

NON-RESTRICTIVE TECHNOLOGY

THE **REBOOT TO RESTORE** CONCEPT

in Computer-based Businesses and Services

Faronics™

Introduction

This white paper discusses some of the challenges organizations face when managing public access computers with multiple users, as well as computers in corporate settings. It discusses the various approaches to managing those challenges, and introduces a new approach in the form of non- restrictive, reboot-to-restore technology.

Government and Corporations

Government and corporate workplaces are becoming increasingly computer oriented and many employees do the majority of their work on computers. Typically, corporate workstations have only a single user, but the problem of malware still poses a major threat to these environments. Many corporations have large networks, and the larger a network, the more difficult it is to manage the problem of malware. Company security, maintenance, and productivity becomes dependent on the computer management software IT administrators choose.

Additionally, employees must be given the freedom to use their workstations as they see fit and use the programs and applications they need to perform their jobs. This often means providing inhouse support for those programs, and if even a minor configuration change is made, it may require a lengthy process to solve the problem, even if it is as simple as restoring an accidentally deleted toolbar. These wait times for technical support can hinder productivity and create frustration for employees.

Healthcare

The healthcare industry represents a unique and highly specialized computing environment. The information contained on computers is often time sensitive and can be mission critical, so uptime is essential. Another issue is that patient-related information must be securely protected in order to adhere to HIPAA compliance.

Healthcare environments often involve managing a large number of computers at multiple locations, and training labs that are used for new and junior staff need to be available and operable at all times. Users can sometimes make program changes that leave the computer labs with varying configurations, which makes instructing difficult and increases support needs to maintain the uniformity of the lab computers.

Malware is a serious issue for healthcare computers, as viruses can significantly slow down machines, and spyware can compromise patient privacy. Hospitals often have public access terminals as well, provided for friends and family of patients, and these terminals can often become badly infected with malware. Hospital IT administrators often struggle with managing the problem of malware while maintaining an open and available technological environment.

Computer-based Businesses and Services

One result of the technological boom has been computer-based businesses and services. Perhaps the most common example of this is Internet cafes. Internet cafes provide a service to those who do not have access to or own a personal computer. These businesses also exist on an international scale, servicing tourists and travelers who are maintaining their communications with home.

Internet cafes can field a dangerous combination of innocent clickers and malicious users. Users who don't know the effect their keystrokes and deletions may have, can destroy an operating system, while malicious users can do the same thing intentionally.

On the international scene, more and more travelers are using digital cameras, USB devices, and other removable media that could potentially contain malware. The staff at Internet cafes can vary; some can be technologically savvy enough to spot potential issues before they happen and can troubleshoot technical problems. As a result, Internet cafes can often have several machines out of order. Downtime in Internet Cafes is a serious issue because the computers represent the livelihoods of the owners. However, these same owners must provide a relatively unrestricted environment for patrons who want to use specific programs, such as messaging programs, games, or P2P file sharing applications

Libraries

Due to increasing demand, more and more libraries are offering public access computers for patrons not only to search the library catalog and do in-house research, but also to browse the internet, do word processing, and use related applications. Providing these types of services in academic libraries is a relatively new development and requires effective management techniques. Libraries need to find a way to manage the problems that accompany those services.

One of those problems is malware, which has become an issue with the introduction of public access computing in libraries. Viruses, spyware, rootkits, and keyloggers pose a threat to the security and productivity of library computers, and IT administrators need to find a way to deal with those threats, while still offering a relatively open environment in order to provide those services to their users.

It follows then that libraries need workstations to be operable and available in order to provide those services. Computer downtime means a decrease in resources available to library users. Patrons may unintentionally change a computer's configuration or alter the registry settings, which can result in frequent calls to the helpdesk for minor but time consuming issues. Libraries need to find a way to maintain computer uptime while protecting systems from blended threats.

Managing Public Access and Corporate Workstations

Typically, there are two common approaches to managing public access and workplace workstations: the lock-down approach and the reactionary approach.

Lock Down Approach

IT administrators commonly respond to technological issues with a restrictive defense. Locking down computers prevents user mischief and defends against malware. This response means less rebuilding of machines and possibly less technical support resources required, but can place severe restrictions on the users' technological environment. This approach also doesn't help maintain uniform configurations across labs or multi-user networks.

Reactionary Approach

If labs are not locked down, the IT staff is most likely using a reactionary approach to maintain security. The reactionary approach means dealing with computers on an individual basis and using re-imaging or rebuilding as a method of keeping computers uniform and protected. The problems with this approach are many, given the amount of time it takes for the rebuilding process, and the correlating downtime of the machine. This approach only deals with temporary symptoms of a problem, rather than addressing the cause.

The Non-Restrictive Reboot-to-Restore Concept

There is another option for managing these kinds of workstations. Despite the endless variety of public access or corporate computer environments that exist, non-restrictive technology is applicable to all of them. With this technology in place, patrons and employees always have the freedom to use workstations as they desire and are fully protected against blended threats, but downtime and technical support costs are eliminated.

Non-Restrictive Technology Benefits

Non-restrictive technology offers an unrestricted environment for patrons and employees, and eliminates obstacles to initiate technology in businesses and workplaces.

- It enhances computer performance by eliminating the need for most routine hard drive maintenance, and ensures consistent configurations across an enterprise.
- Users are given full access to computers without time consuming management restrictions, such as are needed in managing Group Policies.
- Finally, nonrestrictive technology significantly lowers Total Cost of Ownership for technology assets because of a vast reduction in time and cost spent maintaining and rebuilding machines.

Faronics Deep Freeze

Faronics has been a pioneer of non-restrictive, reboot-to-restore technology since 1999. Faronics Deep Freeze provides an unrestricted environment for users that leaves IT staff free for more valuable and proactive activities. Deep Freeze offers the ability to standardize workstation configurations, from the programs installed on the machine to the placement of desktop icons.

- Computers are ctompletely restored to their original configurations on restart.
- Downtime is dramatically reduced and maintenance costs decrease significantly.
- Computers no longer have to be rebuilt or re-imaged, as all software-related issues are essentially eliminated.

Internet cafe owners can rest easy knowing their computers are completely protected, while offering a completely open and unrestricted environment for their patrons. Users can freely download communication applications or use removable media. Whatever hackers, mischief makers, or innocent clickers do to a computer, Deep Freeze makes the damage disappear instantly. Staff do not need to be technologically savvy to solve problems, as a simple reboot will restore a computer to its original state.

Healthcare IT administrators can use Deep Freeze to securely protect health information systems from improper access or alteration. The need for rebuilding, re-imaging, or troubleshooting mission critical workstations is gone, and workstations always remain HIPAA compliant. Deep Freeze is invisible and places no restrictions on users' abilities to work with training resources, and employees are always assured of working computers with standard configurations. Deep Freeze enterprise capability also allows administrators to control multiple computers in several different locations for flexible management and deployment options.

Libraries are among the most difficult of public access environments to manage, and Deep Freeze allows IT professionals and reference staff to easily protect and preserve their workstations. Patrons enjoy an unrestricted environment to work in, while avoiding the frustration of downtime due to software conflicts, registry and operating system corruption, and lost network and Internet connections. Operating systems will not fragment or corrupt over time, as they would with policy based tools designed to restrict functionality.

Deep Freeze deletes all malware on restart. If administrators want to allow individual users to make permanent changes to a computer, they can create a Thawed partition. Profiles can be set up to be saved locally on the Thawed partition. In the case of roaming profiles, the profile data can be retained both on the server and on the Thawed partition.

Deep Freeze provides a complete security solution for multiple environments. It offers business resiliency because workstations are back up and running with a quick restart; even enterprise backup systems don't offer that kind of resiliency in the face of malicious attack or system volume corruption. Resiliency also means reduced risk to revenue streams and customer relationships. Deep Freeze helps increase productivity because there are fewer system problems, less downtime, and fewer support calls. This system stability means fewer IT support staff are required. Finally, Deep Freeze is a 100% effective security tool that removes any spyware, adware, keyloggers, or other information theft software from systems after each reboot.

About Faronics

Faronics delivers market-leading solutions that help manage, simplify, and secure complex IT environments. Our products ensure 100% machine availability, and have dramatically impacted the day-to-day lives of thousands of information technology professionals. Fueled by a market-centric focus, Faronics' technology innovations benefit educational institutions, healthcare facilities, libraries, government organizations, and corporations.

Faronics

www.faronics.com

Faronics' solutions help organizations increase the productivity of existing IT investments and lower IT operating costs. Incorporated in 1996, Faronics has offices in the USA, Canada, Singapore, and the UK, as well as a global network of channel partners. Our solutions are deployed in over 150 countries worldwide, and are helping more than 30,000 customers.

UNITED STATES
5506 Sunol Blvd, Suite 202
Pleasanton, CA, 94566 USA
Call Toll Free: 1-800-943-6422
Fax Toll Free: 1-800-943-6488
Email: sales@faronics.com

CANADA & INTERNATIONAL
1400 - 609 Granville Street
P.O. Box 10362, Pacific Centre
Vancouver,BC,V7Y 1G5
Phone: +1-604-637-3333
Fax: +1-604-637-8188
Email: sales@faronics.com

SINGAPORE
20 Cecil Street, #104-01,
Equity Way, Singapore,
049705
Phone: +65 6520 3619
Fax: +65 6722 8634
Email: sales@faronics.com.sg

EUROPE
8 The Courtyard, Eastern Road,
Bracknell, Berkshire
RG12 2XB, England
Phone: +44 (0) 1344 206 414
Email: eurosales@faronics.com

COPYRIGHT: This publication may not be downloaded, displayed, printed, or reproduced other than for non-commercial individual reference or private use within your/an organization. All copyright and other proprietary notices must be retained. No license to publish, communicate, modify, commercialize or alter this document is granted. For reproduction or use of this publication beyond this limited license, permission must be sought from the publisher.