Version: 2.0

Maytech Resilience and Uptime Statement

January 2018
Author: Maytech

maytech
GLOBAL DATA TRANSFER

Maytech's products are used by business and public service worldwide for business critical operations and as such is designed for high volume and high availability. This document outlines the infrastructure and policies adopted to provide high availability and disaster recovery.

Server centers

Maytech services are provisioned from eleven global hubs: hubs in Europe, the USA, UAE, Australia, West and South Asia. On signup, customers select a service hub and data is never transferred or replicated outside the chosen hub.

All data centers benefit from strong physical and electronic security, uninterruptible power and fire suppressant systems.

Connectivity

At all data centres we take feeds from multiple transit providers. In the event that one provider's service is down or degraded our gateway routers automatically reroute traffic through an alternative link.

Hardware

Maytech products run on enterprise grade hardware. Servers operate in fully redundant failover clusters.

Operating systems

Servers run the Linux operating system selected by enterprise, government and telcos worldwide for unrivalled stability and security. Updates and security patches are applied daily.

Monitoring

Service is monitored by over 100 monitoring daemons continuously probing for fault conditions at levels ranging from basic hardware health to emulated file transactions. Ports are monitored for suspicious activity such as password scams or DoS attack. The duty engineer is immediately alerted of any error condition.

Data security and backup

Customer data is stored over multiple drives and devices. The storage arrays are configured as RAID 6 which means that several drives would have to simultaneously fail to compromise data integrity. Furthermore each RAID array is synced to a secondary array. The probability of data loss through hardware failure is infinitesimally small.

Maytech retain onsite snapshots of customer data for 28 days. Any files accidentally deleted over this period can be restored. We do not keep enduring incremental backups or offsite backups of customer data.

Uptime

It is rare that we need to bring the service down for upgrade or maintenance. If necessary this would take place at the weekend with 5 days warning. The uptime average for 2017 is 99.98%.

Disaster recovery

In the event of a disaster which prevents us from offering service from one of our data centers we would be in a position to quickly resume service from an alternative facility.