RelianceOne™ Trusted Platform

Measured Boot

RelianceOne™ Trusted Platform is a flexible security architecture for building secure launch solutions. It is a collection of integrated security capabilities – measured boot, firmware independent key management, secure remote updates, and out-of-band runtime protection – that customers can deploy incrementally to match threat levels and budget constraints.

The platform's Measured Boot capabilities provide comprehensive boot integrity verification by measuring every component from power-on through kernel launch. The platform creates a cryptographic chain of trust that detects any unauthorized modifications to firmware, bootloader, kernel, or system configurations. Every boot component is measured and recorded in tamper-resistant Trusted Platform Module (TPM) registers, providing cryptographic proof of system integrity.

MEASURED BOOT DELIVERS

Dual Root of Trust defeats firmware or early boot stage attacks

- Static Root of Trust for Measurement (SRTM) measures firmware and early boot components from the moment you power on.
- Defense-grade Dynamic Root of Trust for Measurement (DRTM) uses Intel TXT to reset the processor into a known-good state immediately before launching the kernel, establishing a clean trust boundary even if earlier boot stages were compromised.

Overcome Unified Extensible Firmware Interface (UEFI) Secure Boot Weaknesses

- Leverages a Trusted Platform Module (TPM) to supplement attestation, removing sole verification burden from boot-time software that must trust itself.
- Protects against Direct Memory Access attacks that UEFI Secure Boot cannot prevent or detect.

Detect Unauthorized Changes to Boot Behavior or System Settings

- Measures bootloader configurations (GRUB settings, boot parameters).
- Measures kernel command-line arguments and loaded configuration files.
- Prevents configuration-based attacks that bypass code verification.

Comprehensive Boot Chain Measurement

- Every boot component is cryptographically measured and recorded in tamper-resistant TPM Platform Configuration Registers (PCRs).
- TPM only unseals secrets when PCR values match expected (sealed) values.
- If measurements don't match, TPM refuses to release keys – system cannot access encrypted data (like an encrypted kernel).

Detect Sophisticated Boot Attacks

- Identifies bootkits, rootkits, and firmware-level malware.
- Prevents unauthorized kernel module loading or parameter changes.
- Blocks attempts to disable security features via configuration tampering.

IDEAL USE CASES

Defense and Intelligence: Tactical edge servers, unmanned systems, Command, Control, Communications, Computers, Cyber, Intelligence, Surveillance, and Reconnaissance (C5ISR) with zero-downtime requirements.

Critical Infrastructure: Industrial control, healthcare, financial systems requiring tamper-evident security.

Any Application Needing: Verifiable boot integrity, detection of firmware/bootkit attacks, defense against sophisticated persistent threats.

TECHNICAL HIGHLIGHTS

Platform: Intel x86 with optionally TXT support | TPM 2.0.

Measured Components: UEFI/BIOS firmware, bootloader (GRUB/systemd-boot), kernel, initramfs, kernel command line, bootloader configuration files.

Trust Mechanisms: SRTM (TPM extends from power-on) | DRTM (Intel TXT with tboot for late launch).

Corporate Headquarters
50 Minuteman Road
Andover, MA 01810 USA
+1 978.967.1401 tel
+1 866.627.6951 tel
+1 978.256.3599 fax

International Headquarters
Mercury International
Avenue Eugène-Lance, 38
PO Box 584
CH-1212 Grand-Lancy 1
Geneva, Switzerland
+41 22 884 5100 tel

Learn more
Visit: mrcy.com/
Contact: mrcy.com/contact-us