



Implementing an effective Desktop Security Policy



NetSupport School

Implementing an effective Desktop Security Policy

Introduction

As schools continue to provide better access to computer hardware, networks and internet resources, IT staff and classroom teachers alike face new challenges. IT staff need to manage the challenges posed by computer labs and school networks as well as effectively control both new software deployment and user access. Teachers need to manage students who are using their computers in a lab or multi desktop classroom to ensure that their time is spent focussed on learning and their assigned tasks.

Children want to learn and often the best way is to experiment. Unfortunately lab computers may be used four or five times per day for different classes and as such, they are resources that schools cannot afford to allow to endure too much practical experimentation.

The scope of desktop security within the classroom falls into three key categories:

- Protection of the desktop software and its configuration to allow for its continued use
- Protection of the local desktop, supporting files and configuration
- The control of student behaviour on the desktop and the protection of content

For each of these three categories, there are different approaches, methodology and products available that will allow a school to achieve these objectives in some way or fully. The approach undertaken by NetSupport is to provide classroom technology solutions that work together seamlessly and remove the administrative overhead from the classroom network.



Protection of the desktop software and its configuration to allow for its continued use

The classroom computers are a valuable resource. Potentially on occasions their availability is taken for granted but as soon as a system becomes unavailable, particularly in lessons where there is a necessity for one system per student, this can have an immediate impact on the productivity of the lesson.

There are two approaches to protecting a working desktop. These two approaches are either to take a copy (an image) of the ideal working environment which can then be restored as and when required; or alternatively, to revert configuration changes or damage to the existing desktop and therefore remove the need to re-image systems at a future point in time. Both approaches have benefits and, as one would expect, limitations.



NetSupport Protect provides a similar level of protection but approached from a different direction. Rather than taking a copy (an image) of everything on a PC from a given point in time, and providing the ability to restore that back in the future, NetSupport Protect will monitor all changes to the fixed disk from a given point in time and allow a system to be restored back to that original point when required.

Imaging a system typically involves installing all of the software, configuration and ancillary devices required for a system and storing an exact copy of the entire contents of the hard drive, either locally on the PC or, more typically, on a central network server. At the point where a failure occurs on the local desktop PC, the machine can be re-booted and restored back to a previous point in time. This provides a perfect safety net for the classroom systems. However, it also provides a number of potential limitations. The first of these not least is the space required to store images for desktop computers. This can be limited if all the hardware within a given classroom is identical, since a common image can be shared for all. In addition, even though students may be set to store all of their working documents to network drives, there is always a risk that valid updates on the local computer since the time the image was created will be lost once it is restored. Depending on the size of the image, there will also be a time factor in the process of restoring its image. If a school has back to back ICT lessons, then even a 20 minute delay in computer availability could have an impact on the teaching schedule.

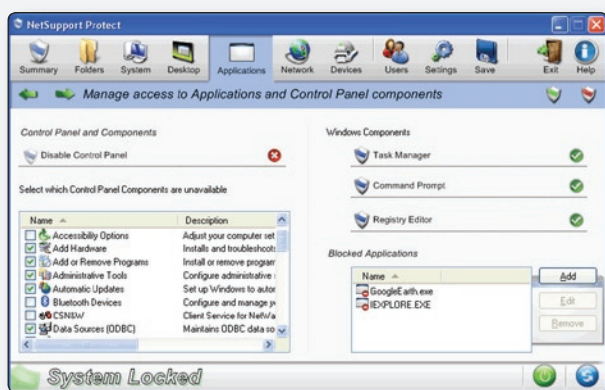
This is a subtle but important difference in the approach. Both methods provide successful restoration to a previous point in time. One requires the entire disk contents to be imaged up front, the latter, NetSupport Protect, removes the need for an image to be taken and simply tracks changes. The space required to store the changes to a hard disk over a given period of time is far less than the space required for a full disk image and, more importantly, the time to restore is therefore significantly lower. Same outcome, but a more efficient approach.

Protection of the local desktop, supporting files and configuration

As discussed above, solutions exist to restore a computer to a previous point in time. An equally valid approach to effective desktop security is to remove the ability for a desktop user, either accidentally or maliciously, to delete or modify files or configuration critical to the effective operation of the desktop computer. This partially could be achieved by using system-wide policies, an example being Active Directory. By the creation and use of templates across all machines, a central system administrator could limit the scope of access for desktop users. Naturally, this approach requires a high degree of technical competence for implementation and, potentially, ongoing maintenance to be assured that all the potential loopholes are applied. Once again, NetSupport Protect provides a similar level of control but is presented in a manner that requires limited technical competence and limited day-to-day management. Once applied, NetSupport Protect can control all aspects of user behaviour.

These can include:

- Preventing the copying, deletion and renaming of files and folders
- The ability to hide sensitive folders
- Preventing the creation of certain types of files
- Restricting changes to the desktop, taskbar and system settings
- Locking the control panel, task manager, command prompt and registry
- Restricting applications that can be utilised on the system
- Preventing files from being downloaded
- Preventing web browsers from running



This approach provides two distinct benefits for the typical school classroom. The first is clearly the ease of implementation and management and the removal for centralised administration. The second is the ability to provide practical controls without impacting on teacher interaction. In a classroom managed by administrator policies, if a teacher wished to show a student a certain action that required raised Page : NetSupport Protect - Whitepaper (c)copyright NetSupport Limited 2008 - www.netsupportprotect.com privileges, the teacher would need to log out of the student PC, log back in as themselves, highlight or explain the actions, log back out of the system and once again log in as the student. With NetSupport Protect a teacher via submission of a password could automatically suspend the desktop security settings again highlight the information to the student and re-apply. Continuing the NetSupport theme of standardised desktop products, when used in conjunction with NetSupport School, our classroom management package, the product can be set to automatically release restrictions at the point where a teacher takes remote control of a student desktop and again, automatically re-apply the security settings at the point the remote control session is terminated.

The control of student behaviour on the desktop and the protection of content

Having identified that there are tools available to both restore a previous version of a desktop computer and tools available to prevent the corruption of an existing desktop computer, the final requirement for effective desktop security is to control and guide student behaviour while using the resource.

Even though a system may have quite complex security policies in place, there would always be vulnerabilities that need to be addressed, not least the protection of userspecific data on the computer or their network drives. Again, there are a number of methods available for addressing the potential issues, which could include:

- Copying information from the PC on to a USB memory stick
- Copying information from the PC on to a CD/DVD drive
- Students installing new software from a USB / CD/DVD drive on to a desktop computer
- Students downloading inappropriate content or applications from the internet
- Students creating additional network drives and moving data between different classroom computers or the entire class.

There are a range of products under the category of “end-point security” that provide effective tools to disable or lock down the external elements of a desktop computer, ie USB ports, CD/DVD drives etc. These products typically work efficiently and effectively but are solely focussed on this one aspect of the computer lifecycle. As before, system security policies can also be utilised to provide limited and inflexible end-point security. For example, a system can have its DVD drive disabled. Naturally this approach provides the desired level of security, but removes that valuable resource from the system for its lifespan.

NetSupport Protect provides a more structured approach to end-point security. In the case of CD/DVD and USB devices, security is provided at a number of levels. The device can be inaccessible at all times; the device can be accessed so that data on the device can be read, for example Word documents or PDF files, but at the same time file copying to or from the device remains disabled; or the device can be made available at times appropriate for the class. In effect, rather than removing the flexibility for these resources to be incorporated within the classroom, NetSupport Protect allows their use when needed and prevents the risk of abuse when not. As one would expect, unrestricted use memory devices is one of the most frequent causes of viral outbreaks in a school network. NetSupport Protect also provides the tools to restrict available network drives, the ability to view network neighbourhood and to prevent new drive mappings being created. NetSupport Protect can also prevent new software being downloaded and installed by limiting the creation of specific file types and will enter lock down mode if an attempt is made to disable its operation.



Conclusion

As we have discussed, for all aspects of effective desktop security, there are a range of both approaches and solutions available for the ICT classroom. All provide benefits and limitations but with appropriate review, can deliver the required levels of functionality. NetSupport are unique in providing an integrated solution to cater for all aspects of desktop security and in addition, providing a seamless integration into an existing classroom management application, so that both teacher and student time is spent utilising the valuable technology resources in the classroom, and not lost due to system downtime.

Written by: A.Kingsley 02/2008 (updated 10/2009)

All of the features discussed in this whitepaper are provided as standard in NetSupport School.



Contacts

For more information visit www.netsupportschool.com
or contact us at the following locations :

United Kingdom

NetSupport Ltd (Head Office)
NetSupport House
Towngate East
Market Deeping
Peterborough
PE6 8NE
United Kingdom

Phone: +44(0)1778 382270
Fax: +44(0)1778 382290

Rest of the World

NetSupport Ltd (International Channel Team)
NetSupport House
Towngate East
Market Deeping
Peterborough
PE6 8NE
United Kingdom

Phone: +44(0)1778 382270
Fax: +44(0)1778 382290

Canada

NetSupport Canada
445 Applecreek Blvd, Suite 119
Markham, Ontario
L3R 9X7

Customer Care: 1-877-440-TECH
Sales: 1-888-901-7474

United States, Central & South America

NetSupport Inc.
Meadows Commerce Center
6815 Shiloh Road East, Suite A-7
Alpharetta, GA 30005

Customer Care: 1-877-715-HELP
Sales: 1-888-665-0808