SOPHOS

Windows Vista:
Is it secure enough for business?

Five years after the release of Windows XP, Microsoft's primary stated goal with Windows Vista has been to reduce security vulnerabilities and overall susceptibility to malware and other threats. A number of new security features have been introduced in an attempt to reflect the heightened priority of security. This paper describes Windows Vista security, provides an insight into the level of protection it provides for business users, and assesses how far the new features measure up to Microsoft's aspirations for its new desktop operating system.

A Sophos white paper

November 2006

Windows Vista:
Is it secure enough for business?

Overview

Microsoft's latest desktop operating system, Windows Vista, contains a wide range of new features, from the user interface to the heart of the operating system. However, it is the new security-related technologies which were given top priority by Microsoft in response to the many criticisms of the vulnerabilities in Vista's forerunner, Windows XP. Developments include improved monitoring and reporting on security status, minimized opportunity for attack and improved defense against spyware. There is also a new mechanism to prevent rogue code from being able to make malicious changes to the operating system kernel, and improved browser and firewall functionality.

> *If you look at our investment in the next version of Windows [Vista], security would jump out as the thing we've spent the most time on – Microsoft has a big responsibility here.*
>
> *Bill Gates, RSA Conference 2006, San Jose*

Windows Security Center

Windows Security Center (WSC) runs in the background, monitoring and reporting on the security status of a computer. First introduced by Microsoft in Windows XP Service Pack 2, the enhanced version in Vista provides greater integration both with other Vista security features and with third-party security solutions.

As with Windows XP, WSC monitors the internet firewall and checks the status of automatic updates and anti-virus software but it has been extended in Vista to include monitoring of anti-spyware applications. Monitoring of the security settings in Internet Explorer 7 and of the new User Account Control function (see below) has also been added.

Part of the reasoning behind the enhancements to WSC is to raise end-user awareness of security issues by alerting them to any problems. While this clearly has home-user benefits, businesses and other organizations like education and government institutions will find this both insufficient and annoying and so might well choose to disable these end-user alerts.

In addition, some security vendors have reacted negatively to the fact that WSC cannot be automatically disabled when their alternative security solutions are installed, although Sophos cannot see why any vendor should object to a built-in security center reporting on the status of its software.

User Account Control

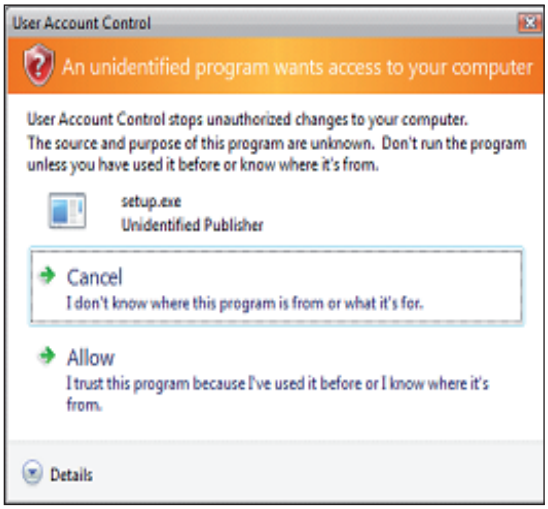
User Account Control (UAC) is one of the most important security features in Windows Vista. Its objective is to minimize the opportunity for attack, preventing the installation of today's malware threats, in a scenario where end users are given local administrator rights. As with Windows XP,

end users are given administrator rights by default. However, instead of invoking administrator status in a blanket fashion across all applications, the Vista login generates two security tokens: StandardUser and Administrator.

By default, Vista assigns the StandardUser token to applications, so applications that do not require administrator rights will run with no user intervention. However, many applications require administrator privileges and in this case the Administrator token is invoked and the user is asked to cancel or allow the program as appropriate, as shown on this page.

> *One thing is clear: Microsoft has to deal decisively with the perception that UAC imposes an unacceptable trade-off between performance and security. In its current incarnation, too many people are likely to dismiss it completely, and if that happens, everyone loses.*
>
> *Ed Bott's Microsoft Report*[1]

From a security point of view UAC is a significant step forward and the principle of the least required privilege is theoretically a good one as, by default, registry and file system access are restricted. This means that malware is prevented from automatically copying itself to locations such as the Windows system folder and cannot be written to registry keys in order to be automatically launched by the operating system. The principle of the StandardUser token also prevents malicious applications from writing to the memory space of other processes, a technique commonly used by malware to bypass personal or client firewalls.



Vista's UAC: adding a layer of security

Unfortunately UAC is not just secure but intrusive, with a high level of alerts, many of which are not intuitive for non-technical users. The danger is that they will automatically select "Allow" when prompted, without fully considering whether they should. The other danger is that UAC can be disabled – and indeed many beta testers chose to do this – which removes the improved security.

Windows Defender

Windows Defender is a free anti-spyware program built into Windows Vista that will detect and remove some adware, spyware and other unwanted programs. The software uses automatic updates provided by Microsoft analysts to help detect and remove new threats as they are identified. This protection does not offer comprehensive anti-malware protection, in spite of the fact that the information in WSC implies that it does.

Windows Defender only supports Windows XP Service Pack 2 or later, or Windows Server 2003 Service Pack 1 or later. It does not support other operating systems including Windows 95/98/Me and 2000. And because it is targeted at the consumer market it does not offer any central administration capabilities. So it offers little to multi-platform, centrally managed enterprise networks.

Kernel protection

Two new mechanisms have been introduced to protect the operating system kernel – Kernel Patch Protection (KPP), or PatchGuard, and mandatory signing of drivers.

KPP has been implemented in 64-bit Vista to prevent a particular type of malicious activity that manipulates the operating system kernel, causing serious security breaches and adversely impacting the stability, reliability and performance of the operating system and user applications. Commonly known as "rootkits" this type of malware is often used to hide other potentially unwanted software, such as bots and spyware. KPP prevents kernel mode drivers from extending or replacing operating system services and should therefore stop rogue drivers from making malicious changes to the kernel.

KPP has not been added to 32-bit Vista since many programs (including security software) use the kernel space in an undocumented way and Microsoft was concerned about compatibility with the existing application set. This means that 32-bit systems remain vulnerable to rootkit attack. However, the second kernel protection mechanism – mandatory signing of drivers – has been implemented in both 32-bit and 64-bit Vista and can be set to prevent unsigned drivers from loading.

Some security vendors have complained that they are being "locked out" of the Vista operating system kernel by KPP. This is because they need to be able to make changes inside Microsoft's kernel in order to ensure their existing products can support 64-bit versions.

While it is true that there will now be some dependency on Microsoft to deliver kernel interfaces which could slow all security vendors down, this is more than compensated for by the additional security offered by a locked down kernel. Windows Vista with KPP is a step in the right direction for customers – although, since this is a software mechanism it is quite likely that it will be circumvented by malware writers sooner or later – and security vendors should embrace and work with it rather than fight it.

Internet Explorer 7

Windows Vista's built-in web browser, Internet Explorer 7 (IE7), includes security enhancements designed to protect users from phishing and spoofing attacks. In protected mode it helps prevent data and configuration settings from being deleted or changed by malicious websites or malware.

Integrity level	Description
Low	Untrusted
Medium	Default for most standard user processes
System	Unrestricted access to the system
High	Administrative process can install files

Four levels of Mandatory Integrity Control

The feature is enforced by a new mechanism, called Mandatory Integrity Control, whereby every process has an integrity level assigned and each level limits access to system objects (registry, file system, other processes. etc).

The new IE7 protected mode actually runs IE with the integrity level "Low" – which is lower than the default for most user processes. This happens for all security zones except the trusted zone. Downloaded programs inherit the low integrity level which should prevent malicious programs and PUAs from infecting the system and integrating with the browser.

IE7 also has a phishing filter, which helps users browse more safely by advising them when websites might be attempting to steal their confidential information. The filter works by analyzing website content, looking for known characteristics of phishing techniques and using a global network of data sources to decide if the website should be trusted.

There is much discussion about Microsoft's attitude to user privacy and many users are concerned that information is being sent to Microsoft. Microsoft's response is that the phishing filter will not send it personally identifiable information. But interestingly, the IP and URL database will be managed by MSN—the same entity that promised its advertisers "unprecedented, rich web demographics."[2]

Windows Firewall

Windows Vista includes a new firewall that goes beyond the Windows XP Service Pack 2 firewall. Application-aware outbound filtering has been added as have location-based profiles, which allow users to set up different rules based on the network location.

However, the default policy is still to allow all outgoing traffic and the default settings will not provide any additional protection over the firewall in XP SP2.

A checklist for securing Windows Vista

You should plan your migration to Windows Vista now because it is fundamentally more secure than its predecessors, although you might like to monitor reports of its quality and stability before setting a date for starting your migration.

1. Install a security solution such as Sophos Anti-Virus to protect against known and unknown malware
2. Ensure Windows Vista is automatically patched against vulnerabilities wherever possible at least for critical security patches
3. Use 64-bit Vista for critical machines because Kernel Patch Protection makes it more secure and it's less likely to be successfully targeted by malware.
4. Make sure your security vendor supports 64-bit versions of Vista; in particular ensure its HIPS (Host Intrusion Prevention System) functionality is 64-bit compatible.
5. Train end users on how to interpret and action User Account Control (UAC) alerts in order to ensure you get the benefit of UAC.
6. Leave Windows Security Center in place as it is of benefit to remote and home workers. But if you have management tools that enable you to monitor the status of your network centrally, consider disabling WSC's end-user alerts.
7. Use a centrally managed security solution, such as Sophos Endpoint Security, that enables you to monitor Vista computers, set and enforce policy, and rapidly identify and fix problems from a single point.

In addition, although some management is available through Group Policy, the central management function does not provide enterprise administrators with the visibility, monitoring, policy configuration and rapid response capability that enterprise-level security management consoles deliver.

Other security features

Windows Vista also includes improved Wi-Fi security, readiness for multi-factor authentication, BitLocker data protection, a Network Access Protection client, and improved auditing for compliance.

In Windows Vista, wireless networking is more secure by default, and includes support for the latest and most secure wireless networking protocol, Wi-Fi Protected Access 2 (WPA2).

Windows Vista comes with an API to make it easier to add smart card and other systems such as biometrics to Windows authentication, to make it harder for hackers to gain access to computers and data through password cracking or social engineering techniques.

Enhanced encryption enables organizations to protect against theft or loss of corporate intellectual property. Windows Vista has improved support for data protection at the document, file, directory, and machine level, including the ability to define which employees have access to certain data. Encryption keys can now be stored on smart cards. The BitLocker disk encryption system provides some protection against hacking attacks that involve booting from removable disks.

The Network Access Protection (NAP) client can be used to prevent rogue or unprotected computers gaining full access to a network, although it will only really be implementable once the necessary server components are released with the next release of Windows Server, codenamed Longhorn, expected to be release late 2007.

Finally, to aid with compliance, Windows Vista monitors and logs accesses to restricted resources for example to enable businesses to identify unauthorized users attempting to access sensitive data.

Conclusion

Microsoft has invested a lot of time and resource into the security push for its new version of Windows. Windows Vista brings a number of positive improvements that means home users will be more secure. However, it is by no means a secure operating system and although it provides increased security against malware, it will not stop it. There is no doubt that Vista-aware malware will appear soon after the release of the operating system. To meet the needs of business users, Microsoft will have to significantly improve its malware expertise and support services, operating system coverage, and central management capabilities. ◆

The Sophos solution

Sophos Anti-Virus for Windows 2000/XP/2003/Vista supports both 32-bit and 64-bit versions of Vista and includes our HIPS technology Behavioral Genotype Protection.

To find out more about Sophos products and how to evaluate them, please visit www.sophos.com

Sources

1 blogs.zdnet.com/Bott/

2 “Microsoft’s Vista won’t stop the Windows security aftermarket”. Yankee Group Research, Inc. May 2006

About Sophos

Sophos is a world leader in integrated threat management solutions purpose-built for business, education and government. With 20 years’ experience and consolidated anti-virus, anti-spyware and anti-spam expertise SophosLabs protects even the most complex networks from known and unknown threats. Our reliably engineered, easy-to-operate products protect over 35 million users in more than 150 countries from viruses, spyware, intrusions, unwanted applications, phishing, spam and email policy abuse. Round-the-clock vigilance has resulted in our increasingly rapid international growth, expanding user base and continuous profitability. Our instant response to new threats is matched by business-focused, 24/7 technical support, and has led to the highest levels of customer satisfaction in the industry.

Boston, USA • Mainz, Germany • Milan, Italy • Oxford, UK • Paris, France
Singapore • Sydney, Australia • Vancouver, Canada • Yokohama, Japan

SOPHOS
WWW.SOPHOS.COM