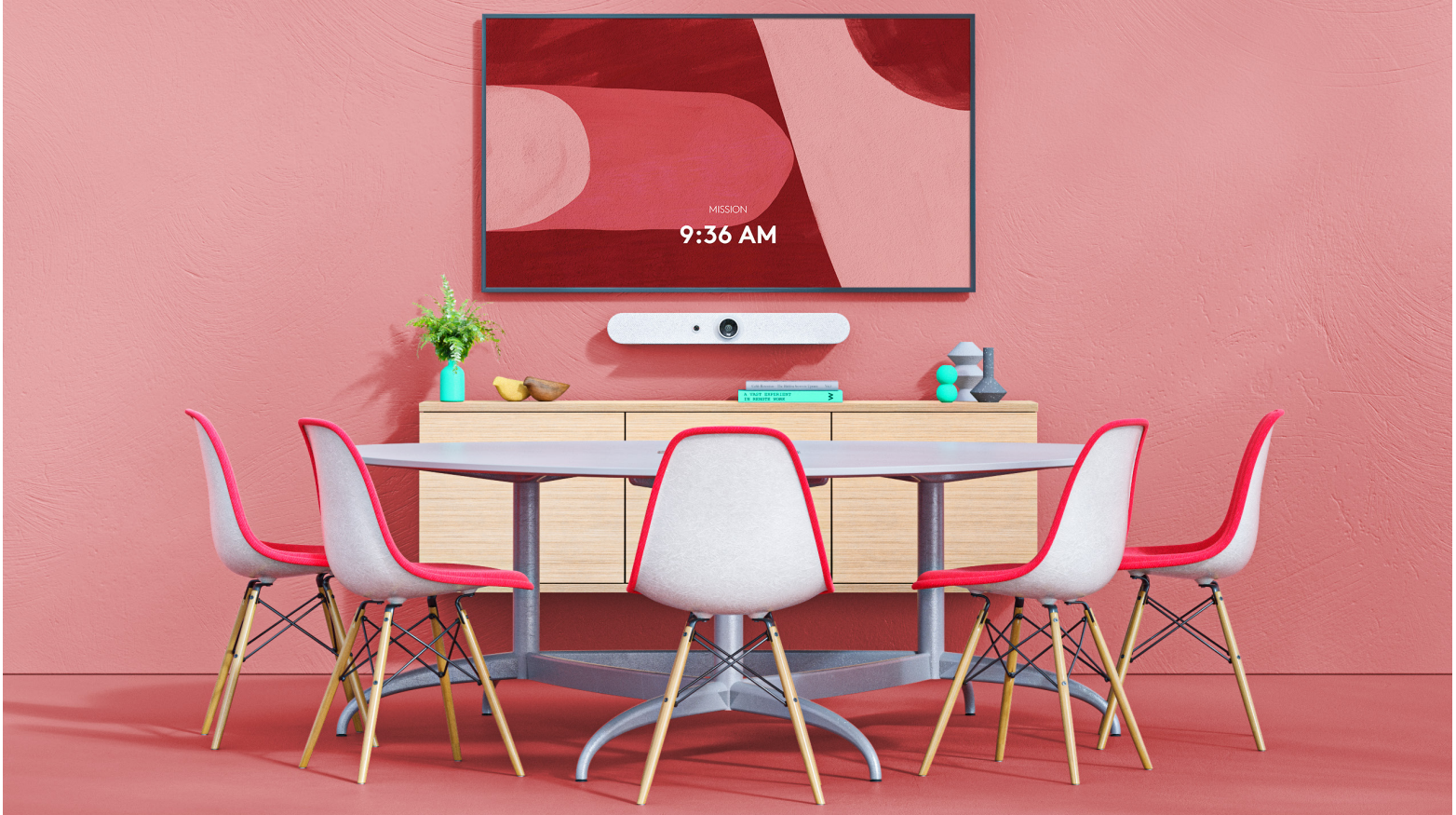
logitech

SECURITY & PRIVACY IN LOGITECH VIDEO COLLABORATION DEVICES

RALLY BAR, RALLY BAR MINI, AND ROOMMATE



INTRODUCTION

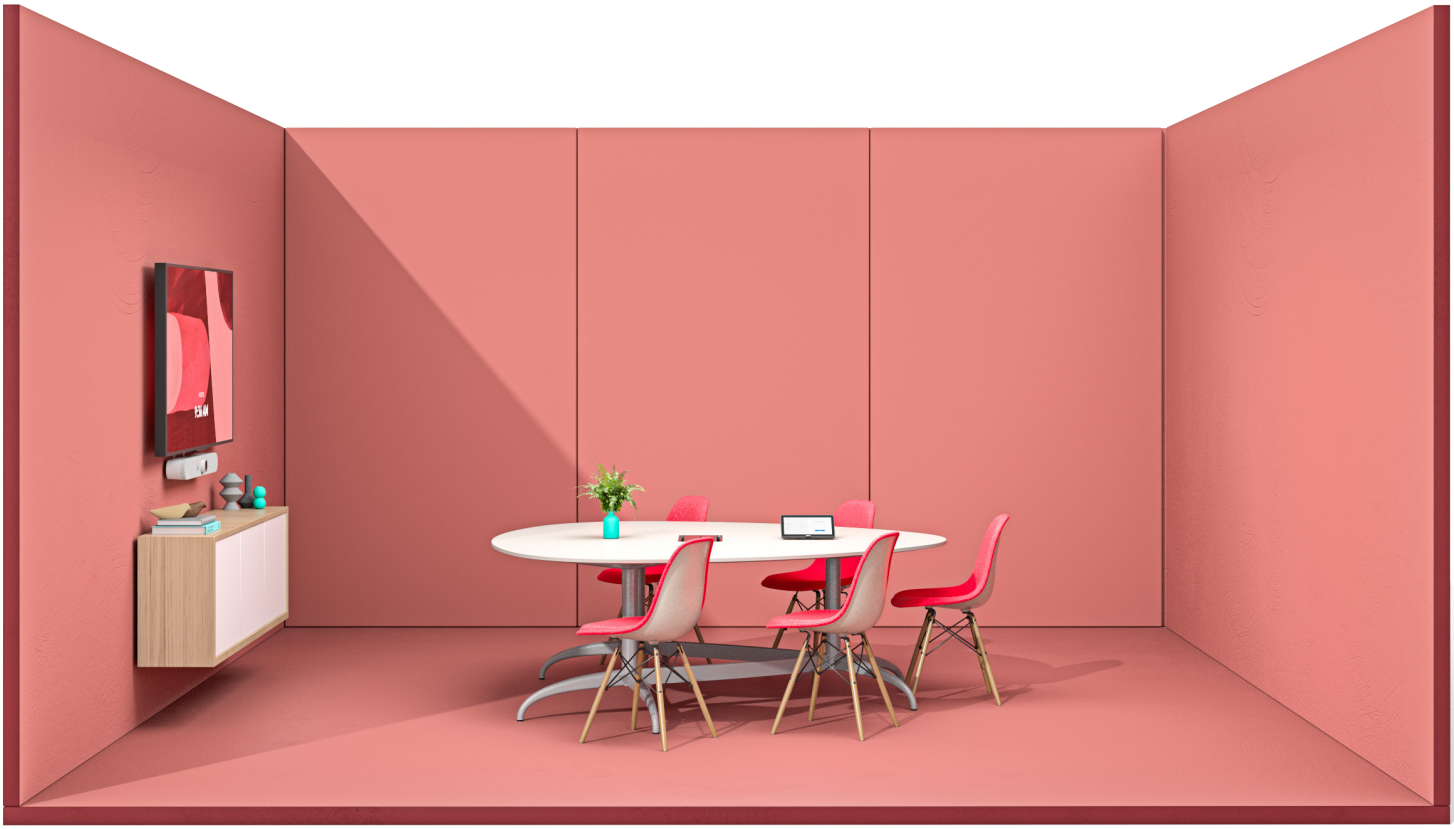
The following whitepaper describes our approach to security and privacy for Logitech® Rally Bar, Logitech Rally Bar Mini, and Logitech RoomMate.

Logitech, a world leader in products that connect people to the digital experiences they care about, offers a range of collaboration tools that are easy to use with virtually any application almost anywhere.

Rally Bar and Rally Bar Mini are Logitech's premier all-in-one video bars for medium and small meeting rooms. With brilliant optics, powerful audio, and AI-driven performance, these conference cameras set a new standard for video collaboration. Both can be deployed at scale in USB or appliance mode, with exceptional flexibility and ease.

With Rally Bar, Rally Bar Mini, and RoomMate, security and privacy are critical aspects of product design. They are all based on Android 10, which provides best-in-class security, privacy, and performance. In these areas, Android 10 is a significant improvement over previous versions of the Android operating system.

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



INFORMATION SECURITY

SECURE DEVELOPMENT LIFECYCLE (SDLC)

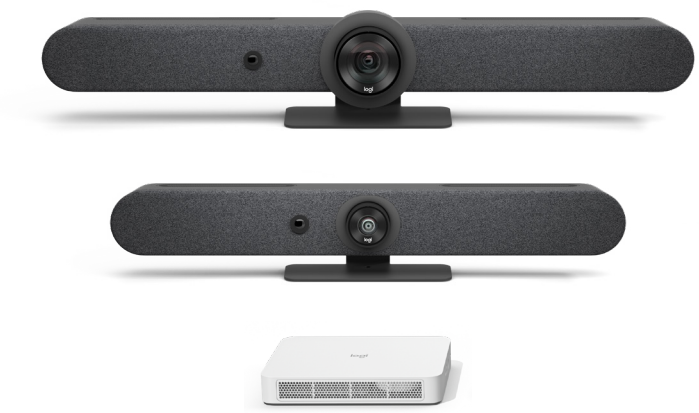
Rally Bar, Rally Bar Mini, and RoomMate were developed following best practices for a secure development lifecycle. The SDLC has security review gates at each stage of system development – design, implementation, and release. During the design phase all design documents are reviewed by internal and external experts in security.

The implementation phase has both automated and human reviews of the code produced by the development team. 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 Rally Bar, Rally Bar Mini, and RoomMate 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

Rally Bar, Rally Bar Mini, and RoomMate include security and privacy designed in – from the start of product development through implementation, release, and updates.

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

- **Start with a strong foundation:** As a baseline, the platform is based on Android 10, which includes enhanced security and stability.
- **Avoid universal default passwords:** Rally Bar, Rally Bar Mini, and RoomMate follow industry best practices and California state law in never having a universal default password. The devices have no default password.
- **Keep software updated:** "Over the air" software updates are used to keep the software for Rally Bar, Rally Bar Mini, and RoomMate constantly up to date with the latest release.
- **Maintain software integrity:** All software images are encrypted and digitally signed during production. Rally Bar, Rally Bar Mini and RoomMate verify the signature of each software image before installing or upgrading the software, thereby maintaining its integrity and authenticity.
- **Communicate securely:** All communications between Rally Bar/Rally Bar Mini/RoomMate and the cloud take place using Transport Level Security (TLS). 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.
- **Protect personal data:** While Rally Bar, Rally Bar Mini, and RoomMate 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

Rally Bar, Rally Bar Mini, and RoomMate contain several applications that are used in day-to-day operation. Securing the device requires that Logitech carefully manage 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. Rally Bar and Rally Bar Mini utilize the built-in SELinux Policies, a component of the Android system.

HARDWARE SECURITY

The hardware components of the Rally Bar, Rally Bar Mini, and RoomMate 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. A hardware-based anti-rollback feature is enabled to prevent an updated system from being reverted to an earlier, and possibly less secure, set of software.

Physical security is further enhanced with tamper-evident and resistant covers for the hardware ports.

SECURITY VALIDATION

Internal quality assurance processes utilize 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

Rally Bar, Rally Bar Mini, and RoomMate implement their own firewall rules to effect port filtering and blocking, thereby reducing the attack surface which is exposed to the network.

EXTERNAL DEVICE INDICATORS FOR RECORDING AND PRIVACY

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

APPLICATION SANDBOXING

Applications are prevented from interfering with each other on the platform via the use of 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.

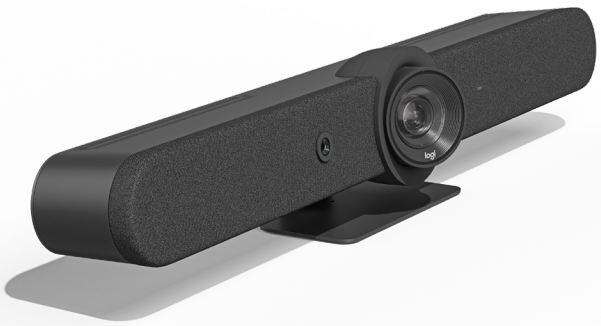
SECURING DATA - ENCRYPTED STORAGE

Hardware-level encrypted storage is used to store all data on Rally Bar, Rally Bar Mini, and RoomMate.

BACKEND DATA SECURITY

Communication between Rally Bar/Rally Bar Mini/ RoomMate and Logitech back end systems that support them, including over the air updates, are carried out over encrypted channels using Transport Layer Security (TLS) which 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 as well as 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 Rally Bar, Rally Bar Mini, and RoomMate, visit our website at logitech.com/vc.

CONTACT

To report a security concern regarding Logitech products, visit logitech.com/security.

For other inquiries, visit logitech.com/contact.

Logitech Inc.
7700 Gateway Blvd.
Newark, CA 94560
Published November 2020