FORTRA™
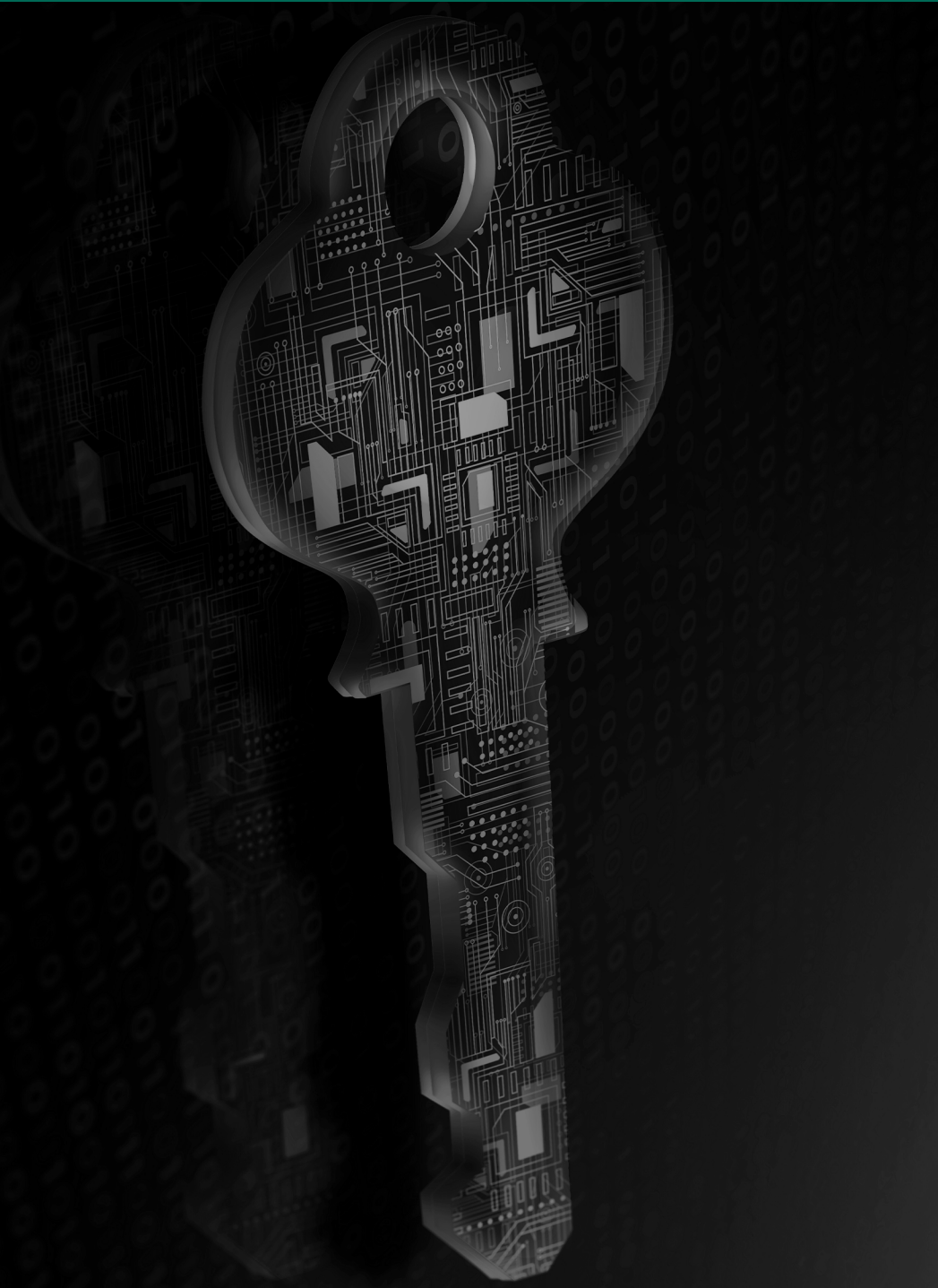
Zero Trust
File Transfer

Zero Trust File Transfer

Zero trust is about more than network segmentation. Fortra can help you encrypt and securely share data with authorized individuals while protecting it from viruses and malware.

Our Zero Trust File Transfer bundle enables automatic file sharing, scanning for malware or viruses, and encryption, giving you total control over files wherever they travel. The result is portable, persistent data security for files of all sizes and sensitivity levels, as well as meaningful progress towards your zero trust goals.

The Problem

For many organizations, security methods like PGP encryption are not enough because once files are downloaded and unencrypted, those files can still be shared with unauthorized recipients. They need a way to apply Zero Trust tenants to their file transfers.

Another common limitation is not being able to send large files securely and efficiently with external parties – a critical situation when trying to share proprietary manufacturing files, media, or sensitive video footage.

In addition, with growing regulatory, state, and government policies around file protection, companies also have to make sure files are protected in line with compliance requirements.
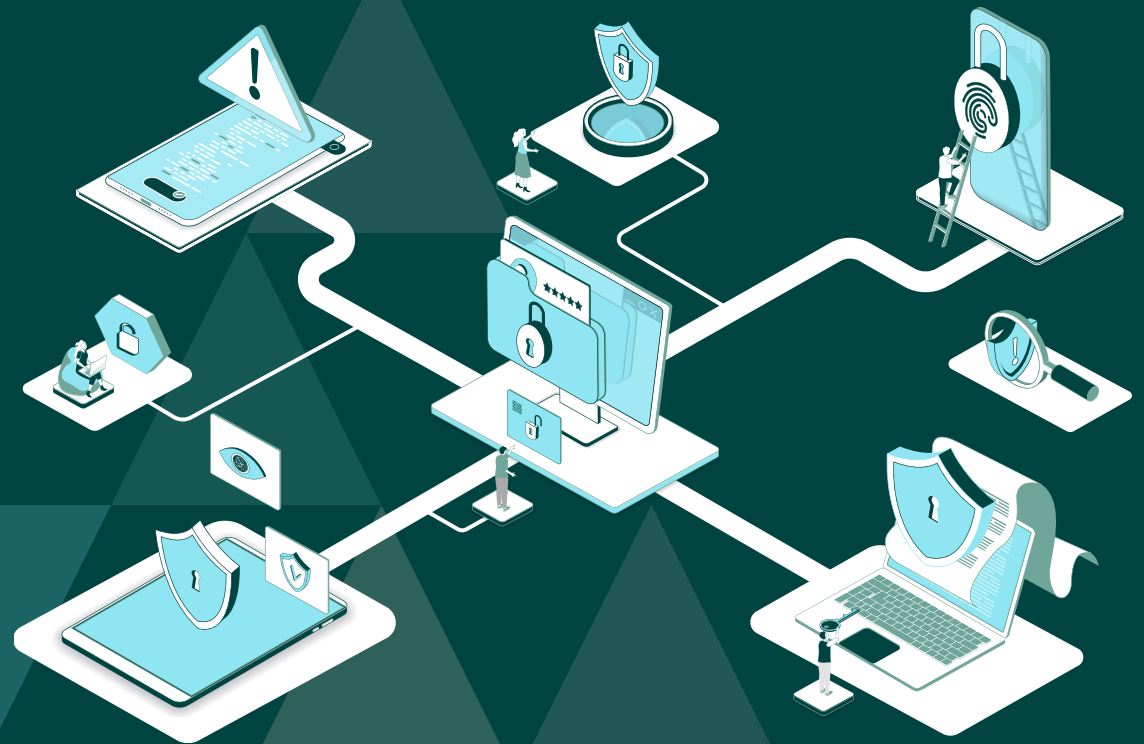
The Solution

Securing documents in transfer and at rest with secure file transfer (SFT) is an important step to protecting the data vital to your organization, trading partners, and customers. In a Zero Trust Security framework, no person or system attempting to access data is automatically trusted.
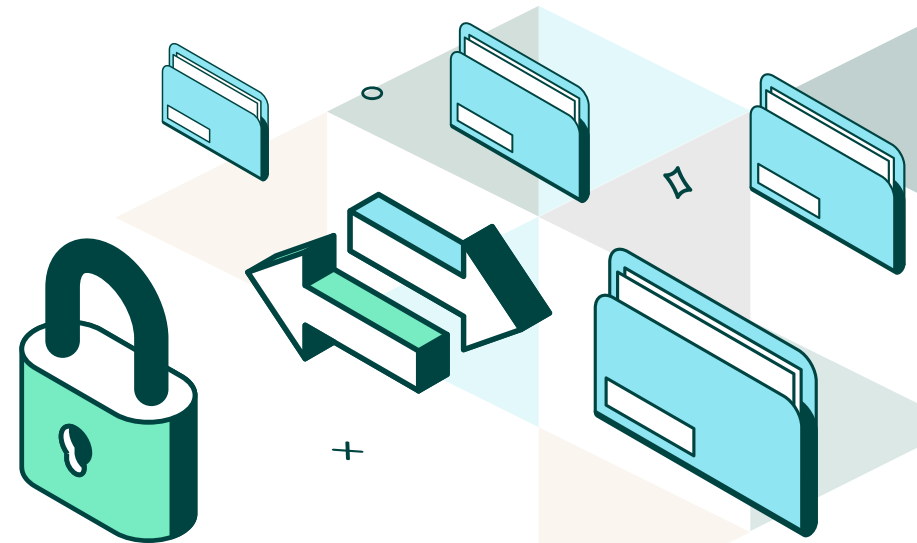
This bundle combines the power of the following Fortra solutions:

▶ Secure File Transfer

▶ Secure ICAP Gateway

▶ Secure Collaboration and File Access Control

▶ Encryption

How It Works

Your team needs to collaborate externally, but sensitive data is involved.

Fortra can help share sensitive data via browser or encrypted email with or managed file transfer solution.

Zero Trust means exactly that-so files can stay protected even offline, controlling who has access and where they can be shared.

Access to Fortra-protected documents can be revoked at any times, even if the user is offline.

Your valuable data remains protected throughout its collaborative orbit.

Common Use Cases

- **Send or receive large files via email with encryption.** Encryption stays with the file even after download and access can be revoked at any time.

- **Add protected files to shared folders.** Wrap them in protection so only authorized users can open and download the file, depending on policies, and once files are downloaded, you still have control.

- **Securely upload files to web forms.** Enable GoAnywhere to apply secure collaboration to each attachment, sending a protected download link to recipients and only allowing authorized individuals to access.

- **Inspect files for threats and sensitive information.** Before files are sent or received, catch and sanitize them for viruses or malware. Remove unwanted metadata or sensitive information before continuing to share the file.
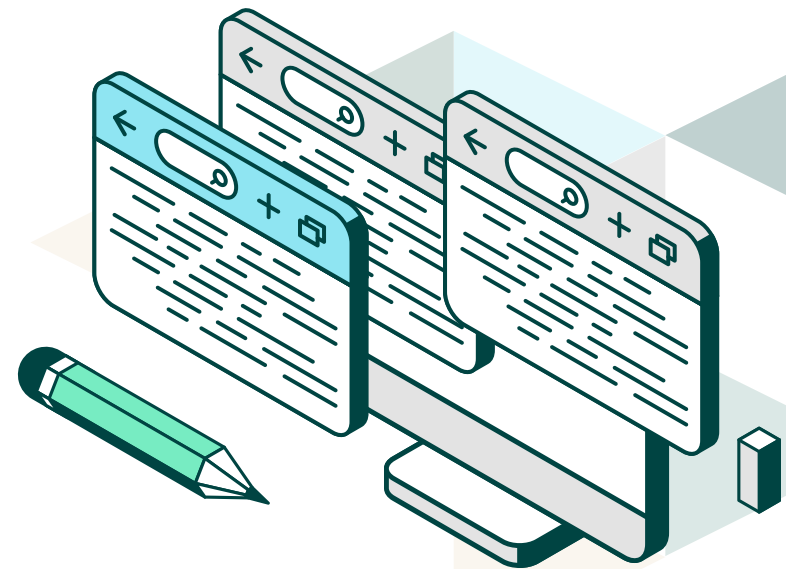
GoAnywhere Customer Requirements

The bundle enhances GoAnywhere SFT's file encrypted for documents supported by our secure collaboration plugin. GoAnywhere customers must own Advanced Workflows and Secure Forms.

Data Residency

Digital Guardian Secure Collaboration data all currently resides in the U.S. If you have additional questions about this, our team would be happy to discuss further with you.

Let Us Help Protect Your Data with Zero Trust File Transfer

Ready to add layers of protection to your data security defense?

REQUEST A DEMO>>

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.