OnTime

Powered by ClockedIn

Why Industrial Android Devices Run a Fixed Android Version

Table of Contents

Introduction

IT teams reviewing a purpose built Android terminal will often check the Android version against Google's public support dates for consumer devices and conclude that the equipment is out of date. This note explains why industrial Android hardware, including time and attendance terminals, point of sale terminals, kiosks and handheld scanners, is deliberately locked to a single Android version, and why that version is supported in a different way from a phone or tablet.

Certified as a complete package

Industrial Android hardware is not sold as a general-purpose computer. The device is designed, tested and approved as a complete package, with the hardware, the operating system and the application firmware validated together. In the payment sector this happens under formal standards such as PCI PTS, and the same principle applies to other regulated and safety sensitive devices.

Changing the Android version breaks that package. A new operating system release would invalidate the certification and require the whole device to go back through the approval process, which can take many months and cost a considerable amount of money. For this reason, manufacturers fix the Android version at the point of design and do not move it during the life of the product.

Chipset and driver support

The chipsets used in industrial devices are chosen for cost, availability and long production runs rather than for the latest features. A consumer phone chipset may be superseded within a year. An industrial chipset is expected to remain in production for

five years or more so that the device can be manufactured, repaired and replaced consistently over that period.

Chipset manufacturers typically provide driver and kernel support for only one or two Android releases before moving on. Without that support, the device manufacturer cannot build a newer version of Android for the hardware even if they wanted to. The Android version is therefore tied to the chipset, and the chipset is tied to the production life of the device.

Stability over features

The organisations buying industrial devices value stability above everything else. A retailer or hospital with several hundred terminals in the field needs every one of them to behave in exactly the same way for five to seven years. An operating system upgrade that changes permissions, APIs or the user interface is a risk to their operation rather than a benefit, because it can alter how a tested application behaves without warning.

Fixing the operating system removes that risk. Every device in the estate runs the same known build, the application is tested against that build, and updates are delivered to the application rather than to the operating system underneath it.

Security within a fixed version

A fixed Android version does not mean an unpatched device. Manufacturers provide security patches within the version that the device was designed for, addressing vulnerabilities in the operating system components the device actually uses. This is the same model used for embedded and appliance style equipment across many industries.

The attack surface of an industrial terminal is also much smaller than that of a phone or tablet. The device is locked down to run a single application, with no user access to the operating system, no app store, no browser and no ability to install additional software. Many of the vulnerabilities that drive consumer Android updates relate to features that simply do not exist on a locked down terminal.

A sealed appliance, not a general purpose computer

For all of these reasons, industrial Android devices should be assessed in the same way as any other embedded appliance rather than as a consumer device. The relevant questions are whether the manufacturer provides security patches for the fixed version,

whether the device is locked down to its intended application, whether the supplier supports the hardware for its expected lifecycle, and whether the device communicates securely with the systems it connects to.

The Android version number on its own does not answer any of those questions.

Summary

Certification	Hardware, operating system and firmware are approved together. Changing the Android version invalidates that approval.
Chipset support	Chipset vendors support one or two Android releases. The device manufacturer cannot build a newer version without that support.
Stability	Large estates need identical behaviour for five to seven years. An operating system upgrade is a risk, not a benefit.
Security	Patches are provided within the fixed version. A locked down single application device has a far smaller attack surface than a phone.
Assessment	Judge the device as a sealed appliance: patch commitment, lock down, lifecycle support and secure communication, not the version number.