secRMM

Security Removable Media Manager

Whitepaper- Legal (Law Firms)

OVERVIEW. Law firms are responsible for the management and security of client's property including documents kept on internal networks. A firm has the ethical duty to keep information relating to the representation of a client confidential.[1] The American Bar Association ("ABA") Resolution 109, adopted August 2014, addresses cybersecurity issues with respect to data breaches. The resolution encourages all private and public sector organizations to develop, implement, and maintain an appropriate cybersecurity program that complies with the applicable ethical and legal obligations, and is tailored to the nature and scope of the organization, and the data and systems to be protected.[2] Law firms in particular have a heightened responsibility with respect to potential data breaches because of their ethical and legal obligations to protect confidential information.

New commentary to Rule 1.1 of the *Model Rules of Professional Conduct* requires attorneys to "keep abreast of changes in the law and its practices, including the benefits and risks associated with relevant technology."[3] Law firms have recognized the benefit of removable media mounting to their network through the USB port to efficiently access and share sensitive data. In addition firms allow associates and employees to bring their own devices ("BYODs") to perform their tasks at work. However, without logging or authorization of BYODs and other removable media write activity anyone within a firm has the ability to remove client's confidential information. The firm will have no record of confidential data leaving and possibly becoming a data breach. Clients expect and trust that their confidential information is secure and properly managed. Imagine a client being informed that anyone with access to the firm's internal network has the ability to simply copy all confidential data onto a USB thumb drive or smart phone. Obviously this could harm the firm's reputation, not to mention subject it to civil liability and/or ethical violations. Thus, a law firm needs to implement an enterprise security program ("ESP") that addresses the security hole presented by removable media mounting through USB ports to ensure they are adequately protecting their client's confidential information.

---

[1] ABA Model Rule 1.6- Confidentiality of Information.

[2] ABA Resolution 109, Cyber Security Legal Task Force- Section of Science & Technology.

[3] ABA Model Rule 1.1- Competency, Commentary.

secRMM BENEFITS TO LAW FIRMS…

SIMPLE AUTHORIZATION MODULES. secRMM provides simple authorization modules for firms to control the who/what/where/when/how of data being written from their network to removable media. Unlike other competing solutions, secRMM lets firms control what files the end-user can copy from both the local computer and the network. Additional functions allow for firms to control removable media write activity based on userid, removable media serial number, removable media internal IDs (i.e. VIDs and/or PIDs) and the program that is being used to perform the write operations. The solution can also prevent unauthorized devices from mounting to the Windows Operating System. When an individual attempts to perform an unauthorized copy or mount secRMM logs the event. This enables firms to further investigate why the user was attempting to perform that activity and helps stop future potential breaches.

CONTINUED USE OF "BRING YOUR OWN DEVICES" ("BYODs") WITH SECURITY. With the increasing use of BYODs organizational networks cannot be adequately secure without procedures in place to limit/prevent write activity or monitor the who/what/where/when/how of files being written. secRMM is the only solution capable of providing source file names for write operations to virtually all removable media- smart phones (iPhone, Blackberry, Windows, Android, etc.), tablets, USBs, and CD/DVDs. This allows firms to easily and centrally evaluate activity being performed on endpoint terminals. secRMM provides for effective assessment of potential risks by monitoring and collecting detailed forensic data about removable media write activity or even attempted write activity.

ADDED PROTECTION TO ENCRYPTION TECHNOLOGY. secRMM works seamlessly with hardware/software encryption technologies to generate security events which informs a system administrator when an encrypted device has been mounted, and whether authorization was granted.

INTEGRATED WITH MICROSOFT SYSTEM CENTER SUITE OF PRODUCTS. secRMM is tightly integrated with the Microsoft System Center suite of products; including System Center Configuration Manager ("SCCM"), System Center Operations Manager ("SCOM"), SCOM Audit and Collection Services ("ACS"), and System Center Orchestrator. This allows the system administrator to set up alerts, notifications, tasks, reports, and can optionally generate SNMP traps, among other desirable capabilities.

COMPLETE SOURCE PATH. secRMM is the only Data Loss Prevention ("DLP") software capable of capturing the complete source path of a file being copied to a removable media storage device.

secRMM DOES NOT REQUIRE ITS' OWN FRAMEWORK. secRMM easily integrates into the enterprise management framework firms are currently using. This makes secRMM particularly cost effective compared to other solutions. secRMM accomplishes this by utilizing the base Windows Operating System components. Furthermore, secRMM is completely functional within the Windows Event Log and the base Microsoft Management Console ("MMC"). Given these efficiencies Squadra is able to provide the software at *affordable pricing*.

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