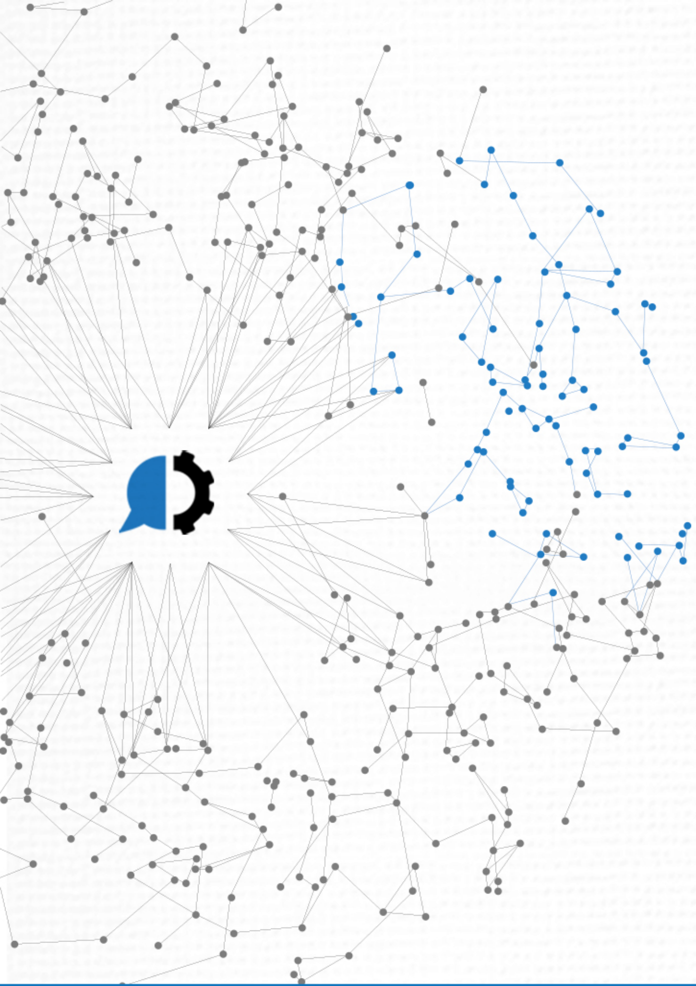


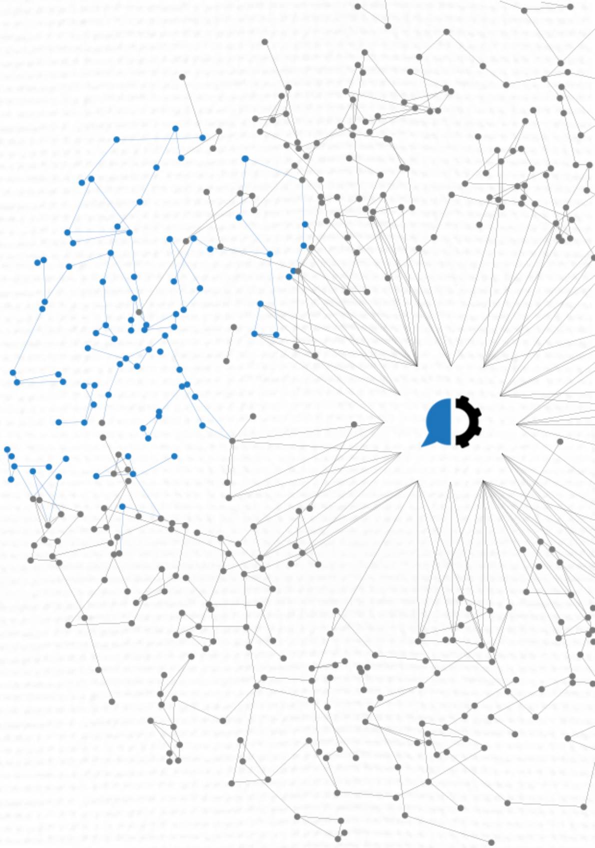
GO ANYWHERE®
Managed File Transfer

Are You Avoiding These Top 10 File Transfer Risks?

www.goanywhere.com

Today’s Agenda

1. Introduction
2. 10 Common File Transfer Risks
3. Brief GoAnywhere MFT Overview
4. Question & Answer



UP NEXT

Today's Presenter

GOANYWHERE® Managed File Transfer

Rick Elliott

Lead Solutions Consultant
HelpSystems

Introduction

GOANYWHERE®
Managed File Transfer

Have you ever caught yourself saying…?

- We don’t have an IT department, so I FTP from my desktop.
- We’re a small/medium sized company – we don’t have to worry about these things.
- We’re a large corporation – I’m pretty sure we have this covered.
- It’s OK, our network administrators will take care of this.
- It’s OK, our system administrators will take care of this.
- We’ve never been hacked!

Some data breach statistics

- According to the Identity Theft Resource Center, there were **1,093 data breaches** in 2016, which was a 40% increase over 2015.
- Worldwide spending on security-related hardware, software, and services rose to **$73.7 billion** in 2016 from $68.2 billion a year earlier.

(Source: Bloomberg Technology)

Still think you aren’t vulnerable?

GO ANYWHERE® Managed File Transfer

- Do you have a password guessing feature on your FTP server? Is it activated?
- Do you force password changes on a regular interval?
- Do you have DOS and Brute-Force features? Are they enabled?
- Do you have Malicious Name features? Are they enabled?
- Is your Anonymous functionality disabled?
- Do you have password intelligence built in?
- Do you utilize 2-Factor Authentication?
- Is your MFT Server “old”?
- Do you use “Freeware”?

The elephant(s) in the room

The elephant(s) in the room

Reports of Tens of Thousands and sometimes Millions of points stolen and used for fraudulent bookings.

The elephant(s) in the room

IHG®
ARMY HOTELS
FEATURING
Holiday Inn Express
STAYBRIDGE SUITES
CANDLEWOOD SUITES

The elephant(s) in the room

1.5 Million records leaked. Official statement from ESEA was that the hacker requested $100,000 ransom.

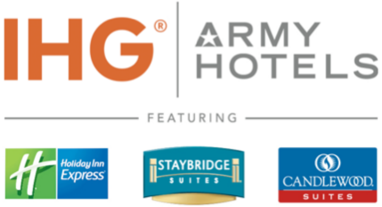
The elephant(s) in the room

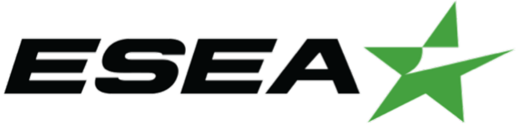
IHG®
ARMY HOTELS
FEATURING
Holiday Inn Express
STAYBRIDGE SUITES
CANDLEWOOD SUITES

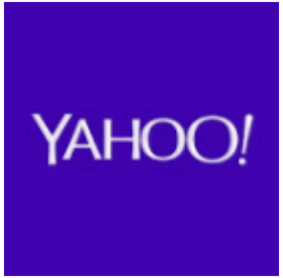
The elephant(s) in the room

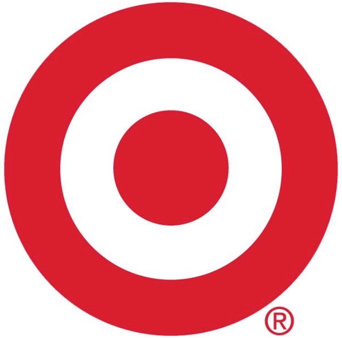
EVERY SINGLE ACCOUNT
WAS HACKED …
3 Billion!

The elephant(s) in the room









The elephant(s) in the room

40 Million Instances of Credit and Debit Card Information were stolen!

The elephant(s) in the room

The elephant(s) in the room

IHG® ARMY HOTELS

FEATURING

Holiday Inn Express STAYBRIDGE SUITES CANDLEWOOD SUITES

ESEA

experian™

143 Million American’s information was exposed!

YAHOO!

The elephant(s) in the room

The elephant(s) in the room

IHG® ARMY HOTELS

FEATURING

Holiday Inn Express

STAYBRIDGE SUITES

CANDLEWOOD SUITES

ESEA

Are you SURE?

YAHOO!

Risk #1:
Giving away user IDs and passwords via FTP transfers

GO ANYWHERE®
Managed File Transfer

Risks:

- FTP isn’t a secure transfer protocol.
- User credentials aren’t encrypted in FTP transfers – they’re sent in the clear.
- This data can be sniffed and stolen during transit.

Solutions:

- Use secure protocols like SFTP, OpenPGP, FTPS, HTTPS/AS2.
- Always ensure user IDs and passwords are encrypted, even at rest!
- Never store your user IDs and passwords on your local computer.
- Always disable the “Anonymous” account!

Risk #2:
Sending unsecured plain text emails

Risks:

- Communicating sensitive data through email.
- Storing email data on Exchange Servers.
- Sending emails to wrong address.

Solutions:

- Utilize a Secure Mail Server.
- Don’t allow sensitive data to be kept in the Exchange Server.
- Take advantage of encrypted file storage retrieval with password access.

Risk #3:
Exposing data to the DMZ (Demilitarized Zone)

GO ANYWHERE® Managed File Transfer

Risks:

- Files are often temporarily stored in the DMZ by trading partners.
- These files are at a higher risk of being accessed by hackers.
- The DMZ is more exposed to the internet.
- Using the DMZ can require the use of manual scripts. This = more vulnerabilities.

Solutions:

- Install a Reverse Proxy Gateway.
- Keep all data inside your private network.
- Only allow access upon user authentication.
- **NEVER** store data on a DMZ Server!

Risk #4:
Having open ports in your network

Risks:

- Inbound firewall rules allow hackers to gain basic system access.
  - This can allow them enough privileges to compromise your systems.
  - This gives access to critical applications & services.
  - This allows potential direct access to your production systems.

Solutions:

- Communicate through a reverse proxy.
- Don’t allow inbound firewall rules from DMZ or Internet.
- Ensure you maintain PC firewalls and security patches.

Risk #5:
Using your own proxy software

Risks:

- Often older technology
- Misleading or incorrect configurations
- Inbound and outbound port configurations required

Solutions:

- Use modernized reverse proxy technology.
- Maintain proxy control within your Private Network, not in the DMZ.
- Don’t have inbound ports into the Private Network.

Risk #6:
Writing and maintaining scripts

GO ANYWHERE®
Managed File Transfer

Risks:

- Manual scripts prone to human error
- Replicated and duplicated scripts
- Time-consuming to track down and fix problems
- No centralized auditing and alerting
- Lack of security mandates and compliance reporting

Solutions:

- Use centralized and generic role-based scripting solutions.
- Receive automated notifications from error handling routines.
- Implement detailed logging and auditing functionality to support compliancy and federal, state, and local mandates.

Risk #7:
Using free, outdated PC applications

GO ANYWHERE® Managed File Transfer

Risks:

- Dedicated personnel is needed for administration.
- There’s assumption of mandate and compliancy regulation reporting.
- They’re dependent on community advice and reporting for issues, bugs, and updates.

Solutions:

- Use certified security software with administration, training, and education.
- These solutions are trusted, with certified compliancy and mandate reporting.
- They are regularly updated and include feature rich product enhancements.

helpsystems

Risk #8:
Not having proper key and certificate management

GO ANYWHERE® Managed File Transfer

Risks:

- This opens the door to your system for anyone to get access.
- Stolen userID’s and passwords can be utilized by anyone.
- Access to certificate or key authentication is compromised.
- Command line access to key management = vulnerable.

Solutions:

- Install a secured, encrypted key management system.
- Implement role-based and logged access to key or certificate updates.
- Use centralized access for all communication key and certificates.

Risk #9:
Lacking internal security controls

GO ANYWHERE® Managed File Transfer

Risks:

- Internal security controls are often overlooked.
- These include:
  - Customer sign-ons
  - Allowed IP addresses
  - Automatic IP blacklists
  - Unblocked brute-force attacks

Solution:

- Get granular with your cybersecurity.
- Build a secure infrastructure that allows communication with controlled access.

Risk #10:
Not securing your system with the right permissions

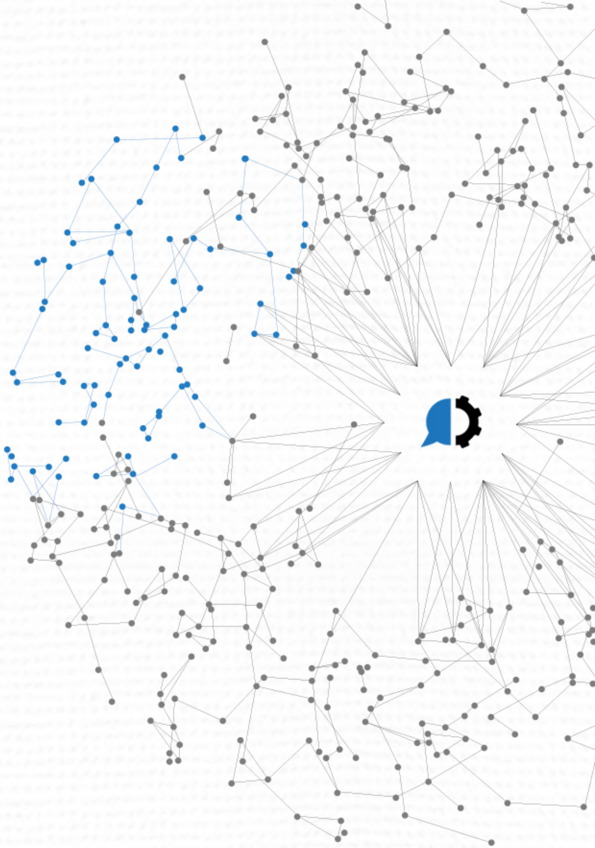
Risks:

- Did you see what we've been talking about?
- Bueller? Bueller?? **Anyone???**
- YOU ARE VULNERABLE IF YOU USE FTP!

Solution:

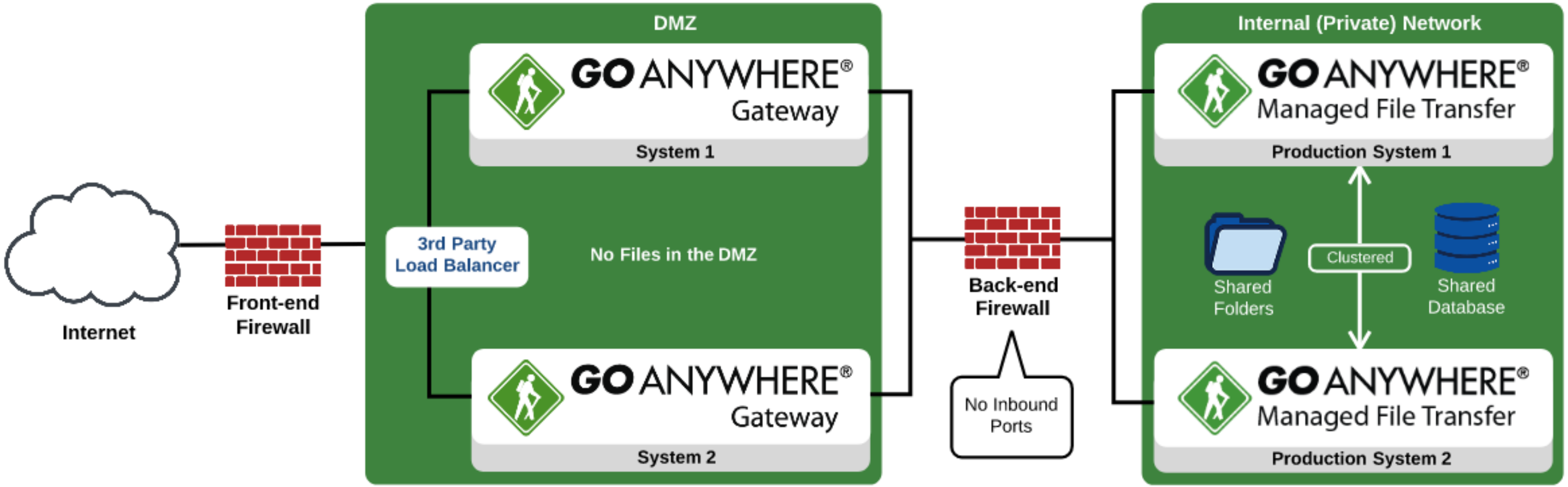
- Just say no!
- Disable FTP!
- Use SFTP or FTPS or HTTPS/AS2 for communication security!

GoAnywhere MFT Overview



UP NEXT

Secure your front door!



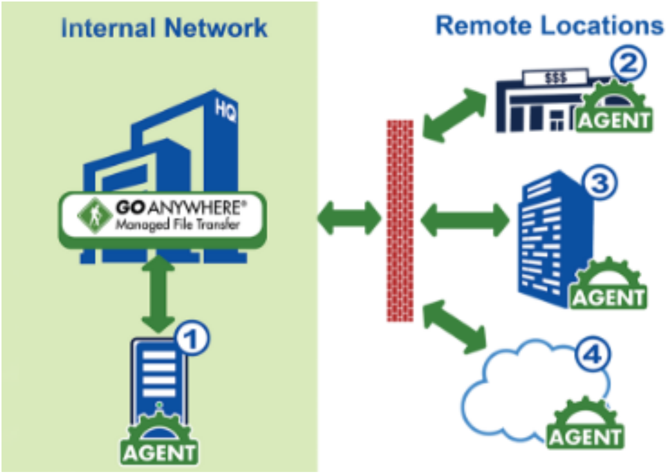
GoAnywhere MFT allows you to communicate securely through your DMZ using NO inbound firewall rules into your private network. Round-Robin load balancing to a clustered installation provides High Availability and faster throughput!

Alternatives to FTP (internal & external)

GO ANYWHERE® Managed File Transfer

Agents

- With GoAnywhere MFT agents, IT admins can:
  - Enjoy centralized control of remote file transfers and workflows
  - Create Agent Templates with registration rules to easily deploy Agents on a large scale
  - Monitor remote locations for new, modified and deleted files on the system

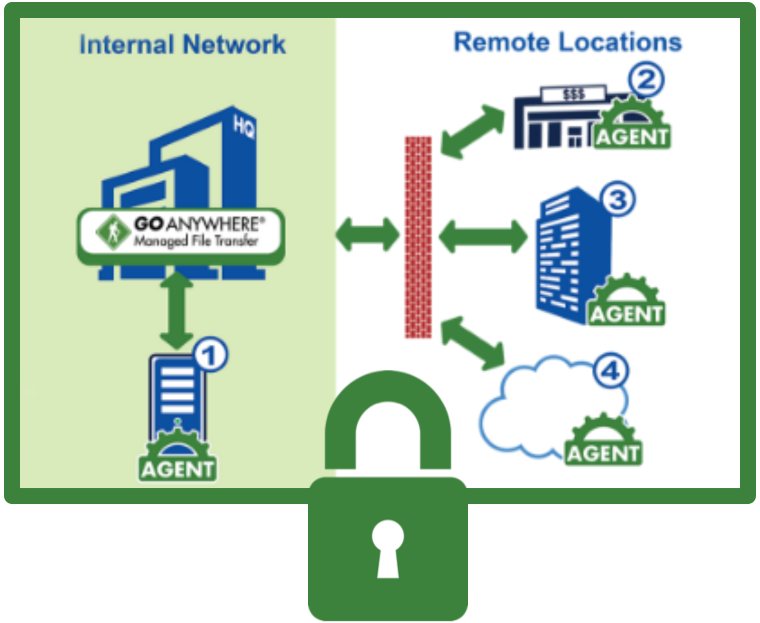


Alternatives to FTP (internal & external)

GO ANYWHERE® Managed File Transfer

Agents

- With GoAnywhere MFT agents, IT admins can:
  - Enjoy centralized control of remote file transfers and workflows
  - Create Agent Templates with registration rules to easily deploy Agents on a large scale
  - Monitor remote locations for new, modified and deleted files on the system



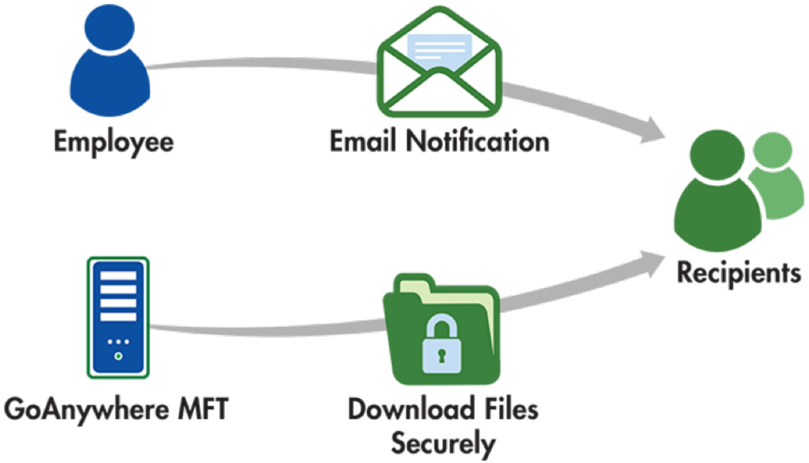
helpsystems

Alternative to secure data in Exchange

GO ANYWHERE® Managed File Transfer

Secure Mail

- The Secure Mail module in GoAnywhere MFT allows your employees to send messages and files as secure "packages" on an ad-hoc basis.
- Recipients will get an email with a unique link to each package, allowing them to download the message and files through a secure HTTPS connection. This is a great alternative to regular email since there are no file size or file type restrictions.

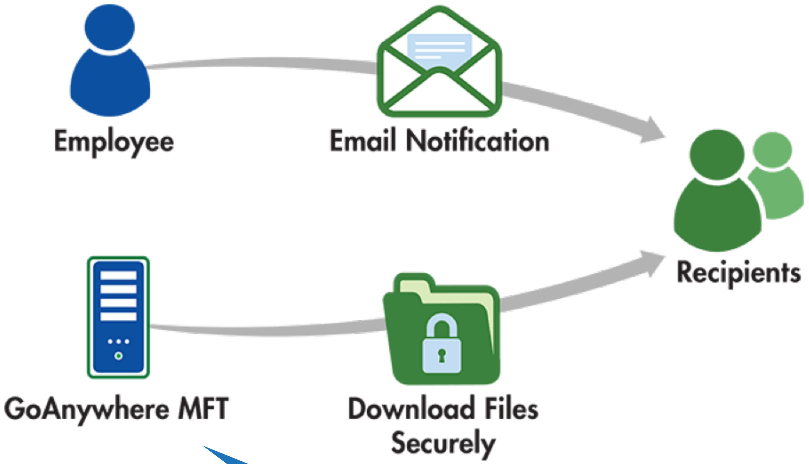


Alternative to secure data in Exchange

GOANYWHERE® Managed File Transfer

Secure Mail

- The Secure Mail module in GoAnywhere MFT allows your employees to send messages and files as secure "packages" on an ad-hoc basis.
- Recipients will get an email with a unique link to each package, allowing them to download the message and files through a secure HTTPS connection. This is a great alternative to regular email since there are no file size or file type restrictions.



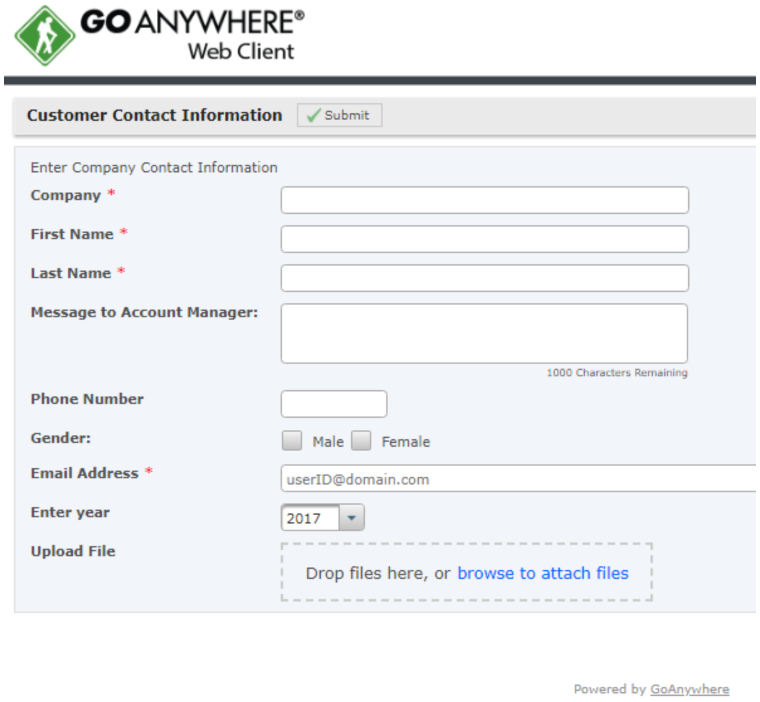
Includes Outlook Plugin!

helpsystems

Alternatives to FTP

Secure Forms

- Secure Forms allow end-users to fill out custom forms with one or more input values and (optionally) upload files through the HTTPS Web Client in GoAnywhere, or submit forms by making SOAP or REST requests from your custom built applications.
- When a form is submitted, a Project in GoAnywhere is executed to automatically process the submitted values and files.



GO ANYWHERE®
Web Client

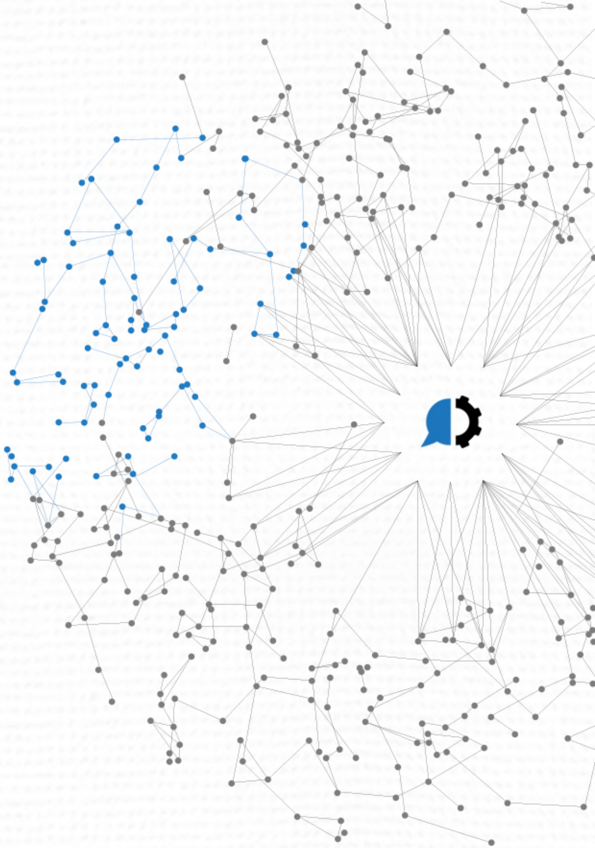
Customer Contact Information ✓ Submit

Enter Company Contact Information

Company *	
First Name *	
Last Name *	
Message to Account Manager:	1000 Characters Remaining
Phone Number	
Gender:	□ Male □ Female
Email Address *	userID@domain.com
Enter year	2017 ▾
Upload File	Drop files here, or browse to attach files

Powered by GoAnywhere

Question & Answer



UP NEXT

Thank you for joining us!

New to GoAnywhere? Download our free 30-day trial at www.goanywhere.com/trial.

Contact us with any questions!

- goanywhere.sales@helpsystems.com
- Toll-free 1-800-949-4696
- Direct (402) 944-4242