Global Information Assurance Certification Paper

Interested in learning more about security?

SANS Institute InfoSec Reading Room

Laptop Security: Windows® Vista vs. XP

Laptop Security: Windows® Vista™ vs. XP

GIAC Gold Certification

Author: Gregory F. Hill, ghill@freshbaked.com

Adviser: Joey Niem

Accepted:

Contents

Introduction:..... 4

The Importance of Securing Laptops..... 4

Case 1. The Stolen Laptop..... 5

Case 2. The Compromised Laptop..... 7

Case 3. Insider Stealth Activities..... 8

Windows Vista Technical Information..... 10

TPM (Trusted Platform Module) Chips Support..... 10

Smart card, Biometric Support..... 10

Windows Vista Wireless Enhancements..... 11

Protocols and Core Networking Components..... 11

IEEE 802.11 Wireless Changes and Enhancements..... 12

Network Infrastructure..... 13

User Account Control (UAC)..... 14

Sidebar Gadgets..... 16

Internet Explorer Version 7 (IE7)..... 16

BitLocker™ Drive Encryption..... 17

Encrypting File System (EFS)..... 23

Rights Management Service (RMS)..... 24

Remote Laptop Security (RLS)..... 24

Virtual PC (VPC) 2007..... 24

Windows Defender..... 25

Windows Firewall..... 26

Windows Vista Task Manager..... 27

Windows Service Hardening..... 27

Network Access Protection (NAP)..... 28

Group Policies (GP)..... 29

Windows Security Center..... 30

Address Space Layout Randomizer (ASLR)..... 31

Windows Vista Deployment..... 32

Windows Vista Hardware Requirements..... 33

   Windows Vista Editions 33

   Windows Vista Security Features 34

Summary/Conclusion..... 34

Should Windows Vista be installed on older laptops?..... 34

Works Cited..... 36

Index..... 41

Introduction:

Laptop computers are an irresistible target for criminals, resulting in hundreds of thousands of thefts and millions of electronic intrusions causing billions of dollars in losses. The majority of these computers run the Microsoft XP operating system, which, although containing many security enhancements over its predecessors, is nonetheless frequently compromised.

Microsoft boasts that its new operating system, Windows® Vista™, is significantly more effective at protecting computers, especially laptops. What follows is an examination of the failings of Windows XP and the new and improved features of Windows Vista.

The Importance of Securing Laptops

A recent SANS Newsletter cited securing laptops as the top challenge in the years ahead. [1] The importance of laptop security, both in homes and businesses, is overshadowing all other security concerns because:

- The percentage of laptops to desktops sold is escalating from less than 20% in 2002 to an estimated 50% in 2007. [2]
- Laptops are portable, easily concealed, and are often left in areas where potential thieves have easy access.
- The average laptop is more expensive than the average desktop.[2]
- Sensitive data is often contained on the hard drive to facilitate working without the base network. Here is an illustration from Information Security Magazine: "It's been more than a year since an unattended laptop disappeared

from the U.S. Department of State's Washington, D.C., headquarters. Two top-level administrators were fired and four others received career-ending reprimands for losing a notebook computer that contained sensitive nuclear weapons proliferation data. Despite an intensive investigation and a $25,000 reward, the FBI has been unable to recover the missing laptop." [3]

- Laptops often access outside networks, such as the Internet, using Wi-Fi and cell technologies that are less secure than an attached private network.
- Sophisticated thieves are able to extract credentials from stolen laptops allowing them to access private networks and find and use information to enable identity theft, corporate espionage and other lucrative illegal schemes.

Here are three examples of the damage that may be encountered by owners of laptop computers:

Case 1. The Stolen Laptop

Over 600,000 laptops are pilfered every year. [4] This represents the second costliest category of the estimated $67,000,000,000 in annual computer crime losses.[5]

Airports and automobiles are frequent locations for laptop thefts, but surprisingly, most are stolen in the workplace.[6) In a recent case in Colorado a laptop containing data for 988 students was stolen from a faculty member's office at Metropolitan State College of Denver.[7]

Windows XP was installed on the laptop and password security was the only form of protection mentioned.

What are the logical steps the cyber thief will take once in possession of the stolen laptop?

A typical first step is recovering cached credentials. A simple way to accomplish this is to boot the machine with a floppy or CD/DVD, run a program such as pwdump2 to extract the user names and encrypted passwords, then use a tool to crack (decrypt) the passwords.

With the "John the Ripper" cracking tool, I was able to obtain the data from a computer in approximately two hours. If the crook is a professional, he will log into the network long before security administrators are alerted and passwords are changed. This speed of entry allows the intruder to proceed unhindered.

Once the network is violated, the analysis begins to uncover further possibilities for fun and profit. The thief will have a suite of software to scan the disk and find Social Security Numbers or other valuable data. Additionally, if the owner of the laptop stores personal information such as drivers license number, bank or credit card numbers, etc. the perpetrator may also exploit that information. The thief may use decrypted credentials to make purchases from online accounts with stored credit card numbers if he finds any in the browser history log.

Once the passwords are cracked and Windows is started, the laptop may also be used as a temporary host for other illegal activities, such as hacking into other machines, launching malware (malicious software designed to infiltrate or damage computer data) and denial of service attacks (DoS), or to route or forward SPAM.

All of the above is easily accomplished with the average XP computer (all references to Windows® XP in this article refer to XP with Service Pack 2 installed, sometimes known as XPSP2). If the owner used the Encrypting File System (EFS) to encode all of the sensitive data on the disk and used a strong password, they may feel secure, but the system is still easy to breach using the cracked user name and password.

If the criminals are unable to crack the running system, they will remove the hard drive and install it in another machine to obtain the same result. There are other techniques as well, including hacking into the computer using standard software tools (called remote attacks), used because XP always loads critical system routines into the same memory addresses.

Case 2. The Compromised Laptop

A laptop does not have to be physically stolen for valuable data to be extracted. A few unguarded moments are all that is needed to add malicious software either at the site or remotely. Aspiring thieves, or their electronic proxies, are constantly monitoring for unattended computers either in person or on the Internet and private networks. In fact, the FBI lists the introduction of viruses and other stealth software as the most costly computer crime, ahead of laptop theft. [8]

Networked computers are usually protected by industrial-strength firewalls, secure managed mail services, anti-malware software, anti-virus software, and a dedicated staff of security professionals who constantly monitor the system and keep it patched and maintained. Laptops only share this protection when connected locally.

Most Windows XP portables have local group policy (GPO) settings that start other protection when the machine is not connected to the main network. These safeguards include enabling automatic updates, switching on the Windows Firewall, and activating Windows Defender and a client-side anti-virus program.

Despite these protections, thousands of XP machines are infiltrated every day by malware in the form of viruses, Trojan horses, logic bombs, trapdoors, etc. Once the software is installed, it can carry out a number of insidious functions on the compromised machine, including capturing activity information such as logs and keystrokes, corrupting data, adding other malware, searching for and transmitting certain types of information like Social Security and credit card numbers, sending email, etc.

Thieves extract information from the laptop, and may be able to infiltrate the local area network (LAN) once the mobile computer is reattached.

Case 3. Insider Stealth Activities

Employees and other trusted insiders often access computers without proper authority. They can easily attach external hardware, such as USB storage devices to steal sensitive files or credentials for processing and decrypting outside the network. While companies frequently disable this capability, it is seldom done with laptops because they are more dependent on external devices to be functional.

When unauthorized users gain control of a Laptop that is connected to the network, a whole new world of vulnerabilities unfolds. Direct intrusion tools may be used to send spoofed

packets to obtain network information, unveiling new ways to breach security. Passwords are cracked to log in with administrator permissions, backdoors are built for later incursions, and permissions on the laptop are changed to allow remote access.

Surreptitiously, the computer may be scheduled to send stolen information using normal methods that will not attract attention, such as email, ftp, http, etc. to external machines. Additionally, sniffers or other software may capture network traffic and transfer it to the cyber bandit's equipment to extract valuable information, passwords, etc.

For businesses or homes using laptops connected wirelessly, spies may camp within range of wireless routers and intercept traffic when strong encryption and passwords are not enabled. Recent surveys of wireless networks indicate that many use default names and passwords or easily guessed keys that may be decrypted in a matter of minutes, allowing complete access to the network.

Laptops running XP are often configured to automatically connect to wireless access points (WAPs) with default names. Crooks can set up their own WAPs with the same names and trick unwitting users to connect and expose their traffic. These are called "evil twins" and can often be found near airports or other high-use areas. Some trick users who are searching for WAPs by using names like "Free Airport Wireless", or something mimicking a corporate WAP.[24]

Another popular approach is the "man in the middle", where the user logs on to the correct network, but is actually passing through another WAP that records all of the information sent.

For the laptop user, equal diligence is required both inside and outside to prevent the computer and the network from being compromised. The rest of this paper explains features of Windows Vista that will make the job easier.

Windows Vista Technical Information

Security features in the Windows Vista operating system have been designed to address the vulnerabilities exposed in laptops running XP and described in the 3 scenarios above and many more. Each Windows Vista feature is described below:

TPM (Trusted Platform Module) Chips Support

Windows Vista TPM Services Architecture supports a TPM (Trusted Platform Module) version 1.2 microchip on the motherboard. The TPM stores keys, passwords, and certificates in encrypted form using RSA, SHA-1 and HMAC. [25] A TPM chip increases the security of BitLocker encryption by making more secure encryption schemes available, along with the certainty that an encrypted disk cannot be read if removed from the machine. The disk also cannot by read if the TPM chip is tampered with in any way. [9]

Smart card, Biometric Support

Windows Vista provides a new authentication architecture that is simpler for other companies to build interfaces, thus allowing easier implementation of strong authentication devices such as smart cards and biometric devices like fingerprint or retina

scanners. Microsoft believes this will lead to a proliferation of these devices for the Windows Vista operating system.

Windows Vista Wireless Enhancements

Microsoft has increased the security of connections to wireless networks with the Windows Vista platform by adding support for encryption technologies not supported in XP, such as native support for the highest level of standards-based security currently available for wireless networks, Wi-Fi Protected Access 2 (WPA2).

Windows Vista allows users to determine the preferred connection order of wireless networks whether or not they broadcast their SSIDs (Service Set Identifier). [10] Windows XP had no facility to designate a non-broadcasting wireless network as a preferred connection. This forced users to configure routers to broadcast their SSIDs and advertise their existence to hackers, or manually connect their laptops each time they restarted.

Windows Vista also has a long list of wireless enhancements not found in XP that augment the security, efficiency, manageability, and ease of use for users:

Protocols and Core Networking Components

- Next Generation TCP/IP Stack incorporates features like receive window auto tuning and compound TCP and Explicit Congestion Notification (ECN) support to increase speed and stability.
- Policy-based Quality of Service (QoS) allows setting of inbound and outbound throttle rates and the receive window size.
- Server Message Block 2.0 (SMB) supports larger buffer sizes and fewer packets than SMB 1.0 in XP.

- Http.sys enhancements improve management of HTTP (Hyper Text Transfer Protocol – used by all web sites) with better authentication, performance and logging than XP.
- WinINet enhancements support IPv6 and better decompression to make web downloads faster. Also supports uploads greater than 4 GB.
- Windows Sockets enhancements give better security, stability, logging and diagnostics.
- Network Driver Interface Specification (NDIS) 6.0 offloads more network traffic processing to the network adapter, saving Central Processing Unit (CPU) cycles.
- Network Awareness provides a platform to allow the operating system and other applications to adjust to changes in network connections.
- Windows Peer-to-Peer Networking enhancements include the addition of Windows Meeting Space and other user-to-user improvements over XP.

IEEE 802.11 Wireless Changes and Enhancements

- The Native Wi-Fi architecture is no longer an emulation of standard Ethernet 802.3, allowing for specific wireless improvements.
- User interface improvements for wireless connections include the new Network and Sharing Center.
- Wireless Group Policy enhancements allow easier and centralized configuration of wireless connections.
- The changes in Wireless Auto Configuration provide more tools to thwart malicious wireless users and supports non-broadcast networks.
- WPA2 Support is direct (when loaded on an XP machine it must be configured indirectly from a Windows Vista or Longhorn machine).

- Integration with Network Access Protection (NAP) when using 802.1X authentication allows limited or no access to computers that do not meet health requirements.
- Host-based Extensible Authentication Protocol (EAPHost) infrastructure for greater security.
- Wireless connections on Windows Vista now support the Network Diagnostics Framework making them much easier to troubleshoot.
- Command-line support for configuring wireless settings (not available on XP).
- Single Sign On makes it simpler to use the Domain login for wireless network authentication.

Network Infrastructure

- The Network Policy Server is an improved version of the Remote Authentication Dial-In User Service (RADIUS) server, incorporating NAP and IPv6 support.
- Remote Access and Virtual Private Network (VPN) connection enhancements allow smoother connections with greater security.
- Dynamic Host Configuration Protocol **(**DHCP) enhancements include support for IPv6 (DHCPv6), the new Internet Protocol (IP) addresses (128 bit instead of the current 32).

Probably the most important of these enhancements are:

1. Group Policy additions, which allow network administrators to configure the wireless behavior of all laptops when they connect to the base network through Active Directory (AD).
2. Enhanced diagnostics, which allow better end-user support in business environments and make it easier for individual

users to figure out why they are having trouble connecting. [11]

User Account Control (UAC)

Vist	XP	Vista Extension	Security Type
X			Unauthorized Access

In Windows XP, all users are automatically created as local administrators in order to allow them to install, update and remove software, backup files and directories, and other system-wide tasks. Local administrators have read, write, and execute permissions to all Windows resources, as well as all Windows privileges. Although convenient for the user, this exposes the computer to a variety of threats originating from hackers or malware. Since the user has all permissions and privileges, any process that impersonates that user will also have the same power to install and run programs, change existing programs, and add, delete, and modify files and folders.

The solution for XP is to remove the user from the local administrator group and run as a standard user (a user with the least amount of permissions and privileges required to perform basic tasks). This, however, creates another set of problems, because administrative privileges are required to run some programs, and to install, update and change others. In fact, standard users do not have privileges necessary to change and add printers or even modify time settings. There was no plan in XP to allow standard users to temporarily acquire administrative privileges in order to perform tasks for which they had inadequate authority.

UAC fulfills that function in Windows Vista. Instead of using the "Run As" procedure, or logging off and logging on as a local administrator, the standard user in Windows Vista has the option of seamlessly acquiring the necessary privileges and permissions during the flow of the task that requires them, by providing administrator credentials. In addition, administrators themselves actually run as standard users, acquiring administrator rights seamlessly only when necessary.

In this way, all interactive users normally run with minimum permissions, so it is much more difficult for the system to be compromised. An additional benefit of running with minimum permissions is that malicious software must also request permission before it can install itself. [12]

Figure 1 - Windows Vista Sidebar

Sidebar Gadgets

Vista	XP	VE	Security Type
X			Malware

The Sidebar is new with Windows Vista and consists of a vertical column that can be placed to the right or left side of the desktop and populated with applications called "Gadgets". The sidebar usually consists of mundane items which display the time, weather, and headlines, but savvy users may include monitoring gadgets that alert them to internet security threats, the status of their firewall and available memory, connection state, network activity, etc. [13]

Internet Explorer Version 7 (IE7)

Vista	XP	VE	Security Type
X	X	X	Malware

A favorite avenue of entry into computers from the web is through the web browser. Internet Explorer, version 7 has added many security features to prevent this type of invasion, and most of the additions are available on both XP and Windows Vista. However, on Windows Vista, IE7 runs in Protected Mode in concert with User Account Control (UAC) making sure that it runs with as little permission as possible, thwarting most web-borne malware from secretly installing software. If one of these programs tries to invoke the system installer, Windows Vista will warn the user and ask permission to install the program.

Protected mode also makes it more difficult for browser-based malware to do damage by changing browser properties or settings, such as adding unwanted toolbars.

BitLocker™ Drive Encryption

Vista	XP	VE	Security Type
X			Data Access

BitLocker (only included on Ultimate and Enterprise versions of Windows Vista) encrypts the entire Windows volume of the hard drive, including the files from which user names and passwords are extracted. [9] If BitLocker is installed on a machine with a TPM chip the hard drive cannot be read on another computer. For better protection, an external USB flash drive should be used with the TPM chip, which will ensure the drive cannot be accessed without both the credentials and the flash drive. The flash drive should always be stored separately from the laptop.

This feature requires a separate partition of at least 1.5 gigabytes to store the system files, which cannot be encrypted. Encryption of the main volume is accomplished using the motherboard's TPM chip, if one is present.

In the absence of a TPM chip, BitLocker can still be implemented using the CPU and a key stored on a removable Universal Serial Bus (USB) flash drive. This option requires a change to the Group Policy Objects to activate, and since most laptops being used today don't have TPMs, laptop owners should know how to make the change to take advantage of BitLocker.

First, key gpedit.msc into the "Start Search" box that appears when the Start button (which is now a round Windows Vista logo instead), and press enter. Windows Vista will run programs in this manner without using the "Run" button. UAC will ask you if you want to continue (yes) and then will display the Group Policy Object Editor.

Second, double-click "Administrative Templates" under "Local Computer Policy" and "Computer Configuration". Then double-click on "Windows Components", "BitLocker Drive Encryption" and "Control Panel Setup: Enable advanced startup options", whew! (See Figure 2 - BitLocker Drive Setup)

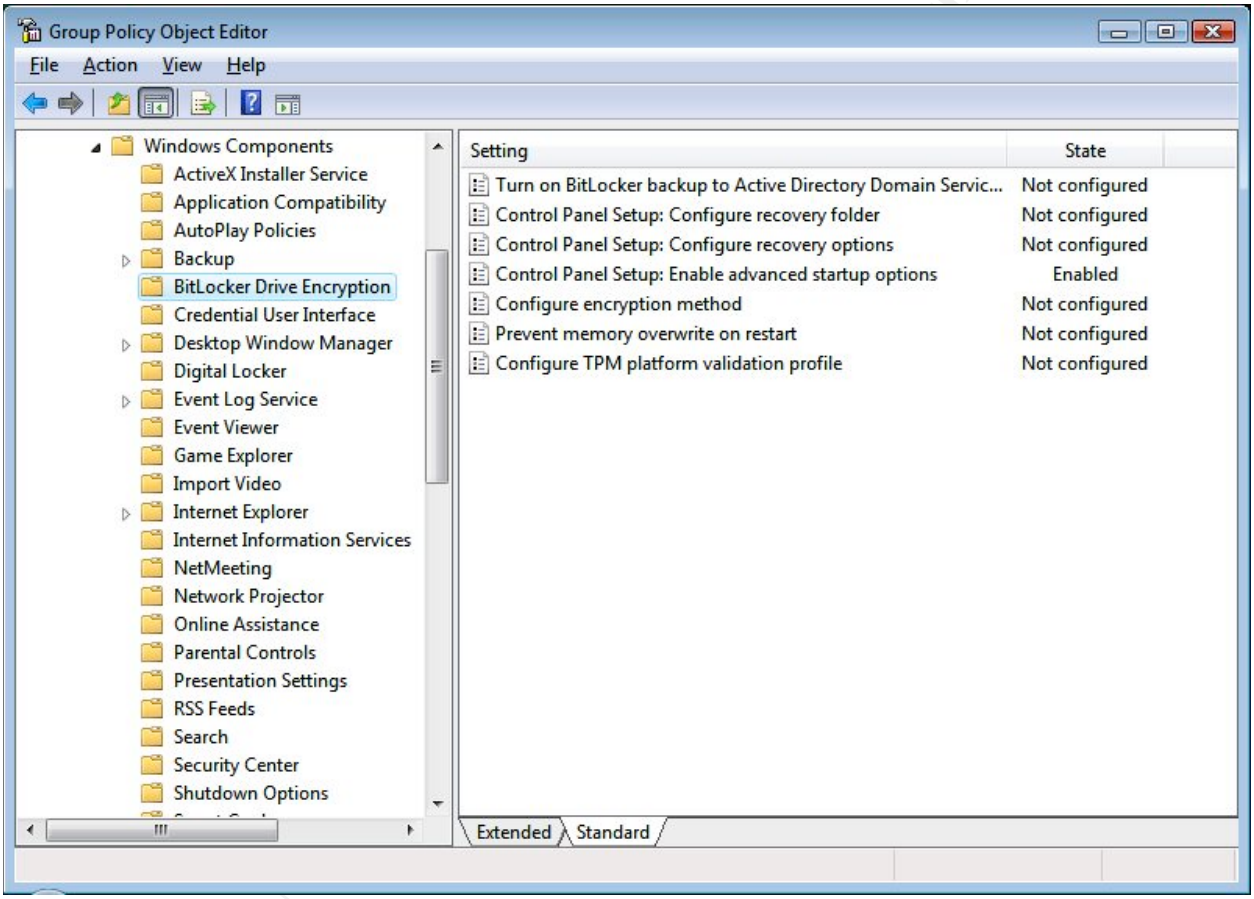


Figure 2 - BitLocker Drive Setup

Next, click the "Enable" radio button on the Enable advanced startup window (see Figure 3 - BitLocker Startup Options). Then make sure the checkbox to the left of "Allow BitLocker without a compatible TPM" is checked and click the "OK" button.

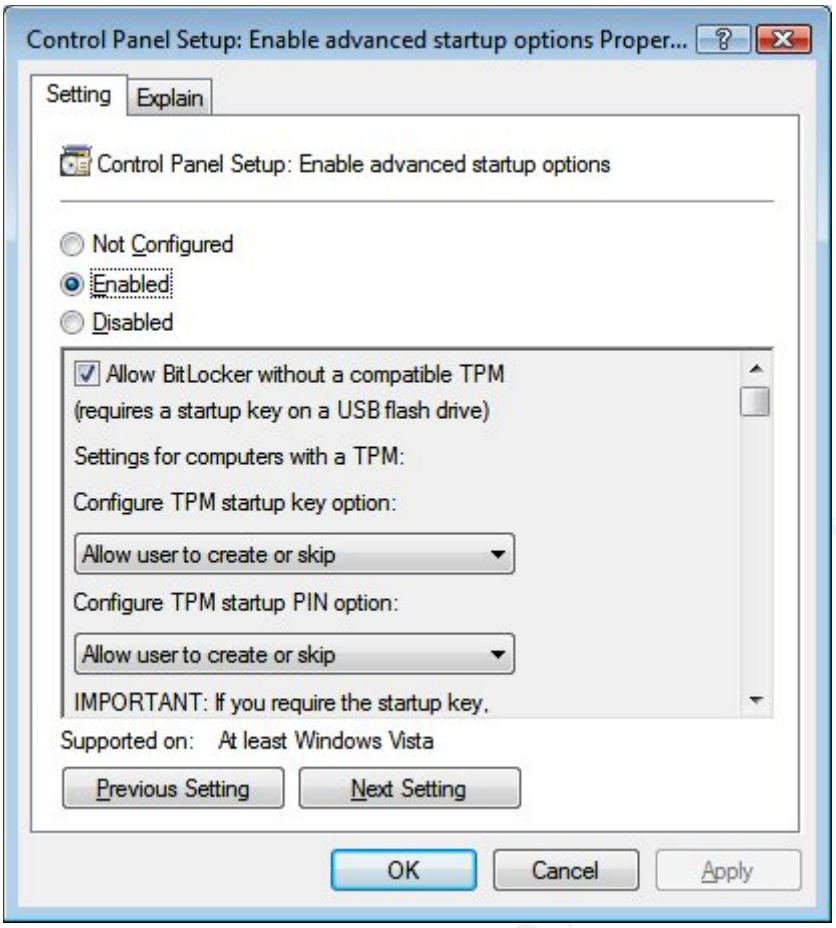


Figure 3 - BitLocker Startup Options

When the next window appears, click "Require Startup USB key at every startup" (see Figure 4 - BitLocker Drive Encryption).

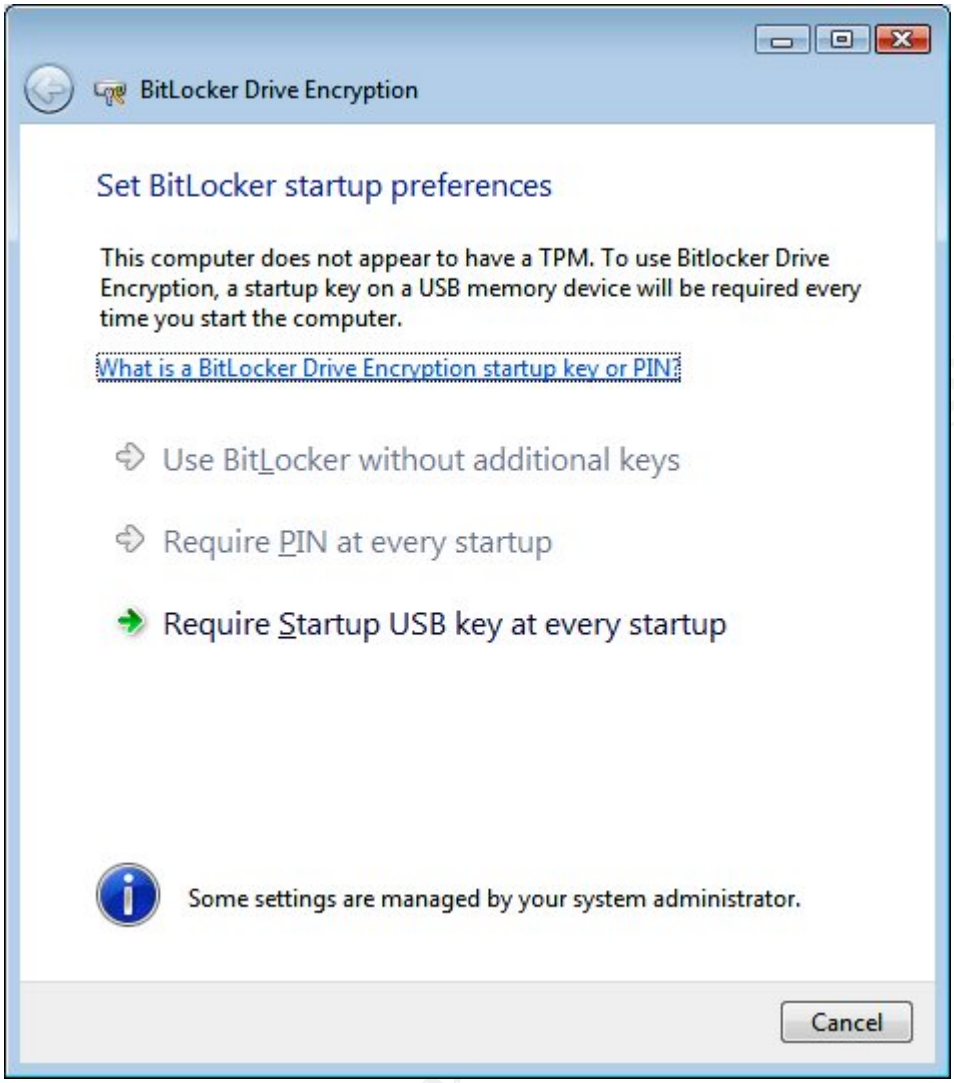


Figure 4 - BitLocker Drive Encryption

Once the TPM chip has been bypassed, type "bitlocker" in the "Start Search" button of the start menu (see Figure 5 - BitLocker Start), and click "BitLocker Drive Encryption" at the top of the menu. Once again, you will be asked to verify the process by UAC.

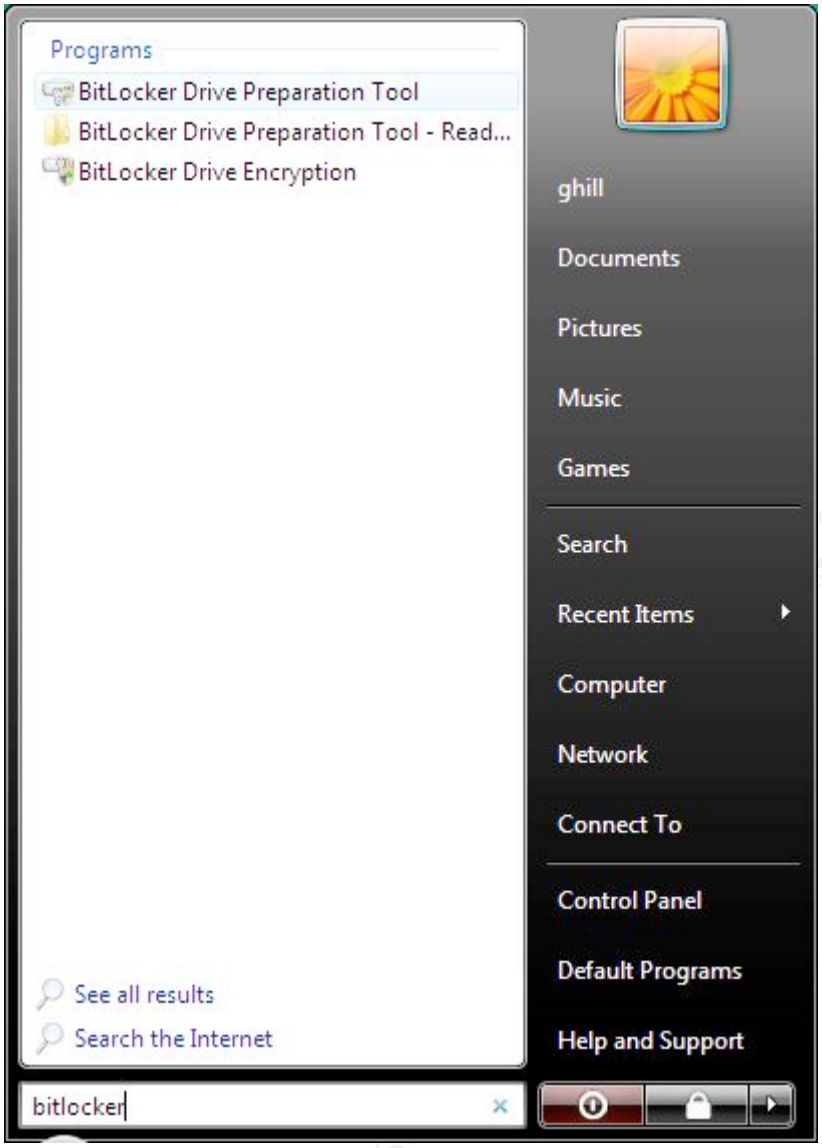
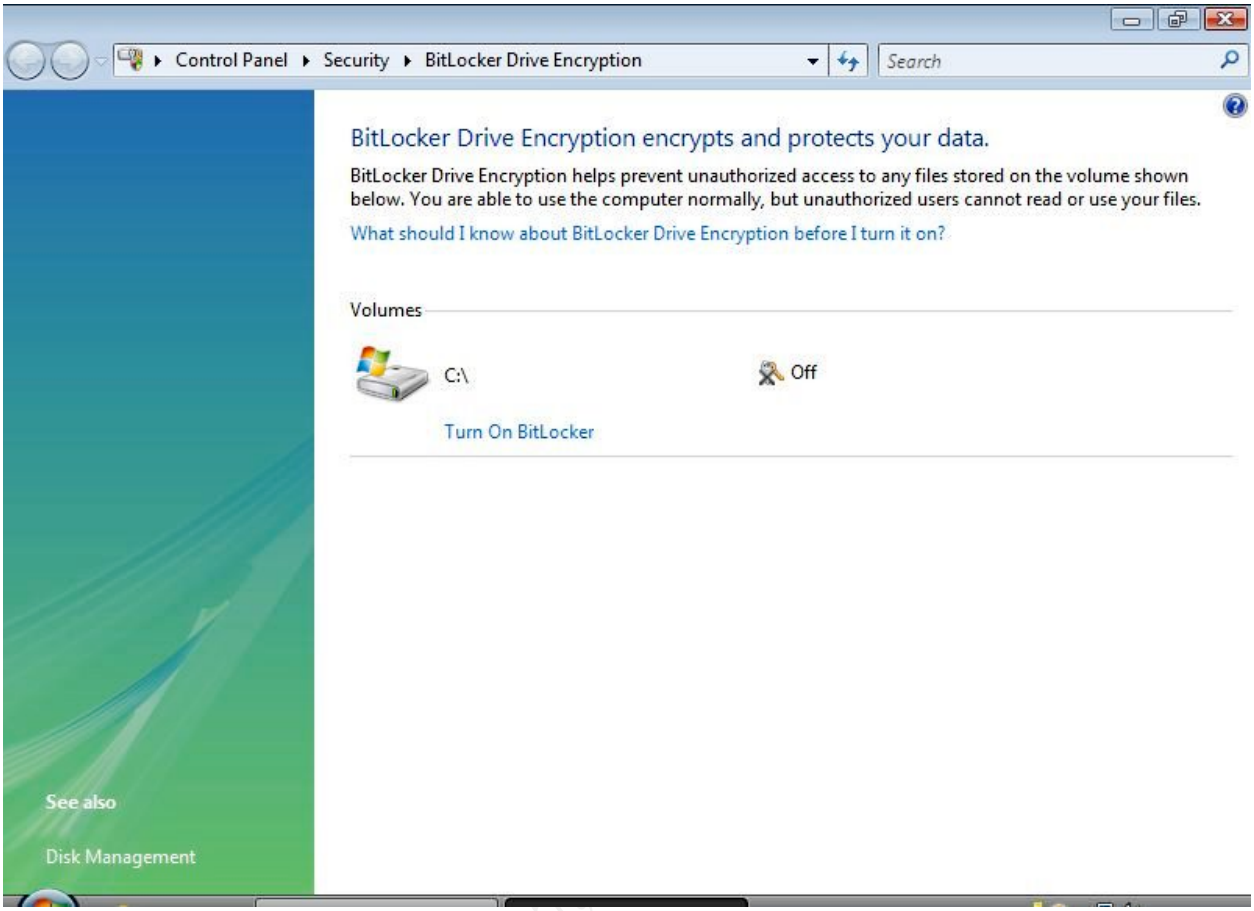


Figure 5 - BitLocker Start

Select "BitLocker Drive Encryption" and the following window will appear:



Click on "Turn On BitLocker" and BitLocker will then be installed (patience required).

When BitLocker is used with the TPM chip, it will not start Windows if the drive is moved to another machine or TPM settings are changed. If the flash drive is used without a TPM module, the hard drive could be moved to another machine and decrypted if a flash drive containing either the user or the recovery key is taken along with the computer. This illustrates the importance of removing the flash drive when leaving the machine unattended. Using the "Hot Glue Gun" method of deactivating USB ports renders BitLocker unusable on machines without TPM chips.

The BitLocker default encryption is AES-128-CBC (Advanced Encryption Standard – 128 bit – Cipher Block Chaining) with an

additional diffuser, "to protect against ciphertext-manipulation attacks, and is independently keyed from AES-CBC so that it cannot damage the security you get from AES-CBC" [9]. Other encryption schemes are available to administrators through group policies.

BitLocker eliminates at least two methods of mining data from a stolen PC. First, credentials can't be extracted because the files that contain them are encrypted. Second, the disk can't be accessed from another machine or operating system because the TPM and/or flash drive is required along with the credentials used to encrypt the disk.

Encrypting File System (EFS)

Vista	XP	VE	Security Type
X	X	X	Data Access

Files and folders on both Windows Vista and XP may be encrypted using EFS. This does not provide enough protection under XP because the files are automatically decrypted when the user logs on. The Windows Vista version contains a number of enhancements, including the ability to store user and recovery keys on smart cards, encryption of the paging file (fertile ground for thieves, often containing unencrypted data on XP), encryption of the offline file cache, control from new group policy keys, and support for more certificates and keys for different encryption types.

So, even without BitLocker, sensitive data on Windows Vista laptops can be protected from thieves by using EFS to encrypt folders and files and keeping the smart cards with the user and recovery keys stored separately from the machine.

Rights Management Service (RMS)

Vista	XP	VE	Security Type
X	X		Data Access

RMS primarily protects email, documents, and web content as they travel across the network. It is primarily a server-based system with a nearly identical operation on either XP or Windows Vista. RMS integrates with both IE7 and SharePoint, but requires Windows Rights Management Services for Windows Server 2003 or a later version running on a network server along with Rights Management-enabled applications running on the client. These prerequisites make RMS viable primarily in large, sophisticated applications.

Remote Laptop Security (RLS)

Vista	XP	VE	Security Type
X	X		Data Access

RLS is not included in Windows, but may be obtained from various 3rd parties. In its basic form, RLS encrypts selected files on the laptop and only decrypts them if the user can authenticate over an Internet connection. In the event of theft, the owner of the computer may deactivate the remote authentication, rendering the files inaccessible. RLS is currently available on both XP and Windows Vista, but, given the more robust developer tools available for Windows Vista, undoubtedly additional advanced "Vista-only" products will be available in the near future.

Virtual PC (VPC) 2007

Vista	XP	VE	Security Type
X		X	Data Access

VPC 2007 is a free download application from Microsoft that allows running a "virtual" copy of Windows Vista on systems running Windows Vista Business, Enterprise, and Ultimate editions. A virtual version of Windows can be used to test software and patches before implementing them on the production system, possibly saving data destruction and system crashes. [14]

Windows Defender

Vista	XP	VE	Security Type
X	X	X	Malware

Defender is available on both Windows Vista and XP, but when running on Windows Vista, it "…takes advantage of many of the platform enhancements in Windows Vista, including improved caching technology—which allows scans to run faster—and User Account Control, which enables the software to run without administrator privileges…". [15]

Defender is a spyware and malware scanning and removal tool, similar to third party tools like Webroot's Spy Sweeper and various freeware and shareware packages. Some anti-virus tools, notably products from McAfee and Norton, also remove spyware and malware. Defender has the advantage of being free, as a part of Windows Vista and a free download for XP. Spyware is a category of malware that primarily captures information and transmits it to sometimes legitimate companies, often installed with the user's permission as part of "free" software.

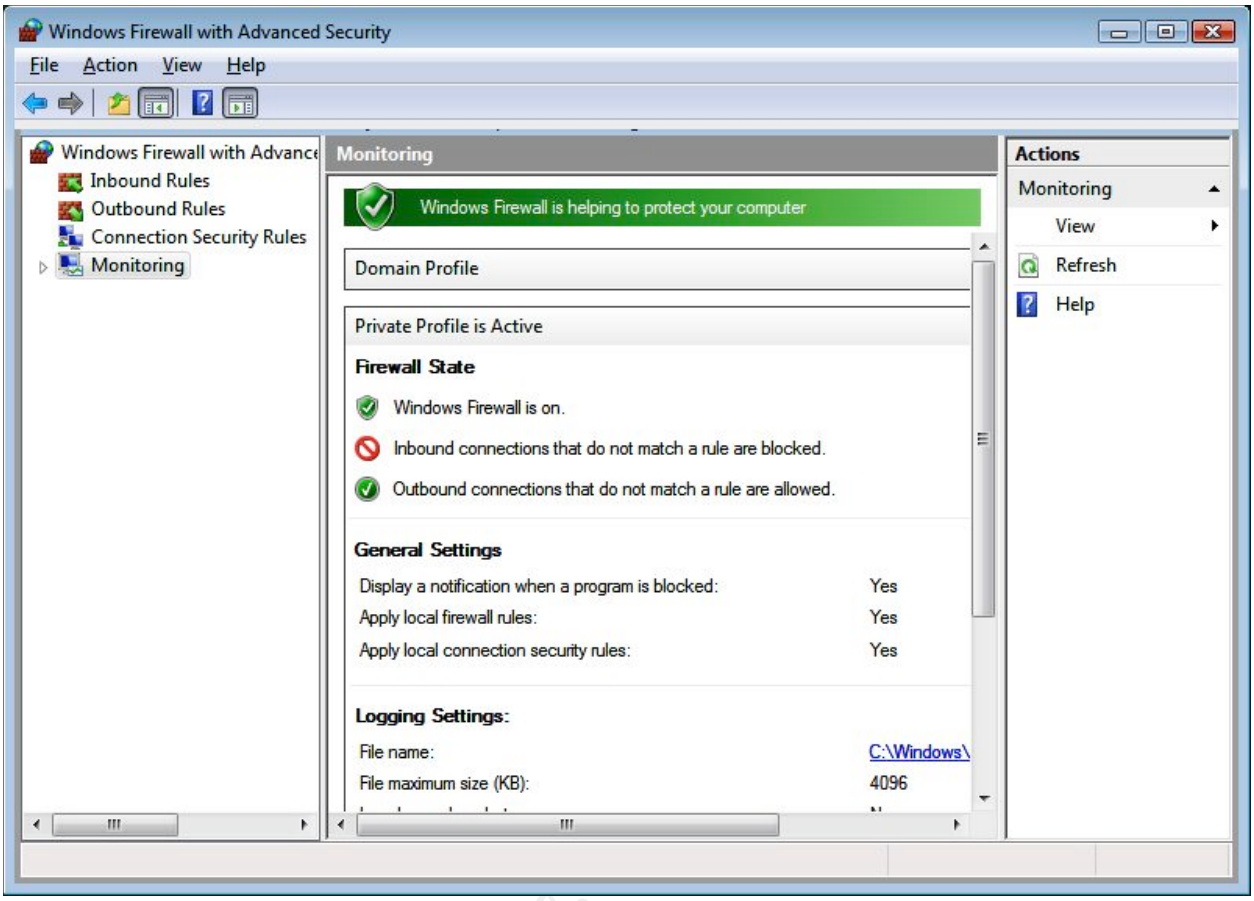


Figure 6 - Windows Vista Firewall

Windows Firewall

Vista	XP	VE	Security Type
X	X	X	Data Access

The addition of outbound filtering to XP's inbound filtering will give administrators control over peer-to-peer sharing and other dangerous activities. In addition, the firewall in Windows Vista is integrated with network awareness, allowing its settings to change depending on the network to which it is connected. Also, the firewall is now integrated with IPSec for simpler configuration and reduction of policy conflicts.

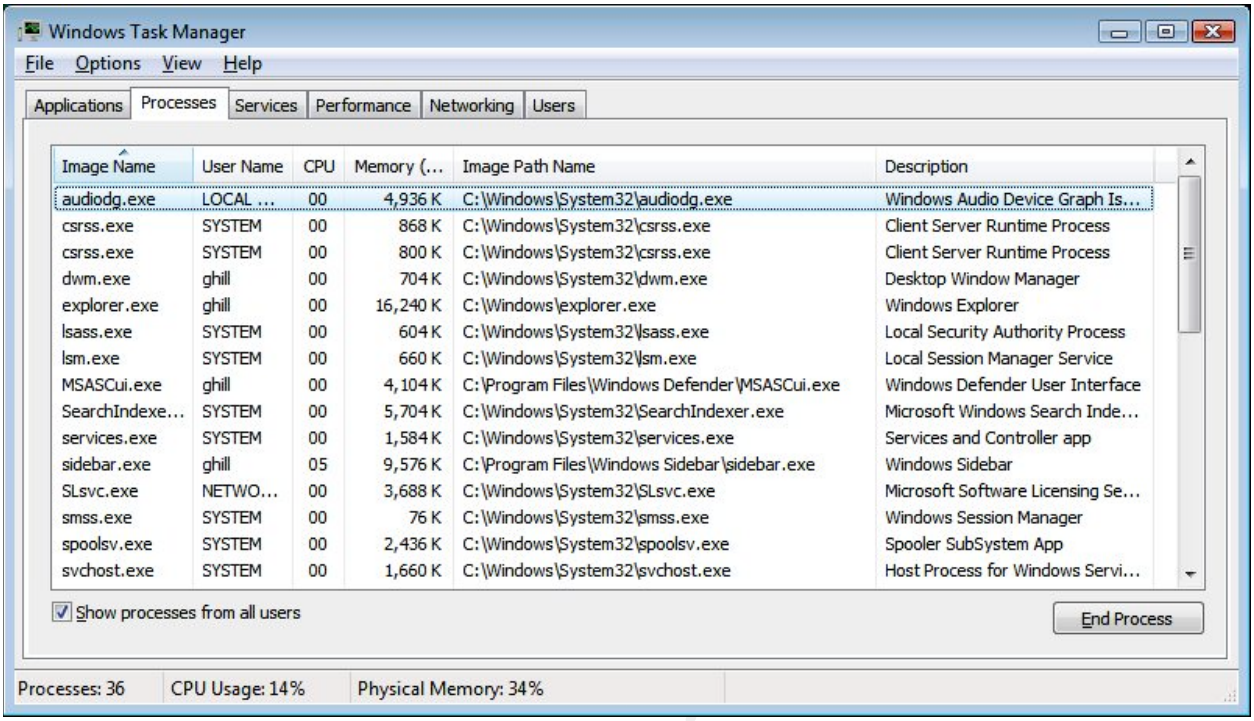


Figure 7 - Windows Vista Task Manager

Windows Vista Task Manager

Vista	XP	VE	Security Type
X			Detection

Under the "Processes" tab of the Task Manager, a new column is added which contains the description of the process. Additional columns may be added to further identify running programs, including the exact location of the executable. This is an invaluable aid when tracking down programs that could compromise security.

Windows Service Hardening

Vista	XP	VE	Security Type
X			Unauthorized Access

This new feature on Windows Vista makes it difficult for intruders to gain entry to systems services, but if a service is compromised, the network itself is harder to attack.

In XP, services, which are long-running (usually active from startup to shutdown)application programs that run in their own sessions, and usually as a highly privileged account, such as Local System, and they usually have access to the network. These characteristics made services popular with malware exploiters who have been able to use them to do anything they wanted at any time. The Blaster worm was a particularly devastating example of malware that exploited a service, in that case the Remote Procedure Call (RPC) service.

In the Windows Vista operating system, services have been hardened and secured in four ways:

1. Running services with Least Privilege, automatically implemented by UAC.
2. Service Isolation allows services to reserve and access items with a unique id that cannot be hijacked by malware.
3. Restricted Network Access means that services are automatically configured in the Windows Vista Firewall with the lowest privileges needed during network access.
4. Session 0 Isolation is used in Windows Vista to keep user programs (and malware) out of session 0 by reserving it exclusively for services. [16]

Network Access Protection (NAP)

Vista	XP	VE	Security Type
X			Unauthorized Access

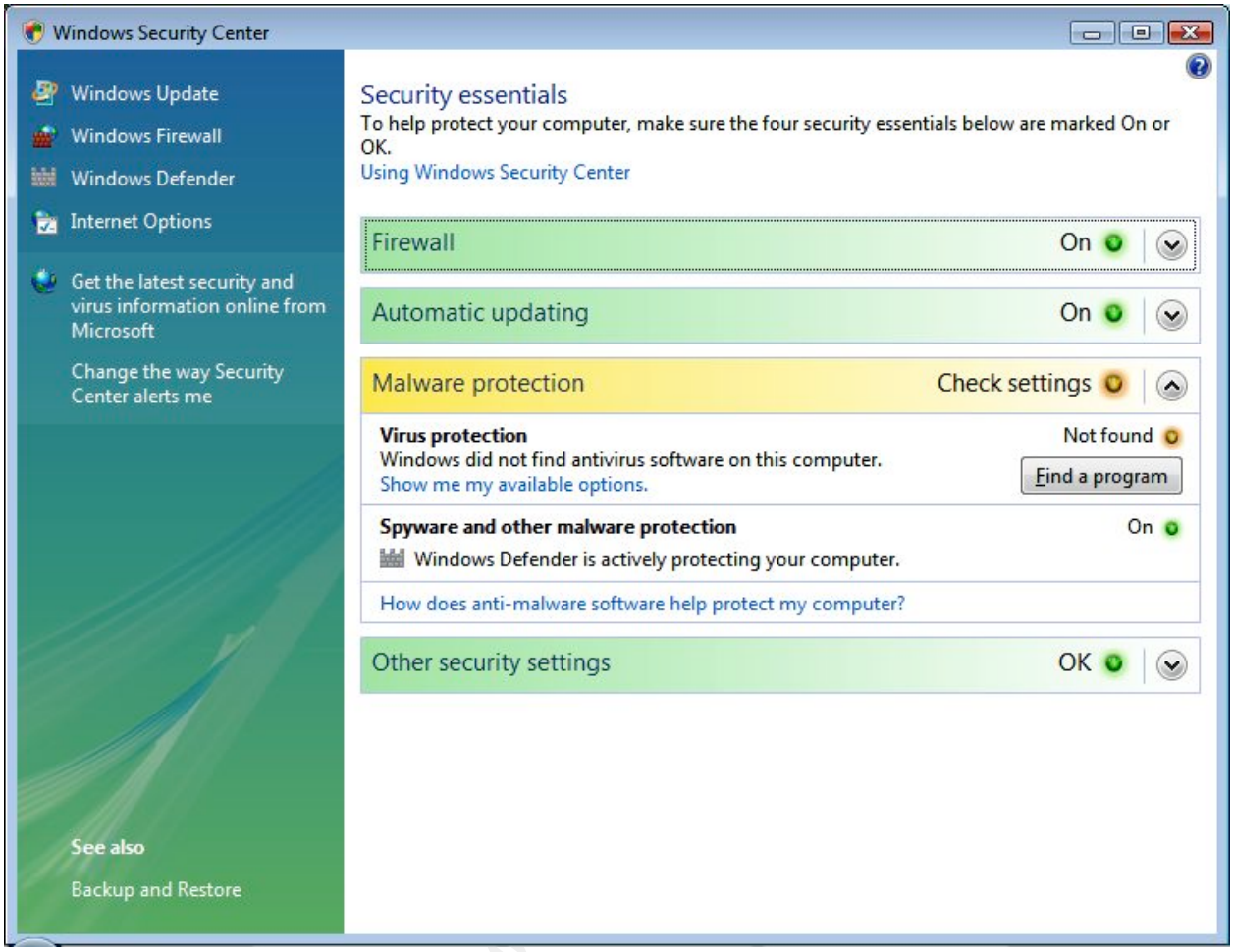
Windows Vista is the first Windows operating system to implement NAP, which reports health information to network NAP servers. Network Administrators can use NAP to establish minimum health restrictions to deny network access to machines that do not meet stated requirements. For example, the network NAP server may reject connections by computers that are not at the specified service pack or patch level, or are not running a specified operating system edition by accessing the NAP health information provided by Windows Vista.

Group Policies (GP)

Vista	XP	VE	Security Type
X	X	X	Device Control, Data Access

GPs can be used to restrict a multitude of activities, including what may be downloaded to attached devices. Using group policy to disable downloads to USB devices is preferable to the "Hot Glue Gun" technique, and equally effective. In fact, using GP for Device Control allows Administrators to allow some users to write to USB devices, allow others only read access or none at all.

A large number of security-oriented Group Policies have been added to Vista in addition to Device Control items.



Windows Security Center Figure

Windows Security Center

Vista	XP	VE	Security Type
X	X	X	Detection

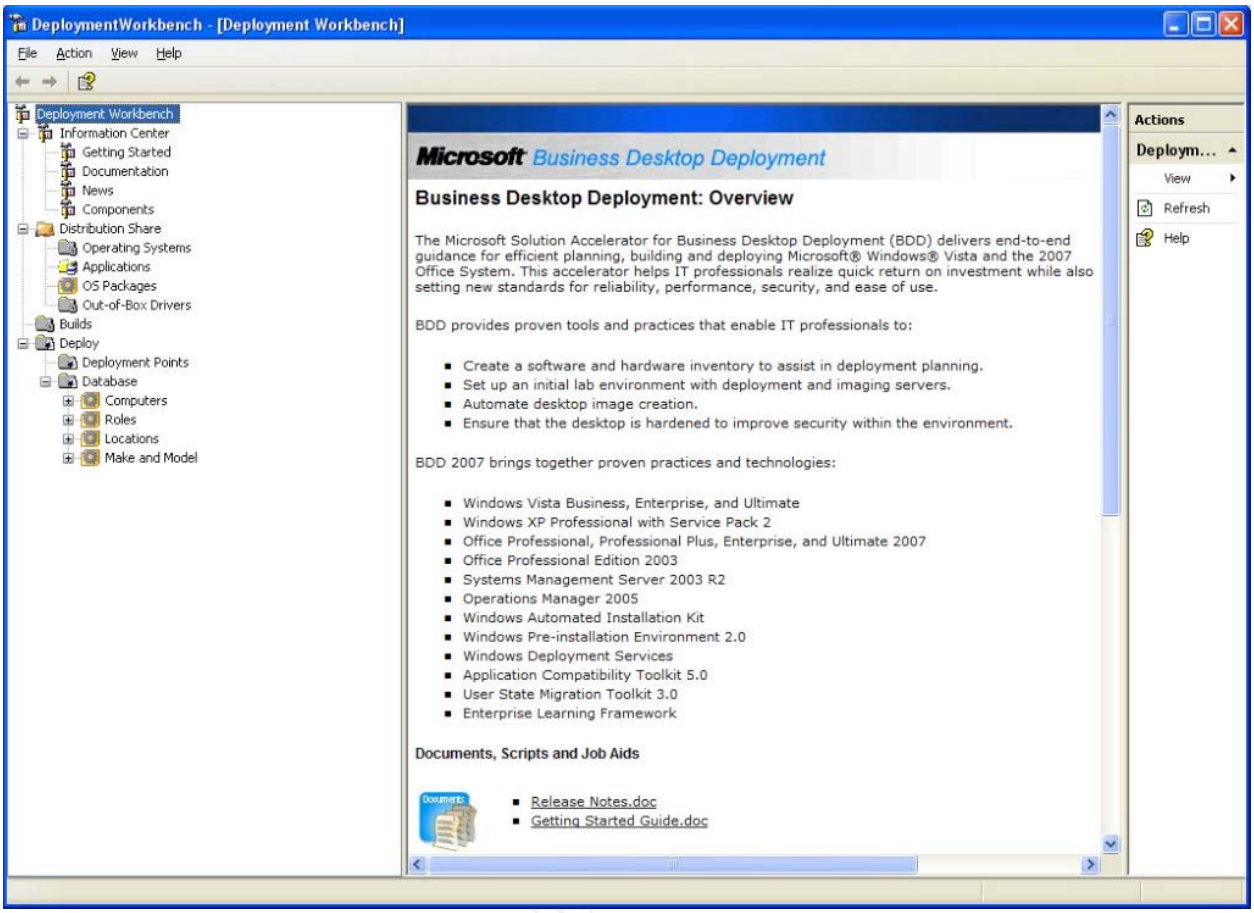
The Security Center puts the interfaces of many of the security components in one place for ease of monitoring and configuration. It contains the Firewall, Automatic Updates, Antivirus, Spyware and Malware protection, Internet Security Settings, and User Account Control.

Address Space Layout Randomizer (ASLR)

Vista	XP	VE	Security Type
X			Unauthorized Access

ASLR is a feature that has been used for years on Linux and Unix systems, but is implemented for the first time on a Windows system on Windows Vista. When Windows Vista boots and applications start, ASLR loads programs and their associated memory at random memory offsets, foiling remote attacks and memory manipulation vulnerabilities that expect executables to be located at specific addresses. Microsoft estimates that 99% of remote attacks will fail due to this feature. [15]

ASLR is automatically implemented with the default configuration and requires no setup. Tests by third parties have unearthed some bugs in the initial versions that make the ASLR included with the current version of the Windows Vista operating system slightly less effective than a perfect implementation. [17] Nevertheless, ASLR makes Windows Vista far more resistant to these kinds of attacks than its predecessor. [15]



Windows Vista Deployment

Companies installing multiple copies of Windows Vista may use a free tool from Microsoft: The Deployment Workbench/Business Desktop Deployment 2007 (BDD 2007). This tool allows administrators to create Windows Imaging (WIM) format objects of Windows Vista to load laptop or desktop computers in a few steps (light touch) or a single step (zero touch) over a network or from a DVD. Most importantly, virtually all of the security features mentioned above may be installed and configured with the hardening component of BDD 2007, which also incorporates Hardware Abstraction Layer (HAL) independence and language neutrality. This allows the same Windows Vista image to be deployed on more than one hardware platform, further simplifying

the install effort. All security features, including BitLocker, may be installed and configured using BDD2007 with little or no human intervention.

A serious flaw in Windows XP is that most of the security configuration must be done manually by administrators, which negatively impacts the operation of the system by the users. This results in security features not being turned on in the first place, or being turned off at the request of frustrated users. Windows Vista addresses both of these problems with BDD 2007 which is able to configure all security features automatically and permits the features themselves to be unobtrusive to the users.

Windows Vista Hardware Requirements

Due to the increased hardware requirements, users and companies wishing to upgrade laptops from previous Windows operating systems to Windows Vista may find it difficult. The Windows Vista Hardware Requirements Table below shows the minimum supported requirements, called "Vista Capable" by Microsoft, and the actual practical minimum specifications, termed "Vista Premium Ready".

Type	CPU	RAM	Disk Size	Disk Free	Graphics RAM	Optical Drive
Vista Capable	800 MHz	512 MB	20 GB	15 GB	VGA	CD-ROM
Vista Premium Ready	1 GHz	1 GB	40 GB	>15 GB	128 MB	DVD-ROM

Windows Vista Hardware Requirements Table

Windows Vista Editions

Vista Edition	Upgrade Price	Aero	BitLocker	XP Version
Home Basic	$99.99	No	No	Home
Home Premium	$149.99	Yes	No	Home
Business	$199.99	Yes	No	Professional
Ultimate	$279.99	Yes	Yes	Professional
Enterprise	Volume	Yes	Yes	Professional

Table 1 - Windows Vista Editions and Prices

Table 2 - Windows Vista Security Features, below, contains my subjective determination of the value of new and improved protections in Windows Vista. For example, most security professionals would consider the disk encryption function provided by BitLocker to be essential on the vast majority of laptops. So, if a company's current mobile computers do not have this feature, they should consider the cost of adding it to current equipment as an offset of the cost of upgrading.

Windows Vista Security Features

Vista Security	XP	Vista Improved	Threat Type	Importance
BitLocker™	No		Data and Unauthorized	1
UAC	No		Unauthorized Access	2
Firewall	Yes	Yes	Unauthorized Access	3
Service Hardening	No		Malware	4
Group Policies	Yes	Yes	Data and Unauthorized	5
NAP	No		Unauthorized Access	6
ASLR	No		Unauthorized Access	7
Task Manager	Yes	Yes	Malware	8
EFS	Yes	Yes	Data Access	9
RMS	Yes	Yes	Data Access	10
Virtual PC 2007	Yes	No	Malware	11
Defender	Yes	Yes	Malware	12
IE7	Yes	Yes	Malware, Detection	13
Security Center	Yes	Yes	All	14
Sidebar Gadgets	No		Malware	15

Table 2 - Windows Vista Security Features

Summary/Conclusion

Should Windows Vista be installed on older laptops?
The answer is probably not. For reasonable performance, Windows Vista machines should be no older than a year, have 1 GB of memory or more (my tests indicate at least 2 GB is required for adequate performance for power users), a large hard drive (at least 60 GB), a fast processor (2 GHz or faster), a TPM chip, a DVD drive, and an advanced graphics card (able to use at least

128 MB of memory, minimum). Microsoft has a tool available for determining which computers on a network are good candidates for Windows Vista, called the Windows Vista Hardware Assessment Tool.

So, what is the final tally for security features in the Windows XP vs. Windows Vista comparison? There are 6 completely new features and 9 features that existed on XP, 8 of which have been enhanced on Windows Vista. The only feature that appears to operate identically on both XP and Windows Vista is the new Virtual PC 2007.

Obviously, Windows Vista Ultimate and Enterprise versions are dramatically superior to Windows XP. If a laptop user is satisfied with the security level provided by Windows XP and doesn't plan to upgrade to a BitLocker version of Windows Vista, there are probably not enough compelling reasons to upgrade.

As the chart in Table 2 - Windows Vista Security Features illustrates, many features are improved. Users will have to evaluate whether or not the enhancements are sufficient to justify the time and expense involved in a migration to Windows Vista.

For new laptops, it is clear that the security enhancements of Windows Vista over XP are both numerous and effective. However, some of the built-in features are not as complete as similar software available from third parties. For example, Windows Defender is not as thorough at catching malware as some other commercial products. There are also some holes in defenses of the Windows Vista operating system, the most obvious of which is the lack of virus protection. But, as a baseline desktop operating system, Windows Vista out-of-the-box is arguably the most secure product available. So, in most cases, anyone

purchasing a new laptop computer should opt for pre-installed Windows Vista rather than XP.

Conversely, users with existing laptops running XP should analyze their equipment to determine if any of the features incorporated in Windows Vista (or by extension, applications whose Windows Vista versions provide features that XP versions do not) to determine if the additional hardware and Windows Vista software costs are justified. Still in its infancy, the new Windows, has few Windows Vista-only enhanced applications. Deciding to upgrade will be a clearer decision when more software utilizing Windows Vista features exists.

Works Cited

1. **Webmaster**. Security Alert. *Metro State College of Denver, Colorado.* [Online] February 28, 2007. [Cited: March 10, 2007.] http://www.mscd.edu/securityalert/index.htm.

2. **Will Poole**. Will Poole: WinHEC 2006. *Microsoft.com.* [Online] May 23, 2006. http://www.microsoft.com/presspass/exec/poole/05-23WinHEC06.mspx.

3. **Schneier, Bruce**. Microsoft BitLocker. *Schneier on Security.* [Online] May 2, 2006. [Cited: February 26, 2007.] http://www.schneier.com/blog/archives/2006/05/bitlocker.html.

4. *Top Ten Security Challenges in the Coming Year.* **SANS**. 2006, Cybersecurity Technology Update, p. 4.

5. **Singer, Michael**. PC milestone--notebooks outsell desktops. *Cnet News.* [Online] June 3, 2005. [Cited: March 10, 2007.] http://news.com.com/PC+milestone--notebooks+outsell+desktops/2100-1047_3-5731417.html.

6. **Netscape.** 600,000 laptops get stolen every year: 10 things about laptop theft. *Netscape.com.* [Online] September 28, 2006. [Cited: January 23, 2007.] http://www.netscape.com/viewstory/2006/09/28/600000-laptops-get-stolen-every-year-10-things-about-laptop-theft/?url=http%3A%2F%2Flaptopcom.blogspot.com%2F2006%2F09%2F600000-laptops-get-stolen-every-year.html&frame=true.

7. **Evers, Joris.** Computer Crime Costs $67 Billion, FBI Says. *Cnet News.* [Online] January 19, 2006. [Cited: February 28, 2007.] http://news.com.com/Computer+crime+costs+67+billion,+FBI+says/2100-7349_3-6028946.html.

8. **Google.** How many laptops are lost and stolen each year in the US and world wide? *Google Answers.* [Online] December 14, 2005. [Cited: February 21, 2007.] http://answers.google.com/answers/threadview?id=605878.

9. **Gralla, Preston.** Windows Vista: 15 Reasons to Switch. *PC World.* [Online] January 26, 2007. http://www.pcworld.com/article/id,128656-pg,1/article.html.

10. **Cobb, Michael.** Windows Vista: Security issues to consider. *TechTarget.com.* [Online] February 27, 2007. [Cited: March 4, 2007.] http://searchsecurity.techtarget.com/tip/0,289483,sid14_gci1245006,00.html?track=NL-422&ad=578184&asrc=EM_NLT_1049864&uid=2314925.

11. **Cheng, Joel Santo Domingo and Cisco.** Putting Windows Vista PCs to the Test . *PC Magazine (PCMag.com).* [Online] January 29, 2007. http://www.pcmag.com/article2/0,1895,2087931,00.asp.

12. **Brooks, Jason.** Microsoft's Virtual PC 2007 Is a Good (and Free) Virtualization Option for Windows Users . *eWeek.com.* [Online] February 22, 2007. [Cited: February 23, 2007.] http://www.eweek.com/article2/0,1895,2097928,00.asp?kc=EWEWEMNL022307EP33A.

13. **Windows.** Windows Vista: Features Explained. *Microsoft.com.* [Online] January 30, 2007. [Cited: February 23, 2007.] http://www.microsoft.com/windows/products/windowsvista/features/default.mspx.

14. **Microsoft.** Understanding and Configuring User Account Control in Windows Vista. *TechNet.* [Online] http://technet.microsoft.com/en-us/windowsvista/aa905117.aspx.

15. **U of Bochum.** TPM Compliance Tests. *Chair For System Security, University of Bochum, Germany.* [Online] http://www.prosec.rub.de/tpmcompliance.html.

16. **Microsoft.** The Windows Vista Security Guide. *The Windows Vista Security Guide.* [Online] November 8, 2006. [Cited: February 2, 2007.] http://www.microsoft.com/technet/windowsvista/security/guide.mspx.

17. **Anon.** New FBI Computer Crime Survey. *Federal Bureau of Investigation.* [Online] January 18, 2006. [Cited: March 1, 2007.] http://www.fbi.gov/page2/jan06/computer_crime_survey011806.htm.

18. **Korzeniowski, Paul.** Locking Down the Laptop. *Information Security Magazine.* [Online] February 1, 2007. [Cited: February 22, 2007.] http://infosecuritymag.techtarget.com/articles/february01/features_laptop_security.shtml.

19. **Whitehouse, Ollie.** ASLR in Windows Vista. *Symantec.* [Online] March 1, 2007. [Cited: March 15, 2007.] http://www.symantec.com/enterprise/security_response/weblog/2007/03/aslr_in_windows_vista.html.

20. **The Cable Guy - Microsoft.** Connecting to Wireless Networks with Windows Vista. *Microsoft TechNet.* [Online] April 10, 2007. [Cited: March 10, 2007.] http://www.microsoft.com/technet/community/columns/cableguy/cg0406.mspx.

21. **Bradley, Tony.** Windows Vista Sidebar Gadgets for Security. *About.com.* [Online] February 11, 2007. [Cited: February 25, 2007.] http://netsecurity.about.com/b/a/256839.htm?nl=1.

22. **Microsoft.** New Networking Features in Windows Server "Longhorn" and Windows Vista. *Microsoft TechNet.* [Online] November 30, 2006. [Cited: March 23, 2007.] http://www.microsoft.com/technet/network/evaluate/new_network.mspx.

23. **Wole Moses.** Security Watch: Services Hardening in Windows Vista. *Microsoft TechNet Magazine.* [Online] January 2007. [Cited: March 23, 2007.] http://www.microsoft.com/technet/technetmag/issues/2007/01/SecurityWatch/?related=/technet/technetmag/issues/2007/01/SecurityWatch.

24. **Abdollah, Tami.** Wi-Fi hot spots may deliver user directly to hacker, thief. *Chicago Tribune.* [Online] March 25, 2007. [Cited: March 25, 2007.] http://www.chicagotribune.com/business/chi-0703230622mar25,0,1306986.story?coll=chi-business-hed.

25. RSA gets its name from the surnames of its inventors: Ron Rivest, Adi Shamir and Leonard Adleman, and is an algorithm used for public key encryption. SHA-1 is a cryptographic hash function designed by the National Security Agency (NSA) as a U. S. government standard. HMAC is a keyed-hash message authentication code; a type of message authentication code (MAC) calculated using a cryptographic hash function in combination with a secret key. It is used to verify both the data integrity and authenticity of a message.

Index

Address Space Layout Randomizer, 33
ASLR, 8, 10, 33
Biometrics, 11
BitLocker, 10, 11, 18, 24, 25, 35, 36
Defender, 8, 10, 27, 36
EFS, 10, 25
Encrypting File System, 25
FBI, 4, 7
Firewall, 8, 10, 28, 32
firewalls, 8
GP, 31
GPO, 8
Group Policies, 10, 31
Group Policy Objects, 19
IE7, 10, 18, 26
Internet, 4, 7, 8, 18, 26, 32
Internet Explorer, 18
malware, 6, 7, 8, 15, 18, 36
NAP, 10, 30, 31
Network Access Protection, 30
Remote Laptop Security, 26
Rights Management Service, 26
RLS, 26
RMS, 10, 26
Security Center, 8, 10, 32
Service Hardening, 10, 29
Sidebar Gadgets, 10, 17
Smart cards, 11
Task Manager, 10, 29
TPM, 11, 18, 19, 24, 25, 35
Trojan, 8
Trusted Platform Module, 11
UAC, 10, 15, 16, 18
User Account Control, 15, 18, 27, 32
Virtual PC, 10, 26, 36
Virtual PC 2007, 10, 36
Vista, 1, 7, 9, 10, 11, 15, 16, 17, 18, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36
VPC, 26, 27
Windows, 1, 5, 7, 8, 11, 15, 24, 26, 27, 28, 29, 31, 32, 33, 34, 35, 36, 37
XP, 1, 5, 7, 8, 10, 15, 17, 18, 25, 26, 27, 28, 29, 30, 31, 32, 33, 35, 36

Last Updated: February 16th, 2012

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

RSA Conference 2012	**San Francisco, CA**	**Feb 26, 2012 - Feb 27, 2012**	**Live Event**
SANS Secure Singapore 2012	**Singapore, Singapore**	**Mar 05, 2012 - Mar 17, 2012**	**Live Event**
SANS Germany 2012	**Stuttgart, Germany**	**Mar 05, 2012 - Mar 10, 2012**	**Live Event**
Mobile Device Security Summit	**Nashville, TN**	**Mar 12, 2012 - Mar 15, 2012**	**Live Event**
BETA SEC528 SANS Training Program for the New CompTIA Advanced Security Practitioner Certification	**Boston, MA**	**Mar 12, 2012 - Mar 17, 2012**	**Live Event**
SANS 2012	**Orlando, FL**	**Mar 23, 2012 - Mar 30, 2012**	**Live Event**
SANS Abu Dhabi 2012	**Abu Dhabi, United Arab Emirates**	**Mar 31, 2012 - Apr 05, 2012**	**Live Event**
SANS Northern Virginia 2012	**Reston, VA**	**Apr 15, 2012 - Apr 20, 2012**	**Live Event**
SANS Cyber Guardian 2012	**Baltimore, MD**	**Apr 30, 2012 - May 07, 2012**	**Live Event**
SANS Secure Europe 2012	**Amsterdam, Netherlands**	**May 07, 2012 - May 19, 2012**	**Live Event**
SANS Security West 2012	**San Diego, CA**	**May 10, 2012 - May 18, 2012**	**Live Event**
SANS Secure Indonesia 2012	**Jakarta, Indonesia**	**May 14, 2012 - May 19, 2012**	**Live Event**
SANS Toronto 2012	**Toronto, ON**	**May 14, 2012 - May 19, 2012**	**Live Event**
SANS Secure India 2012	**OnlineIndia**	**Feb 20, 2012 - Feb 25, 2012**	**Live Event**
SANS OnDemand	**Books & MP3s Only**	**Anytime**	**Self Paced**