maytech
ONLINE BUSINESS SOLUTIONS

FTP-Stream : Security & Confidetiality Statement

Maytech provides FTP-Stream service to a diverse range of organizations including Fortune 500 companies and government agencies worldwide who entrust FTP-Stream wih confidential data and mission critical processes.

Maytech recognize the importance of confidentiality and security when handling sensitive customer data. This document outlines our security arrangements and confidentiality policy.

Physical Security

Maytech servers are located in private suites at Redbus Interhouse, London E14, NAC Cedar Knolls NJ, USA and HK Tech, Hong Kong. The buildings benefit from strong physical and electronic security, uninterruptible power and fire suppressant systems.

Firewall

The Maytech networks are protected by a stateful packet inspection firewalls.

All ports, other than those required for the provision of service are closed.

Operating Systems

The FTP service runs on Sun Enterprise T5120 servers running the Solaris operating system – widely regarded as the most secure O/S available. Servers are automatically updated from Sun with all available security updates

Administrative Access

Only two people at Maytech hold the root passwords for the servers. Regular password changes are enforced.

Customer Access

Customer data is held in virtual private servers or ZFS filesystems that are completely isolated. Customer access is restricted to the service protocols purchased, we do not allow access by other protocols such as SSH or telnet.

Encryption

Control panel access is over HTTPS, this traffic is therefore encrypted. Customers can subscribe to the Encryptions module which provdes encrypted file transfers using FTPS, SFTP, and HTTPS.

External Threats

Maytech take all precautions against external threats. Our network is fully protected by stateful packet inspection firewalls, we operate a number of techniques to protect against malicious attacks such as Denial of Service Attacks.

Confidentiality

Each customer's data resides in a dedicated ZFS filesystem and can never be visible to any unauthorized party. Additionally, within each account, data for each FTP login is invisible to other logins unless in a shared folder.

Maytech will never disclose any data to a third party. Maytech will never view or download your data unless instructed by you do so.

Data Persistence and Backups

Although Maytech provide a high-availability service using duplicated RAID arrays, filesystem snapshots and failover clusters, we do not keep permanent or incremental backups of customer FTP data File deletes are permanent there are no persistent copies of the data.

Further Security Measures

To meet regulatory or other demands you may need to show extra care in data security and integrity. Consider end-to-end encryption using PGP or other strong encryption technology. Some FTP software including CuteFTP Professional has built-in support for public key encryption.

Revised March 2008