# Windows 7 security: A great leap forward or business as usual?

The public release of Windows 7 is approaching fast. Debates and discussions have been raging on the security improvements in the new platform, and some potential problems have also emerged. In this white paper, we run through the most significant changes and additions, and look at what they might mean to users and administrators.

by Chester Wisniewski, Senior Security Advisor, Sophos

A Sophos white paper

September 2009

# Windows 7 security: A great leap forward or business as usual?

## Can Windows 7 succeed where Vista didn't?

The much-heralded Windows Vista had a mediocre reception on its initial release, and never really took off despite great efforts from Microsoft to encourage hardware vendors to use it. Many businesses, wary of numerous issues, opted to stick to the tried and trusted XP until the new platform stabilized with service packs and upgrades.

But Microsoft took a different course – it rushed to create a replacement platform.

The upgrades included with Vista focused on visuals and certain speed improvements. But the platform introduced a number of new or improved security features, most notable of which was the User Account Control (UAC) system, which was designed to prevent unauthorized execution of code. UAC was widely criticized for its intrusive popups, and its reliance on the understanding of a largely untrained user base that is more likely to ignore or disable the alerts than to take the time to decipher their meaning.

Some other minor additions, such as basic encryption with BitLocker and the Address Space Randomization system, provided a little extra security, while some items such as the one-way firewall and the Security Center remained largely unchanged.

With Windows 7, Microsoft showed that it is paying attention to its critics and has attempted to deal with a number of these issues.

Some of the changes are largely cosmetic, with further upgrades to the desktop look and feel that continue the direction taken by Vista, following the lead of a certain rival operating system with a far better reputation for glossy visual appeal and user-friendly design.

Under the hood, there are new additions and serious upgrades to previous security measures that offer the promise of greater security as well as ease of use. Microsoft overhauled the interface between users and Vista's security controls with the Vista Security Center becoming the more fun-sounding, if a bit ambiguous, Action Center. In addition, the company redesigned the UAC, expanded the firewall into a more complete feature and extended encryption. Microsoft also promises a new user-friendly VPN system.

The implementation and completeness of these new ideas will be significant factors in Windows 7 gaining traction with users and IT departments that have resisted upgrading their systems. For the many that have waited so long, upgrades are no longer a choice. Microsoft hopes to avoid a repeat of the Vista experience—so marketing and sales will be pushing hard on customers to upgrade to Windows 7. It is almost certain that Windows 7 will push XP aside. Therefore, the safety level of the new platform will have a massive influence on computer users worldwide, whether they like it or not.

## Action stations: Windows Security Center rebadged but not replaced?

Microsoft introduced Windows Security Center with XP and it has remained largely unchanged ever since. With Windows 7 it has been given a major revamp. The new Action Center combines the existing management and control of the firewall, updating and anti-malware protection with a selection of additional system maintenance tasks, including backup, troubleshooting, anti-spyware, UAC and the general state of network security settings.

Windows Vista Users accustomed to the constant stream of alert popups and the old system tray shield badge will experience the biggest change. Windows 7 presents more detailed listings of potential issues, which often come with useful information and advice. Integration with anti-malware solutions is much more granular, enabling products to inform the operating system when they need updating. In Vista, the only information the Security Center could provide was "out of date" or "more than 30 days out of date." Products can also feed their own customized information to users, enabling them to make more informed choices, and users gain a level of customization (e.g., they can disable functions they are not interested in monitoring).

The new Action Center icon looks like a waving flag; it features a small red mark when something important needs fixing. At first glance it seems like a good idea to do away with the popups, which became almost invisible for many users thanks to their frequent appearance. But the flag icon could be a step too far: The new alerting system may be so obscure as to be rendered useless.

The improved integration and control, and more granular messaging, will help most users and security solution developers. However, striking the right balance between keeping users informed and flooding them with irritating alerts remains tricky.

## Access denied: UAC simplified, but still ruined by pester power?

As part of the Action Center lineup (and therefore a core security feature of the platform), the UAC system has also had a radical revision to minimize its impact on the user. In Vista, where it first appeared, the system quickly became notorious for presenting an excess of intrusive alerts and demands for confirmation, which quickly turned off users who consequently turned off the system. Changes to system settings were the main cause of these—rather than new software installations or installed programs trying to adjust a setting (when alerts are more expected and in some cases even appreciated). The new system has a finer level of controls than the simple on or off of the earlier version; it defaults to prompting only when third-party programs try to make changes and allowing changes initiated by the user. A simpler slider system enables a user to set more or less strict protection with ease. In addition, the occasionally rather scary dimming (and often brief blacking out) of the screen that accompanies the alerts by default can also be disabled. Microsoft also redesigned popups to be more informative.

Microsoft promised a significant decrease in the number of popups, and, indeed, the popups in Windows 7 now have improved information on exactly what is being permitted—so it should make the system more effective. However, it is unclear whether many users will use the system correctly—that's because most users lack the understanding required to make informed calls, and many are unlikely to think beyond simply making the popup disappear. On a standard desktop running with the "protected administrator" default user, making the popup disappear is as simple as clicking yes or no; the default selection is no, so users who have trained themselves to simply hit the Enter key will find themselves protected from unwanted changes and most likely frustrated by non-functional software.

Another issue with these default settings is that malware could bypass the system by injecting itself into a trusted application and running from there. Indeed, some malware has been observed spoofing UAC-style prompts to obtain user permission to operate unimpeded.

The system is improved from its previous, barely usable state. But it still lacks the features of platforms with more ground-up security models, where such alerts generally provide adequate context and detail so users can grasp exactly what is being asked and require an administrator password even from a logged on administrator—which forces users to consider what they are allowing and take responsibility for their own safety. The UAC concept is user-driven rather than expert-driven, so it is a questionable approach in a world where end-user expertise is rare. Although personal files and tools will require user approval and operation, core system assets should be more rigorously protected.

## Border control: Windows Firewall finally fully functional?

One of the most significant security improvements introduced in the XP era was the Windows Firewall. Initial off-by-default versions proved entirely inadequate, so with SP2 Microsoft made a major step change in the security of users worldwide by providing firewalling as a standard feature.

Of course, with only inbound protection rather than the bidirectional control provided by proper firewall solutions, it was far from ideal. Although the basic stateful packet-filtering provided some protection from common exploits, it lacked any advanced features; and without central management, policy enforcement and auditing were unsuitable for serious business networks. For most well-informed administrators, it was just another thing to disable before rolling out more comprehensive protection. If nothing else, though, it gave the inexpert, or just lazy, everyday home user a bare-bones level of protection from many forms of attack.

With the new OS, Windows Firewall finally comes of age. The new version provides appropriate inbound and outbound port and protocol filtering including IPv6 support and a raft of features. Detailed user-level configuration is available, but at the corporate network level the improvements are even more significant, with complete management and reporting well integrated into the group policy subsystem.

This all sounds like a major boon to home and business users, but it depends on how broadly it's adopted, which in turn depends on how willing people are to adapt long-standing security practices. Home users—again, all but the most ill-informed—are using their internet security suites to provide both anti-malware and firewalling, generally with specialist firewall design and integration with behavioral anti-malware providing a much higher level of protection. At the business level, similar practices will apply in most cases, with providers of corporate security solutions bundling desktop firewalling with their other protective layers and providing their own centralized management and reporting systems. Security admin specialists will be charged with monitoring and maintaining all protection in bigger networks. In addition, they will still have to control anti-malware, NAC and other security implementations that are not so well integrated into Microsoft's own control systems. Security specialists may also face a steep learning curve with the Group Policy Object management style (although it's familiar to user-level software and policy administrators, and suited to their needs) because it's so unlike standard workflow patterns in existing security management systems, which are specifically designed to cope with the complex needs of firewall configuration.

For most home and work users, splitting the task of security management between multiple tools, usage layouts and support systems will be a pretty obvious timewaster. The use of firewalls from existing, trusted providers seems likely to remain the norm for the foreseeable future.

## Tunnel ahead: DirectAccess, a simple VPN for all?

For corporate administrators, one of the most interesting new security features in Windows 7 is likely to be the new DirectAccess system, which is essentially a built-in VPN client designed to allow users to "simply and more securely access corporate resources when out of the office" (source: Microsoft Windows 7 main page). It is intended to be fully integrated, always on and compatible with firewalls and NAT setups, and to allow both remote access to corporate networks and remote management of logged-in systems by network admins. Remote users are growing ever more commonplace and the issues they present to network security administrators expand in complexity along with their numbers and requirements. Microsoft has recognized the need for major improvements in remote connectivity, so it appears that it will make it very simple and easy to stay safe on the road.

However, there are some major implementation and security issues here. The first big stumbling block an admin will hit when trying to implement DirectAccess is its complete reliance on IPv6. Although theoretically a much superior and more scalable technology to IPv4, IPv6 has yet to make much if any headway in the real world. This means that admins will need to implement IPv6 both on workstations and on the corporate networks, with the inevitable associated learning curve and security lapses when implementing complex and unfamiliar technology for the first time. The alternative, as recommended by Microsoft, is to implement translation technologies at both the workstation and server sides, likely to require different tools and systems for the two, with the associated additional overhead and several more levels of complexity for the administrator – and of course the additional security risk that complexity brings.

Those persuaded to bite the bullet and become early adopters of IPv6 should remember the lessons of the IPv4 introduction – when large numbers of severe vulnerabilities were discovered. It seems inevitable that similar issues will be found with IPv6 when the user base has built up and stumbled across them, and early adopters will be embroiled in a taxing cycle of firefighting and patching until the bugs are ironed out.

There are also some potential dangers in the way Microsoft recommends using the system, which is intended to tunnel traffic securely into corporate networks but allow other activities such as web browsing to use the machine's typical (usually wireless) connection, presumably to save on corporate resources. This approach will immediately sound alarm bells with security-conscious admins who see such a setup as an open bridge between their carefully protected networks and the threat-riddled frontiers of the internet. In other words, this approach should be avoided at all costs.

When IPv6 finally becomes the norm, this system will be a great leap forward. But it is premature and somewhat lacking in completeness of vision, so serious network admins will stick with their existing VPN providers for some time to come.

## Locked out: BitLocker, a business-ready encryption system?

BitLocker disk encryption, which was introduced in Vista, has been somewhat extended and improved in Windows 7. Again, it is included only in the Enterprise and Ultimate editions. It has some hardware requirements as well, including a compatible BIOS and a separate unencrypted boot partition from which to access the encrypted system drive. For optimum performance, a trusted platform module that provides a range of services like tamper protection to allow trusted boot, key storage and basic cryptographic functions, is recommended. In its Transparent Operation Mode, it provides little more than integrity checking on boot, with decryption failing, or at least requiring additional confirmation before proceeding, if unauthorized modifications have been made. The User Authentication Mode offers a more secure level of encryption, requiring a user password or a key stored on a USB drive before the protected system or other volumes are decrypted.

Windows 7 includes an additional set of functionality for encrypting USB removable drives, which should be compatible with Windows Vista without changes. XP users will require a new plugin to access data stored on encrypted key drives, which will at least allow read access. The plugin will only provide protection when the drive is disconnected from the machine; when plugged in, all data on the drive is vulnerable to harvesting if the machine is compromised by malware.

Similar to its improvements in the firewall, Microsoft appears to have done a good job of providing a quality encryption system built in to its operating system. But, again, similar to the situation with its firewall, it remains to be seen if the company, which still has long-standing problems inspiring trust on security matters, will persuade admins to migrate from their existing, well-known and trusted expert cryptography providers. Management remains a key issue, with the implementation of centralized key management and disaster recovery lagging well behind the solid implementation at the local level.

Related to BitLocker in name only, AppLocker provides a basic whitelisting system designed to allow only approved software to run on Windows 7 systems. Available only in the Enterprise and Ultimate editions, it is manageable via the Group Policy model.

## More or less: Other security benefits and potential pitfalls

Admins considering implementing Windows 7 in a corporate environment should review a number of other areas where they'll encounter some good points and some hazards.

Some have highlighted the built-in XP mode virtualization system, which provides full compatibility with older software, as a great benefit to users. Others have pointed out the potential security drawbacks – with good reason. There is little centralized management available for XP mode virtual systems. Moreover, as with any virtual machine, the guest system will require all the usual patch management and client security software to keep it safe. Many inexperienced users think virtual guest systems are protected by the security of the host – not subject to their own patching and anti-malware requirements. Therefore, these users tend to leave these virtual guest systems open to attack and infestation, so significant use of such systems by home users may lead to the growth of infected machines attacking the rest of the world.

In a corporate setting, there appears to be little need for XP mode because most professional software runs without difficulty on native Windows 7. The main target of XP mode appears to be gamers clinging to aged favorites. Most admins should simply disable XP mode in the corporate desktops; and those who must allow it should follow the usual requirements for virtualization, with all the extra work of patching and client-side security conducted as scrupulously as possible.

There have been rumors that European anti-trust regulations may force Microsoft to provide a so-called "E Edition" for the European marketplace. This edition will enable users to select from a range of leading browsers during installation, with the operating system opened up somewhat to allow it to function without Internet Explorer. Although this may be of interest to home users intrigued by the perceived added security and usability of some browsers, corporate software management is generally better served by Microsoft's regular, if often rather tardy, patching system. Moreover, few businesses will be prepared to fully trust the relatively under-supported open-source alternatives for the time being. For most, using IE as a default and alternatives available as secondary browsers if required is likely to remain the standard.

Microsoft has been heavily criticized for some time for stubbornly clinging to the default setting in most Windows releases to hide file extensions, which has been exploited by malware authors for many years to disguise their wares as something other than what they are. The issue has been around since Windows NT, and is widely regarded as one of the simplest moves Microsoft could make to show it is serious about keeping its users away from malware.

The password authentication model presents a major stumbling block to Microsoft's highly valued usability, and the company seems to have recognized that the model also has flaws as a security system. One addition to Windows 7 that seems likely to be universally welcomed is the built-in support for biometric devices. It handles fingerprint readers and comes with API access for developers of other types of biometric identification.

A growing number of devices now have integrated fingerprint readers. Although the readers have been implemented with varying degrees of success, this could move authentication away from the easily cracked or stolen password model toward more personal, unique and certain ways of confirming identities. The success or failure of this new model will depend greatly on the close integration of devices with platforms, software and web services, and Microsoft has taken an important step toward providing its end of this package.

## With all these new features, will Windows 7 keep me safe?

Whether its motivation arises from a genuine desire to do things better or simply a sensible business case for appearing more credible on security issues, Microsoft has attempted to move closer to an appropriate security model. The company has provided some interesting and useful tools to assist its users and network admins in maintaining control over their systems and data. However, many of these new tools have flaws of one kind or another – and some show serious shortcomings in completeness of vision and thoroughness of implementation. Still others seem like excellent and complete packages waiting only for the rest of the world to be in a position to use them.

Of course, we never expected the new platform to do away with the need for anti-malware and other security and control solutions. But at least Microsoft will be covering most of the security issues for its wide user base of under-educated, under-motivated home users once its new Security Essentials free desktop anti-malware arrives.

Most businesses will stick to third-party expert security providers. But it's possible the decrease in numbers of easy targets elsewhere will reduce the numbers of zombies, spam bots and DDoS contributors pumping spam and malicious attacks toward our networks.

You can read more about the security issues that impact IT professionals on Chester Wisniewski’s blog:
**http://www.sophos.com/blogs/chetw/**

Boston, USA | Oxford, UK

SOPHOS
WWW.SOPHOS.COM