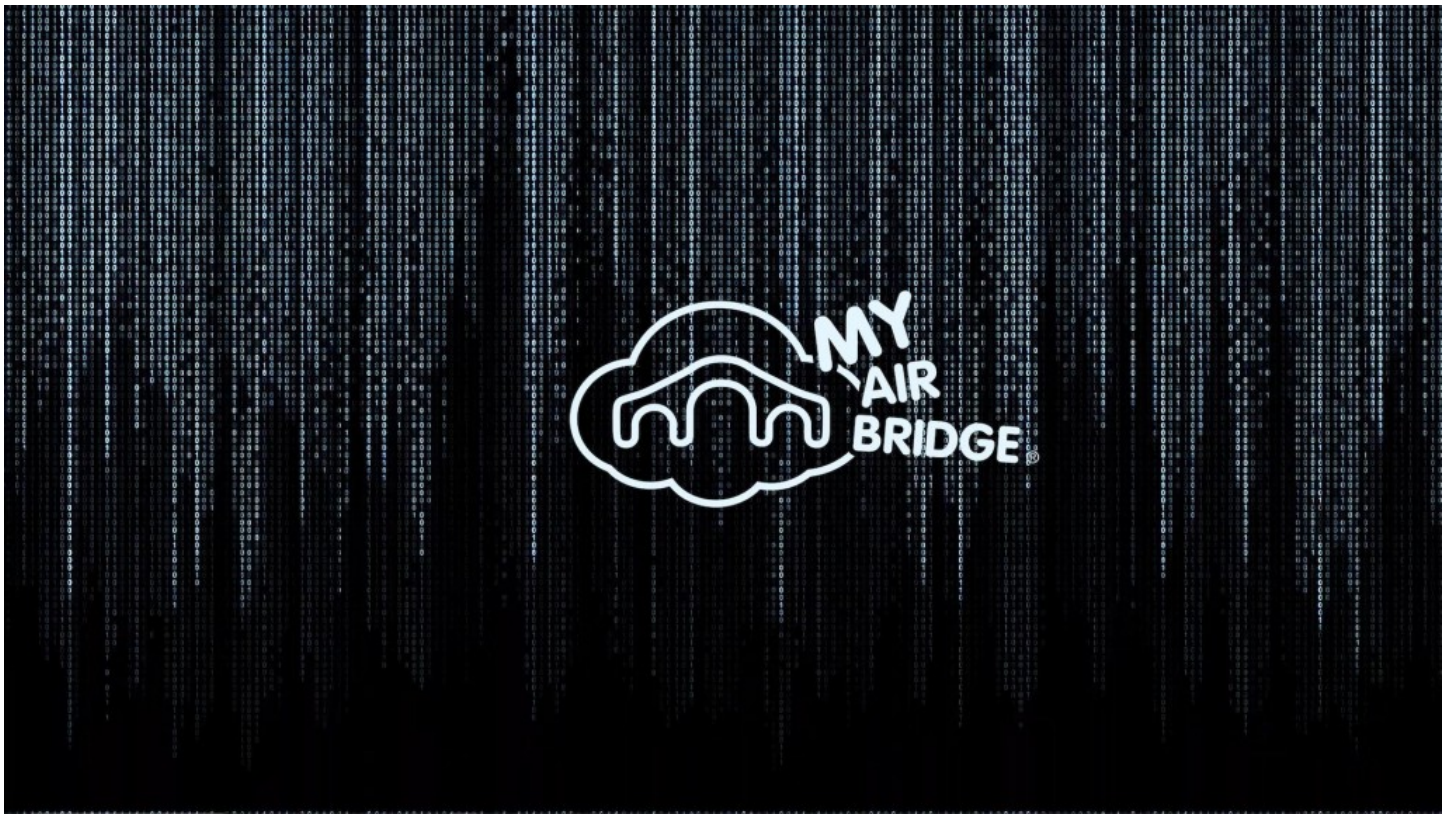
File transfer & file sharing service with a strong end-to-end encryption



England, London, Mar 16, 2021 (Issuewire.com) - Strong end-to-end encryption for online data transfers up to 100 GB per single transfer (and even more). MyAirBridge.com can provide exceptional data security. Users love it for its versatility and simplicity, and the improved security measures bring the app to the top.

MyAirBridge, founded in 2013, is a file transfer service, file sharing service, and cloud storage with headquarters in London and Prague. For the last few years, it's been one of the leading cloud apps, mainly thanks to its versatility and security.

The app offers a perfect middle ground between direct data transfers and online storage, and both of these platforms are interconnected into one functional unit. It offers possibilities for users who are looking for an efficient data transfer tool for free, and for users who need to work with data on a professional level. Thanks to that, MyAirBridge is being used even by prestigious brands like Disney, Reuters, Viacom, Virgin Media, and Warner Brothers.

But where MyAirBridge really stands out from its competitors is its great focus on data security.
The app offers the highest possible encryption A+ for data transfers. In addition, it offers its users the ability to secure their transfers with a password. As of this year, MyAirBridge also added new improved security measures to keep their users' data perfectly safe.

The app now allows the use of end-to-end encryption. This kind of encryption secures the data against

eavesdropping by the administrator of the communication channel and also by the server administrator in charge of the server through which users communicate. Thus, even the server administrator cannot eavesdrop on client communication that the server mediates.

The users can choose their own password or have a strong password automatically generated by the app. The password must then be sent to the other party - the recipient of the data. A random variable - called "salt" - is added to the design of the key, so that it is difficult to break the password. Salt is a randomly generated 128-bit content sent to the PBKDF2 derivation function. There, with the help of 100,000 iterations, it creates a master key that has 256 bits. In this way, a master key is generated.

Subsequently, the original data is encrypted with the master key using the AES-GCM encryption algorithm. Advanced Encryption Standard is a standardized algorithm used to encrypt data in computer science. It is a symmetric block cypher that encrypts and decrypts data divided into blocks of a fixed length with the same key. It is used, for example, for wireless Wi-Fi networks within the WPA2 security that follow the IEEE 802.11i standard.

This creates encrypted data. All this takes place only in the sender's browser and the opposite process in the recipient's browser. No one else, not even the communication channel administrator or the server administrator, can access the password, master key, or the original data.
For users that are looking for a versatile yet simple app with exceptional data security, MyAirBridge is a perfect choice.

Contact: Hanka Zykova
PR manager MyAirBridge.com
London/Prague
pr@myairbridge.com
www.myairbridge.com

Media Contact

MyAirBridge.com

pr@myairbridge.com

07914615616

9 Chapel Place, 2nd Floor

Source : MyAirBridge.com