DATA SHEET

RelianceOne™ Trusted Platform

Runtime Protection

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.

Runtime Protection provides continuous hardware-enforced protection against kernel-level attacks. Operating independently of the operating system; i.e., out-of-band from the OS kernel, it detects and blocks exploitation attempts in real-time without requiring kernel patches, driver modifications, or OS-specific integration.

A minimal hypervisor design avoids performance degradation – a Rust-based hypervisor operates below the OS to intercept attempts to disable critical CPU security features. Attackers are prevented from clearing memory protections, privilege enforcement, or other hardware security mechanisms.

The minimal design intercepts only security-critical CPU operations, avoiding performance disruptions from hardware interrupt handling.

No OS modification needed - deploy on any Linux® system without patches or recompilation.

RUNTIME PROTECTION DELIVERS

Out-of-Band Protection

- Operates below the operating system in a thin memory-safe Rust hypervisor layer.
- Protects against kernel-level exploits and rootkits, so an attacker cannot disable protections even with kernel privileges.

Blocks Privilege Escalation Techniques

- Detects and denies exploitation attempts in real-time.
- Prevents attackers from disabling memory write protection.
- Blocks attempts to clear supervisor/user memory isolation.
- Stops kernel exploits that disable CPU security features.

Minimal Performance Impact

- Only intercepts security-critical CPU operations, not hardware interrupts, resulting in negligible impact on system performance.

OS-Agnostic Deployment

- No kernel patches or recompilation required.
- Works with any Linux distribution unmodified.
- Transparent to applications and system services.

Real-Time Detection and Logging

- Logs all attempts to disable security features.
- Provides forensic audit trail of exploitation attempts.
- Enables security incident investigation and threat analysis.

IDEAL USE CASES

High-Value Target: Systems likely to face sophisticated kernel exploit attempts.

Zero-Trust Architectures: Defense-in-depth where kernel compromise is assumed possible.

Mission-Critical Systems: Platforms where kernel stability and security are paramount.

Long-Lifecycle Platforms: Systems that cannot be frequently patched but need runtime protection.

Any Application Needing: Protection against kernel exploits, rootkits, and privilege escalation without OS modification.

TECHNICAL HIGHLIGHTS

Implementation: Minimal Rust-based hypervisor (Type-1).

Protection Method: Hardware virtualization to intercept security-critical CPU register modifications.

Monitored Operations: Memory protection controls, privilege separation mechanisms, CPU security features.

Performance: No hardware interrupt interception – minimal performance overhead.

OS Support: Any Linux distribution without kernel modification.

Logging: Real-time audit trail of attempted security feature modifications.

Current Policy: Detect and deny attempts to disable protected features.

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

MADE IN USA