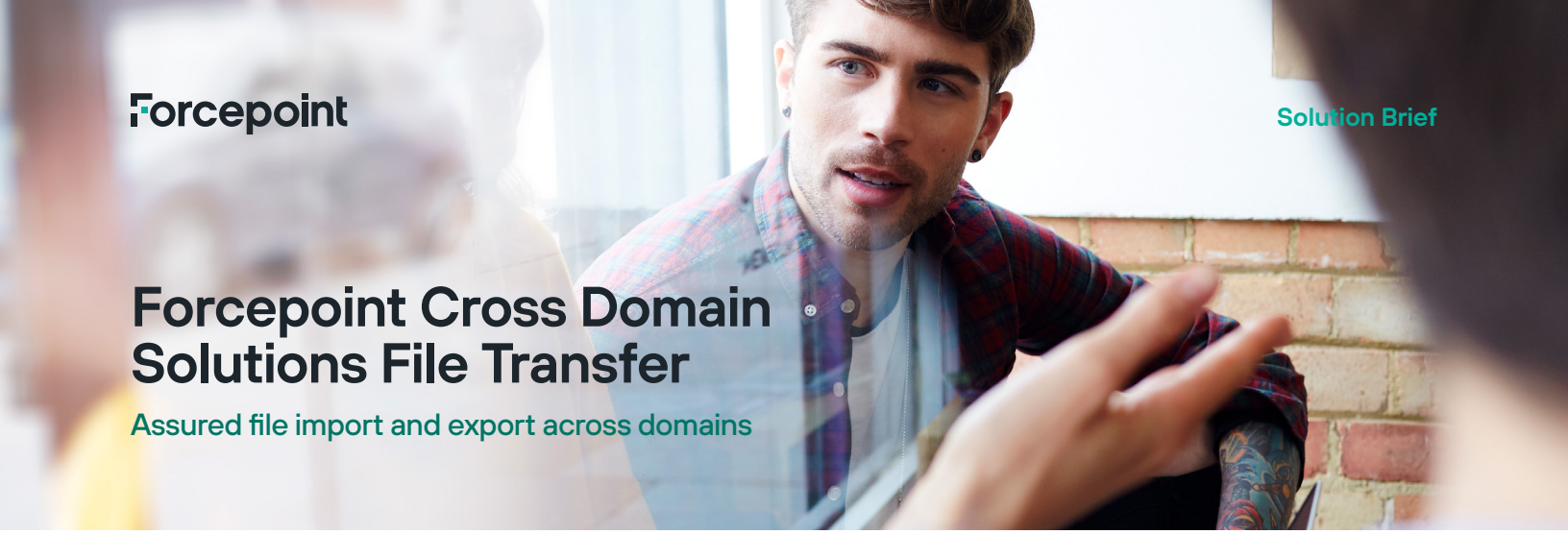


Forcepoint

Solution Brief

Forcepoint Cross Domain Solutions File Transfer

Assured file import and export across domains

Key Advantages

- High-assurance cross domain solution for file transfer between networks
- Transformation that removes known and zero-day malware threats
- Policy enforcement that prevents data breaches
- Modular approach using COTS products for a low-risk, low-cost cross domain solution
- Simple-to-use applications for manual and automated file transfer
- Proven technology being deployed and accredited for use between the internet and classified networks

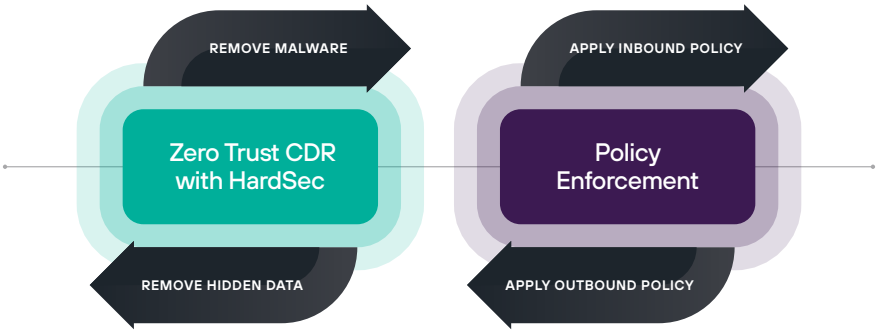
Organizations running segregated networks have a need to move files into and out of those networks. Files may have to be transferred automatically as part of a workflow or manually by authorized users. However, bringing files into a network risks the import of malware. Unfortunately, traditional security controls tasked with preventing such malware. Such as anti-virus and sandboxing can no longer be relied on to ensure that content is safe to import.

Exporting files out of a network risks leaking sensitive information. Commercial Data Leakage tools are limited in their ability to search deep inside complex content to apply policy.

Three Forcepoint technologies combine to provide secure file transfer:

- Zero Trust Content Disarm and Reconstruction (CDR)
- HardSec—iX Appliance
- Policy Enforcement

These three technologies provide a high-assurance cross domain solution to remove malware and to stop data breaches by removing hidden content and applying policy based on the data transferred.



Zero Trust CDR

Zero Trust CDR is an innovative solution to the malware problem. Data can contain hidden malware that is capable of avoiding traditional detection-based security techniques such as anti-virus scanning and sandboxing. Zero Trust CDR is a zero-trust process which completely removes the threat of malware in content by using a technique called transformation. Transformation involves passing only the business information to the destination, not the data carrying it. Transformation works by first extracting the information into simple data structures, verifying the structures are as expected before building the information back into brand new data to deliver.

For Cross Domain File Transfers, Zero Trust CDR is provided by the Forcepoint Information eXchange (iX) appliance.

HardSec—Forcepoint's iX appliance

The verification phase of transformation in Zero Trust CDR can be delivered using a hardware-only device. This sits in the middle of the iX Appliance to verify the data as it passes through. Since the data is in simple data structures, the verification can be done in the hardware using field-programmable gate array (FPGA) chips. The hardware device provides both an independent verification of the transformation process and a hardware assured separation between a trusted and untrusted network.

Hardware enforced verification is provided by the Forcepoint High Speed Guard.

Policy Enforcement

Policy enforcement is a Forcepoint solution to help prevent data leakage and to avoid the import of unsuitable content. Complex data can contain information that should not be brought in or released out of a network. Policy enforcement uses deep content inspection to look inside complex content and applies policy based on the configured rules. All content, including nested data, is inspected and passed to the rules for evaluation. Content that does not pass the policy can be blocked or removed and administrators notified with the iX appliance (Zero Trust CDR) and High Speed Guard (HardSec).

Secure File Import

When importing files, the Forcepoint iX Appliance removes any threat of malware from the files. When deployed with the Forcepoint High Speed Verifier, a high-assurance cross domain solution can be built providing protocol breaks, flow control, transformation, and verification.

The addition of Forcepoint's Data Loss Prevention (DLP) security solution enables policy to be applied based on the inbound content. DLP can apply policy based on the file type, the source and the destination as well as metadata such as protective markings and keywords and phrases in the files to ensure that the file is appropriate to import.

When exporting files, DLP applies policy based on the outbound content, and can apply policy based on the full file content including any embedded data. Rules can be built to apply policy based on protective markings, document meta data, file type, source and destination, and keywords and phrases in the files. Protective markings such as security labels can be found and verified in multiple locations within files, using multiple different formats including those added by popular document labelling tools.

A Forcepoint iX Appliance removes any data hidden in redundant areas of the files. This ensures that data not visible to a manual review does not leak from the protected network.

Deployment of the Forcepoint iX appliance and High Speed Guard ensures a high-assurance cross domain solution with the key controls protected by the hardware enforced device implementing protocol breaks, flow control, sanitisation, authorized release, release control, and an external proxying.

The Forcepoint solution supports the transfer of files using either HTTP(S) or FFSP, the latter being a Forcepoint file sharing protocol that is optimised for transferring files across a network.

Applications that support either of these protocols can be used to transfer files across the secure file transfer solution. Forcepoint provide the following applications which are designed to work wwith the iX appliance (Zero Trust CDR) and High Speed Guard (HardSec):

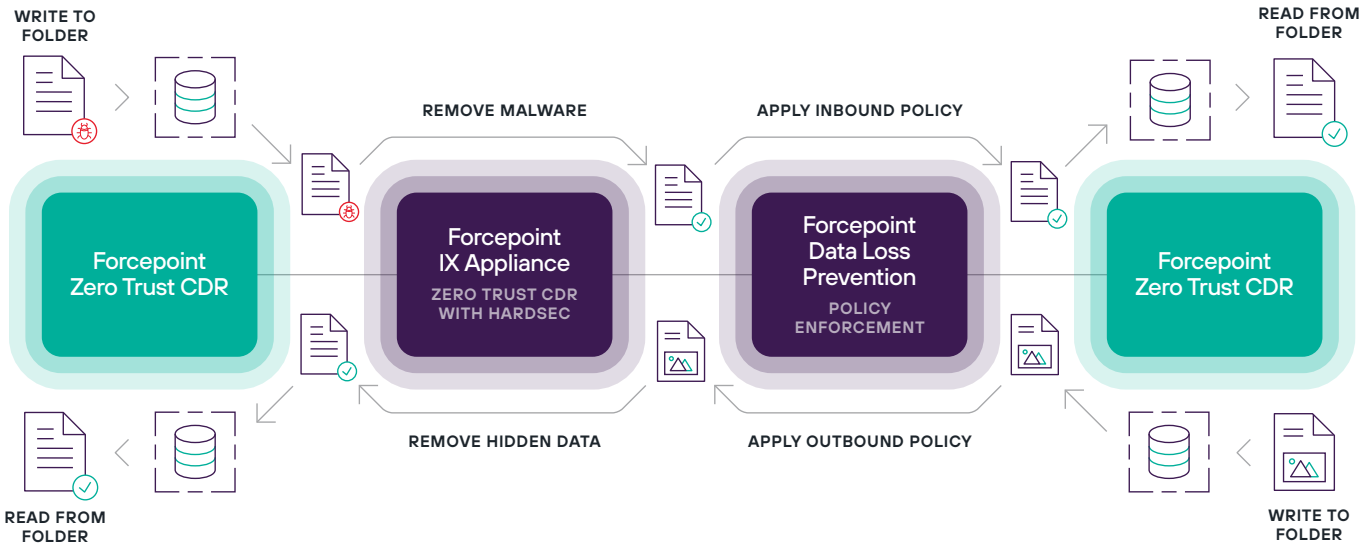
- File Mover
- Personal Exchange

These applications are designed to meet the following use cases:

- Automated File Transfer
- Manual File Transfer
- Isolated Browsing File Transfer

Automated File Transfer

Applications that need to move files across domains from one file store to another can use the Forcepoint File Mover File Utility software. This runs as a service in each network. Applications can write files to a folder and the service will move them across the domain boundary to the destination.



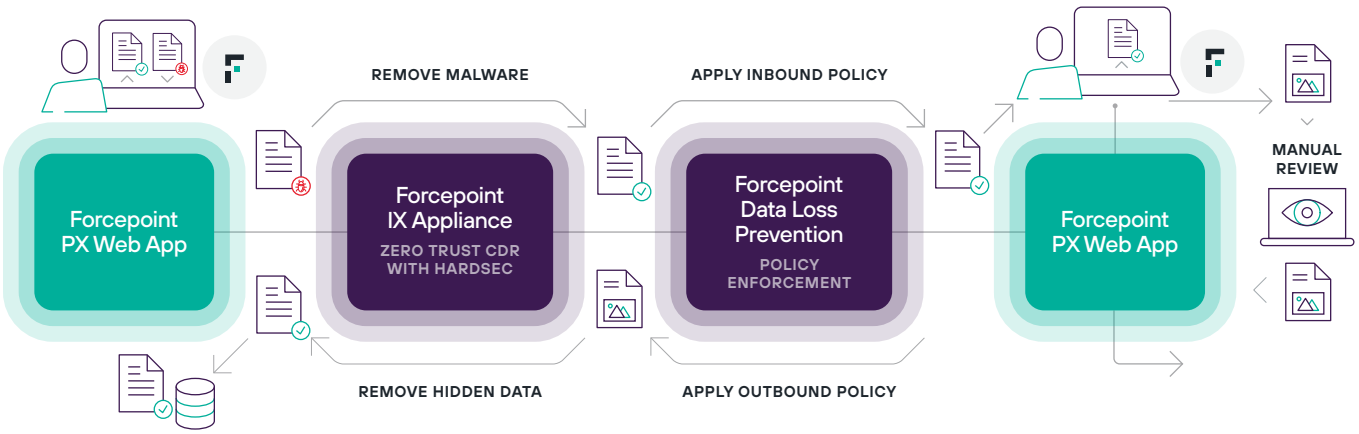
On the source side, the service monitors ones or more file folders and when new files appear, they are automatically transferred across the cross domain solution. If a file cannot be transferred, it is left in the source location, if it is transferred successfully, it is deleted from the source location. The service on the remote side receives files from the gateway and writes them to the configured folder.

Manual File Transfer

Users with accounts in two different networks can move files from their desktop in one domain to their desktop in the other domain using the Forcepoint Personal Exchange (PX) application. PX is a web application that supports user authentication using username and password or single sign-on with Microsoft Active Directory.

Files are selected or drag and dropped into the web app on the source side. The app automatically transfers the files across the cross domain interconnection to the web app on the destination side, from which the user collects them.

A workflow can be created to send files for manual review by a group of reviewers. The manual review process involves downloading the file for inspection before approval or rejection of the file. The user is notified of the review progress via browser notifications and optionally via email.

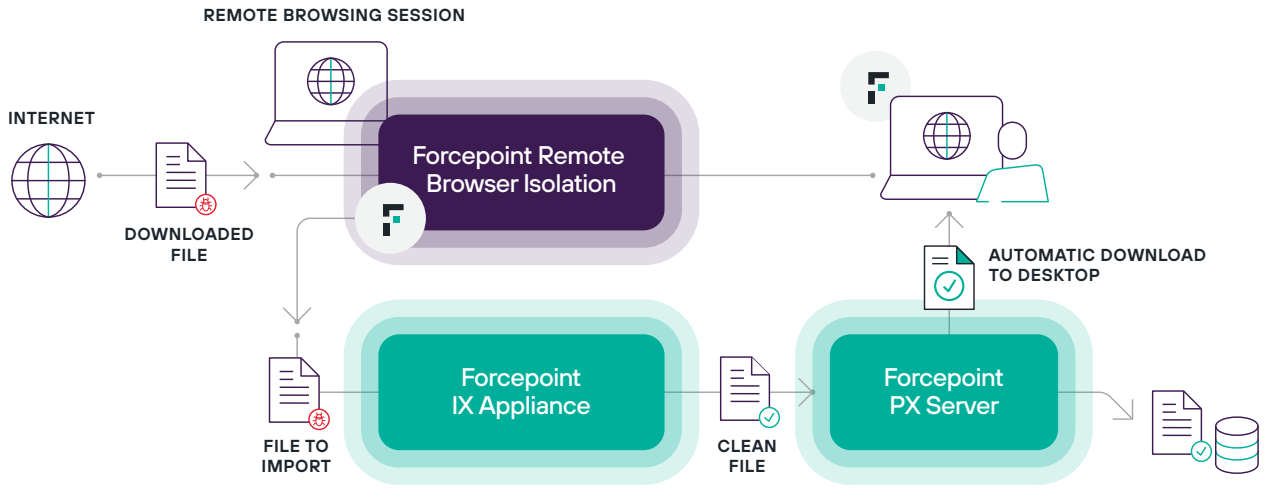


Additional checks can be made on the files by calling out to a checking service. The label checking service assesses Office documents against a set of allowed security markings to determine if the document can be transferred.

All files transferred are audited with a hash of the file and the identity of the user. There is also an option to send a copy of each file to a journal server.

Isolated Browser File Transfer

Users of an Isolated Web Browsing solution can use the Forcepoint PX application to import files that have been downloaded to the isolated web browsing environment. An application is installed into the isolated environment, which enables downloaded files to be shared with the local desktop.



Files are moved across the cross domain interconnection and automatically delivered to the desktop application where they can be saved to the local transfers folder.

Build a Winning Solution

Make sure that everything runs smoothly during and after deployment with Forcepoint Technical Support. Our highly skilled Solutions team have a wealth of expertise and information at their disposal and can be relied upon to act as a natural extension to your in-house team.

Enjoy Unparalleled Protection

We're on the brink of a technological revolution. In the face of relentless and concerted cyber attacks, organizations are being forced to re-evaluate every aspect of how they acquire, share and transact digitally.

Defenses based on the detection of known threats are insufficient. Those based on isolation and sandbox detection inhibit the business and leave too much to chance. What is required? Protection rather than detection.

Zero Trust CDR provides unparalleled protection when transferring files. It ensures all business documents and images are threat free. Advance your web browsing and downloading protection with the addition of Forcepoint Remote Browser Isolation (RBI).

Regulatory requirements and the need to ensure sensitive data does not leave a protected network mean comprehensive controls are required when exporting data.

The PX application enables the introduction of a manual review into a workflow and policy enforcement provides fine grained policy control for the export of data. Isolated browsing solutions can be enhanced to allow users to get the files they need to their protected desktop.

Learn More

For more information visit Forcepoint Zero Trust CDR.

forcepoint.com/contact