logitech

LOGITECH VIDEO COLLABORATION SECURITY & PRIVACY

INTRODUCTION

The frequency and sophistication of cyberattacks are accelerating globally, presenting significant risks to organizations in a hybrid workplace that is becoming more distributed and virtualized by the day.

Todays' cybercrimes can come from anywhere at any time, with hackers exploiting vulnerabilities in both software and hardware, such as cameras, headsets, and other devices.

In this whitepaper, we share our approach to security and privacy for devices running on CollabOS. Currently, these devices include Rally Bar, Rally Bar Mini, RoomMate, Tap Scheduler, and Tap IP.

WHAT IS COLLABOS?

CollabOS is the unifying operating system running on select Logitech video collaboration devices. With CollabOS, these devices work seamlessly together, continuously improve, and are easier than ever to deploy and manage, helping you deliver high-quality, equitable meeting experiences for everyone.

CollabOS further simplifies video conferencing deployment and management by integrating Logitech hardware and third-party applications and scheduling services, such as Microsoft Teams, Zoom, and Robin.

CollabOS continuously improves the user experience for video meeting participants while also extending the life of your VC investment. Firmware updates with new features, enhancements, and security safeguards are automatically shipped to your devices over the air, at no cost to you.

DEVICES POWERED BY COLLABOS

- **Rally Bar** and **Rally Bar Mini** are Logitech's premier all-in-one video bars for large, medium, and small meeting rooms, with a unique optical camera, simultaneous two-way audio, and a secondary dedicated AI camera. Both can be deployed in USB or appliance mode, with exceptional flexibility and ease.

  Learn more about Rally Bar and Rally Bar Mini

- **RoomMate** is a video conferencing appliance for supported conference cameras and peripherals, including Rally System, MeetUp, and third-party audio. It allows you to easily deploy Microsoft Teams® Rooms on Android, Zoom Rooms Appliances, and other leading video conferencing services.

  Learn more about RoomMate

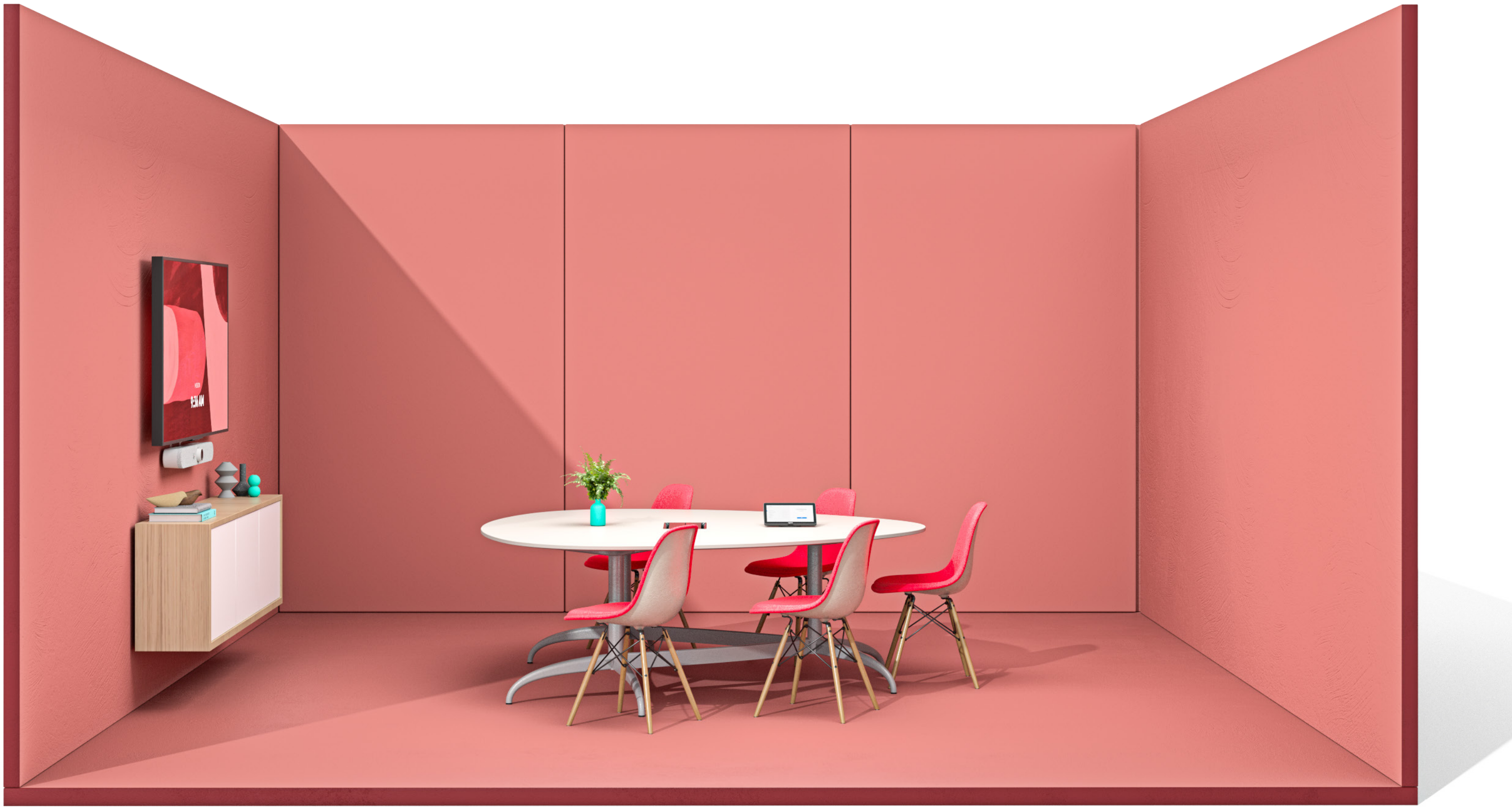
- **Tap IP** is a network-connected touch controller that makes video meetings simple to join across different platforms and applications. With a spacious 10.1" display, low profile, and motion sensor for always-on readiness, Tap IP provides easy content-sharing and a consistent meeting experience across all rooms.

  Learn more about Tap IP

- **Tap Scheduler** is a purpose-built scheduling panel for meeting rooms that enhances the in-office experience. Tap Scheduler makes it easy to see meeting details and reserve a room for ad hoc or future meetings, with colored LED lights showing availability at a distance to help employees quickly find an open room.

  Learn more about Tap Scheduler

SECURITY & PRIVACY



Security and privacy are critical aspects of the design of all Logitech VC products. CollabOS runs on Android 10, which provides best-in-class security, privacy, and performance.

Logitech products are developed using a secure development lifecycle that follows industry best practices during product design, development, and fielding. We meet and exceed security expectations by building in security from the earliest design phases.

This includes a product design review by a Security Review Board composed of security experts from across the organization. We rigorously verify the security of systems and software during development and testing. And we follow STRIDE, the industry standard for classifying security threats.

Note: Unless otherwise indicated, the security and privacy features described in this whitepaper apply to all five devices listed above, which are referred to throughout the paper as " CollabOS devices."

INFORMATION SECURITY

SECURE DEVELOPMENT LIFECYCLE (SDLC)

Security review gates are implemented at each stage of system development for Logitech's SDLC for CollabOS devices, including design, implementation, and release. During the design phase, all design documents are reviewed by internal and external experts in security.

Both automated and human reviews of the code produced by the development team are conducted during the implementation phase. Static analysis is performed on all source code, with any resulting issues flagged and reviewed by the development team and security specialists.

All software development for CollabOS devices follows industry standards, including but not limited to the following:

- Android Secure Coding Standard
- SEI CERT Oracle Coding Standard for Java
- SEI CERT C Coding Standard
- SEI CERT C++ Coding Standard

Before software is released, it is run through a thorough set of tests for both functionality and security. System updates and new releases also follow the SDLC, and software in the field is maintained and updated with any necessary security patches for issues discovered between major releases.

SECURITY AND PRIVACY BY DESIGN

Security and privacy are designed into CollabOS devices from the start of product development through implementation, release, and updates.

Here is a non-exhaustive list of the steps we take to strengthen the security of these devices:

- **Starting with a strong foundation:** As a baseline, the platform is based on Android 10, which includes enhanced security and stability.
- **Avoiding universal default passwords:** Logitech CollabOS devices follow industry best practices and California state law in never having a universal default password. The devices have no default password.
- **Keeping software updated:** "Over the air" firmware updates are used to keep CollabOS devices constantly up to date with the latest release.
- **Maintaining software integrity:** All software images are digitally signed during production and distributed over secure communication links. CollabOS devices verify the signature of each software image before installing or upgrading the software, thereby maintaining its integrity and authenticity.
- **Communicating securely:** Beginning with CollabOS version 1.7, all communications between CollabOS devices and the cloud use Transport Level Security (TLS) version 1.2 and 1.3. TLS 1.1 and 1.0 are disabled on CollabOS devices, and will no longer show up in security scans. Applications running on the platform may use similar or additional forms of communication. We advise you to check with app service providers regarding their security protocols.
- **Protecting personal data:** While CollabOS devices do not contain or store personally identifiable information on the device, video service providers may store Personally Identifiable Information (PII) within their apps. We advise you to check with service providers regarding their PII policy.

INFORMATION SECURITY

DEVICE APPLICATION SECURITY

CollabOS devices contain several applications that are used in day-to-day operation. Securing the device requires that Logitech carefully manages the applications that reside on the device.

Through the process of application whitelisting, we can control exactly which applications are allowed to be utilized. As part of securing the software before it is shipped, we also remove or disable non-essential apps, services, and device drivers, thereby reducing the attack surface. All CollabOS devices utilize the built-in SELinux Policies, a component of the Android system.

ANTI-ROLLBACK FEATURE

The CollabOS-supported devices have a feature that prevents an updated system from being reverted to an earlier, and possibly less secure, set of software.

HARDWARE SECURITY

All CollabOS-supported devices are equipped with several features that enhance the security of the device. A trust enclave is used to protect any required secrets or keys on the device. The hardware utilizes secure boot to verify the validity of boot software and system firmware, which were signed during production.

SECURITY VALIDATION

Internal quality assurance processes use software component security test suites to check each software release for security vulnerabilities. Software cannot be released until it clears the test suite gate.

FIREWALL RULES - PORT FILTERING/ BLOCKING

All CollabOS-supported devices implement their own firewall rules to affect port filtering and blocking, thereby reducing the attack surface which is exposed to the network.

EXTERNAL DEVICE INDICATORS FOR RECORDING AND PRIVACY

All CollabOS recording devices, including microphones and cameras, have clear indicators for when they are in use. Rally Bar and Rally Bar Mini are shipped with lens caps for the conference cameras.

Note: This feature does not apply to Tap IP, Tap Scheduler,or RoomMate which do not have cameras or mics and are not capable of recording video or sound.

APPLICATION SANDBOXING

Applications are prevented from interfering with each other on the platform via built-in application sandboxing. Each application and its data is given its own space in which to work and is restricted from communicating or interfering with the execution of other applications, including the ability to read and write data, which is kept in the per application sandbox.

SECURING DATA - ENCRYPTED STORAGE

Hardware-level encrypted storage is used to store all data on CollabOS-supported devices.

BACKEND DATA SECURITY

Communication between CollabOS-supported devices and Logitech backend systems that support them, including over the air updates, are carried out over encrypted channels using Transport Layer Security (TLS). This provides both an encryption of data in transit and authentication of the system with which the device is communicating.

We leverage Amazon's Internet of Things (IoT) framework and infrastructure to enable secure communication between the device and the backend, as well as securing data at rest in the cloud.

VULNERABILITY AND RISK MANAGEMENT

We actively monitor the security of our products and provide timely updates to address any known vulnerabilities.

INCIDENT RESPONSE

Logitech welcomes customers and security researchers to report issues found in our products so that they may be addressed in the field. We participate in a public bug bounty program by which researchers can help to improve the security of our products by reporting issues they find and receiving credit for their discoveries. Logitech gives appropriate credit to responsible reporters of security incidents that are found to be valid and actionable.

In addition, incidents are recorded and responded to as quickly as possible, and we expect those reporting incidents to follow accepted practices for responsible disclosure.

ADDITIONAL RESOURCES

To learn more about CollabOS-supported devices, including Rally Bar, Rally Bar Mini, RoomMate, Tap IP, and Tap Scheduler, visit logitech.com/vc.

CONTACT

To report a security concern regarding Logitech products, visit logitech.com/security. For other inquiries, visit logitech.com/contact.

logitech

Logitech Inc.
7700 Gateway Blvd.
Newark, CA 94560
Published November 2022

This whitepaper is provided for informational purposes only. Logitech makes no warranties, express or implied or statutory as to the information in this whitepaper. This whitepaper is provided "as is" and may be updated by Logitech from time to time.