CTOUCH®
The power to engage

SECURITY: FREQUENTLY ASKED QUESTIONS

Introduction

Security is an especially important theme to CTOUCH and its customers. For important reasons: the number of invisible threats is on the rise, as is the impact of those threats.

CTOUCH recognizes the importance of a proper and secure implementation. CTOUCH stresses that although there are numerous implementations that can be done regarding security within a touchscreen, it is understood that the surrounding setup of the screen solution (like the network or laptops) needs to have an effective security policy as well.

As CTOUCH we noticed several questions about security remained the topic of conversation. With this FAQ we hope to shed more light on these important topics.

Questions

Generally speaking; what does CTOUCH do (by default) to offer a secure solution?

As CTOUCH we set out to create a touchscreen solution that is secure as well as user friendly. This process started with the inhouse creation of a security baseline. A security baseline can be seen as a set of predefined expected (digital) behaviours of a solution. We specified a baseline for touchscreens with an Operating System and touchscreens without an Operating System.

Once a solution passes the baseline test, it is made available to an independent third-party cybersecurity company, which will verify our findings and will actively PEN-test the solution.

To offer an extra layer of security, we offer regular updates in the first years after production, and when a new vulnerability is found that impacts the safety of our users.

How does CTOUCH ensure that the OS on a touchscreen is safe?

All verification of the OS, security and screen workings is done by CTOUCH in The Netherlands in cooperation with independent third-party companies to ensure the most optimal outcome for our users.

What if an OS that is being used by CTOUCH gets declared end-of-life?

As CTOUCH we are dependent on OS manufacturers like Google. Once Google declares a version of its Android end-of-life (EOL for short) support and patching stops. This has been a thorn in our sides for a long time, because in order for our customers to remain secure, they are forced to buy a new touchscreen or to update to a whole new OS if possible. We solved this now with the Heartbeat Safe programme, offering users a secure and always up-to-date Operating System without hassle.

Can it be argued that not connecting a touchscreen to the network is safer then connecting it?

What we commonly see is that any Android device that is connected to the network is considered "hostile" and "unsafe", so they won't be connected. Not connecting it does not make the solution safer though, it only creates an isolated incident.

Wait, not connecting to the network is safer, right? Actually, no. Because you won't get updates this way. Not managing and patching the touchscreen makes the solution unsafe. CTOUCH is always looking to improve the security and the functionality of our solutions, updating and maintaining patch level is of the utmost importance.

So, connection to a network is safe? This cannot be stated as an absolute. It is particularly important to have a critical look at your network setup to determine how safe it is.

The Riva comes with a host of third-party applications. Are these secure and do they uphold to privacy laws and regulations?

In short yes, but the way Android and its apps works it is common to notice "trackers". These trackers track usage and send crash data to its creator. This is fully anonymous, to uphold GDPR law and practices. This is something we cannot remove (for now) due to the standard function of Android and the way apps are being created.

Is there any other data that leaves the screen? Yes, if you activate EShare. The license is checked against the license server of the owner of the application. By-default no other data leaves the solution, unless otherwise configured or new apps are installed.

Do you have more advice around security?

1. Update, update, update!
2. Be sure to upgrade to the latest available OS. If you are a Heartbeat Safe user, you will be provided with an up-to-date OS version for as long as your touchscreen is used.
3. Find out why hackers want to teach schools a lesson, and what you can do to prevent it here.
4. Take a long, hard look at your security configuration. And if you need a hand with that: we offer Heartbeat, a subscription model in which together we can assess the best way to implement your CTOUCH touchscreen with regards to device – and network setup.