Avecto

Don't give in to user privilege demands in Windows 7

Russell Smith (MSCE), Security Expert and Author

In this article, Russell Smith discusses migration to Windows 7/8 and the various challenges of implementing a least privilege environment which ensures productivity without compromising on security.

Countdown to migration

The expiration of support for Windows XP in 2014 means that Microsoft will no longer provide free security updates, non-security hotfixes, free or paid assisted support, or updates to online help and knowledgebase articles.

As part of the migration to Windows 7, IT departments are choosing to implement least privilege security from the get go. But without the right planning and tools, productivity can suffer, calls to the helpdesk increase, and IT finds itself under pressure to reinstate administrative rights.

Migrating to Windows 7

Not only is Windows XP a security liability, putting businesses at risk of data compromise or downtime caused by malware, but there are many benefits to be gained from the improved security in Windows 7, and Windows 8, that allow them to be more resilient to today's threats out-of-the-box.

Microsoft's latest Security Intelligence Report (Sirv15), compiled using real-world data, shows that Windows XP encountered much the same level of malware as Windows 7 between January and June 2013, but that XP had an infection rate six times higher than Windows 8. The report shows that not only is Windows 7 considerably more secure than XP, but system uptime and reliability will also be improved by moving to Windows 7.

Least privilege security

Much of the additional security provided by Windows 7 is due to User Account Control (UAC), which restricts even administrators to standard user privileges, unless consent is given to carry out operations that could affect system stability. But many IT departments are following Microsoft and industry best practice by issuing as many employees as possible with standard user accounts on Windows 7.
Not only does this significantly decrease the risk of malware infection, but is often a compliance requirement.

The challenges for users with restricted privileges in Windows 7

Even if Windows 7 standard user accounts are easier to work with than in Windows XP, there are still situations where users may not be able to run legacy applications, scripts or operating system tasks without IT implementing a workaround, or without assistance from the helpdesk.

As companies move to least privilege desktops on Windows 7, they often experience an increase in helpdesk calls as users struggle to carry out tasks that were previously possible with administrative rights; or if testing prior to moving to a least privilege desktop wasn't sufficient, there could be applications that no longer work correctly or fail to launch.

Avecto

Notebook users

These issues are particularly difficult for notebook users, who aren't always able to establish connectivity to the corporate network to get support. Therefore, it is common practice to assign notebook users with full administrative privileges.

As it's not possible to predict the tasks notebook users may need to perform when away from the office, which might include installing software so that they can join a web conference, adding new hardware with unsigned drivers, or updating a program to add important functionality, IT is forced to decide between providing notebooks that are properly secured but without the flexibility users require, or to grant administrative rights to ensure that notebooks can be used in any location and situation.

The challenges for users

While the security advantages of least privilege desktops outweigh the cons, it is probable that users will require assistance for tasks that they would have been able to complete themselves with administrative privileges. Additionally, supporting least privilege desktops can be challenging for IT staff too, as a proper understanding of the Windows security model is required, and may necessitate IT staff to receive additional training.

Due to the problems that both users and support staff can experience with least privilege Windows 7 desktops, IT frequently comes under pressure to provide administrative privileges to users, and unless IT staff have the right tools to solve the problems that users encounter, there might be little choice but to reinstate administrative privileges until an appropriate solution can be found. Reinstating administrative privileges, sometimes referred to as privilege creep, is usually seen as a temporary measure, but often remains unchecked, further increasing the chances of malware infection.

Empowering users in a secure environment

Before implementing least privilege and migrating to Windows 7, IT should test applications and Windows features on least privilege desktops, and get user acceptance. During the testing phase, it will become clear where problems are likely to occur.

Using a 3rd-party privilege management solution, such as Defendpoint by Avecto, IT can strike the delicate balance between usability and security, providing users with only the privileges needed to run the programs, scripts and Windows features required, while maintaining optimal security.

Defendpoint's challenge/response authorization capability also permits IT to provide administrative privileges to remote users in situations where unplanned changes have to be made, giving IT confidence that support can be provided when users are out of reach.

With the additional tools provided by Defendpoint, IT can monitor privilege use across a network, and leverage the collected data to create policies so that when users transition to a least privilege desktop, they are able to continue working without any disruption. Defendpoint also contains many other features, such as application whitelisting and customizable messaging, that can be used to improve desktop security.

About Avecto

Avecto is a leader in Privilege Elevation and Delegation Management. Since 2008, the company has enabled over 8 million users to successfully work without admin rights, enabling many of the world's biggest brands to achieve the balance between overlocked and underlocked environments.

Avecto's Defendpoint software has been deployed in the most highly regulated industries, enabling organizations to achieve compliance, gain operational efficiency and stop internal and external attacks.