

# Running A Controlled Windows Endpoint Environment

By: Brien M. Posey, Microsoft MVP

Published: June 2009

## **About the Author:**

Brien M. Posey, MCSE, is a Microsoft Most Valuable Professional for his work with Security and with Microsoft Exchange Server. He has previously received Microsoft's MVP award for Windows Server and Internet Information Server (IIS).

Brien is currently a freelance technical author with over 3,000 technical articles and nearly two dozen books to his credit. As a freelance technical writer, Brien has written for Microsoft, TechTarget, CNET, ZDNet, MSD2D, Relevant Technologies, and other technology companies.

Prior to becoming a freelance author, Brien has served as CIO for a nationwide chain of hospitals and was once responsible for the Department of Information Management at Fort Knox. You can contact Brien by e-mail at [brien@brienposey.com](mailto:brien@brienposey.com)

# Contents

---

- Introduction.....3
- The Five Elements of Desktop Control.....4
- User Privilege Management.....4
- Software Delivery.....5
- Application Whitelisting.....6
- Antivirus and Firewall Control.....8
- Centralized Management.....9
- Conclusion / Recommendations.....9

## Introduction:

Getting control over desktop PCs is fast becoming a major strategic objective of CIOs and IT departments. There is no doubt that a fully-controlled PC is easier to manage and therefore much less expensive, but there are actually several factors that are forcing companies to do away with overly-lenient policies and strengthen their management capabilities of their Windows infrastructure:

- Compliance objectives require better information about and auditing of end-user PCs, as well as tighter policy enforcement.
- Malware is evolving and now taking advantage of downloadable software and online social communities to gain access to PCs
- Helpdesk calls are expensive, and the majority of them are preventable

If your organization is subject to federal regulations related to IT security, then locking down workstations is probably going to be a big priority. After all, nobody wants to go to prison just because workstations were not properly secured.

Even if a company is not subject to the various IT security regulations though, it is still possible to reduce helpdesk costs and reduce the amount of potential damage that can be done by malware by locking down the company's workstations.

The reason why desktop lockdown can reduce helpdesk costs is because on average, relatively few calls are related to hardware failures or to server problems. Most helpdesk calls involve issues related to the workstation's operating system or to the applications that are running on it.

When the IT staff deploys a workstation, the workstation's configuration has typically been tested for stability, and the applications that are installed on the workstation have been proven to be able to co-exist with one another. When users begin making changes to a workstation's configuration or installing unauthorized applications, it places the machine's configuration into an untested state.

As with any untested configuration, problems may or may not result. If the user's changes do cause problems though, those problems will inevitably lead to a call to the organization's help desk.

Estimates from industry analysts as to what a help desk call costs vary widely, but two facts are undisputable in this situation. First, the helpdesk call does incur significant costs in the form of the user's lost productivity, and in the form of a support tech having to take time to help the user. Second, this help desk call would have been easily preventable had the user's workstation been locked down in a way that prevented the user from modifying the configuration.

Costs may be increased even further by the fact that the technician who is working on the problem is most likely unaware of the user's modifications. The technician addresses the problem under the assumption that the machine is configured in a specific way. When the machine's actual configuration does not match the technician's assumptions, it may likely take the technician longer to diagnose the problem than it would if the technician had been aware of the configuration changes in the first place.

The same principles apply to malware infections. Machines that are fully locked down are much less susceptible to damage from malware. Almost every organization runs anti malware applications at the desktop level, but history has demonstrated time and again that it is possible for new types of viruses to wreak havoc on organizations until the antivirus companies can analyze the virus and provide an antivirus definition for it. By that time, the damage may already be substantial. Properly locking down workstations greatly reduces the chances of the machine being susceptible to a malware infection.

## The Five Elements of Desktop Control

Gaining full control over Windows desktops can be broken down into five different elements. Each of these capabilities are required in order to fully realize the benefits of a controlled environment. The five elements are:

1. User privilege management
2. Software delivery
3. Application white listing
4. Antivirus and firewall protection
5. Centralized management

Most of these elements are provided by Windows; at least to a degree, but some are typically better implemented by third party software. In particular, companies are well served by relying on Microsoft products and features in the Windows Operating System to manage user privileges and deliver software packages, updates, and patches. Furthermore, Windows's built-in personal firewall provides adequate service protection, and Microsoft's management systems tie these capabilities together well. However, companies should look beyond Microsoft for the rest of the package – in particular Application whitelisting.

The purpose of this paper is to discuss how these technologies are used in concert to assist administrators in achieving a fully controlled Windows desktop environment. Furthermore, recommendations are provided for the major areas where 3<sup>rd</sup>-party products are required.

## User Privilege Management

What is user privilege management?

User privilege management consists of limiting each user account so that it has the minimal level of permissions necessary for the user to do their job. Often, this means removing the local administrative rights from each user account.

Why is it important?

There are many reasons why it is important to restrict user's privileges. Compliance related reasons aside; the most important reason for restricting user's privileges is to prevent them from tampering with the machine's configuration and from installing unauthorized applications. Doing so leads directly to lowered helpdesk costs.

Another reason why it is important to limit user privileges is because applications running on a workstation typically have the same level of privileges as the user who is running them. Removing a user's administrative privileges won't prevent a malware infection, but it will help to limit the amount of damage that malware is capable of inflicting.

Although removing local administrative permissions from user accounts is a good idea from a security perspective, it is not always a practical solution. The majority of the applications on the market are designed in such a way that the application essentially has the same permissions over the operating system as the user who is running it. In fact, until recently, most applications were coded with the assumption that the end user would have local administrative permissions, and that the application would therefore have free reign over the system.

Removing local administrative permissions from the user accounts on a machine that's running Windows XP will often cause the same sorts of problems that plague Windows Vista. Windows Vista is designed so that all user accounts have a minimal level of permissions. Even the local Administrator is treated as a standard user unless an administrative task is being performed. In such cases, an elevation of permissions is required.

The point is that many applications that ran fine under Windows XP will not run on Windows Vista, due primarily to Vista's new security model. Removing local administrative permissions from a machine that is running Windows XP can trigger many of these same types of problems.

If an organization is running Windows XP, and their desktop applications are able to run without local administrative permissions, then removing those permissions is probably a good idea. After all, removing administrative permissions can prevent a number of potential security problems. However, it is dangerous to assume that the administrative staff has total control over the code that is running on desktop machines, just because the user's local administrative permissions have been revoked.

## **Software Delivery**

Another part of gaining control over your desktops is the software delivery mechanism. This is the application that the administrator uses to deploy applications and / or patches.

Microsoft provides three primary software delivery solutions, each with its own focus. For example, Microsoft offers the Windows Server Update Service (WSUS) as a free utility for deploying patches within an organization. WSUS does have its limitations though. It can only be used to patch Microsoft products, and does not offer application deployment capabilities.

Another mechanism that administrators can use for software delivery is group policies. Group policies are a security mechanism residing on Windows domain controllers. This means that organizations that have a Windows domain in place are already equipped to use group policies for software delivery. The disadvantage to using group policies in this way though, is that they can be cumbersome to manage. Group policies do not automatically download or deploy the latest patches, so administrators must download each patch manually and then create a new group policy setting every time that they want to deploy a patch.

Furthermore, group policies can make it tricky to deploy applications to specific workstations. If an application is to be deployed to a subset of the user base, then the policy for deploying that application must be placed in a location within the group policy hierarchy that will ensure that it will only be applied to the specific users or computers that are being targeted. This means that software delivery related group policy settings may not all exist within a single location within the group policy tree. Instead, they may be scattered throughout multiple levels of the group policy hierarchy.

Microsoft's System Center Configuration Manager (MS SCCM previously known as SMS Server) is Microsoft's premium software distribution product. It is designed to overcome all of the shortcomings associated with WSUS and with group policy based deployment, but has a steep price tag and a steep learning curve.

When an organization is deciding which software delivery mechanism to use, there are a few things to look for. The chosen mechanism needs to be able to easily deploy applications, while maintaining version control and counting the number of licenses that are being used. It also needs to be able to quickly and efficiently deploy patches when ever new vulnerabilities are discovered.

Whether an organization chooses to use one of Microsoft's software delivery solutions or a third party solution, it is important to remember that a software delivery solution will help an organization to install applications and patches onto workstations. However, these types of solutions will not prevent users from installing unauthorized applications on their workstations.

## **Application Whitelisting**

Being that neither user account restrictions nor software delivery mechanisms can completely prevent users from installing unauthorized applications, the third part of achieving a fully controlled Windows Desktop environment is application whitelisting.

The only mechanism built into Windows that is designed to help prevent users from installing unauthorized applications is a special type of group policy setting called a software restriction policy. Unfortunately, software restriction policies are often difficult to implement properly. Furthermore, these policies tend to require a lot of maintenance and are easy for a determined user to circumvent.

The reason why software restriction policies are so easy for a user to circumvent has to do with the way that applications are identified by a policy. Applications are identified by either a certificate, hash, path, or Internet zone.

If an application is identified by a certificate, then the policy will be relatively difficult for a user to circumvent. The problem is that the majority of the applications on the market are unsigned. If an application is unsigned, then it is impossible to create a certificate based software restriction policy for that application.

Hash rules work by making a mathematical hash of an executable file. This hash is then used to positively identify the executable. The problem with software restriction policies based on hash is that any modifications whatsoever to the executable file render the hash invalid. Today, almost every software publisher periodically releases updates to their applications. If the update modifies executable file, then the file's hash is changed, and any hash rules based on the executable file are rendered invalid.

Path rules work by looking at either the location on the hard disk to which an application is installed, or the registry path that references the application. Because of this, path rules are by far the easiest types of software restriction policies for a user to circumvent. If a user wants to get around a path rule, they would typically only have to install the application to a different location than what is normally used.

Internet zone rules allow you to restrict an application based on the Internet zone that the site that a file that is being downloaded from falls into. However, Internet zone rules only apply if the user is downloading a Microsoft Installer Package (.MSI file). All other types of executable files are ignored by the rule.

Because of the way that software restriction policies (SRPs) define applications, it can be extremely difficult to implement software restriction policies in an effective manner. Once software restriction policies are in place, maintaining them so that they remain current can become a huge burden.

Between the administrative overhead of SRPs and the ease with which they can be circumvented, a third-party solution is recommended for application whitelisting. IT departments should choose a solution with the following capabilities:

- 1) Software Identification & Analysis: tie the full context of an application together so an IT person can make an informed decision based on security results, context, etc.
- 2) Automated & Adaptive Whitelisting: automatically handle updates, patches, and all the ways that IT people already deploy software. Don't complicate anything.
- 3) Open Integration with Existing Systems: Tie into your existing infrastructure

This is where Bit9 Parity can make a significant difference in controlling Windows desktops.

Between the administrative overhead associated with using software restriction policies, and the ease with which they can be circumvented, it makes more sense to use a third party product for application whitelisting. Organizations considering investing in such a product should look for a product with the following capabilities:

- Software identification and analysis
- Automated and adaptive whitelisting
- Open integration with existing systems

This is where Application Whitelisting can make a significant difference in controlling Windows desktops.

Application Whitelisting is a new way for enterprises to secure and control their desktops, laptops and servers. It provides IT a mechanism to identify and control applications; to protect Windows computers from malicious malware; and to prevent data leakage by controlling portable devices such as Flash drives.

Bit9 Parity™ application whitelisting can make a significant difference in securing and controlling Windows machines. Bit9 Parity provides IT professionals with a way to automatically whitelist authorized applications that meet certain established criteria such as publisher, repository, application and updater, or applications that are trusted by a specific user.

Parity also features software identification and analysis through the Bit9 Global Software Registry™, an online database of over six billion files (and growing) and over nine million applications (at time of print). Administrators can use the information provided to identify an unknown application or to research specific products, publishers, known vulnerabilities, security scan results, and much more.

Parity is designed with open integration in mind. It offers full integration with all software distribution and patch management systems, and with Active Directory and other Microsoft platform management systems.

## **Antivirus and Firewall Control**

Preventing malware infections is one of the most important steps in maintaining control over Windows desktops. Traditionally, antivirus software has been the primary mechanism for keeping a workstation free of malware, although anti spyware applications and application aware personal firewalls have also been used in recent years.

Although antivirus software has historically done a good job of preventing viral infections, it can no longer be used as the only mechanism for keeping malware out. Even adding anti spyware applications and application aware personal firewalls only helps to a degree.

The main reason for this is that there are simply too many zero day exploits. There are countless documented examples of situations in which a PC that was “adequately protected” suddenly became infested with malware because a new vulnerability was exploited.

Another reason why these types of solutions can no longer be relied upon is because there are too many applications that could be considered to be too invasive, but that are not technically classified as spyware. Because such applications are not classified as spyware, an anti malware application will typically not prevent it from being installed.

With these factors in mind, it makes more sense for anti malware software to act as an organization’s second line of defense against malware, rather than its primary or only line of defense. The application whitelisting mechanism should keep most, if not all, malware off of the workstations. If any malware does make it onto the workstations though, the anti malware software can help to prevent an infection.

Another important workstation defense mechanism is its firewall. It's easy to think of a firewall as simply a mechanism for blocking obscure TCP and UDP ports. Over the last several years though, firewalls have become much more sophisticated and many now offer application filtering capabilities. One technique that some companies are starting to use for securing desktop workstations is to install application firewall software onto each desktop machine, and then use that software to block unauthorized applications.

Although desktop firewalls are absolutely critical to the security of a workstation, it's easy to be overconfident in their abilities. Firewalls are great at blocking restricted ports, but they tend to have some weaknesses when it comes to blocking prohibited applications.

It is important to remember that every desktop firewall application is different, but generally speaking firewalls can only block applications that they know about. For example, if an organization wanted to

block users from installing a particular video game then an application aware firewall would most likely be able to do the job. If however, you wanted to block prevent users from installing any software onto their workstations, then firewalls are not the answer.

Most of the application aware desktop firewalls on the market are designed to allow an administrator to block specific applications, not applications in general. Even if an application level firewall could prevent a user from installing applications though, it would likely lack the sophistication required to be able to do it well.

The reason is that such software might prevent software patches or antivirus definitions from being installed. In order to be truly effective, a desktop lockdown solution needs to have the ability to differentiate between necessary updates and unwanted applications.

This does not mean that organizations should forgo using workstation firewalls though. Workstation firewalls are good for preventing hackers from penetrating a workstation through obscure ports, and for preventing Trojans from “phoning home”. It’s just that firewalls are typically not the ideal solution for managing applications on a workstation.

## **Centralized Management**

The final requirement for organizations wanting to achieve total desktop lockdown is that the desktops must be a part of an Active Directory domain. This allows group policies to be centrally managed at the domain controller level and pushed to the individual workstations at logon. It is possible to secure workstations using local security policies, but local security policies are difficult to maintain since there is no mechanism for centrally managing them.

One commonly used technique for securing workstations is to create a local security policy that handles the workstation’s basic security needs, but without the policy being too elaborate. Simplicity is essential since it is impractical to frequently update each workstation’s local security policy.

The local security policy can be a part of the standard desktop configuration, and can be written to each workstation during its initial setup. The policy’s job should be to protect the workstation prior to the user logging into the network. Once the user logs into the domain, the group policies will augment the local security policy and complete the task of securing the machine. The group policies should contain the majority of your security settings since they are much easier to maintain than local security policies are.

## **Conclusion / Recommendations**

Although Parity is one of the best products on the market for controlling desktop applications, its power can be compounded by using it in conjunction with the various products that you already have in place. Doing so may mean changing some existing application management practices, but the end result will likely be far greater control over the applications that are running on the organization's workstations.

## **About the Whitepaper Sponsor**

### **About Bit9, Inc.**

Bit9 is the pioneer and leader in enterprise application whitelisting. The company's patented solutions ensure only trusted and authorized applications are allowed to run, eliminating the risk caused by malicious, illegal and unauthorized software. Unlike traditional, reactive controls that try to scan and prevent the never-ending list of unauthorized software, Bit9 takes a proactive approach to IT control and security. Bit9 leverages the Bit9 Global Software Registry™ -- the world's largest database of software intelligence - to ensure only authorized applications can run, delivering the highest levels of desktop security, compliance, and manageability.

Bit9 customers include companies in a wide variety of industries, such as retail, financial services, healthcare, e-commerce, telecommunications, as well as government agencies. Founded in 2002, Bit9 is privately held and based in Cambridge, Massachusetts. For more information, visit <http://www.bit9.com> or call 617.393.7400.