleted within 8 hours.

  The user deletes his recording files

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

  Customer data is kept on the server for a long time by default without deletion; if some paid users cannot renew their subscriptions in time for some reasons, we will downgrade these paid users to free users to prevent their important data from being deleted.

Meeting Security

Permission Control

In a meeting, each participant is assigned to a role, and each role is granted different privileges:

Host: There is one and only one host for each meeting. The host has full control over the meeting, and can manage the meeting behavior of all participants during the meeting.

Co-host: The host can designate participants as co-hosts when scheduling a meeting or during a meeting. The co-host and the host enjoy similar permission, and the host can remove the co-host role at any time. Co-hosts can assist the host in organizing and managing the meeting and enhance the efficiency of the meeting.

Attendees: Attendees cannot manage the meeting permission unless authorized by the host.

Speaker: Speakers can share presentations, specific applications, or the entire desktop.

Interpreter: The interpreter is responsible for translating the language spoken by the speaker into the interpretation language specified by the host in a separate audio channel of the simultaneous interpretation feature. The host may assign interpreters when scheduling a meeting or during the meeting.

Guest (webinar only): Guests typically serve as subject matter experts during webinar sessions, giving presentations and lectures, viewing and answering attendee questions during Q&A sessions, and other activities; hosts can designate participants as guests when scheduling a meeting or during the meeting.

Audience (webinar only): Audience usually only supports receiving audio, video, and shared data from the speaker in a webinar and needs permission from the host/co-host before they can speak.

Enterprise Administrator: This role is granted authority to manage enterprise accounts and enforce global and per-user policies. The administrator can also

select the specific Yealink Meeting features that are available to users. The administrator can control all meeting permissions under the enterprise, and can force certain meeting configurations. For non-mandatory meeting configuration, the host can set and change.

Meeting Setup

Waiting room

The host can enable the waiting room when scheduling a meeting or during the meeting. If enabled, attendees cannot join the meeting directly unless the host allows them to join the meeting. Users in waiting room are divided into three categories:

1. Authenticated users within the enterprise
2. Authenticated users outside the enterprise
3. Unauthenticated users

In the waiting room, the host can set which types of users can skip the waiting room to join the meeting:

1. Members in the enterprise
2. Users invited by the host
3. Users invited by attendees

For users in the waiting room, the host can enable automatic entry for the entire meeting duration to prevent the need for the host to manually manage access when users repeatedly join or leave the meeting.

Meeting password

When scheduling a meeting, the organizer can set a meeting password, preventing unauthorized users from accessing the meeting at will.

Only signed-in users can join meetings

If you enable this feature when scheduling a meeting, it can effectively identify participants and prevent unauthenticated users from joining the meeting directly.

Meeting allowlist

If you enable this feature when scheduling a meeting, only invitees and users in the allowlist are allowed to join the meeting. Allowlist settings include: allowing all users in the enterprise, allowing one/multiple enterprise members, and allowing one/multiple user accounts.

Lock meetings

During a meeting, no one is allowed to join the meeting after the host locks the meeting. This feature is suitable for preventing unauthorized users from joining a confidential meeting after all attendees have joined the meeting.

Add password to the meeting link

Attendees can join the meeting through the meeting link shared by the host. This configuration controls whether attendees who get the meeting link are allowed to join the meeting directly through the link.

Meeting watermark

If you enable this feature when scheduling a meeting or during a meeting, the meeting watermarking feature prevents the content during the meeting from being forwarded by random screenshots. Note that this feature is enabled only when **Only signed-in users can join meetings** is enabled.

Allow participants to join before host

If you enable this feature when scheduling a meeting or during a meeting, participants can join a meeting even if the host has not yet joined.

Participant permission management

During the meeting, the host can manage the participant's speaking permission, sharing permission, annotation permission, video permission, recording permission, chat permission, chat log export permission, renaming permission, and other permission.

Remove participants from a meeting

If an unauthorized participant joins the meeting, the host can remove the participant from the meeting and prohibit the participant from rejoining.

One-click to enable security configuration

Yealink Meeting supports providing quick and secure configuration options for specific collaboration scenarios to help hosts quickly set up security features. These options include pausing all activities of participants, private meeting mode, and training/lecture mode.

Identification

User accounts need to authenticate with their user credentials (ID and password) to the Yealink Meeting web portal to start a meeting. The authentication process of Yealink Meeting client or WeChat applet uses a unique token per client, per session to confirm the identity of each participant attempting to attend the session. Each session has a unique set of session parameters generated by the Yealink Meeting. Each authenticated participant must have access to these

session parameters and the unique session token in order to successfully join the meeting.

The authentication method includes account credential login or single sign-on based on OAuth 2.0. Enterprise administrators can enable two-factor authentication (2FA) as an additional security item for logins for enterprise users who authenticate using an account and password.

Application Security

Yealink Meeting client strictly checks the running environment, including root detection, jailbreak detection, debugging detection, injection monitoring, etc., to ensure that the client runs in a trusted environment and to prevent the program from being cracked or exploited by malware.

We also have a dedicated team that performs security assessments and vulnerability checks on Android, iOS, Windows and macOS clients. We also employ third-party components (libraries, SDKs) to find as many vulnerabilities in the application as possible to ensure client security.

Other Security Features

Hybrid Cloud

Yealink Meeting supports a hybrid cloud deployment solution, allowing customers to deploy Yealink Meeting media server, recording server, and gateway server in their internal network. The meeting media data itself is streamed on the internal network, the recording files are stored on the customer's server, and non-sensitive user data will be hosted on the cloud (Microsoft Azure data center) for management.

There are currently three ways to communicate with the sink service and the service on the cloud, and the security assurance methods of the three ways are described as follows:

1. The sink service communicates with the hybrid cloud connector, the communication is secured by TLS protocol and carrying the authentication of hybrid cloud credentials issued on the cloud to .
2. When the sink service communicates with the service on the cloud, the communication is secured by TLS protocol and carrying the developer credentials issued by the cloud.
3. The communication between the sink service and the media is authenticated using developer credentials provided by the cloud. Additionally, an accelerated private network is available for secure media

streaming. However, when all terminals are within the enterprise intranet, the media streams remain within the internal network and do not traverse the external network.

Webinars

Yealink Meeting webinar supports up to 5,000 participants to join the conference at the same time, distinguishing between broadcasters and interactive parties. Broadcasters can share video, audio and screen during the conference, and interactive parties are able to view the video, audio and screen sharing shared by broadcasters. The webinar allows the host the enable the webcast feature and stream the meeting to third-party live platforms to realize an unlimited number of audience. Use AES to protect webinar content and screen sharing in the Yealink meeting client, and use the RTMPS (TLS) encryption standard when third-party services also support the standard.

The webinar supports attendee registration. The guest invitation will be sent separately from the audience invitation.

Webinars with registration

- Manual registration approval: The webinar host will manually approve or deny whether the registrants receive information to join the webinar.
- Auto-approved registration: All registrants for the webinar will automatically receive information on how to join the webinar.

Webinars without registration

- Participants can join the webinar directly with the meeting ID and password. After the webinar is over, participants will not be able to join the webinar using the same information.

Rooms

Yealink Meeting Rooms is Yealink Meeting's software-based meeting room system. It features video and audio conferencing, wireless content sharing, and an integrated calendar running on off-the-shelf hardware. Communications are established using TLS encryption, and meetings, webinars and message content are encrypted using AES.

Yealink Meeting Rooms provides multiple options for logging into the meeting room account, including the administrator account password, cloud account and password, and activation code. Additionally, it offers the option to use a meeting room management password for locking the Rooms application. This feature ensures the security of your Rooms application by preventing unauthorized individuals from making changes to the application and its settings.

Chat during a Meeting

Yealink Meeting supports private chat or group chat in a meeting, and the host can control whether to allow participants to have chat permission. These chat messages, including text, images, files, etc., are encrypted using TLS. Meeting chat encryption uses secure communication so that only the intended message recipient can read the secure message.

Open API/SDK

Yealink Meeting opens API to provide third-party developers with a secure portal to use Yealink Meeting services. Through Yealink APIs, developers can use Yealink Meeting features, such as enterprise member management, meeting management, and meeting control. Yealink API is a REST-like API based on HTTP. The REST-like style utilizes URLs to represent resources and interacts with the API through the HTTP protocol. API relies on the semantics and methods of HTTP. To ensure the security of API usage, the transport protocol uniformly uses HTTPS, and all requests require authentication. If you use Yealink API without providing the correct credentials, the request will be denied.

We provide the download of the Yealink Meeting Client SDK, but users of the Client SDK are required to undergo authentication. This helps to filter out requests initiated by anonymous traffic and identify whether the SDK requester has the necessary permissions to use the relevant APIs or SDKs.

Compliance and Certification

GDPR

Yealink Meeting has passed the assessment of the EU General Data Protection Regulation (GDPR), which means that Yealink Meeting products and services provide strict protection measures for users' data and privacy aspects.

ISO27001 Information Security Management System

It has been considered as the most authoritative and strictest information security system certification standard in the world and is accepted worldwide. Yealink's certification of data center, management system, R&D, and functional departments demonstrates our alignment with international standards in information security management. We possess robust capabilities in identifying and controlling information security risks, ensuring the delivery of safe and reliable services to our global customers.

ISO9001 Quality Management System

It is the most mature quality system framework in the international arena. The certification signifies that Yealink has implemented a quality management system in line with the seven principles of ISO9001. We have achieved international standards in R&D, operations, maintenance, and customer support services. This ensures our ability to consistently deliver qualified products that meet customer expectations and satisfaction continuously and stably.