

FARONICS

ANTI-EXECUTABLE™

ABSOLUTE Protection from
Unauthorized Executables



Faronics Anti-Executable Compared to Limited (Restrictive) Users & Group Policies

TECHNICAL WHITEPAPER

Last modified: October, 2005

Faronics

Toll Free Tel: 800-943-6422

Toll Free Fax: 800-943-6488

International Tel: +1 604-637-3333

International Fax: +1 604-637-8188

www.faronics.com

©1999-2006 Faronics Corporation. All rights reserved.
Deep Freeze, Anti-Executable, and WINSelect are trademarks
and/or registered trademarks of Faronics Corporation.
All other company and product names are trademarks of their respective owners.

Introduction

System administrators are constantly looking for ways to restrict user access to certain programs. In the Windows environment, two of the most common approaches to application blocking have been Limited (Restricted) Users and Group Policy.

When properly configured, Windows 2000 and Windows XP can provide some application blocking functionality via Limited (Restricted) Users and System Policies and Group Policies. Many organizations employ these approaches to ensure users cannot access certain areas of the computer and or install most off-the-shelf software. However, these approaches require the Network Administrator to be very knowledgeable and to spend large amounts of time setting and maintaining the Policies.

Faronics Anti-Executable is an ideal application-blocking utility because it is based exclusively on a whitelist concept. Upon install, Anti-Executable creates a whitelist of all currently installed applications, and any new executable file that is not on the whitelist is considered unauthorized and will not run or install. Anti-Executable does not require any further administrative knowledge or maintenance because the list of authorized applications is populated and updated automatically.

Anti-Executable also offers exceptional security to protect against present and future blended threats, and its seed technology allows fast and efficient imaging and deployment across an enterprise.

Weaknesses of Limited & Restricted Users in Windows 2000 or Windows XP

In theory, all users not granted full administrator rights should not be able to install software on their workstations. This means that viruses and other malware should not be able to harm the workstation when attacking a user logged in with non-administrative credentials. In reality, however, spyware and viruses often take hold effortlessly. How can this be?

Malware creators do not limit their executables to install only on Administrator accounts—they want their executables to install on any type of account, and code their creations accordingly. Limited Users are unable to change either system registry settings or critical system files. Therefore, they cannot install any new programs if the installation requires system registry changes or system services available only to the Administrator. However, Limited Users are still allowed to save, download, run, and install applications that can either be installed without system registry changes.

For example, take one of the most dangerous threats in a computing environment—the Windows root kit. A root kit can be a group of low-level programs that undermine the operating system and cannot be detected by usual methods. Root kits are sophisticated pieces of software designed to exploit vulnerabilities in the operating system to ensure the kit gets installed, regardless of user restrictions. There is an additional concern because of the way some legitimate software companies design and program their software offerings. There are some applications that only run properly with Administrator privileges. This is a security risk since, in order to run the application, the user has to have some administrative privileges, thus leaving the workstation vulnerable.

System and Group Policies Compared to Anti-Executable

System and Group Policies are used to control what a user can do and how the user's environment is configured. System and Group Policies can be applied to all users or all computers, or specific users, groups, or computers. Group Policy features the ability to block applications through a Software Restriction Policy that can be applied as a Group Policy Object (GPO). This begs the question—why would I need to install Anti-Executable if I already have a tool with similar functionality that comes with the operating system?

Anti-Executable was designed from the ground up to be a security solution, so it takes a different approach to block applications than Group Policy deployments do. Anti-Executable provides protection to workstations in a wider range of scenarios that may or may not be addressed by Group Policies.

Group Policies are applied generically, but restrictions must be created as policy exceptions in order to let certain users do more than others. The result is more admin time to perform constant updates and maintenance, which means higher costs and more structure to manage.

Group Policies do not provide any protection against blended threats, and Admin accounts remain unprotected because they require unrestricted access. As well, sometimes Group Policies don't protect temporary folders, so applications could be installed there and then launched from any Office application.

Another limitation of using Group Policies is that they cannot control or restrict the functionality of some of the applications in a user's environment. Anti-Executable protects all applications installed on the workstation, regardless of the application provider.

And finally, Group Policies can sometimes lock down a computer so tightly that users' computing environments can become restricted, impacting how users work, study, or access information. Anti-Executable does not restrict any computer functionality while protecting against known and unknown threats.

Group Policy Security Levels

Group Policies regarding software restrictions can work in one of two security levels: Unrestricted or Disallowed. When running in the Disallowed mode, no applications are permitted to run locally, and exceptions must be put in place for each individual application that are allowed to run on the local workstation. That list of exceptions is called the whitelist. In the Unrestricted mode any application can be run, except those that are specifically designated to be blocked, ie. applications on a blacklist.

In most cases, creating and updating a list of applications and their associated hashes take great deal of time, so many administrators default to running their Group Policies in the Unrestricted mode, using a list of applications they do not want run on their systems. This blacklist approach requires administrators to update their list for every new version of an application or threat they wish to block.

Anti-Executable Security Levels

Anti-Executable has two security levels. However, it always runs in a mode similar to the Disallowed security level in the Group Policy. The main difference between the two is that Anti-Executable builds a list of all the applications installed on the workstation when the software is installed. This whitelist of executables is used to determine what programs are allowed to run on workstations. This drastically simplifies setup, as administrators do not have to create their own list of applications and import it into the Group Policies. Anti-Executable automatically assumes that if an application is not present in the whitelist, then it should be blocked from executing. Anti-Executable runs at a very low level and is very difficult to bypass.

Anti-Executable also takes protection one step further with Network, Copy and Delete Prevention options. Network Prevention blocks the execution of all executables on a network drive; Copy Prevention prevents users from copying executables from the Internet or removable media to the workstation; Delete Prevention prevents all executables on a workstation from being deleted or renamed—regardless of whether or not they are authorized by Anti-Executable. These options provide extra protection against resourceful users who might try to run unauthorized programs by copying them to a different location or renaming them.

Maintaining a whitelist with Group Policies has proven to be time consuming. To add an application to the list of allowed executables on Group Policies-protected workstations, a new exception to the Policy must be created and added to the system. That list includes updates of already installed applications, so the list continues to grow and become more difficult to manage. In contrast, to include new applications in an Anti-Executable environment, the administrator only has to deactivate Anti-Executable and install the new application(s); this can be done locally, automatically, or through the console. Once re-activated, Anti-Executable automatically detects the application and adds it to the list of authorized executables.

Other benefits of Anti-Executable include a quick and easy install process and 100% workstation protection—regardless of the user's permissions. Anti-Executable can be installed in an enterprise, non-Active Directory environment, as well as stand-alone, non-networked workstations or laptops. Anti-Executable also supports Windows 9x environments. Workstations are always protected, even when not connected to the network, and the program is easy to manage through the Enterprise Console.