secRMM

Security Removable Media Manager

Manage Your Organizations Encrypted Devices with secRMM

Many organizations either choose or are required to use hardware or software encryption technology to provide a layer of security for removing sensitive files from their network. secRMM provides the perfect solution to manage and control encrypted file copies to removable storage devices. No longer do organizations have to rely on company policies and procedures to limit the use of the USB port. Now with secRMM they can actively manage, secure, and audit USB port activity internally.

secRMM's simple authorization policy rules allows organizations to control who, what, where, when, and how data is copied from their network to their preferred encrypted storage device(s).

In addition, secRMM's detailed monitoring provides organizations advanced forensic analysis to combat unlawful and/or unauthorized disclosure of sensitive information.

Manage Your Security

- Know when *ANY* removable storage device has mounted
- Allow the copying of files to the chosen encrypted device(s) (whitelisting) by the VID and/or PID
- Log all file copies made to removable storage devices
- Capture and log the exact files being copied
- Audit the complete source file path (local drives & network shares)
- Log all failed attempts to copy files to *ANY* removable storage device.

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