Hosting, Data Management and Security

The core Mобензи platforms are professionally hosted and managed by Amazon Web Services (AWS) in a highly secure Virtual Private Cloud (VPC) environment.

Hosting

Our engineers have spent years refining the Mобензи hosting environment. AWS operates highly scalable cloud infrastructure which includes hardware, software (such as the operating system and data storage) and networks upon which the Mобензи platforms run. Servers are hosted in private subnets where security group filters and network access control lists (ACLs) are utilised within a VPN environment to ensure your data is safe.

According to Gartner, Amazon is the world leader of Cloud Infrastructure as a Service (IaaS) and boasts an impressive list of clientele including organisations like NASA. A collection of case studies is available which highlight the benefits and successes of AWS.

Hosting Environment Security

As a Mобензи customer, you can be assured that we host our systems on top of some of the most secure computing infrastructure in the world. Our primary data centre is professionally hosted and managed by Amazon Web Services (AWS).

The AWS infrastructure is designed and managed according to security best practices and compliance standards. The

Mобензи hosting environment within AWS has multiple additional levels of security including general user access rights, specific host firewall rules and host lockdown. Access to the environment other than through the application platforms we offer is only possible via whitelisted IP addresses through a specific VPN and additional Windows domain authentication.

Application Security

Mобензи Researcher supports granular permissions control which can be used to limit data access and editing rights in addition to many other system privileges. Modifications made via the web console to captured submissions are audited automatically, storing original value, timestamp and user who modified the submission. Completed surveys are periodically uploaded and removed completely from fieldworker devices once the server acknowledges receipt. This limits the amount of data present at any given time on a device. If in an area with coverage, completed surveys are uploaded and removed approximately every 60 seconds. Data are encrypted in transit using transport layer security (TLS) which is most commonly referred to as Secure Sockets Layer (SSL).

In addition to the standard Android OS access controls, Mобензи Gateway can be used to implement additional security protocols on the device including remote wipe, local encryption and PIN or biometric authentication.

Data Centre Availability

AWS data centres are organised into Availability Zones and Regions. Regions are dispersed and located in 7 separate geographic areas around the world. Availability Zones are distinct locations within a region that are engineered to be isolated from failures in other Availability Zones.

The Mобензи platforms are hosted in the Ireland region using the Amazon Elastic Compute Cloud (Amazon EC2) service. For security reasons, specific details regarding the data centre’s location are not divulged. Amazon certifies that it adheres to the Safe Harbor Privacy Principles agreed upon by the US, the European Union and Switzerland, respectively.

Amazon EC2 offers a highly reliable environment where replacement instances can be rapidly and predictably commissioned. The service runs within Amazon’s proven network infrastructure and data centres. The Amazon EC2 Service Level Agreement commitment is 99.95% availability (per service year) for each Amazon EC2 Region. The Amazon S3 Service Level Agreement commitment is 99.9% (per month). Beyond AWS infrastructure and service availability, Mобензи’s systems and operational teams ensure that the applications and services running in EC2 are available. Automated monitoring systems immediately notify engineers of system failures or outages.

Data Redundancy (Backups)

Mобензи has redundant systems situated in other Availability Zones to mitigate the complete failure of a region.

Multiple backup strategies are in place to mitigate partial and complete data loss events. A full backup of the database is performed once a week, differential backups every 24 hours, and transaction log shipping backups every 10 minutes. All backups are stored in Amazon Simple Storage Service (S3) and encrypted with a 256 bit key. A full snapshot of the servers are taken every 24 hours.

Mобензи Support

Mобензи staff never access user-provided data, except where granted permission by an authorised user - and typically only to provide support or assistance.

Mобензи staff with access to user-provided data are bound by contractual confidentiality and non-disclosure agreements. Access to user-provided data by Mобензи staff is controlled and audited by automated systems. Mобензи staff are only able to access selected user-provided data via authorised computer terminals and access from these terminals may be terminated at any time.

Footnotes

1 http://aws.amazon.com/whitepapers/Gartner_MQ_OCT_2012/
2 http://aws.amazon.com/solutions/case-studies/