







Tech Insight: Execute Disable Bit (XD-Bit)



Toshiba EasyGuard™ technology is a series of hardware and software enhancements to business-class notebooks that greatly improve mobile computing. By providing users with increased data security, system protection, simple connectivity and ease of use, EasyGuard™ technology is continued evidence of Toshiba's vast experience in mobile computing and our ongoing commitment to providing users with a better, more reliable notebook experience.

Toshiba EasyGuard technology comprises a number of features some of which may or may not be available on a particular Toshiba notebook depending on the model selected. See www.easyguard.toshiba.com for detailed information.

Toshiba EasyGuard™ Four core elements for more confident computing

-  **Protect & Fix**
Fortifies vital information and vulnerable components against the stress and hazards mobile computers are exposed to every day.
-  **Secure**
Helps defend your data and your notebook against loss, theft or viral attack.
-  **Connect**
Helps you locate and establish a wired or wireless connection effortlessly and quickly.
-  **Optimize**
Allows you to customize the notebook's system performance so you can be more productive.

What is Execute Disable Bit (XD-Bit)?

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

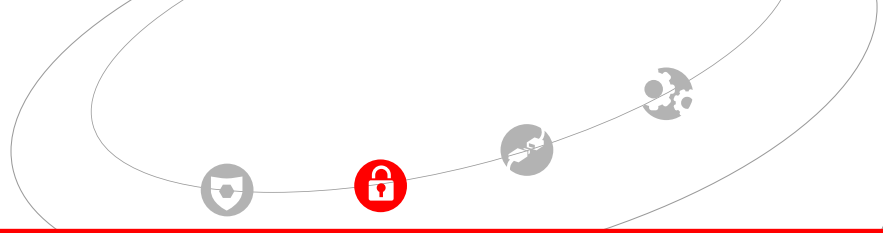
When a malicious worm attempts to insert code into the buffer, the processor disables the code execution, helping to prevent damage or worm propagation. In other words, even if infected code is present in the notebook, so long as the processor does not execute it, the code cannot cause any damage. This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

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

The DEP process can either be 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 XD-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. The 32-bit version of the Windows® OS (beginning with Windows® XP Service Pack 2) uses the XD-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)

- Adds a layer of protection from worms and viruses and enables 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 unknown code execution, thereby helping to prevent virus damage or worm propagation

DEP configurations

- Four DEP configurations offer enhanced user flexibility