



FOR IMMEDIATE RELEASE

Media Contact:

Stephanie Scrivens
Tresys Technology
P: 410-290-1411 x151
E: sscrivens@tresys.com

TRESYS TECHNOLOGY ANNOUNCES LATEST RELEASE OF FiST 4.0

USB cleansing appliance has unique filtering, disinfection and deep content inspection

Columbia, MD, May 24, 2010 -- Tresys Technology, a provider of technology and services for customers with high security requirements, today announced the availability of release 4.0 of its File Sanitization Tool (FiST), the only solution approved to deal with the challenges of USB drives and other removable media in high risk DoD environments.

Tresys' FiST is a unique solution that sanitizes mobile media to enable the secure use of these media in mission critical environments. FiST identifies malicious code, viruses, trojans, rootkits, steganography, and malformed software, removes that code and makes the media safe for use and from infecting DoD systems. FiST uses virus scanners and multiple filtering techniques to provide deep content inspection on numerous file types to ensure their validity and integrity.

In a well-publicized set of events in November of 2008, a set of targeted malware threats were introduced into operational military environments by USB thumb drives, allegedly by organizations connected to foreign intelligence operations. In the aftermath, most of the U.S. Government halted use of USB thumb drives and other types of mobile media except under strict controls. In the past month, the U.S. Government has partially lifted the ban allowing the limited use of removable data devices under strict requirements. These requirements include approval by the unit commander and approved procedures and hardware.

"In 2008, Tresys was asked to develop a solution that would provide ongoing assurance that only known good content could be moved into and out of its information domains," said Karl MacMillan, VP of Technology for Tresys. "We quickly produced a working prototype to address immediate threats, and today have an appliance-based solution that offers extensive functionality and support for more devices and file types."

Earlier releases have been deployed in operational units in active theaters, and as evaluation units for a variety of USG and friendly foreign government entities. With the final approval in February of a plan to permit use of mobile media again, the release of version 4.0 is timed to provide the latest features with the first widespread field implementations.

FiST v4.0 includes the following new features and enhancements:

- Support for 22 file types, including Microsoft® Office 2007 and NX PowerLite v4 archive files
- Support for rewritable optical media (CD-RW, DVD+RW, and DVD-RW) as the data destination devices
- Ability to conduct secure network updates of virus definitions and logging for later pattern analysis
- Ability to sanitize up to 16 GB of data per one USB device
- Ability to configure, import and export dirty and clean lists
- Support for sanitization and secure erase of IronKey S100 Enterprise and S200 Basic, Personal, and Enterprise hardware encrypted USB devices
- Support for sanitization and secure erase of MXI hardware encrypted USB devices
- Support for Mac OS files where FiST generates media and files that can be read using a MacSecure
- More intuitive administration interface with added functionality

For additional information on features and benefits and how to purchase FiST please visit www.tresys.com/file-sanitization-tool.php. FiST is available for Government agencies.

About Tresys Technology

Tresys innovates and applies advanced technologies to quickly solve the needs of customers who require agility and responsiveness to meet their security requirements. Leveraging secure open source software, our products and services support the most sensitive security missions around the world. As a result Tresys enjoys a distinct reputation for shifting the way governments and businesses approach security. For more information, visit: www.tresys.com.