Marchex

SECURITY AND TRUST

Next-level security for peace of mind

Meeting security requirements of many Fortune 500 companies

At Marchex, we put our customers first. We uphold high standards as the only conversation analytics company to exceed industry standards for reliability and maintain a comprehensive data security program designed to safeguard your data.

Protecting your business 24/7

Security

- Comprehensive multi-layered data security program
- SOC 2 Type II certified for security
- HIPAA compliant

Privacy

- TRUSTe verified
- EU-US Privacy Shield Framework compliant

Reliability

- Fraud Prevention blocking 90% of spam and robocalls with patented Clean Call® technology
- Cloud-based elastic computing capacity for scalable solutions
- 100% call infrastructure availability for 4 years and running
- 24/7/365 systems monitoring

SOC 2 TYPE II · TRUSTe VERIFIED · HIPAA COMPLIANCE · EU-US PRIVACY SHIELD

Encryption and Access Controls

Sensitive customer data is securely stored, and encrypted at rest (AES-256) and in transit (TLS 1.2 and above). Role-based access controls ensure that access to sensitive data is restricted to authorized customer users and relevant Marchex personnel.

Comprehensive and Dynamic Security Program

Marchex has implemented a comprehensive, multi-layered data security program that includes audited role-based access controls, encryption of sensitive data at rest and in transit, intrusion detection, and more.

Our security program includes:

- Physical security of all data processing facilities
- Comprehensive security policies and procedures
- Network and Platform security controls
- 24/7/365 systems monitoring
- Testing and auditing of all controls
- Corrective action and incident response plans

Data Center Security

- 24/7 permanently-assigned guard staff to manage interior and exterior security
- 360-degree cameras
- Current government-issued photo ID required for access
- Biometric palm scanner requiring ID card access and hand geometry measurements
- Retina scan access controls for restricted areas

Comprehensive Security Policies

- Criminal background check for all personnel
- Annual security awareness training for all personnel
- Annual risk assessments
- Change management controls
- Patch and vulnerability management controls

Local Device Security

- Lockout policy for unauthorized login attempts
- Complex password policy with expiration and history control
- Centralized profile and security management to protect data against viruses and malware

Network Security

- Virtual LANs for all environments
- Strict zone firewall policies restrict access to only essential protocol traffic
- Technical controls restrict data access to specifically-authorized users
- SSL 2048 bit encryption for client/server communication
- Secure FTP exclusively for client data

To learn more, visit marchex.com/security-and-trust

Platform Security

- Access controls that include robust user-permission model
- Flexible, yet strong, application-level password enforcement
- Data integrity controls

Service Operations Center

- Technical center is staffed, monitoring systems 24/7/365
- Service Operations Center staff are typically the first responders to any service/security issues
- Hands-on engineering support, as needed

Operations Security

- Active server health monitoring
- Comprehensive server logging
- Real-time log monitoring
- Intrusion Detection Systems (IDS)
- Penetration testing and vulnerability scans

Reliability Security

- N+1 configuration for all call infrastructure
- Virtualized server cluster with multiple hosts per service
- Multiple daily backups of all data in all client-facing environments

Marchex