The World Starts on ami

TEKTAGON™ XFR

Platform Root of Trust Solution

Firmware attacks are on the rise …

83% of all businesses have experienced a firmware attack in the past two years.

Source: 2020 Security Signals Report commissioned by Microsoft®

- 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 can be impossible to detect without specialized hardware

Root of Trust Must be Trustworthy

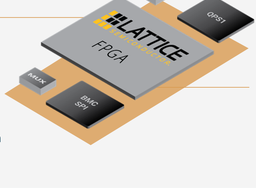
It's essential for every platform to be trusted at boot time

Platform trust requires validated firmware

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

Introducing Tektagon XFR

- Utilizes Lattice® FPGA to provide an independent Platform Root of Trust with maximum flexibility
- Secure firmware update of recovery image
- Configurable modular code
- Flexible run time flash protection

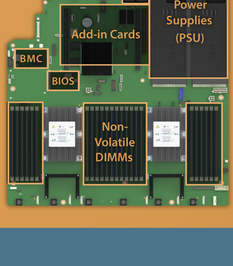


- SPI and runtime filtering
- Compliant to NIST® SP 800-193 PFR Guideline
- Compatible with Intel®, AMD®, ASPEED®, Arm®, RISC-V® and other silicon vendors

What does Tektagon XFR Secure?

BMC and BIOS firmware.

Tektagon XFR can also monitor and secure other firmware accessible by the BMC.



Complete PFR Protection

Protect
Continuously monitors SPI and SMBus and blocks any unauthorized instructions

Detect
Detects attempts to corrupt and compromise the platform firmware

Recover
Restores platform firmware and authenticates the recovery image

- NIST SP 800-193 compliant
- Compatible with most silicon vendors
- Out-of-box compatibility with other AMI products

Unique Value

Maximum flexibility - Minimizes platform ecosystem/vendor lock-in and adaptable to OEM/ODM designs

More secure - Seamlessly integrates firmware security with BIOS and BMC firmware

Faster time to market - Reference design available to OEMs/ODMs to reduce the design cycle

Unparalleled aftersale support - Industry recognized porting and technical support

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

ami