# This is why Windows 64-bit is more secure than 32-bit Windows

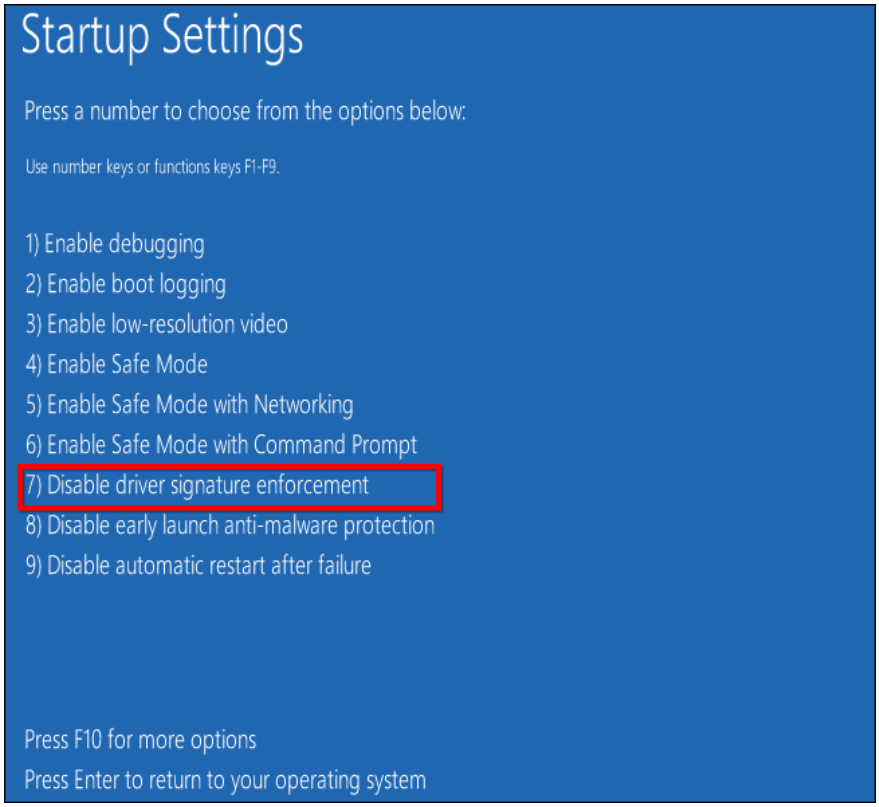
In fact, the 64-bit version of Windows does not simply allow you to use RAM on the 4GB amount, but it also ensures more security than the 32-bit version.

Today most new systems are 'released' in the market, which is defaulted to 64-bit Windows. If you've used Windows XP for a long time before switching to Vista, Windows 7 or Windows 8, you're probably familiar with the 32-bit Windows management system.

In fact, the 64-bit version of Windows does not simply allow you to use RAM on the 4GB amount, but it also ensures more security than the 32-bit version.

In addition, 64-bit Windows operating systems are not immune to malware, but they have more security features. Some of these features also apply to 64-bit versions of other operating systems such as Linux. Linux users will get advanced security features when switching to the 64-bit version.

## 1. Mandatory Driver Signing (Drivers must be pre-tested)




64-bit Windows is forced to implement MDS - Mandatory Driver Signing. All driver code on the system must be digitally signed. These include Kernel-Mode device drivers and User-Mode drivers, such as printer drivers.

MDS prevents strange drivers (provided by Malware) from running on the system. Malware creators will have to find some way to get through the signing process (for example, via boot-time rootkit, making the driver infected, causing "hard" drivers to run. on the system more.

MDS is also used on 32-bit versions of Windows. However, MDS does not continue to be compatible with older 32-bit drivers.

To disable MDS during development on 64-bit versions of Windows, you must attach the Kernel Debugger, or use special boot options.

## 2. Address Space Layout Randomization (ASLR)


ASLR is a security feature that makes the program's data location randomly arranged in memory. Before ASLR, the data location of the program in memory is predictable, making attacks on the program simpler. With ASLR, an attacker must guess the correct location in memory when trying to exploit a vulnerability in the program. Incorrect predictions can result in the program crashing, so an attacker will not be able to try again.

This security feature is also used on 32-bit versions of Windows and many other operating systems. However, on 64-bit versions of Windows, ASLR is much more powerful. 64-bit systems have a much larger address space than 32-bit systems, so ASLR is also much more efficient.

## 3. Kernel Patch Protection

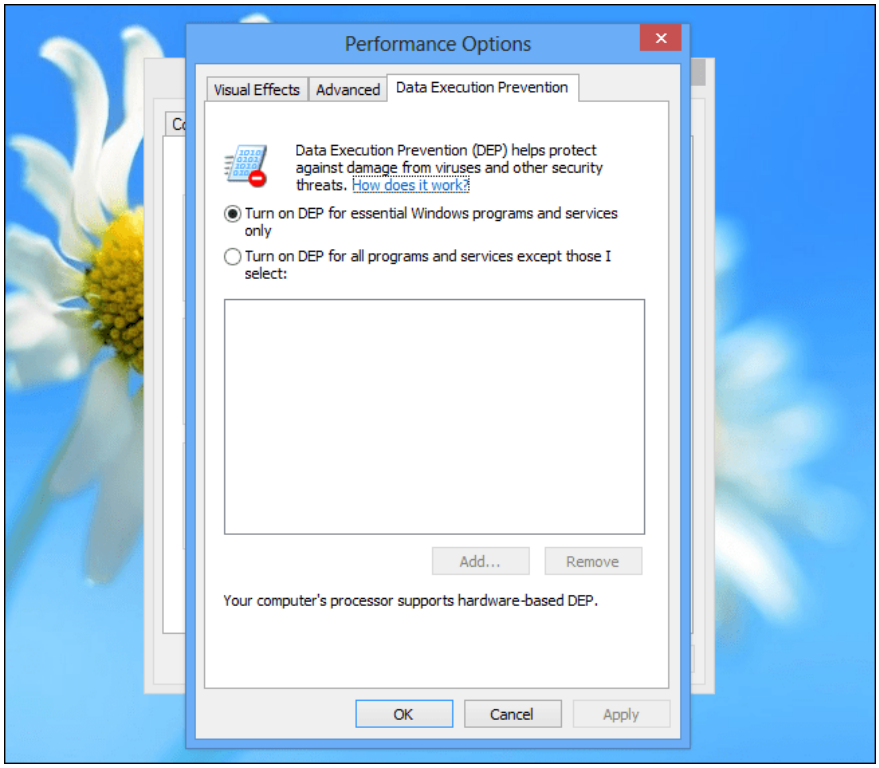
Kernel Patch Protection - KPP, also known as PatchGuard, is a security feature only available on 64-bit versions of Windows. Patch Guard prevents software, even the driver running in kernel-mode.

According to Wikipedia, the Patch kernel is the Kernel (kernel) modification process of supported or unsupported Windows operating systems by filling security holes. Microsoft never supports Kernel Patching, the simple reason is that Kernel Patching reduces system reliability.

Although you can apply Patch Guard on 32-bit Windows, many 32-bit antivirus software uses the ability to fill the system to work so this blocking is not applicable.

A good example is PatchGuard that prevents rootkits from changing Windows operating principles or being located in the operating system kernel. If this happens, Windows will immediately turn off using BlueScreen or Reboot.

## 4. Data Execution Protection (DEP)




DEP allows the operating system to mark certain areas on memory as 'non-executable' (not executed) by setting 'NX bit'. This memory area is only allowed to store data and cannot execute user commands.

For example, on non-DEP systems an attacker can use some kind of buffer overflow to write code into the memory area of ??the application that can then be executed. With DEP, an attacker can write code into the memory area of ??the application - but this area will be marked as unenforceable and cannot be done to prevent the attack.

On 64-bit Windows operating systems with hardware-based DEP (if you have a modern CPU, 32-bit versions of Windows also support hardware-based DEP). However, DEP is always enabled for 64-bit programs, while by default, it is disabled for 32-bit programs for compatibility reasons.

The DEP configuration dialog in Windows only applies to 32-bit applications and processes because of Microsoft documentation, that DEP is always used for all 64-bit processes.

# 5. Compatible WOW64

64-bit Windows operating systems can run 32-bit Windows operating system programs, but require it to have a special compatibility layer with the WOW name (Windows 32 on Windows 64).

This compatibility layer enforces some limitations for 32-bit programs, which can prevent 32-bit malware from working. 32-bit malware will not be able to run in kernel mode - only 64-bit programs can do it on 64-bit operating systems, so 32-bit malware will be maximized.

64-bit Windows also stopped supporting older 16-bit programs like Turbo C / C ++ and many 16-bit antivirus programs.

In addition to preventing ancient 16-bit viruses, this will also force many companies to upgrade their 'ancient' 16-bit programs that can 'stick' their unpatched vulnerabilities.

## Refer to some of the following articles:

1. Instructions for upgrading from Windows 10 32-bit to 64-bit

1. Compare Firefox 64 bit and 32 bit performance

1. These are the reasons why you should use a 64-bit Chrome browser

**Wish you have moments of fun!**