

Secure Computing® is a global leader in Enterprise Security solutions. Powered by our TrustedSource™ technology, our award-winning portfolio of solutions help our customers create trusted environments inside and outside their organizations.

# Protecting the Enterprise in a Windows Vista Environment

## Table of Contents

The Nature of Commercial Operating Systems .....	2
Windows Vista – Raising the Bar.....	2
A Critical Look at Vista’s Security Enhancements .....	3
Limitations.....	3
Circumventing Vista’s Protections .....	4
Vista Security: The Good and the Bad .....	4
User Account Control (UAC) .....	4
Windows Firewall.....	5
Kernel Enhancements .....	5
Windows Vista Address Space Layout Randomization (ASLR).....	5
Using Third-Party Systems with Windows Vista .....	5
The Greatest Risk .....	6
Considerations for Security in A Windows Vista-Based Environment .....	7
Secure Computing and Windows Vista Environments .....	7
SecureOS.....	8
Unified Threat Management.....	8
TrustedSource .....	8
Summary and Conclusion.....	9

### Secure Computing Corporation

#### Corporate Headquarters

4810 Harwood Road  
 San Jose, CA 95124 USA  
 Tel +1.800.379.4944  
 Tel +1.408.979.6100  
 Fax +1.408.979.6501

#### European Headquarters

Berkshire, UK  
 Tel +44.0.870.460.4766

#### Asia/Pac Headquarters

Wan Chai, Hong Kong  
 Tel +852.2598.9280

#### Japan Headquarters

Tokyo, Japan  
 Tel +81.3.5339.6310

For a complete listing of all our global offices, see [www.securecomputing.com/goto/globaloffices](http://www.securecomputing.com/goto/globaloffices)

## The Nature of Commercial Operating Systems

---

The Microsoft Windows Vista operating system represents a new direction for Microsoft, and it is significantly different from previous versions of Windows. There are some areas where Vista has done well in bringing security and added functionality into the mix, and there are some areas that need improvement. But, any commercial operating system, from Microsoft or any other vendor, is never secure enough on its own.

There is no such thing as a perfect commercial operating system. To think that Vista, or any other commercial operating system from Microsoft or any other vendor would be completely bulletproof would be flawed logic. Microsoft has focused heavily on security in its Vista release, and that is a positive for users. However, there are many complaints about Vista's security, and many users, bloggers, and armchair industry observers are quick to point out that Vista still has security flaws. The fallacy of their argument is that they assume that it would be possible for Vista to have none, and that is incorrect. Of course, Vista has flaws, and within this paper, we will look at some of them, and how to improve on them by running Vista with gateway security and a unified threat management platform based on a Secure Computing® security appliance that runs on a separate, hardened, and unbreakable operating system.

With more than 50 million lines of code contained in Windows Vista, security vulnerabilities are inevitable, regardless of how thorough Microsoft may have been. In fact, if a commercial operating system were completely bulletproof and absolutely secure, it would probably be unusable to most consumers.

The very nature of flaws and vulnerabilities is that in many cases, they are completely unpredictable until they have been exploited. There should therefore be two central focuses in achieving security: First, to create a more secure operating system. To set out to create a completely flawless and impenetrable operating system with any significant functionality, is of course, impossible but the OS vendor should, at the very least, place great emphasis on security and strive to achieve the greatest level possible. In addition to that, issue regular security patches to address flaws and vulnerabilities that could not have been foreseen in the original design. This first focus is the domain of the OS vendor, and Microsoft, despite some criticisms and existing vulnerabilities, has at least succeeded in bringing security to the forefront. Compared with other commercial operating systems, Windows Vista has an advantage in some areas, while competing systems retain an advantage in others. That is not to say you should not purchase Vista; in fact there are many advantages that the OS delivers, and despite some high-profile security criticisms, the OS still has several useful security-related innovations. Yes, there are vulnerabilities and security holes, but still, Vista represents a major step forward over previous versions in regards to security. Use it, but use it with caution as you would any OS, and do not expect the Windows Vista security features to provide you with all the security you need.

The second focus is on creating a security infrastructure that can work with the operating system, made up of specialized security products, including dedicated security appliances, authentication devices, and software that includes URL filters, anti-virus, anti-spam, anti-spyware, and global reputation engines. This second focus is the domain of the security vendor. The most ideal approach then, is not to look exclusively to the OS for security, no matter how secure that OS claims to be; but rather, to take advantage of the security of the OS while at the same time putting together an integrated security infrastructure built with products from vendors who specialize in security. Deploy Windows Vista to get the latest features available, and to enjoy the new focus on security that Microsoft has initiated. But don't expect Vista to be a perfect security platform, as it is not, and was not meant to be a security platform. It is, first and foremost, a commercial operating system, and must be used with other security tools to be most effective.

## Windows Vista – Raising the Bar

---

Vista is said to represent a philosophical change at Microsoft with the adoption of defense-in-depth, multilayer security, and the principle of least privilege; in addition to revising their product development process to incorporate security improvement to a greater degree. Compared with other Windows operating systems, Vista is the most secure to date. While some of the security improvements

have brought problems of their own (a side effect that will be discussed later in this paper), it does nonetheless represent a new and positive direction. A brief overview of the most important security improvements follows:

**User Account Control** – This feature was designed to allow users to change common settings while running as a standard user without having to have administrative privileges. As a result, ordinary users can make non-threatening changes to their systems, but at the same time, are locked out from making other changes that could result in improper configuration or negatively affect system stability.

**Authentication** – Vista’s new authentication architecture supports passwords and smart cards, and also makes it easier for developers to integrate stronger authentication methods, such as biometrics and hardware tokens.

**Anti-Malware** – Vista includes Windows Defender, which protects against pop-ups, spyware, and some other security threats. Vista can also prevent many different worms, viruses, and other types of malware from entering the system.

**Network Access Protection** – This feature is an agent that prevents a Vista client from connecting to the network unless it has been configured with the proper security updates and virus signatures.

**Firewall** – Vista includes a personal software firewall with application-aware outbound filtering, making it useful for filtering out potentially risky or unauthorized applications.

**Windows Service Hardening** – This service restricts some Windows services from performing unusual activities in the file system, registry, or network that may allow malware to install itself or attack other computers in the network.

**Internet Explorer Enhancements** – Building on User Account Control, Vista limits Internet Explorer so that users can easily browse the Web, but not modify user files or settings by default.

**Data Protection** – This feature helps to protect your sensitive data by enforcing document usage policies.

## A Critical Look at Vista’s Security Enhancements

---

Vista attempts to do a lot—far more than any previous version of Windows—but in setting out these ambitious goals, Vista has become an incredibly large and complex operating system with over 50 layers of dependencies. There is a natural relationship between the number of lines of code in a given program (in this case, over 50 million lines) and the number of expected vulnerabilities.

A secondary factor to consider is that, to at least some degree, the new security features of Vista have come at the cost of greater complexity for the end user. Security and simplicity are natural enemies. Of course, all users want their systems to be secure, but very few want to actually do anything about it. Generally, users want to use simple passwords, they don’t want to be presented with cryptic access messages and constant yes/no decisions, and they want security to work right out of the box without the need for detailed configuration.

Is it possible to have strong security, and still have it be user-friendly? Yes, it is. But it is not possible to have it with Windows Vista’s security features alone. Vista’s scope of security does not go far enough, and the security that does exist is often too complicated for ordinary end users. To have strong, user-friendly security in a Windows Vista environment, it must be incorporated with a third-party system.

### Limitations

The security features of Vista do have limitations, and no security expert would seriously recommend that an enterprise with sensitive information rely exclusively on Vista for network security.

Windows Defender, for example, is an anti-malware tool meant for individual users only, not the enterprise. Anti-malware is best approached with a multi-layered strategy, with Vista’s Defender working only as one part of an extended group of anti-malware technologies, if at all.

Additionally, Vista's firewall is not, nor was it designed to be, a full-fledged network firewall. It is described as a "personal" firewall, and even at that level, it does not possess the same security functionality and safeguards as a security appliance that runs on a hardened OS. Nonetheless, it can offer some security functionality to individual workstations that lack any other firewall.

### Circumventing Vista's Protections

Vista's security is generally an improvement over Windows XP, but there are still ways to get around the protections and attack the computer. Social engineering techniques and phishing will still continue, and if the phisher is clever enough, it's easy to bypass any protections that are put up. Additionally, attackers may choose to focus on application-layer attacks which often are able to bypass the operating system, since they attack individual programs and not OS vulnerabilities.

### Vista Security: The Good and the Bad

During the first six months of availability for Windows Vista, Microsoft released four Security Bulletins and updates that addressed 12 vulnerabilities. Of those 12, the National Institutes of Standards (NIST) rated ten of them as High severity, one as Medium severity and one as Low severity. Vulnerabilities, especially ones rated "High," are never good, and this certainly points out the fact that Vista's security is not perfect. However, one must not lose sight that virtually every other available operating system, including Linux distributions and the Apple Mac OS X, has had a similar or greater amount of vulnerabilities for their first six months of availability as well. It is inevitable that any commercial operating system will have vulnerabilities.

The Windows Security Center is beneficial in the sense that it automatically handles the monitoring of Vista's multiple layers of security continuously and in the background. However, the limited choices in disparate third-party solutions that can be easily utilized for security within the security center will be a problem for those who wish to achieve the highest level of security possible.

### User Account Control (UAC)

User Account Control (known as "User Account Protection" in the earliest release of Vista) makes it possible for someone to run as a standard user, while still performing some administrative tasks. Unix-based operating systems deliver some level of enhanced security over earlier versions of Windows, by running applications at the minimum necessary level of privilege. UAC brings this concept to the Windows environment.

In the past, many ordinary users of Windows had to be configured as "Administrator" because even tasks like installing a printer required administrative rights. This creates several security issues. For example, if the pre-Vista Windows user is running as an Administrator, then any application he/she is using is by default also running with administrative privilege. If a hacker compromises the application being run by the user, the hacker assumes the rights of the user and is able to quickly gain full administrative rights to the PC.

User Account Control adds an element of balance to account privilege, by reducing the necessary level of privilege necessary for normal day-to-day tasks, while also adding additional restrictions to those tasks that truly require administrative rights, such as installing software. Once enabled, if a task or application requires administrative privilege, the user is prompted with a Windows Security Dialog telling the user that the task requires administrative rights and asking the user to authenticate with administrative credentials.

While this model does solve some of the problem of ordinary users having unnecessary Administrator privileges, it creates another problem. It is often seen as unwieldy and confusing, and may produce too many alerts, using overly complex and technical terms in its user messages. This model is anything but user-friendly and transparent. It transfers decisions directly to the end user that, in a system that incorporates a third-party gateway firewall protection system with Vista, would be made automatically. End users faced with such an abundance of yes/no questions that are often difficult to understand, will tend to simply accept everything just to get the task at hand completed.

## Windows Firewall

Microsoft includes a personal firewall in Vista that includes application-aware outbound filtering, which is an important feature for any firewall. This feature could, for example, allow an administrator to permit a given application (such as P2P or IM) to run locally, but also prevent it from communicating across the network.

The Vista firewall however, is very limited in comparison to commercial firewall solutions. The Vista firewall still is not able to restrict specific application commands, and lacks time-based rules, IDS/IDP capabilities, and the ability to monitor active connections. It also provides only very rudimentary logging capabilities, and fails to address the lack of any central management features that would make it useful in a business setting. While it may be adequate for a casual home user that is not connected to a corporate network, it falls short as a business tool in many ways. By default, half of the Vista firewall's security features are disabled, and block only inbound traffic, with all outbound traffic permitted. Configuring the Vista firewall to block outbound connections is a difficult process that may require assistance from an expert.

Finally, simply running a firewall on the same operating system and on the same machine as user applications and potentially sensitive user data is a poor policy decision.

## Kernel Enhancements

Two new kernel enhancements include enforced driver signing and kernel patch protection. Enforced driver signing requires drivers running at the kernel level to be tested and digitally signed by Microsoft. This ensures that the driver comes from a legitimate source and has been tested by Microsoft to minimize instability issues. Kernel patch protection (Patch Guard) prohibits the kernel from being patched by a third-party product, a feature that mitigates the risk of Trojans and rootkits taking over the operating system at the kernel level.

Unfortunately, both of these enhancements apply only to the 64-bit version of Windows Vista, and the majority of users run the 32-bit version.

## Windows Vista Address Space Layout Randomization (ASLR)

ASLR randomizes both the stack and heap and further randomizes the address and location of EXE and DLL files that are part of the operating system. Randomizing makes it much more difficult for exploits that take advantage of memory flaws such as buffer overruns, and perhaps rootkits, to be effective against Vista.

Note that ASLR is certainly not a replacement for flawless code, but in an OS with 50 million lines, flawless code is an ideal that is impossible to achieve. While ASLR makes it more difficult for a given exploit to work, it does not make it impossible. For example, in Windows Vista Beta 2 an EXE or DLL is loaded into one of only 256 different memory locations; hence if an exploit needs the address of the EXE or DLL it still has a one in 256 chance to succeed.

Still, one in 256 is better odds, and this brings up the wisdom of a multi-layered security defense. If one security system has a small chance of allowing an attack to get through, two security systems with equal odds working together will dramatically reduce the odds against attack, rendering the attack nearly impossible. A multi-layered defense strategy dramatically decrease the odds that an attack will get through.

While ASLR will help to thwart the actions of some malware, such as those dependent on buffer overflows and perhaps some legacy rootkit technology because of the added complexity it brings to bear, it can also possibly introduce its own new security issues and may be problematic with legacy software. If a legacy application is hard-coded to look for an operating system DLL at a specific location, it will not work with Vista while running ASLR.

## Using Third-Party Systems with Windows Vista

The security enhancements of Windows Vista do make it more capable of surviving attacks than previous versions, but it by no means makes your network bulletproof. There are several factors that underscore Vista's continued vulnerability, and the need for third-party security and gateway protection when using Vista:

- The user's ability to override Vista security and run a rogue or untrusted application at an elevated privilege or kernel level poses a significant risk that will remain unmitigated in the Vista 32-bit version. A secure operating system should be able to contain and mitigate the actions of rogue software. Having a UAC that places most of the decision-making responsibility on the end user is not an acceptable solution to the problem.
- Hacking tools have evolved at a faster rate than most vendor security initiatives. One only has to look at the state of "fuzzing" technology; fuzzing programs provide for an automatic replacement of normal input and interfaces for a given protocol or application. This automated "replacement" input is computer-generated, ambiguous and random in nature. By design, a fuzzer automatically seeks to cause abnormal behavior in the protocol or application. The abnormal behavior is indicative of a software bug and can be further tested to determine if the abnormal behavior (bug) is exploitable. The use of these automated fuzzing tools by the research community to discover bugs and enable them to then create exploitable vulnerabilities has clearly outpaced software developers' security initiatives.
- 32-bit implementations of Windows Vista will be the most widely deployed and will lack many of its key security mechanisms found in the 64-bit versions. Hence, the largest part of the installed base will be the most vulnerable.
- In order to meet the constraints of operating on Windows Vista, many third-party applications will require major software revisions. The lack of security products that are able to work with Windows Vista to grasp the enormity of the problem. Further, in the broader market of business software, many vendors have not yet made the commitment to support the 64-bit version because of the ever-changing requirements of writing software that is fully compatible with Vista. When Vista begins to gain widespread adoption, some vendors will be forced to roll out solutions quickly to meet market demands, and in all likelihood will introduce new previously unseen vulnerabilities in both the application and perhaps even with Vista. While Microsoft expects Vista adoption to outpace that of Windows XP software, vendors may still have plenty of time—according to Forrester Research, they do not expect Vista to reach mass deployment until 2008.
- While Windows Vista does address, to a limited degree, spyware and known malware, it does not address the spam problem that Bill Gates in 2004 promised would end in two years, nor does it in any way address today's fastest-growing threat—the data leakage issue that is fueling identity theft.

Setting aside for the moment any criticisms of Microsoft's security features, it is important to understand the nature of security and the best way to approach it. Most security analysts recommend using disparate software to mitigate "common faults" that exist in software, e.g., when using a single software for both the operating system and the protective security software. If the operating system software bug results from a common fault within the software, then the same vendor's software used as a protective mechanism may in fact also be vulnerable to the same fault, thereby negating its protective capability. That is, if the security software is run on the same server and the same OS as the applications being run, any vulnerabilities on the commercial OS could be used to exploit the security software as well.

The goal of the security system is to protect, among other things, the OS. But if the security system runs on the very OS and server it is trying to protect, then the security system itself may be at risk of attack. While it is beneficial for the OS to include these features for basic desktop protection, it is only a beginning—a supplemental protective measure, which is better than nothing. Multi-layered security is the most effective type of security. However, security must go beyond the protective features of the commercial OS, and the security should be run on a separate, dedicated appliance, and on a separate, hardened OS designed specifically to be the foundation of the security architecture.

### The Greatest Risk

All of the above-mentioned features of Windows Vista, while somewhat problematic, do provide additional security utility. There are valid criticisms that have been made about these and other Vista features. However, the greatest risk of all is that a Vista user could gain a false sense of security. Vista users must not rely exclusively on the built-in security features of the OS. Regardless of how good they may be, and regardless of how many patches Microsoft issues in the future, the approach of running security alongside other productivity applications, on the same server, and on the same commercial OS

as all other applications, is inherently flawed. By design, a commercial OS must have certain usability features and a greater level of access than would a hardened OS used exclusively for security applications run on a separate security appliance. Running a software firewall directly on a workstation may be adequate for home users with low security requirements, but it just doesn't fit the bill for good corporate security. Yes, Vista has more security features than before. But even if one does get around the flaws that have been identified by many observers, it would be a grievous mistake to believe that the built-in security contained in Vista would be enough to protect the enterprise—or for that matter, even a small- or medium-sized business.

## Considerations for Security in a Windows Vista-Based Environment

1. The security enhancements in the Windows Vista operating system will drive hackers to further expand their application-layer and Web-application attacks. Hence, gateway security at the application layer will be more important than ever in a Vista environment. Since Vista does not incorporate gateway security, it must be provided by a third party.
2. The inability of anti-virus or anti-malware products working with Windows as a third-party security product will necessitate that, in order to protect a Windows Vista network, malware will need to be detected on the wire and neutralized before it reaches the operating system. Signature-based anti-virus, IDS and IPS products working at the kernel level of the operating system are simply inadequate without an additional layer of protection at the gateway.
3. Weak passwords continue to be a problem, and Vista has no solution to mitigate this problem. Hackers will naturally shift their attacks to the weakest link, which will increase the need for stronger authentication. Further, the lack of significant improvements in combating insider threats will still need to be addressed by third-party solutions. Identity and Access Management (IAM) will be a necessity in addressing the issues of weak passwords for remote and internal users and also provides a necessary additional layer of security for the required segmentation and access control within the intranet.
4. Spam will not go away with Vista's security improvements. In fact, social engineering is poised to increase via email and messaging as hackers probe for weak links to overcome any resistance imposed by new security enhancements in other attack vectors. Hence, anti-spam bolstered with global sender reputation capabilities such as Secure Computing TrustedSource™ will be a necessity within a Vista environment.
5. One of the fastest-growing crimes in America today is identity theft, and it is being fueled by data leakage. Windows Vista in a 64-bit enterprise version offers a new feature called Trusted Platform Module (TPM) that provides for the storage of digital certificates, encryption keys and passwords on a hardware "chip" on the system motherboard. This provides for the encryption of the entire hard disk, including the operating system and boot sector. Whole disk encryption is significantly more secure than traditional file- or folder-level encryption. However, this is also available only on the 64-bit version of Vista.

## Secure Computing and Windows Vista Environments

Microsoft has added security features to Vista, and despite some existing vulnerabilities, it is a step in the right direction. But no serious security expert would claim that running Windows Vista reduces or eliminates the need for third-party security products. The Vista security features are just one layer in a multi-layered defense built on Secure Computing's Unified Threat Management environment. Protecting your Windows Vista environment with Secure Computing's all-encompassing suite of security products lets you make the most of Vista, without having to deal with the complexities and limitations of Vista's own security tools.

One concern that has been raised about Vista is the slow pace with which some third-party vendors have been able to incorporate their products with Vista. Many products, including some security products, that users have gotten accustomed to, will not work with Vista. Deploying a Secure Computing gateway appliance means this is not a concern, because the security infrastructure is contained within a separate gateway appliance running a completely separate operating system that is used only for the security applications and nothing else.

## SecureOS

Secure Computing's patented SecureOS® Type Enforcement® technology provides a resilient foundation to Secure Computing's Sidewinder® line of gateway security appliances. There is a significant difference between a commercial operating system and a "hardened" operating system. It is certainly possible to argue all day about the relative advantages and drawbacks of Windows Vista, but in regards to security, it comes down to this: Vista is a commercial operating system, and as such, should not be used to run your network's security. SecureOS is a closed, hardened OS that runs Secure Computing's gateway security appliances. Because it is not necessary to run productivity applications on the operating system, the appliances can run in a heightened state of security that would be impossible with a commercial operating system. SecureOS and Type Enforcement technologies protect everything in the system—every file, directory, application, and more—against root access. All software hosted on the Sidewinder appliance is protected, and installing malicious software or orchestrating a buffer overflow attack, or any number of other known or unknown attacks, is impossible. Type Enforcement, upon which SecureOS is built, is a mandatory access control (MAC) technology. This approach allows the Sidewinder's software to be hard-coded by the developer, so that no user under any scenario is allowed to reduce the level of access restriction imposed by the software itself. This also makes it impossible for any foreign software to be executed on the Sidewinder. By itself, Windows Vista would never be able to provide this level of protection. But Windows Vista with Secure Computing's gateway security appliances can.

## Unified Threat Management

The concept of Unified Threat Management (UTM) centralizes multiple security functions onto a single platform, usually a separate appliance that functions as a firewall. One of the most innovative developments in firewall technology, UTM is the fastest-growing segment of the firewall market. The result is much simpler management, greater efficiency, and less expense; in addition, this model provides a greater measure of protection just by virtue of being on a separate appliance (and typically a separate OS as well). While Windows Vista does offer multiple security functions, Vista's security environment cannot truly be called Unified Threat Management because it does not contain all the elements of firewall—intrusion detection and prevention, anti-virus, anti-spam, and URL filtering—and it merely places the security functions it does have at the desktop level, not taking into account the need for gateway protection.

There are many reasons, beyond simple convenience and practicality, for combining multiple threat protection applications under the same interface and on the same dedicated appliance. Most attacks today are blended attacks, which do not use any single attack vector exclusively. For example, a blended attack may target multiple protocols, such as email (SMTP) and Web (HTTP). It may do this first by sending out an email, which in itself may not contain any malware, but instead tricks the recipient into clicking on a Web link. The recipient is then taken to an infected site, where the malware is then downloaded onto the computer. Mitigation of this sort of attack can take place either in the email messaging protection (anti-spam) application, which would recognize the nature of the attack, or in the second stage, where the user attempts to go to the infected Web site and would be blocked by the URL filter, which would recognize the site as not being legitimate.

## TrustedSource

In a complex threat environment, simple reactive systems are not enough. While signature-based prevention may well be one important part of a multilayered protection environment, signature-based systems cannot detect malware that has not yet been discovered and categorized. This presents one of the most important reasons for going beyond the security protections included in Windows Vista—Vista does nothing to address zero-day attacks.

A zero-day attack, one which targets a vulnerability that has not yet been patched, or uses new virus code that has not yet been included in signature databases, is beyond the scope of Vista, and requires the special technology included with Secure Computing appliances. Secure Computing's TrustedSource is a reputation system, which keeps tracks of a sender's behavior and whether a sender is deviating from known behavior. TrustedSource assigns a reputation score, and classifies senders into categories based on an in-depth analysis by processing more than a dozen behavior attributes for each sender. Through this method, TrustedSource accurately defines a precise reputation score for every sender, offering effective protection against spam, viruses, and other types of unwanted traffic.

## Summary and Conclusion

---

Upgrading to Windows Vista can be a safe and sound choice, if done in conjunction with your overall security strategy. Windows Vista does indeed have some security vulnerabilities and concerns, but at the same time, there have been security improvements in this operating system. This seemingly incompatible statement actually is very obvious on many levels. Vista is a much larger operating system with many more features than ever before, many of them having to do with security. But because it is new, and not just a mere standard upgrade, one must expect it to be imperfect.

There are two basic errors in judgment that are made with regard to upgrading to Vista: First, to believe that it should not be done at all, and second, that it should be done in isolation and without additional security protection. In addressing the first error, there is no reason that a successful upgrade to Vista cannot be executed, so long as it is done within the framework of an overall third-party security infrastructure. With regard to the second error, it is possible to be lulled into a sense of false security by believing that the many security features of Vista render all other security precautions unnecessary. This would be a very dangerous practice indeed. Regardless of how stable, complete and secure the operating system may or may not be, running firewall and other security software on the same OS as the day-to-day productivity software is a disaster waiting to happen. Firewall and other security-related software requires a hardened operating system running on a separate dedicated appliance to provide for isolation, and to allow the commercial OS (in this case, Vista) to do its job unimpeded.

Upgrading to Vista can allow individuals to take advantage of the additional features of the OS. The upgrade can be worry-free if done with the following strategies in mind:

1. Preserve your third-party security environment, which should be run separately, on a dedicated appliance running a hardened operating system.
2. Maintain a complete Unified Threat Management security strategy, which incorporates multiple security functions on multiple layers. The security protections of Vista are but one layer, and do little to accomplish gateway protection.
3. Incorporate reputation-based technology that goes beyond all standard security protections to protect against zero-day attacks.