

24 May 2008

By: Marius Oiaga, Technology News Editor

## [Dissecting Microsoft's Vista SP1 vs. XP SP3 Feature Smackdown](#)

*XP SP3 is viewed as a milestone to Vista SP1*



Windows XP -  
Windows Vista  
Microsoft

At the end of April, just as Microsoft had released Windows XP SP3 to manufacturing, and with Windows Vista SP1 RTM'd since February, the face-off between the two operating systems simply went to the next stage. Now, Microsoft has hardly been a stranger to comparisons involving its Windows clients available on the market, and the [XP Professional vs. Vista Business](#) or the [feature comparison between Vista editions](#) are illustrative examples in this respect. For the Redmond company the release of the latest service packs proved nothing more than an opportunity for a new operating system measuring contest. Microsoft's latest Windows Feature Comparison involves Windows XP SP3 Professional and an unspecified edition of Windows Vista, but because of references to Windows BitLocker Drive Encryption, it has to be at least the Enterprise SKU if not the Ultimate edition. Microsoft has taken into account features connected intimately with the security, management, deployment, mobility and productivity facets of the two products. As far as Microsoft is concerned, placing Vista SP1 and XP SP3 under the same microscope can only benefit its latest Windows platform. The Redmond company is of course dealing with the strong momentum of XP on the operating system market. Vista did top the 140 million sold licenses milestone by the end of March 2008, grabbing over 14% of the market according to Net Applications, but XP still holds the lion's share with over 70%, and by all signals it is here to stay. The combination of extended support planned until 2014 and Service Pack 3 make Windows XP a formidable obstacle in the way of Vista's adoption. Microsoft is reliable in the perspective that it is delivering a superior operating system with Vista as compared to XP, and that SP1 comes only to improve the quality and performance of the product. More so than anything else, the Redmond company knows that this is the right time to push hard for broad enterprise deployments of Vista. SP1 is traditionally regarded as a maturity milestone for the Windows client and Vista makes no exception to this rule, with corporate migrations bound to pick up even if only through hardware refreshes as XP availability via OEM and retail channels will end this summer. Microsoft simply has to make sure that XP SP3 is not viewed as an equivalent to, or a viable alternative of Vista SP1. This is the role of the [Windows Vista SP1 vs. Windows XP Professional SP3 feature comparison](#). **My Vista Is Secure!** If there is one drum that Microsoft has beaten relentlessly since the advent of Vista, it is the superior level of security the latest Windows client brings to the table. The Security Development Lifecycle (SDL), defense in depth, Windows BitLocker Drive Encryption, Windows Firewall, Internet Explorer 7 Protected Mode and the ActiveX Installer Service are the security features enumerated by Microsoft as advantages Vista has over XP. "The Microsoft SDL makes security a top priority throughout the development cycle by mandating a repeatable engineering process that every developer must follow, and by verifying that process before product release", the company stated. "The SDL is an evolving process that implements rigorous standards of secure design, coding, testing, review, and response for all Microsoft products. The SDL helps remove vulnerabilities and minimize the surface area for attacks, improves system and application integrity, and helps organizations more securely manage and isolate their networks." Windows Vista is the first Windows client to be developed entirely under the SDL. And the results have already been demonstrated repeatedly throughout 2007 by [Jeff Jones](#), a Security Strategy Director in Microsoft's Trustworthy Computing group, at least in respect to Vista vs. XP. But Vista's security improvements are not limited to code quality, because SDL is in the end a way to reduce the volume of vulnerability, as well as ensure that the flaws that do get through will pose only a low risk to end users. At the same time, Vista also

delivers advanced protection against buffer overruns."In Windows Vista, DEP is enabled by default for most components. Windows Vista introduces additional DEP policies that allow software developers to enable DEP in code, independent of system-wide compatibility-enforcement controls", Microsoft explained. "DEP works best with Address Space Layout Randomization (ASLR), another defense capability in Windows Vista that makes it more difficult for malicious code to exploit a system function."Vista also delivers service hardening, a move that has made system services run with the least possible privileges. By comparison, In Windows XP SP3 DEP is not even enabled by default and mitigations such as Address Space Layout Randomization and service hardening are non-existent. BitLocker Drive Encryption is also a feature exclusive to Vista, namely to the Ultimate and Enterprise editions, and also not available in XP is the ActiveX Installer Service. "With Windows Vista, IT pros can now easily deploy and update ActiveX controls in a standard user environment. The ActiveX Installer Service enables IT pros to use Group Policy to define approved host URLs that standard users can then use to install ActiveX controls", Microsoft informed. Both [Vista SP1](#) and XP SP3 deliver a default Windows Firewall, but this cannot be considered anything more than a basic feature and should not be relied on to keep the operating systems safe by itself. But what is an excellent and often overlooked security feature for Vista is IE7 Protect Mode. Getting IE7 to run with the least possible privileges under the User Account Control is without a doubt an advance in terms of security. But what Microsoft fails to tell end users is that all the extra security features in Vista are nothing more than mitigations. Neither IE7 Protect Mode nor ASLR or all the other features are security boundaries. This means that they can be bypassed or hacked. Do they add value to Vista? By all means! And even more than what XP SP3 has to offer, but Microsoft has yet to revolutionize the security of Windows and probably will fail because of the need to not break all connections between the operating system and the environment of software and hardware products built around it. **My Vista Handles Better!**In terms of management Vista offers advances in terms of Group Policy settings, standard user accounts, reliability and diagnostics, event management and task scheduling. "Windows Vista has more than 500 additional Group Policy settings compared to Windows XP", Microsoft stated. "In Windows Vista, Group Policy settings are better targeted at specific scenarios, such as wireless networking, power management, removable storage, and printer management."Microsoft's view is that User Account Control as a management feature succeeded in making users with standard privileges... well, a standard. But in the end UAC is also a security mitigation, whatever benefits it might bring to system administrators that need to restrict user privileges. But true management features are related to reliability and diagnostics. "Windows Vista includes built-in diagnostics that automatically detect and diagnose common support problems and help users resolve the problems on their own. Problems that Windows Vista diagnostics address include failing disks, degraded performance, lack of network connectivity, and failure to start up properly", Microsoft revealed. Vista also delivers a new Windows Eventing system designed to permit IT professionals to troubleshoot problems by extracting information from the event logs. And while in XP the task scheduling capabilities were nothing short of basic, Vista permits an entire new level of flexibility in this respect. **My Vista Deploys Better!**Image-based setup (IBS); deployment, compatibility and asset-inventory tools; the Windows Setup and worldwide single-image deployment account for the evolution of Vista SP1 in comparison to [XP SP3](#). IBS refers to the new way to distribute Vista, via the Windows Imaging Format. Perhaps the biggest advantage of WIM over other image file formats is the fact that it's file-based and hardware independent. Still, through its deployment tools Microsoft does support WIM images for Windows XP, even if not at the same level of offline-servicing as Vista. "Windows Vista provides a new set of deployment tools. Some of these tools, such as Sysprep, now ship as core parts of the operating system. The remaining tools are in the Windows AIK and include Windows PE 2.1, Windows System Image Manager (Windows SIM), and ImageX. These tools are optimized so that business customers can reduce the

number of images they maintain and so that servicing those images is easier. And MDT 2008-the next version of Microsoft Business Desktop Deployment (BDD)-takes full advantage of Windows Vista's deployment improvements", Microsoft added. **My Vista Is Mobile!**Through the Windows Mobility Center, Sync Center, improved offline file and folder management, Network Projection, Secure Sockets Tunnel Protocol (SSTP), wireless networking and power management, Microsoft touts Vista SP1 as superior to XP SP3. The Windows Mobility Center and the Sync Center are centralized locations from where end users can access all the mobility and synchronization options without having to hunt for them. At the same time Vista delivers a tad extra when it comes down to offline file and folder synchronization via the Delta Sync protocol. Vista is also more aware than XP in terms of power usage. Additionally with Vista SP1, Microsoft delivers support for the latest wireless security protocols, such as Wi-Fi Protected Access 2 (WPA2). "SSTP is a new tunneling protocol that uses Hypertext Transfer Protocol (HTTP) encapsulation over a Secure Sockets Layer (SSL) channel. Because SSTP uses SSL traffic (TCP port 443), SSTP can be used in many different network configurations-for example, when VPN clients or servers are behind network address translation (NAT) devices, firewalls, or proxy servers. SSTP requires Windows Server 2008 and Windows Vista with SP1", the Redmond company explained. **My Vista Is Productive!**Advanced productivity is one of the promises Microsoft made with Windows Vista. A revamped graphical user interface complete with desktop search, an overhauled Start Menu and a redesigned Windows Explorer are all meant to deliver a boost in productivity. However, Vista's biggest problem in this respect is performance. The operating system needs a sturdy hardware infrastructure to say the least in order to deliver its full kick, and will perform poorly on machines tailored in accordance with XP's specifications. This is one aspect where Vista's productivity suffers despite the additional advances delivered to the operating system.