FORTRA™

Five Key Use Cases for Threat Protection

Key Use Cases from Fortra Customers

1. Healthcare
2. Internet Service Provider
3. IBM i Platform
4. Defense
5. Supply Chain

Want to make sure files are free of malware as they are sent or received?

Need to prevent sensitive information from being sent to the wrong recipient?

Take file transfers to the next level with Fortra's SFT Threat Protection. Here are **five ways** our customers are taking advantage of this powerful bundle for more file security.

GoAnywhere®

Managed File Transfer

Clearswift®

Email Security

1 Healthcare

Healthcare

A large North American health and dental insurance company wanted to move away from its previous file transfer solution, Axway (one of several vendors their parent company used). They wanted their own, single system – one that could apply robust automation functionality to file exchanges with their partners, as well as deliver the auditing and reporting needed to meet industry compliance requirements. In addition, they required high availability and clustering to ensure the large volume of files they exchange could be executed even if one server went down or become unavailable.

With the SFT Threat Protection bundle, this healthcare organization can simply **check a box in GoAnywhere to turn on easy anti-virus protection through the Clearswift Secure ICAP Gateway to scan all inbound file transfers.** Then, content like embedded malware, triggered executables, and other undesirable data can be automatically detected and stripped, while allowing non-malicious content to continue – keeping business flowing.

With their deployment to Azure, the GoAnywhere and Clearswift combo offered the automation ease they sought through Automated Workflows as well as encryption, clustering, and flexibility in both pushing and pulling files. They used Fortra's services team to help expedite their file migration transfer process transition.

WHAT THEY NEEDED:

- Automation
- High availability
- Ability to deploy on Azure

SOLUTION:

- Block PII
- Scan all inbound file transfers for malicious content, while allowing safe content to continue
- Automation functionality
- High availability and clustering for push/pull flexibility

2 Internet Service Provider

Internet Service Provider

This satellite communications and internet service provider was already using GoAnywhere’s large library of Cloud Connectors to ensure their secure file exchange process can work smoothly with many cloud applications they already count on, such as SharePoint, Google Cloud Storage, and ServiceNow. Having added the SFT Threat Protection bundle of GoAnywhere MFT and the Clearswift Secure ICAP Gateway, **they are now assured that files pulled from third parties are scanned and cleaned of harmful data,** including hidden meta data or executable triggers.

The company also added the Secure Forms module to make it easier for their customers to complete and submit custom-made forms. Once completed, form data can be executed and processed through Automated Workflows for a more streamlined, secure forms process internally.

WHAT THEY NEEDED:

- **Secure retrieval of files from third parties**
- **Ability to make their own secure forms**
- **Automation**
- **Quick implementation**

SOLUTION:

- **Connect to applications like SharePoint, Google Cloud Storage, and ServiceNow**
- **Scan all inbound file transfers for malicious content, while allowing safe content to continue**
- **Ease form completion, processing, and security**
- **Automatically process files on submission**

3 | IBM i Platform

IBM i Platform

As a large, private, non-profit healthcare organization, satisfying stringent industry compliance requirements for information security was top-of-mind when securing a file transfer solution. They run their system on an IBM i platform and appreciate the **layers of security protection as they continue to add more IBM i products to their tech stack.**

Specifically, GoAnywhere and ICAP help IBM i users to do the following:

- Eliminate scripting or programming of manual file transfer processes with GoAnywhere
- Create, import, and export SSH keys and SSL certificates (without cryptic commands)
- Remove risks of accidental exposure of critical information or receiving hidden threats within documents or images via the Secure ICAP Gateway
- Remove need to create additional IBM i user profiles for trading partners

WHAT THEY NEEDED:

- **Help with compliance**
- **Ability to deploy on the IBM i**

SOLUTION:

- **No more manual processes**
- **SSH key and SSL certificate creation and management**
- **Security of critical information without accidental exposure or hidden threats**
- **No need for additional user profiles for trading partners**

4 Defense

Defense

A large player in the US defense industry needed to receive a daily file that detailed a list of companies not allowed to do business with the country. This XML file had to work with both SFTP and HTTPS servers and, due to the nature of the data contained, be highly secured.

The SFT Threat Protection bundle of GoAnywhere MFT and the Clearswift Secure ICAP Gateway **met the government industry organization's strict need for FIPS 150-2 requirements** and gave them the ability to deploy to Azure Gov Cloud via an inbound SFTP server. As GoAnywhere is listed on the approved, Common Criteria-certified product list for NAIP for government procurements for managed file transfer solutions, it was a top choice for this government vendor.

WHAT THEY NEEDED:

- **Help with government requirements**
- **Robust security**

SOLUTION:

- **Both SFTP and HTTP severs can secure highly sensitive data**
- **Scan all inbound transfers for malicious content, while allowing safe content to continue**

5 Supply Chain

Supply Chain

This supply chain company takes advantage of some of the additional features and modules available from the two solutions in Fortra's SFT Threat Protection bundle – GoAnywhere MFT and Clearswift's Secure ICAP Gateway. They selected the file transfer and threat protection bundle to not only handle their day-to-day secure transfers, but also to ensure they had **the most advanced file scanning and anti-virus features added.**

In addition to secure, managed file transfers, Secure Forms, and a SharePoint Cloud Connector, they added the Optical Character Recognition (OCR) module which can extract text from image files, embedded images, and scans within an electronic document, or a scan of a document for added data security.

WHAT THEY NEEDED:

- **Advanced file scanning and anti-virus**
- **Ability to scan images**

SOLUTION:

- **Control and anti-virus as part of the file transfer process**
- **Scan inbound files for malicious content while allowing safe content to continue**
- **Detect and remove active content within files**
- **Identify sensitive data in images and mask or redact**
- **Process, secure, and streamline forms**
- **Integrate with cloud applications (e.g. SharePoint)**

Summary

Our customers rely on the powerful combination of secure file transfer, threat protection, and DLP this bundle provides. The end result: confidence that files are being sent securely, without the risk of exposing any data that shouldn't be exposed.

Whether you're a long-time GoAnywhere MFT customer looking to take file security to the next level, or simply shopping around for a way to automatically, securely move files and protect them from malware, we hope these use cases gave you inspiration to do the same for your organization.

If you'd like to see this bundle in action, you can **request a live demo** or simply contact us at goanywhere.com.

FORTRA™

About Fortra

Fortra is a cybersecurity company like no other. We're creating a simpler, stronger future for our customers. Our trusted experts and portfolio of integrated, scalable solutions bring balance and control to organizations around the world. We're the positive changemakers and your relentless ally to provide peace of mind through every step of your cybersecurity journey. Learn more at fortra.com.