

Let us Act Now, Execute together!

When EOL Silicon Meets the CRA Clock



The Problem

Bay Trail, Apollo Lake & the Compliance Gap

The CRA expects support to outlive end-of-life. Vulnerability handling must run for at least five years from market placement, and for long-life industrial and edge products, typically longer, tied to the expected service life. “Until the chip is EOL” doesn’t satisfy it.

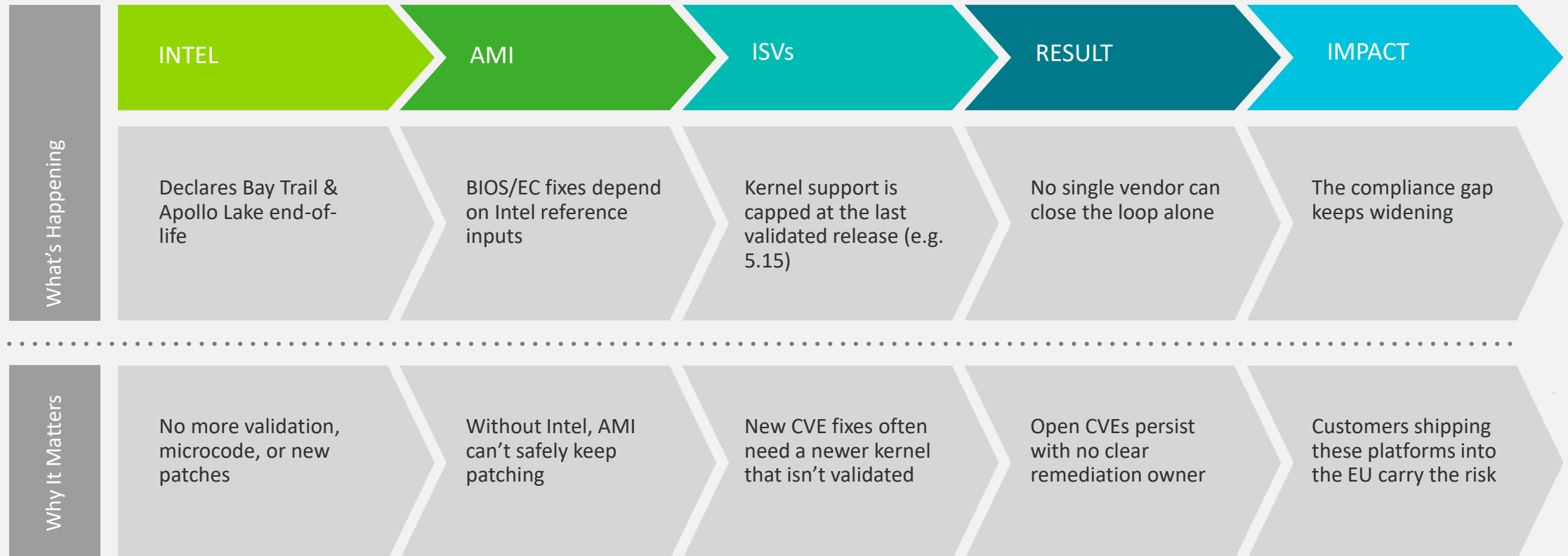
Bay Trail and Apollo Lake are already EOL at Intel. No more validation, no more new microcode, no new fixes from the silicon vendor.

Closing a CVE isn’t one company’s job. It takes Intel (silicon/microcode) + AMI (BIOS/EC) + the OS vendor (kernel) all moving together, and that chain has broken.

The result: a widening, unresolved gap. Customers still shipping on these platforms into the EU have no clean technical path to close it, and no single vendor can close it for them.

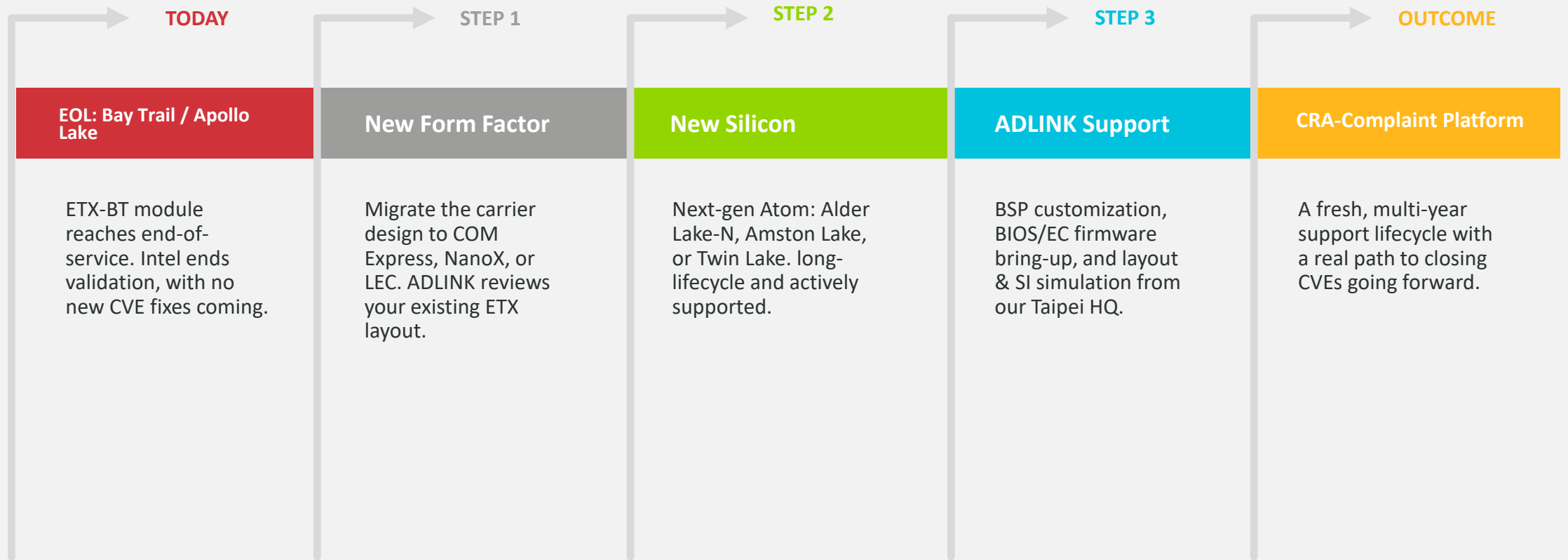
Closing a single CVE on EOL silicon takes three vendors moving together. Today, that chain is broken.

Why There's No Clean Fix



A clear, supported path from yesterday's silicon to a CRA-ready platform.

The Migration Path



Turn This Into Your Next Design Win

Customers still running Bay Trail or Apollo Lake aren't stuck -> they're due for an upgrade. Here's how we make that conversation easy.



Flag It Early

Let existing Bay Trail / Apollo Lake customers know this, With reporting obligations from 11 Sep 2026 and full CRA compliance from 11 Dec 2027, this is a 'when,' not an 'if.'



We Support the Migration

Carrier design review, BSP customization, BIOS/EC firmware bring-up, and layout & SI simulation from our Taipei HQ, with a strong track record.

**STOP STRESSING, LET
GO, AND MOVE ON**

Let's Move Together

We'll join customer visits with you and get samples out fast, so your project moves at speed with ADLINK at your side.