



Feature Guide Read-Only Blanketing



1 Introduction

RES PowerFuse enables you to quickly and easily configure a secure and easy-to-use environment for your users. However, some settings need special attention. A user should be able to save his files on a secure location, without causing problems to the system he works on. He should also be able to locate his files easily, without having to search his entire computer for them first. The only solution for this seems to be that the administrator has to set read-only access to the files and folders on the computer manually or with extensive scripting methods. He also needs to create exceptions to specific folders, like the user's profile directory, but also folders that specific software needs to have write access to. This causes a lot of time-consuming labor.

RES PowerFuse's Read-Only Blanketing is the solution. Read-Only Blanketing is based on proven AppGuard technology. It enables administrators to render all local drives on a server or workstation running RES PowerFuse read-only. This can be done with a single click of a button. Exceptions like the temporary directory are made automatically and exceptions can be configured by the administrator.

Time	File	Process	Computer	Username	S..	Operation	Action
13:32:01.712	c:\document...	thunderbird.exe	RES\QA...	RES\luij...	0	16448 - read dir_cre...	BLOCK
13:32:01.712	c:\document...	thunderbird.exe	RES\QA...	RES\luij...	0	16448 - read dir_cre...	BLOCK
13:32:01.712	c:\document...	thunderbird.exe	RES\QA...	RES\luij...	0	16448 - read dir_cre...	BLOCK
13:32:01.712	c:\document...	thunderbird.exe	RES\QA...	RES\luij...	0	16448 - read dir_cre...	BLOCK
13:31:54.411	c:\config.msi...	pexplorer.exe	RES\QA...	RES\luij...	0	132 - open write	BLOCK
13:31:54.395	c:\config.msi	pexplorer.exe	RES\QA...	RES\luij...	0	16448 - read dir_cre...	BLOCK
13:31:54.395	c:\config.msi	pexplorer.exe	RES\QA...	RES\luij...	0	16448 - read dir_cre...	BLOCK
13:31:36.321	c:\msocache	pexplorer.exe	RES\QA...	RES\luij...	0	16448 - read dir_cre...	BLOCK
13:31:36.321	c:\msocache	pexplorer.exe	RES\QA...	RES\luij...	0	16448 - read dir_cre...	BLOCK
13:31:36.321	c:\msocache\...	pexplorer.exe	RES\QA...	RES\luij...	0	1051008 - write get...	BLOCK

Read-Only Blanketing Log



2 Read-Only Blanketing

Case 1: Terminal Server

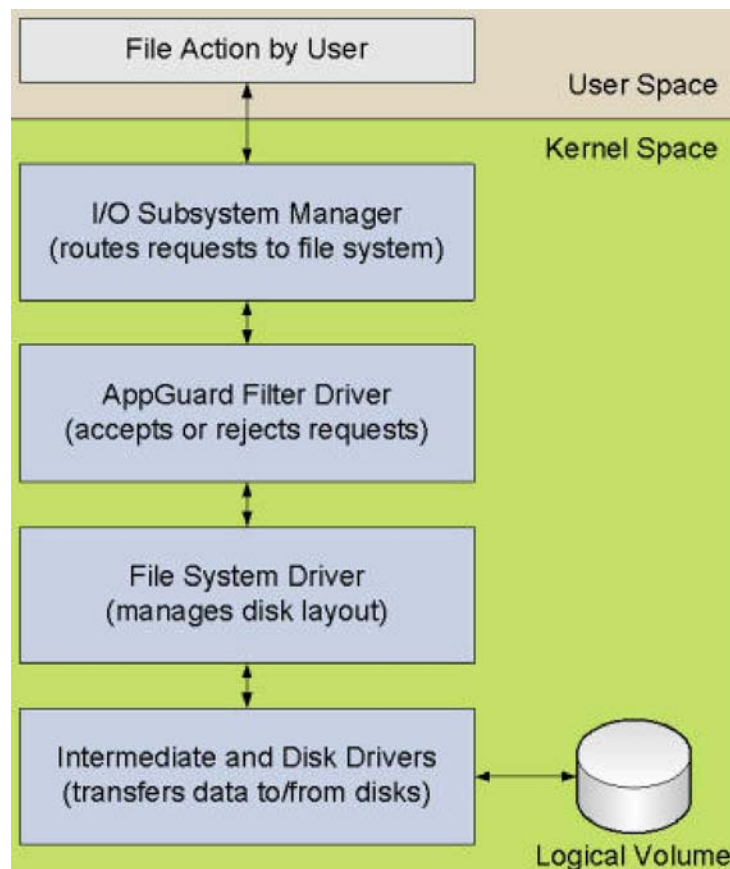
Employee Z works at Company Y and makes use of a Terminal Server environment. He uses many applications on the Terminal Server, like Microsoft Office. By default, his files and documents are saved on his home drive, but because it is possible to browse to other folders in the "Save As" dialog box, it is possible to save files on other locations, like his local disk. When employee Z then logs on to a different Terminal Server, he cannot retrieve his saved documents. If files can be saved on various locations, they can easily be misplaced, and it may take a lot of time to retrieve them. The administrator needs to use extensive scripting methods on every computer to set security permissions on files and folders to prevent this from happening.

Case 2: Laptop

User Y works at the same company. As an information worker, he works with documents, presentations, and other data all day. Each day, he spends a considerable amount of time locating files he worked on before. User Y could work much more efficient if all his files would always be available at the same location. As a Poweruser, user Y has access to all folders and files on his laptop, which means he can accidentally overwrite and delete application files and other important data. This may result in loss of information and applications may stop working. He may also lose track of files and their location.

How does Read-Only Blanketing work?

Read-Only Blanketing in PowerFuse offers a solution to situations as described above. Read-Only Blanketing enables you to effectively safeguard data against unauthorized access or modification, because it renders all local drives on all computers read-only, without touching Windows security permissions on files and folders.



Security Management Layout

Read-Only Blanketing works when it is set to "Blocking" or "Learning" mode. Before enabling Read-Only Blanketing, run Read-Only Blanketing in "Learning" mode to configure it.

The user's profile directory, temp directory, and other system directories are automatically excluded from Read-Only Blanketing. When a user accidentally tries to save a document to a local drive, Read-Only Blanketing blocks this. The



user is notified and the event is recorded in the Read-Only Blanketing log.

You can configure other exceptions on global and application level in the Global Authorized Files section of the Security Management node in the Real Enterprise Manager. This authorization may be "execute", "modify" or both.

Read-Only Blanketing:	Enabled	Updated by lujtenj 20051122
New security mode:	<input type="radio"/> Disabled <input type="radio"/> Learning <input checked="" type="radio"/> Enabled	
Security events:	<input checked="" type="checkbox"/> Log security events <input type="checkbox"/> Notify user about security events <input type="button" value="Message..."/>	
AppGuard driver version:	2005.7.3.3	<input type="button" value="Apply"/>

Read-Only Blanketing Setup

Security

With Read-Only Blanketing an administrator is able to render all local drives on all computers read-only. By doing this, the administrator prevents important application files from being overwritten or even deleted by Powerusers. The user's profile is automatically excepted from this rule. All local drives on all computers are secured with a single mouse click. It is possible to set specific exceptions. Read-Only Blanketing is based on proven AppGuard technology, guaranteeing a highly secured computer.

Administrator benefits

Read-Only Blanketing is very easy to configure. It is no longer necessary to write complicated scripts and run these on all workstations, laptops, and Terminal Servers. You can secure all local disks on every computer with a single mouse click. Read-Only Blanketing benefits from AppGuard technology. All blocked write actions by the user can be reviewed in the Read-Only Blanketing Log, which makes Read-Only Blanketing very easy to monitor and to configure. It is possible to run Read-Only Blanketing in "Learning" mode. This enables you to fine-tune the environment before rendering it read-only.

User benefits

With Read-Only Blanketing enabled the user is forced to save his files in a specified folder, because all other folders are rendered read-only. This prevents files from being saved on many different locations of his system. Because all files of the user are stored on the correct location, retrieving files will be very easy: users cannot misplace their files. Files of various users will not get mixed up. By using Read-Only Blanketing your users will be more content.



3 Conclusion

When Read-Only Blanketing is enabled, all local drives of an environment are rendered read-only. It is no longer possible for a user to overwrite and delete important files on his workstation or on the Terminal Server. Not only does this secure the user's workstation against corruption and loss of information, but it safeguards the entire Terminal Server environment. With Read-Only Blanketing, all user files are always available at the same location, which makes it easier for the administrator to manage the user and makes it easier for the user to retrieve his files.



DISCLAIMER

RES created this guide to supply information that assists you with the installation of the RES PowerFuse product and framework. Although the greatest care has been taken to make this document as accurate as possible, Real Enterprise Solutions Nederland B.V. (The Netherlands), RES EMEA B.V. (Europe), and Real Enterprise Synergy Inc. (USA) cannot guarantee the complete accuracy of the information provided in this publication. This publication and the RES PowerFuse program can be changed or terminated at any given time without further notice. Real Enterprise Solutions Nederland B.V. (Netherlands), RES EMEA B.V. (Europe), and Real Enterprise Synergy Inc. (USA) disclaim any loss directly or indirectly due to using RES PowerFuse and its features or the information that is presented in this publication. This information is not warranted for any purpose.

Real Enterprise Solutions Nederland B.V. (Netherlands), RES EMEA B.V. (Europe), and Real Enterprise Synergy Inc. (USA) disclaim any loss which could directly, indirectly, or seemingly be related to the use of RES PowerFuse, the RES Subscriber, upgrade packs, PowerPacks, any other RES-supplied software, or the use of information provided by Real Enterprise Solutions Nederland B.V. (Netherlands), RES EMEA B.V. (Europe), or Real Enterprise Synergy Inc. (USA) through any other documents.

COPYRIGHT

Copyright © 1998-2006 Real Enterprise Solutions Development B.V., All rights reserved, patents pending. RES, PowerFuse, and the PowerFuse Logo are registered trademarks of Real Enterprise Solutions Development B.V. Windows is a registered trademark of the Microsoft Corporation in the United States and all other countries. All other product names, company names, marks, logos, and symbols are trademarks of their respective owners.

⚠ WARNING: *RES PowerFuse is protected by copyright law and international treaties. Unauthorized reproduction, distribution, reverse engineering, or decompiling of the program or any portion of it, may result in severe civil and criminal penalties, and will be prosecuted to the maximum extent possible under the law.*