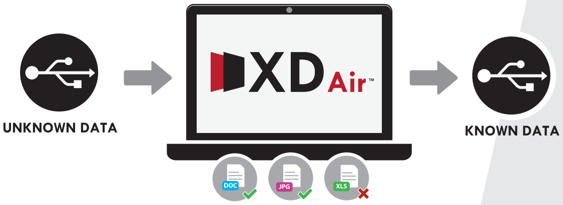
TRESYS
TECHNOLOGY

XD Air

SECURING AIR GAP TRANSFER

USB devices are often the convenient go-to means of transferring files between systems, whether internally, or from external sources. These devices, and the data on them, present a significant malware risk inbound, and potential data loss outbound. XD Air is a secure platform that inspects and cleans files on removable media to mitigate the risk of introducing malicious content or inadvertently releasing classified or confidential data. By performing deep content inspection of complex file types on removable media, XD Air enables secure transfer of only known good content. Deep content inspection exposes threats and hidden data missed by conventional anti-virus and anti-malware. These traditional scans only identify known bad data, an approach that leaves the system vulnerable to new exploits and targeted or zero-day attacks, and does nothing to prevent unintentional release of hidden data.



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

USE CASES

COMMERCIAL

Employees routinely use USB sticks to transfer files between computers, whether between home and work, or different machines at work. They bring back USB sticks from trade shows and conferences, and don't really know what those sticks may do to your computer. XD Air can help protect your machine from infection by allowing you to transfer only known good files from the source stick to a trusted destination stick before putting it in one of your corporate machines.

CRITICAL INFRASTRUCTURE

Nuclear Regulatory Commission Guidance states that secure data transfer must "ensure that the data, software, firmware, and devices are free from known malicious code, Trojan viruses, worms, and other passive attack." The scope of this regulation includes protecting against the full spectrum of portable media threats, including data-borne and device-borne threats. Traditional anti-virus scanning can address some of these threats, but not the full spectrum. Using XD Air in a secure deployment provides the full scope of protection against data, software, firmware, and device threats.

GOVERNMENT

While file transfer between networks of different security levels is essential to supporting operational needs, it is no secret that Government networks are prime targets for exploitation. XD Air meets the requirements of JTF-GNO CTO 10- 004A for Removable Flash Media Device Implementation. XD Air is the only USCYBERCOM-approved tool for the transfer of classified data between high risk networks using portable media.

BENEFITS

XD Air is purpose-built to protect against removable media threats. It isolates the “dirty” side, where it reads data from media of unknown provenance, from the “clean” side, where known good files are written to the target media; while protecting itself from attack. XD Air also provides state-of-the-art protection against malware and viruses, and integrates new filters as technology requirements change. To support forensics on the original files, XD Air can store the source media image to a controlled and isolated environment for off-box analysis. XD Air supports inspection and remote logging to central facilities for aggregated analysis of events. Other benefits include:

- Assists reliable human review of data as part of document release decisions (pre-review to expose hidden content and post-review to verify cleansing)
- Mitigates against many types of zero-day exploits
- Mitigates against device exploits
- Enables the use of removable media in secure areas
- Secures supply chain & corporate distribution of information assets
- Permits scanning of devices & content from unknown or untrusted sources, can be bundled with firmware locked USB thumb drives to enable protection of the enterprise from incoming devices
- Enables sharing of vital information in forward locations, including moving data between coalition partners (e.g., delivering command instructions & situation briefs)
- Supports configurable enforcement of a custom security policy

SUPPORTED FILE TYPES

Microsoft Office (97-2010)	Word (.doc, .docx, .docm)	Excel (.xls, .xlsx, .xlsm)	PowerPoint (.ppt, .pptx, .pptm)
Text & Presentation Files	ASCII & UTF-8 text files (.txt, .csv)	Portable Document Format (.pdf)	
Compressed & Archive Files	BWT zip (.bz2) Pkzip (.zip)	UNIX tar (.tar)	GNU zip (.gz)
Image Files	Joint Photographic Experts Group (.jpg, .jpeg) Windows Metafile (.wmf) Portable Network Graphics (.png)	Windows Bitmap (.bmp) Windows Enhanced Metafile (.emf)	Tagged Image Format (.tif, .tiff) Graphics Interchange Format (.gif)
Other Files	Extensible Markup Language XML (.xml)	Pre-Validated Signed Files (.pgp, . gpg)	

SUPPORTED MEDIA TYPES

USB Flash Drives	CD/DVD	Solid State Drives	SD Cards*	Portable Hard Drives	Hardware-Encrypted USB Flash Drives	Compact Flash*	Floppy Disks*

** denotes with supported adaptor and/or drive*

ABOUT TRESYS TECHNOLOGY

Tresys Technology delivers effective, secure, state-of-the-art solutions to continually changing cybersecurity threats. We have unparalleled expertise in high assurance architectures for enterprise and mobile computing, protecting access, transfer, and storage of our customer’s information assets. Tresys clients include critical infrastructure, mobile solution providers, military, and civilian government agencies worldwide. Tresys’ certified and accredited products protect information and ensure that the appropriate data gets to the correct location in a timely and secure manner.