



Plan your migration now!

Ten things you should do to secure Windows Vista

1 Don't give up your security software

Even though Vista includes a whole new set of security features, you should still be vigilant in updating your security solution – especially as there is little doubt that it won't be long before Vista-aware malware appears.

2 Keep taking the patches

Ensure that you configure Vista so that it is automatically patched against vulnerabilities, and keep yourself in the picture by registering for Microsoft's advisories.

3 Check your security vendor supports 64-bit Vista...

You should use 64-bit Vista for critical machines because Kernel Patch Protection, or PatchGuard, is more secure and is less likely to be successfully targeted by malware.

4 ...especially for HIPS

HIPS (Host Intrusion Prevention System) has an important role to play in defending against zero-day threats, so you should particularly ensure that your HIPS vendor supports 64-bit functionality.

5 Get your end users' support

Train end users on how to interpret and action User Account Control (UAC) alerts or you won't get the benefit of this significant new feature.

6 Make the most of Windows Security Center

Use Windows Security Center (WSC) for remote and home workers where it is definitely beneficial but, if you have management tools that let you monitor the status of your network centrally, consider disabling WSC's end-user alerts.

7 Don't just rely on Windows Defender

Windows Defender is good for protecting home users against spyware but it doesn't protect against all malware threats and doesn't offer the central administration capabilities that enterprises need.

8 Add a centrally managed firewall

You need your firewall to filter outbound as well as inbound traffic, and you also need visibility of the firewall status and configuration across your network – so you should replace the Vista firewall with one that offers this range of functions.

9 Add a web filtering solution

Although Internet Explorer includes enhancements to protect you from phishing and spoofing attacks, most organizations will also want specific protection in place at the web gateway.

10 Centrally manage your security

Use a centrally managed security solution, such as Sophos Endpoint Security, that enables you to monitor Vista computers, set and enforce policy, and rapidly identify and fix problems from a single point.

Sophos is a world leader in integrated threat management solutions purpose-built for business, education and government. With 20 years' experience and consolidated anti-virus, anti-spyware and anti-spam expertise SophosLabs protects even the most complex networks from known and unknown threats. Our reliably engineered, easy-to-operate products protect over 35 million users in more than 150 countries from viruses, spyware, intrusions, unwanted applications, phishing, spam and email policy abuse. Round-the-clock vigilance has resulted in our increasingly rapid international growth, expanding user base and continuous profitability. Our instant response to new threats is matched by business-focused, 24/7 technical support, and has led to the highest levels of customer satisfaction in the industry.

Boston, USA • Mainz, Germany • Milan, Italy • Oxford, UK • Paris, France
Singapore • Sydney, Australia • Vancouver, Canada • Yokohama, Japan

© Copyright 2006. Sophos Plc. All rights reserved. All trademarks are the property of their respective owners.

tt/061129

SOPHOS
secured.