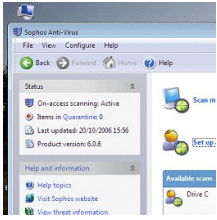


23 October 2006

By: Marius Oiaga, Technology News Editor

[Symantec and McAfee Should Have Prepared Better for Vista](#)

Comments Sophos



Sophos, as well as Kaspersky, have gone AWOL, at least judging from the perspective of McAfee and Symantec who are spearheading the criticism against Microsoft's Kernel Patch Protection technology. Rallying with the Redmond Company, Sophos' position on Patch Guard is that Symantec and McAfee have just been caught unprepared by Vista. Neither Symantec nor McAfee have commented in any manner Sophos' statement. "Symantec and McAfee may be struggling with HIPS because they haven't coded their solutions with 64-bit Vista in mind," explained Richard Jacobs, CTO of Sophos. "We've taken a different approach to HIPS, by focusing more on catching bad behavior by analyzing code before it executes. Additionally, we are building our technology by making use of supported Microsoft interfaces rather than by trying to subvert the kernel by 'hooking' calls to it. That's why we're ready for 64-bit Vista, and others aren't." Sophos found no reason to comply over Microsoft's Patch Guard since Sophos Anti-Virus with built-in HIPS has been successfully tested on 32- and 64-bit versions of Windows Vista. Sophos does a little more than suggest that the complaints issued by McAfee and Symantec regarding them being locked out of Vista's kernel, as well as Microsoft's anti-competitive practices are unsubstantiated. In their view, Patch Guard is a positive step for Window Vista's security, and dismisses Microsoft's anti-competitiveness. At the heart of Sophos' conclusion is Microsoft's commitment to deliver a similar level of kernel support and integration to third party security developers as it does to its in house security product team. As an argument, Sophos delivers a screenshot with Sophos Antivirus running on Vista. But there is only so much praise for Vista's Patch Guard. In the end, Sophos turns the page and declares Vista "more secure" but by no means 100% secure, thus justifying the need for antiviral solutions. "It's clearly the case that we and other vendors will now have some dependency on Microsoft to deliver kernel interfaces for new security innovations, which could slow us all down," continued Jacobs. "However this is more than compensated for by the additional security offered by Vista. PatchGuard is a step in the right direction for customers, and we believe that security vendors should embrace and work with PatchGuard rather than fight it."