

16 October 2006

By: Marius Oiaga, Technology News Editor

## [Symantec Advises Microsoft on PatchGuard](#)

### *Delivering a mitigation*



Calling Microsoft's view on the security environment limited because of its focus on the traditional aspects of protection such as file-based scanning anti-virus and firewall and its ignorance of behavior-blocking technologies, Symantec has issued a number of advises designed to point the Redmond Company in the right direction. Coincidentally, Symantec's right direction is the opening of PatchGuard in 64-bit Vista which is also shared by a consistent share of the security industry that has fallen in behind Symantec and McAfee.

“Whatever Microsoft’s intent, whether it is DRM or security, they have clearly avoided addressing some important issues. They have been disingenuous and have misled vendors under false pretenses during the development of Windows Vista,” commented Oliver Friedrichs, director of emerging technologies in Symantec Security Response.

According to Symantec, Microsoft's PatchGuard aims to secure digital rights management on top of the enhanced protection implied by a locked down kernel. In fact, protecting against the copying of audio and video content requires a secure media path that can be achieved via kernel control. “Microsoft has to prevent anyone from writing a driver that will intercept protected content. As a result, they have implemented a significant portion of the Palladium NGSCB security model,” explained Friedrichs.

In this context, Friedrichs has taken onto himself to voice Symantec's position on PatchGuard. On Symantec's Security Response Weblog Friedrichs presented a model that would mitigate the issue at hand by continuing to deliver protection for Windows Vista kernel for both DRM and security while also permitting the integration of third party security solutions. Friedrichs is the author of the following enumeration:

- Symantec is not recommending that Microsoft remove PatchGuard from Windows Vista. That has never been a point of contention.
- Symantec has provided Microsoft with recommend APIs that will allow legitimate, authorized, and certified security vendors to leverage the same capabilities that we have in prior versions of Windows.
- Symantec has been asking for these capabilities for well over one year now, and therefore, these concerns are not a new development to Microsoft.
- Symantec has repeatedly suggested that Microsoft establish a new certification model that will certify legitimate vendors who seek to extend the Windows Vista kernel. This certification, on top of existing driver certification steps, will ensure that certified vendors are not attempting to bypass Windows DRM and that certified vendors are not malicious and are making genuine enhancements to Windows Vista.

### RELATED LINKS

[Microsoft Details Kernel Patch Protection in Vista](#)

[Microsoft Opens Vista's Core](#)

[Vista PatchGuard Hacked](#)

[Symantec Attacks Windows Vista's Security Features](#)

[McAfee Aims for Microsoft's Jugular](#)

[Vista's Patch Guard is Killing Next Generation Behavior-Blocking Technologies and Future](#)

[Security Models](#)

[Symantec Predicts Windows Vista to Be a Security Liability](#)

[Microsoft Increasing Security Risk with Vista](#)

[Vista Colors Preview](#)

[Update on the Windows Vista Start-up Sound](#)

[What You Don't Know Can't Hurt You = Microsoft's Approach to Security](#)

[Vista-Ready Products for the Holidays from Microsoft's Partners](#)

[Windows Vista Help and Support](#)

[Vista User Account Control Requirements Available](#)