mercury

RelianceOne™ for Linux®

Robust protection for operationally-deployed Linux systems

- Simplify Mandatory Access Control (MAC) policy creation
- Remove unnecessary OS functionality to thwart attackers
- Data protection of data, configuration files, and executables
- Rapidly address cybersecurity requirements with a single product

Designed using a threat model that assumes an attacker will gain administrative (root) access to the system, RelianceOne for Linux maintains the integrity and confidentiality of critical applications, data, and configurations while assuring operations. RelianceOne for Linux is compatible with RedHat and other binary-compatible distributions. It is designed, developed, and maintained by a dedicated team of engineers with more than 40 years of combined Linux and technology protection experience.

SIMPLIFIES MANDATORY ACCESS CONTROL

- Denies by default access to protected entities even from root-level users.
- Controls and restricts direct access to system hardware resources, such as peripherals and storage devices.
- Enables secure software updates.

ENABLES OS HARDENING & ATTACK SURFACE REDUCTION

- Prevents unsigned module loading and enforces keychain controls.
- Limits an attacker's ability to debug or subvert protected applications and their libraries.
- Removes potentially harmful kernel functionality and features.

REMAINS SECURE DURING RUNTIME AND REST

- Authenticates protected entities, verifying that they have not been altered, and only decrypting files as needed (decryption keys are protected and stored out-of-band from attacker).
- Ensures sensitive applications, data files and configuration files are cryptographically bound to a particular deployment hardware, defeating any effort to copy and run applications on non-authentic or instrumental hardware.
- Verifies file signatures on data and configuration files before they can be accessed by a protected application.

HELPS ACHIEVE SECURITY COMPLIANCE

- Works with other Linux Security Modules such as SELinux to address multiple levels of security requirements including confidentiality and integrity of specific applications, libraries, and data stores.
- Enables application allowlisting to enforce static deployments — deployments that cannot be modified at runtime — of mission-critical embedded systems.
- Reduces the impact of many zero-day exploits that would compromise root or administrative functionality of the OS, protecting the system between vulnerability disclosure and patch implementation.

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