use case #11

File Security Screener

Creating a secure data import

advenica

Creating a secure data import

The File Security Screener (FSS) is designed to automatically handle security scanning for content that needs to be imported to or transferred between different secure IT domains. All file types will be security scanned, sanitised and transferred. The degree of security scanning and sanitation required before importing or transferring a file may vary based on the ruleset which has been predetermined. The File Security Screener can be configured to act differently based on source, trust-levels and many other criteria. The scanning solution is hardware protected by Advenica's data diodes.

Secure file import

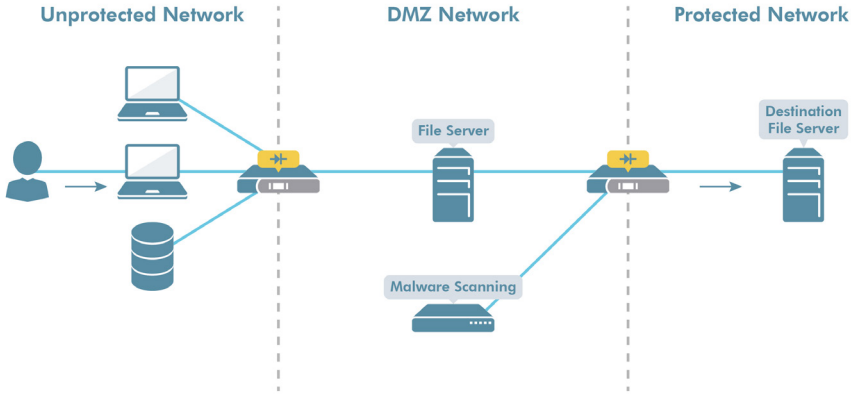
Advenica's Cross Domain Solutions provide efficient and automated counter measures for malware and at the same time assure separation for the connected networks. Advenica's File Security Screener is designed for the national security segment as well as other high security environments like critical infrastructure. The solution provides:

Importing files into secure environments poses a great security threat

- Malware scanning by integrating third-party solutions such as OPSWAT MetaDefender Core and sandboxing environments.
- High assurance protection from information leaks by using data diodes.
- High assurance separation between different import sources using data diodes.
- Caching of data to be scanned, allowing service on the central equipment without data loss.
- Customisable import rules based on the source of the information/file type.
- Scalable solution with ability to increase the number of connected source networks or increase throughput.

Third party scanning functions can be e.g. multi antivirus engines, mathematical/ statistical functions, custom sandboxes or CDR engines (Content Disarm and Reconstruction). In the normal setup of the solution, antivirus scanning is handled by third party software (OPSWAT MetaDefender Core).

File Security Screener,
a unique solution of combining Data Diodes and File Sanitization

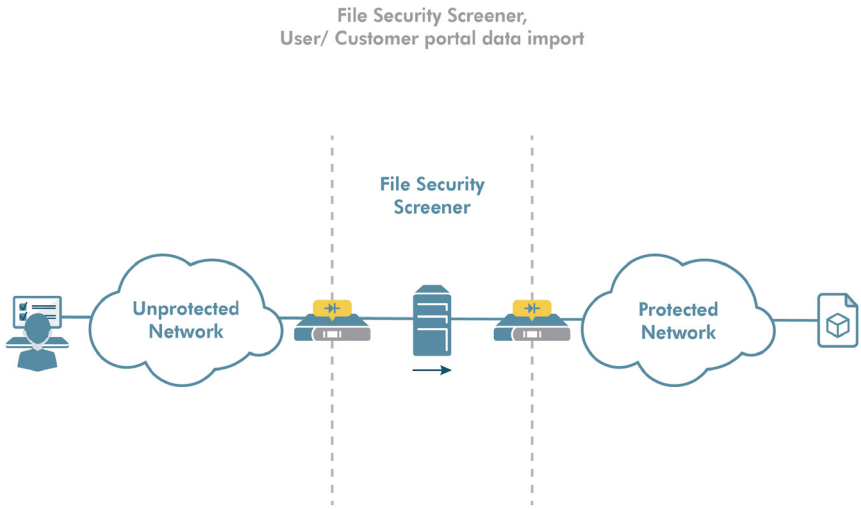


Use cases

Here are a number of use cases on secure procedures for importing data:

1# User portal data import

Portals are often used both for external and internal sharing and collecting of various types of information. Such portals are natural hubs between potentially large numbers of different parties and therefore present an effective attack vector for spreading malicious content, intentionally or unintentionally.



Self-service portals have come to be the de-facto solution as a customer service interface. This leaves trivial tasks such as handing digital documents from the organisation to the self-service portals. In return, freeing up the organisations resources for better use.

Yet these documents need to be trustworthy in order to securely process them further, or even open such documents in a trusted domain computer, without the risk of malware infection.

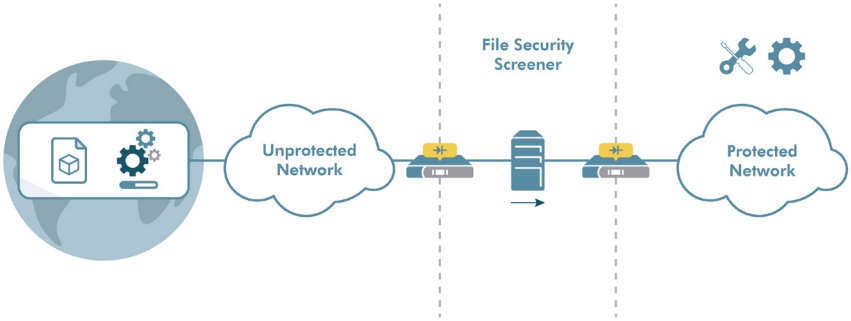
The FSS solution can be integrated into almost any self-service portal solution by its many interfaces. You can keep your existing customer interfacing portal and integrate it to the FSS solution which fetches the documents securely, analyses, scans and sanitises them. They are then transferred to production environments where the documents can be used with high confidence that no harmful or malicious events occur. The FSS customer portal offers:

- Integration to existing customer portal solutions
- SFTP, NFS, SMB, HTTP interfaces for integration
- Automated dataflow from ingress to egress
- Scanning, analysis, and sanitisation of incoming data
- Centralised solution that can serve multiple sources and destinations
- Reporting, alerting and analysis of the processed data

2# Importing SW updates to a secure production environment

A great way to decrease vulnerabilies of a computer environment is to keep all software up to date. As different threats to IT environments evolve, so do SW vendors' efforts to counter these threats and plug any known vulnerabilities in the system. There are also examples of SW update packages being used as the delivery mechanism for malware. Importing SW updates to your IT environment should thus always be done with due diligence, taking precautions for attacks.

File Security Screener,
Importing SW updates to a secure production environment



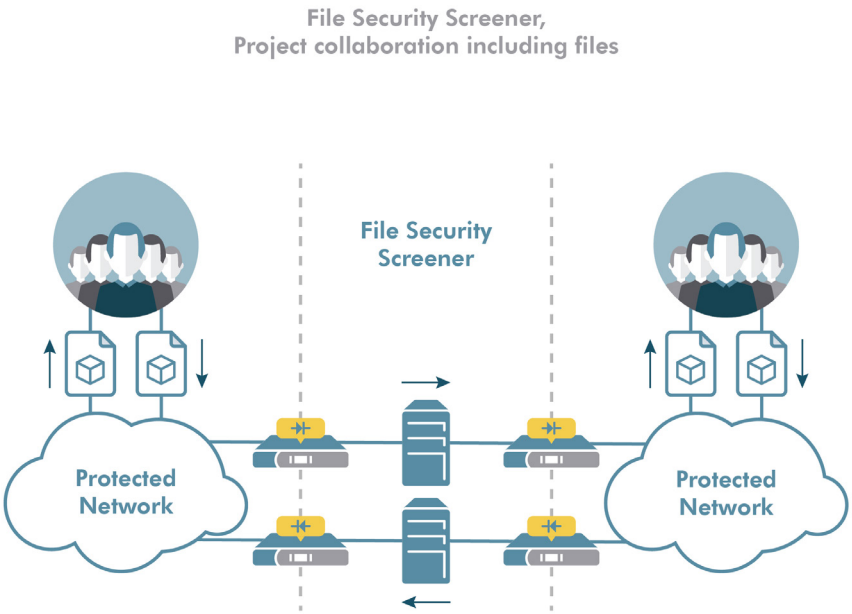
An effective way of ensuring safe SW update imports is to run the entire package through a scanning and sanitation system, such as the FSS. In this use case, software updates can be securely imported to the secured network, along with other files, such as virus definitions etc. Before import, all files are scanned for malware and other threats including steganography, which are actively removed using the OPSWAT MetaDefender Core and its CDR functionality. The FSS offers a vulnerability scanning to detect outdated and vulnerable dependencies in software updates that are scanned. You can mitigate known vulnerabilities even before those are installed into your production. The FSS system supports:

- Secure verified updates to your trusted production environment
- Automated workflow for bringing in update from several sources
- Reporting and analysis of the software updates and found threats
- Increased zero-day threat detection with delayed scanning procedure
- Large files, up to 100GB
- File transfer capacity: 300Mbps (scale up is possible)
- Quarantine and archive of files are supported
- Log and monitoring through Syslog and SNMP
- External heartbeat from source networks to protected network supported

Although SW update packages can be large in size and compressed inside multiple layers, the FSS is able to open all layers for thorough scanning. The process of fetching SW updates can also be automated. The uplink data diode can be assigned to regularly scan for available updates at predefined sites and download them for scanning without manual triggering.

3# Importing project and coordination data

Sharing and distributing sensitive or confidential information between parties in joint projects or otherwise coordinated efforts is vital for the success and timely completion of any larger undertaking. Just as in other use cases, sharing data always poses a risk, even when there is a good level of trust between the different parties. Also, when more than one organisation attempts to protect confidential shared information, the protection level is only as strong as the weakest one in the group.



Regardless of what type of information needs to be brought in from collaboration partners, vendors, consultants or customers, it can all be imported using either an automated or a manual approach or a combination of the two. In the automated setup, data assigned to be shared by outside organisations is stored in an agreed location which the FSS will automatically scan for new content, retrieve all new data and after scanning and sanitation, move it to the assigned destination. Even email traffic related to a project can be routed through the FSS and rendered safe before use. The FSS system supports:

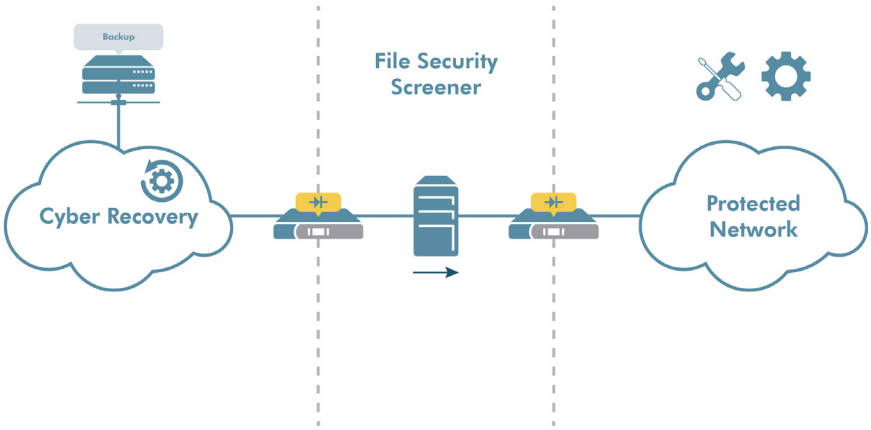
- Large files, up to 100GB
- File transfer capacity: 300Mbps (scale up is possible)
- Quarantine and archive of files are supported
- Log and monitoring through Syslog and SNMP
- External heartbeat from source networks to protected network supported

The FSS can also be used for sending back information to relevant parties if so desired, to ensure a true end-to-end safe chin of communications.

4# Cyber recovery/recovering production environments

In the case of a need to restore a production IT environment from either a standard backup domain or an air-gapped cyber recovery environment, it is vital to make sure no malicious code is moved back into the production system to cause a recurring crash of production servers. In practise, there are numerous examples of this happening and the only way to eliminate the risk is to scan and sanitise everything before restoring it to production for continuing business operations.

File Security Screener,
Cyber recovery/ Recovering production environments



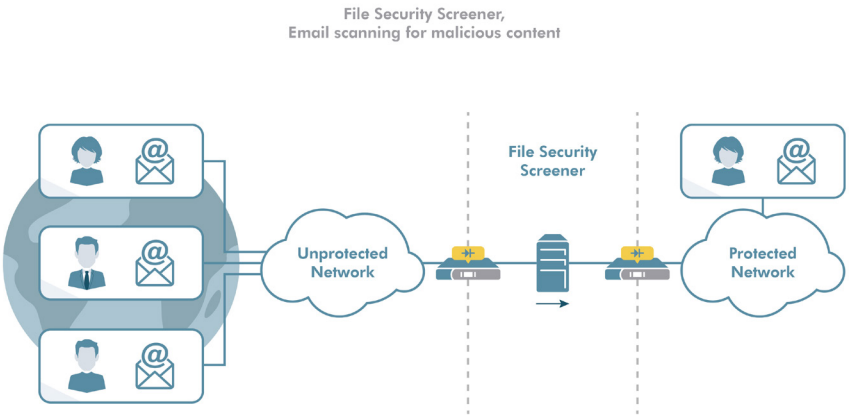
Even though a well protected cyber recovery environment with an operational air gap, data isolation and immutability significantly improves the ability to restore a failed production system, there is always the risk of malware or ransomware having made its way into the data that is being restored. In case of a major failure that requires cyber recovery, the relatively small delay caused by scanning and sanitising the restored information is insignificant compared to the benefits of added security and real added business resilience.

The FSS system supports:

- File transfer capacity: 300Mbps (scale up is possible)
- Quarantine and archive of files are supported
- Log and monitoring through Syslog and SNMP
- External heartbeat from source networks to protected network supported

5# Email scanning for malicious content

Today, email is probably the most common channel for initiating attacks towards an organisation. The File Security Screener can be set up to scan email headers, message content and attachments. Combined with Advenica's ZoneGuard, an Information Exchange Gateway, a host of additional rulesets can be applied based on a number of different allowlisting and/or blocklisting options.



Untrusted email attachments pose a significant threat to organisations. Whether the attachment is sent in a malicious phishing email or someone sends an infected attachment unknowingly, opening and running such a file in a trusted production computer can end up compromising the whole environment.

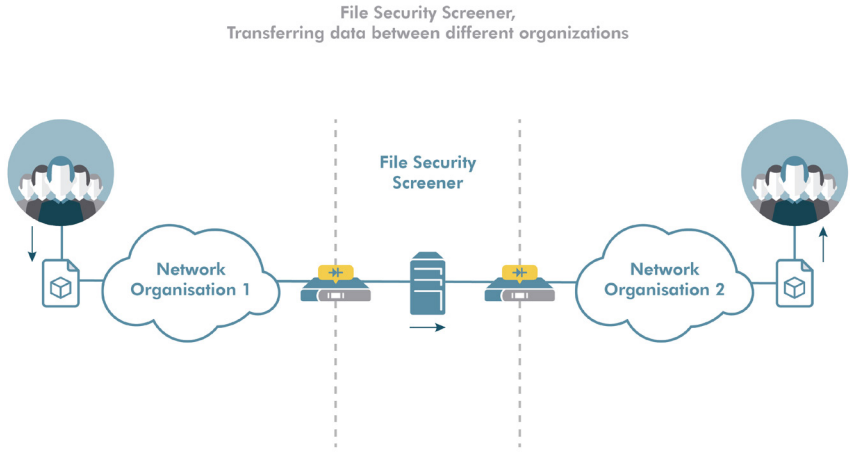
The FSS solution can handle email attachments by directing emails that contain attachments to the FSS pipeline. This ensures that these are scanned, analysed, and cleaned properly before sent onwards to trusted environments for use.

Advenica's data diodes and ZoneGuard can handle and transport incoming emails securely to the restricted DMZ for thorough inspection. Once the attachment has passed the inspection scans, it will be sent to the production environment, cleaned and safe to handle. All this can be automated to fit an organisation's email dataflow, so no manual user interaction is required. Email scanning offers:

- Integration to existing email flow
- Processing of email attachments by up to 32 anti-virus, CDR and DLP engines
- Metadata cleaning of incoming emails
- Automated dataflow from incoming emails to cleaned attachments
- Centralised solution that scales well
- Reporting, alerting and analysis of the processed data
- Integration by SMTP, SFTP, SMB or NFS protocols

6# Transferring data between different organisations

Both private and public organisations have increasing needs to share information and transfer information. This can be between government authorities, private entities and government bodies, corporate global head quarters and their regional offices etc. Even when a significant level of trust exists between the parties, it still is important to take all possible precautions to avoid exposing vital IT environments and confidential information to any kind of theft or malicious attack. Using the FSS scanning and sanitation features, bringing in data even through the open internet keeps the protected environments safe.



Sharing data can be accomplished in various ways, like using specific folders as “mailboxes” out of which files will be automatically fetched, scanned and passed on to predetermined destinations. Depending on the rulesets in the FSS Core, infected files can be quarantined for later analysis or cleaned and delivered. Should malware or vulnerabilities be detected, and the suspect file quarantined, the recipient will receive a 0 (zero) bit file with the original filename to indicate that a transfer was attempted but the file was contaminated and therefore detained within the system. All events can be viewed and analysed at a later time. The FSS system supports:

- Large files, up to 100GB
- File transfer capacity: 300Mbps (scale up is possible)
- Quarantine and archive of files are supported
- Log and monitoring through Syslog and SNMP
- External heartbeat from source networks to protected network supported

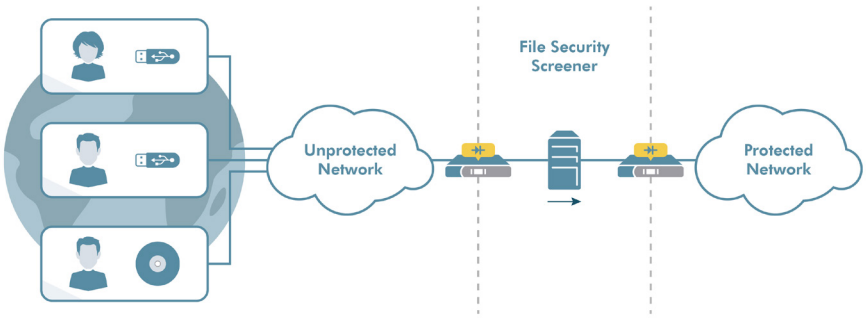
7# Importing data in various formats using the Kiosk solution

As part of the FSS solution, Advenica has developed an additional automated way to import non-trusted files from various storage medias such as USB and CD/DVD, securely and in a controlled manner to an organisation's network environment.

Organisations, private or public, that have a need to import data in different formats from geographically wide areas in a secure and standardised manner, can use this centralised and scalable FSS/Kiosk solution to guarantee malware-free data flows. After importing data from CD's, DVD's or USB sticks, all data is inspected, cleaned and forwarded based on rules set by the organisation. The transfer and cleaning process is automated so that the user only needs to follow a few very simple instructions on the screen. No in-depth training is required.

The KIOSK is widely configurable for end users. The KIOSK appears to the user as a simple device to which storage media can be fed and files are transferred to the secure network/domain. The KIOSK user interface is configurable with AD authentication and user rights capping for managed data transfer.

File Security Screener,
Importing data in varying formats using the Kiosk solution



The FSS Kiosk solution supports:

- AD Integration
- Scalable amount of KIOSK devices and Destinations
- Support for large files up to 100 GB
- Logging and monitoring Possible (Syslog and SNMP)
- High availability configuration when needed
- Supports removeable media such as USB sticks or CD/DVDs
- Encrypted SFTP connection

Advenica provides expertise and world-class high assurance cybersecurity solutions for critical data in motion up to Top Secret classification. We enable countries, authorities and companies to raise information security and digitalise responsibly. Founded in 1993, we are EU approved to the highest level of security. Our unique products are designed, developed and manufactured in Sweden.

Read more at advenica.com

advenica

ISO 9001 CERTIFIED
ISO 14001 CERTIFIED