SHADOWSTOR™

Leading the Way to Safer Computing.

SHADOWSTOR

COMPETITIVE ADVANTAGE PAPER

ShadowStor Introduction

Providing Security, Data Protection and Disaster Prevention Solutions

ShadowStor solutions provide a new way to solve current security, data protection and disaster recovery problems. Our unique approach provides “Disaster Prevention”, eliminating security, data protection and disaster recovery problems before they occur. Why recover from a server or PC disaster when you can prevent it?

Today’s Challenges with System Security, Data Protection and Disaster Recovery

Businesses are facing serious challenges with keeping servers, desktops, and laptops online. System downtime can be potentially devastating to a company’s revenue, day-to-day business operations and productivity. Some of the challenges administrators and users of servers and PCs experience are:

Server and PC Uptime

- Keeping up with the onslaught of new virus and worm outbreaks is difficult and takes time for recovery. The virus or worm has already hit before a fix is available. This puts a company in reactive mode to security and disaster recovery issues.
- Patches and system service packs are difficult to test, distribute and manage while avoiding server and PC downtime.
- Many company’s have requirements that systems are available 24x7 365 days of the year to support global company sites and an international customer base.

IT Complexity

- Increasing numbers of applications are required to address security and disaster recovery problems. This adds to the complexity for an IT organization to implement and manage.
- IT complexity is increasing while IT budgets are shrinking requiring IT administrators to try and do more with less.

Cost

- Server and PC downtime is extremely costly and disruptive to day-to-day business operations.
- Server and PC downtime leads to lost business opportunities.

How System Security, Data Protection and Disaster Recovery Challenges are being Addressed Today

There are many solutions on the market today that are trying to solve system security, data protection and disaster recovery challenges, but the problem with the approach of many of these solutions is they are addressing challenges that should never exist. In many instances, the product that is supposed to be solving a particular issue with security, data protection or disaster recovery is intrusive and compounding the problem.

If the approach to these challenges was more proactive, then many of these issues could be eliminated. This would provide a disaster prevention solution rather than a disaster recovery product. This would resolve the unmanageable problems IT organizations and server and PC users are experiencing with system downtime, increased IT complexity and the associated costs.

Here are some of the challenges with system security, data protection and disaster recovery and how products on the market today are compounding them:

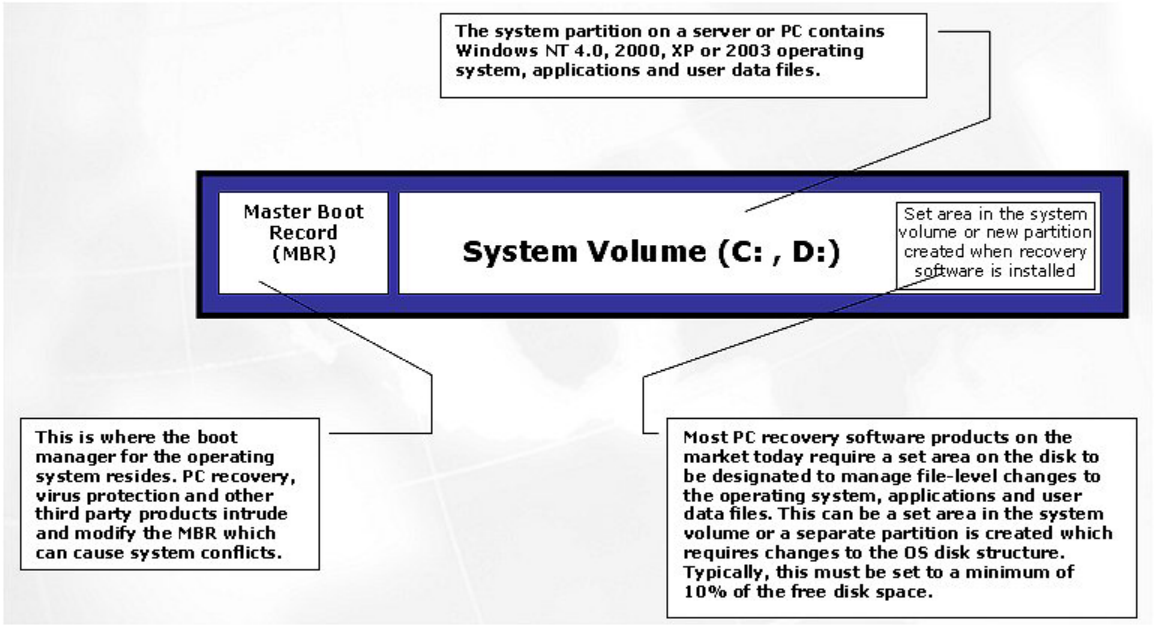
1) **Intrusive Changes to Your Server or PC** – Unwanted and intrusive system changes occur in internet history files, unwanted cookies, temporary files, spam applications or spy ware. Also, application installations, OS updates and patches can leave a system in an unstable state resulting in system downtime.

   Compounding The Problem – Many of the solutions are changing the original OS installation and disk structure, thus compounding the problem. Some modify the Master Boot Record (MBR) which can cause conflicts with virus protection products, boot managers and disaster recovery products. Some products require a set amount of disk space or a separate recovery partition resulting in disk structure changes.

   The solution should be non-intrusive to minimize system downtime, eliminate supportability issues and have zero impact to the current system configuration or IT infrastructure. The following diagram explains the way current disaster recovery products work:

Hard Drive Layout of Current Recovery Products

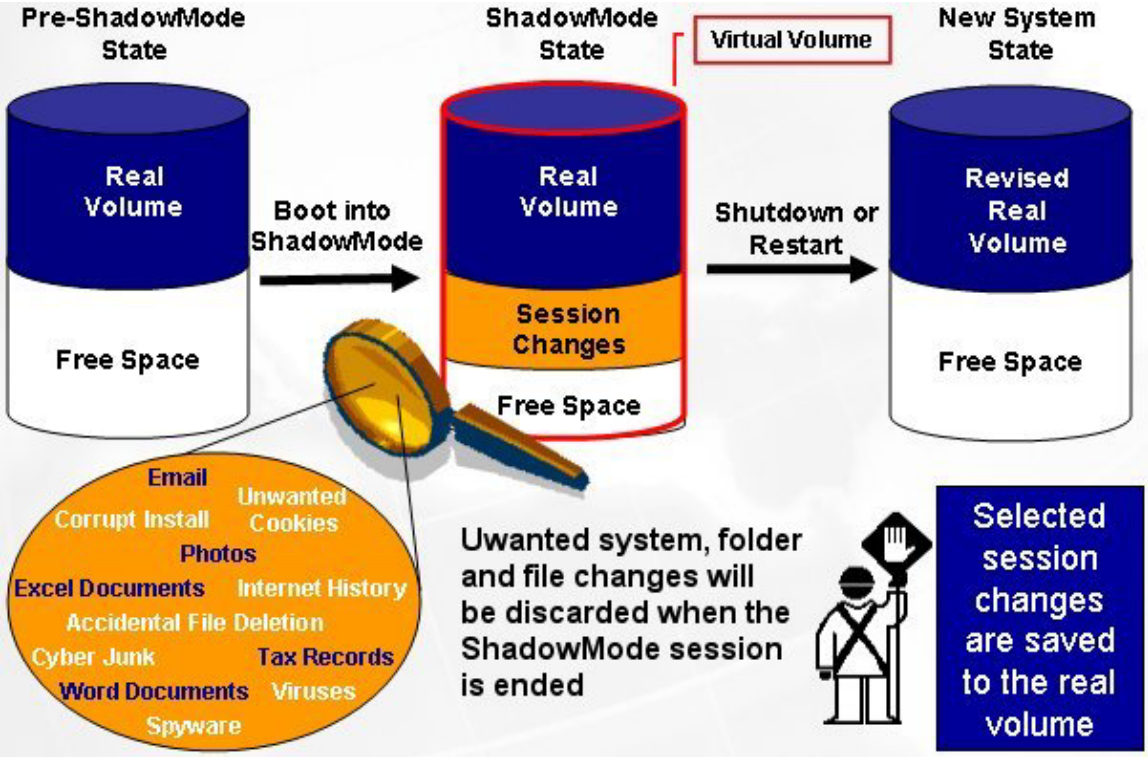
Intrusive to the MBR, volume and disk structure



The ShadowStor Approach – ShadowStor solutions have zero impact to the current configuration of your server or PC. There are no modifications to the MBR, partitions or disk structure. ShadowStor technology captures a snapshot of your system and runs an exact duplicate of your server or PC in a virtual state. This virtual state, called ShadowMode, allows the user to use the server or PC without actually writing to disk. If systems changes and folder or files changes occur during a ShadowMode session, then these changes can be automatically or manually committed to disk or discarded. This gives full control back to the IT professional and server or PC user.

ShadowMode – Virtualizing Your Volume(s)

Non-intrusive to the MBR, volume and disk structure



Another advantage to the ShadowStor approach is no set amount of disk space or separate partition is necessary to track changes. ShadowMode takes advantage of free space in the protected volume(s). Once a ShadowMode session is ended, the space that was utilized is freed up and given back to the volume. The amount of space used to track changes during a ShadowMode session is minimal and can be monitored in the ShadowUser or ShadowServer user interface.

In summary, ShadowMode provides the following features & benefits:

- Changes or writes are re-directed to another area on disk.
- Original volume is completely protected and kept intact.
- Folders and files can be automatically committed to disk.
- Folders and files can be included in the exclusion list feature and always written to disk.
- Entire system wide changes can be committed to disk.
- No matter what changes or deletions are made in ShadowMode, the user can return the computer to its original optimal state.

2) **Malicious Changes to Your Server or PC** – Viruses and worms are creating an on-going management nightmare for IT organizations. One problem with the current approach to resolving virus and worm issues is you are reactive, rather than proactive at eliminating viruses from getting to the server or PC. You don't get a fix for the problem until it has already hit your server or PC.

   Compounding The Problem – Virus protection products modify the MBR, thus creating conflicts with boot managers, disaster recovery and other products. This can make the server or PC unstable or inoperable.

   The ShadowStor Approach – ShadowMode doesn't allow viruses or worms to be written to the server or PC. If you run in ShadowMode, the virus or PC may get written to the virtual volume, but it can be discarded before changes are committed to disk. This approach is the first line of defense to security, data protection and disaster recovery and prevents problems from ever existing. This method provides a disaster prevention layer to your system rather than applying virus or worm updates after the disaster has occurred.

3) **Impact on System Performance** – As soon as a server or PC is put into production, some type of system degradation takes place. This can be caused by intrusive changes, malicious changes or many times it is hard to track down what has impacted the original optimal state of the system. Multiple products are needed such as disk defragmenters, virus protection software, internet blockers and disaster recovery products to slow down, but not eliminate system performance degradation.

   Compounding The Problem - Current system security, data protection and disaster recovery products don't address maximizing system performance adequately. For example, most disaster recovery products use a "point-in-time" method. This method takes an initial snapshot of the server or PC at a particular time, then based on schedule settings, takes an incremental snapshot to track file-based changes from one point-in-time to the next.

   This approach presents a false sense of security in that it doesn't really eliminate the disaster from occurring. In most disaster recovery products, it is tracking all changes on the system which includes intrusive files such as internet history files, unwanted cookies, temporary files, spam applications and spyware and may include malicious viruses or worms which cause the system problem.

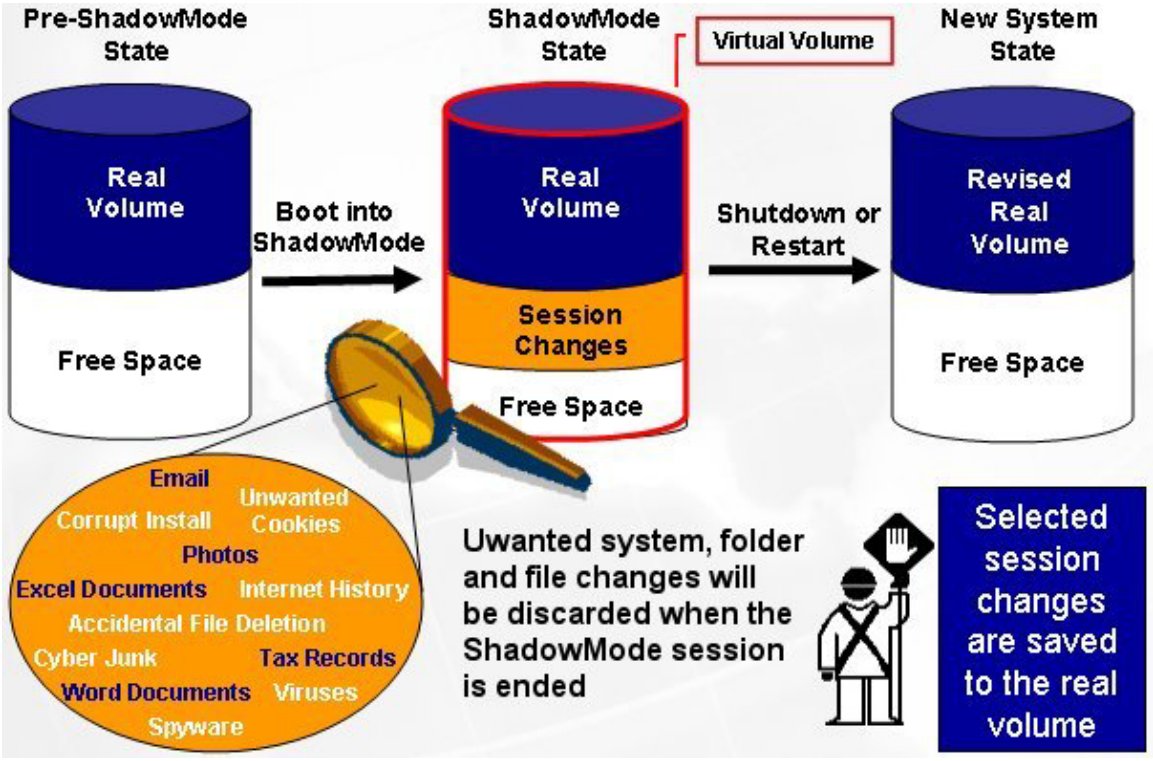
With a point-in-time method, it is assumed that the system will degrade over time and eventually it will be necessary to roll the system back to a point-in-time where it worked. By rolling the system back, you may be able to get it working again and minimize downtime, but you don't know if it is running at an optimal state. Trying to troubleshoot system changes and understand what caused the system degradation over time is extremely time consuming and almost impossible to diagnose.

The point-in-time file-based approach that most recovery products use also is taxing on the server or PC. Some of the popular recovery products on the market today require a set amount of disk space, a minimum of 10% of free space and up to 50%, and require on average 10 - 15% of system resources to track those file changes. This presents a trade-off of system resources vs. disaster recovery protection that isn't worth it to most IT professionals and server or PC users.

The ShadowStor Approach – The ShadowStor approach eliminates the ability for unwanted changes and intrusive and malicious files from ever being written to the server or PC. You can then install your operating system and applications and configure it once for maximum performance. Then, by only committing system changes, folders or files to disk when you so choose, you control what actually gets written to the server or PC. This approach allows you to preserve the original optimal configuration of the server or PC.

ShadowMode – Preserving Optimal System Performance

Current recovery products only track system degradation



As depicted in the graphic, session changes are saved or discarded and disk space and system resources are released once the ShadowMode session is ended. On average, a ShadowMode session uses less than 1% of system resources and temporarily has minimal impact on free disk space.

The ShadowStor approach makes it much easier to diagnose any system performance issues that may occur. Though system degradation can't be completely eliminated as long as files are being written to disk, it can drastically reduce disk fragmentation, intrusive and malicious files or other problems from getting to the server and PC and causing degradation problems.

4) **Accidental or Unwanted Changes to Your System** – People make mistakes and apply changes to systems that they wish they could reverse. These types of problems are not preventable, but they are recoverable. In many instances, systems are a shared resource. This is the case in lab environments, training centers, public kiosks, libraries and home PCs. Unwanted software installations or folder / file modifications can place a system in an inoperable or less than optimal state. Many times, the only way to recover from this situation is to go through the time consuming process of reinstalling the operating system, applications and reconfiguring the system. Another method is re-imaging the system which can be time consuming and difficult as well.

   Compounding The Problem – The way many of the recovery products provide system or data recovery is to give the end user access to the incremental file-changes to a system from one point-in-time to the next. These incremental file-changes are presented as a long list of folders and files and are very difficult to; 1) Know what incremental point-in-time to search 2) Remember what folder or file names changed over time 3) What point-in-time to roll the system back to in order to get your server or PC and data back to where you want it.

   The ShadowStor Approach – By running your system in a ShadowMode session, you can eliminate the need to track and manage what changes occurred at different points in time. By entering a ShadowMode session, committing files to a specific location on the disk or network, you can end a ShadowMode session and have your system in the exact state it was prior to the session with your personal data intact. This solution makes the management of shared systems and system change tracking very simple.

   If a system is a shared resource in a library, test lab, training center or public kiosk, the scheduler can be set to automatically end and restart a ShadowMode session to eliminate any changes that have taken place. This preserves the system performance and configuration with no IT resources or management required.

   For example, begin a ShadowMode session prior to installing applications, OS updates or patches. Once installations have occurred, the system can be tested before the changes are applied. If there are any issues, the session can be ended and the server or PC is returned to it prior configuration.

   Another example, a home PC could be placed in ShadowMode prior to your children playing games. The games could be installed, played and when the

ShadowMode session is ended the system is returned to its prior configuration. This approach allows you to control what changes take place from one point-in-time to the next rather than trying to figuring out what changes have taken place over time. This eliminates tracking application, OS update and patches, intrusive and malicious file changes and provides a confidence level that you know exactly what state the server or PC is in at any given point in time.

Summary

The ShadowStor approach should be your first choice for security, data protection and disaster prevention

ShadowStor solutions dramatically increase server and PC availability while reducing the cost to manage and maintain them. ShadowStor leverages intelligent snapshot technology, open file management and system protection methods to create powerful but easy to use solutions for enterprise IT organizations, test labs, help desks, libraries, public kiosks, and home users. ShadowStor technology and solutions provide:

- **Mission Critical Data Protection**
- **Complete System Uptime Protection**
- **Exceptional Speed in Recovery**
- **Reduced Total Cost of Ownership**
- **No Touch Recovery Capability**

Next Steps

ShadowUser Online - If you would like to try ShadowUser or ShadowServer, you can download a 30-day evaluation copy at www.shadowstor.com. The trial is a full functioning version of the product and will time out after 30 days from the install. Volume pricing and licensing is also available for ShadowUser and ShadowServer.

ShadowStor Leading the Way to Safer Computing™

Our Mission at ShadowStor is to provide solutions that secure your servers and PCs, allow you to control what system changes occur, and save you money by eliminating system downtime. ShadowStor solutions provide server and PC security to avoid unwanted changes to a system that can corrupt or degrade system security and stability, and can result in downtime and data loss. By avoiding these problems, you can save time and money and get to the tasks that really matter. ShadowStor products are perfect for home offices, enterprise work environments, test labs, training centers and libraries.