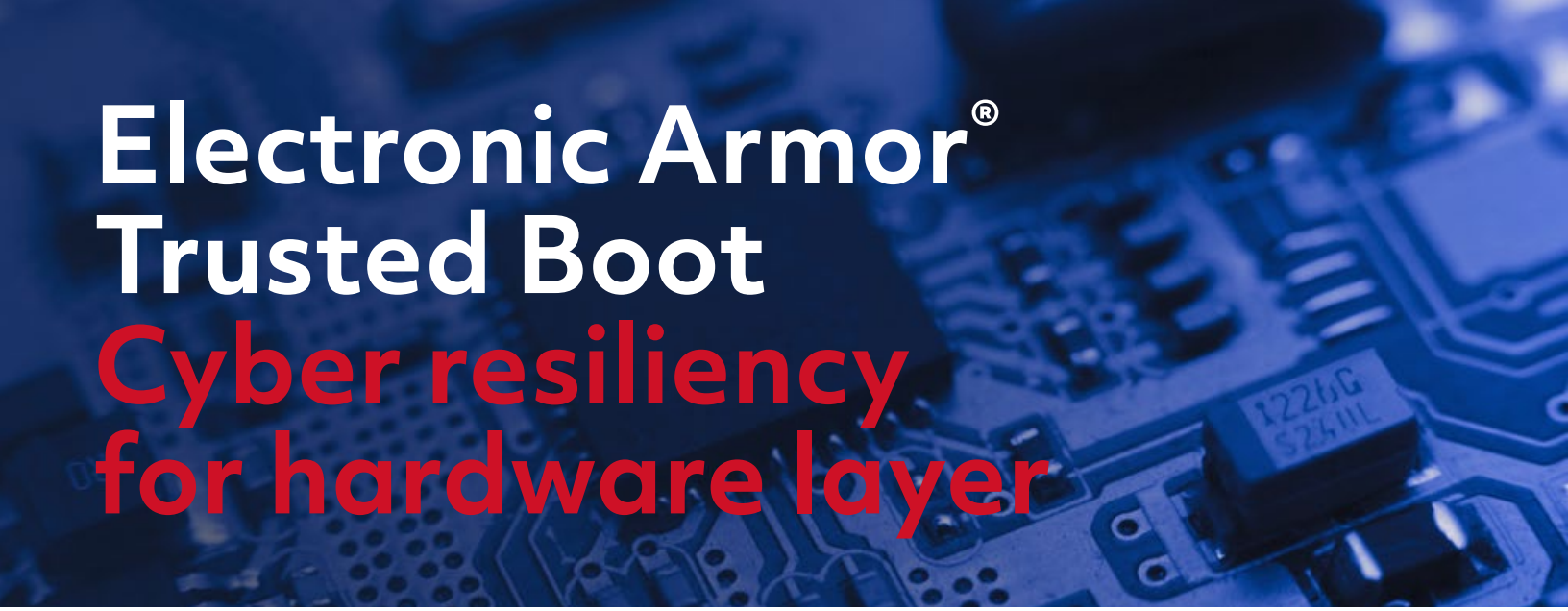

Electronic Armor® Trusted Boot

Cyber resiliency for hardware layer

As threats against U.S. military systems continue to grow in scope and sophistication, many government programs and prime contractors have recognized the need for significantly stronger security mechanisms to protect critical defense technologies against boot-level and runtime attacks.

We need total firmware protection

These systems are increasingly software dependent, making them a desirable target for adversaries to exploit. They also present inherently unique cyber-protection challenges because of their often remote deployments and detachments from managed networks making detection, adaptation and response to evolving cyber threats difficult. Many of these systems utilize commercial off-the-shelf processors (COTS) and equipment, which hackers can easily exploit, or legacy systems, which are also highly vulnerable to bad actors. Stronger security mechanisms are needed to protect our critical defense systems and ensure they continue to operate as designed in cyber-contested environments.

To help solve this issue, Raytheon Technologies Electronic Armor Trusted Boot (EA-TB) offers an integral solution for cyber resiliency and technology protection.

The EA Trusted Boot Solution

EA-TB is a hardware-based foundation for ensuring secure boot and runtime integrity for commercial off-the-shelf (COTS) processors such as Intel-, ARM- and PowerPC-based systems. EA-TB defends against boot-level attacks and kernel/application modification, and protects against attackers gaining persistence on a system. It can also be deployed with Electronic Armor Operating System (EA-OS). When combined with EA-OS, it provides a comprehensive hardware and software solution that enables U.S. defense programs to meet Department of Defense (DoD) program protection and cybersecurity requirements.

KEY CAPABILITIES

- Defensive hardware-based platform providing root of trust, attestation and monitoring
- Enforces secure boot and measured boot from power on to application load
- Ensures data-at-rest protection
- Provides system-level integrity and protection against boot-level attacks

EVERY SIDE OF CYBER

It complies with TPM 2.0, integrates with third-party Internet Protocol (IP) and has minimal performance impact. EA-TB is portable to multiple hardware root of trust (HRoT), from COTS Field Programmable Gate Arrays (FPGAs) to government off-the-shelf (GOTS) and provides firmware for security enhancements to Unified Extensible Firmware Interface (UEFI) and Trusted Platform Module (TBM). Additionally, EA-TB provides an event detection/ response and logging framework.

This ensures confidentiality and integrity of sensitive software applications and data sets throughout the program life cycle.

How it works

EA-TB includes IP cores and firmware/ software running in a customer-defined hardware root of trust (HRoT) for field-programmable gate arrays (FPGAs) or secure processors. It provides boot level and runtime monitoring, crypto services, and an event and response framework with logging and board-level and system-level binding. It cryptographically measures code loaded and executed during the duration of the boot sequence and validates it against known values before allowing a system to boot up.

EA-TB also provides firmware for security enhancements to Unified Extensible Firmware Interface (UEFI) and Trusted Platform Module (TPM).

Additionally, EA-TB's seamless integration with EA-OS provides an enhanced kernel and application monitoring solution and extends trust through the boot processes so protection starts when the system powers on.

EA-TB can be installed on legacy hardware to beef up resiliency without significant modifications to a customer's security architecture.

Electronic Armor Trusted Boot

Raytheon
Intelligence & Space
1100 Wilson Blvd.
Rosslyn, VA 22209-2249
cyberresiliency@raytheon.com
raytheon.com/cyber/electronicarmor

Raytheon Technologies

www.RTX.com