

19 May 2007

By: Marius Oiaga, Technology News Editor

Graham Cluley
Sophos

[Sophos: We Don't See Any Advantage in Deploying Windows Vista](#)

Saying no to the Wow...

Windows Vista, Microsoft latest operating system made available on January 30, 2007, is applauded by the Redmond Company as the most secure Windows platform to date. In the first 100 days on the market, Vista has sold approximately 40 million licenses and it is lagging behind various Linux distributions and Mac OS X Tiger in terms of the vulnerabilities that have impacted the platform. Find out what Sophos, a world leader in IT security and control solutions, has to say about Windows Vista and Microsoft's baby steps into the security industry. Sophos has had security solutions in place for Vista since November 2006, even before Microsoft released the operating system to Software Assurance customers. Sophos Anti-Virus for Windows Vista received the prestigious Virus Bulletin VB100 award in 2007, outperforming newcomer Microsoft with OneCare. Still, although it does run Vista internally, Sophos has not completely rolled out the operating system, because it sees no advantages in such a move. Just as I have promised earlier this week, today, you are in for a real treat: an interview with **Graham Cluley, Senior Technology Consultant at Sophos**.

1. How has Microsoft's latest operating system impacted the threat environment? Has Sophos' role changed in any way? Our role hasn't changed at all. Many different types of threats continue to affect Windows Vista users as well as users of earlier versions of Microsoft operating systems (and indeed alternative OSES). It is true that some malware finds it more difficult to operate on Vista, or may be completely incompatible with Vista. However, it is likely that we will see more malware which is "Vista-compatible" as time progresses. The hackers will be sure to code their attacks to work with Vista as they see a growing population of users adopt the new operating system.

2. Microsoft's Michael Howard has revealed that the company plans to reduce the number of critical vulnerabilities in Vista to half, compared to XP. Is that a valid expectation? It's not in our nature to examine chicken entrails and predict the future number of vulnerabilities with such precision, so we'll leave that to Microsoft! However, it's encouraging to hear that they are thinking positively. The only thing that is certain is that there will be more vulnerabilities and more attacks, and that Windows Vista users will need to take security seriously.

3. Obviously, Windows Vista is neither impenetrable nor foolproof. Jim Allchin, former Co-President, Platforms & Services Division, revealed - before he departed from Microsoft - that anti-virus programs are essential to the security of the operating system. What does Sophos have to offer for Windows Vista, for both the 32-bit and 64-bit editions of the operating system? We announced our [solution for Windows Vista](#) in November last year. We support both 32-bit and 64-bit versions of Windows Vista. While other security vendors were not happy with how Vista implemented its increased security, Sophos worked closely with Microsoft and fully supports new functionality, such as Kernel Patch Protection (also known as PatchGuard).

4. What is Sophos' perspective on the ANI file format handling vulnerability? The code dates back to Windows 2000. Should it have survived for so long, through so many versions of Windows? Is it just a case of Microsoft delivering poor code quality even with Vista? I don't think anyone sensible believed that Vista would be perfect and would contain no vulnerabilities. The ANI vulnerability has affected many versions of Windows, and has been exploited widely by hackers. Sensible companies and home users will have rolled-out the patch from Microsoft, and made sure that they are monitoring future vulnerabilities in Microsoft's code that come to light.

5. Is Microsoft sending customers the message that their security solutions are better equipped to protect Windows? Is the fact that they deliver both the operating system and the security solutions for it a

conflict of interest? I know that the actual performances of OneCare and Forefront speak for themselves, but could you comment on Microsoft's OneCare and Forefront releases?Sophos welcomes Microsoft's role as a responsible newcomer to the anti-virus market. The launch of the consumer product Microsoft OneCare highlighted the need for *real* protection amongst many home users who have been traditionally poorly protected. Real professionals in the anti-virus marketplace, such as Sophos, are allies in the aim to clean up the Internet, and have years of experience in helping businesses defend themselves against the threats. I don't think it would be appropriate for us (as a competitor) to comment on the quality of Microsoft's security protection products. After all, you would expect us to say that they were inferior wouldn't you! So that's not very helpful to people. What I would suggest is that anyone considering switching their anti-virus protection to **any** other security product (Microsoft, or otherwise) would be sensible to research the independent comparative reviews by competent testing laboratories. Any company considering switching its protection will be interested in a number of factors which include, but are not limited to, detection rates, resource usage, speed, technical support, OS platform coverage etc. Undoubtedly, Microsoft will face some interesting challenges in trying to convince businesses that it is a serious player in the security space. Many sysadmins perceive that Microsoft code has introduced flaws into their company, and may not feel comfortable using a solution which is likely to be targeted heavily by the hackers because it is widely used by consumers. Additionally, many companies may not put Microsoft on their shortlist in the first place because it does not support Oses such as Mac OS X, Lotus Notes, UNIX etc.

6. Sophos is taking the wind out of the sales of Symantec and McAfee, in the enterprise security market. Is Forefront an able-bodied competitor? Sophos, Symantec and McAfee are in a three horse race for enterprise security protection, and are frequently competing when corporations evaluate their defenses. Microsoft Forefront is a new product, which has yet to establish its pedigree, and will be automatically excluded from many shortlists because it fails to support non-Microsoft operating systems. Microsoft wants companies to feel safe when they use the Internet, and not to feel that Microsoft is doing nothing about the security problem. The company also wants to do something to stem any move amongst consumers away from Windows and to alternative operating systems such as Apple Mac and Unix. How effective Microsoft will be in the enterprise security segment remains to be seen - without a doubt, they are likely to face more challenges in the business market than protecting home users.

7. Is Microsoft, with the User Account Control, training users to blindly agree to warnings? There is a danger that users will begin to automatically click "go ahead" every time UAC displays a warning message. If people get into this habit (which sadly is just human nature) then it effectively will be the same as having no protection in place at all.

8. The belief that upgrades should be performed following the availability of the first service pack is somewhat generalized. What is your opinion on the matter? Should customers wait to deploy Vista until SP1? Has Sophos deployed Vista internally? Obviously, we have some computers running Windows Vista in our development and testing departments, but we have not rolled out Windows Vista internally. We don't currently see that there would be any advantage in doing that. Companies will need to decide for themselves if Windows Vista is appropriate for rolling out inside their enterprise. I would imagine that many companies would need to upgrade their hardware to get maximum return from the software.

9. If you were to choose the safest operating system, out of Windows Vista, Mac OS X and Linux, what would your choice be? I don't think it's as simple as to say which OS is the safest. All Oses are as safe (or unsafe) as the user sitting in front of them. All companies need to ensure that their users' computers are being properly defended with security software, the latest security patches and a healthy serving of user education.

10. Where will the future take Sophos? What are your company's plans for 2007? We're seeing a considerable rise in competitive displacements, which are primarily customers switching from Symantec or McAfee to Sophos. Over 2000 enterprises switched to Sophos from our

competitors during the first three months of this year. Companies are finding that they don't have to live with the pain of their existing solutions, and that there is an alternative that can deliver considerable benefits. Sophos is uniquely positioned to deliver a single client and integrated policies at desktops and gateways, fighting the threat and lowering management complexity and cost. You can expect to see us announcing some exciting new developments in our product line which will help more and more companies secure and control their business.