

## Seven for 7: Best practices for implementing Windows 7

The early reports are in, and it's clear that Microsoft's Windows 7 is off to a fast start—thanks in part to Microsoft's liberal Windows 7 beta program and the pent-up demand for a new OS from Vista and XP users. Windows 7's market share is already 6%, a figure that is being driven by users clamoring for tighter security, faster boot-up times, greater stability and enhanced ease of use, according to market researcher Net Applications.

By Jonathan Tait, Product Marketing Manager, Sophos

and Jason De Lorme, ISV Architect Evangelist, Microsoft

# Seven for 7: Best practices for implementing Windows 7

## Introduction

The early reports are in, and it's clear that Microsoft's Windows 7 is off to a fast start—thanks in part to Microsoft's liberal Windows 7 beta program and the pent-up demand for a new OS from Vista and XP users. Windows 7's market share is already 6%, a figure that is being driven by users clamoring for tighter security, faster boot-up times, greater stability and enhanced ease of use, according to market researcher Net Applications.

## Best practices for Windows 7 security

If you're planning to roll out Microsoft's Windows 7, now is the time to strategically review your endpoint and data protection practices for all your Windows PCs, no matter which versions of the operating system you're running. There are several best practices any organization—whether a small, medium or large enterprise—should follow to protect its Windows machines from the potentially disastrous consequences of being attacked by viruses, spyware and other forms of malware:

## 1. Stop the threats

An obvious but important step is to use anti-virus software to prevent, detect and remove all the different types of malware that have the potential to cause considerable damage to your systems and your data.

One of the most common methods to detect viruses is to search for known patterns, or signatures, in executable code. However, with the increase in the number and complexity of unknown malware threats, it's possible for a user to be infected with new malware for which no signature yet exists. To counter such so-called “zero-day” threats, you should guard your platforms with an anti-virus solution that provides proactive protection that identifies new viruses by studying their behavior and prevents them from executing.

To ensure that your anti-virus solution is doing what you expect it to, you need to keep it up to date. Because new viruses can spread quickly, it is important to have an automatic infrastructure in place that can update all the computers in your organization seamlessly, frequently and on short notice to stay ahead of the latest threats.

Another simple way to prevent threats from slowing you down is to stay informed. Subscribe to anti-virus vendor mailing lists and review security-oriented blogs for up-to-date information on virus threats, support, technical information and new product developments.

### Recommendation

Data Execute Prevention (DEP) prevents code from executing in areas of memory intended for data storage. We recommend you check your BIOS settings to enable DEP support (NX enable) and to enable DEP for all applications.

Address Space Layout Randomization (ASLR) randomizes the locations in your computer memory that Windows will load essential system libraries. When used with DEP, ASLR makes it more difficult for malware to take advantage of security vulnerabilities in your browser, plugins and applications.

By deploying Sophos Endpoint Security and Data Protection in conjunction with Windows 7 you can benefit from even greater security. Sophos provides a run-time Host Intrusion Prevention System (HIPS) to watch the behavior of your applications as they run. This enhances your protection against zero-day malware by looking for behaviors that are malicious before a signature has ever been written.

The central management console, Sophos Enterprise Console, allows you to monitor, update, and take actions from a single point to be sure your anti-virus software is operational, up to date and compliant with policy across your entire organization. With it, you can be confident that your Windows 7 computers are safe, and easily schedule scans to check for malware at times when your computers are not in use.

## 2. Ensure safe web browsing

The internet has rapidly become a mission-critical tool for many businesses. As a result innocent websites have become targets for malware writers and hackers looking to infect visitors with the aim of stealing company confidential information, spreading malicious code or even creating botnets for distributing further malware or spam.

Thousands of systems are infected every day through users innocently browsing trusted sites that have been subject to SQL injection attacks, exploiting security vulnerabilities and inserting malicious code.

It's a tough job balancing employee productivity by opening up the internet with ensuring protection against all the potential threats out there, but there are some simple steps you can take to get you on your way.

### Recommendation

Windows 7 includes Internet Explorer 8 by default and is protected by both DEP and ASLR. In addition, it introduces a new security feature to protect against surfing to malicious sites called SmartScreen. SmartScreen presents a warning for cross-site scripting, phishing, and other known malicious destinations. This combined with IE8's protected mode makes for much safer surfing.

Sophos enhances this by providing a Browser Helper Object (BHO) that plugs into IE to analyze dynamic content on websites for malicious code and exploits. If dangerous web code is found an alert can be presented to the user, as well as reported back to Enterprise Console for centralized logging and reporting.

In addition, you can further protect your computers with a web security appliance that will stop malware and block anonymizing proxies and other unwanted applications at the gateway. Implementing a layered approach to web security means that your computers are protected both in and out of the office.

### 3. Keep computers patched

Rogue hackers are focusing more than ever on exploiting holes in third-party plugins and anything that retrieves content from the internet. Attackers continue to target the operating system, but are increasingly looking to applications your browser loads to view media, documents, and other file types.

Regularly check the websites of your third-party application vendors to find out whether they have released updates. Many software vendors also issue security advisories. For example, Microsoft runs a mailing list that warns of security loopholes and other problems found in Microsoft's software, and offers patches to button them up. Check with your vendors and subscribe to their notification lists to be sure you are aware of new issues as they are discovered.

When a new security hole is found in an application or operating system and a patch is available, organizations should be ready with an infrastructure for testing that the patch works properly and for rolling it out across their user base as quickly as possible.

#### Recommendation

Windows Update helps keep your computers safer—and your software current—by gathering the latest security and feature updates from Microsoft via the internet. In Windows 7 this is now part of Action Center, which makes updating even easier.

To ensure that Windows Update is turned on when computers are connected to your network, you can use the network access control features in Sophos Endpoint Security and Data Protection. It will assess managed and unmanaged computers and can also check that other key security software is enabled and up to date.

### 4. Bolster your data loss prevention (DLP)

The malware threat used to be about the writers making as much noise as possible to gain notoriety. However, more recently it has become a criminal enterprise that's out to steal personal information. In light of this, you should also consider the steps you can take to protect your data from accidentally getting into the wrong hands.

There are four components of data protection that you need to consider:

- » **Application control** enables you to manage the applications you allow employees to use. This ensures adherence to your security policy, and that sensitive data cannot leave your organization via applications such as peer-to-peer file sharing or instant messaging.
- » **Device control** provides a way to define and apply a comprehensive policy across your organization that controls what devices your employees can and cannot use. Employees have the flexibility they need but don't put the business at risk.
- » **Data control** ensures that users are not accidentally transferring sensitive data to their devices and applications. Implementing a data loss prevention solution can be costly and complex, so look for a solution that delivers this functionality as an integrated part of the endpoint solution.
- » **Encryption** ensures that the data on laptops and USB thumb drives is protected for all eventualities—because people lose things. Implementing encryption may not be as straight-forward as many people believe, so there are several factors to consider: You need to ensure that the initial implementation is successful; that you can manage and change the encryption policies across your organization; and, above all, that the solution doesn't get in the way of your users' daily tasks.

### Recommendation

Windows 7 retains the data protection technologies available in Windows Vista like the Encrypting File System (EFS) and built-in Active Directory Rights Management Services technology. These technologies provide an excellent platform for protecting data at rest.

For data in motion, Sophos provides DLP integrated directly into its endpoint client software. By taking advantage of Sophos' centralized management capabilities all security policies can be managed within a single console. In a single scan, Sophos Endpoint and Data Protection can enforce DLP rules at the same time it looks for malware and other suspicious content.

Windows 7 provides for more granular USB port controls through the deployment of Group Policy Objects (GPOs) that can help you protect sensitive data. Windows 7 also provides improvements to its BitLocker technology by introducing BitLocker To Go, which enables encryption to be deployed to FAT32-based removable disk drives like USB memory sticks and portable hard disks.

Sophos Device Control builds upon Windows 7's approach by enabling more granular controls, down to a per-device basis, while managing your policies using the groups already defined for other security functions.

Windows 7 adds to the application controls available for Windows XP and Vista with the introduction of AppLocker. AppLocker enables administrators to take a whitelist/blacklist approach to application management that eases the burden by not relying on hashes or signatures of applications. This provides an easier method of updating and deploying software without needing to approve every minor revision.

The Sophos approach also allows application updates without the need for GPOs. Sophos policies are managed through Enterprise Console

and the burden of defining applications is left to SophosLabs. Once a policy has been established, SophosLabs continuously updates the software definition list, and can even detect applications that are already installed, or require no installation. This style of application control not only detects applications during installation, but also at run-time. Sophos policies can be enforced against Windows XP, Vista and 7 installations, easing the transition to newer operating environments.

Microsoft BitLocker is a full disk encryption feature included in the Ultimate and Enterprise editions of Microsoft's Windows Vista and Windows 7. With the release of Windows 7, BitLocker added a new feature to encrypt removable devices. Sophos provides a management framework that enables an organization to centrally manage both its Windows XP desktops and BitLocker encrypted drives on Windows Vista and Windows 7.

## 5. Manage user privileges

Windows 7 provides more ways than ever to ensure a safe secure computing environment. With the introduction of User Account Control (UAC) Microsoft provides more control for network administrators to ease users into running with standard user accounts. When UAC is enabled it prevents users from making system level changes without an administrator's approval. This better secures desktops from drive-by malware attacks taking advantage of users Administrative rights, but also simplifies the process for administrators to authorize behaviors that they know to be safe.

In addition to running users without administrative privilege, Sophos recommends making a few additional changes in your Windows 7 deployment to take full advantage of the enhanced security Windows 7 provides.

For example, Microsoft has introduced a capability to better manage password rotation. In combination with settings that require you to change your password every X days (90 is a good default) and not reuse up to X passwords (5 is recommended) you can now set a GPO to not allow you to change your password until it is expired. Sophos recommends taking advantage of this capability because it prevents people from continuously rotating their password to subvert policies and return to their original passwords.

## 6. Prevent security loopholes

With more and more employees looking for increased mobility, it's becoming harder for you to ensure that all computers, including roaming laptops, are meeting the levels of security you need to protect your business, such as running an up-to-date anti-virus solution and having their firewalls enabled.

Sophos recommends you deploy comprehensive security policies to check that any computer accessing the network—even those not owned by the company—are in full compliance. Such policies ensure that only those that do meet your required standards are permitted access to your corporate network—if they don't meet the standards, you can keep them at bay.

### Recommendation

Windows 7: Network Access Protection (NAP) was introduced in Windows Vista and remains a key component of Windows 7. NAP is designed to help administrators maintain the health of the computers on the network, which in turn helps maintain the overall integrity of the network. It is not designed to secure a network from malicious users.

Sophos integrates Network Access Control (NAC) into endpoint protection to help you to identify managed and unmanaged computers with potential security flaws

enabling you to choose to either block non-compliant computers or ensure that security is improved to meet a required standard before allowing access.

Sophos Application Control can also assist organizations by ensuring only approved versions of applications are running. You can specify versions to allow to execute, such as Internet Explorer 8, and Firefox 3, but not older versions. This can help secure your environment against outdated or less secure programs.

## 7. Educate your users

A safe-computing policy should include rules that prohibit:

- » Downloading executables and documents directly from the internet or via email
- » Running or opening unsolicited executables, documents and spreadsheets
- » Playing computer games or using screensavers that did not come with the operating system

Keep in mind that a written policy is only as strong as the technology you use to protect your systems and prevent employees from engaging in risky behavior to begin with.

### Recommendation

If you haven't done so already, establish a policy for safe computing and distribute it to all employees. Make sure they read and understand the policy, and know who to contact with questions or in the event their machines have been attacked or infected.

When possible it is a best practice to block access to known malicious vectors from being delivered via email or downloaded from the web. Examples include .exe and .com files, .msi, .vbs and .bat. Technologies like the Sophos Email Appliance and Sophos Web Appliance can also determine a True File Type to prevent users from simply renaming dangerous files for transmission.

## Conclusion

For enterprise deployments, Sophos builds on the new Windows 7 security features and enhances overall security management across your business, enabling you to get the most out of your investment in this new release.

Combining the solutions from Microsoft and Sophos will help you meet compliance and regulatory requirements, improve security and provide the presence and expertise that are required in today's demanding technical environments.

Sophos is a Gold Certified Microsoft ISV, with competencies in Security, Mobility, Information Worker, ISV/Software and Networking Infrastructure. Sophos is committed to Microsoft standards, and shipped Windows 7 certified products on the same day that Microsoft released Windows 7.

Sophos also provides compatibility for legacy Microsoft platforms right back to Windows 98. This combination allows you to protect all your Windows machines with comprehensive and consistent security.

Boston, USA | Oxford, UK  
© Copyright 2010. Sophos Plc

*All registered trademarks and copyrights are understood and recognized by Sophos.  
No part of this publication may be reproduced, stored in a retrieval system, or transmitted by any  
form or by any means without the prior written permission of the publishers.*

**SOPHOS**  
WWW.SOPHOS.COM