

Applying the Principle of Least Privilege across the Enterprise

Locking Down Desktops by Removing Local Administrator Privileges

White Paper

When users login to their computers with local administrator privileges they greatly increase the risk of security breaches by viruses, malware and malicious users. By removing administrative privileges and implementing the security best practice of Least Privilege these threats can be avoided and network security increased. However, when managing a least privilege computing environment systems must not only be locked down, but also still allow end users to perform all necessary tasks for their jobs. This paper presents several least privilege implementation options and discusses the benefits and issues associated with managing each solution.

Document Revision 2.00

Kevin Sullivan
Director of Product Management
DesktopStandard Corporation

About the Author

As the Director of Product Management at DesktopStandard, Kevin Sullivan integrates market needs and emerging requirements to guide the direction and functionality of DesktopStandard products. Prior to joining DesktopStandard, Kevin was a key member of the Product Management team at Quest Software, and was a successful Product Manager for Aelita's Active Directory solutions. He is a Microsoft MVP (Windows Server – Group Policy), and with his experience in Active Directory enterprise management he brings broad perspective and in-depth understanding of customer needs to the product development process.

Sullivan holds a B.A. from Berklee College of Music, and is a Microsoft Certified Systems Engineer (MSCE Windows 2000). He has consulted on large scale enterprise systems management and directory implementation projects, both as an independent consultant and with IBM Global Services. He has contributed to many technical articles and books, created in-depth training programs for Windows Server 2000/Active Directory deployment and Systems Management Server (SMS), and has designed and implemented large scale roll outs of Windows 2000/Active Directory, SMS, LANDesk, ZENworks, Tivoli, and other directory and systems management technologies.

ksullivan@desktopstandard.com

About the Company

BeyondTrust Corporation is the leading developer of enterprise security products that eliminate the need for security administrators to place trust in computers or users. BeyondTrust solutions provide protection from zero-hour threats, data theft, and unauthorized malicious use while increasing productivity and compliance.

BeyondTrust Privilege Manager was the first product to allow administrators to assign permissions to applications and tasks, enabling the security best practice of Least Privilege in Windows environments. BeyondTrust Privilege Manager has won many prestigious awards, including "Excellence in Management of Least Privilege - Customer Trust 2006" (*Info Security Products Guide*), "Best of TechEd 2006 - Security Finalist" (*Windows IT Pro/SQL Server Magazine*), and "Best Product of 2005 - Policy Management" (MSD2D People's Choice Security Award).

For more information, visit www.beyondtrust.com.

BeyondTrust Corporation • 125 Brewery Lane • Portsmouth, NH 03801 • USA

Legal Disclaimer

BeyondTrust and Privilege Manager are trademarks of BeyondTrust Corporation. This document is for informational purposes only. BeyondTrust offers no warranties, express or implied, in this document. Microsoft, Microsoft Outlook, Microsoft Exchange, Microsoft Internet Explorer, Microsoft Windows, Microsoft Windows 2000, Microsoft Windows XP, and Microsoft Windows Server 2003 are trademarks of Microsoft Corporation. Other names mentioned herein may be trademarks of their respective owners.

Contents

- Executive Summary..... 4**
- Introduction to the Principle of Least Privilege 4**
- Benefits of a Least Privilege Environment 5**
 - Protect Against Zero-Day Exploits5
 - Prevent Unauthorized Malicious Use5
 - Increase Productivity and Compliance6
- Barriers to Implementing Least Privilege..... 6**
 - Insufficient Time and Resources.....6
 - Office Politics.....6
 - Lack of a Solution Ensuring End-User Productivity6
- Common Solutions for Implementing Least Privilege..... 7**
 - Poking Holes in Security7
 - Security Templates8
 - Upgrading Software.....8
 - RunAs8
 - Windows Vista9
- BeyondTrust Privilege Manager..... 9**
- Summary..... 10**

Executive Summary

“It is imperative that we not only deploy and centrally manage a supportable and effective security policy but that we do so in a way that enables our users to continue to be productive and perform those responsibilities that are required for their job roles.”

Applying the Principle of Least Privilege is a critical security component or an objective for most organizations. Companies who are not concerned with applying this best practice may simply be unaware of it or unwilling to attempt the implementation due to the issues presented in this paper. Regardless of where an organization stands, understanding the concept is important.

Local administrative privileges are available for specific computing needs. Some common examples of why individuals must have administrative privileges include: system configuration changes, installation of applications, running applications that require elevated privileges, and execution of system level privileges (such as remotely rebooting a system). However, these needs do not justify running systems with administrative privileges while performing day to day activities.

When a user logs in to their computer with administrative privileges any viruses, spyware or malware they encounter will be able to install and run with the elevated privileges of the user. This greatly increases the risk of security breaches. Malicious users can also more easily gain access to private data with administrative privileges. The majority of users today login as a local administrator and are putting their network security at unnecessary risk. Will Poole, Microsoft's Senior Vice President of Windows Client, estimates that “85% of all corporate users run their systems as Administrators.”

(<http://www.microsoft.com/msft/speech/FY05/PooleFAM2005.msp>)

When implementing a least privilege computing environment problems arise when typical users require the rights necessary to perform system level tasks, such as installing an application or changing the system clock. Suddenly there is a need to elevate an individual user so that they can maintain their operational efficiency and perform their job. Problems also arise when users must run applications that require administrative privileges. These issues are difficult to address for many reasons, as explained in this paper.

It is often said that when security is increased operational efficiency suffers and that organizations must find the right balance between these needs. This does not have to be the case. By enabling users to perform their jobs and increasing security, productivity will be increased by reducing the downtime caused by security breaches. It is imperative to not only deploy and centrally manage a supportable and effective security policy, but also to do so in a way that enables users to continue to be productive and perform their job roles.

Introduction to the Principle of Least Privilege

“[The Principle of Least Privilege] requires that each subject in a system be granted the most restrictive set of privileges (or lowest clearance) needed for the performance of authorized tasks. The application of this principle limits the damage that can result from accident, error, or unauthorized use.”

“[The Principle of Least Privilege] requires that each subject in a system be granted the most restrictive set of privileges (or lowest clearance) needed for the performance of authorized tasks. The application of this principle limits the damage that can result from accident, error, or unauthorized use.” This quote is taken from the *Department of Defense* (DOD-5200.28-STD), also known as the orange book. Even though its roots date back more than 30

years, the message is still current and even more important in today's digital economy.

In a least privilege environment, users have the privileges necessary to perform their duties only when they need them. Every time a user is granted privileges that go beyond what is required for a specific task, we put our system at risk.

Many articles over that past few years have discussed the problems of spyware, viruses, rootkits, Trojans, worms, and the effects of user permissions. *eWeek* published an article discussing their labs tests showing the different malware risk levels for typical users versus administrative users. Their results were staggering.

eWeek used identical machines, varying only the user's group membership and visited a series of Web sites in an effort to install various types of adware and spyware bundlers. On the machine with only standard user permissions, none of the malware installed completely. A virus scan performed after reboot could find only a single threat, which consisted of one file in the browser cache. The system managed by a local administrator was not nearly as fortunate: After reboot a virus scan found 19 threats consisting of three memory processes, 503 files and 2,500 registry keys—all of which had installed. (<http://www.eweek.com/article2/0,1895,1891447,00.asp>)

Benefits of a Least Privilege Environment

Applying the Principle of Least Privilege to an enterprise computing environment provides a number of benefits.

Protect Against Zero-Day Exploits

By enforcing a least privilege environment, security administrators have a more proactive, forward-looking means of combating viruses and malware than just awaiting the latest anti-virus and anti-spyware definition updates from vendors. While anti-virus and anti-spyware solutions are important components of a security strategy, they are not a complete solution. A least privilege approach complements those tools by eliminating local administrative privileges for end-users, neutralizing malware that takes advantage of administrative privileges to compromise machines. This approach also protects against zero-day exploits (viruses for which anti-virus software has not yet been devised).

Prevent Unauthorized Malicious Use

In a least privilege environment, only authorized applications can be installed and end-users can no longer make system changes. The danger that end-users will either knowingly or unwittingly install malicious software or make problematic system changes is eliminated. By helping ensure that users do not make computer or file modifications the security of corporate data is also increased.

Increase Productivity and Compliance

When a secure, locked-down environment is implemented in a way that still enables end-users to run the applications and manage the system settings necessary for their jobs, corporate productivity increases. End-user computer downtime and IT help desk requests decrease because computers are secured against common problems. Administrators also gain better control over software licensing because they can ensure that only authorized applications are installed. A more consistent environment with less malware also means that administrators no longer need to devote large blocks of time to troubleshoot computers. Compliance with regulatory mandates, such as the Sarbanes-Oxley Act, HIPAA, and the Gramm-Leach-Bliley Act, are also increasing the drive for the greater desktop security and standardization provided by least privilege solutions.

Barriers to Implementing Least Privilege

“We are all here to do business and when the core business is [negatively] affected by a security initiative, we know who will win.”

Why do so many organizations continue to run an environment in which they know their systems are at risk? Why don't they just get rid of administrative privileges? The answers to why organizations continue to run in this environment are less complicated than how to address them.

Insufficient Time and Resources

IT organizations that continue to endure an environment that does not adhere to the Principle of Least Privilege typically do so because they do not have the time or resources to figure out how to address the issue.

Office Politics

Another barrier to adoption is office politics. Sometimes those in power insist upon having local administrative rights. Users also often confuse privileges with status and insist on having the same rights as another user with a different job.

Lack of a Solution Ensuring End-User Productivity

Commonly, an organization may have done the initial research to figure out how to achieve a least privilege environment and found that there are specific situations in which users need administrative privileges to be productive, such as to run a certain application or to make certain system level changes.

The following common tasks all require administrative privileges. To successfully implement a least privilege environment either a solution must be found that enables end-users to accomplish these tasks, or else end-users must be able to accomplish their work without being able to perform these tasks:

- Running applications that require administrative privileges
- Changing system time

- Installing printers
- Installing other hardware
- Manually changing system level configuration
- Installing ActiveX controls or other Internet Explorer components
- Installing applications

Some organizations have implemented a least privilege environment by simply removing users' local administrative privileges without a plan to address the required activities that users will no longer be able to perform. Typically in this situation users will resist the change and operational people will demand that the rights be returned. As soon as an executive at a high enough level realizes that operational efficiency has decreased and there is no plan to restore productivity, changes will be made to undo the security gains and restore administrative rights. While this approach is well intentioned, employees are hired to meet business needs and they must be enabled to perform their required jobs.

Common Solutions for Implementing Least Privilege

Common solutions for implementing a least privilege environment include poking holes in security to grant the precise combination of privileges required, security templates, upgrading software to a version that does not require administrative privileges, *RunAs*, the User Account Control features of Windows Vista and BeyondTrust Privilege Manager. While organizations may face challenges when attempting to restrict privileges, as discussed below, in the end they will benefit from the improved security and reduced downtime.

Poking Holes in Security

Poking holes in security means determining and providing the exact permissions required by each application that needs administrative privileges. To accomplish this, someone must identify exactly what administrative privileges an application actually requires. It is a tricky solution. What registry values would require read/write access control? To what parts of the protected file system is an application attempting to write? This is not a trivial undertaking because the list of applications that require some level of elevation can be extremely long.

There are tools available on the Web to perform registry monitoring and file system monitoring. Essentially, you run the application while monitoring its registry and file system access requests. The application must be used thoroughly, meaning all of the functions a typical user would use must be checked for elevated privilege requests. The logs generated by these tools can be daunting. From the logs all of the privileges that must be granted can be identified.

Once you interpret the log information Group Policy can be used to push the required permissions to systems that need them. Remember that once

permission to alter (write/modify/etc) a securable object is granted, it will always be there and give the user, or the malware, the ability to perform tasks on the system outside of the scope of the application itself. A small hole has been poked in the desktop security in order permit the application to run.

This solution is problematic for many reasons. It is difficult and time consuming to implement. It is easy to make errors. If applications require privileges to protected file system folders like System32, Windows, or other protected areas of the file system, granting write access is a serious security concern. Lastly, the problem will continue to evolve as more applications and users are introduced—it may be difficult to keep up with the number of requests.

Security Templates

Security templates are an organized, predefined group of settings for security policies. Security templates can be deployed using Group Policy objects (GPOs) to affect either a single or multiple computers. While security templates may be easier to manage than poking holes in security, described in the previous section, they suffer from all of the same weaknesses. Please refer to the previous section for an explanation of the problems commonly encountered with Security Templates.

Upgrading Software

One solution that is generally beyond a system administrators control is to upgrade software to a version, if available, that does not require administrative privileges to run. This option is problematic because businesses have little or no influence over the vendor if the upgrade is not available. If the software was developed in house or if you are a large organization and the software vendor counts on your use, then you may have influence over the upgrade process.

RunAs

RunAs solutions were a useful workaround a few years back, especially for administrators. When running utility products or administrative tools, someone who has administrative responsibilities can perform their daily tasks while running as a least privileged user. When they need to perform a task that requires elevated credentials, they can run that task under the context of a different user.

The caveats here are that the users must have essentially two accounts—one least privileged account and one Administrative account. This ultimately increases the network security exposure. Also, the passwords for these administrative accounts are commonly communicated throughout the organization. This is done simply for the sake of productivity. For example, if an influential user demands to have something fixed, installed, or modified an admin may give them the password of the privileged account over the phone and instruct them to use *RunAs* to finish the task. The user may then circulate the password with the intention of helping others.

Another problem with *RunAs* solutions ventures deeper into how software actually works. Since *RunAs* solutions execute the application or process under the security context of a different user, that application does not have access to the correct `HKEY_CURRENT_USER` hive in the registry. This is where all of the profile data is stored. Since it is protected space, the process running under the context of a different account cannot read from or write to it. Some applications simply will not work in this situation. Running under the security context of a different user may also cause problems reading and writing to Network Shares, as these are based on the account whose context you are running in. It is possible that your local user account and the *RunAs* account that has been applied will not have access to the same resources.

Windows Vista

Microsoft is introducing a new technology, User Account Control (UAC), in the upcoming release of Windows Vista. The goal of UAC is to allow all users, including local administrators, to run with non-administrative privileges when they are not required. This is an important move for Microsoft and validates the seriousness of the security threat posed by running with elevated privileges.

With UAC there are two only types of users: protected administrators and standard users. The only difference is membership in the local administrators group. UAC takes effect when a user attempts to do something that requires elevated privileges. The behavior varies for the different types of users.

- When a protected administrator attempts to perform a task that requires administrative privileges he or she may be prompted to consent to the process elevation. UAC tries hard to determine if a process requires administrative privileges. If the detection fails then the protected administrator can always invoke the Consent UI manually.
- When a standard user attempts to perform a task that requires elevation, a prompt asks for the local administrator username and password.

An important implication is that if standard users need to run applications or execute processes that require elevation, then the user must provide a password for an account with administrative privileges. By distributing the administrator password to standard users corporate security is compromised. With the local administrator password a standard user can perform any administrative function. This will allow a user to circumvent security policies, and run or install applications as an administrator. There is also nothing to prevent a user from sharing the password with other coworkers.

BeyondTrust Privilege Manager

BeyondTrust Privilege Manager provides a mechanism to handle the usability and password management problems that arise when organizations implement least privilege and remove administrative privileges. Privilege Manager gives companies a way to handle: application level permissions and privileges, software installation permissions, access to approved ActiveX

content, and more. These permissions and privileges are provided on a per-process basis. This means that while the user is not running the given task those permissions are not available. This is a critical component of the solution and a critical part of a least privilege management model.

With BeyondTrust Privilege Manager rules are created that specify exactly which processes, applications, installation packages or ActiveX controls will receive which privileges or permissions. These rules are communicated to the individual systems or users that are targeted by rules set in Group Policy. Administratively this is easy to implement and manage in an enterprise environment. Once the business requirements are understood, policy rules are created and automatically communicated to the end points. An important element here is that unlike some of the methods mentioned above, Privilege Manager rules are only in effect when the exact process which the rule targets, is launched. Elevated or modified privileges are only available to the specified processes they can not be exploited anywhere else on the system. The solution is transparent to the end user and does not require any administrator password management, as there is no use of a secondary user account.

Summary

Whether driven by security concerns, business needs or mandated by compliance standards, applying the Principle of Least Privilege is a prudent move for organizations. Eliminating unnecessary administrative rights protects against zero-day exploits, prevents unauthorized malicious use, and will increase productivity and compliance when correctly implemented.

Unfortunately, organizations must often overcome hurdles before they can implement a least privilege environment. In addition to removing unnecessarily elevated privileges, companies must ensure that users can still run applications and perform tasks that their jobs require. Any implementation that results in a decrease in productivity will be quickly overridden.

A variety of solutions for implementing least privilege are now in common use. While some of the solutions are more secure and easier to implement than others, all of them are preferable to an environment with no attempt to adhere to the Principle of Least Privilege.