

23 January 2007

By: Ionut Ilascu, Editor, Software Reviews



Malware Buffering

Install and run untrusted programs in "quarantine"

Protection against all sorts of malware is always on the table when it comes to computers. There are myriads of applications that boast about securing your computer, but the truth is that most of them are securing the computer from you. Firewalls, anti viruses, anti spyware, they all fail in providing that feeling of safety we all long for. Why must there always be a vulnerability that can be exploited? Fortunately, technology is taking very alert steps towards progress and new ideas of protection are available with each year. Tomorrow's security will no longer rely on behavior detection and virtualization is the method for protecting our computers. TrustWare came up with the idea of applying the same process of a virtual machine on software. This way, virtualization is achieved at a program level and all the data that could harm your machine's running will be written in a virtual folder that does not allow any application inside to write into the registry. To put it simply, you will install, execute and write directly into quarantine. Once you have enabled the protection of BufferZone, it will be like having two computers in direct connection with one another. A file protected by TrustWare's application will be displayed with the shortcut .lnk extension on the disk and the real file will actually be placed in the BufferZone protected folder. The flexibility of BufferZone allows the user to choose which applications should run in the virtual folder and which are permitted to write directly to disk. Also, if you need a file out of the "quarantine" or as TrustWare puts it, out of the BufferZone, a context menu of the right click command gives you the chance to do just that. The interface provided by BufferZone is clean and vividly colored, the options running down in the left side of the application window. Summary option gives you all the information about the current state of BufferZone. There are the unauthorized changes that have been prevented from occurring and the number of both privacy and system threats that have been stopped. For each of these elements you are also given the total number of threats and unauthorized changes. The prevention is made by cunningly redirecting the modifications in your PC to a virtual environment. This way, no unauthorized modification will be applied to the PC and the image of the computer will remain intact. Whenever you open an application that connects directly to the Internet, BufferZone will shelter it and display in the BufferZone Programs window. The installing of the programs while BufferZone is running will be done in the safe zone and uninstalling an application in this case is done from BufferZone only. The Policy menu of the application lets the user set the Application Control settings for new executables and scripts created on the HDD, making sure that they will run in the virtual folder so that nothing can harm your machine. Whenever an unknown program is executed, you can configure BufferZone to take one of the following actions: run the program in BufferZone, prompt the user for taking a decision on the fly, deny execution or run it outside BufferZone. Device Control is also available and you can block every door to your computer while you are freely browsing the Internet. The devices available are CD/DVD ROMs, Floppy Disks, USB flash memory devices, network paths and USB HDDs. The protection options offered for each of them includes denying the access, open it in BufferZone, Confidential and no protection whatsoever. Amazingly enough, BufferZone is equipped with a firewall. It is not state of the art, but it allows the user to control the way applications communicate via ports. This way you can restrict or allow the communication through certain ports, or to certain network addresses. The major drawback in this case is that there is no browse option and you will have to manually enter the path to the application that will have to follow your rules. The firewall option is limited in what concerns adding a range of ports to close or open for a certain application, as well as defining a range of IPs. Configuring BufferZone is revealed in

Configuration option. There are no complicated settings and even a beginner could set the program up with no help at all. Setting the rules for the program to follow is the first option available. You can block the access to confidential files and folders, prevent some files from being opened and executed; or go straight to advanced rules and set email clients to run outside BufferZone, add exceptions to the rule and allow some programs (like operating system components) to interact with those in BufferZone (usually "outsiders" cannot interact with the files inside the virtual folder). You can add programs that are harmless and can always run outside the protected directory. Going down to Passwords, you can set an admin's password to restrict the access to the settings area of the software. This way no change can take effect in Configuration without the required password being provided. Once you have installed BufferZone, you will notice a red border around the protected applications. This can be really annoying for some users (me included). Fortunately, the application allows disabling this border. The downside of disabling it is that for learning if a certain program is running in the safe folder, you will have to open BufferZone. The place of the virtual drive can be changed to any drive you want (it will be placed in the root of the drive). The default C: may not always be the best choice for all the users. The developer seems to have thought of about everything there is for protecting the computer BufferZone resides in and you can set the action when a trusted program executes an unknown script or macro. **The Good** Truly amazing application and the innovative protection will guarantee the security of your computer. Any type of user can easily work with it after a short period of accommodation and getting to know how exactly the application works. I liked that for the already installed applications, the protection is activated once you execute them. Moving a program out and in the BufferZone is made easily. **The Bad** Besides the firewall drawbacks expressed in the review, no problems were registered. However, the red border is really annoying and removing it leads to another disadvantage. **The Truth** Innovative technology similar to the one used in [WindowZones](#). I guess the gate towards new protection methods is wide open. The 30 days trial period allows a full testing of the application. *Here are some snapshots of the application in action:*