

3 November 2007

By: Marius Oiaga, Technology News Editor

Windows XP -
Windows Vista
Microsoft

[Microsoft Offers a Complex Windows Vista vs. Windows XP Perspective](#)

Security-wise

A new standard of security is an integer aspect of the evolution puzzle represented by the move from Windows XP to Windows Vista. The Redmond company applauded not only the Wow factor of its latest Windows client, but also a new milestone in user protection, synonymous with the delivery of its most secure platform to date. But while Microsoft has been beating the drum of Vista as an epitome of security, the young product offered little in support of the company's claims that it was an apex of the Windows operating system. This changed toward the end of October, when the company made available its [Security Intelligence Report](#) covering January - June 2007 and offering a complex perspective over the comparison between Vista and XP, security-wise. "Since our last Security Intelligence Report, Microsoft is extremely excited to have successfully launched Windows Vista, the most secure Microsoft operating system to date. Windows Vista is the first operating system developed end to end using our Security Development Lifecycle (SDL). Using the SDL helped us to maintain a focus on security during the development of Windows Vista and to ensure that it was the highest quality product we could release. Several security-related features were also included in Windows Vista, including User Account Control (UAC), Kernel Patch Protection for x64 Windows, Internet Explorer 7 with Protected Mode, Windows Defender, and Address Space Layout Randomization (ASLR)," revealed George Stathakopoulos, General Manager, Microsoft Product Security Center. The Secure Development Lifecycle is a complex methodology applied to the software development process in order to bulletproof a product. The end purpose of software build under the SDL is to deliver a minimal window for attacks, due to the reduced volume of security vulnerabilities concomitantly with the toning down of the overall severity rating. Microsoft has revealed repeatedly that its target is in fact to melt down SDL in the general development process, identifying the two in order to create security-focused products. But at the same time foolproof software cannot be the final milestone of the development process. "We understand that security is a journey and not simply a destination. Microsoft remains vigilantly committed to working with our partners in the security space to enable a safe and secure computing experience on the Internet," Stathakopoulos added. Still, users have to understand that while Microsoft has made extensive efforts to increase the security of Windows Vista, the extra features introduced are nothing more than [mitigations and not actual boundaries](#). And yes, UAC, ASLR, IE7 Protect Mode, PatchGuard and mandatory driver signing are not security boundaries. In this context, Microsoft Technical fellow Mark Russinovich explained that while the items are indeed beneficial to the overall security score of Vista, they are by no means a guarantee of protection made to end users. In the end it all comes down to the cost and the time associated with implementing security boundaries and the final impact delivered. Microsoft not making a guarantee about the extra security mitigations in Vista, is a silent confirmation of the fact that the Windows operating system continues to be vulnerable and exposed to attacks even with the Vista version. But this does not mean that SDL did not add value to Vista. "Microsoft has released just six security bulletins for Windows Vista during the first six months of 2007. This demonstrates that our practices are working and reinforces our continued investment into processes like the SDL. All the same, we realize there is still a long road ahead of us and there is a lot of work to be done to further protect the entire PC ecosystem," Stathakopoulos explained. Six security bulletins in the first six months of 2007 for Vista is nothing short of a positive review onto itself of the security and code quality of the platform. According to statistics made

available by Microsoft, the first half of 2007 brought with it in excess of 3,400 new vulnerabilities across the industry. Vista may be swimming in "shark infested waters" but it is not positioned as a perfect item of prey, and the small amount of security patches are an argument in this regard. **Counting Security Holes** While the volume of vulnerabilities decreased in the first half of 2007 compared to the last half of 2006, down by 4.6%, the vast majority of the new security holes were rated as critical, and experienced an ascendant trend. This translates into a new trend for the threat environment that now tends to focus increasingly on High severity vulnerabilities that permit by definition the complete takeover of an attacked system. In addition, attackers are also continuing to simplify exploits. The easier it is to exploit a security flaw, the higher the risk to the end user. At the same time, more complex exploits are easier to mitigate. And yet another factor that directly influences the risk level is public availability of exploit code. Microsoft informed that in the past couple of years, just 26% of vulnerabilities had public proof-of-concept code available in the wild. The Redmond company additionally pointed out that starting with 2004, the threat environment is less focused on operating systems, be them Windows, Mac OS X, Linux or Unix, indicating "a decreasing percentage of vulnerabilities are from operating systems. One possible interpretation of this trend is that security vulnerability researchers are focusing more on applications, as operating system security continues to improve. An alternate explanation could be that the number of new applications is growing far faster than the number of new operating systems and that the application proliferation is simply reflected in the vulnerability disclosure trend," Microsoft stated. **Vista or No Vista, It's Still Windows** In the end security is a cocktail of aspects raging from code quality, as it results from the development process, the level of activity of the threat environment and the exposure of the software. Even since the business launch of its latest operating system Microsoft was confronted with the problem of malware infecting Vista. More explicitly, at that time, without any actual Vista designed threats, the Redmond company had to deal with the risks of compromising delivered by legacy malicious code. To some extent, as Sophos has shown, Windows Vista is by no means [immune to legacy malware](#). However, [a later report from Symantec](#) indicated that Vista can get away quite immaculate, although it warned that the threat environment will adapt to the new operating system with specific threats. Microsoft too confirmed that that Vista is not a silver bullet solution, and urged end users to adopt a security solution. "Infection rates observed by the Microsoft Windows Malicious Software Removal Tool (MSRT) are significantly lower on Microsoft Windows XP Service Pack 2 (SP2) and Windows Vista compared to older operating systems. Moreover, the MSRT has proportionally cleaned malware from 60.0 percent less Windows Vista-based computers compared to computers running Windows XP SP2. Similarly, the MSRT has proportionally cleaned malware from 91.5 percent less Windows Vista-based computers than from computers running Windows XP without any service pack installed," the company claimed in the Security Intelligence Report. **Vista vs. XP** According to the numbers harvested by the Malicious Software Removal Tool, the volume of Vista machines disinfected in the first half of this year is 60% smaller than that of XP machines. The comparison was of course made between Vista and XP with Service Pack 2 installed. The numbers read a tad differently when it comes down to taking into consideration the original release of Windows XP without any service pack installed. In this context, Microsoft disclosed that MSRT cleaned 91.5% less Vista operating systems than XP stripped of the additional service packs. And on top of it all, the statistics for Vista are even more encouraging when the users run with the User Account Control enabled, not permitting the installation of malicious code requiring administrative privileges involved in social engineering schemes. "Windows Defender has proportionally detected 2.8 times less potentially unwanted software on computers running Windows Vista than on computers running Windows XP SP2, based on the normalized data. Likewise, the number of detections of potentially unwanted software on computers running Windows Vista was half of the number of detections of potentially unwanted software on computers running Windows Server 2003, after normalization. It is worth noting

that proper use of Internet Explorer security zones can have a profoundly positive impact on security," Microsoft stated. **The Grass Is Greener and More Secure on the Vista Pasture** According to Microsoft the grass is greener and more secure on the Windows Vista pasture, compared to Windows XP. The company's position is understandable, first of all as a marketing campaign designed to educate the users. In the end security is a matter of perspective and perception. And with Vista, along with additional endeavors such as Windows Live OneCare and the Forefront line as a foundation, Microsoft is attempting to build a strong reputation on the security market, one that has been missing from the company's portfolio so far. And in this context the sheer differences between Vista and XP without any SP speak from themselves as to Microsoft's commitment to protecting its users. "Windows Vista will continue to make a difference in the PC ecosystem. At this point in the life cycle, we see that Windows Vista has fewer security vulnerabilities reported to this point and that we find far less malware on it than on previous versions of Windows. I'm not claiming that Windows Vista is perfect-no software is. However, all of the focus that Microsoft put on security while developing Windows Vista definitely decreases the likelihood of a successful attack on a Windows Vista-based system, due to a vulnerability or bug in the software, and more likely from a socially engineered attack," concluded Vinny Gullotto, General Manager, Microsoft Malware Protection Center.