White Paper

PowerBroker Desktops: Compelling Reasons for Least Privilege

By Derek Melber
Microsoft Group Policy MVP

February 2011

Derek Melber, MCSE, MVP, is an independent consultant, speaker, author, and trainer. Derek's latest book, The Group Policy Resource Kit by Microsoft Press, is his latest best-selling book covering all of the new Group Policy features and settings in Windows Server 2008 and Vista. Derek educates and evangelizes Microsoft technology, focusing on Active Directory, Group Policy, Security, and desktop management. Derek speaks and trains for MISTI, TechMentor, Windows Connections, and TechEd.

beyondtrust®
privilege. made simple

www.beyondtrust.com

BeyondTrust
2173 Salk Avenue
Carlsbad, California 92008
Phone: +1 818 – 575 - 4000

Table of Contents

Golden Rule for Windows: Users should not be configured as local administrators on their desktop.

When they are granted this level of privilege, bad things can and typically do occur. The reasons to move users away from having local administrative privileges are very compelling and obvious. When users have local administrative privileges they can, in essence, control every aspect of the desktop transforming their desktop into a rogue computer on the network that cannot be managed.

Moving a user to a least privilege environment, where they do not have local administrative privileges, can save money in many different ways, not to mention downtime, helpdesk cycles, and loss of money due to incorrect desktop configurations performed by the user. Implementing a least privilege desktop environment for every user in your organization can save over $1200 per desktop per year![1]

When considering attacks only against Microsoft Windows, over 90% of all attacks are invalid on a desktop where the user is a standard user.

Why Remove Users from Local Administrators Group?

There are many reasons to consider removing users from the local Administrators group on their desktop. Some of the reasons are more common and obvious than others. In the end, all of the reasons lead to a more secure, compliant, stable, and productive environment for the entire corporation. There are also reasons that might not be mentioned here, but are valid for many companies around the world. Again, gaining more knowledge on why the removal of users from having local administrative access is key.

First, if users no longer have local administrative capabilities the overall desktop is protected better than if the user is a local administrator. The key protection is from malware, viruses, worms, adware, and other malicious code. Studies have been performed with a desktop that has the user logged on as administrator compared to a desktop where the user is a standard user. The differences are staggering. When considering attacks only against Microsoft Windows, over 90% of all attacks are invalid on a desktop where the user is a standard user. Most recently, the ***Here You Are*** virus was completely negated on all desktops where the user was a standard user. When statistics are above 90% it is a very compelling reason to forbid users to be local administrator.

Secondly, if a user has local administrative capabilities nearly any software can be installed. This includes malicious software that can be used to attack the network and servers. Many tools such as network sniffers, password crackers, and port scanners can be used by the local user if they have local administrative privileges. Due to the nature of most of the applications the user must have local administrative privileges. If the user is a standard user these applications will not work or will have limited capabilities.

[1] Gartner, Inc., "Organizations That Unlock PCs Unnecessarily Will Face High Costs," Michael A. Silver, Ronni J. Colville

Next, the installation of software can become very costly for a corporation that does not monitor what is being installed. Any application that the user can download, bring in from home, or in some other way pirate can be installed by a user that has local administrative privileges. Although the user installed the software, the corporation is responsible for the license for the software since it is installed on a corporate computer. When the license police come knocking on the door there will be little the company can do to bypass paying for the license of the software that was installed by the user.

The biggest issue to realize is that any desktop that is controlled by the user logged in as a local administrator is a rogue computer. This means that the IT staff, helpdesk, and domain admins have no control over a computer in this state. The user can, in essence, do anything to the desktop and the domain administrators can't do anything to deny the activity.

The biggest issue to realize is that any desktop that is controlled by the user logged in as a local administrator is a rogue computer.

What a User Does with Local Administrative Privileges

When a user is granted local administrative privileges it gives them power over the desktop that can make the computer instable, insecure, and potentially an excellent computer for attack purposes. Again, even the domain administrators are helpless when it comes to these actions, since the local user is the one in complete control.

Initially the local user can take the computer out of the Active Directory domain. This might not seem like a very powerful action, but consider what is controlled from the domain down to the desktop. First, all Group Policy settings configured in GPOs linked to the domain, organizational unit (OU), and sites are negated. In addition, the domain user accounts are no longer available for the user to use for logons. In addition, logon scripts will no longer apply, as these are associated with the domain user account. Finally, all Active Directory domain related applications and services are now broken. This will include Exchange, SharePoint, network resources, etc.

Next, the entire suite of IP address settings can be altered by a user that has local administrative privileges. At the onset, the IP address and subnet mask can be altered in such a way to cause the computer to fail to communicate with any other computer on the network. Modification of the default gateway can cause the computer to be isolated from other networks, such as the Internet. The modification of the DNS IP address will break Active Directory, Kerberos logons, and all Group Policy from Active Directory. As you can see, nearly every aspect of the IP settings can take the computer out of the hands of the network administrators.

Finally, when a user is configured to have local administrative privileges the user can alter all aspects of the Registry. This would include settings for security, applications, operating system functions, and more. There is really not much the user can't alter that is configured in the Registry. Once the Registry is manually altered, Group Policy settings are nearly helpless and worthless at that point. Group Policy refresh does not look at the Registry

setting, rather it looks at versioning of the policy, which is not altered with a manual hack of the Registry. Again, the user has control over the desktop, not the domain administrators.

Possible Solutions to Least Privilege

When considering least privilege for your desktops the biggest hurdle is to get applications that require local administrative privileges to run when the user is a standard, least privilege, user. If the user has no local administrative privileges, all applications and operating system functions requiring this higher level of privilege will fail. There are many solutions for this issue, although to be honest some are not very realistic. Regardless, here is a list of solutions to applications that require local administrative privileges.

First, if we look at the core reason for the failure of the application we can solve this issue. This issue is that the application needs to access files, folders, and Registry entries that only administrators have permission to access. The access control list (ACL) is configured with only the Administrators group having permission the resource.

When a user with standard user privileges attempts to access the file, folder or Registry access is denied. To solve this issue, all files, folders, and Registry entry ACLs can be modified to include the user. Tools like Filemon and Regmon can help you track down these resources for each application. The biggest issue is that you might never finish finding all of these ACLs to change. This task is huge and can take many years to come close to completing.

Another solution that is constantly being offered is to upgrade the application to a newer version. There are many applications that can be solved by this solution; however, there are more applications that do not fit into this category than do fit. Even if your application fits into this category, consider the cost and time involved. The new application will require new licenses and knowledge for the new features. The old application might need to be uninstalled and the new application installed. All of these considerations equal additional cost, which might be very hefty if there are very many users using the application.

If the software was designed and created internally, the application might fall into the category of just being re-architected, reengineered, and updated. There are limiting factors with this solution, too.

If the application was created long ago, there may not be any internal resources that can update the code. In all honesty, there may not even be many external resources that understand the language the application was initially written in. A redesign of the application might be possible with newer languages, but the complexity of program might prohibit this solution as well. In the end, updating internal software is rarely a valid solution.

A final solution is to look outside of the application and implement a solution that solves least privilege directly and across the board. A solution like PowerBroker Desktops is a seamless, simple, light, yet extremely powerful solution to the least privilege issues. Since these applications require local administrative privileges, PowerBroker Desktops grants this level of privilege to the application.

The user does not run as a different user, the entire desktop environment is not elevated, nor are any applications allowed to run elevated. PowerBroker Desktops creates simple Group Policy rules, which alter the security privilege of the application immediately. The user is not aware of the elevation in anyway, giving them seamless access to all required applications.

What Does PowerBroker Solve For Least Privilege?

When looking for a solution to least privilege, more than just applications must be solved. Yes, applications becomes the biggest stumbling block for solving least privilege; however, it is not the most complicated of the issues. For example, consider the issue of installing a local printer for Windows XP where the user is a standard user. There is not simple ACL that can be changed to allow this. This issue is a built-in issue and takes more than just a modification to an ACL. PowerBroker for desktops solves the issue with applications, installing local printers, and much more.

As discussed above, PowerBroker Desktops solves all applications that require local administrative privileges. By altering the application privileges, the application is allowed to run in an environment where the user is a standard user. Figure X illustrates how the application is elevated.

Figure X. PowerBroker Desktops includes the required security group SID(s) to the process token to allow the application to run elevated.

PowerBroker Desktops can solve off the shelf applications or internally developed applications. With the altering of the process token PowerBroker Desktops does not care about the internal complexity or requirements of the application. When the application attempts to access a file, folder, or Registry entry as a local administrator, it has the privileges it needs.

PowerBroker Desktops also solves all of the nagging operating system functions that require local administrative privileges. Windows XP has many more of these functions than Windows 7; however, both have a fair share of functions that require local administrative privileges. Desktop functions that typically need local administrative privileges include:

- Installing local printers
- Altering IP address properties
- Altering clock properties
- Defragging the hard drive

An ever-growing area that causes least privilege solutions to fail is the installation of ActiveX controls from the Internet. As cloud computing becomes more mature and common, ActiveX controls become more prevalent and needed. ActiveX controls require the user to be a local administrator in order for them to be installed. Obviously, users need to run these controls and applications that the ActiveX controls are associated with. Giving users local administrative access just to perform this action is not required, as PowerBroker Desktops can elevate these installations for the standard user.

Most medium and large organizations, and even some smaller organizations, have hundreds, if not thousands, of applications within the corporation. With users being so dynamic and needing different environments, the user needs to be able to install applications on an as-needed basis. Many of these applications require local administrative privileges in order to be installed. PowerBroker Desktops can elevate these installations so the user can remain a standard user.

How Much Can Be Saved by Implementing Least Privilege?

You might be thinking that implementing a least privilege solution for production desktops in your organization might cost more money than save money. That is just not the case and examples over time have proven that least privilege saves money… a lot of money… when implemented in an organization. There are many situations that could create an environment that costs the company money for not implementing a correct least privilege solution.

First, consider the scenario where a company decides to overlook a least privilege solution at all. In essence, keeping the same scenario that so many companies have today, which is all users are local administrators on their desktop. This scenario has been evaluated many times, but most recently by the Gartner group. In the study by the Gartner group, a least privilege desktop was compared to that of a typical corporate desktop, where the user is a local administrator. After considering all of the downtime, reinstallations of applications/OS, loss of productivity troubleshooting, IT/Helpdesk time, etc, the Gartner group analyzed and reported that a least privilege desktop could save $1236 per desktop/per year. Here is a snippet from the report:

"The Gartner TCO model shows a significant reduction in TCO between a managed desktop where the user is an administrator, compared with a desktop where the user is a standard user. Among the most remarkable observations is that the model shows a 24 percent decrease in the amount of IT labor needed for technical support."

Gartner, Inc., "Organizations That Unlock PCs Unnecessarily Will Face High Costs," Michael A. Silver, Ronni J. Colville, Dec.19, 2008.

In another scenario, if a company were to go to the opposite extreme, which is to just remove all administrative privileges without considering the consequences, this too is a high price solution. There have been studies on this scenario, looking at the overall cost that is associated for a desktop where the user is a non-administrator, but there is no solution in place for them to run required applications and features.

There are many business applications that require local administrator privileges, features like installing printers and defragging the hard drive, and installation of ActiveX controls… all require local administrative privileges. If the user is restricted from these actions, it will require them to call the Helpdesk in order to get these actions accomplished, if they can be accomplished by the Helpdesk. The studies have shown that in this scenario a user will be required to call the Helpdesk around 5 times per year, at a cost of $30 per call. This equates to $150 per desktop/per year. The true issue is that the user might still be restricted from running business applications!

In a final scenario, consider a company that does implement least privilege, but not for everyone. There are many viruses and worms that run around the Internet. In a recent study of one of the most recent viruses, it was proven that not implementing least privilege on all desktops is costly.

Consider a situation where a virus runs freely on a computer where the user is a local administrator (typically all viruses function this way!). If there is a portion of the desktops that don't have least privilege implemented, the unprotected desktops are a haven for the virus. If the desktops where least privilege is not implemented are essential to the income of the company, a major issue can be created. The study of this situation calculated that it took approximately 4 hours of the entire IT staff to solve the virus issue. If you consider that the average IT staff member makes $75000, and the staff is around 50 total (for a medium sized company), that would equate to $7200 for that four hours of virus evaluation time. This does not include the time required to reinstall all of the desktops that were affected! (Note: In this scenario, it was determined that ONLY the computers that were not running in least privilege were infected by the virus!)

Summary

PowerBroker Desktops by BeyondTrust is the solution to least privilege for desktops. If the company is under a compliance regulation, required to implement least privilege, or just wants to increase security and productivity internally, PowerBroker Desktops can meet these needs.

PowerBroker Desktops takes the power and management out of the hands of the end user and puts them back in the hands of the network administrators, where they belong. Once PowerBroker Desktops is implemented security of the entire increases, since malware, viruses, adware, and worms, as well as malicious attack tools are negated for standard users.

PowerBroker Desktops elevates the applications that are required by the user to be productive and effective. PowerBroker Desktops not only elevates applications, but also elevates operating system functions, installation of ActiveX controls and installation of required business applications.

Finally, PowerBroker Desktops saves money for the corporation. Desktop reimaging is reduced, employee productivity increases, helpdesk calls decrease, and network outages due to viruses decreases. All of these factors reduces the total cost of ownership of your corporate desktops.

About Derek Melber

Derek Melber, MCSE, MVP, is an independent consultant, speaker, author, and trainer. Derek's latest book, The Group Policy Resource Kit by Microsoft Press, is his latest best-selling book covering all of the new Group Policy features and settings in Windows Server 2008 and Vista. Derek educates and evangelizes Microsoft technology, focusing on Active Directory, Group Policy, Security, and desktop management. Derek speaks and trains for MISTI, TechMentor, Windows Connections, and TechEd.

About BeyondTrust

BeyondTrust is the global leader in privilege authorization management, access control and security solutions for virtualization and cloud computing environments. BeyondTrust empowers IT governance to strengthen security, improve productivity, drive compliance and reduce expense. The company's products eliminate the risk of intentional, accidental and indirect misuse of privileges on desktops and servers in heterogeneous IT systems.

With more than 25 years of global success, BeyondTrust is the pioneer of Privileged Identity Management (PIM) solutions for heterogeneous IT environments. More than half of the companies listed on the Dow Jones Industrial Average rely on BeyondTrust to secure their enterprises. Customers include eight of the world's 10 largest banks, seven of the world's 10 largest aerospace and defense firms, and six of the 10 largest U.S. pharmaceutical companies, as well as renowned universities.

The company is privately held, and headquartered in Los Angeles, California, with East Coast offices in the Greater Boston, Washington DC, as well as EMEA offices in London, UK.

Visit www.beyondtrust.com for more information.