Security

InReality Platform Security

Device:

All communication between the InReality Device Manager solution and InReality's cloud is through an SSL Secure tunnel with authentication. InReality devices uses PCI Compliant Transport Layer Security (TLS) Version 1.2. to provide additional communications privacy and data integrity between applications over the network. TCP ports used are 80 and 443 and Protocols are HTTP and HTTPS. We do not support web proxies or proxies of any type

Platform:

InReality's Platform is deployed on Amazon's Web Services platform and leverages its built-in security features. AWS uses AES 256 Bit encryption for all applications, data storage and communication for distributing resources like Applications and Over-the-Air (OTA) Firmware updates. All data exchanges are via SSL endpoints using HTTPS. Once data is received by the Platform from our sensors, it is our policy to encrypt it as it passes between our internal services, and to encrypt it when it is at rest.

Custom Launcher or Home Screen

- InReality's custom launcher or Home screen only allows whitelisted apps to be shown on the Home screen.
- Users will not be able to access any other apps or files on the device. This provides a level of security from users sideloading other apps or accessing the files on the device.

Operating System/Monitoring

InReality is committed to providing a simple and reliable methodology for keeping its media player family up to date with the latest system patches and security updates. InReality actively monitors the Android and Linux community for security vulnerability alerts.