efficēon PROCESSOR

Transmeta CORPORATION

Product Sheet

Transmeta™ Efficeon™ Processor with AntiVirusNX™ Technology

In response to the escalating threat of computer virus attacks, Transmeta has introduced a new feature on Efficeon processors - called AntiVirusNX - that can detect common viruses and render them harmless for Efficeon-based computers. AntiVirusNX works in conjunction with Microsoft's Data Execution Protection (DEP) technology in Windows XP Service Pack 2 to detect and prevent attempts by attackers to overflow memory buffers with malicious virus content. AntiVirusNX represents a significant deterrent to the ever increasing threat of computer viruses, many of which (including the recent Sasser, Blaster, Code Red, Bugbear worms) have leveraged buffer overflows as a means of entry into a computer operating system.

AntiVirusNX™ TECHNOLOGY

Some of the most devastating attacks, including numerous worms, as well as many other malicious programs, attack computers by attempting to insert and execute code from data regions of system memory. The Data Execution Protection (DEP) feature in Windows XP Service Pack 2 leverages the Efficeon processor's AntiVirusNX technology to stop this malicious code immediately if it attempts to execute and thereby infect the computer. This combination offers significant improvements against software worms and viruses, providing enhanced security and safer computing.

How Buffer Overflows Spread Viruses

Buffer overflows in software programs account for a large number of computer intrusions. Buffer overflows occur when the data intended for software is actually larger than the memory area set aside for that data.

An analogy would be pouring the entire contents of a pitcher into a glass; once the glass is full, the excess liquid pours over the side. Malicious code hidden in the overflow is then executed by the computer.

Virus & Worm Examples

- Sasser Worm
- Blaster Worm
- Bugbear Worm
- Code Red Worm
- Klez Worm
- Welchia Worm

Computer WITHOUT AntiVirusNX	Application Exploits a Buffer Overflow	Virus Infects Computer
▪ Computer cannot take advantage of Data Execution Protection. ▪ Computer is more vulnerable.	▪ Data overflows buffer with virus code & overwrites return address. ▪ New return address points to virus.	▪ Virus within buffer is executed. ▪ System is infected and may attempt to infect other systems.

Transmeta AntiVirusNX & Microsoft DEP

The combination of Data Execution Protection (DEP) and AntiVirusNX technology marks all program memory locations as non-executable unless the location explicitly contains executable code. It does this by relying on the Efficeon processor to mark memory with an attribute indicating that code should not be executed from that memory.

Computer WITH AntiVirusNX Protection.

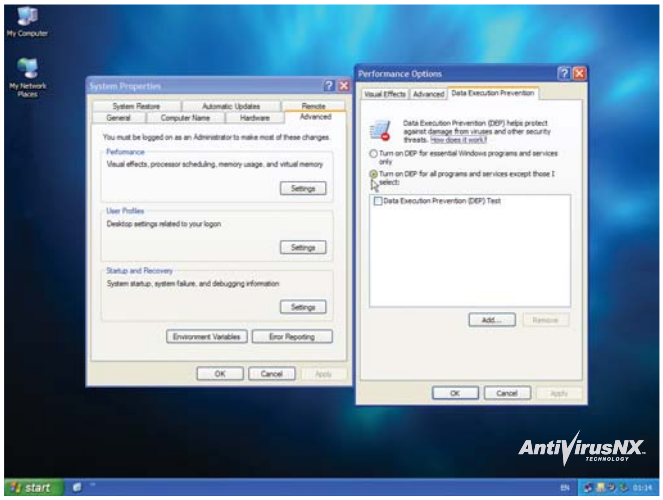
- Efficeon identifies malicious code when execution is attempted.
- Efficeon's data execution protection shields system from virus.
- Efficeon notifies the Windows operating system.

Transmeta AntiVirusNX Technology:

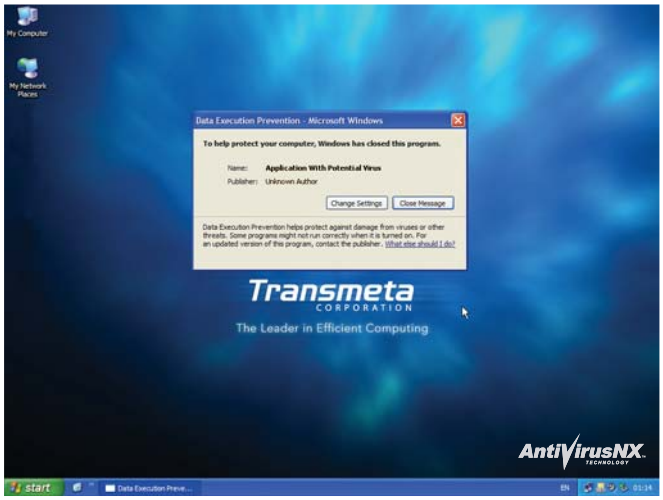
- Works closely with DEP to identify code entering an Efficeon processor after a buffer overflow occurs.
- Shields Efficeon processors from buffer overflow vulnerabilities by marking the code as non-executable.
- Complements 3rd party anti-virus software. For full protection, users are strongly recommended to install and regularly update 3rd-party anti-virus software to enhance overall system security.

Transmeta Efficeon Processor with AntiVirusNX Technology

AntiVirusNX Technology & Data Execution Protection in Action



AntiVirusNX and Data Execution Protection can easily be enabled or disabled using a new interface located in the System Properties section of the Control Panel. It can be configured to protect against viruses and threats for all programs and can also be configured to exclude specific programs. AntiVirusNX technology does not prevent all viruses or worms from damaging a user's PC, just ones based on buffer overflow vulnerabilities.



When a threat is detected, AntiVirusNX denies the application its execution privileges and shuts it down, protecting the computer from the potentially hazardous code. AntiVirusNX has been tested to protect against buffer overflow attacks on the Windows XP with Service Pack 2. For full protection, users are strongly recommended to install and regularly update 3rd-party anti-virus software to enhance overall system security.

Transmeta Efficeon Processor Core

To maximize performance and responsiveness, the Efficeon processor features a state-of-the-art 256-bit-wide VLIW (Very Long Instruction Word) engine that can issue up to 8 instructions per clock cycle. A large 1MB L2 cache and support for SSE & SSE2 instructions help make for a compelling multimedia experience.

Transmeta Code Morphing Software

Transmeta's proprietary Code Morphing Software (CMS) runs at the heart of the Efficeon processor, dynamically optimizing and translating x86 instructions into VLIW native code. This unique combination of hardware and software allows the processor to be more efficient, adding intelligence to Efficeon not found in other x86 microprocessors to manage power consumption and heat dissipation.

With the new Code Morphing Software for the Efficeon processor, Transmeta further extends its leadership in power management, offering a solution that provides high performance for multimedia applications while consuming less power for performing the same amount of work.

Transmeta Enhanced LongRun™ Power Management

LongRun power management technology provides Code Morphing software with the ability to adjust the Efficeon processor core operating voltage and clock frequency dynamically, depending on the demands placed on the processor by software. Because power varies linearly with clock speed and by the square of voltage, adjusting both processor voltage and clock frequency can produce cubic reductions in power consumption, whereas conventional processors can adjust power linearly only by adjusting the effective operating frequency.

LongRun power management policies are implemented within Code Morphing software, and can detect different workload scenarios based on runtime performance information, and then exploit these by adapting processor power usage accordingly. This ensures the processor delivers high performance when necessary and conserves power when demand on the processor is low. All power adjustments are transparent to the operating system and the user.

Transmeta CORPORATION

For more information, visit **www.transmeta.com**

efficēon PROCESSOR

UNITED STATES & EUROPE
Transmeta Corporation
World Headquarters
3990 Freedom Circle
Santa Clara, CA 95054 USA
Tel: (408) 919-3000
For US Sales Inquiry: sales@transmeta.com
For Europe Sales Inquiry: sales-eur@transmeta.com
www.transmeta.com

JAPAN
Transmeta Japan
KDDI Bldg Annex 3F
2-3-3 Nishi-Shinjuku
Shinjuku-ku Tokyo 160-0023
Japan
Tel: +81-3-5325-9580
sales-jp@transmeta.com
www.crusoe.jp

TAIWAN
Transmeta Taiwan
7F-1, No.167,
Fu-Hsing North Road
Taipei, Taiwan
R.O.C. 105
Tel: +886-2-2718-0999
sales-tw@transmeta.com
www.transmeta.com.tw

CHINA
Transmeta Shanghai
Room 1202,
Lansheng Building,
No.8, Huai Hai Zhong Road
Shanghai, P.R.C.
Tel: +86-21-63191576
sales-sh@transmeta.com
www.transmeta.com.cn

KOREA
Transmeta Korea
602-603 Imae-Dong,
BunDang-Gu,
SeungNam City, Kyunggi-Do,
463-905 Korea
Tel: +82-19-321-1042
sales-kr@transmeta.com

QUALITY MANAGEMENT SYSTEM
CERTIFIED BY DNV
ISO 9001:2000