



Redmondmag.com

THE INDEPENDENT VOICE OF THE MICROSOFT IT COMMUNITY

Enter Search Term or FindIT Code

Search: [go](#)

[Advanced Search](#)

- HOT TOPICS**
- [New! 2009 Salary Survey](#)
- [New! Windows 7](#)
- [New! Exchange 2010](#)
- [New! Server 2008 R2](#)
- [Automation/Scripting](#)
- [Careers](#)
- [Databases](#)
- [Exchange/Messaging](#)
- [Hardware](#)
- [Internet](#)
- [Interop/Open Source](#)
- [IT Management](#)
- [Network Management](#)
- [Security](#)
- [SharePoint](#)
- [Storage](#)
- [Virtualization](#)
- [Windows Servers](#)
- [XP/Vista/Windows 7](#)
- RESOURCES**
- [Salary Surveys](#)
- [Barney's Blog](#)
- [Pender's Blog](#)
- [The Schwartz Report](#)
- [News](#)
- [Product Reviews](#)
- [In-Depth](#)
- [Columns](#)
- [Forums](#)
- [Redmond Radio](#)
- [Tech Library](#)
- [Sponsored Webcasts](#)
- [Events](#)
- [Subscribe/Renew](#)
- [About Us](#)
- [Sitemap](#)
- [RSS Feeds](#)

Pender's Blog

[Blog Home](#)

Study: Removing Admin Rights is (Still) the Safest Way to Run Windows 7

BeyondTrust dropped in this week to [tell us](#) that eliminating administrator rights for end users can eliminate a lot of the vulnerabilities in Windows 7. It's handy information to have...except that [BeyondTrust said just about the exact same thing](#) a year ago. Well, at least we know that nothing has changed.

Curious to know what Microsoft thought about this, we contacted the company and got this official (and not especially brief) statement, which we quote verbatim:

"Before User Account Control (UAC) was introduced, most Windows consumer and enterprise users ran with administrative rights, which meant that ISVs could inadvertently make their applications dependent on administrative rights. Applications running with administrative rights have the ability to tamper with all user and Windows system data, including the ability to disable anti-virus and other security measures. Introduced in Windows Vista, UAC is a set of technologies that helps legacy applications to run with standard user rights and ISVs to adapt their software to work well with standard user rights. This gives users a more compatible choice to secure their systems by running with standard user rights instead of administrator rights.

"We believe that running users as standard users is good for Windows, the ecosystem, and all of our users. Configuring users as standard users enables parents to more securely share family computers with their children and enterprise administrators to configure standard user accounts for employees, lowering TCO and improving security. It is our hope that with the help of UAC that ISVs will continue to adapt their software to work well with standard user rights."

So...there you go. Standard user rights are the way to go.

Posted by Lee Pender on 03/29/2010 at 3:40 PM

- [News](#) [In-Depth](#) [Sponsored White Papers](#)
 - VC Funding Remains Tight
The market for venture money appears to have bottomed out as VCs remain cautious. 03/31/2010
 - Microsoft Extends Windows 7 Enterprise Trial Offer 03/31/2010
 - Rising Trend Seen for SaaS Security Managed Services 03/30/2010
 - 'Critical' Off-Cycle IE Patch Released 03/30/2010
 - IE 8 Hacks Slowed by Windows Safeguards 03/29/2010
 - China Cyber Threat Looms Large 03/29/2010
- [> More](#)



- [Most Popular Articles](#) [Most Emailed Articles](#)
- Azure and BPOS: Clearing the Fog Around Microsoft's Cloud Computing Offerings
 - Green IT: The Gift that Keeps on Giving
 - 'Critical' Off-Cycle IE Patch Released
 - Backup Basics in Windows Server 2008 R2
 - 'Best Hypervisors' for VDI Tested by Citrix