TRESYS TECHNOLOGY

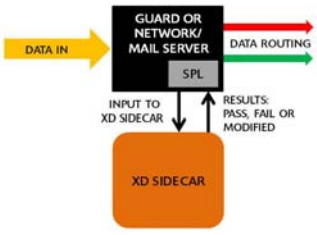
XD Sidecar™

Assured Information Solution for Complex File Type Filtering

Filtering engine that adds deep content inspection of complex file types to existing Cross Domain Solutions and network or mail servers

OVERVIEW

Tresys XD Sidecar offers a complete, cost-effective solution for adding inspection and cleansing of complex file types to existing Cross Domain Solutions (CDS) (as well as to applications requiring the inspection of large volumes of data) to prevent ex-filtration or to provide trusted exchange between parties. Based on the filtering technology of NSA's Assured File Transfer (AFT) CDS, XD Sidecar serves as an 'offload engine' for performing deep content inspection of complex file types—such as Microsoft Office documents, archive files, images, and PDFs—to ensure that only **known good** content is passed between networks. It applies customizable filter configurations to scan files for malicious content, 'dirty' words, hidden data, and appropriate classification prior to transfer via a certified guard/server. Key to its flexibility is **Tresys' Sidecar Protocol Library (SPL)** and **Filter Sidecar Protocol (FSP),** open source-based APIs that reside on the guard/server and the XD Sidecar, respectively, and make it easy to interface XD Sidecar with the existing CDS or server. The SPL and FSP function as the trusted broker to offload filtering from the guard/server and send the results back for appropriate action, either to process the file through to another domain or to quarantine the file for additional review. The SPL and FSP include transfer agents that provide communications for sending, receiving, and controlling the flow of jobs between XD Sidecar and the guard/server and for administrative management of XD Sidecar itself.



XD SIDECAR FILTERING PROCESS

HOW IT WORKS

XD Sidecar supports simultaneous connection to multiple guards/servers. Customizable filter policies are accessed by the approved guard/server as appropriate for the job and are applied against the supported file type(s). The guard/server sends files to XD Sidecar for inspection, verification, and cleansing via FSP. XD Sidecar filters then apply **known good** operating policy to inspect the file (including identifying metadata and macros) and scanning for dirty/clean words, hidden content, and other unsafe attributes. XD Sidecar verifies that a file has passed the filtering process and notifies the guard/server that the file is ready for retrieval. Questionable content is cleansed, when possible, to meet the filtering requirement, prior to being transferred to the guard/server. For files that have been found to violate an element of the **known good** policy, XD Sidecar's PDF Export capability can configure policies to convert those files into PDF files. This ability enables the data to remain available on the output side for review. Following the filtering process, a report detailing verification, inspection, and cleansing is transferred to the management console for review. XD Sidecar performs the complex filtering process, thereby freeing the guard/server to use resources to perform transfers.

SOLUTION BENEFITS

- Enables the addition of complex file type processing to existing systems without having to recertify the complete solution
- Provides robust filtering capabilities, deep content inspection, cleansing, and transformation functions that would be extremely cost-prohibitive to design and implement from inception
- Enables export of rejected files to PDF format-viewable files for safe review of documents on the output side
- Decreases the time and expense required to evaluate, certify, and field new filter processing capabilities and provides a lower risk path to Certification and Accreditation (C&A)
- Supports implementation on virtual or bare metal servers
- Offloads filtering from the guard/server which frees system resources to handle transfers
- Provides additional layers of security to existing processors
- Provides capabilities and critical information quickly

SUPPORTED FILE TYPES

Microsoft® Office (97-2010)

- Word® (.doc, .docx, .docm)
- Excel® (.xls, .xlsx, .xlsm)
- PowerPoint® (.ppt, pptx, .pptm)

Text and Presentation Files

- ASCII text files and Comma Separated Values (.txt, .csv)
- Adobe® Portable Document Format (.pdf)

Compressed and Archive Files

- BWT zip, bzip (.bz2, .bz, .tbz2, .tbz)
- UNIX tar (.tar)
  Note: Windows-generated .tar files are not supported
- Pkzip (.zip)
- GNU zip (.gz)

Image Files

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

Other

- eXtensible Markup Language XML (.xml)
- Pre-validated signed files (.pgp, .gpg)

SUPPORT FOR DEVELOPERS

- A fully compliant Software Development Kit (SDK) is available and contains:
  - Documentation for Filter Sidecar Protocol (FSP)
  - Source code for Sidecar Protocol Library (SPL) [available in multiple platforms]
  - Installation and use instructions

About Tresys

Based in Columbia, Maryland, with offices in Ashburn, VA, Tresys Technology solves the most complex information security problems for a wide array of defense, intelligence, and commercial customers. Tresys provides innovative product and services solutions for hard problems in Cross Domain, Deep Content Inspection, secure operating systems—including SELinux—mobile devices and OSs, and software assurance. Our knowledge of the secure design, certification, and accreditation of complicated custom hardware and software solutions, combined with insight into the sophisticated requirements of our customers, allows us to deliver innovative solutions to modern security challenges. The experience gained from solving real-world problems has enabled Tresys to develop industry-leading and authoritative services. For more information, visit: **www.tresys.com**.

TRESYS TECHNOLOGY