[](https://www.spiceworks.com/user/about/chiradeepbasumallick) [Chiradeep BasuMallick](https://www.spiceworks.com/user/about/chiradeepbasumallick) Technical Writer

November 17, 2022

***A basic input/output system or BIOS is defined as a program fixed and embedded on a device’s microprocessor that helps to initialize hardware operations and manage the data flow to and from the operating system (OS) at the time of bootup. This article explains the eight types of BIOS and discusses its importance in an IT environment.***

**Table of Contents**

* [What Is BIOS?](https://www.spiceworks.com/tech/devops/articles/what-is-bios/#_001)
* [Types Of BIOS](https://www.spiceworks.com/tech/devops/articles/what-is-bios/#_002)
* [Why BIOS Is Important](https://www.spiceworks.com/tech/devops/articles/what-is-bios/#_003)

What Is BIOS?

**A basic input/output system or BIOS is a program fixed and embedded on a device’s microprocessor that helps to initialize hardware operations and manage the data flow to and from the operating system (OS) at the time of bootup.**

Gary Kildall, a U.S. computer scientist, invented the word BIOS in 1975. It was integrated into IBM’s original PC in 1981, and gained popularity with additional PCs over the years, eventually becoming a fundamental characteristic of computers. However, a newer technology – Unified Extensible Firmware Interface (UEFI), has eclipsed BIOS in terms of adoption. Intel declared in 2017 its intention to discontinue support for the outdated BIOS platforms by 2020 and replace them with UEFI.

1975’s CP/M operating system used the Basic Input/Output System, from which the acronym BIOS was derived. Some businesses have reverse-engineered the BIOS, which was initially exclusive to the IBM PC, to manufacture interoperable computers. This initial system’s interface works as a de facto benchmark. The Unified Extensible Firmware Interface (UEFI) is intended to alleviate the technical challenges of the older PC BIOS.

The primary function of BIOS is to mediate between operating systems and the systems they operate on. The BIOS is the intermediate between the CPU and I/O device control information and data flow. In some instances, however, the BIOS may organize for information to flow straight to storage from devices, like graphics/video cards, that need a quicker data flow to function properly.

Most BIOS implementations are tailored to function with a specific machine or motherboard version by connecting with numerous devices, particularly system chipsets.

Initially, BIOS software was stored on the computer motherboard on a ROM chip. In modern systems, the BIOS is stored on flash memory, allowing it to be rebuilt without the need to remove the chips from the motherboard. This enables user-friendly BIOS firmware upgrades to introduce new features or rectify issues. Still, it also makes it possible for the machine to get contaminated with BIOS rootkits. In addition, a failed BIOS update might render the motherboard inoperable. Windows 10 is the most recent iteration of [Microsoft Windows](https://www.spiceworks.com/tech/enterprise-software/videos/microsoft-windows-11-whats-new/) to operate on computers with BIOS firmware.

**See More:**[**What Is Serverless? Definition, Architecture, Examples, and Applications**](https://www.spiceworks.com/tech/devops/articles/what-is-serverless/)

How does BIOS work?

The original IBM PC and XT BIOS omitted an interactive (UI) user interface. At the time, the power-on self-test (POST) still hadn’t adequately initialized a video display adapter, and systems showed error messages or codes on the screen, or they produced a coded sequence of audio to indicate problems. For the IBM PC and XT, developers used the jumper and switches on the motherboard and expansion cards to configure the system’s options.

Beginning in the mid-1990s, it became common for the BIOS ROM to contain a “BIOS configuration utility” (BCU[14]) or “BIOS setup utility,” which is accessible via a specific key sequence upon system startup. This application allows the user to configure system configuration parameters initially specified via DIP switches using a keyboard-controlled interactive menu interface.

The user may select hardware parameters employing the keyboard and video display on a current Wintel-compatible computer using a setup procedure substantially unaltered against that of the ROM-resident BIOS setup programs of the late 1990s. Modern Wintel machines may save BIOS configurations in a flash ROM, possibly the exact flash ROM that contains the BIOS.

Modern machines with the newest versions of CPUs have the functionality required to launch the BIOS right from the system’s ROM. If the system was just turned on (“cold boot”) or the reset button was hit, the complete power-on self-test (POST) is executed. If Ctrl+Alt+Delete was used (a “warm boot”), a particular indicator resting in the nonvolatile BIOS memory (“CMOS”) is verified by the BIOS to circumvent the long POST and memory detection.

The POST detects, tests, and initializes system components, including the RAM, motherboard, chipset, video card, mouse, CPU, keyboard, hard disc drive, optical disc drive, etc.

The BIOS begins boot processing after the option ROM scan is complete and all discovered ROM components with appropriate checksums have been called. Loaded applications may relaunch the system post-boot, but they must deactivate interruptions and other non-concurrent hardware activities that might conflict with the BIOS restarting process. Otherwise, the machine may freeze or crash during the reboot process.

The BIOS uses the boot devices specified in the nonvolatile BIOS storage (or the CMOS). It examines each device for bootability by trying to retrieve the first sector or boot sector. The BIOS advances to the subsequent device if it cannot recognize the sectors. Before accepting a boot sector and deeming the device bootable, certain BIOSes test again for boot sector signature 0x55 0xAA in the final two bytes of the sectors (512 bytes long) if the sector is successfully read.

When the BIOS detects a bootable device, it passes a command to the loaded sectors. The BIOS does not analyze the details of the boot sectors apart from potentially examining the final two bytes for the boot sector’s signature. The boot software interprets data structures such as BIOS Parameter Blocks and partition tables in the boot sectors or by other programs loaded during the boot procedure.

The BIOS’s functionality may be divided into four tasks:

* **Installation of complementary metal-oxide semiconductors (CMOS):**This setup application allows users to modify hardware and system settings. CMOS refers to the nonvolatile memory of the BIOS.
* **Bootstrap loader:** This function of the bootstrap loader locates the OS.
* **Software/drivers:**This function identifies the [device drivers](https://www.spiceworks.com/tech/devops/articles/what-is-device-driver/) and software that interact with the operating system once it is running.
* **Power-on self-test (POST):**It checks the computer’s hardware before loading the operating system.

**See More:**[**What Is PowerShell Scripting? Features and Best Practices**](https://www.spiceworks.com/tech/devops/articles/what-is-powershell-scripting/)

Is BIOS fully secure?

BIOS security is an often-overlooked aspect of cybersecurity, but it must still be controlled to stop hackers from running harmful code on the operating system. Cylance, a security firm, demonstrated in 2017 how current BIOS vulnerabilities might allow ransomware programs inside the UEFI of a motherboard and attack similar PC BIOS weaknesses.

Plundervolt was another unique vulnerability requiring BIOS modification. Plundervolt may be used to tamper with a PC’s power source while the material is being transferred to the memory, leading to inaccuracies and unpatched vulnerabilities. Intel published a BIOS [patch management](https://www.spiceworks.com/tech/devops/articles/what-is-patch-management/) update as a countermeasure.

There are three main ways to safeguard your BIOS: passwords, trusted platform modules (TPM), and complete disc encrypting:

* **Passwords:**The BIOS is launched before the OS, requiring the user to provide a passcode before the OS and allowing most other hardware to start. The user must then provide a second login to access a computer’s functionality. Using two sets of passwords offers additional protection against password-cracking software that circumvents conventional [cybersecurity](https://www.spiceworks.com/it-security/vulnerability-management/articles/what-is-cybersecurity/) measures.
* **Encrypting:**Full-disk encryption transforms information on a storage device into a structure only authorized individuals or systems can decipher. All material on the system’s hard drive is converted from plaintext to ciphertext, safeguarding the whole disc area and all documents on the disk.
* **TPM:**This sort of technology delivers security-related hardware-based capabilities. The Trusted Platform Module (TPM) chip is a safe crypto-processor that performs cryptographic operations. Multiple physical security protocols protect the chip against interference and [unauthorized software (malware)](https://www.spiceworks.com/it-security/endpoint-security/articles/what-is-malware-types-removal/).

**See More:**[**What Is Version Control? Meaning, Tools, and Advantages**](https://www.spiceworks.com/tech/devops/articles/what-is-version-control/)

Types Of BIOS

The main kinds of basic input-output systems (BIOS) include:

1. Legacy (1st generation) BIOS

Older motherboards use legacy BIOS firmware to switch on the computer. Legacy BIOSes have additional constraints; even though similar to UEFI, they dictate how the CPU and components interact. These cannot recognize discs larger than 2.1 terabytes, and their installation systems have text-only menus.

2. EFI

BIOS was the only firmware program in its category for a long while, but Intel recognized its shortcomings. Therefore, it started designing the Extensible Framework Interface (EFI). This produced an open set of standards for producing firmware for hardware devices without requiring the comprehensive framework rendered architecture-first.

The United EFI Forum maintains the Unified Extensible Framework Interface (UEFI) standardization, which evolved from the program. This is a group of technology businesses interested in the development of firmware specifications. The forum comprises Apple, Intel, Microsoft, and IBM, among others.

It is impossible to contrast BIOS with UEFI directly. Despite having the identical objective, which is to run the computer and serve as a bridge connecting the OS and the hardware, they work differently. BIOS is its system, whereas EFI is an adjustable foundation.

3. UEFI

UEFI (Unified Extensible Firmware Interface) may accept discs with a capacity of 2.2 TB or more by using the Master Boot Record (MBR) method as opposed to the more recent GUID Partition Table (GPT) technology. Even though Intel PCs are transitioning from traditional BIOS to UEFI firmware, Apple Mac PCs have never utilized BIOS.

UEFI is the most recent among the two-boot software packages, introduced in 2002. UEFI has superior scalability, speed, programmability, and security compared to BIOS. UEFI does not need a separate bootloader application to run the OS. UEFI also features a superior user interface and higher performance generally.

4. Apple Mac PC’s BIOS equivalent

When Macs migrated to the Intel platform, they implemented Intel’s Extensible Firmware Interface (eventually, the Unified Extensible Firmware Interface). Intel created this system as a substitute for the existing BIOS system.

UEFI was a radical departure from the previous BIOS system. It included not just massive boot disc support but also [firmware](https://www.spiceworks.com/tech/devops/articles/what-is-firmware/)-integrated drivers and programs, a ubiquitous graphics driver, NVRAM, plus runtime capabilities that they can use even after the operating system has been installed.

On the Mac, there is no equivalent to the previous BIOS. UEFI implements several aspects of the booting process. For instance, users may hit the option key during startup to choose the UEFI boot disc or command-R to activate system recovery mode. However, there are no possibilities for modifying hardware characteristics or the boot procedure.

Types of BIOS based on manufacturers

Each motherboard vendor develops a unique BIOS. Because various motherboards have distinct equipment layouts, the BIOS must be tailored to the specific set of hardware. When hardware malfunctions occur, the BIOS will send error messages to warn the user about the malfunctioning hardware. Different companies offering their own PC brands will create and update their respective BIOS versions.

IBM was the original owner of the BIOS software. However, other businesses, like Phoenix Technologies, have created their own versions by reverse-engineering IBM’s original. In doing so, Phoenix made it possible for other companies to manufacture reproductions of an IBM PC and, more critically, non-IBM systems that are compatible with BIOS. Compaq was one business that accomplished this.

Numerous manufacturers now make motherboards with BIOS chips. Asus, Foxconn, Hewlett-Packard (HP), and Ricoh are among the examples. Users may choose to upgrade their BIOS and chipset drivers — the software that allows the operating system to interact with other components, like a video card — to the most current versions. Driver upgrades may boost computer speed or address recently discovered BIOS-level security bugs.

**See More:**[**What Is Configuration Management? Working, Tools, and Importance**](https://www.spiceworks.com/tech/devops/articles/what-is-configuration-management/)

Why BIOS Is Important

The basic input-output system, or BIOS, of a computer, performs several essential tasks:

1. Checks if the system is receiving power

The Power On Self Test is the first task the BIOS performs when the computer is powered on. At the time of the POST, the BIOS verifies that the computer’s architecture can complete the initialization procedure. The system will typically produce a beep if the POST is executed correctly. However, if the attempt fails, the machine often produces a sequence of beeps. These beeps’ numbers, frequency, and sequence may be used to determine why the test failed.

2. Helps the computer to locate software and complete the boot process

The BIOS software often lives on the Read-Only Memory (ROM) or flash memory chip connected to your computer’s motherboard. BIOS is the first program to assume control of the system whenever turned on; therefore, its position within the chip is crucial. If the BIOS were not always situated in the same location within the same chip, the device’s microprocessor would fail to identify it, preventing the boot process from occurring.

3. Protects the system from security threats

Typically, a BIOS security patch is released for a specific cause. A [security vulnerability](https://www.spiceworks.com/it-security/vulnerability-management/articles/what-is-a-security-vulnerability/) is discovered, and the update corrects it. Several Lenovo laptops received a BIOS update that patched several security bugs that an attacker could perhaps exploit to access the storage or run arbitrary code. The majority of security updates are modest and unlikely to harm your system. However, boosting your PC’s security is rarely a bad idea.

4. Helps address deep-seated performance issues

On motherboards, bugs and other flaws are often discovered and resolved at the BIOS level. Indeed, we seldom interact with our BIOS, but it’s unlikely that you’ll notice if you do. Alternately, BIOS faults may emerge in different ways. If you’ve encountered an inconvenient condition on your PC that has continued through several updates (despite the fact that you’ve logged it dozens of times) and still hasn’t been resolved, you may need to check to see if it’s a BIOS issue and if there’s an update available to address it.

5. Checks and loads a functioning OS onto the PC

The BIOS then tries to install the OS through a software named the bootstrap loader, which is intended to identify any accessible OS; if a good OS is discovered, it is put into memory. Additionally, BIOS drivers are installed at this time. These applications are intended to provide the computer with rudimentary control of hardware devices, including mice, keyboards, network gear, and storage devices.