RelianceOne™ Secure Boot

RelianceOne Secure Boot provides the strongest level of boot-time authentication/trust on Intel chipsets, while being more flexible in terms of target Linux® distributions and BIOS variants.

RelianceOne starts much the same way that other boot technologies (such as UEFI Secure Boot) do — verifying BIOS firmware; however, the target system is instructed to store measurements of these firmware level components in an off-CPU TPM (Trusted Platform Module). Once the bootloader launches the RelianceOne Secure Boot module, a signed Intel code module is measured and then loaded into the boot process to measure RelianceOne Secure Boot and clear the CPU state. RelianceOne then regains control and authenticates the rest of the boot components and the boot-time command-line arguments.

RELIANCEONE VERIFIES THE AUTHENTICITY OF BOOT-TIME COMPONENTS THROUGH A MEASURED BOOT SEQUENCE BY LEVERAGING A TPM TO SUPPLEMENT ITS ATTESTATION, AND REMOVING THE SOLE VERIFICATION BURDEN FROM BOOT-TIME SOFTWARE THAT MUST TRUST ITSELF.

Because RelianceOne measures the initramfs and command line parameters, an attacker cannot subvert or interpose late-load security components by modifying early boot components within the initramfs or disable important security features (such as intel_iommu=on). With RelianceOne, measurements (stored in the TPM Platform Configuration Registers or PCRs) are combined to unlock non-extractable key material in the TPM. The unlock attempt succeeds only if the sequence of measurements exactly match a prior trusted state's measurements.

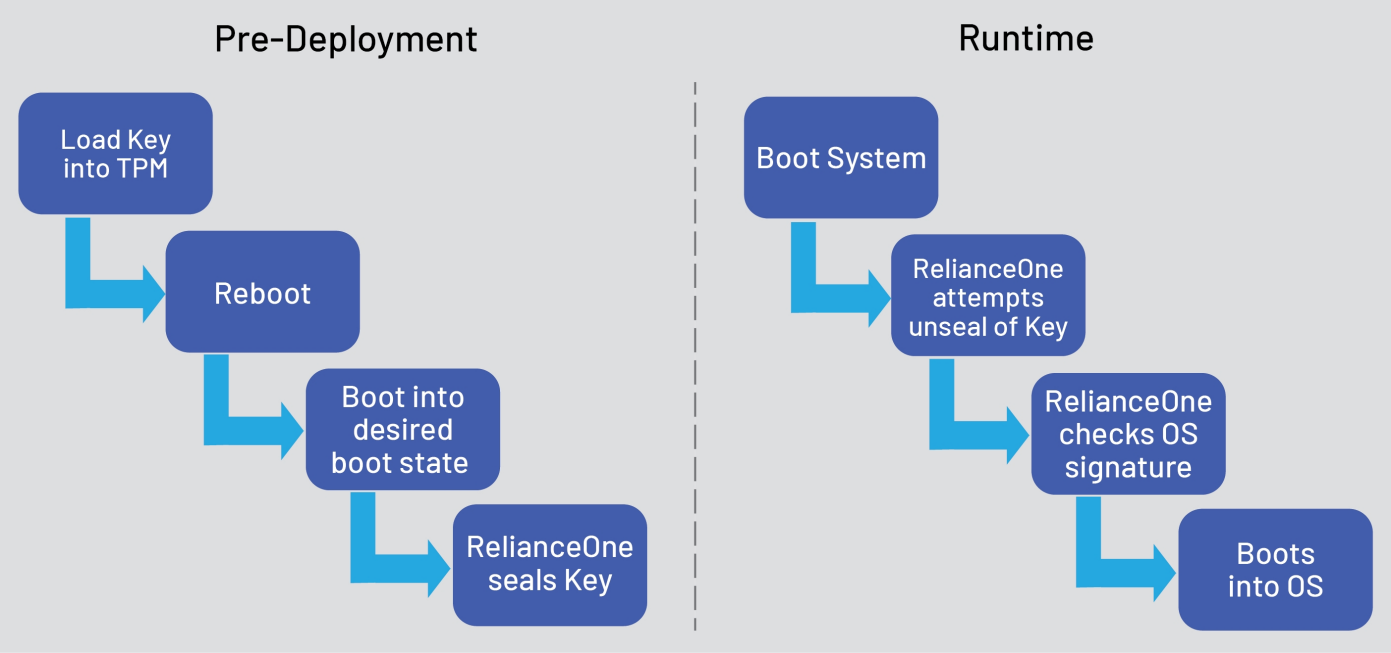
INTEL® SECURE BOOT PROCESS

Since RelianceOne is independent from the kernel or other boot components, it works with most any distribution of Linux including Wind River® Linux®, RedHat® Linux, RedHawk™, CentOS™, and Ubuntu™ on a host using legacy BIOS or UEFI boot.

Using the RelianceOne tooling, the Linux kernel and initramfs are protected and authenticated by customer-controlled key material sealed within the TPM, meaning that they can be updated without reprovisioning the TPM.

RelianceOne and the signed Intel code module only execute in a special state that resets CPU state, protects memory regions from probing, and invokes the IOMMU (Input-Output Memory Management Unit) to protect memory regions even after booting the kernel.

RelianceOne Secure Boot Process



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