secRMM

Security Removable Media Manager

Whitepaper- Government

OVERVIEW. The Federal Information Security Management Act (FISMA) enacted in 2002 set requirements for federal agencies to develop, document, and implement agency-wide programs which provide security controls over information resources that support Federal operations and assets.[1] With the publication of WikiLeaks files obtained by insider Army intelligence analyst Bradley Manny, in 2010, vulnerabilities of sensitive and classified assets on government networks was highlighted. In response President Obama signed Executive Order (EO) 13587 on October 7, 2011 which addressed structural reforms to the oversight of classified information.[2] Executive Order 13587 directs the heads of agencies that operate or access classified computer networks to have responsibility for appropriately sharing and safeguarding classified information. [3] Further, in November 2012, the White House issued the National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs.[4] The importance of agencies implementing safeguards against insider threats was brought yet again to the forefront with the leaking of millions of documents by NSA contractor Edward Snowden.

After such significant breaches of sensitive information agencies are now required to monitor computer networks with unprecedented scrutiny. It is imperative for government agencies to meet the standards that are outlined in the Insider Threat Programs which include having the capability to gather, integrate, centrally analyze and respond to key threat related information. In addition, the Minimum Standards for Insider Threat Programs makes agencies responsible for setting up systems to monitor employee's use of classified networks.

---

[1] 44 U.S.C. §3541, et seq.

[2] Executive Order (E.O.) 13587, Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information (October 13, 2011).

[3] *Id*.

[4] Presidential Memorandum, National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs. (November 12, 2012).

secRMM BENEFITS TO GOVERNMENT AGENCIES…

SIMPLE AUTHORIZATION MODULES. secRMM provides simple authorization modules for government agencies to control the who/what/where/when/how of data being written from internal networks to removable media. Unlike other competing solutions, secRMM lets agencies control what files the end-user can copy from both the local computer and the network. Additional functions allow for the control of 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 try's to perform an unauthorized copy or mount secRMM logs the event. This enables further investigation into why the user was attempting to perform that activity and helps stop future potential breaches.

CONTINUED USE OF BYODs WITH SECURITY. With the increasing use of BYODs networks cannot adequately be secure without procedures in place to limit/prevent write activity and/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 for the ability to 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.

AFFORDABLE SOLUTION. secRMM was developed with government agency requirements in mind. We understand the budget restraints many agencies are now facing. Thus, we created a solution that reduces information security risks without requiring substantial upfront costs and maintenance overhead. While other solutions on the market today claim to protect against a security breach they are not cost-effective. secRMM is able to fill this void by reducing the security risks of removable media mounting to agency networks for an affordable rate. This is accomplished by secRMM *not requiring its' own framework* (i.e. dedicated servers used to implement the solution).

secRMM DOES NOT REQUIRE ITS' OWN FRAMEWORK. secRMM easily integrates into the enterprise management framework agencies are currently using. 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