TEKTAGON™ XFR

Platform Firmware Resiliency

Ensure Platform Firmware Security with Tektagon™ XFR

Tektagon XFR is a vendor-agnostic hardware security solution that protects computing systems starting at power-on, compatible with all current AMI firmware and in adherence to NIST SP 800-193 Platform Firmware Resiliency (PFR) guidelines. This comprehensive Platform Root of Trust solution is the industry's first PFR product to not only detect and protect against firmware attacks, but also recover and re-provision the firmware, eliminating potential downtime and loss of confidential data, making Tektagon XFR the comprehensive solution for platform privacy and security suitable for all types of any compute system hardware designs, including servers, IoT devices and client systems.

Immutable Hardware-Enabled Protection

Tektagon XFR firmware runs on a secure embedded controller chip that enforces platform boot of authorized firmware. It uses an immutable boot loader to establish the root of trust, allowing for validation of the platform firmware with the cryptographic signature of the image. The public key used by the root of trust is permanently fused into the hardware and cannot be altered, but can be revoked through a secure process. Attacks on the platform firmware are detected by Tektagon XFR and prevent a compromised system from booting with the corrupted firmware.

Highlights:

Protect hardware from malicious attacks with the AMI Platform Root of Trust Architecture on dedicated silicon

- Fully NIST® compliant (SP 800-193) with robust Platform Firmware Resiliency (PFR) framework to protect against unauthorized firmware modification and perform system recovery from firmware attacks

Seamless protection and full compatibility with AMI firmware products:

- Aptio® V UEFI Firmware
- MegaRAC® SP-X BMC Firmware
- MegaRAC OpenEdition™ BMC Firmware

Compatible with Intel®, AMD®, ASPEED®, Arm®, RISC-V® and other silicon vendors

True Platform Root of Trust

According to the NIST SP 800-193 Platform Firmware Resiliency (PFR) guidelines, there are three basic requirements for resilient firmware: the firmware must be protected from tampering, corrupted firmware can be detected, and firmware must be able to be recovered. As a secure hardware solution that meets all of these requirements for firmware security, Tektagon XFR stands out as a true Platform Root of Trust solution.

Aptio® UEFI and MegaRAC® BMC Firmware

Tektagon XFR can be used as a standalone solution or together with AMI Aptio eModules and MegaRAC SP-X technology packs to further enhance system firmware security.

Expandable Solution

Tektagon XFR supports hooks, which allow for OEM customization on top of AMI's solution.

Customizable Implementation

Manage platform policies such as peripheral device rules and recovery options.

Customizable Recovery

Tektagon XFR can force recovery on boot failure, preventing booting from tampered firmware. The recovery image can be stored in a dedicated SPI flash or the same SPI flash protected by SPI flash descriptors. Tektagon XFR provides a secure way to update and validate the recovery image.

For more information please visit the request form at ami.com/contact