

Toshiba EasyGuard
Carefree Mobile Computing



Toshiba EasyGuard is the better way to enhanced data security, advanced system protection and easy

connectivity. This next-generation computing experience incorporates technologies enabling optimal connectivity and security, Toshiba hardware innovations and advanced software utilities for carefree mobile computing.

Three core elements for carefree mobile computing

In addressing the need for enhanced data security, advanced system protection and easy connectivity, Toshiba EasyGuard features can be divided into three core elements:

- Secure** Features that deliver enhanced system and data security
- Protect & Fix** Protective design features and diagnostics utilities for maximum uptime
- Connect** Features and software utility that ensure easy and reliable wired and wireless connectivity



What is Execute Disable Bit (XD Bit)?

Execute Disable Bit is a system feature that, if present and enabled, allows the notebook's processor to distinguish between bits of code that should be executed and the ones that cannot be, as they pose a threat to the system.

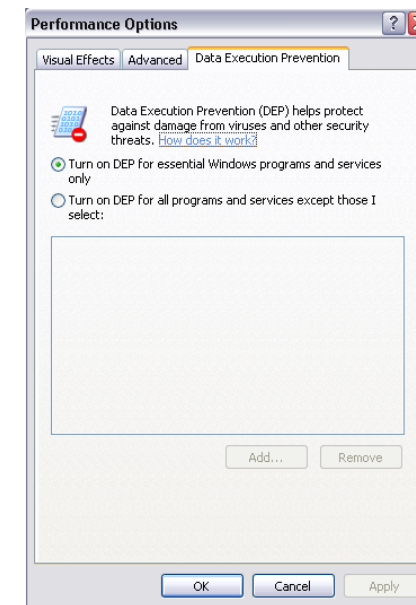


When a malicious worm attempts to insert code into the buffer, the processor disables code execution, preventing damage or worm propagation. In other words, even if infected code is present on the notebook, as long as the processor does not execute it, the code cannot cause any damage. This process, where the system processor disables code execution, is also called Data Execution Protection or DEP.

What is hardware-enforced DEP and how does it work?

The DEP (Data Execution Protection) process can be either hardware-enforced, which requires hardware support or software-enforced, which provides additional exception handling checking and does not require specific hardware support. (Hardware-enforced DEP requires a processor capable of executing the feature as defined by Intel for the Execute Disable Bit.)

DEP marks all processor memory locations as non-executable unless the location explicitly contains executable code. One class of security attacks attempts to insert and execute code from non-executable memory locations. DEP helps prevent these attacks by intercepting such attempts and raising an exception. DEP also relies on processor hardware to mark memory locations with an attribute indicating that code should not be executed from that location. Windows XP Service Pack 2 recognizes this exception and prevents that code from executing.



©2005. Toshiba Europe GmbH. While Toshiba has made every effort at the time of publication to ensure the accuracy of the information provided herein, product specifications, configurations, prices, system/component/options availability are all subject to change without notice. For the most up-to-date product information about your computer, or to stay current with the various computer software or hardware options, visit Toshiba's Web site at www.toshiba-europe.com.

The 32-bit version of Windows (beginning with Windows XP Service Pack 2) uses the Execute Disable Bit feature as defined by Intel when the notebook processor is running in Physical Address Extension (PAE) mode.

DEP Configurations for Windows XP SP2

- ▶ **Opt-in:** DEP is enabled by default for limited system applications and software applications that 'opt-in' and is available on systems with processors capable of hardware-enforced DEP. Technical support may enable DEP for additional applications.
- ▶ **Opt-out:** DEP is enabled by default for all processes. Users can manually create a list of specific applications that are not DEP-enabled by using System Properties.
- ▶ **Always On:** Full coverage for the entire system and all processes run with DEP enabled. It is not possible to 'opt-out' of DEP.
- ▶ **Always Off:** There is no DEP for the system.

Summary of features and benefits

- ▶ **Execute Disable Bit (XD-Bit)** Prevention of buffer overflow virus attacks by enabling the system processor to distinguish between code that can and cannot be executed
- ▶ **Data Execution Protection (DEP)** Process that allows the system processor to disable code execution, thereby preventing virus damage or worm propagation
- ▶ **Four DEP configurations** User flexibility