advenica

File Security Screener

Solution

Importing files into secure environments poses a great security threat if the files are not properly sanitized before transfer. The File Security Screener is a high assurance Cross Domain Solution with malware security scanning and content disarm & reconstruction capabilities.

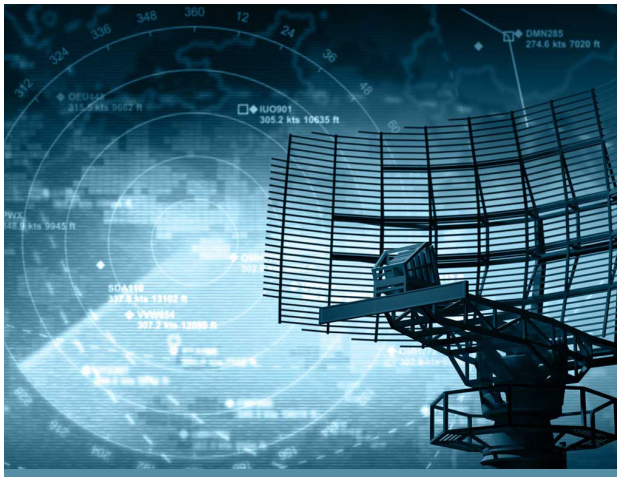
Secure file import

Transferring files between security domains pose risks to the integrity and confidentiality of the receiving system. Malware in your secret network may exfiltrate information, perform sabotage by altering or make information inaccessible by ransomware. To avoid above, all entry points must secure the data *before* it is imported. Advenica's Cross Domain Solutions provide efficient and automated counter measures for malwares and at the same time assure separation for the connected networks.

Unidirectional assurance

Advenica's File Security Screener is designed for the national security segment as well as other high security environments like critical infrastructure. The solution provides:

- malware scanning by integrating to any third-party solution such as OPSWAT MetaDefender Core and sandboxing environments.
- high assurance protection from information leaks by using Advenica´s Data Diodes.
- high assurance separation between different import sources by the use of Advenica´s Data Diodes.
- caching of data to be scanned, allowing service on the central equipment without data loss.
- customizable import rules based on the source of the information and the file type.
- scalable solution with ability to increase the number of connected source networks or increase throughput.



High assurance Data Diodes

Advenica´s Data Diodes DD1000i and DD1000A meets the highest demands on both security and assurance. The integrated proxies are fully separated from the optical diode hardware. Special attention have been given to eliminate the risk of covert channels in the reverse direction, resulting in functions like; one PSU for each side of the data diode and RFI/EMI-reducing internal enclosures to prevent compromising emissions.

SecuriCDS DD1000i is a data diode with hardware based optical separation to assure unidirectional data flow. DD1000i includes proxy services to handle application level protocols and provides an easy integration into any system. It is designed, tested and produced to meet the highest security requirements. In the File Security Screener, special services have been designed in the DD1000i to enable validation and transfer of files.

Configurable actions

The file transfer behaviour is controlled in the File Security Screener by a Ruleset. The Ruleset defines which actions that should be taken on a file depending on external source, file type and result from one or several qualification engines. The Ruleset also includes configuration for prioritisation of file types from one or more sources, archiving of transfered files and setting valid responses from third party scanning.

Third party scanning functions

Third party scanning functions can be e.g. antivirus, mathematical/statistical functions, custom sandboxes or CDR engines (Content Disarm and Reconstruction). In the normal set-up of the solution, antivirus scanning is handled by third party software (OPSWAT MetaDefender Core). Interfaces to other third party functions can be supplied as addons through Advenica´s Professional Services. If interface to several third partly scanning functions exist, the Ruleset allows you to define if one or several scanning functions shall be applied to a single file before allowing it to be imported.

Technical brief

- File transfer protocol: SFTP
- Support for large files, up to 100GBytes
- File transfer capacity: 300Mbps (scale up is possible)
- Interface to OPSWAT MetaDefender Core (basic setup)
- Quarantine and archive of files are supported
- Log and monitoring through Syslog and SNMP
- External heartbeat from source networks to protected network supported

File sanitation

The File Security Screener is designed to automatically handle files and security scanning. Only white-listed file types will be security scanned, sanitized and transferred. The degree of security scanning and sanitation required before importing a file may vary based on the trust of the source network. File Security Screener can be configured to act differently based on source, trust-levels and many other criteria.

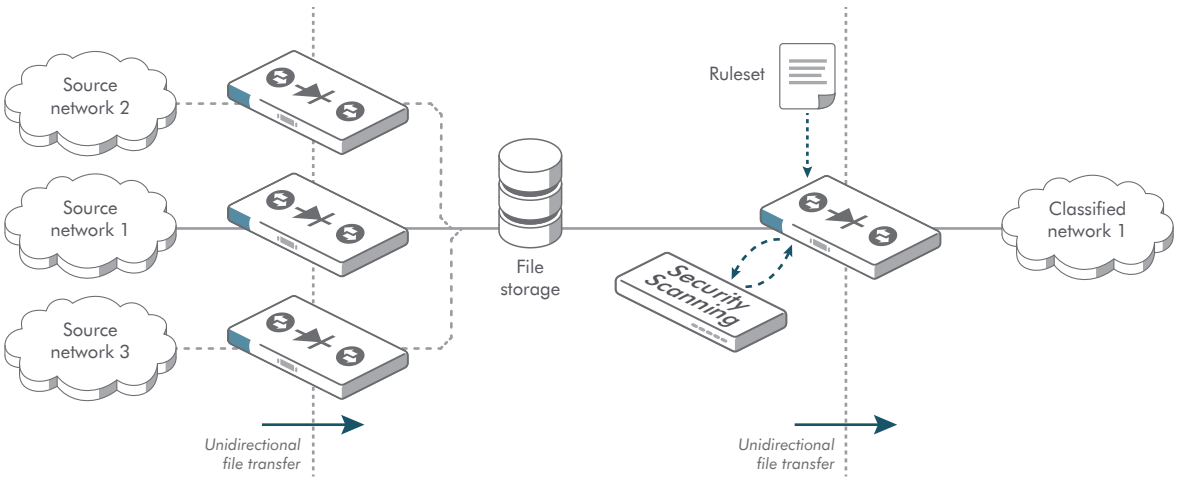
The File Security Screener provides an efficient, scalable and trusted solution for secure file import.

Use case: Secure file transfer to classified network

The solution is designed for securing file transfers to classified networks by qualifying the file before import. In this use case software updates can be safely imported to the classified network, along with other files. Before import, all files are scanned for malwares and threats are actively removed using OPSWAT MetaDefender Core and its CDR functionality.

Use case: Intelligence analysis

The solution supports multiple source networks where files should be imported in to a single security domain for e.g. intelligence analysis. These sources may vary in classification but thanks to the high assurance in Advenica's Data Diodes the separation between the sources are withheld. Even the Open Source Intelligence (OSINT) may be connected through this and used as an input source if needed.



File Security Screener overview.

Doc. no.: 17871v1.3.

ISO 9001 CERTIFIED
ISO 14001 CERTIFIED