

Security in the Shadows

Benchmarking Shadow Copy Functionality with Zlock™ and DeviceLock

By Roman Vasiliev, CTO, Zecurion

Corporate IT departments are becoming increasingly aware of the dangers of *data leakages* posed by *portable USB devices* within the network perimeter. From iPods to USB drives, modern enterprise faces more and more threats from countless employee-owned portable storage devices. In the hands of a disgruntled employee, these devices could seriously damage a company's reputation and even cripple its operations, depending upon the data copied and removed. Fortunately, there are ways IT departments can not only secure devices and users, but also make shadow copies of any data copied or accessed by employees.

There are many security products available today, ranging from basic virus protection to full-blown security suites and in-house designed protocols. Some offer *port* and *device access management* along with additional features, such as logging and monitoring user behavior, centralized administration and management of group policies through Active Directory. Shadow copying, one of the more popular features of these products, produces an automatic copy of information that can be moved to an external drive and stored on the server. Shadow copying helps IT personnel *monitor* and *investigate* incidents or data leakage and can potentially *prevent data losses*.

Some products and vendors offering shadow copy functionality include: Safend (by Safend), Sanctuary Device Control (Lumension), DeviceLock (Smartline) and Zlock (Zecurion). The underlying principle of shadow copying is quite simple; when a file is written by a user to any external media, a record of the data is copied which, along with certain metadata (user name, application, date, and time), is stored on the hard disk and later transferred to the server.

Extensive use of a feature like shadow copying across multiple users within the enterprise has obvious performance implications. First, users continuously move and copy data in the normal course of daily operations. Shadow copying each action requires a significant amount of network resources and bandwidth. Second, in order to analyze the information gathered through shadow copying, a business must devote additional resources to the review and monitoring of the copied information.

Therefore, it is best to develop policies governing the targeted and selective use of shadow copying. These policies can and should be based on two basic criteria: securing at the data level for files or documents and at the user level, depending on individuals' access to sensitive data. For example, a company may choose to monitor new employees during their probationary period, in conjunction with an ongoing program monitoring each employee yearly, focusing on *monitoring* employees with *access* to certain *confidential data*.

Regardless of which selection criteria are chosen, it is important to understand how different products implement shadow copying and what amount of network and IT resources are required to perform the task.

This paper provides detailed information based on benchmarking tests for evaluating the shadow copy functionality of two products: DeviceLock 6.3 (Build 14161) from SmartLine Inc. and Zlock 2.0.1.597 from Zecurion.

The tests were conducted on an IBM ThinkPad T43p notebook with a Pentium M 1.8 MHz and 1 GB of RAM running Windows XP SP2. A flash drive by Transcend JF V60 with FAT32 file system was used as the portable media device.

Copying files

We performed a common operation with *peripheral devices* - *copying* files from a PC hard drive to a flash memory drive.

Operations conducted:

- a) copying a large file (418 MB)
- b) copying many small files (1072 common file size of 393 MB)

DeviceLock showed slightly faster results - 150 seconds (20% overhead) for the large file, and 880 seconds (15% overhead) for the set of small files. Results are shown in Table 1 (below):

	Without Shadow Copy	DeviceLock	Zlock
One large file	125 s.	150 s. (+20 %)	175 s. (+40%)
Multiple small files	760 s.	880 s. (+15 %)	935 s. (+23 %)

Speed however, is only a part of the evaluation criteria. We also tested the comprehensiveness and accuracy of the shadow copy operations for both products. While copying multiple small files, both products' shadow copies performed as expected. However, when copying the larger file (418 MB), we discovered that Zlock's shadow copy appeared in the local directory immediately after starting the operation and its size grew simultaneously along with the copying progress. The complete operation took approximately 175 seconds to complete.

The DeviceLock shadow copy function behaved somewhat differently. Upon starting the operation, a new file icon appeared in the local directory and seemed inactive until the system completed the flash drive copy, taking approximately 135 seconds. The system then continued to claim resources for an additional 15 seconds in order to complete the hard drive shadow copy, for a total of approximately 150 seconds.

Further analysis shows that while Zlock performed the shadow copy in parallel with the file copying operation to the flash memory device, DeviceLock completed majority of the shadow copying only after completing the file transfer to the flash device.

Research on user behavior shows the DeviceLock approach to be vulnerable. Completing the shadow copy process after the data has been copied on to a memory device can introduce potential security issues into the process, as users often shut down the computer immediately after the flash memory copy is complete – leaving the shadow copy procedure incomplete. Additional testing revealed that when shutting down a computer immediately after the completion of the copying operation using the Windows Shut Down option, Zlock completed the shadow copy, as expected, whereas DeviceLock had shadow copied only 7% of the total file. Further tests were conducted to determine the affect on shadow copies when a Windows session is terminated abruptly by a system failure or use of the RESET button, these results will be discussed further in latter sections of this report.

Copying Microsoft Office files

We selected MS Office 2003 for testing the shadow copy functionality and behavior of both products when performing common functions within applications such as saving a document to a flash drive using the "Save As" option and modifying an existing file.

Microsoft Word file

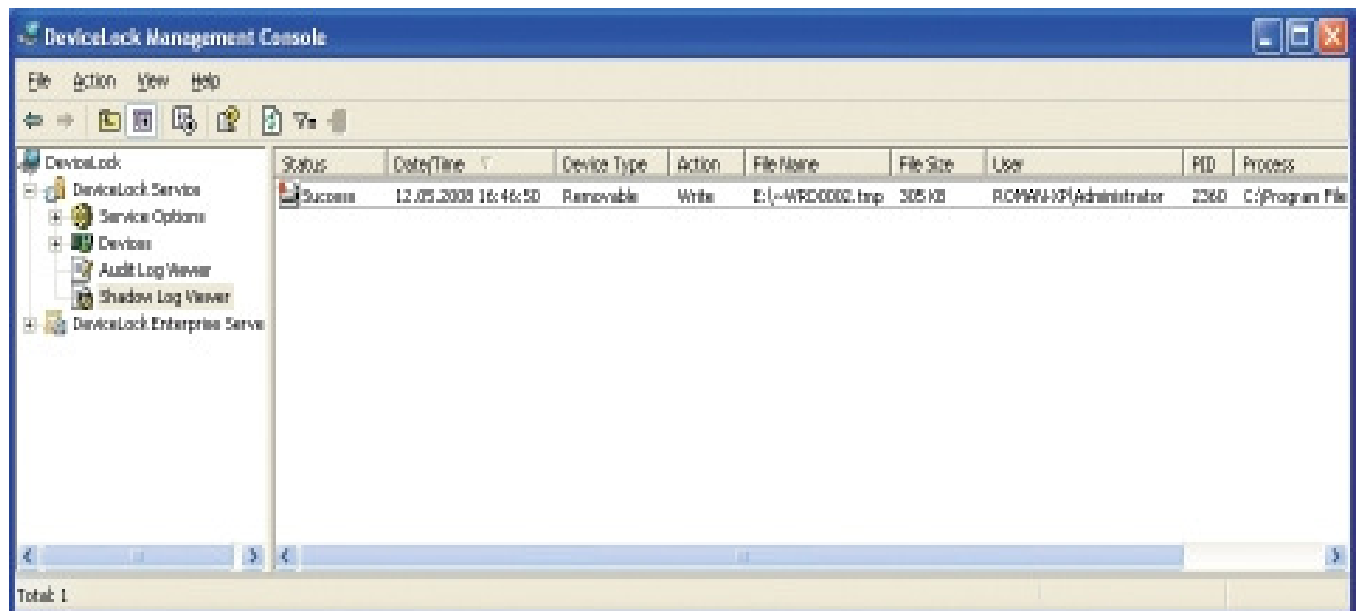
Scenario One - Creating a new file and saving it as Secret Document.doc:

- DeviceLock created a shadow copy of the file and displayed it under ~WRD00002.tmp
- Zlock created a shadow copy file displayed under Secret document.doc

Scenario Two - Modifying the existing Secret document.doc

- DeviceLock - same as in Scenario 1
- Zlock - same as in Scenario 1

(Fig. 1 and Fig. 2 below display DeviceLock console and Zlock console respectively)



Microsoft Excel files (Scenario One and Two as above)

- DeviceLock – Produced similar results to the MS Word shadow copy behavior. In some instances, instead of creating a shadow copy of the Excel spreadsheet, it created a copy of the Windows Explorer web page
- Zlock – Created a valid shadow copy under the same file name and reflected all changes

Microsoft PowerPoint (Scenario One and Two as above)

- DeviceLock – Scenario one, again yielded similar results to the MS Word shadow copy behavior. In Scenario two (editing a PowerPoint file), the program displayed the new file as ~ppt1d.tmp.
- Zlock – Created a valid shadow copy of the same file name and reflected all changes made to the presentation

Microsoft Access (Scenario One and Two as above)

- DeviceLock – In scenario one (saving an Access database), DeviceLock behaved as expected and created a temporary file. In scenario two (editing an Access database file) the shadow copy of the file did not reflect the changes made to the database. A modified .mdb file was not found under any name and it appeared that the shadow copy only contained a .acdb file, which is an Access service file designation.
- Zlock – Created a valid shadow copy under the same name and reflected all changes

Microsoft Outlook (Scenario One and Two as above)

- DeviceLock – The results reflected a similar outcome to the Microsoft Access shadow copy behavior. In some instances, the software failed to save a .pst shadow copy file.
- Zlock – Created a valid shadow copy under the original file name and reflected all changes

It should be noted that saving files via Windows Notepad worked correctly in both products, displaying both the correct file name and content. The result of our in-depth testing indicates that DeviceLock's file naming problem occurs due to an incorrect handling of Microsoft's renaming functions. MS Office applications are known for creating temporary files with unique names during the file-editing process, restoring the file back to the original name when the edits are finished.

Both MS Access and Outlook applications load their working files into memory (memory-mapped files) for better performance. Judging by the results of the tests, DeviceLock may not be properly handling the copying and the naming of these file types.

Shadow Copy Reliability Test

To further understand how these two products implement the shadow copy procedure we performed tests where Windows was abruptly shut down:

- a) Pressing the RESET button during the copying operation
- b) Pressing the RESET button immediately after the copying is completed.

These tests yielded the following results

Scenario	File Location	DeviceLock	Zlock
Press RESET button during copy operation (file size is 18 MB)	Flash memory stick	10 207 232 bits	12 828 672 bits
	Shadow copy on hard drive	Does not exist	12 845 056 bits (100 % of the original file size)
Press RESET button immediately after the file copy operation is completed (file size is 1 MB)	Flash memory stick	Copied 100%	Copied 100%
	Shadow copy on hard drive	Does not exist	Copied 100%
Press RESET button immediately after the file copy operation is completed (file size is 60 MB)	Flash memory stick	Copied 100%	Copied 100%
	Shadow copy on hard drive	3 276 800 bits (52% of the original file size)	Copied 100%

Bottom Line Benchmarking Results

1. While evaluating implementation of shadow copy by DeviceLock, the testing reveals workflow behaviors that can be easily exploited by manipulating the RESET button, effectively bypassing the audit trail process.
2. It appears that any type of analysis performed on the DeviceLock shadow copy archive requires more time and a substantially larger dedication of resources to scrutinize than the Zlock files. Given the numerous issues with DeviceLock's naming of shadow copy data, the integrity of the files remains open to serious doubts.
3. Zlock's shadow copy process is slightly more time consuming when compared to DeviceLock's implementation. However, given the results of our benchmarking tests, Zlock offers a far more secure and mature solution for securing devices on the network.
4. Overall testing shows Zlock to be the more reliable product when implementing shadow copying procedures within a Microsoft Office environment.