Cross Domain Solutions
Trusted Gateway System

Secure information sharing between entities
(agencies, countries, networks)

Forcepoint

forcepoint.com

Whitepaper

Fred Eways
Account Executive
Federal Systems Integrators
July 21, 2020

Table of Contents

The Problems We Solve

Multiple networks = Multiple devices

→   Secure, simultaneous access to segmented networks

→   Secure and rapid data and file transfer between segmented networks—machine-to-machine, person-to-person

→   Facilitating the customer's mission while maintaining the highest degree of network and data security

What are Cross Domain Solutions?

Cross Domain Solutions

→   Facilitate secure information sharing between entities (agencies, countries, networks) with different sensitivity levels through a controlled interface

→   Are built on top of a secure, trusted operating system to achieve a high-assurance platform

Cross Domain Solutions were developed to address the usability and hardware duplication challenge that arises from physically separated networks (typically different security or classification levels).

Divided into three buckets—access, transfer, and hybrid—Cross Domain Solutions work to streamline how users work with the data they need to execute their missions—addressing the human point of interaction between people, sensitive data, and security requirements.

→   **Access:** Provides users a path to data on different networks as allowed by policy

→   **Transfer (Guards):** Provides various mechanisms to securely move data between different networks, while mitigating against viruses, malware, and policy violations as allowed by policy

→   **Hybrid:** Solutions that encompass both access and transfer capabilities

The network segmentation – separation concepts are carried through into the product implementation – separating processes, roles, etc.

These solutions provide:

→   **Support for global missions** with seamless and secure data access and data sharing across security domains

→   **Protection of critical data located everywhere**, from on-premises to the cloud

→   **Protection of mission-critical networks and applications** from sophisticated external attackers

Cross Domain Solutions were developed to address the usability and hardware duplication challenge that arises from physically separated networks.

Why Customers Choose Forcepoint Cross Domain

U.S. Government Raise-The-Bar-compliant
› State-of-the-art filter technologies
› TSABI/SABI "in process" to be completed Q4 2018/Q1 2019

Scalable, enterprise-ready solutions that can support two to 100,000 users
› Flexible implementation options to grow with the enterprise
› Supporting various mission-critical use cases and environments

Cost-effective commercial software business model
› Cost savings and efficiencies realized
› Use of commodity hardware

Market leader in Cross Domain
› Deployed and trusted in more than 100,000 desktops across global governments
› Most comprehensive Cross Domain portfolio on the NCDSMO list
› More than 15 years of experience in Cross Domain development and deployment

Extensive cybersecurity portfolio and expertise in conjunction with Cross Domain

Cleared Professional Services support

More than 15 years of experience in Cross Domain development and deployment.

Cross Domain Product Portfolio

Each of these products are optimized to meet our customers' needs for Cross Domain data transfer and access. They can be deployed individually or collectively as enterprise solutions.

This collection of best-in-class capabilities and products is unmatched in the cybersecurity marketplace. Combining these products provides a very comprehensive architecture.

Trusted Thin Client - Access
Multi-level data and cloud access via a single connection: Thin Client, Virtual Access or Remote Access (ITAR)

High Speed Guard/SP - Transfer
Automated, high-performance data transfer supporting full motion audio/video. SP (special purpose) option for austere, tactical, and mobile forces environments (ITAR)

Trusted Gateway System - Transfer
Multi-directional workflow-based file transfer (ITAR)

SimShield - Transfer
Bi-directional fixed-format data filtering and disguise (ITAR)

Trusted Print Delivery - Transfer
Secure multi-level printing, adding power to cloud solutions and enabling hardware reduction (ITAR)

Trusted Mail System - Transfer
Exchange emails and attachments securely across different networks (ITAR)

WebShield - Access/Transfer
Secure HTTP traffic monitoring for multi-level network multi-cloud access and data retrieval (ITAR)

Trusted Gateway System

Enables safe and simultaneous multi-directional file movement between physically separated networks of varying security and classification levels

→ Specializes in the quick and secure transfer of unstructured files, such as Microsoft Office and PDF files, facilitating critical information-sharing to the right people at the right time

→ Eliminate sensitive file-sharing inefficiencies during mission-critical activities

→ Meets the current U.S. Government "Raise-The-Bar" guidelines

RAISE-THE-BAR

TSABI/SABI
Since 2011/2018

+ Trusted Gateway System is so much an ingrained part of our day-to-day operations that it's very difficult to imagine supporting our mission without it—there's no practical alternative.

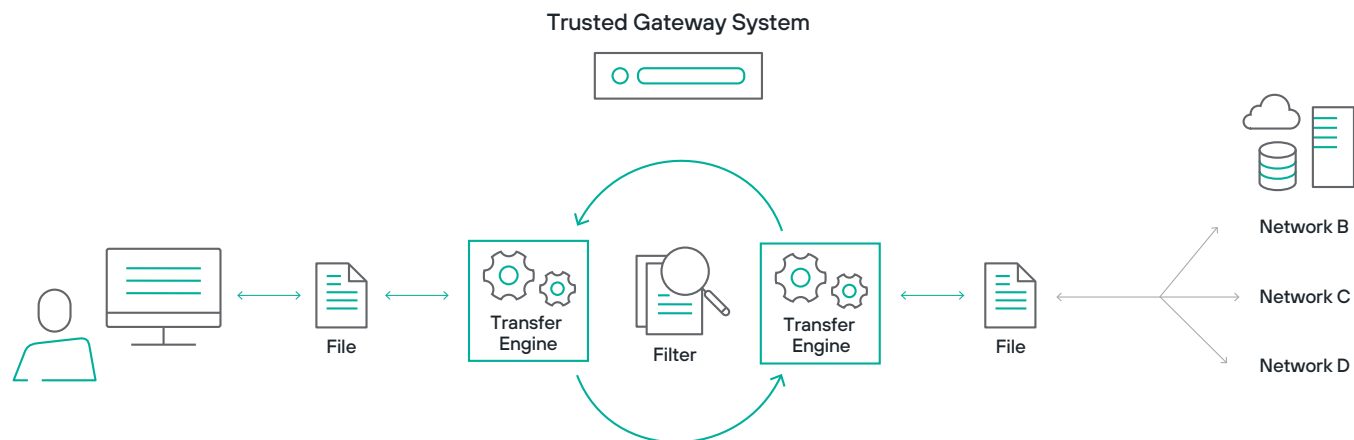THE TOTAL ECONOMIC IMPACT OF A FORCEPOINT CROSS DOMAIN SOLUTION, JUNE 2017

Architecture

Trusted Gateway System

Figure 1. Robust, resilient, and secure architectural design meeting "Raise-The-Bar" requirements

Why Trusted Gateway System

Meeting the need to more efficiently yet securely transfer files within varying classified networks

| Common challenges	Desired state
→ "Sneakernet" → Secure file sharing between international, federal, state is difficult and inefficient with high risk → Risk of network intrusion, file corruption, and data leakage	→ **Eliminate** sensitive file-sharing inefficiencies during mission-critical activitiesSecure file sharing between international, federal, state is difficult and inefficient with high risk → **Quickly and securely** move unstructured files between and within classification levels → **Inspect and sanitize** files with a R.A.I.N.-compliant solution → **Configure** file transfer workflows based on site-specific requirements → **Add** functionality with Forcepoint Trusted Print Delivery and Trusted Mail System

Features Overview

Trusted Gateway System
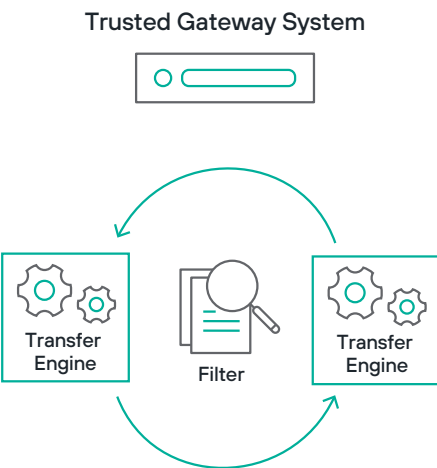
Figure 2. System Features

Features

→ **Operates** on a Red Hat Enterprise Linux 64-bit operating system with Security Enhanced Linux components providing stringent controls

→ **Vast** amount of file types and multiple file sanitization solutions supported (e.g. Glasswall, Purifile)

→ **Automated** bulk uploads via SCP/SFTP (low to high)

→ **Visualization** tool to set/view policy rules, configurations, and administrative status

→ **Robust** archive and audit management capabilities with centralized event logging

→ **Flexible** network configurations to accommodate different environmental requirements

→ **Support** for multi-channel, multi-directional file transfers with one system

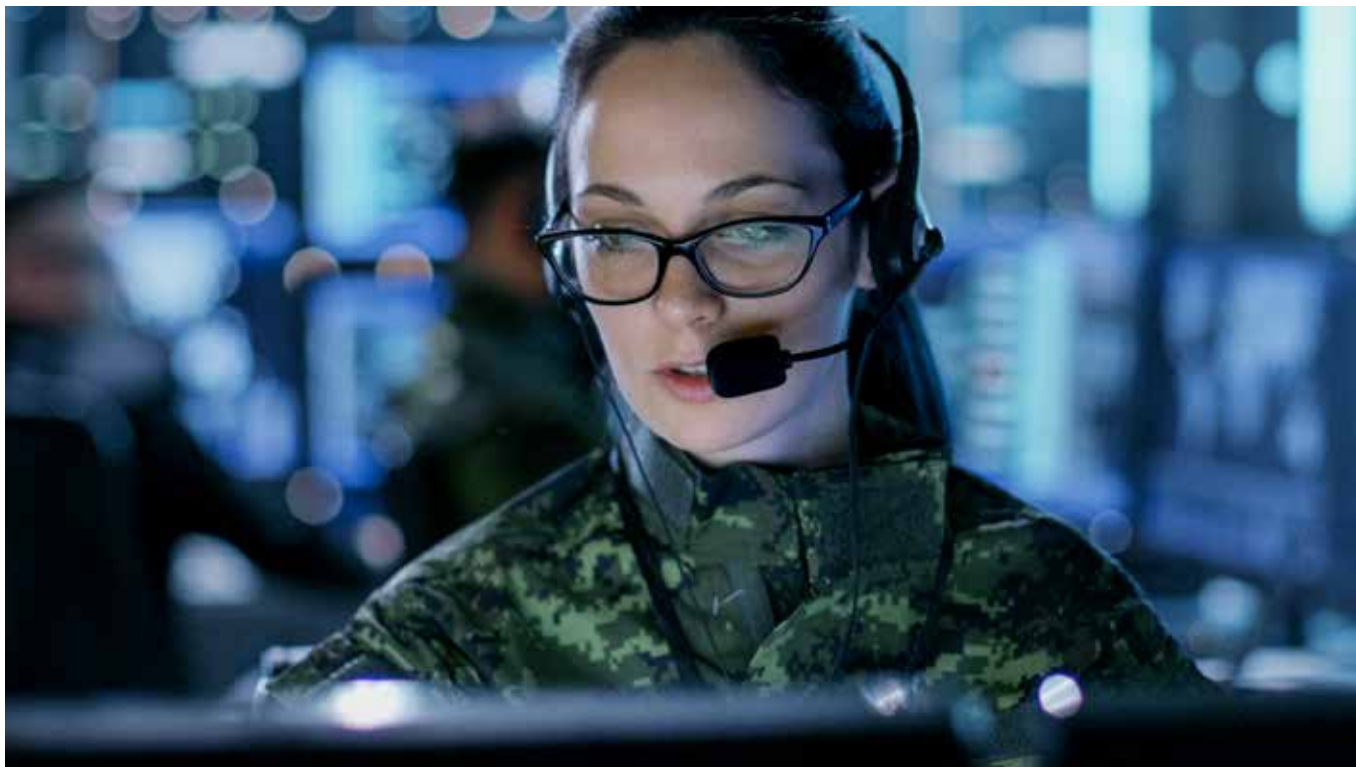→ **Forcepoint High Speed Guard** all version 4 and earlier releases

Configure File Transfers Based on Site Policies

→ **Two-Person Human Review** - a web-based GUI for ensuring two people review documents before release

→ **Template-based Submit** - automatically moves documents between a lower domain and a higher domain

→ **Self-Release** - approved user can create a job and submit to approved destination

→ **Bulk Upload** - ability to transfer large quantities of files from lower to higher-level networks and machine-to-machine

→ **Directory Transfer Service Option (DTSO)** - a secure mechanism provided to transfer directories from a low to a high network

File Inspection and Sanitization Capabilities

FILTER	FILE TYPES SUPPORTED	FILTERING CAPABILITIES
Glasswall	Microsoft Office, PDF	Sanitzes Office and PDF documents. For each document type, the filter creates a new document utilizing the known good content from the input document. The filter is able to extract and import images from documents, allowing embedded images to themselves be filtered (i.e. transformed). The filter also provides the export of a textual version of the document facilitating a dirty word search.
PuriFile	Microsoft Office, PDF	Provides document inspection and sanitization and eases the document workflow process for Office and PDF documents.
Aware	Bmp, png, jpg, j2k, tiff	Supports the conversion of images from one format to another and supports the stripping (reset to zero) of the least significant bit of pixel-based images. Allows support of jpeg2000 (j2k).
ImageMagick	Bmp, png, jpg, gif, tiff	Supports the conversion of images from one format to another and the stripping (reset to zero) of the least significant bit of pixel-based images.
McAfee	All	Scans all file formats for the presence of virus signatures matching those in a stored virus definition list provided by McAfee.
Sophos	All	Scans all file formats for the presence of virus signatures matching those in a stored definition list provided by Sophos.
XML2	XML	XML schema validations using a set of stored schema definition (XSD) files on the guard.
Xerces	XML	XML schema validations using a set of stored schema definition (XSD) files on the guard.
Archive	Zip, tar, iso, gzip, cpio, bzip2	Supports the extraction of artifacts within archives.
PDF Transform	PDF	Cleanses PDF files through a format conversion process.
Dirty Word Search	All	Text search filter used for locating dirty words within any type of file. The filter supports simple text searching as well as regular expressions.
XSLT	XML	XML Stylesheet Language Transformation of XML files. Can perform validation and/or transformation of XML content based on an XML-formatted stylesheet (prepared off-box). This filter enables support of Schematron-generated XSL stylesheets.
File Extension	All	Allows or blocks files based on the extension found in the file name.
File Size	All	Allows or blocks files based on file size.

Summary

Forcepoint provides the most comprehensive and widely used collection of multi-level access and Cross Domain transfer products available today. Forcepoint's Cross Domain solutions are proven for secure access and transfer of information while proactively protecting government and commercial organizations from compromise. Striking the correct balance between information protection and information sharing—a vital component to national security.

As information systems evolve and become more deeply integrated, Forcepoint continues to be a viable partner in securing our most critical infrastructure and systems. Ensuring the proper steps are taken to enable systems to be more interoperable and connected. Both domestically and internationally where needed. Providing information assurance and resiliency in order to effectively leverage networked environments.

Safeguarding information and critical infrastructure is paramount for mission success. Forcepoint is committed to delivering the proven solutions and capabilities for global information sharing and cybersecurity challenges. This proven and ongoing commitment to the customer mission has helped organizations, government agencies, and nations world-wide to more effectively minimize cyber risk.

One Step Ahead.
One Behavior at a Time.

Move to proactive cybersecurity with a human-centric approach.

Forcepoint

forcepoint.com/contact

About Forcepoint

Forcepoint is the leading user and data protection cybersecurity company, entrusted to safeguard organizations while driving digital transformation and growth. Forcepoint's humanly-attuned solutions adapt in real-time to how people interact with data, providing secure access while enabling employees to create value. Based in Austin, Texas, Forcepoint creates safe, trusted environments for thousands of customers worldwide.