

Enterprise Security Benefits of Microsoft Windows 7*

- Designed with a focus on security.
- Helps improve enterprise security by driving Web-based applications to take advantage of its higher security settings and features.
- Helps protect against malware and phishing scams.

Information security is a critical concern for Intel IT. New threats are continually evolving, and over time, this has forced us to invest in various security controls and mitigation strategies. As part of a three-month evaluation of Microsoft Windows 7*, Intel IT identified broad new security capabilities, summarized in Table 1, that significantly enhance enterprise security. These include features designed to address many existing threats and potentially reduce the need for additional controls and mitigation. The security capabilities were an important factor in our decision to deploy Microsoft Windows 7 Enterprise* across Intel's enterprise environment.

Key features include:

- **Improved security foundation.** Microsoft Windows 7 was developed using a secure process designed to reduce vulnerabilities and includes core features designed to block common malware exploits. We found that Microsoft Windows 7 Enterprise was pre-configured with default security settings that in most cases already matched our enterprise requirements.
- **Streamlined Microsoft User Account Control (Microsoft UAC).** We require that all applications function with Microsoft UAC, which in Microsoft Windows 7 has been streamlined so there are fewer user prompts. This can increase users' security awareness and help prevent malware from installing or making changes to users' systems.
- **Microsoft Internet Explorer 8*.** Protected mode and filters make it more difficult to install malware.

We are deploying the OS on new PCs with 2010 Intel® Core™ vPro™ processors, which we are using to improve PC manageability across the enterprise. 2010 Intel Core vPro processors provide key security capabilities that complement Microsoft Windows 7 security; these include secure remote management, more-effective deployment of patches, and isolation of infected PCs.

Table 1. Security Benefits of Microsoft Windows 7*

Improved security foundation	<ul style="list-style-type: none"> ▪ Developed using Microsoft Security Development Lifecycle to reduce vulnerabilities; new core capabilities block common types of malware.
Secure default settings	<ul style="list-style-type: none"> ▪ Most services and applications, including firewall and strong network password encryption, are pre-configured to match enterprise requirements.
Streamlined Microsoft User Account Control	<ul style="list-style-type: none"> ▪ Limits applications to run with standard user rights; streamlined to require fewer prompts; increases security awareness and helps prevent malware installation.
Microsoft Internet Explorer 8*	<ul style="list-style-type: none"> ▪ Protected mode helps protect against malware downloads; new filters detect phishing Web sites and cross-site scripting attacks.
More secure applications	<ul style="list-style-type: none"> ▪ Helps us drive Web-based applications to take advantage of the higher security settings and features in Microsoft Windows 7*.

Background

Intel IT is deploying 64-bit Microsoft Windows 7 Enterprise across our environment, following a three-month technical evaluation that showed the OS meets the key requirements of our business groups.

We are deploying the OS on new PCs with 2010 Intel Core vPro processors, which provide new security and manageability capabilities that complement Microsoft Windows 7.

Information security remains a critical concern for Intel IT; we are acutely aware of our responsibility to maintain the security and integrity of Intel's intellectual property as well as employees' personal information. New threats are continually evolving, and over time, this has forced us to invest in various security controls and mitigation strategies.

Our technical evaluation of Microsoft Windows 7 included an extensive security assessment, including an analysis of capabilities designed to address existing threats.

Security Assessment

We began our security assessment with an early analysis of the enterprise security features of the OS, based on published information from Microsoft and other sources. We then conducted a detailed, hands-on security assessment, including tests of the security features and settings, as part of the Intel IT Microsoft Windows 7 technical evaluation program.

IMPROVED SECURITY FOUNDATION

We found that the OS was designed with an increased focus on security and includes significant core capabilities designed to harden the OS against security threats.

Microsoft Windows 7 was designed and developed using the Microsoft Security Development Lifecycle (SDL) software security assurance process, which systematically addresses software security during development to reduce vulnerabilities in the OS. This increased our confidence in the security of the code.

We also identified and enabled key capabilities designed to block some of the most common types of malware exploits. These capabilities include:

- Data Execution Prevention (DEP), which works with the Execute Disable (XD) bit in Intel® Core™ processors to help prevent exploits that use buffer overflow.
- Address Space Layout Randomization (ASLR), which makes it harder for hackers to target specific memory addresses.
- Safe Structured Exception Handling (SEH), designed to block exploits that use the SEH overwrite technique.

Microsoft Windows 7 includes a number of other core security features that can help prevent problems caused by malware or poorly written applications. An example is kernel patch protection, also known as PatchGuard, in the 64-bit OS that we are deploying. This blocks attempted changes to the Microsoft Windows 7 kernel. In addition, kernel-mode code integrity checks help block malware attacks by requiring digitally signed device drivers.

SETTINGS AND CONTROLS

During our testing, we determined that most Microsoft Windows 7 Enterprise default settings matched our security requirements. These default settings include the requirement that applications use strong authentication, based on Kerberos v5*, and encryption for

passwords sent over networks. The default settings provided additional confirmation that the OS was designed with a focus on enterprise security.

In addition, several tools provide more granular controls that help us identify security events and enforce security policies. An example is the Event Viewer, which makes it easier to examine and interpret individual security-related and other system events. We can also apply more granular settings when defining group policy objects to enforce configurations or group policy preferences for specific groups of users.

STREAMLINED MICROSOFT UAC

Microsoft UAC improves security awareness by helping ensure that applications and users run with standard user privileges. With Microsoft UAC enabled, users are prompted to approve sensitive functions like installation of software or changes to protected system areas. This notification allows users to make informed choices and potentially prevents malware from installing or making changes to their systems. We consider this an important benefit and require that all applications function with Microsoft UAC at its highest settings.

In Microsoft Windows 7, Microsoft UAC has been enhanced so that it generates fewer prompts. We believe the increased usability will help raise users' security awareness. Because prompts occur less frequently, users may be more likely to consider the implications of each prompt they see rather than automatically clicking to approve it.

In the future, we would like to see more granularity and configurability that would enable us to further customize Microsoft UAC to our specific enterprise security requirements.

MICROSOFT INTERNET EXPLORER 8*

We are migrating to Microsoft Internet Explorer 8, which is included with Microsoft Windows 7. This adds several important security capabilities. On Microsoft Windows 7, the browser operates in protected mode by default, running without administrative privileges and prompting users if a Web site tries to install software. This helps protect against automated malware downloads.

The application also includes other features that help protect Intel and our employees against malicious Web sites:

- The SmartScreen Filter helps users avoid phishing Web sites that attempt to gather their information for malicious purposes and alerts them if a site they are trying to open has been reported as unsafe.
- A cross-site scripting (XSS) filter helps detect and disable cross-site scripting attacks, an increasingly common type of threat.
- InPrivate browsing allows users to surf the Web without storing information such as cookies and passwords on their PCs. This potentially provides privacy and security benefits when users are accessing confidential information.

NETWORK LOCATION AWARENESS

PCs running Microsoft Windows 7 automatically detect the type of network connection available; applications such as Microsoft Internet Explorer 8 and Windows Firewall can use this information to apply different controls depending on the network type. For example, more-restrictive settings can be used if users are connected to a public network rather than the enterprise network.

DRIVING DEVELOPMENT OF MORE SECURE APPLICATIONS

Adoption of Microsoft Windows 7 is helping to increase the overall security of our enterprise environment by driving the development of more-secure applications. We have raised our security requirements based on the security settings and capabilities in Microsoft Windows 7. For example, we require that applications run in standard user mode rather than needing administrative privileges.

During Microsoft Windows 7 application testing, we tested the ability of commonly used internal and external Web sites to function with the strong network encryption and authentication settings of Microsoft Windows 7. We determined that some of these Web sites did not function properly; in these cases, Web sites were required to improve their security posture to meet the higher security settings.

We are also investigating the possibility of making digitally signed applications a requirement for external software suppliers and internal developers.

DISABLED FEATURES

Although the vast majority of Microsoft Windows 7 default features and settings matched our enterprise security requirements, we identified a few that did not. For example, we disabled Microsoft HomeGroup because it is designed for home networking and could be used to share data outside the corporate environment.

Deployment on PCs with 2010 Intel® Core™ vPro™ Processors

We are deploying Microsoft Windows 7 on new PCs based on 2010 Intel Core vPro processors, which optimize performance and

provide capabilities that complement the security benefits of Microsoft Windows 7.

Intel® Core™ i5 vPro™ processors and Intel® Core™ i7 vPro™ processors provide hardware-assisted remote manageability and security capabilities with Intel® vPro™ technology that enable us to better protect PCs down the wire. We are implementing several Intel vPro technology use cases that take advantage of these capabilities, including remote configuration, remote power management, and remote diagnosis and repair.

With remote configuration, our Service Desk technicians can remotely perform functions such as configuring Trusted Platform Module security hardware and resetting hard drive encryption passphrases. Remote power management allows PCs to be remotely booted after hours, enabling faster and more reliable delivery of security patches and other software updates. We are also evaluating a system isolation and recovery use case, which would enable us to protect against the spread of malware by isolating infected PCs at the hardware level.

PCs based on 2010 Intel Core i7 vPro processors also can run up to eight simultaneous hardware-based threads using Intel® Hyper-Threading Technology (Intel® HT Technology), allowing antivirus software and security compliance checks to run unobtrusively in the background while employees use other applications. Other hardware capabilities include Intel® Advanced Encryption Standard New Instructions (Intel® AES-NI). We anticipate that the whole-disk encryption software we are using to protect data on employees' laptop PCs will take advantage of these instructions to accelerate data encryption and decryption performance.

Conclusion

Enterprise security remains a critical concern for Intel IT. We found that Microsoft Windows 7 can significantly enhance enterprise security by offering increased protection against malware and malicious Web sites. It includes new capabilities that are designed to address many existing threats and potentially reduce the need for additional controls and mitigation.

The security features of Microsoft Windows 7 complement 2010 Intel Core vPro processor capabilities for secure remote management, isolation of infected PCs, and more effective deployment of patches.

The increased security capabilities and secure code foundation of Microsoft Windows 7 were important factors in our decision to deploy the OS across Intel.

For more straight talk on current topics from Intel's IT leaders, visit www.intel.com/it.

AUTHORS

David Fong

Senior Information Security Specialist,
Intel IT

Toby Kohlenberg

Senior Information Security Specialist,
Intel IT

Justin Philips

Senior Systems Programmer,
Intel IT

ACRONYMS

ASLR	Address Space Layout Randomization
DEP	Data Execution Prevention
Intel® AES-NI	Intel® Advanced Encryption Standard New Instructions
Intel® HT Technology	Intel® Hyper-Threading Technology
SDL	Security Development Lifecycle
SEH	Structured Exception Handling
Microsoft UAC	Microsoft User Account Control
XD	Execute Disable
XSS	cross-site scripting

AES-NI is a set of instructions that consolidates mathematical operations used in the Advanced Encryption Standard (AES) algorithm. Enabling AES-NI requires a computer system with an AESNI-enabled processor as well as non-Intel software to execute the instructions in the correct sequence. AES-NI is available on Intel® Core™ i5-600 Desktop Processor Series, Intel® Core™ i7-600 Mobile Processor Series, and Intel® Core™ i5-500 Mobile Processor Series. For further availability of AES-NI enabled processors or systems, check with your reseller or system manufacturer. For more information, see http://softwarecommunity.intel.com/isn/downloads/intelavx/AES-Instructions-Set_WP.pdf.

This paper is for informational purposes only. THIS DOCUMENT IS PROVIDED "AS IS" WITH NO WARRANTIES WHATSOEVER, INCLUDING ANY WARRANTY OF MERCHANTABILITY, NON-INFRINGEMENT, FITNESS FOR


ANY PARTICULAR PURPOSE, OR ANY WARRANTY OTHERWISE ARISING OUT OF ANY PROPOSAL, SPECIFICATION OR SAMPLE. Intel disclaims all liability, including liability for infringement of any proprietary rights, relating to use of information in this specification. No license, express or implied, by estoppel or otherwise, to any intellectual property rights is granted herein.

Intel, the Intel logo, Intel Core, and Intel vPro are trademarks of Intel Corporation in the U.S. and other countries.

* Other names and brands may be claimed as the property of others.

Copyright © 2010 Intel Corporation. All rights reserved.

Printed in USA
0710/JLG/KC/PDF

 Please Recycle
323950-001US

