PRODUCT DATA SHEET

GENESYS™

Genesys Cloud security

Keep your customers safe and operations secure

Benefits

- Safe customers — Safeguard the precious data that your customers trust you with when transacting with you.
- Safe operations — Keep your systems secure and run your operations without fear of compromising objectives.
- Easy compliance — Operate with confidence that you're in compliance with international standards and regulations.

Executive summary

It's important to maintain compliance with local and foreign regulations while staying ahead of potential threats from determined hackers. Failure to keep your data secure and operations in compliance can damage your business and your brand. Genesys takes a comprehensive approach to security and compliance of the Genesys Cloud platform, so you can sleep soundly knowing that your customers' data is safe, your operations are secure, and you comply with all applicable regulations and standards.

Proactive security
With tools and processes in place, our security experts proactively find issues before they affect customers.

Continuous monitoring
The right personnel and tools continuously monitor our real-time security conditions and take action, when needed.

Holistic risk management
Risk is managed through comprehensive policies and security controls for third-party vendors, disaster recovery, employee security awareness, cyber insurance and other programs.

Data protection

Genesys applications interact with cloud servers over Transport Layer Security (TLS) transmission to ensure the highest level of security. The TLS terminates only within the Genesys network.

- Sensitive data at rest is encrypted using AES-256; keys are encrypted with a regularly rotated set of master keys.
- Call recordings and screen recordings are encrypted using an individual customer key that can only be decrypted by the customer who owns them.
- Multi-tenant environment security is enforced with barriers and controls that keep your data completely separated, allowing secure access to your organizational data only.

Access control

Genesys authorized users access the cloud environment using multifactor authentication (MFA). All user activities are logged and monitored. Access by privileged users is reviewed periodically. Access permissions use the least-privilege principle and role-based access control mechanisms. These access controls ensure that only users with proper authority and legitimate business requirements are allowed access to your data.

Application security

Development teams are regularly trained on web application security; testing occurs throughout the software development lifecycle. Code for a release is subject to continuous ongoing testing and review using code scanning and penetration tests. These leverage resources and methodologies like Open Web Application Security Project (OWASP) and SANS Top 25.

Standards, certifications and regulations

We support high levels of compliance with many standards and regulations worldwide. In-house personnel continuously monitor the compliance landscape and work to stay ahead of what comes next. So far, Genesys Cloud customers have full compliance with the following:

SOC 2
Controls over security, availability and confidentiality

PCI
Protects customer card information

GDPR
Compliance with EU data protection laws

HIPAA
Protects health information

ISO 27001
Manages information risks

Privacy Shield
Compliance with US-EU and US-Switzerland data transfer requirements

ISO 27018
Code of Practice for Protecting Personal Data in the Cloud

California Consumer Privacy Act
Support for complying with California Privacy law through GDPR API

Resilient cloud services

Reliable and highly available service is a cornerstone of any cloud service offering. Genesys Cloud is architected to support thousands of customers and their users simultaneously, providing high availability. Genesys leverages Amazon Web Services (AWS) infrastructure to host software-as-a-service (SaaS)-based applications. Disaster recovery and business continuity plans are tested regularly to ensure maximum uptime.

Risk management

The entire Genesys Cloud ecosystem is thoroughly monitored and evaluated for potential risks. We then mitigate those risks according to impact and likelihood. The whole process is regularly tested and reviewed to guarantee it remains current. We also address common risks using the following methods.

- Security awareness — Our employees and contractors must pass security training; employees are required to recertify for security and compliance training on an annual basis.
- Vendor risk management — Key third-party vendors must complete a security assessment.

Key features

- People — Experts with a wide array of skill sets work proactively and reactively to ensure safety and compliance.
- Processes — Development procedures and best practices prevent vulnerable code from reaching production.
- Systems — Resilient architecture ensures that you can scale to meet changing demands and recover gracefully from failure.

ABOUT GENESYS

Genesys® powers more than 25 billion of the world's best customer experiences each year. Our success comes from connecting employee and customer conversations on any channel, every day. Over 11,000 companies in more than 100 countries trust our #1 customer experience platform to drive great business outcomes. Genesys on-premise and cloud solutions are built to be fluid, instinctive and profoundly empowering. Combining the best of technology and human ingenuity, we work the way you think.

Visit us at genesys.com or call us at +1.888.436.3797

GENESYS™