Boot Shield
Cyber Resiliency for hardware layer

Commercial-off-the-shelf computer components are a vital part of today's modern weapon systems and critical infrastructure, keeping costs down while speeding up the implementation of new technological advancements. But malicious actors can also obtain and exploit those products.

We need total firmware protection

Attackers are learning to compromise these parts because, if successful, they can launch stealthy attacks that bypass traditional cybersecurity solutions. As our defenses evolve in sophistication, hackers are also finding innovative ways to circumvent detection and mitigation by shifting attacks beyond the operating system to lower points in the technology stack. Embedded exploits allow malicious actors to inject malicious code into hardware and firmware before security tools like virus scanners can even boot up.

By modifying components to make changes at the boot level instead of the operating system, attacks can be made with stealth and persistence that can survive complete system reinstalls. The threat could come from anywhere: from the supply chain to nation-state-sponsored advanced persistent threats. This type of attack is also on the rise, as corporate and government systems are targeted and affected by attacks on boot code.

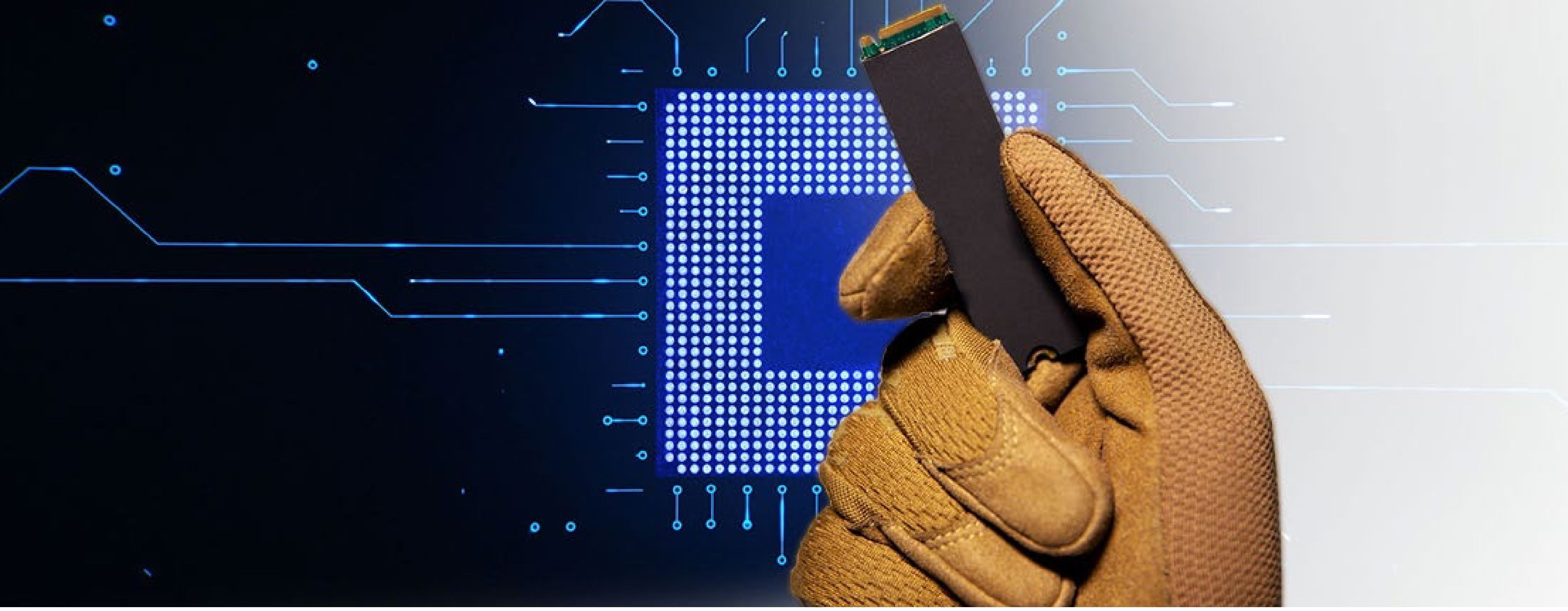
Boot Shield solves this problem by acting as a hardware root of trust and secure boot solution. Providing out-of-band monitoring and protection of desktops, laptops, servers and tablets, this solution blocks attacks from gaining a persistent foothold that could help steal data, access other systems or affect missions or infrastructure.

.

KEY CAPABILITIES

- Provides hardware root of trust, platform attestation and continuous monitoring
- Hardware security extends from Boot Shield card to host processor
- Prevents modern root and boot kit attacks against platform firmware
- Provides integrity verification for system BIOS/UEFI code
- Prevents injection of malicious code into boot sequence

EVERY SIDE OF CYBER



The Boot Shield solution

Boot Shield is a small-form-factor root of trust card that can be installed in desktops, laptops, servers and tablets to ensure integrity of critical system firmware. While cryptographically bound to a host system according to mission needs, the host will not boot without the Boot Shield card's authorization.

Each card has its own microprocessor and uses commercial state-of-the-art security features to initialize in a secure manner. The card also has protections against physical attacks and responds if any tampering to protected elements occurs.

Boot Shield protections cannot be disabled by an administrator or root-level user. Additionally, it provides secure key storage and data protection to extend trust to critical applications and software protection solutions. It provides continuous, runtime monitoring of customer-defined memory elements.

This solution can be procured through Raytheon Technologies' GSA IT Schedule 70 contract #GS-35F-204GA.

How it works

Each card is bound to its host device and prevents loading of an operating system or hypervisor until Boot Shield has validated the current security state of the system. It protects against persistent boot-level attacks that are difficult to detect and eliminate, such as operating system modifications and data exfiltration tools. It also prevents any modification to BIOS settings, system firmware or operating system bootloader code.

After the host's operating system is loaded, Boot Shield further enhances operating system protections products such as Electronic Armor or Countervail by providing out-of-band memory monitoring and key offloading services.

Boot Shield supports a wide array of commercial equipment and is customizable to each customer's needs, providing cost-effective solutions for thwarting boot level attacks against COTS systems. It also provides defenses for legacy systems without replacing Operating System/software running on the existing architecture.

Boot Shield

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

Raytheon Technologies

www.RTX.com