



Tresys XD Air™ Risk reduction
for removable media file transfer



XD Air

Removable Media Threat Protection

XD Air™ is a kiosk that provides the strongest removable media threat protection available. Developed in conjunction with the National Security Agency (under program name FiST), XD Air is the only U.S. Cyber Command-approved tool for the transfer of classified documents via portable media.

An integrated hardware/software package, XD Air:

- Inspects and cleans files on portable media to mitigate the risk of introducing malicious content
- Applies advanced filtering techniques to perform deep content inspection of complex file types, exposing hidden threats and data missed by conventional antivirus and anti-malware protection
- Securely erases destination media
- Detects irregular behavior of removable device firmware, preventing propagation of firmware-based attacks

In short, XD Air secures the air transfer gap by protecting against inbound attacks and malware and also guards against outbound data compromise and loss.

tresys.com

Proven

Successfully deployed in more than 1,000 government and critical infrastructure applications

Sophisticated

Employs the latest tools, filters, and deep content inspection techniques to detect and remove malware and other malicious content from portable media

Flexible

- Enables assured transfer of classified data between high-risk networks
- Assists in the controlled release of sensitive government documents by exposing hidden content and verifying cleansing before release
- Protects against media-borne, data-borne and supply-chain threats when transferring data to secure or critical networks

Hardened

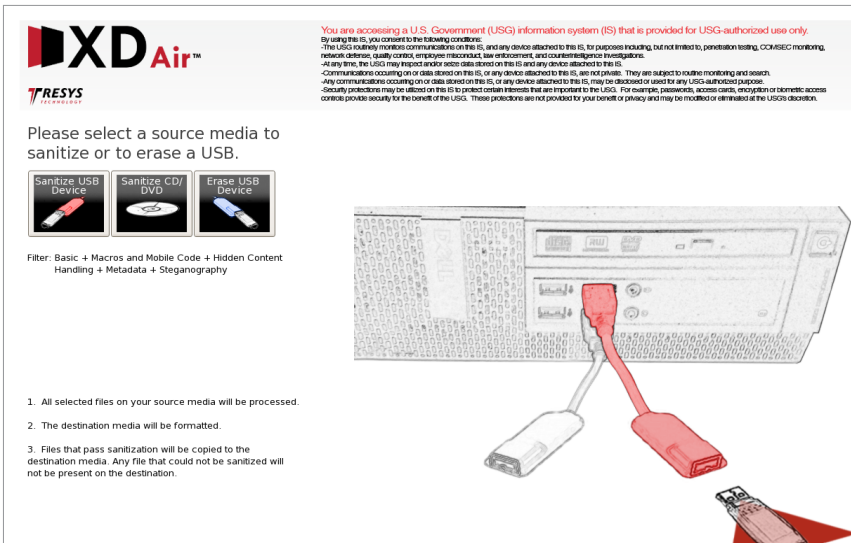
The XD Air product is hardened out-of-the-box against attacks from media-borne malware and does not require additional hardening by the customer to meet to NEI or government requirements

Certified

- Meets Department of Defense's JTF-GNO CTO-10-004A requirements for Removable Flash Media Device Implementation
- Adheres to Nuclear Energy Institute (NEI) 08-09 guidance for secure data transfer using portable media

XD Air™ Goes Well Beyond Conventional Virus Scanning to Uncover Hidden Threats

	Zero-Day Threats	Device	Malware	Steganography	Blacklist Terms	Unknown File Types	Metadata	Embedded Objects	Unrecognized Data	Macros	Obfuscated Text
XD Air™	●	●	●	●	●	●	●	●	●	●	●
Virus Scan	✗	✗	●	✗	✗	✗	✗	✗	✗	✗	✗



XD Air

Removable Media Threat Protection

XD Air Three Methods of Protection

Unlike antivirus-only solutions, XD Air implements three forms of protection to ensure that malicious content does not get transferred into a secure network or facility.

Known Good: XD Air performs deep content inspection on common document types and transfers only “known good” content to clean destination media. This process eliminates hidden data, macros, and executable content. Because it doesn’t rely on signatures of known malware, this process is effective against zero-day attacks.

Known Bad: All files are also scanned with multiple antivirus engines as an added layer of defense.

Known Source: By verifying the signature of digitally signed files and determining that content exactly matches a signed manifest, XD Air helps establish the trusted transfer of known-source files into secure networks or facilities.

Supported Media Types

- USB flash drives
- CD/DVD
- SD cards
- Portable hard drives and SSDs
- Select hardware-encrypted USB flash drives
- Compact flash
- Floppy disks

8840 Stanford Blvd

Suite 2100

Columbia, MD 21045

410.290.1411

tresys.com

TRESYS