



FEATURES

Detect virus or malware infected files
Quarantine virus or malware infected files
Safe handling of virus and malware infected files
Clean and verify files are cleansed
Remove unknown file types
Remove steganography
Analyze, remove, cleanse embedded objects
Remove or cleanse color or size obfuscated text
Remove macros from documents
Remove or cleanse metadata
Remove unrecognized data
Validate file formats
Embedded object extraction and scanning
Secure device erasure
Hidden content identification and cleaning
Forensic imaging
Strong transactional separation



Anti Virus Software Tools protect only against known bad malware. **FiST** allows only known good content.

Purchasing

FiST is available directly from Tresys Technology. Purchases may be made by either government credit card, organization purchase order, or through the Maryland Procurement Office (MPO) contract number H98230-09-D-0090. Contact Tresys directly to place an order or for additional information about the MPO contract. FiST devices are delivered within six to eight weeks from date of order.

Pricing

Contact Tresys directly to discuss pricing and volume discounts.

About Tresys

Tresys innovates and applies advanced technologies to quickly solve the needs of customers requiring agile responsiveness to security requirements. By 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 business approach security.



8840 Stanford Boulevard
Suite 2100
Columbia, Maryland 21045

Phone: 877-419-7472
Fax: 410-953-0494
E-mail: sales@tresys.com



File Sanitization Tool



USB AND CD/DVD SANITIZING

- **Conducts** deep content inspection and analysis
- **Detects, cleanses, removes** and **stores** (for forensic analysis) malicious hidden content, viruses and malware
- **Addresses** sources of attacks targeting USG systems in portable media

Overview

USB "thumb drives" are widely used to share vital information in forward locations, move data between coalition partners, deliver command instructions and situation briefs and a wide variety of other applications. Recently, USB drives have been identified as an attack vector for various forms of advanced viruses and malware that could impact critical systems. As a result, their use has been restricted or even banned in some environments. Tresys FiST is the only solution that disinfects USB devices and files to enable secure use of the devices for mission critical environments.

Benefits

Enables secure data sharing with USB devices that are widely used to handle vital information in forward locations, move data between coalition partners, deliver command instructions and situation briefs and a wide variety of other applications.

Reduces risk of USB as an attack vector for current forms of attacks and allows integration of new filters and capabilities to deal with emerging attacks as well as additional devices as requirements evolve.

Minimizes support requirements by locking down FiST operations to ensure that minimal user interaction is needed (or allowed) to properly scan and sanitize USB devices and files. A simple CONOPS combined with appliance-like operations reduce the chance of operator error or service interruption.

Captures infected files for forensic analysis to support the identification of attack types, trends and sources.

Laptop-based Kiosk— Built for a COTS 64 bit platform including a laptop to support rapid deployment and mobile operations.

Isolated Environments— Uses SELinux and Tresys' VM Fortress to positively isolate the incoming 'dirty' side of the application where filtering is performed.

Adaptable Filters— Integrates custom government and commercial filters with Tresys' own technologies to provide state of the art identification of advanced malware and viruses.

Forensic Capability— 'Dirty' data is stored for later forensic analysis in a controlled and isolated environment.

Supported Files Version 4.0

Microsoft® Office (97-2007)

- Word (.doc)
- Excel (.xls)
- PowerPoint® (.ppt)

Text and Presentation Files

- ASCII text files (.txt)
- Portable Document Format (.pdf)

Compressed Files

- BWT zip (.bz2)
- UNIX tar (.tar)
- Pkzip (.zip)
- GNU zip (.gz)

Image Files

- Joint Photographic Experts Group (.jpg, .jpeg)
- Windows® Bitmap (.bmp)
- Tagged Image Format (.tif, .tiff)
- Windows® Metafile (.wmf)
- Windows® Enhanced Metafile (.emf)
- Graphics Interchange Format (.gif)
- Portable Network Graphics (.png)



How does FiST work?

- A user inserts a suspect USB drive or other media. It is scanned, cleansed and made ready for use in USG systems and networks. All interactions are guided by an animated graphical user interface.

What happens to infected or unrecognized files?

- Files with unrecognized or prohibited (i.e., executable file) formats will be removed.

Does FiST work with encrypted USB devices?

- FiST currently supports all MXI keys and IronKey Enterprise, Personal and Basic versions for source ('dirty') and destination ('sanitized') files. Other encrypted USB devices will be supported in the future.

