Global Knowledge™

Expert Reference Series of White Papers

Workstation Security Enhancements in Windows Vista

Workstation Security Enhancements in Windows Vista

Glenn Weadock, Global Knowledge Instructor, MCSE, MCSA, A+

Introduction

It is becoming clearer every year that workstations require as much comprehensive IT security attention as servers – particularly as the popularity of mobile workstations (laptops) continues to rise.

Microsoft has advanced several technologies in Windows Vista to increase workstation security. This white paper introduces eight such technologies:

- User Account Control
- IE7 Protected Mode
- Service Hardening
- Windows Resource Protection
- Windows Defender
- TPM and BitLocker
- Network Access Protection
- PatchGuard and Driver Signing (64-bit platform)

Certainly, Microsoft is doing a lot of interesting things outside the Vista codebase – such as reworking the old standbys Regmon and Filemon into a new (but still free) tool called Process Monitor, and continuing to improve and refine WSUS (Windows Server Update Services) – to help admins stay on top of security threats. This white paper focuses on features that ship with the Vista/ Longhorn code base itself (although not necessarily with all versions).

User Account Control

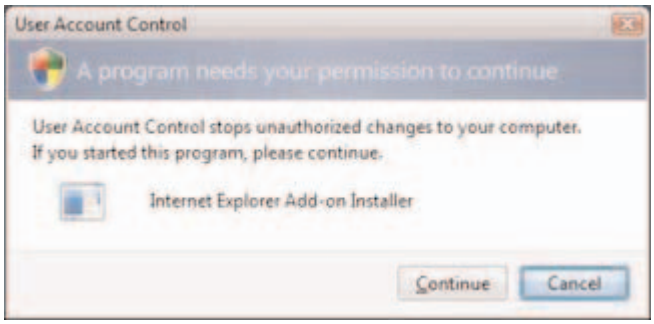

Figure 1. The UAC "confirmation" prompt for a logged-on admin.

This feature, available in all versions of Vista, is probably second only to AERO Glass as the most-discussed Vista innovation. User Account Control, or UAC, was developed to address concerns that viruses and malware can do much more damage to a system when a user is logged on with administrative rights on the local machine, rather than when the user is logged on as a limited or "standard" user. (The concept of the Power User is being phased out in Vista.) UAC is an embodiment of the principle of "least required privilege" – that is, that computers are more secure when users (and services, but we'll get to that in a minute) have the least privilege level required to perform their typical tasks.

With UAC turned on, even when you are logged on as a local administrator, you do not normally execute processes with administrative privileges. If you try to perform an action that does require such privileges, UAC prompts you for confirmation, before elevating your privileges. The desktop goes dark ("secure desktop") and becomes unavailable until you click the Continue button. The idea is to prevent rogue software from doing things you don't want it to do – and, incidentally, to make admins stop to think for a second before executing potentially damaging tasks.

If you are logged on as a standard user, and you try to do something that requires administrative rights, then by default, you will be prompted to provide credentials of an account that does have administrative privileges. You can change this behavior through Group Policy so that non-administrators are simply denied, rather than prompted for credentials.

One "gotcha" with UAC is that it does not integrate with the command prompt. That is, if you open a command prompt normally and perform an action that requires administrative rights, you will simply be denied and not prompted for confirmation, even if you are logged on as a local administrator. You have to think ahead and use the "run as administrator" context-menu option when invoking the command prompt if you intend to perform administrative tasks at the command line.

You can (via Group Policy) modify UAC prompt behavior for the built-in administrator account, as opposed to other non-built-in accounts that you may create and make part of the Administrators group. You can also deploy different UAC settings via Group Policy based on Organizational Unit location in Active Directory, and (with a bit more sleight of hand) based on Windows group membership, through a Group Policy technique called security group filtering. So, before you rush to totally disable this undeniably annoying tool, consider fine-tuning it to see if you can minimize the disruption without giving up the potential benefits entirely.

IE7 Protected Mode

Leveraging User Account Control in the browser, Internet Explorer 7's protected mode option sets up IE to run in a "sandbox" where, basically, the only accessible part of the hard drive for reading and writing is the browser cache in the user's profile. If a program, applet, or control attempts to go outside the sandbox and access the file system or the registry, the user is warned and can permit the action or deny it. The idea is that if IE does happen to run evil code in spite of other protections (firewalls, etc.), the damage will be limited – another example of the "least required privilege" principle.

Actually, IE protected mode uses three levels of privilege: Low, Medium, and High. In protected mode, users (even if logged in as an administrator) run at the Low level. A "user broker" process handles elevation prompts for tasks requiring Medium privilege, and a separate "admin broker" process handles elevation for tasks requiring High privilege (such as installing an ActiveX control).

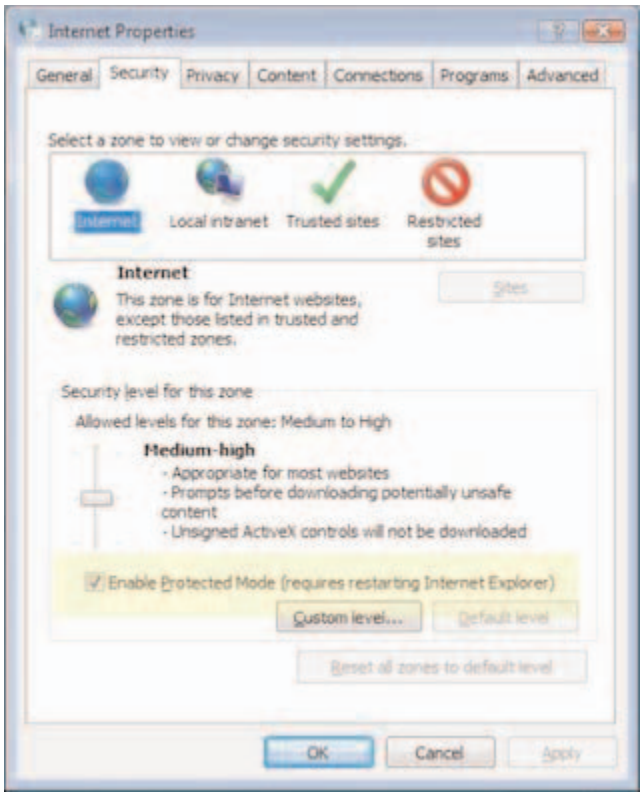

Figure 2. Enabling protected mode for IE.

Note that protected mode, even if enabled, does not apply to locations in the Trusted security zone. Also note that, to improve compatibility, Microsoft virtualizes commonly accessed file and registry locations to per-user profile locations that are safer than the "global" ones. One more "gotcha" is that the built-in administrator account can behave differently than user-created administrator accounts, depending on the UAC settings in Group Policy.

Protected mode is only available in IE7 in combination with Windows Vista, because of its dependence on UAC. However, it is available on all versions of Vista.

Service Hardening

In the past, Windows services (i.e., processes launched by the operating system) have tended to run at a relatively high privilege level (LocalSystem), and certain services are generally loaded in memory at all times. In other words, as targets go, these are pretty attractive! Microsoft has taken some steps to improve the security of services in Vista, making it a bit tougher for the forces of evil to exploit Windows services by piggybacking onto their code. Service hardening doesn't necessarily mean that services will be harder to compromise – just that a service that is compromised won't be able to do as much harm. A worm like Blaster may still infect a service like RPC, but its ability to run rampant will be constrained.

Many services that formerly ran with system privileges now run with local or network privileges, adhering to the principle of least required privilege. Additionally, per-service SIDs (Security Identifiers) allow Microsoft and third-party software vendors to flag file and registry resources to be accessible only to services that need those

resources, using the same sorts of ACLs (Access Control Lists) that have been available in Windows for years, without having to give the services LocalSystem rights. Per-service SIDs also allow the Vista firewall to restrict what specific services are allowed to do in terms of network access. This should help prevent viruses infecting services from spreading across the network – or at least from spreading as quickly. The best news is that Microsoft has already developed service hardening profiles specifying access controls for each service, so these improvements don't require any attention from sysadmins.

Going further, Microsoft has restricted "session zero" (the first session that Windows creates in the Fast User Switching environment, which now extends to domains) to include only services and non-user-specific applications: no user apps can now run in session zero. This protects core system services from user applications, further reducing the attack surface. In Windows XP, the first user to log on to Windows ran his or her apps in session zero; that's no longer the case in Vista, where such apps would run in session one.

Windows Resource Protection

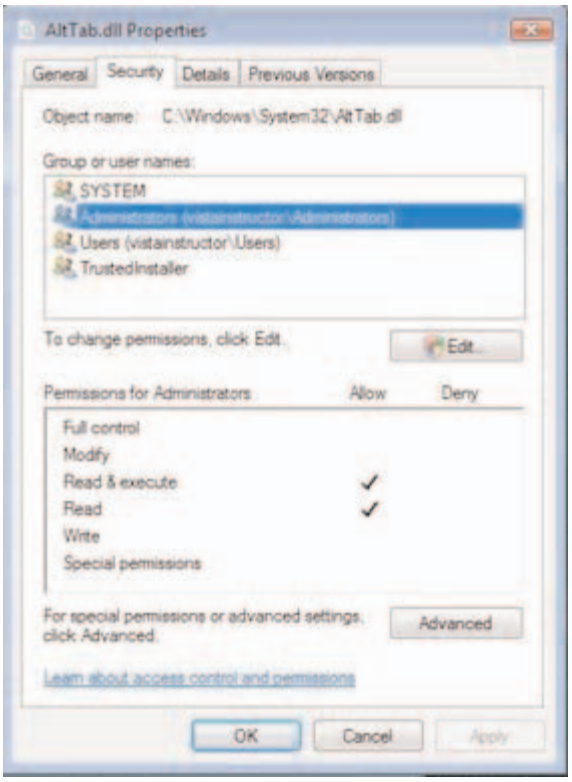

Figure 3. Administrators don't have Modify or Full Control for system files.

Windows 2000 and Windows XP used something called WFP (Windows File Protection) to help ensure the integrity of operating system files. If an application overwrote a system file, WFP would replace it with a known-good copy from a special, compressed folder (Dllcache). This was something of an about-face from the Windows 9x days, in which Microsoft freely granted independent software vendors the right to redistribute updated versions of individual DLLs with their applications, creating the mishmash of DLLs that was responsible for so many blue screens and stomach ulcers.

Windows Vista goes one step further than its immediate predecessors, and prohibits even local administrators from modifying system files. Administrators no longer have full rights to system files, and legacy apps will often find themselves up against a brick wall when attempting to overwrite such files with their own preferred versions. Microsoft refers to this stricter approach as WRP (Windows Resource Protection). Because WRP is better than WFP in that it catches potential problems earlier in the sequence, WFP is no longer included in Windows Vista.

Windows Defender

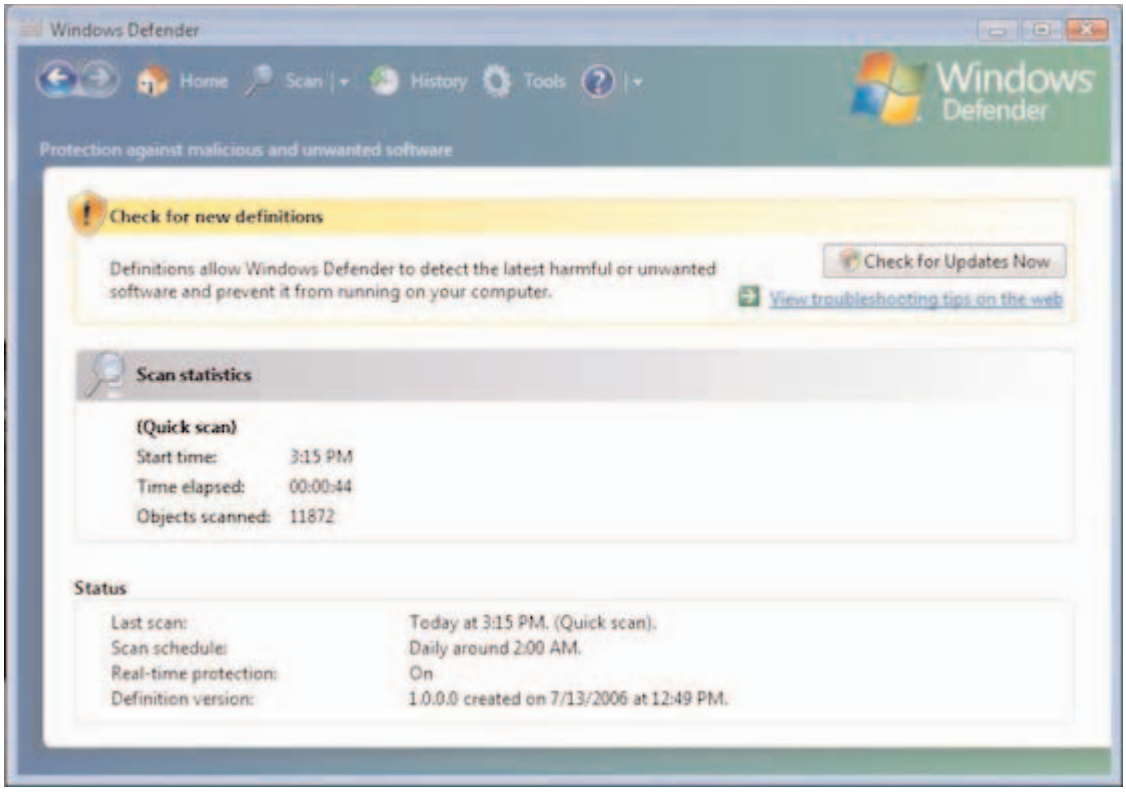

Figure 4. Windows Defender fights malware.

Windows Defender, formerly the Microsoft anti-spyware and anti-malware tool, does just what its name implies and, according to many customers, does it quite well. The tool comes bundled with Windows Vista. Windows Defender also includes Software Explorer, which allows you to browse running processes and services, although in somewhat less detail than available in other administrative tools.

Windows Defender is downloadable and retrofittable to Windows XP. Therefore, you could choose to make it a standard for your organization even if you operate for a time in a mixed-client environment. Additionally, Windows Defender can be mandated by system health policies in organizations deploying NAP (Network Access Protection), discussed later in this paper. And you can deploy a handful of Defender-related settings via Group Policy after installing the windowsdefender.adm template (freely downloadable from Microsoft) into the relevant Group Policy object. Finally, you can use WSUS (Windows Server Update Services) to deploy definition updates to machines running Defender.

TPM and BitLocker

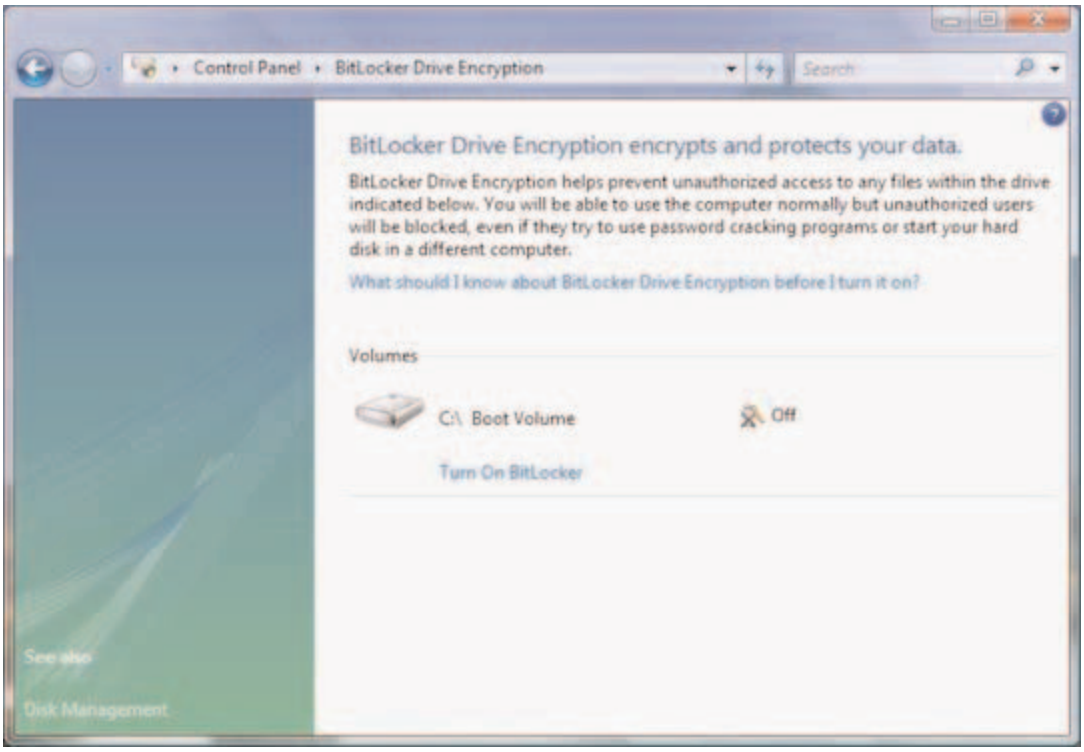

Figure 5. BitLocker = full-drive encryption.

The Encrypting File System, EFS, was a useful method for protecting particularly sensitive files, especially on portable machines. However, it was not transparent to users; they had to take proactive steps to encrypt their folders; hence it was not as widely used as it might have been. BitLocker, new with Vista, encrypts an entire volume.

If the motherboard supports TPM (Trusted Platform Module) v1.2, then the encryption/decryption can be transparent to the user.

Alternatively, on a TPM system, BitLocker can be set to require a PIN before the system will even boot. In the absence of TPM v1.2, a startup key may be stored on a USB flash drive; the key is required to boot Windows Vista.

One benefit of BitLocker is that if someone steals your laptop and attempts to gain access to your files by removing the hard drive and installing it onto a system to which the thief has administrative rights, the hard drive will be inaccessible.

Caution must be taken to maintain adequately secured recovery keys for BitLockered systems – for example, in the event of a motherboard swap, or someone accidentally leaving the flash drive startup device in his jeans during a wash.

Another potential "gotcha" is that BitLocker requires a more complex partitioning scheme than many organizations currently use. You need two partitions for BitLocker. Specifically, you must have an active partition of at least 1.5 GB, and a boot partition (where Windows Vista, programs, and data exist) that actually gets encrypted. The good news is that if you're planning to use the Windows Automated Installation Kit, you can perform automatic disk partitioning prior to installing the OS via answer files created by the System Image Manager.

According to Microsoft's published description of Vista versions, BitLocker is only included with Vista Enterprise and Vista Ultimate. Some companies report having been able to negotiate adding the BitLocker capability to a Vista Business license for additional cost.

Network Access Protection

Network Access Protection, or NAP, is an attractive security capability of Vista in combination with (at least one) Longhorn Server. NAP lets administrators set conditions under which workstations will be allowed to connect to the main network. For example, a laptop user who turned off her firewall over the weekend will not be granted access Monday morning until she turns the firewall back on. Or, even better, the NAP client will automatically turn the firewall back on without her intervention: something called "auto-remediation." (Fixing things automatically is always better than asking the user to fix things.)

NAP also provides for the automatic redirection of "unhealthy" clients to a separate subnet or subdomain, where they could, for example, download security updates in order to bring themselves into compliance with the health policies.

The client-side components of NAP include System Health Agents (SHAs), a Quarantine Agent (which assembles health information from the SHAs), and Quarantine Enforcement Clients (which enforce quarantine on clients that have been deemed unhealthy by a suitably configured Longhorn server). Windows Vista ships with a functioning NAP client. Windows XP can participate in NAP, but to a lesser extent than Vista boxes.

The server-side components include System Health Validators (SHVs), processes that run a Longhorn server that has the Network Policy Server (NPS) service installed; System Health Servers, such as SMS, Tivoli, or Symantec boxes, that feed information to NPS; Network Access Devices, such as switches or DHCP servers; and Remediation Servers, which run in the quarantine network and provide updates to unhealthy clients.

System health policies can be enforced by DHCP running on Longhorn server for clients accessing the network locally, and by the RRAS service for clients accessing the network remotely. Third-party antivirus software vendors are expected to create agents that can extend NAP to include rules for updated virus signatures. Microsoft claims to be working with over 70 partner companies to create agents and remediation servers, and the company is quick to state that NAP is a platform, not a total delivered solution.

In my opinion, the key to NAPs ultimate success in any organization will be the ease of remediation. The first company Vice President who can't log on to the network and who gets frustrated trying to figure out how to update his antivirus signature tables could scuttle the whole concept for everyone. Microsoft is providing the tools, but we'll have to use them carefully to avoid such a scenario.

PatchGuard and Driver Signing

Introduced in Windows Server 2003 SP1 x64 and Windows XP x64, PatchGuard is also a feature of the 64-bit version of Windows Vista (but not 32-bit versions, at least not yet). In a nutshell, it guards against patching the Windows kernel – the core operating system code that defines Microsoft's implementation of the OS, as opposed to its OS interface (the Windows API). Microsoft argues that the kernel's security, reliability, and performance can all be compromised if it is modified by third parties – for example, by a program that redirects system calls to itself ("hooking" into the kernel), or by rootkits that use the kernel to embed software at a nearly undetectable level. That has a big impact on overall security, because the kernel is the lowest, most fundamental level of software in the OS.

Opinions differ: some antivirus firms accustomed to hooking into the kernel have complained (sometimes quite publicly!) that PatchGuard makes life harder for them in their quest to help secure the desktop – for example, in implementing features that resist "retro-viral" attacks that begin by disabling security software. Other observers have opined that if the antivirus software developers rely less on kernel hooks, maybe their products won't slow Windows down quite so much. This debate is likely to continue, but meanwhile, Microsoft is bending; some sort of "PatchGuard API" will be available at some point to antivirus software firms.

Kernel mode software can be engineered to bypass PatchGuard (in fact, it has already been done), which is one reason that Vista x64 also requires that all device drivers be digitally signed either by Microsoft or by a trusted partner (kernel mode signing). While this requirement is sure to limit the hardware compatibility of Vista x64, it should by the same token improve security.

So why didn't Microsoft implement PatchGuard and kernel mode signing in 32-bit Vista? Simple – these steps would break more software than would be acceptable for a mainstream operating system. Vista x64 is enough of a "niche" product that Microsoft felt it could make these changes in that version without as much collateral damage in the form of broken applications.

Conclusion

With Windows Vista, Microsoft continues its multi-year effort to make Windows a secure computing platform. The challenge the company faces is that, with its continued dominance in the operating system space, it remains the biggest target. However, Vista seems highly likely to prove a more secure platform than Windows XP has been, especially if organizations find ways to use the new security features without unduly inconveniencing users – and if we all do not become as numbed to UAC prompts as most of us have become to the near-ubiquitous "Are you sure?" dialog box!

Learn More

Learn more about how you can improve productivity, enhance efficiency, and sharpen your competitive edge. Check out the following Global Knowledge courses:
Migrating to Windows
Vista Implementing and Maintaining Windows Vista

For more information or to register, visit www.globalknowledge.com or call 1-800-COURSES to speak with a sales representative.

Our courses and enhanced, hands-on labs offer practical skills and tips that you can immediately put to use. Our expert instructors draw upon their experiences to help you understand key concepts and how to apply them to your specific work situation. Choose from our more than 700 courses, delivered through Classrooms, e-Learning, and On-site sessions, to meet your IT and management training needs.

About the Author

Glenn Weadock is a longtime instructor for Global Knowledge and co-course-director with Mark Wilkins of the seminars Implementing and Maintaining Microsoft Windows Vista, Migrating to Windows Vista, and Deploying Group Policy. He also consults through his Colorado-based company, Independent Software, Inc., and is the author of 18 computer books.