

GLOBAL HEALTHCARE / UPGRADE ENABLEMENT

THE UPGRADE BLOCKER, SOLVED

A global healthcare fleet of 2,000+ Android devices, stuck on an end-of-support OS since 2022, upgraded in place with zero factory resets.

CLIENT	SECTOR	ENGAGEMENT	SCALE
Global healthcare organisation	Healthcare	Android upgrade enablement	2,000+ devices, multiple countries

THE CHALLENGE

An update path that demanded a factory reset

Since 2022 the organisation had been unable to move its estate from Android 10 to Android 12. The block sat in the OEM's over-the-air update component: every attempt failed unless the device was first factory reset, unworkable across thousands of dispersed devices running critical workflows. A vendor OTA portal existed, but without the rollout control, visibility and process integration the organisation needed. ADB, intent-based and filesystem approaches were each ruled out for a managed fleet at scale, while Android 10 passed end-of-support and patch-lag risk grew.

THE APPROACH

A replacement update component, inside the security model

Working within Android's application trust and signing model, and with the customer's authorisation, I introduced a replacement OTA component deployable through standard enterprise workflows. It drew on OEM configuration already present across the fleet, needed no root access and left the OS image untouched. Instead of the legacy pathway, it delivered update payloads straight to Android's native update engine, enabling reliable in-place upgrades with no reset. It integrated with the existing MDM through Android managed configurations, keeping upgrade scheduling under the customer's control and status tracked device by device on their own dashboards.

THE OUTCOME

In place, and future-proofed

2,000+	Zero	1-week
DEVICES UPGRADED IN PLACE	FACTORY RESETS REQUIRED	SCOPING TO DEPLOYABLE SOLUTION

The fleet is upgrading in place, devices keeping their configuration, enrolled state and application data. Upgrades run through the organisation's own device-management and reporting infrastructure, off single-vendor tooling; the same mechanism carries future Android versions as they arrive, moving the estate off an end-of-support OS and unwinding the risk built up since 2022.

NOTE

Published in anonymised form by agreement; specifics generalised for security and partner sensitivity. Validated 2026.