UEFI ADVANTAGES OVER LEGACY MODE

REASONS TO USE UNIFIED EXTENSIBLE FIRMWARE INTERFACE (UEFI) NATIVE MODE

INDUSTRY SPECIFICATION

Device vendors have redefined the interface between the OS and platform firmware. The interface, defined in various UEFI specifications, replaces the older Basic Input/Output System (BIOS). Old BIOS computers need to be replaced, and newer UEFI computers should switch to UEFI native mode for several technical advantages:

Secure Boot

UEFI Secure Boot is an optional setting that enforces signature checking of the boot process. Secure Boot ensures only signed binaries and those matching whitelisted hashes may execute at boot time. Impacts include:

- Malware protection for the pre-boot environment
- Insider threat countermeasures to limit approved boot media and peripherals
- Supply chain risk mitigation through customized key hierarchy

Secure Boot can be customized to support any operating system or hypervisor that supports UEFI native boot. Signed updates provide zero-touch maintenance of Secure Boot variables and firmware updates. Legacy BIOS has no consistent, standardized security solution or update mechanism.

GUID Partition Table (GPT) Support

GPT replaces the obsolete Master Boot Record (MBR) partition scheme. GPT allows for storage media boot partitions greater than 2 TB in size, more than 4 partitions (up to 128), and the use of newer storage media such as PCI Express devices. Data integrity is also improved through redundant disk layout structures.

Platform and Architecture Independence

UEFI supports x86, x86_64, ARM, ARM64, PowerPC, Itanium, and other architectures. UEFI may also be emulated via hypervisors like Hyper-V, VMware, Xen, KVM, and others. UEFI simplifies device management through a homogeneous firmware experience.

Consistent Variables and Services

A standardized set of variables, services, and drivers are common to all UEFI implementations regardless of host device. UEFI on a desktop PC features the same core set of UEFI capabilities found on a device such as a smartphone. Application developers can create software tools without worrying about platform-specific firmware quirks commonly found with BIOS. Firmware developers can isolate platform-specific code through modularization.

Modular and Extensible

UEFI firmware modules can be added, removed, or updated by vendors and device owners. New modules can be created to extend the capabilities of a device's firmware. Modules may interact with device resources (e.g. network adapters, RAID controllers), UEFI environment variables, and kernel-mode drivers. Firmware structure is standardized.

Improved Boot Performance

Some UEFI modules and drivers can be loaded in parallel, rather than legacy sequential, to reduce boot time. Updated and larger Option ROMs can be used to initialize expansion devices such as graphics, audio, networking, and storage controllers. Bootable binaries and media can be given recognizable names as opposed to cryptic part and serial numbers.

CALL TO ACTION

Devices running in legacy mode or with Compatibility Support Module (CSM) enabled should be switched to UEFI native mode. The switch can be made non-destructively on deployed machines, or applied to new machines that replace older devices. UEFI advantages to security, user productivity, and device capability should be embraced to the extent possible.

REFERENCES

Vulnerability Solutions Office (2017, July 27). UEFI Defensive Practices Guidance. National Security Agency. U/OO/217598-17

Developer Zone (2011, March 21). About UEFI. Intel. Retrieved from http://software.intel.com/en-us/articles/about-uefi

James, Justin (2011, October 19). 10 Things You Should Know About UEFI. Tech Republic. Retrieved from http://www.techrepublic.com/blog/10-things/10-things-you-should-know-about-uefi

Hardware Dev Center (2017, May 2). UEFI Firmware. Microsoft. Retrieved from https://docs.microsoft.com/en-us/windows-hardware/manufacture/desktop/uefi-firmware

DISCLAIMER OF WARRANTIES AND ENDORSEMENT

The information and opinions contained in this document are provided "as is" and without any warranties or guarantees. Reference herein to any specific commercial products, process, or service by trade name, trademark, manufacturer, or otherwise, does not constitute or imply its endorsement, recommendation, or favoring by the United States Government, and this guidance shall not be used for advertising or product endorsement purposes.

CONTACT INFORMATION

Client Requirements and General Information Assurance/Cyber Security Inquiries
Cybersecurity Requirements Center (CRC)
410-854-4200
Email: Cybersecurity_Requests@nsa.gov