GAPFRUIT

STRATEGY

Making Devices Trustworthy

A Roadmap for OEMs to meet regulatory and lifecycle requirements to avoid redesign, liability, and recalls.

Overview

For OEMs, regulations and liability expectations require security to be built in from the start. Adding it later often results in costly redesigns or issues that cannot be fixed once devices are already in the field. This is driven by a simple fact: connected devices are rarely touched physically; they are operated remotely. Trust can no longer be assumed; it must be proven - that's Zero-Trust.

The Problem with Implicit Trust

Most connected devices still rely on assumptions: that the device is genuine, the update is unaltered, and the data is correct. These assumptions are exactly where modern attacks strike, exploiting gaps in unverified trust. For OEMs, this creates a significant business risk. A compromised device in the field can trigger product liability, reputational damage, and costly hardware recalls.

Map to achieve trustworthy devices

Building trustworthy devices has become a steep and demanding climb for OEMs. This roadmap breaks the challenge into manageable, logical steps, enabling OEMs to achieve trustworthiness efficiently and without disrupting existing development processes.

1

Authentic – Establish Device Authenticity via Birth Certificate

Do this: Establish a hardware-rooted device identity during manufacturing by issuing TPM-attested and PKI-backed Birth Certificates.
Achieve: Proof of origin and verifiable device authenticity.
Impact: Prevents counterfeit or manipulated devices from entering the field.

2

Trustworthy - Guarantee Software Integrity

Do this: Generate a Software Bill of Materials (SBOM) for every release, cryptographically sign all software artifacts, and apply M-of-N multi-signature approval policies for releases.
Achieve: Verifiable authenticity and integrity from the BSP to applications.
Impact: Enables audit-ready compliance, faster vulnerability response.

3

Resilient - Sustain Trustworthiness by Design

Do this: Adopt a board support package that isolates critical components, enforces least-privilege capabilities, and supports zero-touch deployments with transactional fleet management.
Achieve: Continuous resilience and operational continuity, even under attack or during unexpected system conditions.
Impact: Extends product lifetime, reduces maintenance and support costs, and positions OEMs as reliable partners in regulated and security-critical markets.

Trustworthy devices aren't created at once; they are engineered step by step to form lasting device trustworthiness — the foundation to reduce regulatory and liability risks.