The World Starts on ami®

TEKTAGON™ BFR

Platform Root of Trust Solution

What is Tektagon BFR?

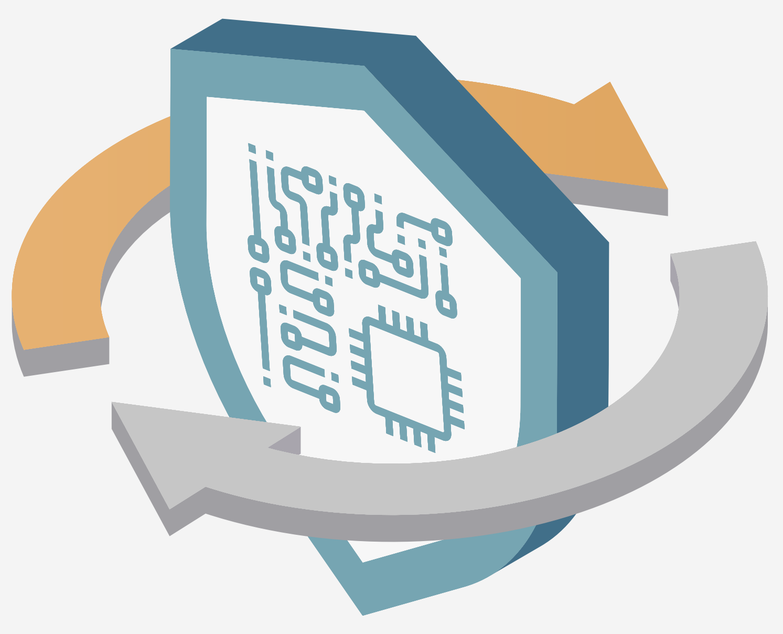
Root of Trust (RoT) is a cryptographic platform security solution used to:
- Validate the boot process
- Ensure the system's firmware is intact
- Attest the system's firmware has not been tampered with

Platform Root of Trust takes it a step further by placing RoT on a physical chip with an immutable boot loader

Tektagon BFR
- Strengthens computing system security
- Protects the BMC and BIOS from booting unauthorized firmware
- NIST® SP 800-193 Compliant - Platform Firmware Resiliency (PFR) Guideline
  - Protect firmware from unauthorized modification
  - Detect unauthorized modification of firmware
  - Recover from unauthorized modification of firmware

Why is AMI developing a security product?
- With 35 years of deep expertise in BMC/BIOS firmware development, firmware security is the next step

Tektagon BFR Features



- **NIST Compliant Security Product**
- **Out of box compatibility:**
  Aptio® V UEFI Firmware
  MegaRAC® SP-X BMC Firmware
  MegaRAC OpenEdition™ BMC Firmware
- **Silicon vendor agnostic, compatibility:**
  Intel®
  AMD®
  Arm®
  RISC-V®
  Other silicon vendors
- **Secure firmware update of recovery image**

How Does Tektagon BFR work?

Is your platform Secure?

It's essential for every platform to be trusted at boot time

- At the office
- At home
- In the field

Platform trust requires validated firmware

- All firmware

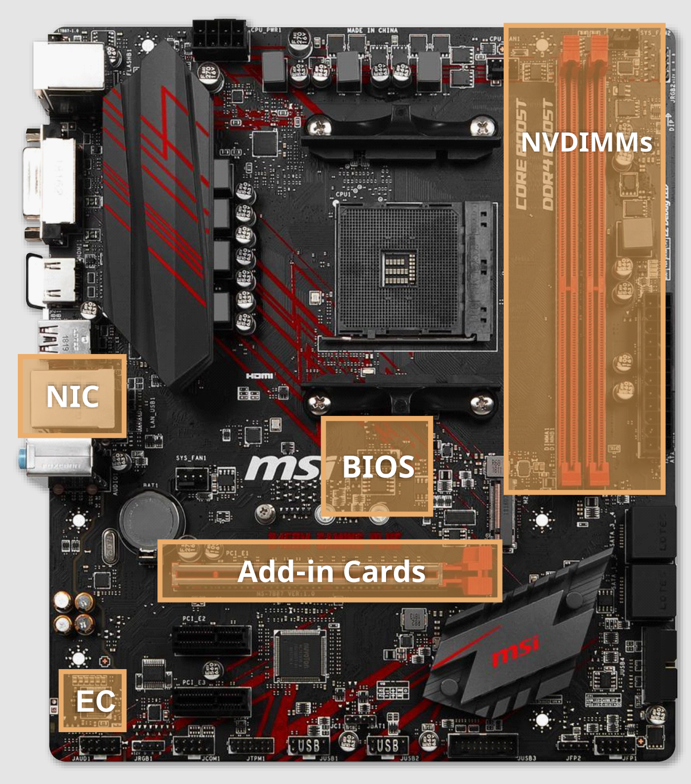
Are you aware of ALL the firmware running on your platform?

- BIOS …

What does Tektagon BFR Secure?

Tektagon BFR validates your BIOS firmware is secure!

Tektagon BFR also secures the rest of your platform firmware!

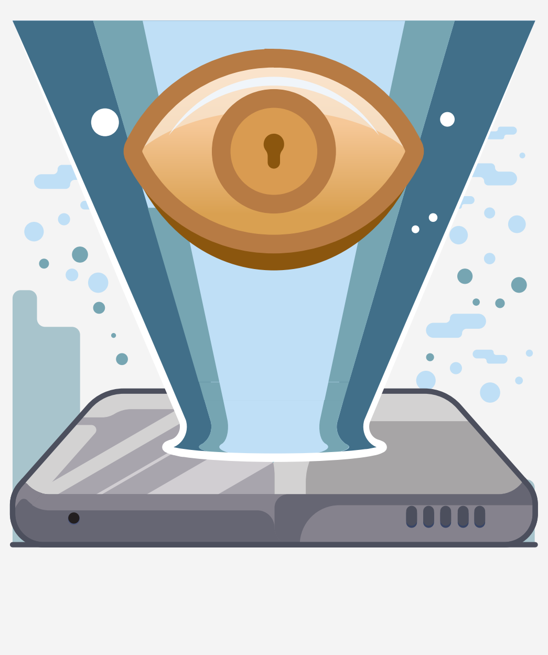


Who does Tektagon BFR benefit?

- **Embedded, Industrial, and IoT device consumers**
  Resilient firmware helps to provide functional safety
- **Client computer consumers**
  More likely to be exposed to network-based exploits
- **Suppliers hoping to reduce platform RMA / field repairs due to firmware issues**
  Tektagon BFR allows forced recovery through physical presence if firmware prevents boot

Why do you need Tektagon BFR?

- **Firmware attacks are becoming more common**
- **Attackers want a persistent foothold on platform**
- **If platform firmware is compromised, the entire platform is compromised**
- **Compromised firmware may be impossible to detect without specialized hardware**
- **NIST compliance may be required for some contracts**



Why do you want Platform Root of Trust from AMI?

- **AMI Security products designed to be automatically integrated with AMI firmware products**
  - Out-of-box compatibility with Aptio V, MegaRAC SP-X and MegaRAC OpenEdition
  - Fast, easy, cost-effective way to secure your platform firmware
- **AMI security product integration provides an entire suite of security tools from the same trusted company**
  - AMI CLEFS signing service support planned in future update
- **Fast, knowledgeable support directly from experienced AMI engineers worldwide**

For more information, visit AMI Sales at ami.com/contact

ami®

w02