secRMM

Security Removable Media Manager

secRMM Delivers Unrivaled Security Auditing

Removable storage devices provide convenience and efficiency. Unfortunately, these devices can be a real threat, leaving companies susceptible to data theft. Squadra Technologies', secRMM, gives organizations the perfect tool to securely manage data assets while at the same time permitting productivity with the use of these devices.

secRMM's simple authorization policy rules allows organizations to control the who, what, where, when, and how of data copied from their network to removable storage devices. In addition, **secRMM's detailed monitoring provides organizations advanced forensic analysis to combat unlawful and/or unauthorized disclosure of sensitive information.**

secRMM Logs:

- Successful file copy operations
- Failed (unauthorized) file copy operations
- Time removable storage event occurred
- UserID of end-user performing file copy operations
- ID of removable storage devices
- Exact source file; including the file name, drive and directory from which it came
- Rule/policy changes (administrative changes)
- Removable Storage devices going on-line/off-line

Squadra Technologies
7575 West Washington Ave.
Suite 127-252
Las Vegas, NV 89128
+1 (562) 221-3079

For More Information Contact:
info@squadratechnologies.com

Free Trial Download Visit:
www.squadratechnologies.com

SUCCESSFUL FILE COPY OPERATIONS. secRMM delivers simple audits/reports letting system administrators *see* the who, what, where, when and how of data being written to removable media. Out of the box, without any security policies in place, secRMM operates in monitoring mode. Monitoring mode logs all file copy operations.

FAILED (UNAUTHORIZED) FILE COPY OPERATIONS. secRMM's flexible authorization policies/rules grant organizations the ability to prevent file copy operations. Included is the ability to control the removable storage file copy operations based on UserID, removable storage device serial number, removable storage device internal ID (i.e. VIDs and/or PIDS), drive from which the file is being written from and the program that is being used to perform the write operations. Once rules/policies have been implemented and a subsequent FAILED WRITE event occurs the same information as a successful file copy operation is collected.

TIME REMOVABLE STORAGE EVENT OCCURRED. secRMM logs the exact date and time any removable stroage event occurred.

USERID OF END-USER PERFORMING FILE COPY OPERATIONS. secRMM logs the UserID of any end-user mounting a storage device through the USB.

IDENTIFICATION OF REMOVABLE STORAGE DEVICES. secRMM logs the removable storage device product IDs and vendor IDs (PID and VIDS) for all devices. secRMM works seamlessly with smart phones, tablets and encrypted storage devices.

EXACT SOURCE FILE – FILE NAME/DRIVE. secRMM captures the complete source path of successful and/or failed file copy operations to removable storage devices. The complete source path includes the file name and the drive from which the file is being or attempting to be copied from, whether on a local or a network drive. This granular information provides the administrator with the ability to monitor and refine the file system protection within the domain. By capturing the source file secRMM provides the ability to set rules/policies which whitelists certain directories within the domain while prohibiting the transfer of files from other directories.

RULE/POLICY CHANGES – ADMINISTRATIVE CHANGES. Not only does secRMM monitor the activity of the end-user but additionally monitors and logs all rule/policy changes (ADMINISTRATION CHANGE) performed by the system administrator. secRMM records the security rule prior to a change and then records the new rule modified by the administrator.

DEVICES GOING ON-LINE/OFF-LINE. In addition to monitoring when a removable media device comes online, secRMM also records when devices go offline. By capturing the offline event the system administrator has yet another piece of information to identify the exact time security incidents occurred.

Squadra Technologies
7575 West Washington Ave.
Suite 127-252
Las Vegas, NV 89128
+1 (562) 221-3079

Free Trial Download Visit:
www.squadratechnologies.com

For More Information Contact:
info@squadratechnologies.com