Realtime publishers

"Leading the Conversation"

The Essentials Series:
Eliminating Administrator Rights

The Business Benefits of Eliminating Administrator Rights

sponsored by

by Greg Shields

The Business Benefits of Eliminating Administrator Rights.....1
Operational Benefits.....2
Security Benefits.....3
Compliance Benefits.....4
Not Just for Enterprises.....5

Copyright Statement

The Business Benefits of Eliminating Administrator Rights

The first article one of this series engaged in an extended definition of the Principle of Least Privilege. Starting with a very high-level look at privilege assignment, that discussion showed how Least Privilege requires the lowest set of privileges possible to be assigned in order to accomplish any particular task. It further requires that privileges assigned for the purposes of accomplishing one task are not leveraged to perform another unauthorized task. Because of these requirements, the granular assignment of privileges requires the combination of three parts: the role a user has in the organization, the activities the user needs to accomplish, and the corporate policies of that organization. Aggregating these three elements results in a list of the processes and applications each user role is approved to accomplish.

The third article will discuss how these high-level ideals are manifested within the Windows operating system (OS). But know for now that the end goal is for processes and activities within the OS to be assigned elevated privileges only when those privileges are specifically required. This process ensures that an individual user is not granted wholesale Administrator privileges for the purposes of solving a single issue. A much better approach is in distributing privileges to individual applications and processes based on the needed activities of the user.

The end result of this approach in a Microsoft Windows environment is the significant reduction of Administrator privileges across the board. Users who were previously granted Administrator rights to resolve the privilege needs of a single application can now have those rights removed. IT administrators themselves can be more specifically granted the privileges they need to manage the computing environment. The rights formerly assigned to every action of a specific person are now more granularly assigned to the specific activities and applications that require elevation.

Eliminating Administrator rights enables a set of benefits to the organization, which can be broken into benefits related to operational improvements, security enhancements, and a greater ability to fulfill compliance requirements. The business stands to gain from each related to this right-sizing of security privileges.

Operational Benefits

The first set are those related to operational benefits. These benefits relate to improvements in organizational workflow, the standardization of settings within the environment, and the ultimate ability of IT and the business to get the job done:

- *Standardized settings are assured.* The Windows OS has thousands of potential settings that can be standardized using various techniques. This standardization of settings ensures that each desktop behaves in ways similar to others. It ensures greater uptime in the environment by ensuring that known-bad configurations are avoided, while those that enhance usability are enforced. The problem with standardization in environments with widespread Administrator rights is the ability for the local user to reconfigure the desktop at will. When individual users retain the ability to move away from standardized settings, this increases the complexity of the overall IT environment and reduces the ability of IT administrators to keep the environment up and operational.
- *Users are prevented from installing unlicensed and unapproved applications.* One of the capabilities given to users with Administrator rights is the ability to install new software. When a user is granted traditional Administrator rights, the user gains the ability to install any software to their computer without requiring the normal workflow steps usually required by IT. Although this setup means that the user can more quickly install the software they need, it also means that IT no longer fully owns the software inventory process. Inappropriate and/or unlicensed software can be installed to desktops without the knowledge of IT or the business. This can introduce the potential for data compromise in the case of known malware or can be a license violation in the case of legitimate software. Thus, granting Administrator privileges to users gives them the authority for the installation without the responsibility of security and proper licensing.
- *More efficient use of hardware resources.* Inappropriate software, especially software downloaded from illegitimate Web sites, adds a resource burden to business hardware. This resource burden is especially problematic in the case of malware code. By retaining control over which software is installed to desktops across the environment, IT ensures that available hardware is used with the best possible performance and the least possible downtime.
- *Reduced cost of ownership for desktops.* Related to the previous bullet point, the more time IT is required to spend with each individual desktop, the more costly that desktop is to maintain. The installation of inappropriate software along with the inappropriate reconfiguration of standardized settings often results in an increased rate of problems as well as an increased level of downtime for that desktop. By eliminating Administrator rights and ensuring greater standardization, IT will reduce the costs associated with maintaining each individual desktop.
- *Fewer calls to the Service Desk.* In the end, all of these benefits are associated with a reduction in the number of support calls to the Service Desk. When desktops can maintain a standardized configuration, users are more likely to accomplish their assigned tasks through their required applications and processes.

Security Benefits

Operational benefits are important to the business side of the IT organization. But the elimination of Administrator rights also impacts the environment's security posture. These benefits go far in ensuring the safety and security of critical corporate data by preventing the installation of malicious software and the configuration of known-insecure settings:

- *Security configurations cannot be overwritten.* Though many organizations may not engage in a high level of desktop customization for visual purposes, nearly all enforce configurations that are known to improve the security posture. These security settings relate to the automated installation of security patches, enabling and configuration of the firewall, and other desktop and application lockdowns that ensure the safety of the environment. As with those discussed in the previous section, virtually all of these settings grow suspect in environments in which local users with Administrator rights can disable them at will. By eliminating traditional person-based Administrator rights, organizations can ensure that users retain the ability to accomplish system tasks they require—networking changes, printing, and so on—while being prevented from adjusting settings related to system security.
- *Malware infections are inhibited.* Very little of a user's daily processing requires the use of Administrator privileges. Yet when users run with Administrator privileges during their daily use, they unnecessarily expose themselves to the potential for malware infection. Such is particularly the case when users browse the Internet. When the browser's process is launched without administrative privileges, it is very difficult for accidentally downloaded malware to infect the system. This is the case because making any changes to the protected areas of the Windows OS—those areas most desired by malware—requires administrative privileges. Thus, browsing the Internet with the lowest-possible set of privileges goes far in preventing most known forms of malware infection.
- *Enhanced data protections.* The user-initiated download and installation of malware is not the only mechanism by which computer systems can be compromised. When a user elsewhere in the network accidentally infects their computer with malware that is designed to replicate, its replication can be inhibited by ensuring it runs with the least possible privileges.

Compliance Benefits

In addition to the operational and security benefits, eliminating Administrator rights assists with an organization's ability to maintain industry and regulatory compliance. Virtually all organizations fall under some form of regulation—the Sarbanes-Oxley Act (SOX) for corporations, the Health Insurance Portability and Accountability Act (HIPAA) for medical organizations, the Gramm-Leach-Bliley Act (GLBA) for banking institutions, the Federal Desktop Core Configuration mandate for federal entities, and others. Though each regulation is unique in the text of its requirements, all require some form of technical control that ensures the safety and security of sensitive data in the environment.

Without going into the individual requirements of each regulation, the following benefits relate to the fulfillment of the spirit of each. By controlling and effectively logging user and administrator activities, the fulfillment of compliance regulation requirements can be assured:

- *Logging of user activities can be assured.* The native logging systems within the Windows OS suffer from the limitation that any administrative user can clear the logs at will. This limitation means that a user with administrative access can clear any record of their activities if desired. With the assurance of activity logging a primary requirement of virtually all compliance regulations, preventing log erasure is a key necessity for the secure and compliant IT environment.
- *Data access can be protected.* Virtually all corporate data must be accessed through some form of application. When the access to that application has been elevated through the assignment of Administrator privileges, the user may have the ability to leverage that access for other unauthorized purposes. Conversely, when granular privileges are assigned based on individual activities, the likelihood of data breech is reduced due to a reduction in the count of potential activities that can be accomplished by the user.
- *The power of IT administrators can be limited based on their responsibilities.* Lastly, with traditional privilege models, IT administrators must be given Administrator access if they are to have the rights necessary to do their jobs. This all-or-nothing approach to permissions enables rights for administrators that go above and beyond their individual needs. Using the Least Privilege mode, privileges assigned to administrators can be tailored specifically to only the activities required by the individual. This setup reduces the spread of Administrator access to IT administrators, and is a key technical control required by many compliance regulations.

Not Just for Enterprises

Though many of the benefits identified appear to relate to the enterprise large-scale organization, they hold the same value to smaller businesses as well. In comparison with large-scale organizations, which tend to have IT and security policies in place and a high level of process maturity, smaller businesses are often forced to use an adhocracy model. Because of the "get the job done" nature of small businesses, the potential tends to be higher for one-off system configurations due to special needs. Because of the trends in this type of workflow, it can be argued that the reduction of Administrator rights in smaller organizations is equally, if not more, important to the security and operations of the environment. Eliminating traditional person-based Administrator rights provides the same level of protection for small businesses as it does for large, enterprise-scale organizations.