

**GO ANYWHERE<sup>®</sup>**  
Managed File Transfer

## How to Prevent Data Breaches with GoAnywhere

[www.goanywhere.com](http://www.goanywhere.com)



**Dan Freeman**

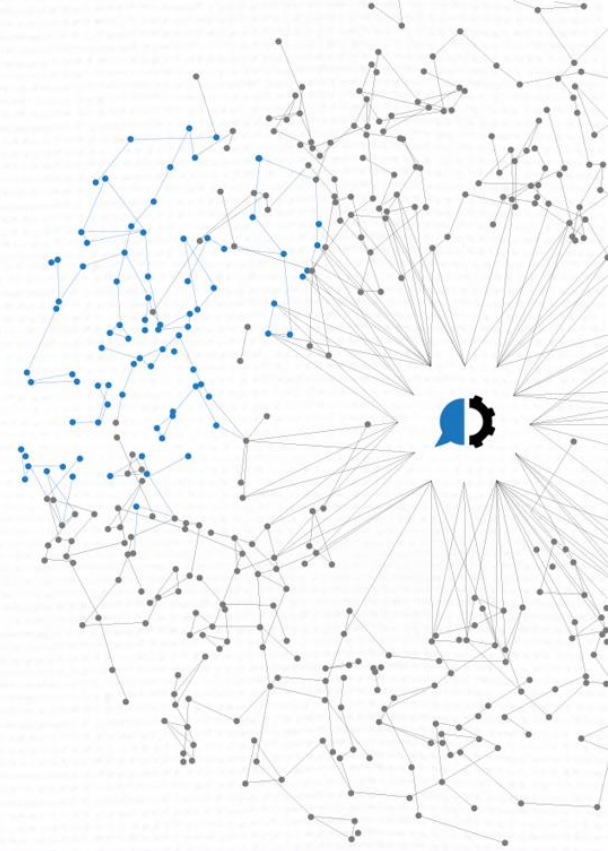
*Senior Solutions Consultant, CISSP*

**HelpSystems**



## Agenda

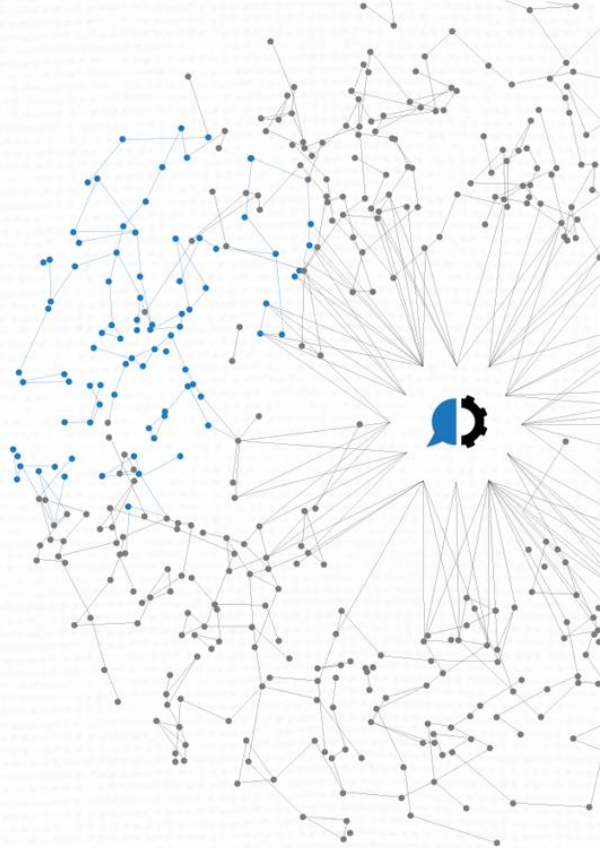
1. The risk of data breaches
2. How can managed file transfer help?
3. Live GoAnywhere demo
4. Q&A



UP NEXT

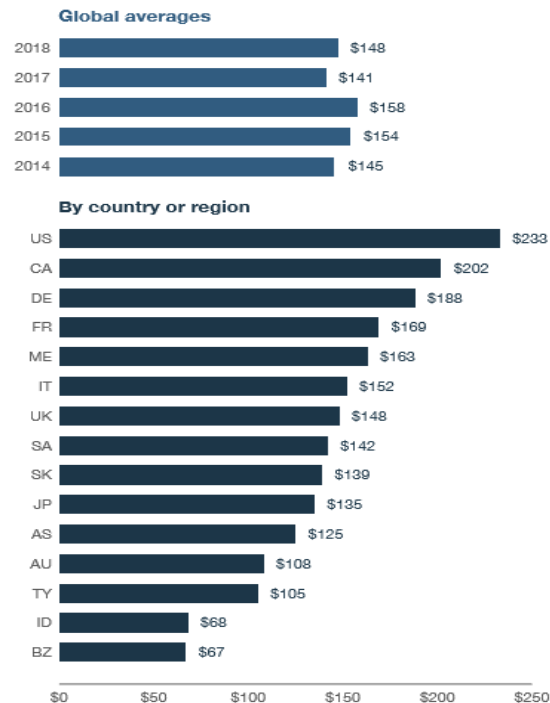


# The Risk of Data Breaches



UP NEXT

- ▶ The consolidated average per capita cost for all samples was \$148 compared to an average of \$141 last year.
- ▶ The United States, Canada, and Germany continue to have the highest per capita costs at \$233, \$202, and \$188, respectively.
- ▶ Turkey, India, and Brazil have much lower per capita costs at \$105, \$68, and \$67, respectively.



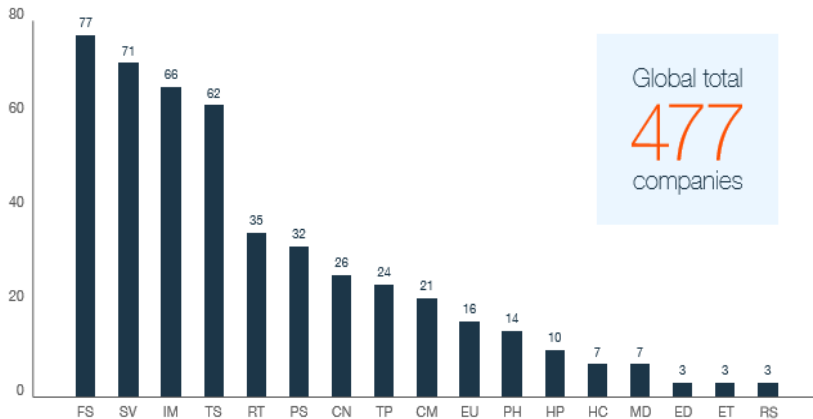
# Cybersecurity Statistics – Cost

## Frequency of Data Breaches by Industry

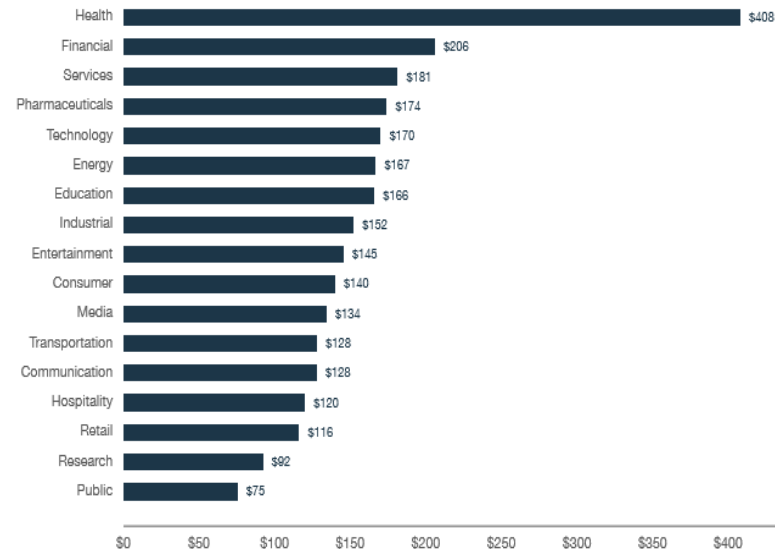
### ► Per Capita Cost by Industry

- > FS – Financial Services
- > SV – Services
- > IM – Industrial Manufacturing
- > TS – Technology
- > RT – Retail
- > PS – Public Sector
- > CN – Consumer
- > TP – Transportation
- > CM – Communications
- > EU – Energy
- > PH – Pharmaceuticals
- > HP – Hospitality
- > HC – Healthcare
- > MD – Media
- > ED – Education
- > ET – Entertainment
- > RS – Research

Figure 3. Frequency of benchmark samples by industry

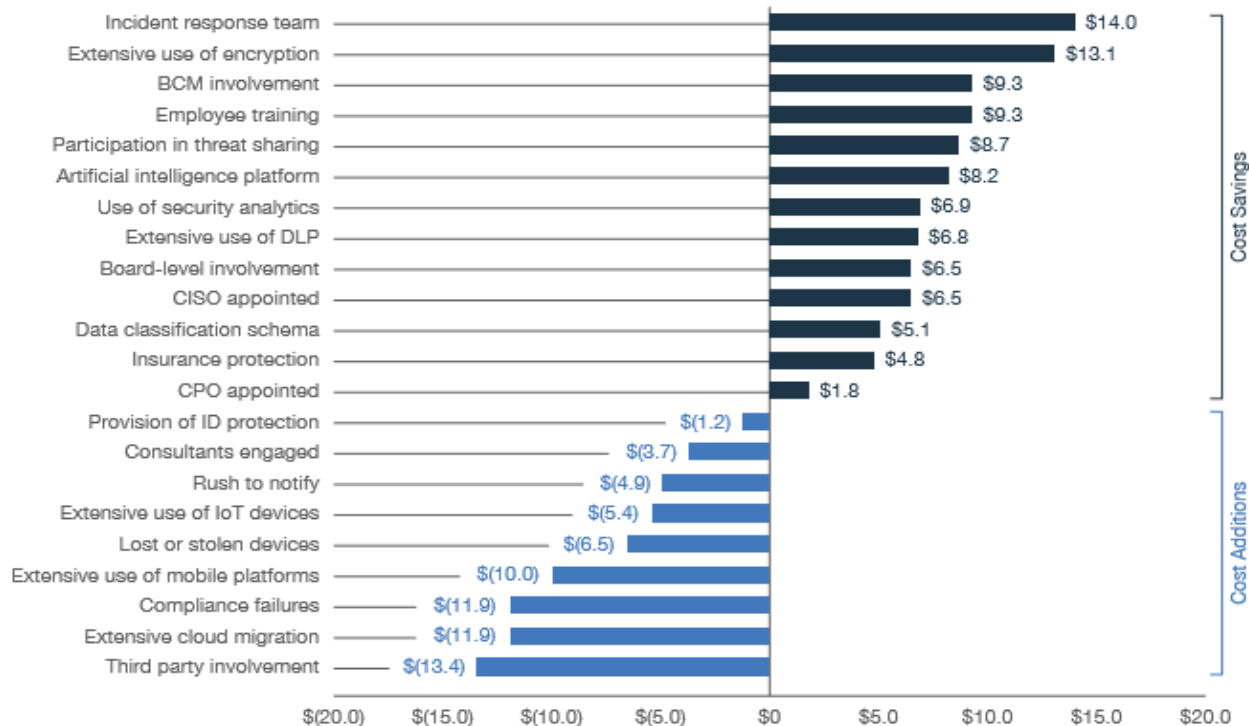


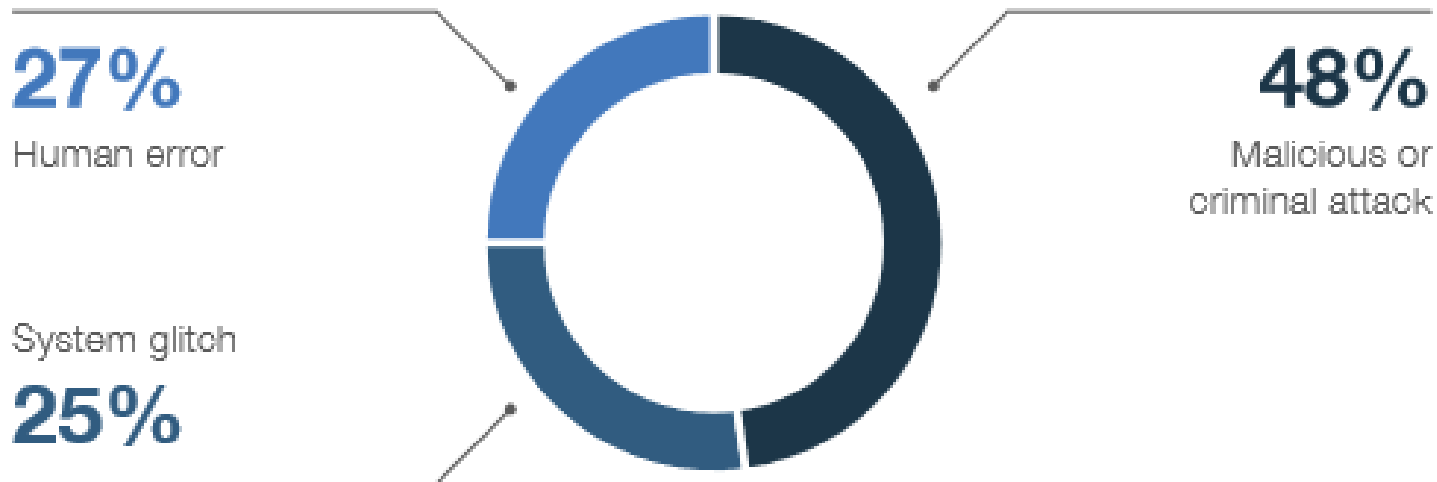
Measured in US\$



# Cybersecurity Statistics – Cost

Measured in US\$








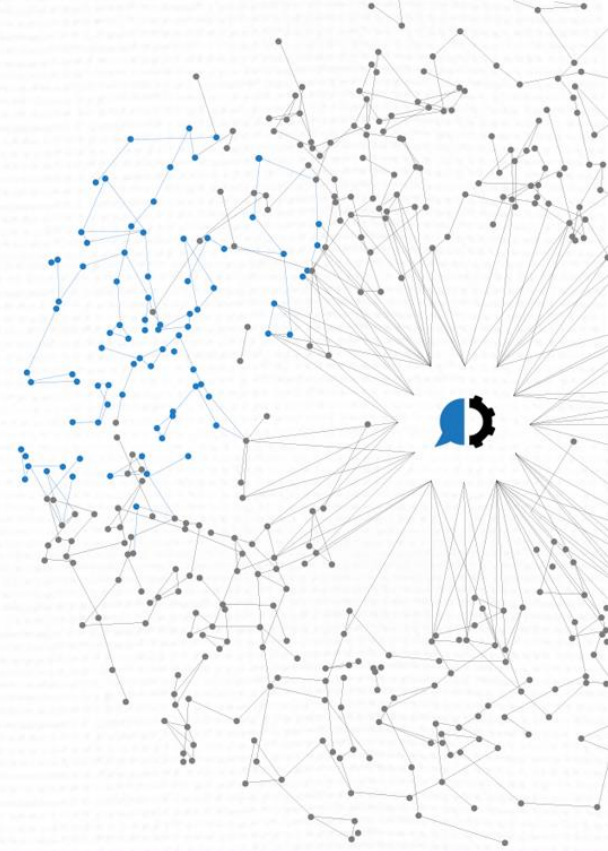
# Cybersecurity Statistics – Key Findings

- ▶ Global cost of data breach increased in 2018
  - ▶ 6.4% total cost, 4.8% per capita, 2.2% size (number of records)
- ▶ Average cost of data breach – 3.8 million
- ▶ Hackers and insider threats comprised 48% of total breaches
- ▶ Faster breach can be identified, lower the costs
  - ▶ Mean Time To Identify (MTTI) – 197 days
  - ▶ Mean Time To Contain (MTTC) – 69 days
  - ▶ Both MTTI/MTTC were highest for malicious/criminal attacks vs. human error
- ▶ Third-party involvement cost increase
  - ▶ Cost increased by \$13 per compromised record
  - ▶ Those undergoing cloud migration saw increase by \$12 per record
- ▶ Loss of customer trust = loss of customers = loss of “bottom line”





## How can managed file transfer help?



UP NEXT

# How MFT Helps Prevent Data Breaches



## **Encryption**

Encrypt sensitive data in transit and at rest, server-to-server, user-to-system, and person-to-person.



## **Alerting**

Get alerted automatically when files process or triggered events (e.g. upload, download) occur.



## **Automation**

Create automated workflows to achieve end-to-end automatic encryption and file transfers.



## **Audit and Access**

Detailed audit logging and granular access controls for clear insight into user activities.



01

## **On the move**

Apply encryption in transfer using the latest ciphers and protocols.

02

## **At rest**

Utilize AES 256 bit encryption at rest or protect via OpenPGP.

03

## **Manage your encryption keys**

Database-driven KMS for certificates, SSH, and PGP keys.

04

## **Master encryption key(s)**

Leverage AES 256 bit encryption for GoDrive, Secure Mail, Secure Folders, and Encrypted Folders. Rotate as needed.



01

## **System alerts**

Specific system events and thresholds.

02

## **Triggered events**

Web user events able to apply desired “action” depending upon set conditions defined.

03

## **Project logic**

SMS or SMTP alerting on success/failure or conditional processing.

04

## **Built-in alerts**

Scheduler and Monitors (coming soon: SLAs).



01

## Projects

Business function created by selecting certain action or task items to carry out data manipulation and/or movement.

02

## Scheduler

Kick off projects on time table. Built in repeat options for retries upon success, failure, or conditional logic.

03

## Monitors

File system monitoring for certain file types and actions to pass filelist to project.

04

## Triggers

Multitude of file system actions as well as able send email alert, kick off native commands, or call Projects.

05

## API

GoAnywhere Command lets via script or webservice calls via SOAP or REST.



01

## **Administrative RBAC**

Maintain job separation of duties and least privilege with unique roles for specific admin access.

02

## **Multi-factor authentication**

Both for web and admin users. Option for MFA on all service listeners.

03

## **Built-in accounts disabled**

Forced admin user creation upon first login.

04

## **Detailed logging**

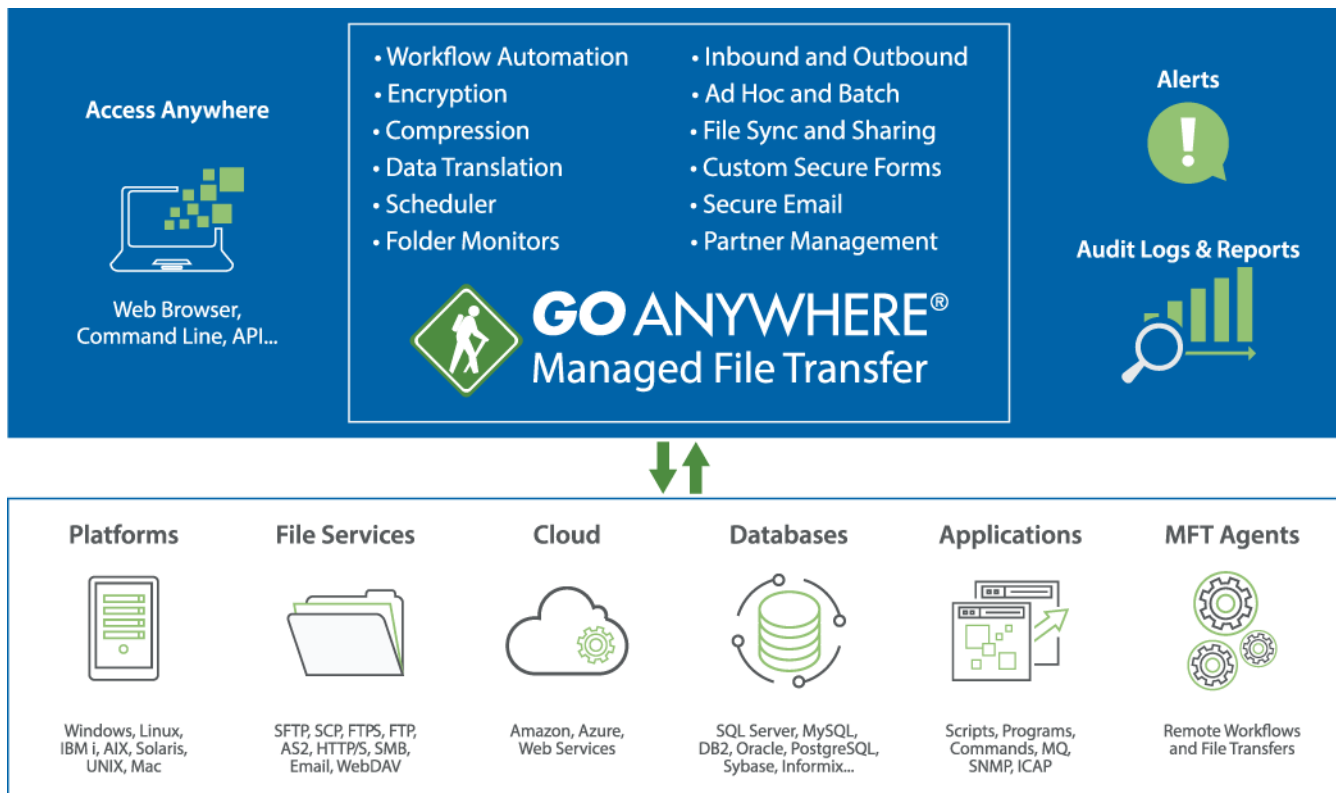
Logs on all service listeners, protocols, admin, and web user activities. File audit logs for insight into file activities.

05

## **Syslog options**

Ability to leverage a central syslog server to pass all logging events.

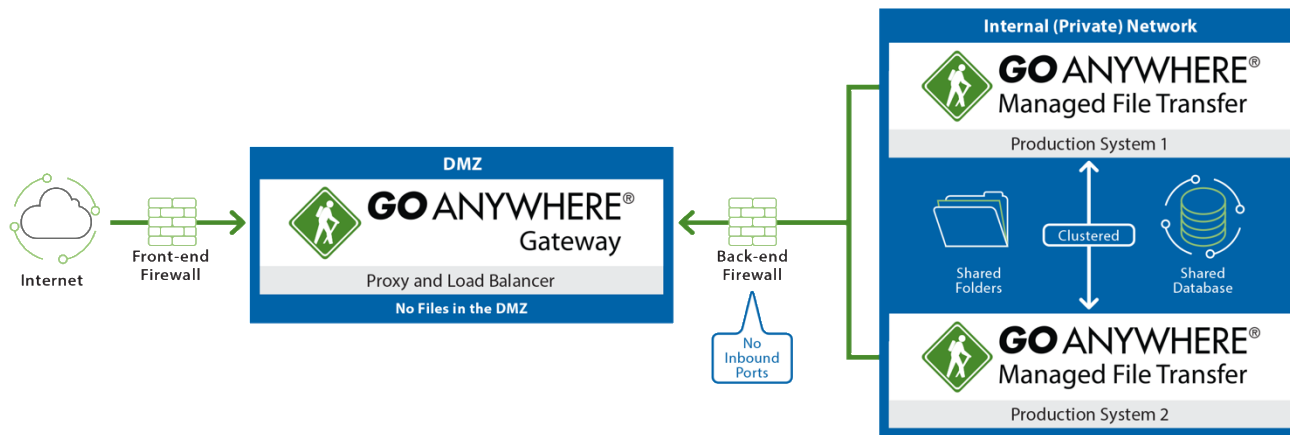
# GoAnywhere Overview





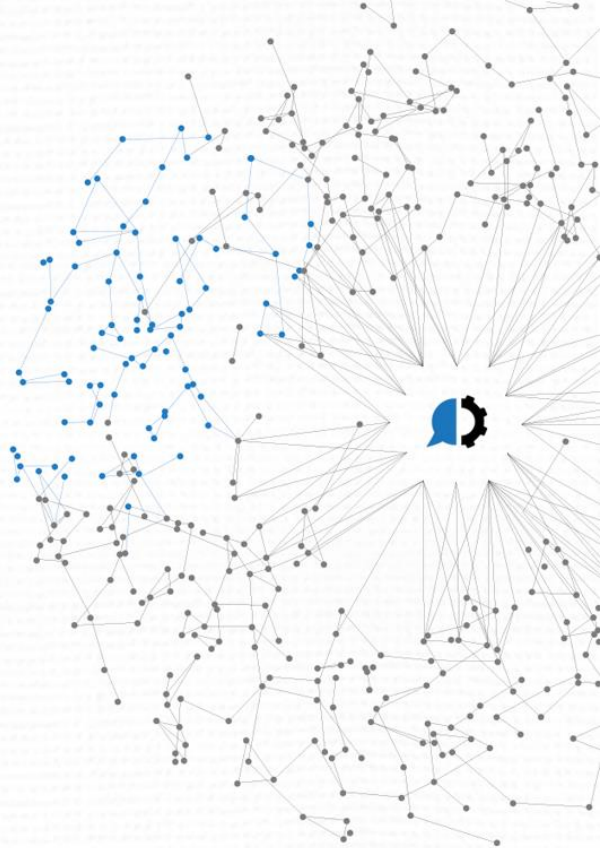
# DMZ Secure Gateway

- ▶ No incoming ports are opened into the private (internal) network.
- ▶ No sensitive files are stored in the DMZ.
- ▶ User credentials are maintained/stored in the private network.
- ▶ Gateway supports FTPS, SFTP, SCP, and HTTPS file transfer protocols.
- ▶ No special hardware components. This is a software-only solution.





# Live GoAnywhere Demo



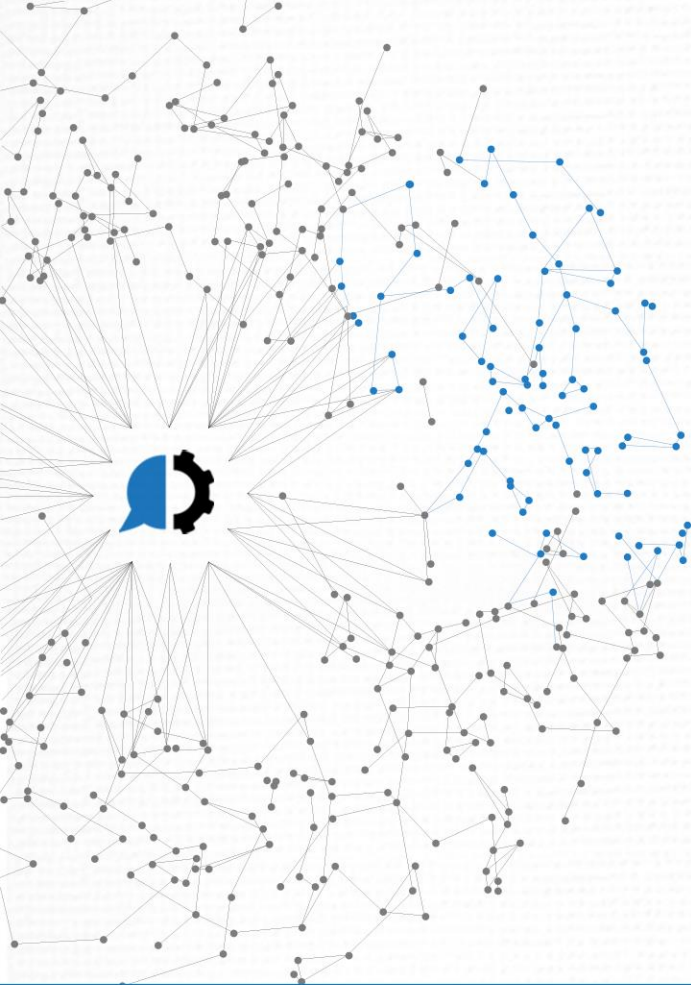
UP NEXT

# Thanks for joining us!

What's next?



- ▶ **Fill out the survey that pops up after the webinar.**  
We'd be happy to answer your questions and would love your feedback!
- ▶ **Go deeper with a custom GoAnywhere demo.**  
Request yours at [www.goanywhere.com/demo](http://www.goanywhere.com/demo)
- ▶ **Let us know how we can help you.**
  - ▶ [dan.freeman@helpsystems.com](mailto:dan.freeman@helpsystems.com)
  - ▶ [goanywhere.sales@helpsystems.com](mailto:goanywhere.sales@helpsystems.com)
  - ▶ USA and Canada: 1-800-949-4696
  - ▶ Outside the USA: 1-402-944-4242



Any  
Questions



[www.goanywhere.com](http://www.goanywhere.com)