

Protecting Firmware Integrity with FIPS-Validated Crypto

wolfBoot

wolfBoot is a portable secure bootloader that provides firmware authentication and power-failure-safe update mechanisms for Intel-based systems.

Designed with a minimal hardware abstraction layer (HAL), wolfBoot runs independently of any operating system or bare-metal application. Leveraging the wolfCrypt FIPS 140-3-certified cryptographic engine, it verifies firmware signatures during boot, preventing unauthorized code execution and ensuring trusted startup. wolfBoot supports DO-178C certification up to DAL-A, enabling use in safety-critical aerospace and defense systems that require the highest level of software assurance.

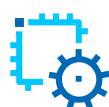
It has been integrated on Intel x86-64 platforms, including the 13th Gen Intel® Core™ i7 processor, delivering flight-grade reliability and security. Its lightweight HAL design simplifies integration with Intel® Firmware Support Package (Intel® FSP), UEFI, and CoreBoot, providing efficient hardware initialization and certifiable assurance.

Supporting rollback protection, secure firmware updates, and post-quantum algorithms (ML-DSA, LMS, XMSS), wolfBoot delivers DO-178C DAL-A-ready security for mission-critical systems built on Intel hardware.



Secure boot and firmware updates for embedded devices

Key Intel-Enabled Features



Secure Firmware Updates



Post-Quantum & Hybrid Crypto



Anti-Rollback Protection



Fail-Safe Updates

Powered by Intel® Core™ processors, wolfBoot delivers:

- Cryptographic acceleration ensures fast and verified firmware delivery
- Hardware-optimized crypto libraries enable future-ready encryption
- Boot-time integrity checks prevent unauthorized firmware downgrades
- System resilience is enhanced by rapid recovery from update failures

Intel Products and Technologies

- [Intel® Core™ Processors](#)

Notices & Disclaimers:

Intel technologies may require enabled hardware, software or service activation. // No product or component can be absolutely secure. // Your costs and results may vary. // AI features may require software purchase, subscription or enablement by a software or platform provider, or may have specific configuration or compatibility requirements. Intel Statement on Product Usage: Intel is committed to respecting human rights and avoiding causing or contributing to adverse impacts on human rights. See Intel's [Global Human Rights Principles](#). Intel's products and software are intended only to be used in applications that do not cause or contribute to adverse impacts on human rights. © Intel Corporation, Intel, the Intel logo, Intel Core, and other Intel marks are trademarks of Intel Corporation or its subsidiaries. Other names and brands may be claimed as property of others.

Ordering Guidance:

- [Buy wolfBoot](#)

Country/Geo: Worldwide

Verticals: Avionics, Automation, Defense, Aerospace, Embedded and Industrial

Use Cases: Safety Certifications, Mission Critical Deployments, Cybersecurity, Encryption, Secure Boot, Transport Protocols

Learn more:

- [wolfBoot Solution](#)