



- [RSS Feeds](#)
- [Subscribe](#)
- [Newsletters](#)
- [Events](#)
- [Digital Library](#)

- [Home](#)
- [News](#)
- [Blogs](#)
- [Video](#)

- [Software](#)
- [Security](#)
- [Hardware](#)
- [Mobility](#)
- [Windows](#)
- [Internet](#)
- [Global CIO](#)
- [Government](#)
- [Healthcare](#)
- [Financial](#)

- [SMB](#)
- [Jobs](#)
- [Application Security](#)
- [Attacks/Breaches](#)
- [Encryption](#)
- [End User/Client Security](#)
- [Perimeter Security](#)
- [Privacy](#)
- [Security Administration/Management](#)
- [Security Blog](#)
- [Security Discussions](#)
- [Security Reviews](#)
- [Security Stories](#)
- [Storage Security](#)
- [Vulnerabilities](#)

Smarter technology for a Smarter Planet.

[Download the service management whitepaper](#)

- [E-mail](#)
- [Print](#)
- [BOOKMARK](#)
- [Take Us With You](#)
- [Buzz up!](#)

Windows 7 Less Vulnerable Without Admin Rights

Most Windows 7 vulnerabilities can be mitigated by administrative rights limitations, report from BeyondTrust finds.

By [Thomas Claburn](#)
InformationWeek

March 29, 2010 09:05 AM

More Security Insights

Whitepapers

- » [Automating Virtualization Management: Critical Management Practices for Next Generation Data Center](#)
- » [Application Infrastructure Automation: Tools for fast and cost-effective application deployment](#)

Webcasts

- » [Extending DFS: Storage Management](#)
- » [Lessons From the "2009 Data Breach Investigations Report"](#)

Reports

- » [Cybersecurity Balancing Act](#)
- » [Google Rethinks The Operating System](#)

Videos



[Bay Area Internet Solutions](#)

Taking away the administrative rights from Microsoft Windows 7 users will lessen the risk posed by 90% of the critical Windows 7 vulnerabilities reported to date and 100% of the Microsoft Office vulnerabilities reported last year.



Windows 7 screen shot.

[\(click for larger image and for full photo gallery\)](#)

It will also mitigate the risk of 94% of vulnerabilities reported in all versions of Internet Explorer in 2009 and 100% of the vulnerabilities reported in Internet Explorer 8 during the same time period.

Finally, it will reduce the danger posed by 64% of all Microsoft vulnerabilities reported last year.

These findings come from a study conducted by BeyondTrust, which perhaps unsurprisingly sells software that restricts administrative privileges. The company argues that companies need its software to protect themselves, particularly during the time between Microsoft's publication of vulnerability information and the application of Microsoft's fixes.

"Enterprises continue to face imminent danger from zero-day attacks as new vulnerabilities are exploited before patches can ever be developed and deployed," said BeyondTrust EVP of corporate development Steve Kelley in a statement. "Our findings reflect the

critical role that restricting administrator rights plays in protecting against these types of threats."

The risks poses by unchecked administrative rights aren't exactly new.

Here's what Microsoft had to say about such privileges in 1999: "Unauthorized or unknowledgeable people who have administrator privileges can maliciously or accidentally damage your organization if they copy or delete confidential data, spread viruses, or disable your network. It is vitally important to properly manage the users and groups that have administrative control over the servers and domain controllers in your network."

Latest IT Jobs

- » [Web Developer](#)
US Environmental Protection Agency, Washington, DC
- » [Engineer V Network](#)
AT&T, Atlanta, GA
- » [Senior SW Engineer-Database](#)
IconStaff, Waltham, MA

[More Jobs >](#)
[Post a Job >](#)

Subscribe to IT Jobs by: [Email](#) [RSS](#) [Twitter](#)

Powered by [JobThread](#)

Featured Community

Stay connected and informed by visiting our Enterprise IT Community!



Become a member today for instant access to [free InformationWeek research](#), expert advice, peer perspectives, and more on the following topics:

- [Application Performance Management \(APM\)](#)
- [Security Management](#)
- [Mainframe 2.0](#)