Phoenix
SecureCore™

Phoenix SecureCore – The right firmware for x86 computing devices.

Phoenix SecureCore is the latest firmware for x86-based computing devices. SecureCore incorporates UEFI technology, binary compatibility with the Intel Framework and sophisticated endpoint security technology for the next evolution of BIOS.

Continued Industry Leadership at the Core of the Device

With Phoenix SecureCore, Phoenix continues its industry leadership by providing a platform for ensuring that Mobile devices, Embedded systems, Servers and Desktops meet all current and emerging standards and requirements.

SecureCore includes support for the Unified Extensible Firmware Interface (UEFI) specifications. UEFI specifications are part of an industry initiative to define the next generation of computing platform. UEFI ensures an efficient interface between a device's operating system and the platform firmware. In addition to UEFI, SecureCore supports the Framework drivers for Intel® silicon.

SecureCore builds on top of our existing code base. This method provides a smooth transition to new technologies and firmware enhancements while seamlessly supporting backward compatibility and our customer's value add investments in product specific configuration options and customizations.

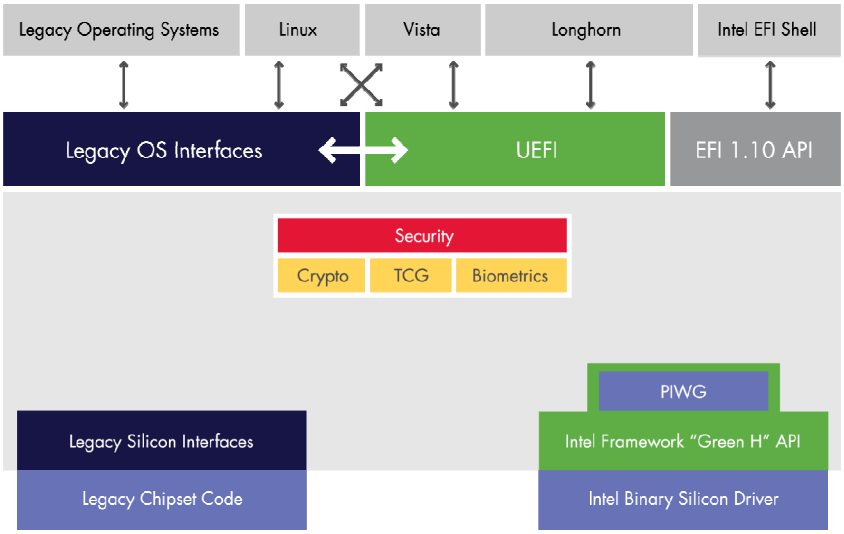
Phoenix SecureCore includes enhanced endpoint security including embedded cryptography, TCG 1.2, integrated biometric and smartcard and support for Microsoft® Bitlocker™ and Flexgo technologies. Everything you need from firmware for Microsoft® Vista™ Premium logo support is included.

Phoenix works closely with all leading silicon vendors to support the latest silicon and technology initiatives including Intel® vPro™ Technology with AMT3.x, VT, TXT and VA, and the AMD Torrenza initiative.

Additional Included Features

- Phoenix Preboot Authentication – Modular architecture from Phoenix for device security that requires a user to authenticate identity before the system boots up.
- Phoenix TCSubscribe™ — An optional add-on to the SecureCore™ platform, provides built-in tamper resistance and other specialized, high-assurance functions for pay-as-you-go and subscription x86 devices.
- UEFI – Phoenix fully supports the Unified Extensible Firmware industry standards. For more information on UEFI go to www.uefi.org

- Phoenix TCSubscribe – software-based secure execution environment, supports secure metering functions and works with all Intel x86 CPUs and chipsets.
- SecureCore Preboot Authentication – Phoenix has created a preboot authentication standard, based on a set of application programming interfaces, that allows for easy integration of third-party two-factor authentication devices, such as biometric fingerprint sensors and smart tokens.
- StrongROM authentication of CSS – Phoenix SecureCore includes the embedded cryptographic engine, StrongROM, which allows authentication of the firmware itself. Starting at the firmware level, SecureCore provides a secure root of trust for operating systems. StrongROM can complement a TPM 1.2 chip in a system to further enhance device security, or provide a level of cryptographic security by itself for systems that do not contain the TPM 1.2 chip



Key Advanced Technologies:

- Intel Framework
  - Montevina
- Intel® vPro™ Technology
  - Intel® AMT
  - Intel® VT
  - Intel® TXT
  - Virtual Appliance (VA)
- UEFI 2.0
  - Windows Server 2008
  - Vista SP1
- WHEA
- Animated 'GIF' Splash
- Phoenix CoreArchitect
  - IDE Visual Studio plug-in
- X64 Source level Debug
- AMD Torrenza
  - Multi-processor, multi-core
  - AMD HyperTransport™
  - IPMI / Remote management

Phoenix Technologies Corporate Headquarters
915 Murphy Ranch Road
Milpitas, CA 95035 USA
408.570.1000 main
408.570.1001 fax