Questionmark takes security seriously and operates trustable, scalable and robust OnDemand Solutions for managing and delivering assessments. Questionmark OnDemand, which contains multiple layers of security including physical safeguards, access control, environmental management and an uninterruptible power supply, is protected by firewalls to appropriately allow and restrict access.

This document lists some of the key security features of Questionmark's OnDemand Service to allow you to compare it to other services

	Questionmark OnDemand	Competitive Product
Data Centre		
ISO 27001 and 9001 accredited Data Centre	Yes	
Data Centre PCI DSS v1.2 Compliant	Yes	
Two-factor authentication for staff and visitors	Yes	
24/7 personnel intrusion alarms	Yes	
24/7 monitored digital surveillance cameras	Yes	
24/7 environmental and network monitoring	Yes	
N+1 redundant air conditioning system	Yes	
Data Centre conncted to 2 separate utility power grids	Yes	
Data Centre with diesel generators with 30 hours fuel under full load	Yes	
N+N 10-500 KVA UPS to ensure continuous steady flow of power	Yes	
Data Centre interconnected and peering with multiple Tier 1 and Tier 2 carriers	Yes	
Servers stored in locked steel cages/cabinets	Yes	
Data Centre in non-descript building to ensure anonymity	Yes	
Concrete bollards to impede access via outside impact	Yes	
Network security		
Browser traffic encrypted with SSL v3 (with SSL 2.0+ upgrade support)/TLS	Yes	
Redundant firewalls protect from Internet	Yes	
Host based firewalls protect each server	Yes	
Intrusion Detection System (IDS)	Yes	
Antivirus updated regularly	Yes	
Engineers connect via Bastion Host	Yes	
Virtualization used for rapid deployment and upsizing	Yes	
Application monitored 24/7 with immediate alerts	Yes	
Application status and recent uptime publicly visible	Yes	
Application security		
Separate Presentation, Business and Data tiers	Yes (participant software)	
Each customer's data protected from other customers	Yes	
SSO available for login via customer's systems	Yes	
All use of service logged	Yes	
Administrator/author capability controlled by permissions	Yes	
Administrator/author access controlled at topic level	Yes	
Able to set tests to only be taken at test centres	Yes	
IP address restrictions on administrator login	Yes	
Application development culture of security code reviews	Yes	
Automation of system configuration and updates for reliability	Yes	
Internal teams perform penetration tests on other teams's software	Yes	
Data Security Policy		
Formal Data Security Policy	Yes	
Background check on all new employees	Yes	
All employees sign confidentiality agreement	Yes	
All employees trained on data security	Yes	
All employees pass data security test annually	Yes	
Formal strong password policy enforced internally	Yes	
Customer data removed from Data Centre uses secure transfer and disk encryption	Yes	
Customer data removed from Data Centre tracked individually	Yes	
Hard drives degaussed or similar at end of life or swap-on-fault	Yes	
Service Continuity		
Multiple redundant Internet connections to ensure 99.9+% uptime	Yes	
All tiers use redundant load balancing for fault tolerance	Yes	
All power and networking elements have redundancy	Yes	
System updates performed without downtime	Yes	
Backups stored offsite and encrypted using AES 256	Yes	
Continuous online monitoring of uptime worldwide	Yes	
Customer online status portal	Yes	
Robust communication plan in place in case of disruption	Yes	
Emergency response team in place	Yes	
Disaster recovery plan in place	Yes	
Documentation and Support		
Documentation of security available (under NDA)	Yes	
Documentation: dozens of online product manuals and best practice guides	Yes	
Searchable knowledge base with 100s of articles	Yes	
Text/chat support worldwide	Yes	
VOIP support worldwide eliminating international calls	Yes	